ISSN 2237-7409

ELEMENTOS

Revista de Ensino e Pesquisa em Classes, Operações e Propriedades de Estruturas Algébricas

Ano 2014

ELEMENTOS REVISTA DE ENSINO E PESQUISA EM CLASSES OPERACIONAIS E PROPRIEDADES DE ESTRUTURAS ALGÉBRICAS.
Rio Branco: Edufac, 2014 Anual. ISSN: 2237-7409 (on line)

Ficha catalográfica elaborada pela Biblioteca Central da UFAC.

B546e Elementos Revista de Ensino e Pesquisa em Classes, Operações e Propriedades de Estruturas Algébricas. – v. 2, n. 2 (jan./dez. 2014) – Rio Branco : Edufac, 2014.
94 p.

Anual
ISSN: 2237-7409 (on line)

1. Álgebra – Periódicos. I. Universidade Federal do Acre. II. Título.

CDD.: 512
CDU.: 512

Marcelino G. M. Monteiro CRB/11 - 258

Associação Brasileira das Editoras Universitárias

Editora da Universidade Federal do Acre

Revista
ELEMENTOS

COMITÊ EDITORIAL

Projeto Gráfico
Edufac

Revisão
Prof. Dr. José Ivan da Silva Ramos (UFAC)
Msc. Ormifran Pessoa Cavalcante (UFAC)

OBJETIVO E POLÍTICA EDITORIAL

A revista Elementos tem como principal intenção a divulgação dos estudos, pesquisas e relatos de experiências desenvolvidos sobre tópicos da Matemática ligados às Estruturas Algébricas, dentro e fora da Universidade Federal do Acre. Como forma de resgatar pensamentos e práticas de ensino uma seção de cada edição da revista é composta de uma entrevista com educadores experientes.

A publicação dos textos ou artigos, de autoria individual ou coletiva, é feita dentro de um padrão técnico de qualidade editorial, como forma de promover a produção intelectual – acadêmica e científica.

Apresentação

A idéia de criação da revista Elementos nasceu da necessidade da divulgação dos trabalhos realizados pelos membros do Grupo de Ensino e Pesquisa em Classes, Operações e Propriedades de Estruturas Algébricas (GEPCOPEA), grupo de pesquisa cadastrado do CNPq, desde o ano de 2009.

De início, apostando também na nacionalização e, posteriormente, na internacionalização de suas matérias, evitamos especializá-la em uma única temática como percebemos nas muitas revistas que primam pela qualidade editorial e pelo nível daquilo que publicam. Isso pode significar para esta revista algumas reformulações, inclusive na sua política editorial, durante os primeiros anos de sua existência.

A permissão para publicações de experiências no uso de objetos matemáticos abstratos ou não, ligadas à política de ensinamentos, tem a intenção de encorajar mais pessoas a se lançarem na maravilhosa arte de escrever Matemática, inclusive sob forma de uma narrativa que socialize metodologias e conhecimentos.

Submissões de textos fora de um padrão científico serão evitadas. Assumimos assim o risco de que um Matemático anônimo e inexperiente, mas com uma brilhante idéia, deixe de usar o espaço de nossa revista para divulgá-la. Atenuamos esse problema insistindo na divulgação das edições lançadas e na disponibilização de chamadas regulares para publicação.

O fato de o conselho editorial ser composto por pesquisadores de diversas Instituições de ensino, especialmente os Consultores ad hoc, permite que tanto a comunidade acadêmica quanto os membros do comitê editorial local possam se submeter aos critérios de uma chamada para publicação, sem que seja ferida a imparcialidade e a transparência no aceite de uma matéria a ser publicada.

O comitê editorial é soberano na escolha de suas entrevistas e informativos, publicando o que julgar pertinente à cada edição. Em contrapartida, deverá fazer suas escolhas respeitando a proposta de criação desta revista, primando pela regularidade anual de suas edições e pela valorização de seus leitores.

Por se tratar de uma revista eletrônica, muitos autores, sob a luz de pareceres favoráveis, podem contribuir regularmente com suas edições, submetendo para análise seus relatos de experiências e artigos científicos.

Revista
ELEMENTOS

Editorial

Caros Leitores: é com alegria que apresentamos a quarta edição da revista Elementos. Neste número, temos a satisfação de trazer ao vosso conhecimento uma entrevista com professores que, a nosso ver, foram fundamentais para o ensino e divulgação da matemática no município de Rio Branco. Nesta conversa, são contadas suas histórias de vida e de como ingressaram na arte de ensinar Matemática. Infelizmente, alguns desses professores não puderam comparecer por motivos diversos. Ressaltamos que tentamos realizar a entrevista com o Professor Ezi Santos, no entanto, ele se encontrava com sério problema de saúde e, antes do término desta edição, veio a falecer. Ficam a nossa eterna gratidão e homenagem a esse tão importante professor e a tantos outros que, como os que foram mencionados em nossa entrevista, foram os precursores do ensino de Matemática em nosso Estado.

Além dessa entrevista, são apresentados artigos e relatos de experiência relacionados à matemática pura, frutos de reflexões sobre temas abordados no dia a dia da docência. Um desses artigos é proveniente de uma dissertação de mestrado vinculada ao Profmat, o mestrado profissional em matemática, e outro é consequência de uma orientação no PET "conexões de saberes", programas vinculados ao CCET, Centro de Ciências Exatas e Tecnológicas da Ufac. Isso mostra que a revista Elementos está realizando, na medida do possível, o seu papel de divulgação das ações realizadas pelo CCET inerentes à Matemática.

Para finalizar, disponibilizamos uma nota histórica, relacionada ao importante matemático Leonhard Paul Euler, bem como um momento de descontração, evidenciado por um conto.

Desejo a todos uma boa leitura.

Sérgio Brazil Júnior
(Professor Associado 3 do CCET/Ufac)

Sumário

Revista
ELEMENTOS

Entrevista

Professora Maria Auxiliadora de Oliveira Silva

Falando Livremente

Eu nasci em Xapuri, em 1949, e lá eu comecei os meus estudos. Em 1967, nós viemos para Rio Branco, morar no bairro Seis de Agosto. O meu dom toda vida foi ser professora. Eu nasci para ser professora. Neste mesmo ano, eu fui apresentada ao Governador Jorge Kalume por meu Pai de criação que era compadre e amigo dele. Com a indicação e a afirmação do Governador de que eu estava empregada, eu fui me apresentar para Flavia de Barros Pimentel, secretária de Educação, à época. Já me chamando de Chuchu, nome pelo qual sou conhecida no município de Xapuri, me disse "você já está empregada". Você vai trabalhar na Escola Maria Angélica, no turno da noite, e vai ensinar história e matemática.

Cheguei a minha casa e comecei chorar, porque eu não era boa aluna em matemática. Em Xapuri, da sexta para a sétima série eu passei na recuperação. Pensei! Deus meu, como vou ensinar matemática? A Solonir, esposa do Caio, minha vizinha, me deu o seguinte conselho:

— Chuchu, não chora, tu fazes o seguinte, tu pega os livros de Matemática e vai resolvendo os exercícios. Tu resolves o primeiro, resolve o segundo.

— Eu disse: é mesmo?

— Ela disse: é.

Eu parei de chorar e assim eu fiz. Comecei a resolver os livros e fui me apaixonando pela Matemática.

Eu gostaria de deixar bem claro que eu sou pedagoga. Eu não sou formada em matemática. Fiz o Ensino Médio na Escola Normal Lourenço Filho, depois, prestei o vestibular e cursei Pedagogia e continuei me apaixonando pela matemática, mas assim, estudando. Fiz didática, tanto no Ensino Médio, como na faculdade. E, graças a Deus isso foi muito bom para a minha vida, porque eu tinha o conhecimento das dificuldades da Matemática. Hoje, por onde eu ando, eu recebo agradecimentos.

Os meus filhos e meus netos foram meus alunos lá no Instituto Imaculada Conceição. Lá, ocorreu o seguinte episódio: na véspera de um dia de prova, minha filha Any chegou choramingando. Perguntei o que havia acontecido e ela me respondeu que seus colegas pediram uma cópia da prova, afirmando eles que sabiam que eu já havia dado a ela.

Eu contava isso pros meus alunos atuais, observando que, se eu tivesse feito isso com meus filhos, eles não seriam o que são hoje em dia. Graças a Deus, a Any é formada. Ela tem a didática e é formada em Economia, e a Grace é professora do Colégio Meta e também professora do Estado do Acre. Eu só tenho que agradecer a Deus por tudo isso, pelo conhecimento, enfim.

Era pra trabalhar 25 anos. Eu trabalhei 44. Mas, já perto do final da minha carreira, fui para casa chorando, depois de um dos dias em que atuei como professora efetiva. Então, a Any falou:

— Mãe, eu deixei o método de ensino tradicional, porque na vida tudo vai passando. Antigamente era o tradicional, mas chega uma época que nem os alunos o aceita mais.

Eu comecei voltar da escola pra casa, sempre chorando. Então, Any foi ao município de Cacoal, em Rondônia, fez uma pós-graduação em Didática e foi trabalhar também no Instituto Imaculada Conceição. Eu fiquei encantada, depois que nós começamos a trabalhar com projetos. Ela me explicou e me orientou como trabalhar de uma nova maneira. A gente ensinava a teoria matemática até o término do primeiro semestre. Do segundo semestre em diante, ao invés de eu

ensinar para eles, eram eles que montavam um projeto de estudo, observando o tema, introdução, desenvolvimento e a conclusão. Eles que iam buscar os conhecimentos.

Lá no colégio tinha uma sala própria para isso. Uma sala climatizada. A gente ia pra lá e assistíamos as apresentações dos trabalhos. Quando os alunos chegavam à sala de aula, eu já começava a aprender com eles. Por outro lado, eles aprendiam muito mais do que quando eu estava ensinando. Foi uma benção na minha vida.

Depois que a Any saiu da Escola e seguiu a profissão dela que é de economista, eu continuei e fiquei ensinado Matemática. Mas, hoje em dia, em alguns casos, quando o aluno tira nota ruim, acabam culpam o professor. Muitas vezes os pais nem conversam com seus filhos. Além disso, hoje em dia você não pode mais por limites em algumas crianças e adolescentes. E eu percebi que era hora de parar quando a mãe de um de meus alunos foi até a Escola e agrediu-me verbalmente sem me dar chances de falar. Já faz três anos que eu parei.

Mas, eu só tenho que agradecer a Deus, pela minha profissão, pela minha família. Ter lecionado também significou uma felicidade na minha vida.

Pergunta: *Professora, a senhora lembra-se de alguma referência bibliográfica*?

Lembro-me sim. Gostava muito do livro daquele Giovanni, e demais também do livro do Bianchini. Esses aí são os que eu mais gravei na minha memória.

Pergunta: *Como que a senhora gostava de dar aula*? *A senhora falou que ensinou uma época usando o método tradicional*?

Eu ensinei uma época pelo método tradicional. A forma tradicional é aquela na qual você é quem diz e determina tudo. Mas também aprendi a ensinar utilizando uma nova metodologia, na qual é permitido aos alunos buscar o conhecimento e também transmitir para gente. Essa prática de ensino me emocionava muito.

Pergunta: *A senhora influenciava essa busca*?

Sim, influenciava. Eu os ensinava a fazer projetos de estudo, era tudo na base de projetos. Eu aprendi a usar essa metodologia com minha filha Any e passei a praticar.

Pergunta: *Lembra-se dos alunos*?

Lembro. Por onde eu ando hoje em dia ouço muitas palavras de agradecimento. Em muitos casos meus, ex-alunos me reconhecem, mas para eu reconhecê-los é mais difícil.

Pergunta: *Em quais escolas a senhora lecionou*?

Eu comecei a dar aulas na escola Maria Angélica, depois fui dar aulas na Escola Marechal Arthur da Costa e Silva-Ética (José Rodrigues Leite). Nesse tempo, a Francisquinha, do Moacyr, era diretora da Escola Aluysio Carneiro Dantas. Como ela havia sido minha colega de sala e seus filhos haviam sido meus alunos, ela conhecia a minha capacidade de trabalho e, por isso, me contratou como professora daquela Escola. Foi ela quem conseguiu um contrato de ensino pra mim, junto à Prefeitura de Rio Branco. Como a Prefeitura de Rio Branco tinha convênios com o Instituto Imaculada Conceição, eu fui encaminhada para dar aulas lá também. Só naquela Escola fiquei 30 anos.

Pergunta: *O que a senhora está achando do ensino da matemática nos dias atuais*?

Fica um pouco difícil para o professor, que não pode mais botar limites. O aluno pode fazer o que quer, inclusive sair da sala de aula. Nas minhas turmas, eu não permitia o uso da calculadora. Para fazer os cálculos os alunos tinham que saber a tabuada. Inclusive, eu tenho aqui um exemplo de uma tabuada, diferente daquela tradicional, que, a meu ver, é mais fácil deles aprenderem. Essa daqui eu ainda divulgo, através de cópias que eu vou distribuindo. Já está toda amarrotada. Ela vai e volta. Eu também não deixava usar o celular. Pelo que eu vejo, hoje em dia, isso é permitido por alguns professores.

Considerações finais: O meu sonho era ser professora. Sempre convivi bem com meus colegas. E quero mencionar o professor Airton, que me ajudou muito. Ele é professor de Física.

Deus é muito bom comigo, porque eu tive dificuldade em aprender Matemática. Fui aprendendo com o dia a dia. Fiz Pedagogia e passei então a ter facilidade para mostrar os caminhos para os meus alunos.

Eu ainda continuo incentivando as pessoas. Quando alguém me diz que não gosta de Matemática, eu conto a minha história como exemplo. Chegada a hora em

que você tem que aprender, é só você querer e se dedicar. Se você quer, você é capaz e vai conseguir.

Recentemente me mandaram um convite para receber uma homenagem, no próximo mês de dezembro, na Câmara dos Vereadores. Eu aceitei o convite, juntamente com vários professores de matemática.

Por fim, eu também quero agradecer a oportunidade de, nesta entrevista, poder contar um pouco da minha história como professora de Matemática.

Professor Edmundo Costa da Silva

Falando livremente

Eu sou de Assis Brasil, do seringal. Não tive dificuldade em Matemática, mas sim, em Língua Portuguesa, porque a localidade em que eu vivia fazia fronteira com o Peru. Então, a gente misturava os idiomas Português e Espanhol.

Vim para cá em 65, 66, fazer o curso de admissão, mas, lá (Assis Brasil), era tudo em Espanhol. Nunca tive Português, História do Brasil. Isso tudo tive que estudar sozinho. Fiz a admissão e passei na primeira fase, lá no Colégio Acreano. Meu professor de Matemática, na quinta série, foi o Pelegrino, na sexta, Alcides Dutra, na sétima, o prof. João de Almeida e, na oitava, foi meu irmão Aquileu.

Em um dos episódios que aconteceu comigo, o Alcides Dutra me mandou para o quadro escrever “João nasceu” e eu não sabia escrever “nasceu”. Então ele me chamou de “burro”, o que meus colegas tentaram justificar, dizendo que eu era peruano!

Na oitava série, eu fui servir o exército e por isso tive que estudar à noite. Eu dormia muito em sala de aula. Então, nos informaram que os alunos que tinham

mais de 20 anos podiam fazer o segundo grau (hoje chamado de ensino médio), em menos tempo, cursando o Supletivo. Eu fui um dos que foi fazer. Depois, prestei o vestibular para Matemática, passei, e comecei a graduação. Quando estávamos no 5º período, surgiu uma oportunidade e eu fui participar do Premen-Programa de Expansão e Melhoramento do Ensino, oferecido pelo Cecine-Centro de Ensino do Nordeste, em Pernambuco. Depois, então, eu voltei para Rio Branco e comecei novamente a ensinar. De início, ouvi muitos pais falarem que não podiam ajudar os filhos com "essa Matemática moderna". No caso se referiam aos números naturais, números inteiros e teoria dos conjuntos.

Lembro-me que fui substituir o professor Jesus, meu irmão, que preferiu priorizar as suas outras atividades no Incra. Quando cheguei, fiquei na porta da sala, esperando os alunos da sexta série. Quando a inspetora me viu ali parado foi logo dizendo: entra, meu filho, o professor vai logo chegar. Até o Diretor, prof. Raimundo Gomes de Oliveira, dizia também que eu tinha a "cara" de um menino. A inspetora, até eu deixar de ensinar naquela Escola, me pedia desculpas, sempre que me encontrava.

Também assumi as turmas do Jesus, no Colégio São José. Aconteceu outro episódio. Eu estava em sala de aula, na quinta série, com exercícios de "pertence" e "não pertence", e apareceu um exercício com verbos da primeira conjugação, e eu pensei: lascou-se! Mas a classe respondeu: pertence! E eu disse: está certo, antes que alguém me perguntasse por quê? Depois fui ter com o professor de português, que, junto com a direção da escola, me chamaram a atenção para o fato da necessidade de saber bem o português.

Mas sempre fui ruim de Português. Só pra dar mais um exemplo, quando eu estudava, tinha uma menina que era fera em Português. Sentei perto dela, no dia de uma das provas. Acho que a prova tinha peso 2. Aí pra eu tirar uma nota boa, pedi para ela fazer a prova e me passar as respostas. Assim ela fez e eu copiei tudo. Quando a professora entregou as provas, ela havia tirado 9,5 pontos e eu 4,5 pontos. A menina disse: nem colar você sabe? As provas eram diferentes!

Sobre o comportamento dos alunos em sala de aula?

Eu nunca tive problema com aluno em sala. Eu via, no colégio, os professores sofrendo com os pais que não gostavam que seus filhos fossem

advertidos na frente dos colegas. Na minha época de aluno, o aluno que não se comportava, pegava uma lapada bem boa, ficava calado e, se reclamasse em casa, apanhava novamente.

Pergunta: e referências bibliográficas?
Recordo-me dos autores Márcio Brandão, Osvaldo Sangiorgi e de um que tinha sete autores. Acho que um deles era o Iezzi.

Pergunta: Você deu aulas no Colégio Meta?
Sim. Comecei em 1979.
Pergunta: Tinha diferença entre o ensino público e o ensino privado?

Sim, tinha muita diferença. No colégio particular, os pais dos alunos acompanhavam e cobravam. Já, na escola pública do Estado, a coisa era mais largada. Mas havia aluno bom, tanto no colégio particular quanto, na escola publica. Inclusive, quando eu dava aula no Sesi, um aluno do colégio Meta foi para lá e dava show. Não dava para notar a diferença. Acho que isso depende também do professor. Tem uns que trabalham da mesma maneira, no ensino público e no ensino privado. Tem outros que você pode dar salário de deputado, que a aula deles não muda. Na verdade, não têm comprometimento nenhum.

Pergunta: O que você acha do material apostilado adotado pelo colégio Meta?

Era tudo resumido e tínhamos que trabalhar uma apostila em cada um dos quatro bimestres. Então, eu planejava e aplicava outras atividades complementares.

Pergunta: Como você está vendo hoje o processo de ensino e aprendizagem?

Eu não sei como está hoje, mas até 2007, eu via que a cada ano caía mais o nível de ensino. Eu dizia para o Itamar: se eu aplicar hoje uma prova que eu aplicava há dez anos, nenhum desses meninos faz. Por exemplo, eu não os deixava usar máquina de calcular. Sempre os advertia sobre a possibilidade de a máquina quebrar e de que não custa nada fazer as contas que eles aprenderam. Hoje em dia, se o professor passar uma conta de dividir, tem aluno que não sai do lugar. Se colocar fração ou número decimal, então é que não sai mesmo.

Acontece é que o sistema quer que o aluno passe. Se ele sabe ou não sabe, não interessa. Tinha aula de recuperação. Eram propostas 10 questões para os alunos resolverem e estudá-las. Depois, era isso que caía na prova. Um questionário. Assim, tinha aluno sem condições de passar para o próximo ano, mas, no conselho de classe diziam: "mas ele é tão bonzinho, deixe-o passar!".

Pergunta: você se lembra de seus professores da Universidade?

Sim. Lembro-me de Zé Vicente, Aldair, Ribamar, um de Física, ele dava aula em várias escolas e na Universidade. O professor Hermínio. Muito ocupado. Uma vez, ele deu uma prova e nela eu consegui nota 5,0 ou 6,0 pontos. Percebi que minha nota estava registrada como 8,0 pontos, por estar sentado bem na frente e perto da mesa em que ele ocupava. Perguntei a ele se aquela era mesmo a minha nota, pois eu achava que tinha tirado só 6,0 pontos. Então, ele respondeu tranquilamente: sim! Agora, os 2,0 pontos a mais é por conta de um trabalho que não deu tempo de passar para vocês.

Pergunta: Hoje, se você pudesse voltar no tempo, que profissão você escolheria?

Sei não. Brincadeira! Falavam-me para pegar outros contratos e eu não aceitava, justificando que não queria pegar depressão. Ainda tentei ser bancário. Fiz um concurso na Caixa Econômica e passei nas provas de conhecimento, mas não consegui passar na prova de datilografia. Tinha um cara do meu lado e ele escrevia rapidamente. Enquanto eu procurava as teclas, o cara datilografava rapidamente.

Eu fazia faculdade e dava aula. Tinha dia que eu tinha que sair antes da aula terminar. Muitas vezes dormia 3 ou 4 horas por dia. Mas eu gostava. Apesar de que tinha turmas que eu chegava bem animado pra dar aula e outras que eu ia empurrado. O trabalho do professor não tem aquela rotina. Cada dia tem alguma coisa diferente. Nenhuma aula é igual à outra.

Professor Aquileu José da Silva Filho

Falando livremente

Justamente como Edmundo falou: nós, apesar de brasileiros, fomos criados praticamente no Peru. Quando viemos de lá, no meu caso, eu já vinha com o 2º grau (hoje Ensino Médio) completo. Chegamos entre 65 e 66 e eu logo fui fazer vestibular para Direito. Ainda bem que deu para passar, apesar de eu achar que não sabia nada. Como não havia trabalho naquele tempo, fui para o magistério mesmo e comecei a lecionar, preparando as turmas para o exame de admissão. Como não havia professores para todas as matérias, eu me vi obrigado a lecionar mais de uma disciplina e foi aí que comecei a gostar de matemática, português, história e geografia.

Numa dessas turmas em que eu lecionei todas as matérias, os alunos que estudaram sob minha orientação, por incrível que pareça, passaram em todas as disciplinas do exame de admissão. Aquilo ali me deu ânimo, me deu força e eu continuei lecionando.

O sucesso desses alunos chamou a atenção do professor Peregrino que, apesar de não me conhecer, deu um parecer favorável ao meu trabalho, ao comentar com o professor João de Almeida que eu tinha certa desenvoltura em Matemática. Então, depois da correção das provas, o João de Almeida veio falar comigo. Perguntou onde eu lecionava e eu o disse que não lecionava regularmente em nenhuma escola. Em seguida, ele me perguntou seu gostaria de lecionar, o que respondi que tinha interesse sim.

Nisso, aparece um curso de aperfeiçoamento dos docentes do ensino secundário-Cades, em Manaus. O mesmo professor João me convidou e, mediante o meu aceite, falou sobre a minha ida com o professor Raimundo Gomes, que era o

diretor do Colégio Acreano. Só aí já foi meia bandeja andada. Fui para Manaus, e lá, fiz o aperfeiçoamento para começar a lecionar. Agora uma coisa interessante, gente, eu, que não lecionava modéstia, à parte, já me comparava a muitos que há meses lecionavam matemática. Nesse sentido, o meu irmão Edmundo observou que, apesar do cara estar fazendo o curso de Matemática, ainda se enrolava quando o assunto envolvia fração decimal.

Já no Colégio Acreano, depois de conseguir uma vaga, através do João de Almeida, peguei minha primeira turma, que foi uma quinta série. Fiquei três meses na quinta série. Depois de mais três meses, eu terminei o ano ensinando Matemática para três quintas e uma sexta série. No ano seguinte, além de pegar as turmas que eu já tinha lecionado, peguei uma turma mais adiantada e me vi obrigado a estudar mais para dar aula. Quando cheguei ao quarto ano, ou seja, na oitava série, o domínio dos conteúdos das séries que ficaram para trás já era página virada para mim. Dei aulas até o ano de 1977. Trabalhando no Colégio Acreano, na Ética, na escola normal, no Ceseme, e no Instituto Imaculada Conceição.

E sobre sua formação em Matemática?

Aquele loirinho de matemática da Universidade, que vocês falaram agora pouco o nome dele, Aldair. Ele morava em frente lá de casa, gostava muito de mim, muitas vezes ele chegava lá da Universidade com aquele jeitinho dele e dizia: Aquileu vem cá. Resolve esse problema aqui, que eu não consegui resolver. Será que você resolve? Eu dava uma direção para a resolução do exercício, ele agradecia e se mandava.

Depois, ele me convenceu de ir fazer o curso de Matemática. Eu fui por causa dele. Fiquei até o terceiro ou quarto período e abandonei, porque, trabalhando no planejamento, na área ligada ao setor da Sudam, eu viajava muito, mais do que caixeiro viajante. Muitas vezes eu chegava de viagem na época das provas na faculdade, e tinha que fazer essas avaliações depois de perder várias aulas. Mesmo assim, eu passava e, às vezes, tirava nota melhor do que aqueles que não perdiam uma aula. Aquilo sinceramente me chateava. Por isso, decidi abandonar tudo.

Pergunta: Era possível conciliar os trabalhos que o senhor desenvolvia na sala de aula com a Faculdade de Direito?

Teve uma época, por exemplo, que eu saía de casa seis e meia para começar a dar aula no Colégio Acreano às sete horas. Saía de lá às onze horas. Não ia nem em casa almoçar, porque não dava tempo. Saía de lá, ia para o Colégio das freiras. Chegava lá, começava a aula uma hora. Quando davam três horas, saía de lá e ia para a Escola Normal. Ainda bem que era perto. Quando davam cinco horas, saía da Escola Normal e ia para Universidade, por conta da faculdade de Direito, que era ali onde era o prédio do Banacre. Eu ia tomar café, almoçar e jantar onze horas da noite, em casa.

O doutor Gerson era o diretor da faculdade de Direito. Um dia, ele me chamou para dizer que havia percebido que eu estava com muita falta. Eu justifiquei que tinha que dar aula à noite, no Colégio Acreano. Entrava sete e saía às onze. Então ele pediu que lhe fizesse o favor de pegar uma declaração dos meus horários de aula. Então fui à Escola falar com o professor Raimundo Gomes, o Diretor do Colégio Acreano. Ele pediu que me fosse dada a declaração e eu a levei para a faculdade, com as informações de que de segunda a sexta, das sete às onze, eu dava aulas naquela Escola. O Gerson, então, lamentou a minha situação, mas eu falei que não podia fazer nada. Ou estudava ou trabalhava para alimentar minha família. Então ele decidiu me ajudar. Continue dando tuas aulas. Quando você puder vir, você vem. O que não puder, no final do mês, eu abono tuas faltas, ele disse. Aí eu senti o peso da responsabilidade nas costas. Como eu não assistia às aulas, nos sábados e domingos, eu me reunia com outros colegas que assistiam às aulas e íamos estudar. Na época das provas, os outros colegas ficavam admirados com o meu desempenho. Nem sabiam o duro que eu dava para conseguir me formar.

Depois, eu passei a lecionar Matemática, já formado em Direito. Lembro-me que o Procurador Geral, à época, me chamou e disse que eu não poderia continuar trabalhando assim. Que a Matemática e o Direito são áreas completamente diferentes, incompatíveis. E que, se eu quisesse continuar lecionando, escolhesse uma área de ciências humanas, português, história ou geografia. Qualquer uma dessas servia. Então, eu larguei a Matemática. Nessa época, eu lecionava só no Complexo escolar de Ensino Médio-Ceseme.

Pergunta: e referências bibliográficas?

Eu não seguia um livro específico, mas indicava um dos que estavam disponíveis na época para que os meninos pudessem se orientar nas leituras. Eu costumava indicar Ary Quintela ou Osvaldo Sangiorgi.

Um dia, mostrei aos alunos da sexta série o livro do Márcio Brandão, dizendo a eles que o livro dele era bem didático e que eu também o usava para planejar as aulas. Como eu os advertia de que o bom aluno deve estar preparado para as provas igual a um soldado que vai para a guerra, elaborei uma avaliação, onde 80 por cento dela foi composta por exercícios resolvidos naquele livro. Achei que ia pegar a turma toda, mas foi a melhor nota que a sala já tirou. Eles haviam resolvido todos os problemas antes da prova. Achei bonito, porque motivava a turma a estudar mesmo. O assunto em questão tratava das coordenadas cartesianas. Eu fazia o pessoal resolver todo o livro. Com isso eles acabavam aprendendo e fixando bem os conteúdos.

Pergunta: Você se lembra de ter tido algum problema com alunos em sala de aula?

Eu mesmo não, mas eles às vezes tinham comigo. Eles me chamavam de professor fominha, porque eu, além de não faltar, não gostava de perder tempo. E então, quando eu pegava o último horário, eles já sabiam, eu entrava e ia direto para o quadro. Quando tocava a campainha, ia fazer a chamada. Eu chamava o camarada e, depois dele responder, podia sair de sala. Lembro-me de um episódio que ocorreu na oitava série. Estava chamando fulano, fulano, fulano e ouvi um blamamblum! Olhei e disse: rapaz o que foi isso? Um dos meninos respondeu dizendo que Fulano ia saindo e chutou a cadeira. Antes de chamar os últimos alunos, pedi que um deles fosse chamar o chutador. Ele voltou. Um rapagão! Acabei de fazer a chamada e ele perguntou se havia mandado o chamar? Então eu o perguntei se ele havia chutado mesmo a cadeira. Ele disse que sim e eu o adverti de que um rapagão tão bonito como ele, já na oitava série, deveria levar a sério a instrução que recebia e ser também educado. Continuando, eu pedi que, se ele não me respeitasse na qualidade de professor, respeitasse ao menos os seus colegas, inclusive, observasse que na sua turma havia uma senhora gestante e que foi feio o que ele havia feito. Depois de escutar tudo calado, ele perguntou se eu já tinha terminado e eu disse já. Então ele disse que pensou que eu ia dar a ele pelo menos

três dia de punição. Então, falei: eu não pensei nisso, mas, já que você quer, coloquei a mão no ombro dele e saímos até encontrar o inspetor Alberto. Pedi que ele o levasse até a direção para que ele fosse punido com três dias de suspensão. O Alberto, mesmo pensando que era brincadeira minha, chegou à diretoria com o aluno e falou: Professor Raimundo, Aquileu mandou pedir três dias de punição para esse aluno. Então, o Diretor perguntou o que ele havia feito e ele contou tudo em detalhes. Isso foi o bastante para que o professor pedisse à sua secretária, a senhora Raimundinha, que desse, ao invés de três, seis dias de suspensão, sendo três dias por sua conta.

Graças a Deus, a parte de comportamento, naquele tempo, era muito boa. Depois surgiu a tal de psicóloga, o orientador escolar, e hoje, pelo que eu sei, o professor não pode nem chamar a atenção do aluno. Isso, eu acho, tira a autoridade do professor.

Pergunta: O senhor quer acrescentar mais alguma coisa?

Sim. Eu quis voltar a estudar Matemática, mas meu irmão, Jesus, e o professor Magnésio logo me disseram que eu, estando velho daquele jeito, estava ficando louco e não devia mais sentar em cadeira de estudante. Sinceramente, isso foi um balde água fria.

Eu sempre digo que se eu tivesse concluído o curso de Matemática, hoje eu não estaria sem fazer nada. Poderia estar dando aulas, porque eu gostava muito de ensinar.

Revista
ELEMENTOS

Sobre o determinante de uma matriz de ordem 4

Sérgio Brazil Júnior
Professor Associado da Universidade Federal do Acre

Cristiano de Souza Silva
Bolsista PET/UFAC

Resumo

Os determinantes de matrizes quadradas de ordem 2 e de ordem 3 podem ser obtidos através de cálculos orientados pelos elementos de suas diagonais. Observando a regra de Sarrus, usada no caso em que a matriz é de ordem 3, estabelecemos uma regra similar que nos permite calcular, a partir dos produtos elementares dos elementos de suas diagonais, o determinante de uma matriz quadrada de ordem 4.

Abstract

The determinants of square matrices of order 2 and order 3 can be obtained by calculation guided by the elements of their diagonals. Observing Sarrus rule, used in the case where the matrix is of order 3, a similar rule set that enables us to calculate, from the elementary products of elements of their diagonals, the determinant of a square matrix of order 4.

Palavras chaves: Matrizes e Determinantes

1. Introdução: Justificativa e Objetivos

O estudo do determinante de uma matriz é muito importante, pois este conceito tem implicações importantes para a teoria de sistemas de equações lineares e para o estudo das matrizes invertíveis.

(Livro Boldrini): No livro chinês *Nove Capítulos sobre a Arte Matemática*, cujo autor é desconhecido (250 a.C.), já havia exemplos da resolução de sistemas de equações através de matrizes, bem como algumas noções ligadas a determinantes. No mundo Ocidental, o conceito de determinante começou a ser tratado esporadicamente a partir do século XVII. Nessa época surgem trabalhos de G. W. Leibniz (1646-1716), de G. Cramer (1704-1752), que desenvolveram um método de resolução de sistemas através de determinantes, conhecido por "Regra de Cramer", o que foi publicado em 1750, juntamente com alguns resultados simétricos de J. L. Lagrange (1736-1813). Só no século XIX é que os determinantes passaram a ser estudados mais sistematicamente, a começar pelo longo tratado de A. L. Cauchy (1789-1857), em 1812, tendo sido realizados, em seguida, trabalhos de C. G. Jacobi (1804-1851). A partir de então, o uso de determinantes difundiu-se muito e esse conceito, de um número associado a uma matriz quadrada, mostrou-se extremamente útil para caracterizar muitas situações, como por exemplo, a de saber se uma matriz é invertível ou não e se um sistema admite ou não solução.

O determinante de uma matriz $n \times n$ é definido como sendo a soma dos $n!$(n fatorial) produtos elementares dessa matriz, com sinal positivo ou negativo. Quando se trabalha com matrizes 2×2, temos apenas dois produtos elementares, cujos fatores ocorrem nas diagonais da matriz e, dessa forma, o cálculo do determinante é bastante simples: basta multiplicar os elementos da diagonal principal (produto positivo) e somar com o produto dos elementos da diagonal secundária (produto negativo). Se a matriz for de ordem 3×3, é bastante comum usarmos a famosa regra de *Sarrus* para calcular seu determinante. Tal regra consiste em escrever a matriz e, em seguida, adjuntar as duas primeiras colunas da matriz, logo após a terceira coluna da mesma, obtendo uma matriz com 3 linhas e 5 colunas. Nessa nova matriz temos seis diagonais: trabalhando de "cima para baixo", temos três "diagonais" da esquerda para a direita, e três diagonais da direita para esquerda. Os produtos elementares dessa matriz são exatamente os produtos das entradas dessas diagonais, sendo que os produtos da "esquerda para

direita" são positivos e os da "direita para esquerda" são negativos. Assim, o determinante da matriz é determinado realizando a soma desses produtos. Notemos que os procedimentos para o cálculo do determinante de uma matriz 2×2 e de uma matriz 3×3 são bastante parecidos.

Destarte, o estudo proposto resulta da indagação, realizada em uma aula de introdução à Álgebra Linear, no curso de licenciatura em matemática: *existe um procedimento para o cálculo do determinante de uma matriz* 4×4*, análogo ao procedimento utilizado para o cálculo do determinante de uma matriz* 3×3*?*

No presente texto daremos uma resposta positiva para essa questão. No entanto, deixaremos bem claro que não temos a pretensão de tornar o procedimento aqui apresentado, para o cálculo do determinante de uma matriz 4×4, mais importante que os procedimentos tradicionais.

2. Fundamentos teóricos metodológicos

Para definirmos o determinante de uma matriz quadrada de ordem $n \times n$, $0 < n \in \mathbb{Z}$, precisaremos de alguns resultados preliminares sobre permutações.

Definição1. Uma permutação do conjunto de inteiros $\{1, 2, 3, \dots, n\}$ é um rearranjo desses inteiros em alguma ordem, sem omissões ou repetições.

Exemplos:

1) Para $\{1, 2\}$, temos as seguintes permutações $(1, 2)$ e $(2, 1)$;

2) Para $\{1, 2,3\}$, temos as seguinte permutações $(1, 2, 3)$, $(1, 3, 2)$, $(2,1, 3)$, $(2, 3, 1)$, $(3, 1, 2)$ e $(3, 2, 1)$;

3) Para $\{1, 2,3, 4\}$, temos as seguintes permutações $(1, 2, 3, 4)$, $(1, 2, 4, 3)$, $(1, 3, 2, 4)$, $(1, 3, 4, 2)$, $(1, 4, 2, 3)$, $(1, 4, 3, 2)$, $(2, 1, 3, 4)$, $(2, 1, 4, 3)$, $(2, 3, 1, 4)$, $(2, 3, 4, 1)$, $(2, 4, 1, 3)$, $(2, 4, 3, 1)$, $(3, 1, 2, 4)$, $(3, 1, 4, 2)$, $(3, 2, 1, 4)$, $(3, 2, 4, 1)$, $(3, 4, 1, 2)$, $(3, 4, 2, 1)$, $(4, 1, 2, 3)$, $(4, 1, 3, 2)$, $(4, 2, 1, 3)$, $(4, 2, 3, 1)$, $(4, 3, 1, 2)$ e $(4, 3, 2, 1)$.

Observamos que em geral existem $n!$ (n fatorial) permutações distintas do conjunto $\{1, 2, 3, \dots, n\}$.

Denotaremos por $(j_1, j_2, j_3, \dots, j_n)$ uma permutação arbitrária do conjunto $\{1, 2, 3, \dots, n\}$. Neste caso, j_1 é o primeiro inteiro na permutação, j_2é o segundo, e assim por diante.

Definição 2: Diremos que ocorre uma **inversão** numa permutação sempre que um inteiro maior precede um menor.

O número total de inversões que podem ocorrer numa permutação pode ser obtido da seguinte forma: encontre o número de inteiros que são menores que j_1 e que aparecem depois de j_1, na permutação; logo em seguida, encontre o número de inteiros que são menores que j_2 e que aparecem depois de j_2, na permutação. Faça o mesmo para os inteiros $j_3, \dots, j_{n-1}$. O total de inversões é exatamente a soma desses números.

Exemplo: Considere a permutação $(4, 2, 1, 3)$. O número de inversões é: $3 + 1 + 0 = 4$.

Definição 2: Dizemos que uma permutação é *par* (respectivamente, *impar*) se o número total de inversões for um número par (respectivamente, impar).

Exemplos:

1) Permutações pares: $(1, 2, 3, 4), (1, 3, 4, 2), (1, 4, 2, 3), (2, 1, 4, 3), (2, 3, 1, 4), (2, 4, 3, 1), (3, 1, 2, 4), (3, 2, 4, 1), (3, 4, 1, 2), (4, 1, 3, 2), (4, 2, 1, 3), (4, 3, 2, 1)$.

2) Permutações impares: $(1, 2, 4, 3), (1, 3, 2, 4), (1, 4, 3, 2), (2, 1, 3, 4), (2, 3, 4, 1), (2, 4, 1, 3), (3, 1, 4, 2), (3, 2, 1, 4), (3, 4, 2, 1), (4, 1, 2, 3), (4, 2, 3, 1), (4, 3, 1, 2)$.

Definição 3: Dada uma matriz A, de ordem $n \times n$, definimos um *produto elementar* dessa matriz como sendo um produto de n entradas de A, tais que não ocorram duas de mesma linha ou de mesma coluna.

Observamos que uma matriz A de ordem $n \times n$ tem $n!$(n fatorial) produtos elementares. Estes são os produtos da forma $a_{1j_1}, a_{2j_2}, \dots, a_{nj_n}$, onde $(j_1, j_2, \dots, j_n)$ é uma permutação do conjunto $\{1, 2, \dots, n\}$.

Exemplos: Seja $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}_{4x4}$. Os produtos elementares são: $a_{11}a_{22}a_{33}a_{44}$; $a_{11}a_{23}a_{34}a_{42}$; $a_{11}a_{24}a_{32}a_{43}$; $a_{12}a_{21}a_{34}a_{43}$; $a_{12}a_{23}a_{31}a_{44}$; $a_{12}a_{24}a_{33}a_{41}$; $a_{13}a_{21}a_{32}a_{44}$; $a_{13}a_{22}a_{34}a_{41}$; $a_{13}a_{24}a_{31}a_{42}$; $a_{14}a_{21}a_{33}a_{42}$; $a_{14}a_{22}a_{31}a_{43}$; $a_{14}a_{23}a_{32}a_{41}$; $a_{11}a_{22}a_{34}a_{43}$; $a_{11}a_{23}a_{32}a_{44}$; $a_{11}a_{24}a_{33}a_{42}$; $a_{12}a_{21}a_{33}a_{44}$; $a_{12}a_{23}a_{34}a_{41}$; $a_{12}a_{24}a_{31}a_{43}$; $a_{13}a_{21}a_{34}a_{42}$; $a_{13}a_{22}a_{31}a_{44}$; $a_{13}a_{24}a_{32}a_{41}$; $a_{14}a_{21}a_{32}a_{43}$; $a_{14}a_{22}a_{33}a_{41}$ e $a_{14}a_{23}a_{31}a_{42}$.

Definição 4: Dada uma matriz A, de ordem $n \times n$, um produto elementar $a_{1j_1}, a_{2j_2}, \dots, a_{nj_n}$, multiplicado por $+1$ ou -1, é chamado um *produto elementar com sinal de A*. Usamos o sinal " + " se $(j_1, j_2, \dots, j_n)$ for uma permutação par e o sinal " − " se $(j_1, j_2, \dots, j_n)$ for uma permutação ímpar.

Exemplo:

Produto elementar	Permutação associada	paridade	Produto elementar com sinal
$a_{11}a_{22}a_{33}a_{44}$	$(1,2,3,4)$	par	$+a_{11}a_{22}a_{33}a_{44}$
$a_{11}a_{23}a_{34}a_{42}$	$(1,3,4,2)$	par	$+a_{11}a_{23}a_{34}a_{42}$
$a_{11}a_{24}a_{32}a_{43}$	$(1,4,2,3)$	par	$+a_{11}a_{24}a_{32}a_{43}$
$a_{12}a_{21}a_{34}a_{43}$	$(2,1,4,3)$	par	$+a_{12}a_{21}a_{34}a_{43}$
$a_{12}a_{23}a_{31}a_{44}$	$(2,3,1,4)$	par	$+a_{12}a_{23}a_{31}a_{44}$
$a_{12}a_{24}a_{33}a_{41}$	$(2,4,3,1)$	par	$+a_{12}a_{24}a_{33}a_{41}$
$a_{13}a_{21}a_{32}a_{44}$	$(3,1,2,4)$	par	$+a_{13}a_{21}a_{32}a_{44}$
$a_{13}a_{22}a_{34}a_{41}$	$(3,2,4,1)$	par	$+a_{13}a_{22}a_{34}a_{41}$
$a_{13}a_{24}a_{31}a_{42}$	$(3,4,1,2)$	par	$+a_{13}a_{24}a_{31}a_{42}$
$a_{14}a_{21}a_{33}a_{42}$	$(4,1,3,2)$	par	$+a_{14}a_{21}a_{33}a_{42}$
$a_{14}a_{22}a_{31}a_{43}$	$(4,2,1,3)$	par	$+a_{14}a_{22}a_{31}a_{43}$
$a_{14}a_{23}a_{32}a_{41}$	$(4,3,2,1)$	par	$+a_{14}a_{23}a_{32}a_{41}$
$a_{11}a_{22}a_{34}a_{43}$	$(1,2,4,3)$	ímpar	$-a_{11}a_{22}a_{34}a_{43}$
$a_{11}a_{23}a_{32}a_{44}$	$(1,3,2,4)$	ímpar	$-a_{11}a_{23}a_{32}a_{44}$
$a_{11}a_{24}a_{33}a_{42}$	$(1,4,3,2)$	ímpar	$-a_{11}a_{24}a_{33}a_{42}$
$a_{12}a_{21}a_{33}a_{44}$	$(2,1,3,4)$	ímpar	$-a_{12}a_{21}a_{33}a_{44}$
$a_{12}a_{23}a_{34}a_{41}$	$(2,3,4,1)$	ímpar	$-a_{12}a_{23}a_{34}a_{41}$
$a_{12}a_{24}a_{31}a_{43}$	$(2,4,1,3)$	ímpar	$-a_{12}a_{24}a_{31}a_{43}$
$a_{13}a_{21}a_{34}a_{42}$	$(3,1,4,2)$	ímpar	$-a_{13}a_{21}a_{34}a_{42}$
$a_{13}a_{22}a_{31}a_{44}$	$(3,2,1,4)$	ímpar	$-a_{13}a_{22}a_{31}a_{44}$
$a_{13}a_{24}a_{32}a_{41}$	$(3,4,2,1)$	ímpar	$-a_{13}a_{24}a_{32}a_{41}$
$a_{14}a_{21}a_{32}a_{43}$	$(4,1,2,3)$	ímpar	$-a_{14}a_{21}a_{32}a_{43}$
$a_{14}a_{22}a_{33}a_{41}$	$(4,2,3,1)$	ímpar	$-a_{14}a_{22}a_{33}a_{41}$
$a_{14}a_{23}a_{31}a_{42}$	$(4,3,1,2)$	ímpar	$-a_{14}a_{23}a_{31}a_{42}$

Tabela 1

Agora, estamos em condições de definir o determinante de uma matriz quadrada.

Definição 4: Dada uma matriz A, de ordem $n \times n$, definimos seu determinante, anotado por $det(A)$, como sendo a soma de todos os produtos elementares com sinal de A.

Exemplos:

1) Determinante de uma matriz 2×2. Seja $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}_{2x2}$. Então, temos que $\det(A) = a_{11}a_{22} - a_{12}a_{21}$, que pode ser obtido a partir dos dados da tabela abaixo:

Produto elementar	Permutação associada	paridade	Produto elementar com sinal
$a_{11}a_{22}$	$(1, 2)$	par	$+a_{11}a_{22}$
$a_{12}a_{21}$	$(2, 1)$	ímpar	$-a_{12}a_{21}$

Tabela 2

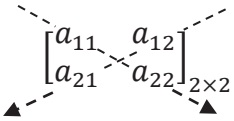
2) Determinante de uma matriz 3×3. Seja $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}_{3x3}$. Então, vale que $\det(A) = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}$, que pode ser obtido a partir dos dados da tabela abaixo

Produto elementar	Permutação associada	paridade	Produto elementar com sinal
$a_{11}a_{22}a_{33}$	$(1, 2, 3)$	par	$+a_{11}a_{22}a_{33}$
$a_{12}a_{23}a_{31}$	$(2, 3, 1)$	par	$+a_{12}a_{23}a_{31}$
$a_{13}a_{21}a_{32}$	$(3, 1, 2)$	par	$+a_{13}a_{21}a_{32}$
$a_{11}a_{23}a_{32}$	$(1, 3, 2)$	ímpar	$-a_{11}a_{23}a_{32}$
$a_{12}a_{21}a_{33}$	$(2, 1, 3)$	ímpar	$-a_{12}a_{21}a_{33}$
$a_{13}a_{22}a_{31}$	$(3, 2, 1)$	ímpar	$-a_{13}a_{22}a_{31}$

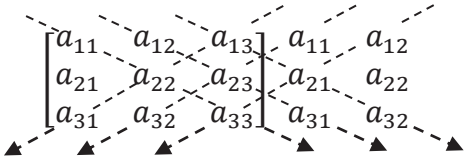
Tabela 3

Na prática, para memorizar a fórmula do exemplo 1, façamos o seguinte: "Realizamos o produto das entradas da flecha direcionada para direita e

subtraímos do produto das entradas da flecha direcionada para esquerda", conforme figura abaixo:



E, para memorizar a fórmula do exemplo 2, realizamos o seguinte: "Acrescentamos à direita da matriz a primeira e a segunda coluna e, em seguida, realizamos a soma dos produtos das entradas das flechas direcionadas para direita e subtraímos da soma dos produtos das entradas das flechas direcionadas para esquerda."



4) Determinante de uma matriz 4×4. Seja $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}_{4x4}$. Da tabela 1, temos $\det(A) = a_{11}a_{22}a_{33}a_{44} + a_{11}a_{23}a_{34}a_{42} + a_{11}a_{24}a_{32}a_{43} + a_{12}a_{21}a_{34}a_{43} + a_{12}a_{23}a_{31}a_{44} + a_{12}a_{24}a_{33}a_{41} + a_{13}a_{21}a_{32}a_{44} + a_{13}a_{22}a_{34}a_{41} + a_{13}a_{24}a_{31}a_{42} + a_{14}a_{21}a_{33}a_{42} + a_{14}a_{22}a_{31}a_{43} + a_{14}a_{23}a_{32}a_{41} - a_{11}a_{22}a_{34}a_{43} - a_{11}a_{23}a_{32}a_{44} - a_{11}a_{24}a_{33}a_{42} - a_{12}a_{21}a_{33}a_{44} - a_{12}a_{23}a_{34}a_{41} - a_{12}a_{24}a_{31}a_{43} - a_{13}a_{21}a_{34}a_{42} - a_{13}a_{22}a_{31}a_{44} - a_{13}a_{24}a_{32}a_{41} - a_{14}a_{21}a_{32}a_{43} - a_{14}a_{22}a_{33}a_{41} - a_{14}a_{23}a_{31}a_{42}$.

Note a dificuldade de se calcular o determinante de uma matriz de ordem 4×4, a partir da definição. Assim, é melhor usar a expansão em cofatores, que trataremos a seguir.

Definição 4: Se A é uma matriz quadrada, então o *determinante menor* da entrada a_{ij}, ou simplesmente o *menor* de a_{ij}, é denotado por M_{ij} e definido como o determinante da submatriz, obtida ao suprimirmos a *i*-ésima linha e a *j*-ésima coluna de A. O número $C_{ij} = (-1)^{i+j} M_{ij}$ é chamado de *cofator* de a_{ij}.

Exemplo: Seja $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}_{4x4}$. O menor de a_{32} é o número obtido por $M_{32} = det\left(\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}_{4x4}\right) = det\left(\begin{bmatrix} a_{11} & a_{13} & a_{14} \\ a_{21} & a_{23} & a_{24} \\ a_{41} & a_{43} & a_{44} \end{bmatrix}_{3x3}\right)$. E este determinante, claro, é o de uma matriz de ordem 3×3. Assim, podemos calcular facilmente e obter o cofator de a_{32}, que é $C_{32} = (-1)^{3+2}M_{32}$.

O resultado a seguir é bem conhecido e será enunciado sem prova, pois sua demonstração foge aos objetivos do presente trabalho.

Teorema 1 (expansão em cofatores): O determinante de uma matriz A, de tamanho $n \times n$ pode ser calculado multiplicando-se as entradas de qualquer linha (ou coluna) pelos seus cofatores e somando os produtos resultantes, ou seja, para quaisquer $1 \leq i \leq n$ e $1 \leq j \leq n$, vale que:

1) $\det(A) = a_{1j}C_{1j} + a_{2j}C_{2j} + \cdots + a_{nj}C_{nj}$, que é uma *expansão em cofatores*, *ao longo da j-ésima coluna* da matriz A.

2) $\det(A) = a_{i1}C_{i1} + a_{i2}C_{i2} + \cdots + a_{in}C_{in}$, que é uma *expansão em cofatores*, *ao longo da i-ésima linha* da matriz A.

Exemplo: Seja a matriz A genérica, de ordem 4×4. Vamos calcular $\det(A)$ fazendo uma expansão, em cofatores, ao longo da primeira coluna de A. Temos $\det(A) = det\left(\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}_{4x4}\right) = a_{11}(-1)^{1+1}det\left(\begin{bmatrix} a_{22} & a_{23} & a_{24} \\ a_{32} & a_{33} & a_{34} \\ a_{42} & a_{43} & a_{44} \end{bmatrix}_{3x3}\right)$

$+ \ a_{21}(-1)^{2+1}det\left(\begin{bmatrix} a_{12} & a_{13} & a_{14} \\ a_{32} & a_{33} & a_{34} \\ a_{42} & a_{43} & a_{44} \end{bmatrix}_{3x3}\right) + \ a_{31}(-1)^{3+1}det\left(\begin{bmatrix} a_{12} & a_{13} & a_{14} \\ a_{22} & a_{23} & a_{24} \\ a_{42} & a_{43} & a_{44} \end{bmatrix}_{3x3}\right)$

$+ a_{41}(-1)^{4+1}det\left(\begin{bmatrix} a_{12} & a_{13} & a_{14} \\ a_{22} & a_{23} & a_{24} \\ a_{32} & a_{33} & a_{34} \end{bmatrix}_{3x3}\right)$.

3. Uma alternativa para calcular o determinante de uma matriz de ordem 4

Vamos, agora, apresentar uma forma alternativa para calcular o determinante de uma matriz de ordem 4×4, como resposta a um questionamento que surgiu em uma aula de introdução à Álgebra Linear, no curso de licenciatura em matemática. Existe um procedimento para o cálculo do determinante de uma matriz de ordem 4×4, análogo ao do cálculo do determinante de uma matriz de ordem 3?

Após alguns momentos de reflexão sobre a questão proposta e de alguns experimentos realizados com matrizes de ordem 4, verificamos que podemos realizar o cálculo de tal determinante da seguinte forma:

Acrescentamos à direita da matriz a primeira coluna, a segunda coluna e a terceira coluna, nessa ordem, logo em seguida, acrescentamos a primeira coluna novamente, depois acrescentamos a quarta coluna, a segunda, a terceira e a primeira coluna, nesta ordem, e então repetimos a segunda coluna; em sequência, acrescentamos a quarta, a terceira, a primeira e a segunda, como mostra a figura abaixo:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} \begin{matrix} a_{11} & a_{12} & a_{13} & a_{11} & a_{14} & a_{12} & a_{13} & a_{11} & a_{12} & a_{14} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{24} & a_{22} & a_{23} & a_{21} & a_{22} & a_{24} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{34} & a_{32} & a_{33} & a_{31} & a_{32} & a_{34} & a_{33} & a_{31} & a_{32} \\ a_{41} & a_{42} & a_{43} & a_{41} & a_{44} & a_{42} & a_{43} & a_{41} & a_{42} & a_{44} & a_{43} & a_{41} & a_{42} \end{matrix}$$

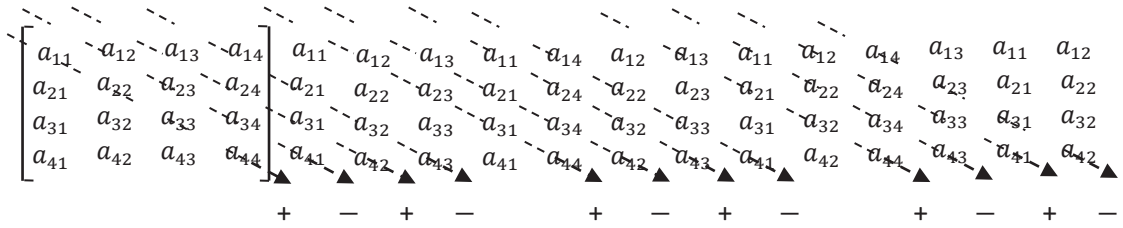
(Figura A)

Observamos, na Figura A, que o índice *j* em cada coluna é a ordem em que as mesmas foram acrescentadas.

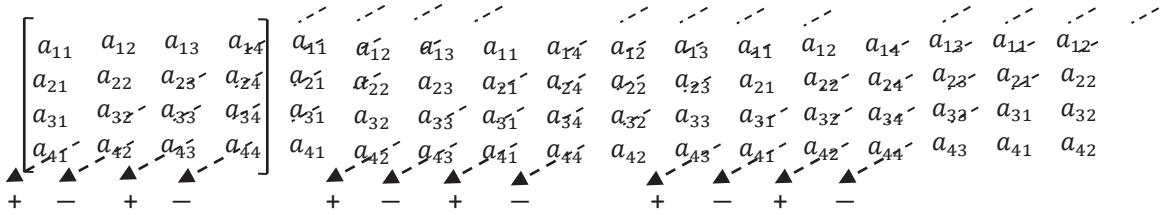
Depois de termos realizado a ação de acrescentar as colunas na sequência descrita acima, verificamos que os produtos elementares, com sinal, aparecem naturalmente, como podemos verificar abaixo, olhando as "flechas" direcionadas para a direita, Figura B, e as "flechas" direcionadas para esquerda, Figura C.

Note que a disposição das "flechas" tem algumas falhas (figuras B e C). Colocamos uma sequência de quatros flechas e pulamos uma diagonal, depois colocamos mais uma sequência de quatro flechas e pulamos mais uma diagonal e, por fim, uma sequência de mais quatro flechas.

Também podemos observar que a paridade das permutações aparece de forma alternada, facilitando com isso os cálculos.



(Figura B)



(Figura C)

Agora, realizando a soma dos produtos das entradas das flechas direcionadas para direita e direcionadas para esquerda, obedecendo a paridade de cada produto, como vemos nas figuras B e C, temos o determinante da matriz de ordem 4×4.

Observamos que para realizar esse procedimento, basta que o leitor memorize a seguinte sequência para alocar as colunas à direita da matriz: 1ª, 2ª, 3, 1ª, 4ª, 2ª, 3ª, 1ª, 2ª, 4ª, 3ª, 1ª e 2ª.

4. Conclusão

Em que pese termos, ao nosso olhar, respondido a questão proposta, não é nossa intenção tentar induzir, principalmente os alunos, que, ao se depararem com o problema de calcular o determinante de uma matriz de ordem 4×4, optem por desenvolver esses cálculos que apresentamos aqui. A forma proposta no presente texto é apenas uma alternativa para o cálculo do determinante de uma matriz 4×4, que pode ser, inclusive, mais trabalhosa que os cálculos, utilizando expansão em cofatores. Veja que, para o cálculo utilizando a forma proposta, tivemos que acrescentar 13 (treze) colunas à direita da matriz, em certa ordem, para que os 12 (doze) produtos elementares surjam. Imaginemos um procedimento como esse para o caso do cálculo do determinante de uma matriz de ordem 5×5. Quantas colunas devem ser acrescentadas à direita da matriz para que os $120 (= 5!)$ produtos elementares apareçam?

5. Referências Bibliográficas

[1] ANTON, H.; RORRES, C. *Álgebra Linear com aplicações*. Tradução de: Claus Ivo Doering. 8ª ed. Porto Alegre: Bookman, 2001.

[2] BOLDRINI, J. L. ...[et al.].: *Álgebra Linear* – 3ª ed. São Paulo: Harper & Row do Brasil, 1980.

Sérgio Brazil Júnior
Centro de Ciências Exatas e Tecnológicas
Universidade Federal do Acre
sbrazil@ufac.br
(68)09984-1022

Cristiano de Souza Silva
Rua Murupi, nº 110; Bairro Vitória - Rio Branco-AC; CEP: 69901-755.
cristiano.souza16@gmail.com
(68) 999867268

Revista
ELEMENTOS

Bases vazias

Dedicado aos alunos de Matemática e Engenharia Civil da Ufac

Lemuel de Freitas Ponce
Mestrando na Universidade Federal do Amazonas-Ufam

José Ivan da Silva Ramos
Professor Associado do Centro de Ciências Exatas e Tecnológicas da Ufac

Resumo

A relação aritmética existente entre as dimensões de dois subespaços W_1 e W_2, de um mesmo espaço vetorial $V(K)$ e as dimensões dos subespaços soma e interseção, respectivamente, $W_1 + W_2$ e $W_1 \cap W_2$, mostram a necessidade de uma explicação a respeito da dimensão do subespaço nulo. Por inclusão, podemos classificar o conjunto vazio Φ como sendo um conjunto linearmente independente. Juntando a isso uma cuidadosa definição de $[S]$, o subespaço gerado por um subconjunto S de $V(K)$, concluímos que $[\Phi] = \{0\}$ e que a dimensão do espaço nulo é zero.

Abstract

The existing arithmetic relation between the dimensions of two subspaces W_1 and W_2 of a vector space $V(K)$ and dimensions of subspaces sum and intersection, respectively, $W_1 + W_2$ and $W_1 \cap W_2$, show the need for an explanation of the dimension of the null subspace. For inclusion, we can classify the empty set Φ as a linearly independent set. Adding to this careful definition of $[S]$, the subspace generated by a subset S of $V(K)$V, we conclude that $[\Phi] = \{0\}$ and that the dimension of the null space is zero.

Palavras Chave: Escalares, matrizes, espaços vetoriais, base e dimensão.

1. Introdução

Depois de entendermos a definição de um espaço vetorial abstrato, é possível que nossas lembranças se atenham à Álgebra que é discutida sobre o plano analítico de Euclides.

A nossa pretensão no pequeno texto aqui elaborado é relatar sobre a ausência de discussão quanto a dimensão do espaço nulo. Comumente ou quase sempre, e quando é citada, a dimensão do espaço nulo, por convenção ou definição, é igual a zero.

Dado que conjuntos linearmente independentes não podem conter subconjuntos linearmente dependentes, o conjunto vazio Φ é LI. Combinando isso com a definição de conjuntos geradores, as bases vazias podem ser consideradas a partir de argumentações que podem ser feitas a respeito dos membros da família dos subespaços de um espaço vetorial.

Revisão bibliográfica

Em [3] (BOLDRINI, J. L.; Costa, S. I. R.; Ribeiro, V. L., Wetzler, H. G.), no capítulo 4, sobre os *espaços vetoriais*, é feita uma abordagem que usa os fatos geométricos dos vetores de $\mathbb{R}^2$ e $\mathbb{R}^3$; define a *soma*, fala da *soma direta* e da *interseção* de subespaços em separado, exemplificando cada uma dessas construções. Em seguida, antes de definir *base* e *dimensão* de um espaço vetorial, relaciona os conceitos de *combinação*, *dependência* e *independência linear*. A relação $\dim(U+W) = \dim U + \dim W - \dim(U \cap W)$, entre subespaços de um espaço vetorial $V(K)$, aparece como um teorema, na pág. 20. A demonstração, deixada a cargo do leitor, é orientada por exercícios colocados no final do capítulo, que termina com uma abordagem sobre mudança de base. Não é dada qualquer explicação para a dimensão do espaço nulo $\{0\}$, apesar de deixar clara a necessidade de termos $\dim\{0\} = 0$, na equação acima, quando a soma $U \oplus W$ é direta.

Em [4] (GONÇALVES, A. S. e Rita M. L), no capítulo 4, as proposições que descrevem um *espaço vetorial* são colocadas de maneira bastante didática. Para concluir os estudos sobre *matrizes linha equivalentes* foram incluídos os *espaços linha* e *coluna* de uma matriz, ligando esses conceitos com o espaço vetorial formado pelas *soluções de um sistema linear homogêneo*.

Com relação à soma de subespaços, na pág. 71, coloca uma definição de *soma* como um exemplo e, em seguida, particularmente, observa que *toda matriz quadrada é soma de uma matriz simétrica com uma matriz antissimétrica* e que *toda função real é soma de uma função par com uma função ímpar*. Os conjuntos linearmente dependentes e independentes são destacados nas páginas 76 e 77, mas o conjunto vazio Φ não é relacionado com essa questão. A discussão sobre a *dimensão do espaço nulo* não é feita, como também não foi incluída a relação $\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$.

Em [7] (LANG, Serge), o capítulo II se refere aos *espaços vetoriais*, *bases*, *dimensão*, *somas* e às *somas diretas*. Podemos observar que praticamente todos os resultados que relacionamos aqui, em nossa Introdução, aparecem lá, de forma direta ou indiretamente. Além disso, o autor explora somente as relações $\dim(U + W) = V(K)$, quando $V(K)$ é soma ou soma direta de seus subespaços U e W. No caso em que $U \oplus W = V(K)$ é uma soma direta, propõe, como exercício, provar que $\dim(U \times W) = \dim U + \dim W$; onde $W \times L = \{(w, l)/\ w \in W \text{ e } l \in L\}$ é o espaço vetorial que relacionamos no item 2.1, da seção 2, deste trabalho. Nenhuma discussão é feita a respeito da *dimensão do espaço nulo*.

Em [8] (LIPSCHUTZ, Seymour), no capítulo 5, separado do capítulo 4 onde são explorados os conceitos de *base* e *dimensão*, é feita a discussão sobre os *espaços vetoriais*. No parágrafo sobre bases e dimensão, a dimensão do espaço nulo é definida como sendo igual a zero. Isso, para combinar com a definição dada de que Φ é um conjunto LI. No mais, o texto apresenta uma riqueza de problemas resolvidos, problemas propostos e problemas suplementares, que ajudam a entendermos melhor a estrutura dos espaços vetoriais.

Quase todas as definições, exemplos e resultados, apresentados nessa discussão, podem ser vistos nos livros aqui relacionados e, a nosso ver, são fiéis ao rigor que esse assunto originalmente exige.

Espaços vetoriais

1.1 Definição: Seja V um conjunto não vazio e $+$ uma operação de adição definida em V, tal que $\forall\ u, v, w \in V$, valem:

A_1: $u + (v + w) = (u + v) + w$;

A_2: $u + v = v + u$;

A_3: $\exists\ o \in V$ tal que $o + u = u + o = u$;

A_4: $\exists - v \in V$ tal que $-v + v = v + (-v) = o$.

Seja K um corpo com o qual possamos construir o conjunto $KV = \{kv/k \in K \text{ e } v \in V\} \subset V$, produto de K por V, a partir da multiplicação por escalar $\therefore kv \in V; \forall\ k \in K \text{e} \forall\ v \in V$, satisfazendo, $\forall\ k, s \in K \text{e} \forall\ u, v \in V$:

M_1: $k(u + v) = ku + kv$;

M_2: $(k + s)v = kv + sv$;

M_3: $(ks)v = k(sv)$;

M_4: $1\ v = v$; onde 1 é o elemento neutro da multiplicação definida em K.

Nessas condições, dizemos que V é um *espaço Vetorial sobre* (*o corpo*) K. Comumente, escrevemos $(V(K), +, \cdot)$ ou simplesmente $V(K)$ para indicar que V é um espaço vetorial sobre o corpo K.

1.2 Exemplos: São exemplos de espaços vetoriais:

$-$ $(\mathbb{R}^2(\mathbb{R}), +, \cdot)$, $(\mathbb{C}(\mathbb{R}), +, \cdot)$ e $(\mathbb{C}(\mathbb{R}), +, \cdot)$.

$-$ $(M_{mxn}(K)(K), +, \cdot)$, o conjunto das matrizes de ordem mxn; é um espaço vetorial sobre K, sendo K um corpo. Se não causar dúvidas, esse espaço pode ser denotado por $(M_{mxn}(K), +, \cdot)$.

$-$ $(P_n(t), +, \cdot)$, o conjunto dos polinômios de grau no máximo $1 \leq n \in \mathbb{N}$, numa variável t e com coeficientes no corpo $\mathbb{R}$, juntamente com o polinômio nulo. Aqui, temos $P_n(t) = \{a_0 + a_1 t + \cdots + a_n t^n / a_i \in \mathbb{R};\ \forall\ i = 0,1, \cdots, n\}$ e as operações de adição e multiplicação por escalar são definidas da seguinte forma: $\forall\ p(t) = a_0 + a_1 t + \cdots + a_n t^n, q(t) = b_0 + b_1 t + \cdots + b_n t^n \in P_n(t)$ e $\forall\ \lambda \in \mathbb{R}$,

$+: p(t) + q(t) = (a_0 + b_0) + (a_1 + b_1)t + \cdots + (a_n + b_n)t^n$

$\therefore \lambda p(t) = \lambda(a_0 + a_1 t + \cdots + a_n t^n) = \lambda a_0 + \lambda a_1 t + \cdots + \lambda a_n t^n$

$-$ $\left(\mathcal{F}_{\mathbb{R}}^{\mathbb{R}}(\mathbb{R}), +, \cdot\right)$, o conjunto $\mathcal{F}_{\mathbb{R}}^{\mathbb{R}}$ das funções reais, munido das operações de adição e multiplicação por escalar, induzidas pelas operações de adição e multiplicação, definidas no conjunto dos números (ver [1], §7 do capítulo 1).

As propriedades da adição e da multiplicação por escalar, em $\mathcal{F}_{\mathbb{R}}^{\mathbb{R}}(\mathbb{R})$, decorrem das propriedades da adição e da multiplicação definidas no conjunto dos números.

A função

$o: \mathbb{R} \longrightarrow \mathbb{R}$

$x \rightsquigarrow f(x) = 0$ é o elemento neutro da adição definida em $\mathcal{F}_{\mathbb{R}}^{\mathbb{R}}$.

E

$(-1)f = -f: \mathbb{R} \longrightarrow \mathbb{R}$

$x \rightsquigarrow (-f)(x) = -f(x)$ é o inverso aditivo da função f.

Por comodidade, vamos denotar um espaço vetorial sobre um corpo K por $V(K)$. A terna, contendo também os sinais com as operações, estará implícita.

1.3 Definição: Seja W um subconjunto não vazio de um espaço vetorial $V(K)$. Se W é um espaço vetorial com respeito às mesmas operações que definem $V(K)$ como um espaço vetorial, então W é denominado de um *subespaço vetorial* de $V(K)$.

Isso significa que, sendo W não vazio, $\forall\, w_1, w_2 \in W$ e $\forall\, \lambda \in K$, vale que $w_1 + w_2, \lambda w_1 \in W$, e mais, para os elementos em W se verificam as propriedades A_1, A_2, $\cdots$, M_4, listadas na definição, em 1.1.

Caracterização de um subespaço vetorial

As propriedades de uma operação definida em um conjunto não vazio quase sempre se transferem para seus subconjuntos. Isso pode ser visto na seguinte caracterização de um subespaço vetorial

1.4 Observação: Seja $V(K)$ um espaço vetorial sobre um corpo K; seja W um subconjunto de $V(K)$. Então, são equivalentes:

a) W é um subespaço vetorial de $V(K)$.

b) Vale que:

i) $0 \in W$;

ii) $w_1 + w_2 \in W$; $\forall\, w_1, w_2 \in W$;

iii) $\lambda w \in W$; $\forall\, \lambda \in K$ e $\forall\, w \in W$.

c) Vale que:

i) $W \neq \Phi$;

ii) $\lambda w_1 + w_2 \in W$; $\forall\, \lambda \in K$ e $\forall\, w_1, w_2 \in W$.

Demonstração: Pode ser feita no sentido a)$\Longrightarrow$ b)$\Longrightarrow$ c)$\Longrightarrow$ a). Mas, independentemente da estratégia de demonstração usada, podemos sempre levar

em conta que as propriedades A_1, A_2, M_1, ⋯, M_4, listadas em 1.1, são herdadas pelo subconjunto (não vazio) W.

No sentido de a) para b), a conclusão é imediata. De b) para c), usando o fato em i), vemos que $W \neq \Phi$ e, por ii) juntamente com iii), vemos que $\lambda w_1 \in W$ e $\lambda w_1 + w_2 \in W$; $\forall\, \lambda \in K$ e $\forall\, w_1, w_2 \in W$. Um bom exercício é a verificação de que c) implica em a).

Notação: Anotaremos $W \leq V(K)$ para indicar que um subconjunto W de $V(K)$ é um subespaço vetorial.

1.5 Exemplos:

$-\ D_n(\mathbb{R})$, o conjunto das matrizes diagonais de ordem n, é um subespaço vetorial de $M_n(\mathbb{R})$.

$-\ W = \{f \in \mathcal{F}_{\mathbb{R}}^{\mathbb{R}}(\mathbb{R}) / f(0) = f(3)\} \leq \mathcal{F}_{\mathbb{R}}^{\mathbb{R}}(\mathbb{R})$.

1.6 Observação: Sejam $V_1(K)$ e $V_2(K)$ espaços vetoriais sobre um corpo K. Então, vale que $V_1(K) \times V_2(K) = \{(v_1, v_2) / v_1 \in V_1(K) \text{ e } v_2 \in V_2(K)\}$ é um espaço vetorial, definindo, $\forall\, (v_1, v_2), (u_1, u_2) \in V_1(K) \times V_2(K)$ e $\forall\, \lambda \in K$, as operações:

$+: (v_1, v_2) + (u_1, u_2) = (v_1 + u_1, v_2 + u_2)$;

$\therefore \lambda(v_1, v_2) = (\lambda v_1, \lambda v_2)$.

O par ordenado $O = (0,0)$ é o elemento neutro da adição definida acima e $-(v_1, v_2) = (-v_1, -v_2)$ é o inverso aditivo de cada elemento (v_1, v_2) em $V_1(K) \times V_2(K)$.

Aqui, não devemos pensar em herança de propriedades. A coisa funciona porque em cada componente do produto cartesiano valem as propriedades A_1, A_2, M_1, ⋯, M_4, listadas em 1.1.

Podemos construir um espaço vetorial mais geral, usando o produto cartesiano. Em 1.6 podemos trocar o corpo K por K_1 e K_2 e considerar os espaços $V_1(K_1)$ e $V_2(K_2)$, desde que tenhamos $K_1 \subset K_2$ ou $K_2 \subset K_1$. Nesse caso, a multiplicação por escalar é definida para λ em K_1 ou λ em K_2, conforme a relação de inclusão entre os corpos K_1 e K_2.

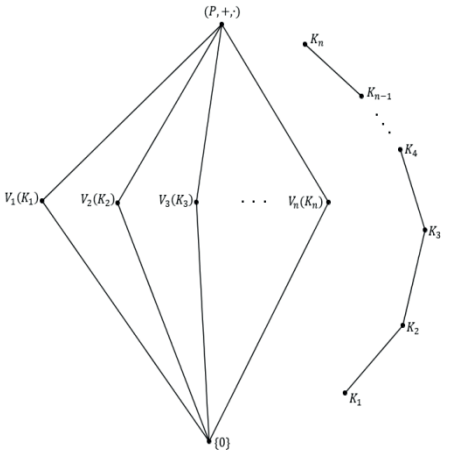
Nesse sentido, consideremos os corpos $K_1 \subset K_2 \subset \cdots \subset K_n$ e $V_1(K_1), V_2(K_2) \cdots, V_n(K_n)$, respectivamente, espaços vetoriais sobre cada um deles, com $3 \leq n \in \mathbb{N}$. O conjunto

$$P = V_1(K_1) \times V_2(K_2) \times \cdots \times V_n(K_n) = \{(v_1, v_2, \cdots, v_n)/v_i \in V_i(K_i); i = 1, 2, \cdots, n\}$$

é um espaço vetorial, definindo, $\forall\ (v_1, v_2, \cdots, v_n), (u_1, u_2, \cdots, u_n) \in P$ e $\forall\ \lambda \in K_1$:

$+: (v_1, v_2, \cdots, v_n) + (u_1, u_2, \cdots, u_n) = (v_1 + u_1, v_2 + u_2, \cdots, v_n + u_n)$;

$\therefore \lambda(v_1, v_2, \cdots, v_n) = (\lambda v_1, \lambda v_2, \cdots, \lambda v_n)$.



Como são os subespaços de P? Podemos montar vários produtos usando os espaços vetoriais que já foram apresentados em nosso texto até aqui e ver como essa coisa funciona.

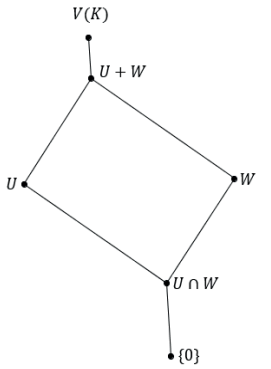
Por exemplo, temos que $\left(\begin{bmatrix} 1 & 0 \\ 0 & 7 \end{bmatrix}_{2x2}, (0, 3)\right) \in D_2(\mathbb{R}) \times W \leq M_2(\mathbb{R}) \times \mathbb{R}^2$, onde $W = \{(0, y)/y \in \mathbb{R}\}$ é um subespaço de $\mathbb{R}^2$.

2. Teoremas relacionados aos objetos de estudo

Denotaremos por $\mathcal{F}_{V(K)} = \{W/W \leq V(K)\}$ a família dos subespaços de um espaço vetorial $V(K)$ sobre um corpo K. É claro que $\mathcal{F}_{V(K)}$ não é vazia, pois $\{0\}$ e $V(K)$, os *subespaços triviais* de $V(K)$, são membros dessa família.

Em $\mathcal{F}_{V(K)}$, podemos definir operações que comumente se percebe nas discussões elementares da teoria dos conjuntos.

2.1 Observação: Seja $V(K)$ um espaço vetorial sobre um corpo K. Sejam W e L elementos quaisquer em $\mathcal{F}_{V(K)}$. Então, vale que:



a) $W \cap L$ é um subespaço de $V(K)$;

b) $W + L = \{w + l/\ w \in W \text{ e } l \in L\}$ é um subespaço de $V(K)$;

c) $W \times L = \{(w, l)/\ w \in W \text{ e } l \in L\}$ é um espaço vetorial que contém uma cópia de W e uma cópia de L.

Demonstração: a) Temos que $0 \in W \cap L \neq \Phi$; já que $0 \in W$ e $0 \in L$. Além disso, $\forall\, u, v \in W \cap L$, vale que $u, v \in W \leq V(K)$ e $u, v \in L \leq V(K)$. Então, $\forall\, \lambda \in K$, vale que $\lambda u + v \in W \cap L$. Portanto, temos que $W \cap L \leq V(K)$.

b) Podemos escrever $0 = 0 + 0$; com $0 \in W$ e $0 \in L$. Então, $0 \in W + L \neq \Phi$. Mais ainda, $\forall\, u, v \in W + L$, eles são da forma $u = w_1 + l_1$ e $v = w_2 + l_2$. E, se λ é qualquer escalar em K, temos que $\lambda u + v = \lambda(w_1 + l_1) + (w_2 + l_2) = (\lambda w_1 + w_2) + (\lambda l_1 + l_2)$; com $\lambda w_1 + w_2 \in W \leq V(K)$ e $\lambda l_1 + l_2 \in W \leq V(K)$. Isso prova que $\lambda u + v \in W + L$ e, assim, vemos que $W + L \leq V(K)$.

c) Que $W \times L$ é um espaço vetorial $V(K)$ é claro! Pensamos como na observação em 1.6. Agora, as cópias de W e L são garantidas pelas funções

$$\begin{array}{lll} \varphi\colon W \longrightarrow \mathcal{W} = \{(w,0)/\, w \in W\} & \text{e} & \psi\colon L \longrightarrow \mathcal{L} = \{(0,l)/\, l \in L\} \\ \quad w \rightsquigarrow \varphi(w) = (w,0) & & \quad l \rightsquigarrow \varphi(l) = (0,l) \end{array}$$

que são homomorfismos bijetivos. Vale que $W \cong \mathcal{W} \leq W \times L$ e também $L \cong \mathcal{L} \leq W \times L$. Que $\mathcal{W}$ e $\mathcal{L}$ são subespaços de $W \times L$, é claro.

2.2 Corolário: Seja $V(K)$ um espaço vetorial sobre um corpo K. Sejam $W_1, W_2, \cdots, W_n$ elementos quaisquer em $\mathcal{F}_{V(K)}$; $3 \leq n \in \mathbb{N}$. Então, vale que:

a) $\displaystyle\bigcap_{i=1}^{n} W_i = W_1 \cap W_2 \cap \cdots \cap W_n \leq V(K)$;

b) $\displaystyle\sum_{i=1}^{n} W_i = W_1 + W_2 + \cdots + W_n \leq V(K)$.

Demonstração: É imediata!

2.3 Exemplo: Os subespaços $\mathcal{W} = \{(x,0)/\, x \in \mathbb{R}\}$ e $\mathcal{L} = \{(0,y)/\, y \in \mathbb{R}\}$ de $\mathbb{R}^2$ são tais que $\mathcal{W} \cap \mathcal{L} = \{(0,0)\}$ e $\mathcal{W} + \mathcal{L} = \{(x,y)/\, x, y \in \mathbb{R}\} = \mathbb{R}^2$. Nem sempre o subespaço interseção está tão embaixo e o subespaço soma está tão em cima. Quando isso acontece simultaneamente essa soma recebe um nome especial.

Se W e L são elementos quaisquer em $\mathcal{F}_{V(K)}$ e $W \cap L = \{0\}$ e $W + L = V(K)$, dizemos que $V(K) = W \oplus L$ é uma *soma direta* dos subespaços W e L.

Em geral, ao unirmos dois elementos W e L de $\mathcal{F}_{V(K)}$, o conjunto $W \cup L$ não é um elemento de $\mathcal{F}_{V(K)}$. Por exemplo, unindo os subespaços $\mathcal{W}$ e $\mathcal{L}$, vemos que $(1,0)$ e $(0,1)$ são elementos de $\mathcal{W} \cup \mathcal{L} = \{v/\, v \in \mathcal{W}$ ou $v \in \mathcal{L}\}$. No entanto, a soma

desses vetores $(1,0)+(0,1)=(1,1)\notin \mathcal{W}\cup\mathcal{L}$, o que mostra que $\mathcal{W}\cup\mathcal{L}$ não é um subespaço de $\mathbb{R}^2$.

2.4 Observação: Seja $V(K)$ um espaço vetorial sobre um corpo K. Sejam W e L subespaços de $V(K)$. Então, vale que $W\cup L$ é um subespaço de $V(K)$ se, e somente se, $W\subset L$ ou $L\subset W$.

Demonstração: Vamos supor que $W\cup L\leq V(K)$ e que $W\not\subset L$. Assim, devemos mostrar que $L\subset W$. Seja l qualquer elemento em L. Como $W\not\subset L$, $\exists\, w\in W$, tal que $w\notin L$. Claramente, temos que $l,w\in W\cup L\leq V(K)$. Por isso, $l+w\in W\cup L$ e vemos que $l+w\in W$ ou $l+w\in L$. Se $l+w\in L\leq V(K)$, temos que $-l+(l+w)=w\in L$. O que é uma contradição com a escolha de w. Então, só pode ser que $l+w\in W\leq V(K)$. Mas assim, vale que $(l+w)+(-w)=l\in W$. Isso mostra que $L\subset W$.

Supondo $W\cup L\leq V(K)$ e que $L\not\subset W$, argumentos parecidos aos que fizemos acima mostram que $W\subset L$.

2.5 Corolário: Sejam $V(K)$ um espaço vetorial sobre um corpo K e $W_1,W_2,\cdots,W_m$ subespaços de $V(K)$; com $1\leq m\in\mathbb{N}$. Então, $W_1\cup W_2\cup\cdots\cup W_m=W\leq V(K)$ se, e somente se, esses subespaços formarem uma cadeia $W_{t_1}\subset W_{t_2}\subset\cdots\subset W_{t_m}$; onde $t_i\in\{1,2,\cdots,m\}$; com $i=1,2,\cdots,m$.

Demonstração: Se $m=2$, temos a mesma situação que em 2.4 e, portanto, temos a cadeia $W_1\subset W_2$ ou $W_2\subset W_1$.

Suponhamos que existe um primeiro inteiro $m>2$, de modo que essa afirmação não vale. Então, para $2\leq m-1<m$ e $W_1,W_2,\cdots,W_{m-1}$ subespaços de $V(K)$, vale que $W_1\cup W_2\cup\cdots\cup W_{m-1}=L\leq V(K)$ se, e só se, esses subespaços formam uma cadeia $W_{t_1}\subset W_{t_2}\subset\cdots\subset W_{t_{m-1}}$; onde $t_i\in\{1,2,\cdots,m-1\}$; com $i=1,2,\cdots,m-1$.

Agora, para os subespaços L e W_m, novamente o resultado em 2.4 mostra que $L\cup W_m=W_1\cup W_2\cup\cdots\cup W_m=W\leq V(K)$ se, e somente se, $L\subset W_m$ ou $W_m\subset L$ se, e somente se, esses subespaços formam uma cadeia $W_{t_1}\subset W_{t_2}\subset\cdots\subset W_{t_m}$; onde $t_i\in\{1,2,\cdots,m\}$; com $i=1,2,\cdots,m$. Assim, não existe o primeiro inteiro $m>2$, de modo que essa afirmação não valha.

Isso termina a demonstração do corolário.

Conjuntos geradores, bases e dimensão de um espaço vetorial

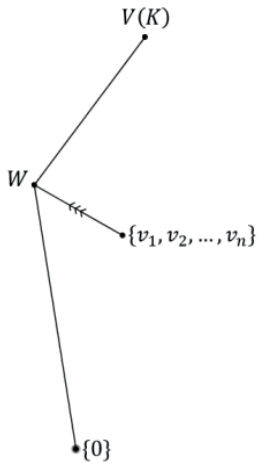
2.6 Definição: Seja $V(K)$ um espaço vetorial sobre um corpo K. O vetor $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$; onde $\alpha_i \in K$ e $v_i \in V(K)$, com $i = 1, 2, \cdots, n$, é denominado uma *combinação linear* dos vetores $v_1, v_2, \cdots, v_n$.

2.7 Observação: Seja $V(K)$ um espaço vetorial sobre um corpo K. Fixados $1 \leq n \in \mathbb{N}$ vetores $v_1, v_2, \cdots, v_n$, vale que:

a) $W = [v_1, v_2, \cdots, v_n] = \{\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n / \alpha_i \in K;\ i = 1, 2, \cdots, n\}$ é um subespaço vetorial de $V(K)$. Ele é denominado *subespaço gerado* por $v_1, v_2, \cdots, v_n$. Nesse caso, dizemos que $\{v_1, v_2, \cdots, v_n\}$ é um $conjunto\ (de)\ gerador(es)$ de W e W é $n\ gerado$.

b) Dentre os subespaços de $V(K)$, temos que W *é o menor subespaço que contém o conjunto* $\{v_1, v_2, \cdots, v_n\}$, no sentido de que, se outro subespaço L de $V(K)$ contém $\{v_1, v_2, \cdots, v_n\}$, então W está contido em L.

Demonstração: a) Pondo $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$, vemos que $0 \in W$ e assim, $W \neq \Phi$. Dados $w_1 = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ e $w_2 = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n$ em W e λ em K, o vetor $\lambda(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n) + (\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n) = \lambda w_1 + w_2 \in W$. Isso mostra que $W = [v_1, v_2, \cdots, v_n] \leq V(K)$.



b) Suponhamos que L é um subespaço de $V(K)$, tal que $\{v_1, v_2, \cdots, v_n\} \subset L$. Então, $\forall\ \gamma_1, \gamma_2, \cdots, \gamma_n \in K$, vale que $\gamma_1 v_1 + \gamma_2 v_2 + \cdots + \gamma_n v_n \in L$. Portanto, todo elemento de W é um vetor de L e assim, temos $W \leq L$.

Dois vetores são (paralelos) linearmente dependentes se um é múltiplo escalar do outro e vice versa. Em um espaço vetorial arbitrário onde os vetores não têm uma representação geométrica, a interpretação da colinearidade é feita por meio de uma equação linear.

2.8 Definição: Seja $V(K)$ um espaço vetorial sobre um corpo K. Dados n vetores $v_1, v_2, \cdots, v_n$ em $V(K)$, com $1 \leq n \in \mathbb{N}$, dizemos que:

a) esses n vetores são *linearmente independentes* (LI) se, e somente se, dados $\alpha_1, \alpha_2, \cdots, \alpha_n \in K$, a igualdade $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$ vale se, e somente se, tivermos $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

b) esses n vetores são *linearmente dependentes* (LD) se, e somente se, na igualdade $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$ temos $\alpha_i = 0$ para algum $i \in \{1, 2, \cdots, n\}$.

2.9 Exemplos:

$-$ Consideremos $\gamma = \{f, g\} \subset \mathcal{F}_{\mathbb{R}}^{\mathbb{R}}(\mathbb{R})$, onde f e g são definidas por $f(x) = \cos x$ e $g(x) = \operatorname{sen} x$, respectivamente. Podemos decidir se esse conjunto é LI ou LD da seguinte maneira: sejam $a, b \in \mathbb{R}$. Fazendo $af + bg = o$; onde o é a função nula, temos $(af + bg)(x) = o(x) \Leftrightarrow (af)(x) + (bg)(x) = o(x) \Leftrightarrow a\cos x + b\operatorname{sen} x = 0$; $\forall\, x \in \mathbb{R}$. Derivando essa última igualdade, temos $\begin{cases} a\cos x + b\operatorname{sen} x = 0 \\ b\cos x - a\operatorname{sen} x = 0 \end{cases} \Leftrightarrow$ $\begin{cases} a^2\cos x + ab\operatorname{sen} x = 0 \\ b^2\cos x - ba\operatorname{sen} x = 0 \end{cases}$. Somando essas equações, temos que $(a^2 + b^2)\cos x = 0$. Escolhendo um x conveniente, temos que $a^2 + b^2 = 0 \Leftrightarrow a^2 = -b^2$. Portanto, temos $a = b = 0$ e γ é LI.

$-$ $\beta = \{(1, 0), (0, 1)\}$ gera $\mathbb{R}^2$. Como os vetores de β não são colineares, β é LI.

2.10 Observação: Seja β um subconjunto de um espaço vetorial $V(K)$ sobre um corpo K. Então, vale que:

a) se β contém um subconjunto LD, então β é LD.

b) se β é um conjunto LD, então β pode conter subconjuntos LD ou LI.

c) se β é LI, então todo subconjunto de β é um conjunto LI.

Demonstração: Ver as referências.

O conjunto $\gamma = \{(1, 0), (0, 1), (1, 2), (-1, 3)\}$ é claramente LD. Além disso, contém $\{(1\ 0), (0, 1)\}$, que é LI, e contém $\{(1\ 0), (0, 1), (1, 2)\}$, que é LD. O item c) pode ser explicado por contradição, utilizando o item a).

O conjunto vazio Φ, por não possuir elementos, está contido em todo subconjunto β de um espaço vetorial $V(K)$. Pelo item a) iremos admitir que Φ é um conjunto LI.

2.11 Definição: Seja $V(K)$ um espaço vetorial sobre um corpo K. Dados n vetores $v_1, v_2, \cdots, v_n$ em $V(K)$, com $n \in \mathbb{N}$, dizemos que o conjunto $\beta = \{v_1, v_2, \cdots, v_n\}$ é uma *base* de $V(K)$ se, e somente se,

a) β gera $V(K)$;

b) β é um conjunto LI.

2.12 Exemplos:

$-$ Vale que $[(1\ 0), (0, 1)] = \mathbb{R}^2$. Como os vetores de β não são colineares, β é LI. Portanto, β é uma base de $\mathbb{R}^2$.

$-$ Temos $\begin{bmatrix} x & y \\ z & w \end{bmatrix}_{2x2} = x\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}_{2x2} + y\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}_{2x2} + z\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}_{2x2} + w\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}_{2x2}$. Isso mostra que $\lambda = \left\{\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}_{2x2}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}_{2x2}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}_{2x2}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}_{2x2}\right\}$ gera $M_2(\mathbb{R})$. Agora, $x\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}_{2x2} + y\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}_{2x2} + z\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}_{2x2} + w\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}_{2x2} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}_{2x2}$ fornece que $x = y = z = w = 0$ e vemos que λ é LI. Então, λ é base de $M_2(\mathbb{R})$.

$-$ É fácil ver que $\alpha = \{1, i\}$ e $\theta = \{1, t, t^2, \cdots, t^n\}$ são, respectivamente, bases de $\mathbb{C}(\mathbb{R})$ e $P_n(t)$. Aqui, é o espaço dos números complexos sobre o corpo $\mathbb{R}$.

2.13 Observação: Seja $V(K)$ um espaço vetorial não nulo sobre um corpo K. Se $1 \leq n \in \mathbb{N}$ e $\gamma = \{v_1, v_2, \cdots, v_n\}$ é um conjunto gerador de $V(K)$, vale que:

a) se γ é LI, todo vetor de $V(K)$ se escreve de modo único, como combinação linear dos vetores de γ.

a) γ contém uma base de $V(K)$.

b) Se η é um subconjunto de $V(K)$ e $\#\eta = m > n$; então η é um conjunto LD.

Demonstração: Ver as referências.

2.14 Consequência: Seja $V(K)$ um espaço vetorial sobre um corpo K. Se β e γ são bases de $V(K)$, elas possuem o mesmo número de elementos.

Demonstração: Se $\#\beta > \#\gamma$, β é LD. Se $\#\gamma > \#\beta$, γ é LD. Resta que $\#\beta = \#\gamma$.

Isso nos dá mais segurança para estabelecermos a definição de dimensão de um espaço vetorial.

2.15 Definição: Seja $V(K)$ um espaço vetorial sobre o corpo K. O número dim $V(K)$, de elementos de uma base de $V(K)$, é denominado de *dimensão* de $V(K)$. Se dim $V(K) = n$, é comum dizermos que dim $V(K)$ é um espaço $n-$ dimensional.

Nem sempre é possível "contarmos" os vetores de uma base de $V(K)$. Por exemplo, $\mathcal{F}_{\mathbb{R}}^{\mathbb{R}}(\mathbb{R})$, o espaço das funções reais sobre o corpo $\mathbb{R}$ não possui dimensão finita.

O último resultado deste parágrafo descreve com exatidão a estrutura de um espaço vetorial e a álgebra que envolve seus subespaços e respectivos conjuntos geradores. A exigência de que os vetores que compõem as bases de um espaço vetorial devem ser linearmente independentes mostra que essas bases possuem o mesmo número de elementos, no caso dos espaços vetoriais serem de dimensão finita. Encerramos este parágrafo mostrando que, se U e W são subespaços de $V(K)$, existe uma relação aritmética entre as dimensões dos subespaços $U, W, U \cap W$ e $U + W$.

2.16 Teorema: Seja $V(K)$ um espaço vetorial $n-$ dimensional sobre um corpo K; com $1 \leq n \in \mathbb{N}$. Então:

a) se $\gamma = \{v_1, v_2, \cdots, v_r\}$ é um subconjunto LI de $V(K)$ e $1 \leq r < n$, vale que:

i) $\exists$ um vetor v de $V(K)$ fora de $[v_1, v_2, \cdots, v_r]$;

ii) o conjunto $\{v_1, v_2, \cdots, v_r\} \cup \{v\}$ é LI.

b) se β é um subconjunto LI de $V(K)$, ele faz parte de uma base de $V(K)$.

c) todo subconjunto LI de $V(K)$, contendo n vetores, é uma base de $V(K)$.

d) se U e W são subespaços de $V(K)$, vale que:

i) dim $U \leq$ dim $V(K) = n$ e dim $W \leq$ dim $V(K) = n$.

ii) dim $(U + W) =$ dim $U +$ dim $W -$ dim$(U \cap W)$.

Demonstração: Para os itens a), b), c) e d), item i), Ver as referências.

Agora, claro que $U \cap W$ está contido em U e em W. Portanto, se $\theta = \{v_1, v_2, \cdots, v_r\}$ é uma base de $U \cap W$ e dim$U = m$, pelo item b), podemos completar esse conjunto com $m - r$ vetores, de modo que $\beta_1 = \{v_1, v_2, \cdots, v_r, u_1, u_2, \cdots, u_{m-r}\}$ seja uma base de U. Da mesma forma, se dim$W = l$, juntamos $l - r$ vetores θ e obtemos uma base $\beta_2 = \{v_1, v_2, \cdots, v_r, w_1, w_2, \cdots, w_{l-r}\}$ de W.

O conjunto $\beta = \{v_1, v_2, \cdots, v_r, u_1, u_2, \cdots, u_{m-r}, w_1, w_2, \cdots, w_{l-r}\}$ tem exatamente $\#\beta = r + (m - r) + (l - r) = m + l - r$ vetores.

Provaremos que β é uma base de $U+W$. Que β gera $U+W$, é claro: cada vetor de U pode ser escrito na forma

$$u = a_1v_1 + \cdots + a_rv_r + b_1u_1 + \cdots + b_{m-r}u_{m-r} + 0w_1 + \cdots + 0w_{l-r}.$$

E cada vetor de W pode ser escrito na forma

$$w = c_1v_1 + \cdots + c_rv_r + 0u_1 + \cdots + 0u_{m-r} + d_1w_1 + \cdots + d_{l-r}w_{l-r}.$$

Portanto, todo vetor de $U+W$ pode ser escrito como sendo:

$$u+w = (a_1+c_1)v_1+\cdots+(a_r+c_r)v_r+b_1u_1+\cdots+b_{m-r}u_{m-r}+d_1w_1+\cdots+d_{l-r}w_{l-r}.$$

Agora, verificaremos que β é LI: pondo

$$(\square): a_1v_1 + \cdots + a_rv_r + b_1u_1 + \cdots + b_{m-r}u_{m-r} + c_1w_1 + \cdots + c_{l-r}w_{l-r} = 0,$$

vemos que

$$v = a_1v_1 + \cdots + a_rv_r + b_1u_1 + \cdots + b_{m-r}u_{m-r} = -c_1w_1 + \cdots + (-c_{l-r})w_{l-r}$$

é um vetor em $U \cap W$. Sendo $\theta = \{v_1, v_2, \cdots, v_r\}$ uma base desse subespaço, podemos escolher escalares $\lambda_1, \cdots, \lambda_r$ de modo que

$$v = -c_1w_1 + \cdots + (-c_{l-r})w_{l-r} = \lambda_1v_1 + \cdots + \lambda_rv_r.$$

Equivalentemente, temos $\lambda_1v_1 + \cdots + \lambda_rv_r + c_1w_1 + \cdots + c_{l-r}w_{l-r} = 0$. Como β_2 é um conjunto LI, vale que $c_1 = \cdots = c_{l-r} = 0$. Substituindo o valor dos $c_i's$ em $(\square)$, temos $a_1v_1 + \cdots + a_rv_r + b_1u_1 + \cdots + b_{m-r}u_{m-r} = 0$. Mas, β_1 é um conjunto LI. Então, vemos que também $a_1 = \cdots = a_r = b_1 = \cdots = b_{m-r} = 0$. Isso mostra que β é LI. Concluímos que β é uma base do subespaço soma $U+W$ e que, precisamente, temos $\#\beta = \dim(U+W) = r + (m-r) + (l-r) = m + l - r = \dim U + \dim W - \dim(U \cap W)$. Isso prova o item d), ii).

Bases vazias

O plural que define este parágrafo tem a ver com a generalidade do espaço nulo. Podemos pensar no vetor nulo de cada um dos espaços dados como exemplo até aqui.

O resultado em 2.7 sugere a seguinte

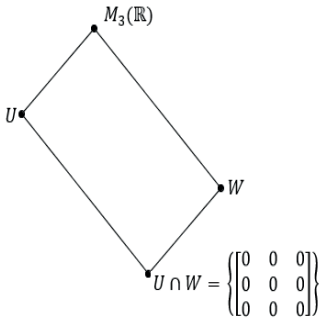
2.17 Definição: Seja $V(K)$ um espaço vetorial sobre um corpo K. Seja S qualquer subconjunto de $V(K)$. Então, $[S]$, o subespaço gerado por S, é definido como sendo o menor subespaço de $V(K)$ que contém S.

Podemos então, em 2.7, incluir o caso em que temos $n = 0$ vetores fixados. Vale o seguinte resultado

2.18 Observação: Seja $V(K)$ um espaço vetorial sobre um corpo K. Então, vale que $[\Phi] = \{0\}$ e $\dim\{0\} = 0$.

Demonstração: Vale que $\Phi \subset \{0\} \leq W;\ \forall\, W \in \mathcal{F}_{V(K)} = \{W/W \leq V(K)\}$. Portanto, $\{0\}$ é o menor subespaço de $V(K)$ que contém Φ. Daí, $[\Phi] = \{0\}$ e $\dim\{0\} = 0$.

2.19 Exemplo: Sejam $M_3(\mathbb{R})$ o conjunto das matrizes quadradas de ordem 3 e dois de seus subespaços $U = \{A \in M_3(\mathbb{R})/\ A^t = A\}$ e $W = \{A \in M_3(\mathbb{R})/A^t = -A\}$. Temos que $U + W = M_3(\mathbb{R})$ e $U \cap W = \{O\}$ é o conjunto unitário formado pela matriz nula. Portanto, $M_3(\mathbb{R}) = U \oplus W$ é uma soma direta dos subespaços U e W.



Agora, mesmo sem avaliarmos quais são as dimensões de U e W, a relação $\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$, do item ii) do item d) de 2.16, juntamente com a observação em 2.18, permite que estimemos que $\dim U$ e $\dim W$ têm paridades diferentes.

Observemos que $\dim M_3(\mathbb{R}) = 9$, $\dim U = 6$ e $\dim W = 3$. Por simples inspeção, vemos que as matrizes $L_1 = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}_{3x3}$, $L_1 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix}_{3x3}$ e $L_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}_{3x3}$ formam um conjunto de geradores LI's de W.

3. Considerações finais

Depois de fazermos a revisão bibliográfica, percebemos que realmente as perguntas dos alunos a respeito do espaço nulo tinham fundamento. Ao consultarmos outros livros, que comumente eram usados aqui em nossa Instituição, percebemos que muitas vezes a discussão não destaca as bases vazias e a dimensão do espaço nulo, que influem diretamente na utilização da equação em ii) do item d) de 2.16.

Em [1] e em [6], os autores STEINBRUCH e HOWARD, respectivamente, também não fazem essa abordagem.

Em [5], um livro que comumente é adotado em um curso de bacharelado ou mestrado, HOFFMAN e KUNZE definem (ver pág. 45) que: *se* S *é um subconjunto de um espaço vetorial* $V(K)$ *sobre um corpo* K; *então* $[S]$ *é a interseção de todos os subespaços de* $V(K)$ *que contém* S.

Ainda, em [5], pág. 56, comenta em parágrafos que: *o conjunto vazio* Φ *é LI por não conter nenhum vetor* e que *a interseção de todos os subespaços de* $V(K)$ *que contém o conjunto vazio é* $\{0\}$.

A definição em 2.17 não entra em desacordo com a definição que temos em [5]; já que $\{0\} \in \mathcal{F}_{V(K)_\Phi} = \{W / \Phi \subset W \leq V(K)\}$.

Nossa intenção, ao relacionar os diagramas/reticulados que indicam os espaços vetoriais, seus subespaços ou cadeias de subespaços, foi a de despertar para o fato de que essas visualizações gráficas complementam a compreensão que se pode ter dessas estruturas.

Por fim, apesar de a motivação ter sido dar uma explicação sobre a dimensão do espaço nulo, acreditamos que este pequeno relato de experiência se configura numa boa discussão sobre o livro didático.

4. Referências

[1] STEINBRUCH, Alfredo e WINTERLE, Paulo; *Introdução à Álgebra Linear*; Editora McGraw-Hill; São Paulo, SP - 1990.

[2] BEZERRA, MARCOS V. A.; *Funções Pares e Ímpares (Generalização de Conceitos)*; TCC-PROFMAT/AC; SBM/IMPA; Rio Branco, AC - 2016.

[3] BOLDRINI, J. L.; Costa, S. I. R.; Ribeiro, V. L., Wetzler, H. G.; *Álgebra Linear*; Harper-Row, São Paulo, SP - 1980.

[4] GONÇALVES, Adilson de Sousa e Rita M. L; *Introdução À Álgebra Linear*; Ed. Edgard Blucher Ltda; São Paulo, SP - 1977.

[5] HOFFMAN, Kenneth e KUNZE, Ray; *Álgebra Linear*; 2ª edição; LTC; Rio de Janeiro, RJ - 1979.

[6] HOWARD, Anton e RORRES, Chris; *Álgebra Linear com aplicações*; 10ª edição; Editora Bookman; Porto Alegre, RS - 2012.

[7] LANG, Serge; *Álgebra Linear*; Ed. Edgard Blucher Ltda; São Paulo, SP - 1971.
[8] LIPSCHUTZ, Seymour; *Álgebra Linear*. Makron Books do Brasil Editora Ltda; Editora McGraw-Hill Ltda – (Coleção Schaum); São Paulo, SP - 1994.

Lemuel de Freitas Ponce
Rua do macarrão, nº 843 – Bairro Belo Jardim I
Rio Branco – Acre.
CEP: 69907-824
lemuel_ponce@yahoo.com.br
(68)3901-2536 e (68)999017315.

José Ivan da Silva Ramos
Rua Maranhão I, nº 133 – Bairro Bosque
Rio Branco – Acre.
CEP: 69900-484
ivanr@ufac.br
(68)3901-2536 e (68)999527503.

Revista
ELEMENTOS

A estrutura algébrica dos vértices de um polígono regular

José Ivan da Silva Ramos
Professor associado do Centro de Ciências Exatas e Tecnológicas da Ufac

Henrique Hiroto Yokoy
Mestre em Matemática e professor efetivo do Colégio de Aplicação da Ufac

Resumo

Desde que o resto da divisão de um inteiro positivo $n \geq 3$ por um inteiro $d > 0$ fica limitado por 0 e $d - 1$, podemos estabelecer uma correspondência biunívoca entre o conjunto das classes residuais módulo n e o conjunto das raízes de ordem n da unidade complexa. Dado que cada uma dessas raízes representa um vértice de um polígono regular, temos, por isomorfismo, que o conjunto desses pontos do plano, aditivamente, é uma cópia do conjunto $\mathbb{Z}_n$.

Abstract

Since the remainder of the division of a positive integer $n \geq 3$ by an integer $d > 0$ is bounded by 0 and $d - 1$, can establish a biunivocal correspondence between the set of residue classes module n and the set of order n roots of complex unit . Given that each of these roots is a vertex of a regular polygon, we have, by isomorphism, that all of these points in the plane, additively, is a copy of the set $\mathbb{Z}_n$.

Palavras chave: Conjuntos, operações, isomorfismos e polígonos.

1. Introdução

Um importante resultado que envolve os números inteiros e o conceito de divisão é o algoritmo da divisão euclidiana: para quaisquer dois inteiros a e b, com $a \neq 0$, sempre existem dois únicos inteiros q e r, tais que $b = qa + r$ e $0 \leq r < |a|$.

O estudo das funções, em conjunto com as estruturas algébricas, permite que façamos boas comparações. Os isomorfismos entre os espaços vetoriais, que estudamos na Álgebra Linear, são particulares exemplos de como podemos associar os aspectos algébricos de duas estruturas. Por exemplo, partindo de uma definição de multiplicação entre pontos (ou vetores) do plano, podemos definir um homomorfismo bijetor do conjunto $\mathbb{C}$ dos números complexos para $\mathbb{R}^2$, que é uma forma concreta de apresentarmos esses números.

Esse é um dos pontos de partida para a comparação entre duas estruturas que queremos fazer. Vamos, a partir das raízes de ordem n da unidade complexa, determinar um polígono regular de n lados e, através de um isomorfismo, mostrar que o conjunto dos vértices desse polígono pode ser identificado como o conjunto das classes de equivalência módulo n, este inteiro. As noções da teoria dos conjuntos, o emprego do Algoritmo da divisão de Euclides, propriedades do Máximo Divisor Comum e as descrições do conjunto dos números complexos, além da identificação das raízes da unidade como sendo vértices de um polígono regular, nos convidam a fazer uma leitura agradável e complementar, no sentido de que os conteúdos estão organizados e rigorosamente de acordo com a linguagem matemática e podem servir de material de apoio para professores e estudantes de matemática.

Os conceitos da Teoria dos Conjuntos englobam operações e suas propriedades e as relações de equivalência, onde destaca-se a relação de congruência modulo um inteiro n. As noções de Aritmética nos permitem concluir que o conjunto quociente de $\mathbb{Z}$ por $\equiv (mod\ n)$, definido por $\mathbb{Z}/_{\equiv (mod\ n)} = \mathbb{Z}_n = \{\bar{z}/z \in \mathbb{Z}\}$, contém exatamente n elementos e que nele podemos definir operações de adição e multiplicação. Nesse contexto, o Algoritmo da Divisão Euclidiana é decisivo. Com isso, a descrição do conjunto dos números complexos, utilizando o conceito de homomorfismo, nos permite ver que $\mathbb{C}$ é isomorfo ao plano $\mathbb{R}^2$ e que nos possibilita apresentar formas mais concretas de um número complexo.

2. Apresentação de resultados

O conceito de polígonos regulares já aparece nos estudos secundários, quando estudamos a área das figuras planas, longe de sabermos da engenhosidade geométrica envolvida na construção desses objetos, a depender das ferramentas que podem ser usadas.

2.1 Polígonos regulares

De início, podemos analisar que a construtibilidade dos polígonos regulares, por meio de régua e compasso, é bastante acessível e, com o uso do Geogebra, dispomos de uma grande ferramenta para construção das figuras mencionadas. Dessa forma, polígonos regulares como triângulos equiláteros, quadrados, pentágonos e hexágonos são naturalmente construtíveis com noções de Geometria Euclidiana.

Em 1726, Gauss, aos 19 anos, mostrou que a construção do heptágono regular e de outros polígonos regulares era impossível através de processos euclidianos, investigou ainda a construtibilidade dos polígonos regulares de p lados, sendo p um número primo.

Nessa investigação Gauss provou o seguinte resultado:

2.1.1 Observação (Teorema de Gauss-Wantzel): um polígono regular de n lados pode ser construído com régua e compasso se, e somente se, $n = 2^{\alpha}$ ou $n = 2^{\alpha}p_1p_2 \cdots p_r$; onde $p_1, p_2, \dots, p_r$ são números primos distintos da forma $p = 2^{2^{\beta}} + 1$ e α e β são números inteiros; ou seja, são números primos de Fermat.

Demonstração (Ver: GONZÁLEZ, N. R; LÓPEZ, P. L.; NÓVOA, E. V. *Teoría de Galois*. Santiago de Compostela. 2013; página 200).

Com isso, é possível prever que:

a) É possível construir os seguintes polígonos (até 20 lados): os de 3, 4, 5, 6, 8, 10, 12, 15, 16, 17 e 20 lados, incluindo todos os construídos por Euclides, tendo em vista que podemos escrever: $3 = 2^0.3$, $4 = 2^2$, $5 = 2^0.5$, $6 = 2^1.3$, $8 = 2^3$; $10 = 2^1.5$, $12 = 2^2.3$, $15 = 2^0.3.5$, $16 = 2^4$, $17 = 2^0.17$ e $20 = 2^2.5$.

b) Os polígonos regulares de 7, 9 e 27 lados não são construtíveis com o uso de régua e compasso.

c) Os polígonos regulares com um número primo de lados são, portanto, o triângulo e o pentágono, construídos por Euclides e os de lados $n = 2^{2^{\beta}} + 1$.

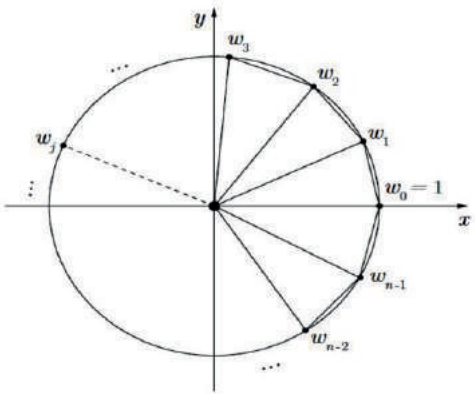
Agora, mostraremos que, ao representarmos geometricamente as raízes de ordem n da unidade complexa, acabamos por obter o desenho de um polígono regular, inscrito em um círculo unitário. Isso, de certa forma, resolve o problema da impossibilidade da construtibilidade através de régua e compasso de alguns polígonos regulares, devido à observação de Gauss, em 2.1.1.

De acordo com as definições sobre módulo e argumento de um número complexo e considerando a forma polar e a representação geométrica de cada raiz da unidade, podemos relacionar o seguinte resultado.

2.1.2 Observação: as n raízes de $1 = 1 + 0i \in \mathbb{C}$, $w_k = cos\frac{2k\pi}{n} + isen\ \frac{2k\pi}{n}$; com $k = 0, 1, \cdots, n-1$, ocupam os vértices de um polígono regular de n lados, inscrito no círculo unitário e centrado na origem do plano de Argand-Gauss.

Demonstração: Sendo $z = 1 = 1 + 0i$, vale que $|z| = \sqrt{1^2 + 0^2} = 1$. Assim, temos $|w_k| = \sqrt{|z|} = 1$, ou seja, cada raiz está sobre uma circunferência de raio unitário e de centro na origem. Além disso, observamos que $\arg(w_{k+1}) - \arg(w_k) = \frac{2\pi}{n}$, o que mostra que essas raízes ocupam os vértices de um polígono regular de n lados, inscrito no círculo unitário de centro na origem.

Figura 01: Representação geométrica das raízes enésimas da unidade



2.1.3 Exemplo:

As raízes são

$w_0 = cos0 + isen\ 0 = 1 + 0i;$

$w_1 = cos\frac{2\pi}{7} + isen\frac{2\pi}{7};$

$w_2 = cos\frac{4\pi}{7} + isen\frac{4\pi}{7};$

$w_3 = cos\frac{6\pi}{7} + isen\frac{6\pi}{7};$

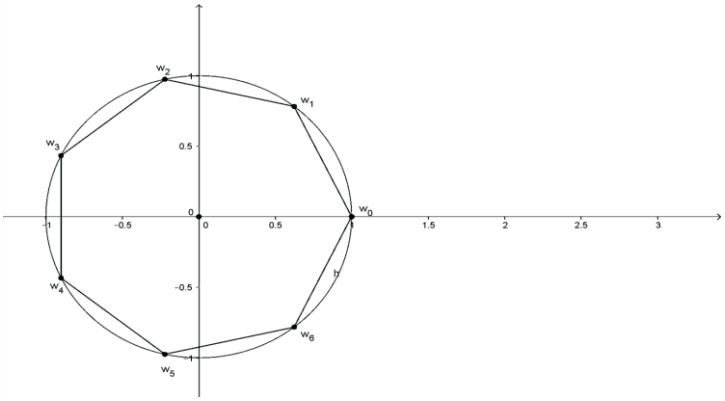
$w_4 = cos\frac{8\pi}{7} + isen\frac{8\pi}{7};$

$w_5 = cos\frac{10\pi}{7} + isen\frac{10\pi}{7};$

$w_6 = cos\frac{12\pi}{7} + isen\frac{12\pi}{7};$

Isso nos dá a representação geométrica abaixo

Figura 02: Representação geométrica das raízes sétimas da unidade



Da mesma forma, conseguimos construir os polígonos de 9 e 27 lados com mais precisão.

De maneira geral, destacamos a facilidade que é, através da representação geométrica das raízes da unidade complexa, construir um polígono regular de $2 < n$ lados, sendo n um inteiro positivo fixo.

Seguimos fazendo, ainda, o uso de construções geométricas como parte da discussão em torno do principal objetivo de nosso trabalho, que é o de podermos mostrar que a estrutura do conjunto desses pontos do plano, que determinam um polígono regular de $2 < n$ lados, pode ser comparada, aditivamente, à estrutura do conjunto das classes determinadas pela relação congruência módulo n, inteiro.

Doravante, $\mathbb{U}_n = \left\{w_k = cos\frac{2k\pi}{n} + isen\ \frac{2k\pi}{n} / \ 2 < n \in \mathbb{Z} \text{ e } k = 0, 1, \cdots, n-1\right\}$ denotará *o conjunto das raízes de ordem* $2 < n$ *da unidade complexa*.

2.2 A multiplicação de números complexos no conjunto $\mathbb{U}_n$

Conhecemos do Cálculo Diferencial que, usando séries de potências, podemos escrever a identidade de Euler: $e^{i\theta} = cos\theta + isen\theta$.

Através dessa relação, podemos observar qual o efeito ao multiplicarmos duas raízes da unidade complexa. Em geral, escrevendo um número complexo na forma $z = |z|(\cos\theta + i\text{sen}\theta) = |z|e^{i\theta}$, teríamos, para cada $k = 0, 1, \cdots, n-1$, as raízes de ordem n da forma $w_k = e^{\frac{2k\pi i}{n}}$, e perceberíamos o efeito somativo no expoente desse produto.

Mas, apostamos no entendimento de que podemos fazer uma boa comparação desses objetos e, mesmo evitando o uso dos conceitos do cálculo diferencial, entender como objetos da Geometria (de Euclides) surgem como elementos de uma Estrutura Algébrica e vice versa.

Os exemplos a seguir dão uma ideia do porquê de termos restringido nossas discussões ao conjunto $\mathbb{U}_n$.

2.2.1 Exemplo: seja $A = \{z \in \mathbb{C}/z^4 = 2\}$. Através de contas simples, percebemos que $A = \left\{\sqrt[4]{2}, \sqrt[4]{2}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right), \sqrt[4]{2}(cos\pi\ + isen\pi), \sqrt[4]{2}\left(cos\ \frac{3\pi}{2} + isen\ \frac{3\pi}{2}\right)\right\}$.

Calculando, por exemplo, algumas potências de $w_1 = \sqrt[4]{2}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right)$, temos:

$w_1 = \sqrt[4]{2}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right)$,

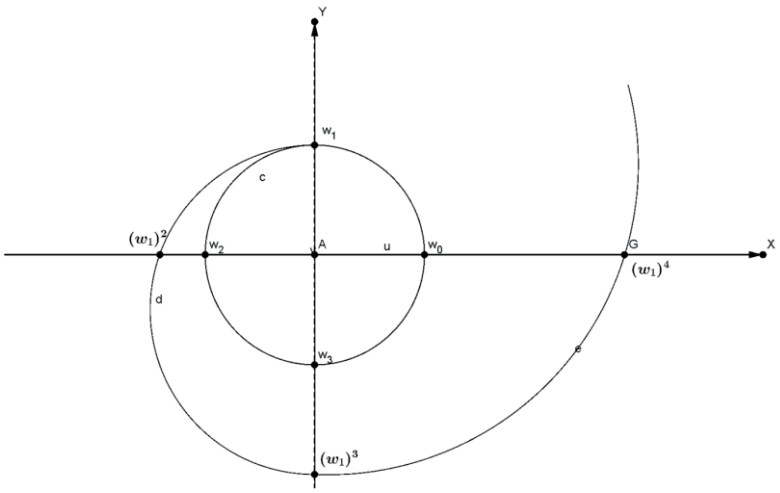
$w_1^2 = w_1 w_1 = \left(\sqrt[4]{2}\right)^2\left(cos\ \left(\frac{\pi}{2} + \frac{\pi}{2}\right) + isen\left(\frac{\pi}{2} + \frac{\pi}{2}\right)\right) = \sqrt{2}(cos\pi\ + isen\,\pi)$,

$w_1^3 = w_1^2 w_1 = \sqrt{2}(cos\pi\ + isen\,\pi)\sqrt[4]{2}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right) = \sqrt[4]{2^3}\left(cos\ \frac{3\pi}{2} + isen\ \frac{3\pi}{2}\right)$,

$w_1^4 = w_1^3 w_1 = \sqrt[4]{2^3}\left(cos\ \frac{3\pi}{2} + isen\ \frac{3\pi}{2}\right)\sqrt[4]{2}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right) = 2(cos2\pi + isen2\pi)$.

Podemos observar, na figura 03, que, embora as raízes quartas de $z = 2$ possam representar vértices de um quadrado, as potências de w_1 "explodem", no sentido de que o módulo dessas potências aumenta e as afasta do conjunto A, quando as afasta da origem do plano. Isso, claro, também mostra que A não é fechado para a multiplicação definida em $\mathbb{C}$.

Figura 03: Representação das raízes quartas de $z = 2$ e potências de $w_1 = \sqrt[4]{2}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right)$



Além deste, podemos exemplificar mais dois conjuntos que não são multiplicativamente fechados em $\mathbb{C}$:

2.2.2 Exemplo: seja $B = \left\{z \in \mathbb{C}/z^4 = \frac{1}{2}\right\}$. Então, alguns cálculos simples mostram que $B = \left\{\sqrt[4]{\frac{1}{2}}, \sqrt[4]{\frac{1}{2}}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right), \sqrt[4]{\frac{1}{2}}(cos\pi\ + isen\pi), \sqrt[4]{\frac{1}{2}}\left(cos\ \frac{3\pi}{2} + isen\ \frac{3\pi}{2}\right)\right\}$. As primeiras potências de $w_1 = \sqrt[4]{\frac{1}{2}}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right)$ são:

$w_1 = \sqrt[4]{\frac{1}{2}}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right)$,

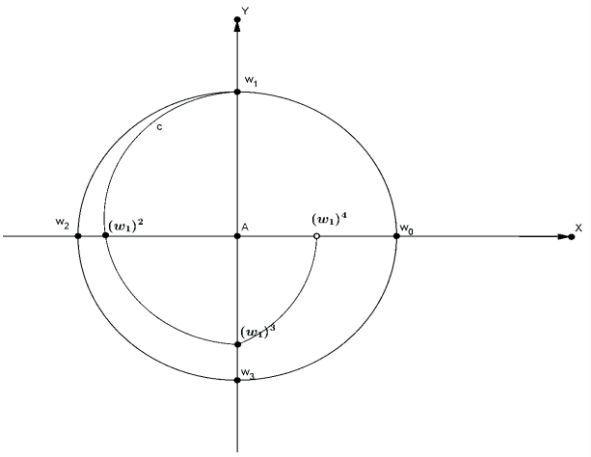
$w_1^2 = w_1 w_1 = \left(\sqrt[4]{\frac{1}{2}}\right)^2 \left(cos\ \left(\frac{\pi}{2} + \frac{\pi}{2}\right) + isen\left(\frac{\pi}{2} + \frac{\pi}{2}\right)\right) = \sqrt{\frac{1}{2}}(cos\pi\ + isen\,\pi)$,

$w_1^3 = w_1^2 w_1 = \sqrt{\frac{1}{2}}(cos\pi\ + isen\,\pi)\sqrt[4]{\frac{1}{2}}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right) = \sqrt[4]{\frac{1}{2^3}}\left(cos\ \frac{3\pi}{2} + isen\ \frac{3\pi}{2}\right)$

$w_1^4 = w_1^3 w_1 = \sqrt[4]{\frac{1}{2^3}}\left(cos\ \frac{3\pi}{2} + isen\ \frac{3\pi}{2}\right)\sqrt[4]{\frac{1}{2}}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right) = \frac{1}{2}(cos2\pi + isen2\pi)$.

Mais uma vez, vemos que, embora as raízes quartas de $z = \frac{1}{2}$ possam representar vértices de um quadrado, as potências de w_1 "encolhem", no sentido de que o módulo dessas potências diminui e as afasta do conjunto B, enquanto as aproxima da origem do plano. Por isso, também concluímos que B não é fechado para a multiplicação definida em $\mathbb{C}$.

Figura 04: Representação das raízes quartas de $z = \frac{1}{2}$ e potências de $w_1 = \sqrt[4]{\frac{1}{2}}\left(cos\ \frac{\pi}{2} + isen\ \frac{\pi}{2}\right)$



Em nosso próximo exemplo, para não induzir um pensamento errado, consideraremos que z não seja um número "real puro", onde $\mathrm{Im}(z) = 0$.

Mesmo assim, o exemplo trata de um caso muito particular de cálculo de raízes e potências de um número complexo.

2.2.3 Exemplo: seja $C = \left\{z \in \mathbb{C}/z^4 = \frac{1}{2} + \frac{\sqrt{3}}{2}i\right\}$. Nesse caso, $|z| = \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2} = 1$ e $C = \left\{cos\frac{\pi}{12} + isen\frac{\pi}{12}, cos\frac{7\pi}{12} + isen\frac{7\pi}{12}, cos\frac{13\pi}{12} + isen\frac{13\pi}{12}, cos\frac{19\pi}{12} + isen\frac{19\pi}{12}\right\}$. Daí, para $w_1 = cos\frac{7\pi}{12} + isen\frac{7\pi}{12}$, temos:

$w_1 = cos\frac{7\pi}{12} + isen\frac{7\pi}{12}$,

$w_1^2 = w_1 w_1 = cos\ \left(\frac{7\pi}{12} + \frac{7\pi}{12}\right) + isen\left(\frac{7\pi}{12} + \frac{7\pi}{12}\right) = cos\frac{7\pi}{6} + isen\frac{7\pi}{6}$,

$w_1^3 = w_1^2 w_1 = \left(cos\frac{7\pi}{6} + isen\frac{7\pi}{6}\right)\left(cos\frac{7\pi}{12} + isen\frac{7\pi}{12}\right) = cos\ \frac{7\pi}{4} + isen\ \frac{7\pi}{4}$

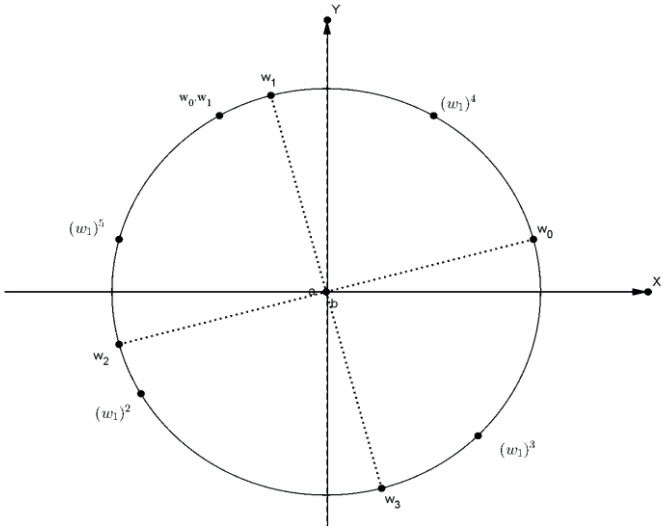
$w_1^4 = w_1^3 w_1 = \left(cos\frac{7\pi}{4} + isen\frac{7\pi}{4}\right)\left(cos\frac{7\pi}{12} + isen\frac{7\pi}{12}\right) = cos\ \frac{7\pi}{3} + isen\ \frac{7\pi}{3}$

$w_1^5 = w_1^4 w_1 = \left(cos\frac{7\pi}{3} + isen\frac{7\pi}{3}\right)\left(cos\frac{7\pi}{12} + isen\frac{7\pi}{12}\right) = cos\ \frac{35\pi}{12} + isen\ \frac{35\pi}{12}$

Percebemos, na figura 05, que o argumento de w_1^n, com $n = 1, 2, 3, 4$ ou 5, não coincide com nenhum dos argumentos das raízes quartas de $z = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ e, assim, a representação geométrica dessas potências não pode coincidir com a representação geométrica dessas raízes.

Além disso, notemos que $w_0 w_1 = cos\frac{8\pi}{12} + isen\frac{8\pi}{12} \neq w_k,\ \forall\ k \in \{0,1,2,3\}$, mostrando que C não é multiplicativamente fechado.

Figura 17: Representação das raízes quartas de $z = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ e potências de $w_1 = cos\ \frac{7\pi}{12} + isen\ \frac{7\pi}{12}$



Notemos que, independentemente dos números complexos que consideramos nesses exemplos, o desenho de um polígono regular, no caso de um quadrado, sempre pode ser feito, o que poderia tornar sem sentido querer comparar o conjunto dos vértices de polígonos regulares, considerando somente o conjunto $\mathbb{U}_n$ das raízes da unidade complexa.

O problema com o fechamento da multiplicação visto nesses exemplos justifica nossa ideia de olhar exatamente no conjunto desses objetos geométricos. Esse é um dos cuidados que temos que ter e que dá sentido aos nossos esforços para tentar comparar $\mathbb{U}_n$ com outro "mundo", onde, de certo, já sabemos podemos manipular objetos com segurança.

2.2.4 Observação: o conjunto $\mathbb{U}_n$, formado pelas raízes enésimas da unidade complexa, é multiplicativamente fechado.

Demonstração: basta lembrar a definição de *argumento* (*principal*) *do número complexo z*. A unicidade do ângulo $\theta = \arg(z) \in]-\pi, \pi]$ e a regra de que o produto de dois números complexos, na forma polar, é igual a um número complexo, cujo módulo é o produto dos módulos e cujo argumento é a soma dos argumentos dos números complexos multiplicados, mostram que o resultado da multiplicação de dois elementos de $\mathbb{U}_n$ é também uma raiz de ordem n da unidade complexa.

3. A álgebra dos vértices de um polígono regular

Conforme nossas observações constantes do item 2, podemos manipular as raízes da unidade complexa com certa segurança. Isso é um convite para investigarmos as propriedades da multiplicação definida em $\mathbb{U}_n$.

Na forma polar, cada raiz da unidade complexa tem módulo igual a 1 e, por isso, multiplicar esses objetos significa, efetivamente, efetuar uma soma.

3.1 Observação: com relação à operação de multiplicação, valem as propriedades, $\forall\, w_h, w_j, w_l \in \mathbb{U}_n = \left\{w_k = cos\frac{2k\pi}{n} + isen\frac{2k\pi}{n} / \, 2 < n \in \mathbb{Z} \text{ e } k = 0, 1, \cdots, n-1\right\}$:

$-$ Associatividade: $w_h\,(w_j w_l) \;= \left(w_h w_j\right)w_l$;

$-$ Comutatividade: $w_h w_j = w_j w_h$;

$-$ Existência de elemento neutro: $\exists\, 1 + 0i = w_0 = cos\frac{2.0.\pi}{n} + isen\frac{2.0.\pi}{n} = cos0 + isen0$, tal que $(1 + 0i)w_h = w_h(1 + 0i) = w_h$;

$-$ Existência de inverso: $\forall w_h \in \mathbb{U}_n, \exists\, w_g \in \mathbb{U}_n$, tal que, sendo $w_g = cos\frac{2g\pi}{n} + isen\frac{2g\pi}{n}$, vale que $w_h w_g = w_g w_h = 1 = 1 + 0i$.

Demonstração: as propriedades de associatividade e comutatividade valem, por herança, de $\mathbb{C}$ para $\mathbb{U}_n$. Como $1 = w_0 = cos\frac{2.0.\pi}{n} + isen\frac{2.0.\pi}{n} = cos0 + isen0$ é uma raiz da unidade, a existência de elemento neutro está garantida.

Agora, sendo $w_h = cos\frac{2h\pi}{n} + isen\frac{2h\pi}{n}$, com $h = 0, 1, \cdots, n-1$, basta tomar $g = n - h$ para termos $w_h w_g = w_g w_h = (1 + 0i) = w_0$.

Continuaremos com os nossos argumentos, de modo que possamos dar uma ideia de como o conjunto $\mathbb{U}_n$, dos vértices de um polígono regular, pode ser visto como uma estrutura algébrica.

Olhemos por um momento as tábuas das operações de adição e multiplicação em $\mathbb{Z}_3$ e em $\mathbb{U}_3$, respectivamente:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\cdot$	w_0	w_1	w_2
w_0	w_0	w_1	w_2
w_1	w_1	w_2	w_0
w_2	w_2	w_0	w_1

Quem olha, mesmo sabendo que a tabela acima e do lado direito provém de uma multiplicação, tende a acompanhar o raciocínio da soma feita na tabela da esquerda, olhando os índices do rodapé de w_k com $k = 0, 1, 2$.
Nesse sentido, o resultado abaixo nos mostra que podemos comparar $\mathbb{U}_n$ com o conjunto das classes de equivalência $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$.

Uma descrição da estrutura de $\mathbb{Z}_n$ pode ser vista em nossa referência de número [4].

3.2 Observação: a função δ, definida abaixo, é um homomorfismo bijetor.

$$\begin{array}{rcl} \delta\colon (\mathbb{U}_n, .) & \longrightarrow & (\mathbb{Z}_n, +) \\ w_k & \longmapsto & \delta(w_k) = \bar{k} \end{array}$$

Demonstração: primeiramente, $\forall\ w_j, w_l \in \mathbb{U}_n = \mathrm{D}(\delta)$, domínio da função δ, se temos $\delta(w_j) = \delta(w_l)$, então vale que $\bar{j} = \bar{l}$. Pela observação em 1.1.20; pág. 21 de [11], temos $j = l$, consequentemente, $w_j = w_l$ e δ é injetiva. Agora, para toda classe $\bar{x} \in \mathbb{Z}_n = \mathrm{CD}(\delta)$, contradomínio da função δ, vale que $x \in \{0, 1, \cdots, n-1\}$, conforme a observação em 1.2.9; pág. 25 de [11]. Assim, para esse inteiro x, a raiz da unidade $w_x \in \mathbb{U}_n = \mathrm{D}(\delta)$ é tal que $\delta(w_x) = \bar{x}$, o que prova a sobrejetividade da função δ.

Por fim, veremos que δ é um homomorfismo. De fato: $\forall\ w_j, w_l \in \mathbb{U}_n = \mathrm{D}(\delta)$, vale que $\delta(w_j . w_l) = \delta\left(\left(cos\frac{2j\pi}{n} + isen\ \frac{2j\pi}{n}\right).\left(cos\frac{2l\pi}{n} + isen\ \frac{2l\pi}{n}\right)\right)$. Assim, vale que $\delta\left(cos\left(\frac{2j\pi}{n} + \frac{2l\pi}{n}\right) + isen\left(\frac{2j\pi}{n} + \frac{2l\pi}{n}\right)\right) = \delta\left(cos\left(\frac{2(j+l)\pi}{n}\right) + isen\left(\frac{2(j+l)\pi}{n}\right)\right)$ e, por isso, temos $\delta\left(w_j . w_l\right) = \delta\left(w_{j+l}\right) = \overline{j+l} = \bar{j} + \bar{l} = \delta(w_j) + \delta(w_l)$. Concluímos, então, que $\mathbb{U}_n \cong \mathbb{Z}_n$.

Esse isomorfismo, além de identificar cada raiz de ordem n da unidade complexa com uma classe $\bar{x}$ do conjunto quociente de $\mathbb{Z}$, pela relação $\equiv (mod\ n)$, diz que resultados que valem para a estrutura multiplicativa de $\mathbb{U}_n$ valem, de maneira equivalente, para a estrutura aditiva de $\mathbb{Z}_n$ e vice versa.

Nós iremos então, por comparação, relacionar algumas propriedades, que, aditivamente, a estrutura de $\mathbb{Z}_n$ possui e, assim, dar uma descrição mais completa da estrutura multiplicativa de $\mathbb{U}_n$.

3.3 Definição: seja G um conjunto não vazio no qual a operação $*$ esteja definida. Então, se $g \in G$, definimos:

a) $\langle g \rangle = \{g^n / \ n \in \mathbb{Z}\}$, o conjunto de todas as potências inteiras de $g \in G$.

b) Se a operação $*$ admite elemento neutro e, o menor inteiro positivo t tal que $g^t = e$, é denominado de *ordem* do elemento g.

c) Se tivermos $\langle g \rangle = \{g^n / \ n \in \mathbb{Z}\} = G$, dizemos que G é um *conjunto cíclico*. Nesse caso, g é denominado de (um) *gerador* de G.

A observação a seguir nos dá uma boa ideia de como podemos aproveitar dessa identificação de $\mathbb{U}_n$ como sendo o conjunto $\mathbb{Z}_n$.

3. 4 Observação: se $2 < n \in \mathbb{Z}$ e n é ímpar, vale que $\prod_{k=0}^{n-1} w_k = 1$.

Demonstração: olhando para as discussões feitas no parágrafo 1.4 de [11], vemos que $\delta\left(\prod_{k=0}^{n-1} w_k\right) = \delta\left(w_{0+1+\cdots(n-1)}\right) = \overline{0+1+\cdots(n-1)}$. E isso é, sob a barra, uma soma de uma P. A. de razão e termo inicial iguais a 1. Assim, esse produto é igual a $\delta\left(\prod_{k=0}^{n-1} w_k\right) = \frac{\overline{n.(n-1)}}{2}$, mas como n é impar, vale que $n = 2k+1, k \in \mathbb{Z}$, ou seja, vale que $\delta\left(\prod_{k=0}^{n-1} w_k\right) = \frac{\overline{n.2k}}{2} = \overline{n.k} = \bar{0}$.

Agora, δ é um homomorfismo bijetor, particularmente, δ é injetivo. E como $\delta\left(1 = w_0 = cos\frac{2.0.\pi}{n} + isen\frac{2.0.\pi}{n} = cos0 + isen0\right) = \bar{0}$, resta que $\prod_{k=0}^{n-1} w_k = 1$. ∎

E o que é $\sum_{k=0}^{n-1} w_k = w_0 + w_1 + \cdots + w_{n-1}$, se $2 < n \in \mathbb{Z}$? Curiosamente, essa soma é nula! Podemos testar isso efetuando alguns cálculos nos casos em que n é pequeno.

Façamos para $n = 4$, assim temos as raízes

$w_0 = cos\frac{2.0.\pi}{4} + isen\frac{2.0.\pi}{4} = cos0 + isen0 = 1$;

$w_1 = cos\frac{2.1.\pi}{4} + isen\frac{2.1.\pi}{4} = cos\frac{\pi}{2} + isen\frac{\pi}{2} = 0 + i;$

$w_2 = cos\frac{4\pi}{4} + isen\frac{4\pi}{4} = -1 + 0i.$

$w_3 = cos\frac{3\pi}{2} + isen\frac{3\pi}{2} = 0 - i.$

Temos uma soma nula, que é $w_0 + w_1 + w_2 + w_3 = 0$.

É claro que a soma de duas raízes da unidade não é uma raiz da unidade. No caso acima, temos que $w_0 + w_1 = 1 + i$ não é uma raiz da unidade. Isso significa que a adição dos números complexos não está definida no conjunto $\mathbb{U}_4$.

Assim, esse fato de que essa soma é nula, que também pode ser verificado com régua e compasso, nos casos em que n é pequeno, imaginando cada elemento de $\mathbb{U}_n$ como um vetor centrado na origem do plano, não deve ser tratado via o isomorfismo que definimos em 3.2.

Agora, vamos definir uma estrutura algébrica amplamente estudada e que termina por dar a noção exata da estrutura de $\mathbb{U}_n$, vista através da identificação desse conjunto com o conjunto $\mathbb{Z}_n$.

3.5 Definições: seja $*$ uma operação definida em um conjunto não vazio G.

a)Dizemos que G é um *grupo* com respeito à operação $*$ (e anotamos $(G,*)$) se, e somente se, $\forall\ g_1, g_2, g_3 \in G$, valem:

− Associatividade: $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$;

− Existência de elemento neutro: $\exists\ e \in G$ tal que $e * g_1 = g_1 * e = g_1$;

− Existência de inverso: $\exists {g_1}^{-1} \in G$ tal que ${g_1}^{-1} * g_1 = g_1 * {g_1}^{-1} = e$.

b) Dizemos que G é um *grupo comutativo* (abeliano) se, além dessas propriedades citadas acima, valer que:

− Comutatividade: $g_1 * g_2 = g_2 * g_1$.

Por toda essa análise que fizemos podemos enunciar o seguinte resultado:

3.6 Observação: o conjunto dos pontos dos vértices de um polígono regular, inscrito em uma circunferência de raio 1, é um grupo abeliano finito.

Demonstração: imediata. (Ver as observações 1.3.4 e 2.3.2 em [11]). Temos que $(\mathbb{Z}_n, +)$ é um grupo abeliano, $\forall\ 2 < n \in \mathbb{Z}$ e vale que $(\mathbb{U}_n, .) \cong (\mathbb{Z}_n, +)$.

4. Considerações Finais

Percebemos que, ao representarmos geometricamente as raízes de ordem n da unidade complexa, acabamos por determinar um processo eficiente de se obter o desenho de um polígono regular; já que, segundo Gauss, por meio de régua e compasso, certos polígonos regulares não podem ser construídos. Com o uso do Geogebra, podemos inserir as raízes enésimas da unidade e, dessa forma, obter um polígono regular, independente da escolha do inteiro $n > 2$.

A volta que demos até conseguirmos identificar o grupo abeliano, formado pelos vértices de um polígono regular, através da estrutura aditiva de $\mathbb{Z}_n$, sempre que $2 < n \in \mathbb{Z}$, representa um passeio agradável pelos conceitos básicos de Álgebra e Geometria. É claro que é possível provarmos que, multiplicativamente, $U = \{z \in \mathbb{C} / |z| = 1\}$ é uma subestrutura de $\mathbb{C}$, mas isso não deixa que percebamos a conectividade que existe entre os importantes conceitos algébricos e geométricos que foram relacionados aqui.

5. Referências

[1] STEWART, Ian. *17 equações que mudaram o mundo*. Traduzido por George Schlesinger; 1ª edição; ZAHAR, 2013.

[2] CONTEÚDO aberto. In: *Wikipédia*: a enciclopédia livre. Disponível em: <https: //pt.wikipedia.org/wiki/Ren%C3%A9_Descartes>. (Acesso em 23.04.2015)

[3] LAUTERT, S. L; SPINILLO, A. G. *As relações entre o desempenho em problemas de divisão e as concepções de criança sobre a divisão*. Psicologia: Teoria e Pesquisa, Brasília, v. 18, n. 3, p. 237-246, 2002.

[4] GONÇALVES, Adilson. *Introdução à álgebra*. 5ª ed. Rio de Janeiro: IMPA 2008.

[5] HEFEZ, Abramo. *Aritmética*; SBM, 2013 (Coleção PROFMAT).

[6] GONZÁLEZ, N. R; LÓPEZ, P.L; NÓVOA, E. V. *Teoría de Galois*. Santiago de Compostela. 2013. Disponível em < http://www.usc.es/regaca/Galois.pdf>. Acesso em (20.03.2015).

[7] PRECIOSO, J. Conceição; PEDROSO, Hermes Antônio. *O problema da construção de polígonos regulares de Euclides a Gauss*. Disponível em

<http://www.portal.famat.ufu.br/sites/famat.ufu.br/files/Anexos/Bookpage/famat_revista_13_artigo_6_0.pdf>. (Acesso em 14.12.2014).

[8] WEISS, William A. R. (2008); *An introduction to set theory*. Disponível em <http://www.math.toronto.edu/weiss/set_theory.html>. (Acesso em 17.08.2014).

[9] CONTEÚDO aberto. In: *Wikipédia*: a enciclopédia livre. Disponível em: <https://pt.wikipedia.org/wiki/N%C3%BAmero_complexo>. (Acesso em 23.04.2015).

[10] GEOGEBRA. *Software de Geometria Dinâmica*. Disponível Versão 4.4.(2013). Acessado: 15 de Dez de 2014.

[11] YOKOYAMA, H. Hiroto; *A estrutura dos vértices de um polígono regular*; TCC-Profmat/SBM/IMPA; Rio Branco-AC; julho de 2005.

José Ivan da Silva Ramos
Rua Maranhão I, nº 133 – Bairro Bosque
Rio Branco – Acre.
CEP: 69900-484
ivanr@ufac.br
(68)3901-2536 e (68)999527503.

Henrique Hiroto Yokoyama
Colégio de Aplicação
Universidade Federal do Acre
Rio Branco - Acre
prof.hiroto@oi.com.br
(68)999613847

Revista
ELEMENTOS

Dedicado para Aízis

Sézani Morais Gonçalves de Carvalho
Mestre em Matemática e servidor da Universidade Federal de Rondônia

Tomás Daniel Menéndez Rodrígues
Professor titular do departamento de Matemática da Universidade Federal de Rondônia

Resumo

A teoria dos Códigos Corretores de Erros, em virtude do forte avanço tecnológico ao qual temos presenciado, em especial nas áreas de telecomunicações, tem exercido papel importante na confiabilidade em transmissões e armazenamento de dados. Neste trabalho apresentamos uma parte dessa teoria, mais precisamente, os códigos lineares, suas características e o seu funcionamento na codificação e decodificação de mensagens.

Abstract

The theory of Error Correcting Codes, due to the strong technological advancement to which we have witnessed, especially in the areas of telecommunications, has played an important role in reliability in transmission and data storage. We present a part of this theory, more precisely, linear codes, their characteristics and their operation in the encoding and decoding messages

Palavras Chave: Espaço vetorial, códigos, código linear, erros, distância de Hamming, peso, codificação e decodificação.

1. Introdução

O avanço rápido da tecnologia tem propiciado grandes vantagens no armazenamento de dados ou na comunicação realizada através aparelhos eletrônicos, como celulares, tablets, microcomputadores. Um aspecto relevante nesse processo é saber se informações enviadas ou armazenadas em alguma mídia serão recebidas ou acessadas de forma íntegra. Tais informações são passíveis de erros? Caso haja erros, será possível detectar e fazer as correções? Pensando em responder essas questões, apresentamos em nosso trabalho os conceitos e resultados relacionados aos Códigos Lineares que fazem parte da Teoria dos Códigos Corretores de Erros.

O que é um código?

Consideremos um alfabeto formado pelos 38 caracteres do conjunto $P = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z, \text{á}, \text{à}, \text{â}, \text{ã}, \text{é}, \text{ê}, \text{í}, \text{ó}, \text{ô}, \text{õ}, \text{ú}, \_\}$, onde "_" representa o espaço entre as palavras. Supostamente, temos que "pneumoultramicroscopicossilicovulcanoconiótico"[1] é a maior palavra escrita com os elementos do conjunto P. Notemos que P possui 38 elementos (caracteres) e que a maior palavra escrita com seus elementos possui 46 caracteres. Por meio de acréscimos de "espaços" ao fim, podemos fazer com que cada palavra escrita com os elementos de P possua exatamente 46 caracteres. Definimos assim um *código* como sendo um conjunto $C \subset P^{46}$ de todas as palavras existentes no nosso idioma. O código C não é eficiente para detectar e corrigir erros, pois, se transmitirmos as palavras *"telefone", "bola" e "caneca"* e, por algum motivo ocorresse um erro em cada uma dessas palavras, de modo que as palavras recebidas fossem *"belefone", "wola"* e *"canela"*, o código C detectaria o erro somente nas duas primeiras palavras, pois as mesmas não pertencem a nossa língua. Porém, somente seria possível a correção da primeira palavra, pois facilmente vemos que, na nossa língua, a palavra que mais se aproxima de *"belefone"* é "*telefone*", todavia, a palavra *"wola"* não poderia ser corrigida, pois existem várias palavras que igualmente se aproximam dela: *bola, cola, mola, sola* e *gola*; o que tornaria a correção impossível no código C.

[1] Doença pulmonar causada pela inalação de cinzas de origem vulcânica.

Exemplo 1: Suponhamos um braço mecânico de base fixa, dotado dos seguintes movimentos básicos: *para cima*, *para baixo*, *para a direita* e *para a esquerda*, aos quais denominamos *"fonte"*.

Os circuitos digitais (ou circuitos lógicos) baseiam seu funcionamento na lógica binária, portanto, cada informação é expressa utilizando-se dos dígitos 0 e 1. Como temos dois dígitos disponíveis para expressar os quatro comandos para o braço mecânico, considerando o corpo galoisiano $F = \{0,1\}$, podemos codificar esses comandos como elementos de $F^2 = \{(0,0),(0,1),\}(1,0),(1,1)\}$. Por simplicidade de notação, consideraremos cada par $(a,b) \in F^2$ simplesmente como ab, e, a cada um dos quatro comandos 00, 01, 10 e 11, denominaremos *"código da fonte"*.

Fonte	Código da fonte
Para a esquerda	00
Para a direita	01

Fonte	Código da fonte
Para cima	10
Para baixo	11

Imaginemos agora que o comando *"para a esquerda"*, convertido para o código de fonte 00, seja transmitido ao braço mecânico e que durante a transmissão ocorra exatamente um erro, de modo que e o comando recebido pelo braço mecânico seja 10, acarretando com isso a movimentação equivocada para cima. Observemos que o circuito digital do braço mecânico seria incapaz de detectar o erro, pois 10 é um comando existente em seu banco de dados.

Diante de uma situação como a acima descrita, o que fazemos é inserir redundâncias através do acréscimo de dígitos nos códigos da fonte, de modo que se possa detectar e corrigir possíveis erros de transmissão, dando origem a um novo código, ao qual denominamos *"código de canal"*:

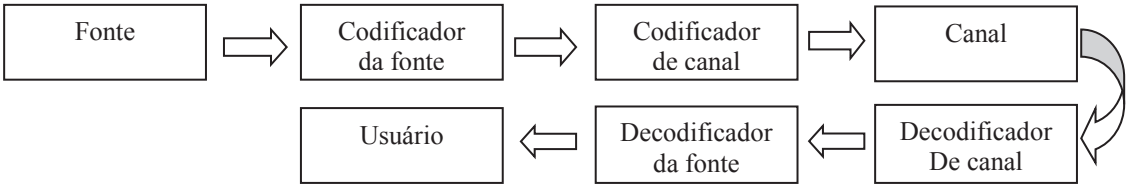
Fonte	Código da fonte	Código de canal
Para a esquerda	00	00000
Para a direita	01	01011
Para cima	10	10110
Para baixo	11	11101

Nesta nova codificação, as duas primeiras posições representam o código da fonte, enquanto as três últimas posições são as redundâncias inseridas.

Reanalisemos o exemplo anterior:

O comando dado *"para a esquerda"* é dado ao braço mecânico, convertido para o código da fonte 00 e daí para o código de canal 00000 e enviado ao braço mecânico. Suponhamos ainda que na transmissão ocorra exatamente um erro de modo que o comando chegue até o braço mecânico como 10000. Notemos que esse comando não existe em banco de dados, o que acarretaria a identificação de um erro pelo circuito digital do braço mecânico. O comando que mais se aproxima de 10000 é 00000 e, portanto, o circuito digital faria a correção, interpretando o comando recebido como 00000 e movendo o braço mecânico, corretamente, para a esquerda.

No diagrama de blocos a seguir são apresentadas todas as etapas, desde o comando dado até a chegada da mensagem transmitida:



O estudo da teoria dos códigos, apresentado nesse trabalho, objetivará a transformação de códigos da fonte em códigos de canal, as detecções e correções de possíveis erros ocorridos durante o processo de transmissão e a decodificação de códigos de canal em códigos da fonte. Consideraremos, nesse estudo, apenas canais simétricos, onde todos os caracteres transmitidos têm a mesma probabilidade (ínfima) de serem recebidos errados. Se um caractere é recebido errado, a probabilidade de ele ser qualquer um dos outros caracteres disponíveis é a mesma.

2. Apresentação de resultados

Definição 1: Denominamos de *alfabeto* um conjunto A finito, cujo o número de elementos representaremos por $|A| = q$. Denominamos de *código* a todo subconjunto próprio de A^n com $n \in \mathbb{N}$. Sendo $u, v \in A^n$, denominamos de *"distância de Hamming"* ao valor $d(u,v) = |\{i, u_i \neq v_i, 1 \leq i \leq n\}|$.

Exemplo 2: Sendo $A = \{0,1\}$, para $n = 4$, temos $|A^4| = 16$ e $\{0000, 0001, 1010, 1011, 1111\} \subset A^4$. Assim: $d(1010, 1011) = 1$, $d(0001, 1011) = 2$, $d(0001, 1111) = 3$ e $d(0000, 1111) = 4$.

Consideremos, de maneira geral, os elementos $u, v, w \in A^n$, tais que $u = u_1u_2u_3 \dots u_n$, $v = v_1v_2v_3 \dots v_n$ e $w = w_1w_2w_3 \dots w_n$. Como $u_i, v_iw_i \in \{0,1\}$ para todo $i \in \{1, 2, \dots, n\}$, se $u_i = v_i$, então $d(u, v) = 0$, caso existam k índices i para os quais $u_i \neq v_i$ então, $d(u, v) = k > 0$, analogamente, $d(v, u) = k > 0$, logo temos sempre $d(u, v) \geq 0$ e $d(u, v) = d(v, u)$.

Para cada índice i, a contribuição da $i - ésima$ coordenada para as distâncias $d(u, v)$, $d(v, w)$ e $d(u, w)$, é 0 ou 1, respectivamente, se $u_i = v_i$ ou $u_i \neq v_i$, $v_i = w_i$ ou $v_i \neq w_i$ e $u_i = w_i$ ou $u_i \neq w_i$. Considerando que a contribuição para a distância $d(u, w)$, da $i - ésima$ coordenada de u e w seja 0, ou seja, $u_i = w_i$, então temos $d(u, w) \leq d(u, v) + d(v, w)$, pois a contribuição da $i - ésima$ coordenada de u_i e v_i e v_i e w_i em $d(u, v) + d(v, w)$ é igual a 0, 1 ou 2. Caso consideremos $u_i \neq w_i$, então não se tem $u_i = v_i$ e $v_i = w_i$, pois seria contrário a hipótese. Assim, temos que a contribuição da $i - ésima$ coordenada de u_i e v_i e v_i e w_i em $d(u, v) + d(v, w)$ é maior ou igual a 1, que, por hipótese, é a contribuição da $i - ésima$ coordenada de u_i e w_i em $d(u, w)$. Portanto, temos sempre $d(u, w) \leq d(u, v) + d(v, w)$. Assim, a distância de Hamming entre os elementos de A^n é uma métrica que denominamos de *métrica de Hamming*.

Definição 2: Consideremos um elemento $c \in A^n$ e $r \in \mathbb{R}$, tal que $r \geq 0$. Dizemos que o conjunto $D(c, r) = \{u \in A^n; d(u, c) \leq r\}$ é um *disco* de centro c e raio r. De maneira análoga, definimos uma *esfera* de centro c e raio r como o conjunto $S(c, r) = \{u \in A^n; d(u, c) = r\}$.

Discos e esferas são conjuntos finitos como veremos a seguir:

Sendo $|A| = q$ e $u \in A^n$ uma palavra desse alfabeto, temos $q - 1$ maneira de preencher uma coordenada de u de modo a se obter um vetor v tal que $v \neq u$. Considerando que exatamente i elementos do vetor v sejam diferentes do vetor u, temos $(q - 1)^i$ possibilidades para essas coordenadas. Como u tem tamanho n e as i entradas distintas, podem percorrer qualquer coordenada de u, temos $\binom{n}{i}$

combinações para v de modo que $d(u,v) = i$. Portanto, o número de elementos da esfera S de centro c e raio i é dado por $|S(c,i)| = \binom{n}{i}.(q-1)^i$. Notemos ainda que $S(c,i) \cap S(c,j) = \emptyset$ quando $i \neq j$ e que $\bigcup_{i=0}^{r} S(c,i) = D(c,r)$, portanto, o número de elementos do disco D é dado por $|D(c,r)| = |\bigcup_{i=0}^{r} S(c,i)| = \sum_{i=0}^{r}|S(c,i)| = \sum_{i=0}^{r}\binom{n}{i}.(q-1)^i$, mostrando com isso que $S(c,r)$ e $D(c,r)$ são conjuntos finitos.

Definição 3: Dado um código C, definimos sua *distância mínima* como sendo um número d, tal que $d = min\{d(u,v); u,v \in C \; e \; u \neq v\}$.

No exemplo do braço mecânico, o código $C \subset F^5$ é tal que $C = \{u_1,u_2,u_3,u_4\} = \{00000, 01011, 10110, 11101\}$. Notemos que $d(u_1,u_2) = d(u_1,u_3) = d(u_2,u_4) = d(u_3,u_4) = 3$ e $d(u_1,u_4) = d(u_2,u_3) = 4$, portanto, $d = min\{3,4\} = 3$.

De maneira geral, para a determinação de d são necessários os cálculos de $\binom{|C|}{2}$ distâncias, onde $|C|$ representa o número de elementos do conjunto C, demandando um custo computacional exagerado, inviabilizando o método.

Considerando C um código de distância mínima d, definimos $\kappa = \left[\frac{d-1}{2}\right]$, onde $\left[\frac{d-1}{2}\right]$ representa a parte inteira do número real $\frac{d-1}{2}$.

Teorema 1: Consideremos C um código de distância mínima d. Então:

i) se $c,c' \in C$ e $c \neq c'$, vale que $D(c,\kappa) \cap D(c',\kappa) = \emptyset$.

ii) C pode detectar até $d-1$ erros.

iii) o código C pode corrigir até $\kappa = \left[\frac{d-1}{2}\right]$ erros.

Demonstração: i) Suponhamos que $D(c,\kappa) \cap D(c',\kappa) \neq \emptyset$, ou seja, existe $u \in D(c,\kappa) \cap D(c',\kappa)$, temos então que $d(u,c) \leq \kappa$ e $d(u,c') \leq \kappa$, mas pela métrica de Hamming, $d(u,c) = d(c,u)$ e $d(c,c') \leq d(c,u) + d(u,c')$, o que implica que $d(c,c') \leq \kappa + \kappa = 2\kappa \leq d-1$, contradizendo a hipótese, pois d é a distância mínima. Portanto se $c,c' \in C$ e $c \neq c'$, então $D(c,\kappa) \cap D(c',\kappa) = \emptyset$.

ii) Sendo d a distância mínima de um código C, sabemos que dada uma palavra $c \in C$, qualquer outra palavra c' do código C está a uma distância no mínimo igual a d da palavra c. Isso significa que podemos introduzir em uma palavra qualquer de C

até $d-1$ erros sem encontrar outra palavra de C, tornando possível a detecção do erro.

iii) Suponhamos que uma palavra $c \in C$ sofra t erros, com $t \leq \kappa$, de modo que r seja a palavra recebida. Temos então $d(r,c) = t \leq \kappa$ e, pelo teorema 1, a distância de r a qualquer outra palavra de C é maior do que κ, assim, a palavra c é univocamente determinada a partir da palavra r.

Considerando um alfabeto A e um número natural n, o conjunto A^n de todas as palavras de tamanho n é um espaço métrico, pois nele temos definida a métrica de Hamming.

Definição 4: Uma função $f: A^n \to A^n$ é uma *isometria* de A^n se, e somente se, f preservar distâncias de Hamming, ou seja, $d\big(f(x), f(y)\big) = d(x,y)$ para todo $x, y \in A^n$.

Vale o seguinte:

Teorema 2: Seja $f: A^n \to A^n$ uma isometria de A^n. Então:

a) f é uma bijeção.

b) f^{-1} é uma isometria de A^n.

c) se g é uma isometria de A^n, $f \circ g$ é uma isometria de A^n.

Demonstração: a) Se $f: A^n \to A^n$ é uma isometria de A^n, então, dados $x, y \in A^n$, tais que $f(x) = f(y)$, temos que $d\big(f(x), f(y)\big) = 0$. Mas, por hipótese, $f: A^n \to A^n$ é uma isometria, então $d(x,y) = d\big(f(x), f(y)\big)$, o que implica que $d(x,y) = 0$. Logo, $x = y$ e f é injetiva. Como A^n é um conjunto finito, segue que f também é uma sobrejeção, e assim, f é uma bijeção.

b) Sabemos que existe f^{-1} em decorrência do item a). Agora, $d\big(f^{-1}(x), f^{-1}(y)\big) = d\big(f\big(f^{-1}(x)\big), f\big(f^{-1}(y)\big)\big) = d(x,y)$. Portanto, f^{-1} é uma isometria de A^n.

c) Se f e g são isometrias de A^n, então $d\Big(f\big(g(x)\big), f\big(g(y)\big)\Big) = d\big(g(x), g(y)\big) = d(x,y)$, logo, $f \circ g$ é uma isometria de A^n.

Nesse sentido, a função identidade $I_{A^n}: A^n \to A^n$ é tal que, para todo $x, y \in A^n$, vale que $I_{A^n}(x) = x$ e $I_{A^n}(y) = y$. Isso mostra que $d\big(I_{A^n}(x), I_{A^n}(y)\big) = d(x, y)$ e que I_{A^n} é uma isometria de A^n.

Definição 5: Dados dois códigos C_1 e C_2 contidos em A^n, dizemos que C_1 e C_2 são *códigos equivalentes* quando existe uma isometria f de A^n tal que $f(C_1) = C_2$.

Os parâmetros fundamentais de um código $C \subset A^n$ são o seu comprimento n, o seu número de elementos $|C| = M$ e a sua distância mínima d. Representamos os *parâmetros de um código* $C \subset A^n$ pela terna $[n, M, d]$.

Teorema 3: Códigos equivalentes possuem os mesmos parâmetros.
Demonstração: Suponhamos que $[n, M, d]$ são os parâmetros de um dado código C_1 de A^n. Sendo C_2 um código de A^n, todas as suas palavras têm comprimento n. Se C_1 e C_2 são equivalentes, existe uma isometria f de A^n tal que $f(C_1) = C_2$ e, pelo item a) do teorema 2, f é bijetiva, logo $|C_2| = |C_1| = M$. Por fim, sejam $x, y \in C_1$ tais que $d(x, y) = d$, temos então, $d(x, y) = d\big(f(x), f(y)\big) = d$, mostrando que a distância mínima em C_2 também é d. Assim, os parâmetros do código C_2 são $[n, M, d]$.

3. Códigos Lineares

Consideremos um corpo finito K com q de elementos, ao qual denominaremos alfabeto e $1 \leq n \in \mathbb{N}$. É fácil verificar que K^n é um k-espaço vetorial de dimensão n.

Definição 6: Um código $C \subset K^n$ é classificado como um código linear quando C for um subespaço vetorial de K^n.

No exemplo do braço mecânico, apresentado anteriormente, temos que $C \subset F^5$ é um subespaço vetorial do espaço F^5 (verifique) e, portanto, um código linear.

Como um código linear é um subespaço de um K-espaço vetorial de dimensão finita, então todo código linear é, também, um K-espaço vetorial de dimensão finita. Sendo k o número de elementos de uma das bases de C (dimensão de C) e, sendo $u_1, u_2, u_3, \dots, u_k$ uma dessas bases, então qualquer que seja $u \in C$, temos, de maneira única, $u = \alpha_1 \cdot u_1 + \alpha_2 \cdot u_2 + \alpha_3 \cdot u_3 + \cdots + \alpha_k \cdot u_k, \forall \alpha_i \in K$ e,

portanto, o número de elementos do código C é $M = |C| = q^k$ ou seja, $\dim C = k = \log_q q^k = \log_q M$.

Definição 7: Considerando d a métrica de Hamming, definimos o *peso* de um vetor u do K-espaço vetorial K^n como sendo o número inteiro $\omega(u) = d(u, 0)$, e o *peso de um código* C, como sendo a distância de Hamming mínima não nula dos vetores de C ao vetor nulo. Em outras palavras: $\omega(C) = min\{\omega(u); u \in C \backslash \{0\}\}$.

Teorema 4: Considerando um código linear $C \subset K^n$, com distância mínima d, temos $\forall\, u, v \in K^n$, $d(u, v) = \omega(u - v)$ e $d = \omega(C)$.

Demonstração: Dados $u, v \in K^n$, pela definição de distância, temos $d(u, v) = d(u - v, 0) = \omega(u - v)$ e, se $u, v \in C$ e $u \neq v$, e a distância mínima do código C é $d = d(u, v)$, então existe $w \in C \backslash \{0\}$ tal que $w = u - v$ e $d = d(u, v) = \omega(u - v) = \omega(w) = \omega(C)$.

Definição 8: Consideremos um corpo finito K com q elementos e um código linear $C \subset K^n$. À terna (n, k, d) *denominamos parâmetros do código linear* C, onde n representa o número de coordenadas de cada vetor (palavra) do código C, k é a dimensão de C sobre o corpo K e d é a distância mínima, equivalente ao peso $\omega(C)$ do código C. Sendo $B = \{u_1, u_2, u_3, \dots, u_k\}$ uma base ordenada de C, onde cada vetor $u_i = (v_{i1}, v_{i2}, v_{i3}, \dots, v_{in})$, com $1 \leq i \leq k$, uma matriz $G = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{bmatrix}$ é denominada *matriz geradora de* C *associada à base* B e não é a única matriz geradora de C, pois, para cada base diferente de C, obtemos uma matriz geradora diferente. Notemos que uma matriz geradora de um código C pode ser obtida de outra matriz geradora, através de transformações elementares sobre as linhas.

Consideremos agora uma transformação linear $T: K^k \to K^n$ de modo que dado $x \in K^k$, tenhamos $T(x) = x \cdot G$. Como $x \in K^k$, então x possui k coordenadas $x_1, x_2, x_3, \dots, x_k$ e, portanto, $T(x) = x_1 \cdot v_1 + x_2 \cdot v_2 + x_3 \cdot v_3 + \cdots + x_k \cdot v_k$, o que implica que $T(K^k) = C$, assim, temos K^k o código da fonte, C é o código de canal e T é a codificação, que leva o código da fonte ao código de canal.

Para obter uma matriz geradora de um código de dimensão k, contido em um espaço K^n, basta tomar uma matriz com k linhas, linearmente independentes e n colunas.

Exemplo 3: Considerando o corpo galoisiano $F = \{0,1\}$, uma matriz $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$ é geradora de um código $C \subset F^5$, cujo código de fonte é composto por vetores de F^3, pois G possui três linhas linearmente independentes.

Notemos, nesse exemplo, que $q = 2$, pois adotamos o corpo finito (galoisiano) $F = \{0,1\}$ e $\mathrm{k} = \dim C = 3$, logo, o número de elementos de C é $M = 2^3 = 8$. O código C é, portanto, o seguinte conjunto:

$$C = \{00000, 10101, 11010, 11111, 01111, 01010, 00101, 10000\},$$

que facilmente pode ser verificado que foi obtido através dos vetores linhas 10010, 11001 e 01110, que constituem uma base de C.

Efetuando operações elementares sobre as linhas da matriz G, obtemos uma matriz G' na forma $[I_k|A]$:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} \xrightarrow{L_2 \rightarrow L_1 + L_2} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} \xrightarrow{L_3 \rightarrow L_2 + L_3} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} = G'.$$

A matriz G' é equivalente por linhas à matriz G, o que implica que suas linhas são LI e em consequência disso formam outra base de C. Dizemos que $G' = [I_k|A]$, com I_k sendo a matriz identidade de ordem k e A uma matriz cuja ordem é $k \times (n-k)$, apresenta-se na forma padrão. A vantagem da utilização da matriz G' é que visualizamos o código de fonte nas k primeiras coordenadas do código de canal, sendo as $n-k$ coordenadas restantes, a redundância acrescida. Cabe salientar que dada uma matriz G de um código C, nem sempre é possível obter para este código outra matriz que se apresente na forma padrão, apenas realizando operações elementares sobre suas linhas. Basta imaginar G uma matriz em que pelo menos uma das suas k primeiras colunas seja nula, porém, aplicando as operações de permutação entre duas colunas da matriz G e multiplicação de uma coluna de G por um escalar não nulo, podemos obter uma matriz G', geradora, na forma padrão, de um código $C' \subset F^5$, que é equivalente ao código C.

Exemplo 4: $G = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{matrix} \overrightarrow{c_1 \to c_4} \\ \overrightarrow{c_2 \to c_3} \end{matrix} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} = G'$.

Teorema 5: Sendo C um código, existe um código C', equivalente a C, cuja matriz geradora se apresenta na forma padrão.

Demonstração: Seja C um código cuja matriz geradora é $G = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{k1} & x_{k2} & \cdots & x_{kn} \end{bmatrix}$.

Utilizando as operações elementares sobre as linhas e operações sobre as colunas de G, temos: as linhas de G constituem uma base de C, então são linearmente independentes e, portanto, nenhuma delas é nula. Consideremos, sem perda de generalidade, que $x_{11} \neq 0$. Como x_{11} é elemento de um corpo, possui um inverso multiplicativo x_{11}^{-1} tal que $\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{k1} & x_{k2} & \cdots & x_{kn} \end{bmatrix} \xrightarrow{L_1 \to x_{11}^{-1} \cdot L_1} \begin{bmatrix} 1 & y_{12} & \cdots & y_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{k1} & x_{k2} & \cdots & x_{kn} \end{bmatrix}$.

Substituindo cada linha dessa matriz, a partir da segunda, pela soma da respectiva linha, com a primeira multiplicada por $-x_{21}$, ..., $-x_{k1}$, respectivamente, temos a seguinte matriz: $\begin{bmatrix} 1 & y_{12} & \cdots & y_{1n} \\ 0 & y_{22} & \cdots & y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & y_{k2} & \cdots & y_{kn} \end{bmatrix}$. A segunda linha dessa matriz possui algum elemento não nulo e, por meio de uma permutação entre colunas, é possível fazer com que esse elemento não nulo ocupe a posição segunda linha e segunda coluna. Multiplicando a segunda linha pelo inverso desse elemento não nulo e somando cada uma das linhas restantes, pela segunda linha multiplicada, respectivamente por $-y_{12}, -y_{13}$, ..., $-y_{k2}$, temos a matriz $\begin{bmatrix} 1 & 0 & \cdots & z_{1n} \\ 0 & 1 & \cdots & z_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & z_{kn} \end{bmatrix}$. Repetindo o processo descrito acima, uma quantidade de até k vezes, obtemos uma matriz $G' = [I_k|A]$, na forma padrão.

Definição 9: O conjunto $C^{\perp}$, que é o complemento ortogonal de C, é um código linear de K^n e será denominado *código dual* de C.

Notemos que $C^{\perp}$ é um código linear, uma vez que é um subespaço vetorial de K^n, pois dados $u, v \in C^{\perp}$, $\alpha, \beta \in K$ e $w \in C$, temos $\langle \alpha \cdot u + \beta \cdot v, w \rangle = \alpha \cdot \langle u, w \rangle + \beta \cdot \langle v, w \rangle = 0$. Além disso, se G é matriz geradora do código C e $w \in C^{\perp}$, então $G \cdot w^t = 0$, o que é facilmente verificável, uma vez que cada linha $v_1, v_2, v_3, \dots, v_k$ de G é um vetor de uma das bases de C e, portanto, $\langle v_1, w^t \rangle = \langle v_2, w^t \rangle = \langle v_3, w^t \rangle = \cdots = \langle v_k, w^t \rangle = 0$.

Teorema 6: Considerando C um código linear contido em K^n, com dimensão k, cuja matriz geradora na forma padrão é $G = [I_k|A]$, temos $\dim C^{\perp} = n - k$.

Demonstração: Vimos anteriormente que $w = w_1, w_2, w_3, \dots, w_n$ pertence a $C^{\perp}$, quando $G \cdot w^t = 0$. Como $G = [I_k|A]$ se apresenta na forma padrão, então, temos:

$$G \cdot w^t = \begin{bmatrix} 1 & 0 & \cdots & 0 & g_{(k+1)1} & g_{(k+2)1} & \cdots & g_{n1} \\ 0 & 1 & \cdots & 0 & g_{(k+1)2} & g_{(k+2)1} & \cdots & g_{n2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & g_{(k+1)k} & g_{(k+2)k} & \cdots & g_{nk} \end{bmatrix} \cdot \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \Leftrightarrow$$

$$\Leftrightarrow \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_k \end{bmatrix} = - \begin{bmatrix} g_{(k+1)1} & g_{(k+2)1} & \cdots & g_{n1} \\ g_{(k+1)2} & g_{(k+2)2} & \cdots & g_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ g_{(k+1)k} & g_{(k+2)k} & \cdots & g_{nk} \end{bmatrix} \cdot \begin{bmatrix} w_{k+1} \\ w_{k+2} \\ \vdots \\ w_n \end{bmatrix}$$

Os $n - k$ elementos $w_{k+1}, w_{k+2}, \dots, w_n$ podem ser escolhidos de forma aleatória. Logo, temos que $\dim C^{\perp} = n - k$.

Teorema 7: Considerando C um código linear contido em K^n, com dimensão k, cuja matriz geradora na forma padrão é $G = [I_k|A]$, temos que $H = [-A^t|I_{n-k}]$ é uma matriz geradora de $C^{\perp}$.

Demonstração: Considerando $i \in \{1, 2, \dots, k\}$, temos cada coordenada w_i de um vetor $w \in C^{\perp}$ escrita como $w_i = -g_{(k+1)i} \cdot w_{k+1} - g_{(k+2)i} \cdot w_{k+2} - \cdots - g_{ni} \cdot w_n$. Assim, $w = (-g_{(k+1)1} \cdot w_{k+1} - g_{(k+2)1} \cdot w_{k+2} - \cdots - g_{n1} \cdot w_n, -g_{(k+1)2} \cdot w_{k+1} - g_{(k+2)2} \cdot w_{k+2} - \cdots - g_{n2} \cdot w_n, \dots, -g_{(k+1)k} \cdot w_{k+1} - g_{(k+2)k} \cdot w_{k+2} - \cdots - g_{nk} \cdot w_n, w_{k+1}, w_{k+2}, \dots, w_n)$. Logo,

$\left\{ \begin{matrix} (-g_{(k+1)1}, \dots, -g_{(k+1)k}, 1, 0, \dots, 0), (-g_{(k+2)1}, \dots, -g_{(k+2)k}, 0, 1, \dots, 0), \dots \\ \dots, (-g_{(k+1)3}, \dots, -g_{(k+1)3}, 0, 0, 1, \dots, 0), (-g_{n1}, \dots, -g_{nk}, 0, 0, 0, \dots, 1) \end{matrix} \right\}$ é uma base de $C^{\perp}$, portanto $H = \begin{bmatrix} -g_{(k+1)1} & -g_{(k+1)2} & \cdots & -g_{(k+1)k} & 1 & 0 & \cdots & 0 \\ -g_{(k+2)1} & -g_{(k+2)2} & \cdots & -g_{(k+2)k} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -g_{n1} & -g_{n2} & \cdots & -g_{nk} & 0 & 0 & \cdots & 1 \end{bmatrix}$ é uma matriz geradora de $C^{\perp}$ na forma $H = [-A^t|I_{n-k}]$.

Teorema 8: Considerando C um código linear de dimensão k, contido em K^n, cuja matriz geradora seja G; uma matriz H, de ordem $(n-k) \times n$, com elementos pertencentes a K, cujas linhas sejam linearmente independentes, é geradora do código $C^{\perp}$, se, e somente se, $G \cdot H^t = 0$.

Demonstração: Como as linhas de H são linearmente independentes, então formam uma base de um subespaço vetorial de K^n, cuja dimensão é $n-k$, mas $\dim C^{\perp} = n-k$. O produto $G \cdot H^t$ consiste no produto interno dos vetores linhas de G pelos vetores colunas de H^t, mas os vetores colunas de H^t são os vetores linhas de H e, caso se tenha $G \cdot H^t = 0$, então os vetores linhas de G e os vetores linhas de H são, entre si, ortogonais, logo, todos os vetores do subespaço gerado por H estão em $C^{\perp}$ e, portanto, H é matriz geradora de $C^{\perp}$.

Teorema 9: Seja C um código linear contido em um espaço K^n, temos $(C^{\perp})^{\perp} = C$.

Demonstração: Consideremos as matrizes G e H geradoras dos códigos C e $C^{\perp}$, respectivamente. Pelo teorema 8, $G \cdot H^t = 0$. Mas se $G \cdot H^t = 0$, então $(G \cdot H^t)^t = 0$ e, pelas propriedades das matrizes, temos que $(G \cdot H^t)^t = (H^t)^t \cdot G^t = 0$ e $(H^t)^t = H$, logo $(H^t)^t \cdot G^t = H \cdot G^t = 0$, o que implica que G é matriz geradora de $(C^{\perp})^{\perp}$, mas, por hipótese, G é matriz geradora de C, portanto, $(C^{\perp})^{\perp} = C$.

Teorema 10: Considerando C um código linear e H a matriz geradora do código $C^{\perp}$, um vetor v pertence ao código C se, e somente se, $H \cdot v^t = 0$.

Demonstração: Pelo teorema 9, temos que $(C^{\perp})^{\perp} = C$, portanto, $v \in C$ se, e somente se, $v \in (C^{\perp})^{\perp}$. Vimos anteriormente que o produto de uma matriz geradora de um código pela matriz transposta, cuja coluna é vetor pertencente ao complemento ortogonal desse código, é igual ao vetor nulo, sendo assim, $v \in (C^{\perp})^{\perp}$ se, e somente se, $H \cdot v^t = 0$.

O teorema 10 constitui uma ferramenta eficiente pra determinar se um dado vetor $v \in K^n$ pertence a um dado código linear $C \subset K^n$, bastando para isso, verificar se $H \cdot v^t = 0$. A matriz H, geradora de $C^{\perp}$, é denominada de *matriz teste de paridade* do código C e o vetor $H \cdot v^t$, com $v \in K^n$, é denominado de *síndrome* do vetor v.

Teorema 11: Consideremos H uma matriz teste de paridade de um código linear C sobre um corpo K. Então, o peso $\omega(C)$ do código C é maior ou igual a p se, e somente se, quaisquer $p-1$ colunas da matriz H são linearmente independentes. Valendo a igualdade se, e somente se, quaisquer $p-1$ colunas de H forem linearmente independentes e existirem p colunas de H linearmente dependentes.

Demonstração: ($\Leftarrow$) Suponhamos que cada $(p-1)-uplas$ de colunas da matriz H sejam linearmente independentes e que $\omega(v) \leq p-1$. Seja $v = v_1 v_2 \dots v_n$ uma palavra não nula de C. Sabemos que $H.v^t = 0$, o que implica que $H.v^t = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ h_{(n-k)1} & h_{(n-k)2} & \cdots & h_{(n-k)n} \end{bmatrix} \cdot \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, gerando o sistema $\begin{cases} h_{11} \cdot v_1 + h_{12} \cdot v_2 + \cdots + h_{1n} \cdot v_n = 0 \\ h_{21} \cdot v_1 + h_{22} \cdot v_2 + \cdots + h_{2n} \cdot v_n = 0 \\ \vdots \\ h_{(n-k)1} \cdot v_1 + h_{(n-k)2} \cdot v_2 + \cdots + h_{(n-k)1n} \cdot v_n = 0 \end{cases}$. Somando as equações e reagrupando, temos:

$(h_{11} + h_{21} + \cdots + h_{(n-k)1}) \cdot v_1 + \cdots + (h_{1n} + h_{2n} + \cdots + h_{(n-k)n}) \cdot v_n = 0$. Como $\omega(v)$ representa o número de coordenadas não nulas de v, teríamos então uma combinação linear nula, com no máximo $p-1$ colunas da matriz H, contradizendo a hipótese inicial de que $\omega(v) \leq p-1$. Assim, $\omega(v) > p-1$, o que implica em $\omega(v) \geq p$ e, portanto, $\omega(C) \geq p$.

($\Rightarrow$) Em contrapartida, se considerarmos $\omega(C) \geq p$ e supormos que existam $p-1$ colunas linearmente dependentes em H, então existem, por exemplo, $v_1 v_2 \dots v_{p-1} \in K$, nem todos nulos, tal que $(h_{11} + h_{21} + \cdots + h_{(n-k)1}) \cdot v_1 + (h_{12} + h_{22} + \cdots + h_{(n-k)2}) \cdot v_2 + \cdots + (h_{1(p-1)} + h_{2(p-1)} + \cdots + h_{(n-k)(p-1)}) \cdot v_{p-1} = 0$, implicando que $v = v_1 v_2 \dots 0 \dots 0 \dots v_{p-1} \dots 0$ pertence ao código C, logo, $\omega(v) \leq p-1 < p$, e, portanto, $\omega(C) < p$, contradizendo a hipótese. Assim, H possui $p-1$ colunas linearmente independentes.

Para demonstrar a igualdade, suponhamos $\omega(C) = p$, temos que todo conjunto de $p-1$ colunas de H é linearmente independente. Se existissem p colunas linearmente independentes em H, então, pelo que foi visto anteriormente, teríamos $\omega(C) \geq p+1$, logo, em H existem p colunas linearmente dependentes. Por outro lado, se, na matriz H existem $p-1$ colunas linearmente independentes e p colunas linearmente dependentes, então, temos $\omega(C) \geq p$. Mas, se $\omega(C) > p$, por

exemplo, $\omega(C) \geq p + 1$, pelo exposto anteriormente, teríamos, em H, que todo conjunto com p colunas seria linearmente independente, contradizendo a hipótese, logo $\omega(C) = p$.

4. Codificação

Exemplo 5: Suponha que desejemos transmitir a mensagem **REVISTA** através de um código linear sobre o corpo galoisiano $F = \{0,1\}$.

Abaixo, mostraremos uma lista de procedimentos necessários até a obtenção do código de canal necessário à transmissão da mensagem:

1) Fonte: (espaço), A, B, C, D, E, F, G, H, I, J, L, M, N, O, P, Q, R, S, T, U, V, X e Z, com 24 caracteres.
2) Código da fonte: notemos que o código da fonte deve possuir no mínimo 24 palavras código, portanto, adotaremos $k = 5$, implicando que o código de fonte está contido em F^5. Utilizemos as seguintes informações:

$espaço = 00000$	$E = 00001$	$J = 01100$	$P = 00011$	$U = 11001$
$A = 10000$	$F = 11000$	$L = 01010$	$Q = 11100$	$V = 01110$
$B = 01000$	$G = 10100$	$M = 01001$	$R = 10110$	$X = 00111$
$C = 00100$	$H = 10010$	$N = 00110$	$S = 10101$	$Z = 11110$
$D = 00010$	$I = 10001$	$O = 00101$	$T = 11010$	

3) Código de canal: por meio do acréscimo de redundâncias, o código de fonte é convertido em código de canal. Suponhamos que desejemos um canal onde cada palavra código tenha comprimento $n = 9$. Temos então que o código C é um subespaço vetorial do espaço F^9. Ou seja, C é obtido através de uma transformação linear $T: F^5 \to F^9$ e, pelo que foi visto, $\dim C = k = 5$. Tomemos quaisquer cinco vetores linearmente independentes de F^9 para obtermos uma base de C e, consequentemente, uma matriz G geradora do código C:

$\{(100010001), (100100010), (001001001), (000010110), (010101010)\}$ é uma base de C, pois os cinco vetores desse conjunto são LI, logo, $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$ é uma matriz geradora do código C, cuja matriz

equivalente por linhas, na forma padrão é $G' = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$.

Assim, temos:

Fonte	Código da fonte	Código do canal (Código da Fonte).G'
Espaço	00000	000000000
A	10000	100000111
B	01000	010001111
C	00100	001001001
D	00010	000100101
E	00001	000010110
F	11000	110001000
G	10100	101001110
H	10010	100100010
I	10001	100010001
J	01100	011000110
L	01010	010101010

Fonte	Código da fonte	Código do canal (Código da Fonte).G'
M	01001	010011001
N	00110	001101100
O	00101	001011111
P	00011	000110011
Q	11100	111000001
R	10110	101101011
S	10101	101011000
T	11010	110101101
U	11001	110011110
V	01110	011100011
X	00111	001111010
Z	11110	111100100

Portanto, as palavras do código a serem transmitidas, na ordem em que aparecem, são: 101101011, 000010110, 011100011, 100010001, 101011000, 110101101 e 100000111.

5. Decodificação

Ao ser recebida uma palavra código, através do canal de comunicação, o decodificador de canal se incumbe da detecção e correção da palavra recebida se, por acaso, por alguma interferência, tenha sofrido algum erro, para depois enviá-la ao decodificador de fonte, e por fim, chegar ao usuário.

Consideremos o vetor c como sendo uma palavra transmitida e o vetor r a palavra recebida. Definimos o vetor erro e como a diferença entre a palavra recebida e a palavra transmitida: $e = r - c$. Quando $e = 0$, significa que a palavra recebida é igual à palavra transmitida e, nesse caso, não houve erro na transmissão. Caso $e \neq 0$, entendemos que houve erro na transmissão. Notemos, ainda, que o peso do vetor e define o número de erros ocorridos na transmissão, ou seja, $\omega(e) = p$, implica em p erros na palavra recebida.

Considerando H a matriz teste de paridade de um código C, considerando c um vetor (palavra) de C, sabemos que a síndrome de c é nula, ou seja, $H \cdot c^t = 0$. Portanto, a síndrome do vetor erro e é dada por:

$$H \cdot e^t = H \cdot (r - c)^t = H.(r^t - c^t) = H \cdot r^t - H \cdot c^t = H \cdot r^t - 0 = H \cdot r^t.$$

Assim, a síndrome do erro é igual à síndrome da palavra recebida. De outra forma, considerando $e = (\alpha_1, \alpha_2, \dots, \alpha_n)$, temos:

$$H \cdot r^t = H.e^t = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ h_{(n-k)1} & h_{(n-k)2} & \cdots & h_{(n-k)n} \end{bmatrix} \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \alpha_1 \cdot h^1 + \alpha_2 \cdot h^2 + \cdots + \alpha_n \cdot h^n =$$

$$= \sum_{i=1}^{n} \alpha_i \cdot h^i$$, onde h^i representa a i $-$ ésima coluna da matriz H.

Teorema 12: Considerando C um código linear contido em K^n, capaz de corrigir até κ erros. Se uma palavra recebida r pertence ao espaço K^n e a palavra transmitida c pertence ao código C são tais que $d(c, r) \leq \kappa$, então existe um único vetor e, tal que $\omega(e) \leq \kappa$, cuja síndrome é igual à síndrome de r, ou seja, $H \cdot e^t = H \cdot r^t$, tal que $c = r - e$.

Demonstração: Para provar a existência, vejamos que, pelo enunciado do teorema, temos $d(c, r) \leq \kappa$ e, por tratar-se de uma métrica, sabemos que $d(c, r) = d(r, c)$ e, pelo teorema 9, $d(r, c) = d(r - c) = \omega(r - c)$, logo, $\omega(r - c) \leq \kappa$ implica que $\omega(e) \leq \kappa$, mostrando a existência de e.

Para provar a unicidade, suponhamos que H seja a matriz teste de paridade de um código C em K^n e que existam $e = (\alpha_1, \alpha_2, \dots, \alpha_n)$ e $e' = (\beta_1, \beta_2, \dots, \beta_n)$, tais que $\omega(e) \leq \kappa$, $\omega(e') \leq \kappa$ e $H \cdot e^t = H \cdot e'^t = H \cdot r$, com r sendo uma palavra recebida. Temos então:

$H \cdot e^t = H \cdot e'^t \Rightarrow \alpha_1 \cdot h^1 + \alpha_2 \cdot h^2 + \cdots + \alpha_n \cdot h^n = \beta_1 \cdot h^1 + \beta_2 \cdot h^2 + \cdots + \beta_n \cdot h^n$, onde h^i representa a i $-$ésima coluna de H. Daí, temos:

$(\alpha_1 - \beta_1) \cdot h^1 + (\alpha_2 - \beta_2) \cdot h^2 + \cdots + (\alpha_n - \beta_n) \cdot h^n = 0$ e, pelo teorema 16, quaisquer $d - 1$ colunas de H são linearmente independentes, portanto, temos $\alpha_i = \beta_i \ \forall i$, logo, $e = e'$.

Exemplo 6: Suponhamos o código que, ao ser transmitida uma palavra do código C do exemplo anterior, a palavra recebida seja $r = 010100101$.

O código C está contido em F^9 e o código de canal está contido em F^5, uma matriz geradora de C, na forma padrão, é $G' = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$, o que implica que a matriz teste de paridade é do código C é dada por $H = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$. Calculando a síndrome de r, temos:

$H \cdot r^t = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$. Vemos que $H \cdot r^t = 1 \cdot h^2$. Como $H \cdot e^t = H \cdot r^t$, então $H \cdot e^t = 1 \cdot h^2$, o que implica que $e = (010000000)$ e, por consequência, $c = r - e = (010100101) - (010000000) = (000100101)$, ou seja, a palavra código transmitida corresponde ao caractere D.

Consideremos um código corretor de erros C contido em K^n, com matriz teste de paridade H, com distância mínima d e capacidade de correção $\kappa = \left[\frac{d-1}{2}\right]$. Como vimos, $H \cdot e^t = H \cdot r^t$ e, se $\omega(e) \leq \kappa$, então e é univocamente determinado por r.

Definição 10: Considerando um vetor v do espaço K^n, definimos o conjunto $v + C$, denominado *classe lateral de v segundo C,* como sendo $v + C = \{v + c, c \in C\}$.

Dados dois vetores $u, v \in K^n$, vale que $H \cdot u^t = H \cdot v^t$ se, e somente se, $u \in v + C$. Isso, porque valem as equivalências $H \cdot u^t = H \cdot v^t \Leftrightarrow H \cdot u^t - H \cdot v^t = 0 \Leftrightarrow H \cdot (u^t - v^t) = 0 \Leftrightarrow H \cdot (u - v)^t = 0 \Leftrightarrow u - v \in C \Leftrightarrow u \in v + C$.

É fácil verificar que o conjunto $v + C$ goza das seguintes propriedades:

I) $v + C = v' + c \Leftrightarrow v - v' \in C$;

II) $(v + C) \cap (v' + C) \neq \emptyset \Rightarrow v + C = v' + c$;

III) $\bigcup_{v \in K^n} (v + C) = K^n$;

IV) $|(v + C)| = |C| = q^k$;

v) $v + C = C \iff v \in C$.

Pelas propriedades II, III e IV, deduzimos que o número de classes laterais segundo C é dado por $\left|\bigcup_{v \in K^n} (v + C)\right| / |(v + C)| = {q^n}/{q^k} = q^{n-k}$.

Os argumentos acima garantem uma correspondência biunívoca entre classes laterais e síndromes, de modo que todos os vetores de uma classe lateral possuem síndromes iguais, e vetores de classes laterais diferentes possuem síndromes diferentes.

Seja x um vetor pertencente a uma classe lateral de v segundo C. Se $\omega(x) = min\{\omega(v_i);\ v_i \in v + C\}$, então dizemos que x é o *líder* de $v + C$. Notemos que o líder de uma classe não necessariamente é único.

Teorema 13: Considerando $C \subset K^n$ um código com distância mínima d. Se $v \in K^n$ é um vetor tal que $\omega(v) \leq \left[\frac{d-1}{2}\right] = \kappa$, então v é o único elemento líder em sua classe lateral.

Demonstração: Sejam $v_1, v_2 \in K^n$, tais que $\omega(v_1) \leq \left[\frac{d-1}{2}\right]$ e $\omega(v_2) \leq \left[\frac{d-1}{2}\right]$. Se $v_1 - v_2 \in C$, então $\omega(v_1 - v_2) \leq \omega(v_1) + \omega(v_2) \leq \left[\frac{d-1}{2}\right] + \left[\frac{d-1}{2}\right] \leq d - 1$, portanto, $v_1 - v_2 = 0$, o que implica em $v_1 = v_2$.

O teorema 13 constitui uma ferramenta importante para a determinação dos líderes de classes de peso menor ou igual a $\left[\frac{d-1}{2}\right]$. Para isso, basta tomar os vetores $v_i \in K^n$, para os quais se tenha $\omega(v_i) \leq \left[\frac{d-1}{2}\right]$. Cada um dos v_i é líder de uma e somente uma classe.

Exemplo 7: Vimos que a matriz teste de paridade do código $C \subset F^9$, apresentado anteriormente, é $H = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$. Sabemos que, nesse código, a distância mínima é $d = 3$, pois vemos facilmente que quaisquer duas colunas de H são linearmente independentes, enquanto que três colunas de H são linearmente

dependentes (teorema 11), o que implica em $\omega(C) = 3, \kappa = \left[\frac{d-1}{2}\right] = \left[\frac{3-1}{2}\right] = 1$, ou seja, C tem capacidade de detecção de dois erros e correção de um erro. Os vetores $v_i \in F^9$, tais que $\omega(v_i) \leq 1$ são 000000000, 000000001, 000000010, 000000100, 000001000, 000010000, 000100000, 001000000, 010000000 e 100000000. Os líderes v_i e suas respectivas síndromes $H \cdot v_i^t$ são apresentados na tabela a seguir:

Líder	Síndrome ($H \cdot v_i^t$)
000000000	0000
000000001	0001
000000010	0010
000000100	0100
000001000	1000

Líder	Síndrome ($H \cdot v_i^t$)
000010000	0110
000100000	0101
001000000	1001
010000000	1111
100000000	0111

Suponhamos que, ao utilizar o código C, descrito anteriormente, a seguinte mensagem seja recebida:

010010110	010101010	000010110	010111001	000010110	101101100
111101101	001011111	101011010			

Suponhamos que a desejamos decodificar e que, no máximo, um erro tenha sido introduzido em cada palavra transmitida. Então, das nove palavras código recebidas r_i, calcularemos suas respectivas síndromes $H \cdot r_i^t$ e os erros e_i, comparando com a tabela anterior e determinando as palavras transmitidas c_i, identificando suas respectivas fontes. Isso pode ser descrito na seguinte tabela:

Palavra (r_i)	**Síndrome ($H \cdot r_i^t$)**	**Erro (e_i)**	**Conclusão**	**Palavra (c_i)**	**Fonte**
01001011	1111	010000000	Houve um erro	000010110	E
01010101	0000	000000000	Não houve	010101010	L
00001011	0000	000000000	Não houve	000010110	E
01011100	0101	000100000	Houve um erro	010011001	M
00001011	0000	000000000	Não houve	000010110	E
10110110	0111	100000000	Houve um erro	001101100	N
11110110	1001	001000000	Houve um erro	110101101	T
00101111	0000	000000000	Não houve	001011111	O
10101101	0010	000000010	Houve um erro	101011000	S

Portanto, a mensagem transmitida foi **ELEMENTOS**.

6. Conclusão

O propósito deste trabalho foi abordar uma das aplicações da Álgebra Linear e Álgebra Abstrata, presente no cotidiano de cada um dos usuários dos

recursos atuais de comunicação e armazenamento, embora grande parte deles desconheça a matemática envolvida no funcionamento desses dispositivos.

A teoria dos Códigos Corretores de Erros, iniciada na década de 40, por Richard W. Hamming, no Laboratório Bell de Tecnologia, nos Estados Unidos, é responsável, nos dias atuais, por congregar várias áreas do conhecimento, tais como matemática estatística, engenharias, informática, entre outras. As pesquisas motivadas por essa teoria têm sido responsáveis por grandes avanços nessas ciências. O trabalho restringiu-se aos códigos lineares, enunciando várias definições e teoremas, bem como os processos de codificação e decodificação, com finalidade de divulgar parte dessa teoria, suas aplicações e sua notável importância na atualidade.

7. Referências

BAHIA, Flaviano; *Um primeiro curso sobre códigos corretores de erros*. In: ERMAC 2010: I Encontro Regional de Matemática Aplicada e Computacional, 2010. Disponível em: <http://www.ufsj.edu.br/portal2-repositorio/File/i-ermac/anais/minicursos/mc8.pdf> acesso em 13 de setembro de 2014.

BARBOSA, Tauan de S.; ASSIS, Aline M.; *Princípios teóricos dos códigos corretores de erros: códigos lineares e cíclicos*. Disponível em: <seer.ucg.br/index.php/estudos/article/download/3364/1951> acesso em 21 de outubro de 2014.

CARVALHO, Sézani M. G.; *Matrizes, determinantes e polinômios: aplicações em códigos corretores de erros, como estratégia motivacional para o ensino da matemática*; Dissertação de Mestrado; UNIR; Porto Velho-RO-Brasil (2014).

HEFEZ, Abramo; FERNANDEZ, Cecília S.; *Introdução à álgebra linear.* 1. Ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2012.

HEFEZ, Abramo; VILLELA, Maria Lúcia T.; *Códigos corretores de erros.* 2. Ed. Rio de Janeiro: IMPA; 2008.

HOFFMAN, Kenneth and KUNZE, Ray; *Álgebra linear.* Trad. Renate Watanabe. 2. Ed. Rio de Janeiro: Livros Técnicos e Científicos; Editora S. A., 1979.

MENEGHESSO, Carla; *Códigos corretores de erros*. Disponível em: <http://www.dm.ufscar.br/dm/attachments/article/5/monografia_carla%20TCC.pdf>; acesso em 21 de agosto de 2014.

MILIES, César Polcino; *Breve introdução à teoria dos códigos corretores de erros*. Disponível em: < http://www.sbm.org.br/docs/coloquios/CO-1-09.pdf>; acesso em 07 de outubro de 2014.

SOUZA, Mário José; *Códigos corretores de erros*. Disponível em: <http://semanadoime.mat.ufg.br/up/34/o/min_mario.pdf>; acesso em 02 de outubro de 2014.

VOLOCH, José Felipe; *Códigos corretores de erros*. Disponível em <http://www.impa.br/opencms/pt/biblioteca/cbm/16CBM/16_CBM_87_06.pdf> ; acesso em 28 de agosto de 2014.

Sézani Morais Gonçalves de Carvalho

Rua Buenos Aires, 2370 – Bairro Embratel

Porto Velho – Rondônia – CEP 76820-858

sezani@unir.br

Tel.: (69)84649249

Tomás Daniel Menedéz Rodriguez

Rua Alípio da Silva, 5815 – Cunia

Porto velho – Rondônia – CEP 76824-508

tomas@unir.br

Tel.: (69)999831397

Revista
ELEMENTOS

Nota Histórica

∗ 15 de abril de 1707, em Basileia, na Suíça.
†18 de setembro de1783, em São Petersburgo, na Rússia.

Leonhard Paul Euler

Leonhard Paul Euler nasceu no dia 15 de abril de 1707, em Basileia, na Suíça, filho do pastor Paul Euler e Margaret Brucker, filha de um pastor. Teve duas irmãs mais novas, Anna Maria e Maria Magdalena. Depois do nascimento de Leonhard, sua família mudou da cidade de Basileia para a cidade de Riehen, onde viveu a maior parte de sua infância. Paul Euler era amigo da família Bernoulli; Johann Bernoulli, que era então o matemático mais importante da Europa, foi a influência mais relevante na vida do jovem Leonhard.

Seus primeiros ensinamentos foram dados por seu pai Paul, que lhe ensinou matemática. Em 1720, aos treze anos, Euler ingressou na pequena Universidade de Basileia, que possuía um famoso departamento de estudos de matemática, liderado por Johann Bernoulli, irmão de Jacob Bernoulli. Johann recusou-se a dar aulas particulares a Euler, oferecendo então um valioso conselho de como estudar por conta própria.

Em 1722, recebe o grau de Mestre em Artes e, no seu exame, deu um discurso em latim, comparando as filosofias de Descartes e Newton. Nessa altura, já recebia, aos sábados à tarde, lições de Johann Bernoulli, que rapidamente

descobriu o seu talento para a matemática.

Nessa época Euler estudava teologia, grego e hebraico, pela vontade de seu pai, para mais tarde se tornar pastor. Porém, Johann Bernoulli resolveu intervir e convenceu Paul Euler de que o seu filho estava destinado a ser um grande matemático.

Em 1726, Euler completou a sua dissertação sobre propagação do som, intitulada de *De Sono*. Na época, ele estava tentando, sem sucesso, obter um cargo na Universidade de Basileia. Em 1727, ele entrou pela primeira vez na competição premiada da Academia de Paris; o problema do ano era encontrar a melhor maneira de colocar os mastros num navio. Ganhou o segundo lugar, perdendo para Pierre Bouguer, mais tarde conhecido como "o pai da arquitetura naval". Euler, entretanto, ganharia o prêmio anual doze vezes.

À época, os dois filhos de Johann Bernoulli, Daniel e Nicolaus, foram trabalhar na Academia Russa de Ciências. No dia 10 de julho de 1726, Nicolaus morreu de apendicite, após viver um ano na Rússia, e, quando Daniel assumiu o cargo do seu irmão na divisão de matemática e física da universidade, ele indicou a vaga em fisiologia, que ele tinha desocupado, para ser preenchida por seu amigo Euler. Em novembro de 1726, Euler aceitou ansiosamente a oferta, porém, se atrasou na viagem para São Petersburgo, pois estava tentando, sem sucesso, uma vaga como professor de física na Universidade de Basileia.

Leonhard chegou a São Petersburgo no dia 17 de maio de 1727. Ele foi promovido de, assistente do departamento médico da academia, assumindo uma vaga no departamento de matemática. Ele se apresentou com Daniel Bernoulli, com quem ele frequentemente trabalhava em uma estreita parceria. Euler aprendeu russo e instalou-se em São Petersburgo. Também aceitou um trabalho adicional como médico na Marinha Russa.

Selo da União Soviética em comemoração aos 250 anos do nascimento do grande matemático Leonhard Euler (1957).

A Academia de São Petersburgo, sob a política de Pedro I, da Rússia, tinha intenção de melhorar a educação naquele País e corrigir a defasagem no campo das ciências do país em relação à Europa Ocidental. Como resultado, a instituição criou um programa de internalização, com o objetivo de atrair estudantes estrangeiros, como Euler. A instituição possuía vultosos recursos financeiros e uma biblioteca abrangente, esboçada a partir das bibliotecas privadas da nobreza e do príncipe Pedro. Poucos estudantes foram inscritos na academia, no sentido de diminuir a grade curricular e enfatizar a pesquisa, oferecendo para o corpo docente tempo e liberdade para prosseguir o questionamento científico.

A benfeitora da Academia, Catarina I da Rússia, que tinha dado continuação à política progressiva da gestão anterior, morreu no dia que Euler foi viajar. A aristocracia, em seguida, teve mais poder durante os dois anos de mandato de Pedro II. A nobreza, desconfiada dos cientistas estrangeiros da Academia, cortou os financiamentos e causou dificuldades para Euler e seus colegas.

As condições melhoram um pouco depois da morte de Pedro II e Euler se tornou professor de física, em 1731, pela sua classificação no ranking da escola.

Dois anos mais tarde, Daniel Bernoulli, que foi perseguido com a censura e sofrido com a hostilidade que enfrentou, partiu de São Petersburgo para Basileia, e, assim, Euler o substituiu como professor de Matemática.

No dia 7 de janeiro de 1734, Leonhard Euler casa com Katharina Gsell, filha de Georg Gsell, um pintor da Academia Gymnasium. O jovem casal construiu uma casa perto do rio Neva. Tiveram treze filhos, dos quais apenas cinco sobreviveram à infância.

Preocupado com a contínua turbulência na Rússia, Euler deixou São Petersburgo em 19 de Julho de 1741. Ele viveu por vinte e cinco anos em Berlim, onde ele escreveu 380 artigos e publicou os dois trabalhos que vieram a ser os mais renomados: *A Introduction in analysin infinitorum*, um texto sobre funções matemáticas, publicado em 1748, e o *Institutiones calculi differentialis*, publicado em 1755, sobre cálculo diferencial. No mesmo ano, ele foi eleito membro estrangeiro, pela Academia Real das Ciências da Suécia.

Selo da antiga República Democrática Alemã, homenageando Euler, no 200º aniversário de sua morte.

Entretanto, Euler é convidado para ser tutor de Friederike Charlotte de Brandenburg-Schwedt, a Princesa de Anhalt-Dessau e sobrinha de Frederico II, o Grande. Euler escreveu mais de 200 cartas dirigidas à princesa, que mais tarde foram compiladas num volume *Best-selling*, intitulado *Cartas de Euler sobre diferentes assuntos da Filosofia natural para uma Princesa Alemã*. Esse trabalho incorpora exposições sobre vários assuntos pertencentes à física e matemática, dando também a conhecer as perspectivas religiosas e a própria personalidade do seu autor. Esse livro veio a ser mais lido do que todas as outras obras matemáticas, e foi publicado dentro da Europa e nos Estados Unidos da América. A popularidade das "Cartas" atesta a capacidade de Euler de se comunicar de maneira eficaz sobre assuntos científicos para um público leigo, uma rara habilidade para um cientista dedicado à pesquisa.

Apesar da imensa e impressionante contribuição para a Academia de Berlim, ele provocou a ira de Frederico II, que o forçou a abandonar Berlim. O rei da Prússia tinha um grande círculo social de intelectuais em sua corte, enquanto Euler permaneceu um matemático sem sofisticações e informal, tanto em seu trabalho quanto na vida pessoal. Euler foi simples, religioso devoto, que nunca questionou a existência de ordens ou crenças convencionais. Euler não era um debatedor qualificado e era um opositor direto de Voltaire, que, por ter uma posição privilegiada na corte de Frederick, fazia dele um alvo frequente de sua sagacidade.

A acuidade visual de Euler piorou ao longo de sua carreira matemática. Em 1738, três anos depois de sofrer uma febre quase fatal, em 1735, ficou quase cego do olho direito, mas, ao invés de se lamentar, apresentou um trabalho meticuloso sobre cartografia para a Academia de São Petersburgo. A visão de Euler se agravou durante a sua estada na Alemanha, na medida em que Frederico II, da Prússia, se referia a ele como "Cyclops". Euler, mais tarde, desenvolveu uma catarata no olho esquerdo, que o deixou quase totalmente cego, poucas semanas depois de sua descoberta, em 1766. No entanto, sua condição parecia ter pouco efeito sobre sua

produtividade, compensada por suas habilidades de cálculo mental e de memória fotográfica. Por exemplo, Euler conseguiu repetir a Eneida de Virgílio, do começo ao fim, sem hesitação. Com a ajuda de seus escribas, a produtividade de Euler, em muitas áreas de estudo, na verdade, aumentou. Ele produziu, em média, um artigo matemático em cada uma das semanas do ano de 1775.

Em 1760, com o alastramento da Guerra dos Sete Anos, a fazenda de Euler, em Charlottenburg, foi devastada pelo avanço das tropas russas. Com isso, o general Ivan Petrovich Saltykov foi obrigado a indenizar Euler pelos danos causados na sua propriedade, depois da tsarina Isabel da Rússia adicionar um pagamento de 4000 rublos, um valor exorbitante, à época. A situação política russa se estabilizaria após a ascensão de Catarina, a Grande, ao trono, quando, em 1766, Euler aceita um convite para voltar à Academia de São Petersburgo. Suas condições foram bastante exorbitantes – um salário anual de 3000 rublos, uma pensão para a sua esposa e a promessa de cargos de alto escalão para os seus filhos. Todas essas condições foram atendidas. Ele viveu o resto de sua vida na Rússia. Contudo, sua segunda estadia no país foi marcada por uma tragédia: um incêndio em São Petersburgo, em 1771, destruiu a sua casa, e quase o matou. Em 1773, faleceu a sua esposa Katharina, após 40 anos de casamento.

Três anos depois da morte de sua esposa, Euler casou com sua meia-irmã, Salome Abigail Gsell (1723–1794). Este casamento durou até o fim de sua vida. Em 1782, ele foi eleito como membro honorário estrangeiro da Academia de Artes e Ciências dos Estados Unidos.

Em Santo Petersburgo, no dia 18 de setembro de 1783, depois de um almoço com sua família, Leonhard estava discutindo sobre a descoberta da órbita de um novo planeta da época, chamado Urano, com o também acadêmico Anders Johan Lexell, quando sucumbiu, por causa de uma hemorragia cerebral. Ele morreu algumas horas depois. Em sua lembrança, o filósofo e matemático francês, marquês de Condorcet, escreveu: *il cessa de calculer et de vivre* — ... ele terminou de calcular e de viver.

Euler foi enterrado próximo de Katharina, no cemitério luterano de Smolensk, na Ilha de Vassiliev. Em 1785, a Academia de Ciências da Rússia pôs um busto de mármore de Leonhard Euler em um pedestal próximo à Reitoria e, em 1837, esculpiram uma lápide para Euler que, para comemorar os duzentos e cinquenta anos do seu nascimento, foi transferida, em 1956, junto com seus restos mortais, para a necrópole do século XVIII, no monastério Alexander Nevsky, no cemitério Tikhvin.

A lápide de Euler no monastério de Alexander Nevsky.

Euler trabalhou em quase todas as áreas da matemática: geometria, cálculo infinitesimal, trigonometria, álgebra e teoria dos números. Deu continuidade aos estudos da física newtoniana, da teoria lunar e de outras ramificações da física. Trata-se de uma figura seminal na história da matemática: suas obras, muitas das quais são de interesse fundamental, compõem um acervo de 60 a 80 volumes. O nome de Euler está associado a um grande número de temas, pois é o único

matemático que tem dois números em homenagem a ele. O número *e*, aproximadamente igual a 2, 71828, e a constante de Euler-Mascheroni, γ (gama), por vezes referido apenas como "constante de Euler", aproximadamente igual a 0,57721. Não se sabe se γ é racional ou irracional.

Referências

[1] WILLIAMS, Rob. «Google Doodle celebrates Leonhard Euler – Swiss mathematician considered one of the greatest of all time» [S.l.: s.n.].

[2] FINKEL, B. F.; "Biography-Leonard Euler". *The American Mathematical Monthly* **4** (12): 300.

[3] GINDIKIN, Semen Grigor'evich e GINDIKIN, Simon; *Tales of Mathematicians and Physicists*, Springer, p. 175, ISBN: 978-0-387-48811-0 (2007).

[4] JAMES, Ioan; *Remarkable Mathematicians: from Euler to von Neumann* Cambridge [S.l.] p. 2. ISBN: 0-521-52094-0; (2002).

[5] DERBYSHIRE, John; *Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics* (Washington, D.C.: Joseph Henry Press); p. 422; (2003).

[6] BOYER, Carl B. e MERZBACH, Uta C.; *A History of Mathematics*; John Wiley & Sons [S.l.]; pp. 439–445. ISBN: 0-471-54397-7; (1991).

[7] FEYNMAN, Richard; «Chapter 22: Algebra». *The Feynman Lectures on Physics: Volume I* [S.l.: s.n.] p. 10; (1970).

[8] INGHAM, Albert Edward; *The Distribution of Prime Numbers; Introduction*, p.2 [Google books]; (1932).

[9] ALEXANDERSON, Gerald; «Euler and Königsberg's bridges: a historical view». *Bulletin of the American Mathematical Society* [S.l.: s.n.] **43** (4): 567; doi: 10.1090/S0273-0979-06-01130-X; (2006).

[10] CROMWELL, Peter R.; *Polyhedra*; Cambridge University Press [S.l.] pp. 189–190; ISBN: 978-0-521-66405-9; (1999).

[11] L'HUILLIER, S. A. J.; «Mémoire sur la polyèdrométrie»; *Annales de Mathématiques* [S.l.: s.n.] **3**: 169–189; (1861).

[12] YOUSCHKEVITCH, A. P.; Biography in *Dictionary of Scientific Biography*; New York (1970-1990).

[13] HOME, R. W.; «Leonhard Euler's 'Anti-Newtonian' Theory of Light»; *Annals of Science* [S.l.: s.n.] **45** (5): 521–533; doi:10.1080/00033798800200371 (1988).

[14] BARON, M. E.; «A Note on The Historical Development of Logic Diagrams»; *The Mathematical Gazette* [S.l.: s.n.] **LIII** (383): 113–125; JSTOR 3614533 (1969).

[15] Euler, Leonhard; Orell-Fussli, «Rettung der Göttlichen Offenbahrung Gegen die Einwürfe der Freygeister». *Leonhardi Euleri Opera Omnia (series 3)* [S.l.: s.n.] **12**. (1960).

Revista
ELEMENTOS

Resolva os seus problemas que eu resolvo os meus

Sérgio Brazil Júnior
Universidade Federal do Acre

É bastante comum, quando se está cursando mestrado ou doutorado, nos depararmos com "problemas" relacionados ao que estamos estudando e que, a princípio, pensamos não ser capazes de solucionar.

O Fato a seguir ocorreu quando este autor estava cursando doutorado em Matemática, na Universidade de Brasília, entre os anos 2000 e 2004. Os nomes que aparecerão no texto são fictícios.

Josué era um aluno de mestrado em matemática muito dedicado e estava prestes a concluir sua dissertação, faltava pouco. Bastava entender e solucionar um problema relacionado ao que estava estudando e bingo! Mas as coisas não estavam andando de acordo com o que Josué esperava. O tempo foi passando e Josué nada de resolver seu último problema, que lhe separava do título de Mestre.

Josué apelou para todos os colegas que faziam mestrado e doutorado, na mesma área de conhecimento. Conversava com um, conversava com outro e nada. Foi então que um amigo, preocupado coma situação de Josué, lhe deu a seguinte ideia:

— Josué, porque você não procura o professor Malabi? Ele pode lhe ajudar.

O professor Malabi era um senhor alto, com cabelo e barba brancas, bastante sério e fechado. Era o "Papa" da área de conhecimento em que Josué fazia mestrado, um pesquisador de ponta, muito ocupado com seus trabalhos e orientações de seus alunos de mestrado e doutorado.

Josué pensou bastante e, como o tempo estava passando e nada de conseguir resolver seu problema, tomou coragem e foi falar com aquele que

supostamente o ajudaria a solucionar seu tão importante problema.

Josué foi até a sala do professor Malabi. A porta estava meio aberta, meio fechada e o Professor estava de costas, digitando algo no computador, possivelmente um novo artigo.

Josué respira fundo e diz:

— Com licença Professor Malabi. O senhor tem um minuto para conversarmos?

O Professor Malabi, continuando o que estava fazendo, sem se virar responde:

— Pois não?

Josué, tomado por uma euforia, fala:

— Professor, é que eu tenho um problema.

O Professor Malabi, sem deixar o angustiado aluno concluir sua frase, rebate de pronto:

— Meu Jovem eu também tenho muitos problemas. Resolva os seus que eu resolvo os meus e ficamos todos bem.

Nota: Josué, após esse "toco", se dedicou ainda mais e, com muito esforço, conseguiu resolver seu problema e por fim, terminou seu tão merecido mestrado.

MESTRADO PROFISSIONAL EM MATEMÁTICA-PROFMAT

O PROFMAT é um programa de pós-graduação gratuito, reconhecido pelo MEC/CAPES e que conduz ao grau de Mestre. As vagas são para professores de escola pública e pessoas da comunidade em geral. Este ano a rede do PROFMAT foi ampliada, oferecendo cerca de 1.500 vagas distribuídas por mais de 65 pólos em todos os Estados e no Distrito Federal do Brasil.

Informações a respeito desse mestrado podem ser obtidas no seguinte endereço eletrônico: www.profmat-sbm.org.br/.

Programa de Aperfeiçoamento para Professores de Matemática do Ensino Médio - PAPMEM

Este programa visa oferecer treinamento gratuito para professores de Matemática do Ensino Médio de todo o país. É realizado, sob diversas formas, desde 1990, abordando assuntos relativos às três séries do Ensino Médio. Atualmente, este programa tem recebido apoio para sua realização da CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

A Universidade Federal do Acre aderiu a este programa em 2012, tendo sido realizada duas edições. Em 2013, haverá mais um encontro entre os dias 21 e 25 de janeiro, na UFAC.

toujours le même nombre de permutations.

Cela il est aussi facile de savoir si le degré peut s'abaisser.

Et d'abord il ne peut s'abaisser plus bas que p, puisque une équation de degré moindre que p, ne peut avoir p pour facteur dans le nombre des permutations de son groupe.

Voyons donc si l'équation de degré p+1 dont les racines x_K s'obtiennent en donnant à K toutes les valeurs y compris l'infini et dont le groupe a pour substitution

$$x_K \quad x_{\frac{aK+b}{cK+d}}$$

a, b, c, d étant un carré peut s'abaisser au degré p.

Or il faut pour cela que le groupe de décomposition (ainsi appelé, étendu) en p groupes de $(p+1)\frac{p-1}{2}$ permutations chacun.

Soient α et ∞ deux lettres conjointes dans l'un de ces groupes. Les substitutions qui ne font pas changer α et ∞ de place sont de la forme

$$x_K \quad x_{m^2 K}$$

Donc si K est un carré et que M est la lettre conjointe de m^2 ou $m^2 M$. Quand M est un carré on aura donc $M^2 = 1$. Alors cette simplification ne peut avoir lieu que pour $p = 5$.

Pour $p = 7$ on trouve un groupe de $(p+1)\frac{p-1}{2}$ permutations où

∞	0	1	2	4	est respectivement pour
0	3	6	5		lettres conjointes

Ce groupe a des substitutions de la forme

$$x_K \quad x_{a\frac{K-b}{K-c}}$$

b étant la lettre conjointe de c et a une lettre qui est ou reste elle-même ou reste en même temps que c.

Pour $p = 11$ les mêmes substitutions auront lieu avec les mêmes notations,

∞	1	3	4	5	9	ayant respectivement
0	2	6	8	10	7	pour conjointes

Ainsi pour les cas de $p = 5, 7, 11$, l'équation monte bien s'abaisse au degré p.

En tout cas cette réduction n'est pas possible dans le cas plus général.