UNIVERSIDADE FEDERAL DE LAVRAS

MARDEN LUCAS ALVARENGA

A HISTÓRIA DA SIMETRIA E OS GRUPOS DE SIMETRIAS EM DUAS E TRÊS DIMENSÕES

LAVRAS

2023

MARDEN LUCAS ALVARENGA

A HISTÓRIA DA SIMETRIA E OS GRUPOS DE SIMETRIAS EM DUAS E TRÊS DIMENSÕES

Trabalho de Conclusão de Curso apresentado à Universidade Federal de Lavras, como parte das exigências do Curso de Licenciatura em Matemática, para a obtenção do título de Licenciado.

Profa. Dra. Andréia da Silva Coutinho
Orientadora

LAVRAS
2023

Dedico este trabalho aos meus pais Marizilda e Jander.

AGRADECIMENTOS

Em primeiro lugar, agradeço ao Criador de todas as coisas sem o qual, não seria possível a sabedoria necessária para a construção desse trabalho; à Nossa Senhora pela intercessão nos dias de desânimo.

Agradeço aos meus pais Jander e Marizilda; sem eles não haveria o suporte necessário para me constituir como pessoa. Obrigado por tanto e por tudo!

Agradeço à minha orientadora, professora Andréia, pela disponibilidade, pelas conversas, reflexões e toda a orientação para que esse trabalho desse certo; obrigado pelo suporte necessário. Será o exemplo de docente e humano ao qual quero seguir.

Também quero agradecer à professora Ana Claudia que me orientou durante a Iniciação Científica. Essa orientação ajudou a gerar parte dos resultados deste trabalho; obrigado por toda a contribuição. Agradeço à FAPEMIG pelo suporte financeiro recebido durante a Iniciação Científica.

Agradeço aos professores e professoras que me auxiliaram durante a minha formação, em especial às professoras que me receberam tão prontamente durante o estágio: Delsiza e Luciana.

Agradeço aos amigos que fiz durante esse percurso, em especial: Douglas, Isabella e Júlia. Com vocês os momentos nesta jornada se tornaram leves e os obstáculos se tornaram meros detalhes.

Agradeço aos meus amigos que se tornaram peças fundamentais de incentivo e tornaram meus dias mais alegres, a todos os que fazem parte da minha vida, antes que sonhasse em me aventurar pela ciência dos números, em especial aos meus companheiros: Christian, Isadora, Nathália e Jeferson.

Agradeço às pessoas que fazem parte da minha trajetória enquanto pessoa: Vivian, Duda, Maria Clara, Rafael e entre outros, o meu muito obrigado!

"Deus é o grande geômetra. Deus geometriza sem cessar. Por toda a parte, existe Geometria". (Platão)

RESUMO

Neste trabalho trataremos sobre o percurso para a resolução das equações algébricas ao longo da História da Matemática e suas reviravoltas, assim como os principais atores envolvidos nesse processo. Além disso, evidenciaremos o processo histórico para a construção da Teoria de Grupos, como consequência direta da simetria observada nas equações algébricas, nesse viés histórico daremos destaque ao matemáticos franceses Evaristé Galois, responsável pelo desenvolvimento do conceito de grupo, e Camille Jordan, responsável pela sistematização do conceito de grupo e a primeira intuição acerca dos grupos de simetrias dos polígonos e dos sólidos. Sistematicamente, apresentaremos a definição do conceito de grupo, bem como suas propriedades imediatas e outros conceitos desenvolvidos posteriormente na Álgebra Abstrata. Também trataremos da construção dos grupos de simetrias associados ao espaço euclidiano em duas e três dimensões e enfatizaremos o destaque para a construção das simetrias para quaisquer figuras e formas definidas sob esses espaços. Os grupos de simetrias, por sua vez, são ferramentas matemáticas fundamentais para a análise e classificação de objetos simétricos. Eles são conjuntos de transformações que preservam a forma, distância e estrutura, como rotações e reflexões. Os grupos de simetria são amplamente aplicados em várias áreas, desde a Física de Partículas e Cristalografia.

Palavras-chave: História da Matemática. Simetria. Grupos. Grupos de Simetria. Camille Jordan.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

A História da Matemática nos leva a refletir que toda a construção do campo científico da Matemática contribui de maneira significativa com os processos de conhecimento e tecnologia, nos fazendo pensar que os processos para a constituição das teorias e conceitos matemáticos nem sempre é linear.

Neste trabalho faremos uma contextualização histórica a partir da busca pela solução das equações algébricas, principalmente naquelas que foram ditas insolúveis e como isso culminou no desenvolvimento de um dos mais importantes conceitos do campo da Matemática Pura, a Simetria, conceito que revolucionou a Álgebra Moderna, através da Teoria dos Grupos passando do "estudo das coisas" para o estudo das estruturas. Além da sua contribuição para a Teoria dos Grupos, a simetria é a peça-chave para a Física-Matemática, tornando possível desenvolver tudo o que conhecemos hoje sobre o universo.

Após analisarmos os fatores históricos que nos levaram ao que conhecemos hoje como grupos, buscaremos defini-los através da Matemática. Tendo como foco os grupos de simetria ligados às figuras geométricas, perpassaremos pela análise e construção dos grupos de simetrias no espaço euclidiano de dimensão dois e, por conseguinte, analisaremos os grupos de simetria em torno dos sólidos platônicos que generalizarão as simetrias no espaço euclidiano $\mathbb{R}^3$.

A escolha pelo estudo das simetrias se deu pela discussão da importância desse ente matemático que revolucionou o pensamento matemático desde a Idade Média e fez suas contribuições para destacadas teorias contemporâneas. Através desse conceito estético pôde-se perceber padrões ocultos na Natureza e na Matemática, e assim foi possível a ascendência do conhecimento humano acerca do ambiente que o cerca.

Este trabalho está dividido em cinco capítulos, começando por esta Introdução. No Capítulo 2 trataremos sobre o percurso histórico pela busca da solução das equações algébricas, percorrendo as equações quadráticas, cúbicas, quárticas e as quínticas, chegando ao desenvolvimento da Teoria dos Grupos por Galois, bem como a construção dos grupos de simetrias feita por Camille Jordan. No Capítulo 3 faremos uma breve revisão teórica de alguns tópicos de Álgebra Linear, assim como no Capítulo 4 faremos uma breve revisão de alguns conceitos e resultados da Teoria de Grupos. Por fim, no Capítulo 5, desenvolveremos a construção dos grupos de simetrias no espaço euclidiano de dimensão dois e três sob a perspectiva de Curtis (1984).

2 UM PERCURSO HISTÓRICO

Neste capítulo apresentaremos um panorama histórico do caminho percorrido pelos grandes matemáticos antigos até o desenvolvimento da Teoria de Grupos. Destacamos que a busca pela resolução de problemas matemáticos nem sempre é linear e que, por vezes, se extravia do objeto e muitos obstáculos são encontrados.

2.1 A Matemática Antiga

Stewart (2012) pontua que o estudo da simetria teve suas origens na antiguidade, mesmo que não houvesse qualquer formalização devidamente explicitada. Esse estudo foi documentado na antiga civilização babilônia e ali houve então a primeira trilha para a concepção desse conceito tão importante na Matemática Moderna.

É sabido que o sistema de numeração babilônio possui características diferentes do sistema decimal que utilizamos. A base desse sistema antigo era a sexagesimal, ou seja, era baseado em potências de 60. Diferentemente do que se imagina, os babilônios possuíam um alto grau de conhecimento matemático, "conheciam os triângulos retângulos e tinham algo semelhante ao que chamamos agora de Teorema de Pitágoras." (STEWART, 2012, p. 20).

A forma de escrita adotada nessa região era da forma cuneiforme, o registro era feito em tábuas de argila, o que consequentemente tornou essas provas históricas resistentes ao tempo. Atualmente é possível ainda encontrar esses registros, sendo um modo de comprovar os fatos matemáticos daquela civilização, uma vez que o calor contribuiu para que o material em argila se transformasse em cerâmica, material de alta durabilidade.

Os escribas babilônios, assim como os sacerdotes no Egito, tinham acesso irrestrito ao conhecimento disponível na época; esses membros do governo registravam seus conhecimentos nas tábulas de argila, visando preservar suas ideias. Em 1930, Otto Neugebauer, ao pesquisar sobre esses registros, concluiu que em uma dessas tábulas havia uma expressiva noção das conhecidas equações quadráticas e como resolvê-las; acredita-se que as resoluções propostas para essas equações tinham base na geometria antiga.

É notório que as grandes descobertas matemáticas tiveram palco na civilização egípcia, especialmente na cidade de Alexandria. Euclides, grande nome da geometria teria nascido e desenvolvido suas obras acerca dessa área nessa cidade egípcia. "Se a matemática tivesse endereço, este seria a casa de Euclides" (STEWART, 2012, p. 35). Acredita-se que Euclides tenha nascido por volta de 325 a.C. e falecido próximo a 265 a.C..

“*Os Elementos*” de Euclides (figura 2.1), uma grande obra que revolucionou a Matemática, reuniu grandes contribuições para a geometria, tão somente quanto para a formalização matemática. É através dessa obra que nascem os axiomas, provas e demonstrações de teoremas, antes somente aceitos como verdadeiros. Também é a partir dos métodos encontrados nessa coleção sobre geometria que os grandes estudiosos da área começaram a pensar na ciência dos números através de uma nova perspectiva. É interessante destacar que a perspectiva matemática para os babilônios e os egípcios era da forma prática, sem quaisquer intenções lógicas, o que contrasta com a perspectiva grega, que traz consigo o pensamento de que os números geram o raciocínio, ou seja, são os meios para desenvolver a racionalidade e é nessa concepção que a obra de Euclides se encaixa.

Figura 2.1 – Página ilustrada, na versão de Sir Henry Billingsley em língua inglesa dos Elementos de Euclides, de 1570.

Fonte: Library of Congress (1570).

Euclides, em sua obra, desbravou inumeráveis conceitos, como a famosa construção das figuras geométricas utilizando a régua e o compasso. É compreensível que, com essas propostas inteiramente novas, surjam então novos problemas, novos pensamentos e então novas soluções e, como consequência desses processos, temos novas ferramentas matemáticas, além de novas teorias matemáticas. De acordo com (STEWART, 2012), em “*Elementos*”, encontramos a partição de ângulos, o que torna possível a construção de polígonos. São esses entes geométricos que nos geram as primeiras figuras geométricas construídas de maneiras "rudimentares".

2.2 Um trajeto nada linear

Os matemáticos egípcios e babilônios preocupavam-se em desenvolver a matemática prática. Pontuamos que Euclides preocupou-se em tornar a Matemática um campo conceitual, trazendo o formalismo consigo, além de inovar na área da geometria. Concomitante a isso, os babilônios preocuparam-se em repassar suas noções de resolução das equações quadráticas aos gregos. Héron, que viveu em Alexandria, procurou esboçar a resolução de um problema típico babilônico, mas com os ideais gregos, empregando algum racionalismo adquirido com as ideias euclidianas.

Nessa época, por volta de 100 a.C., Nicômaco escreveu um livro chamado "*Introdução à Aritmética*" no qual havia uma fuga da representação dos números de acordo com a tradição grega que representava os números como quantidades geométricas através de áreas e comprimentos. Para o matemático em questão, os números possuíam fim em si mesmos e, por isso, utilizava somente números inteiros, sem quaisquer simbolismos. Quando tratamos do simbolismo, verificamos o papel da Álgebra, área da Matemática que registrou pela primeira vez o uso de símbolos para a representação numérica.

> "O simbolismo entrou na Álgebra com o trabalho de um grego chamado Diofanto, por volta do ano 500. A única coisa que sabemos sobre Diofanto é a idade em que morreu, e isso chegou até nós por um caminho de autenticidade duvidosa. [...] Ele escreveu uma obra sobre números poligonais, e algumas partes dela sobreviveram. É apresentada no estilo euclidiano, demonstra teoremas usando argumentos lógicos e tem pouca importância matemática." (STEWART, 2012. p. 52-53).

A escola de Alexandria nos gerou destacados matemáticos como Diofanto, o pai da Álgebra. Em sua obra "*Arithmetica*", o matemático egípcio, Diofanto, nos mostrou como resolver três tipos de equações quadráticas, que segundo Livio (2005), seriam $ax^2+bx+c=0$; $ax^2=bx+c$; e $ax^2+c=bx$, com a,b e c números positivos e pontua que essas formas foram os tipos mais procurados pelos matemáticos árabes por mais de cinco séculos.

Com a queda da Escola de Alexandria, o mundo árabe passou a ter um maior destaque. Na Índia, especialmente, o campo dos números obteve um grande avanço, Brahmagupta, nascido em 598 d.C., resolveu inúmeras equações propostas por Diofanto, além de desenvolver métodos para a solução de equações quadráticas com números negativos. Também, em território indiano, encontramos aquele que deu o nome à Álgebra, Musa al-Khwarizmi, esse matemático foi responsável pela publicação do livro que, durante séculos, foi a base para a teoria das equações. Foi através do título encontrado nesse livro, "*al-jabr*", que se originou a palavra álgebra.

Entretanto, de acordo com (LIVIO, 2005), o primeiro livro que incluía de fato a resolução completa para as equações quadráticas de maneira geral surgiu no século XI, com o matemático europeu Abraham bar Hiyya Ha-nasi, nascido em 1070. Logo, o processo de construção para essa resolução se arrastou por quase três mil anos e parecia entrar em um descanso aparentemente tranquilo.

Porém, não se esperava que no futuro a busca pela solução das equações algébricas passaria por tantas reviravoltas. Se considerarmos os problemas geométricos envolvendo áreas, teremos equações quadráticas, mas se tratando do volume de sólidos, como, por exemplo, o cubo, chegaremos a uma equação cúbica que possui a forma mais geral $ax^3 + bx^2 + cx + d = 0$, com a, b, c, d números reais com $a \neq 0$.

Segundo (LIVIO, 2005, p.80), "os antigos babilônios de fato geraram algumas tabelas que lhes permitiram solucionar algumas cúbicas bem específicas". Entretanto, a solução geral para as equações cúbicas ainda se tornava um desafio para muitos estudiosos daquele período. Mas, eis que surge Scipione del Ferro, nascido em 1465 em Bolonha e, em seu caminho, surge Luca Pacioli frustrado por não conseguir exibir uma solução para as cúbicas, convenceu del Ferro a realizar tal feito.

Em aproximadamente 1515, Scipione del Ferro finalmente conseguiu solucionar a equação do tipo $ax^3 + bx = c$ ou, em linguagem natural: "incógnitas e cubos iguais a números". Porém, o matemático europeu não publicou seu manuscrito, confidenciando-o ao veneziano Antonio Maria Fiore e a seu genro Annibale della Nave. Scipione então faleceu antes mesmo de ver o momento áureo de sua descoberta, deixando-a nas mãos de seu genro.

Entretanto, afetado pela forte fama da Matemática em Bolonha no século XVI e para garantir sua cátedra na universidade, Fiore, em 1535, desafiou Niccolò Tartaglia numa competição de resolução de problemas matemáticos; Tartaglia, era um matemático considerado talentoso. Niccolò Tartaglia nasceu entre 1499 e 1500 em Bréscia, e, em 1534, se mudou para Veneza para exercer o ofício de professor de Matemática. Nessa década, o professor afirmou, em seus escritos, ter conseguido chegar à resolução da equação cúbica $x^3 + 3x^2 = 5$. Essa informação chegou ao conhecimento de Antonio Maria Fiore e este duvidou que Niccolò pudesse ter chegado à resolução de tal equação.

Então, após definirem as regras para que ocorresse a competição pública, em 1535, ocorreu o grande evento. Fiore, que possuía somente uma técnica, a desenvolvida por del Ferro, foi rapidamente derrotado por Tartaglia, que resolveu rapidamente diversas das equações propostas.

> "Para o assombro dos espectadores, Tartaglia esfacelou inteiramente todos os problemas lançados a ele no espaço de duas horas! Fiore não conseguiu resolver um único dos problemas de Tartaglia. [...] De fato, um dia depois de descobrir a solução para $ax^3 + bx = c$, Tartaglia também descobriu a solução para $ax + b = x^3$." (LIVIO, 2005. p. 85).

A fama de Tartaglia, após o desafio, logo se espalhou em todas as regiões da Europa, até chegar aos ouvidos de Girolamo Cardano, matemático, nascido em 1501, que foi auxiliar de Leonardo da Vinci em problemas geométricos. Cardano era um tanto quanto curioso e tinha um gosto hábil por jogos. Logo que ficou sabendo da competição entre Fiore e Tartaglia, seu interesse se aguçou. O matemático em questão fez publicações sobre as práticas aritméticas em um de seus livros e teve o interesse de incluir a solução das equações cúbicas nessas publicações. Entretanto, desgastou-se por vários anos ao tentar encontrar uma solução que de fato funcionasse.

Conhecendo a fama de Tartaglia, Girolamo propôs um encontro para ambos discutirem a resolução dos problemas das cúbicas. Porém, Niccolò inúmeras vezes se negou a encontrar Cardano, alegando que suas ideias seriam restritamente suas, mas isso não perdurou por muito tempo. Tartaglia cedeu ao encontro com Cardano:

> "[...] ele finalmente concordou em divulgar o segredo a Cardano, mas somente depois que o último fez o seguinte juramento solene: "Juro a você pelo Sagrado Evangelho e por meu credo de cavalheiro, não apenas nunca publicar suas descobertas, se me forem reveladas por você, mas também prometo e penhoro minha fé como cristão verdadeiro de as colocar em escritas cifradas para que, depois de minha morte, ninguém seja capaz de as compreender." (LIVIO, 2005. p. 88).

Ludovico Ferrari, secretário da família Cardano, presenciou o juramento, entretanto, era tão confiável quanto Cardano. Mais tarde, alegou que o seu mestre não o teria feito. Ferrari, chegado a casa de Girolamo aos 14 anos, em 1540 conseguiu resolver a equação $x^4 + 6x^2 + 36 = 60x$. Após uma visita ao genro de del Ferro, que possuía os escritos do matemático, com o propósito de verificar as soluções deixadas por Scipione, em 1545, Cardano publicou o livro "*A* *grande arte ou as regras da álgebra, Livro um*” (figura 2.2), considerado como o marco inicial da álgebra moderna. Neste livro, Cardano explorou as soluções das cúbicas e das quárticas, além de apresentar resoluções envolvendo números negativos, irracionais e até casos com raízes quadradas de números negativos.

Figura 2.2 – Fronstispício do livro de Cardano.

Fonte: SANTOS (2008).

No livro de Cardano continha as soluções propostas por Tartaglia, que logo se enfureceu por ter suas ideias roubadas e publicadas de forma tão abrupta. Tartaglia tratou logo de publicar sua obra “*Novos problemas e invenções*” na qual acusava piamente que Cardano lhe havia roubado os métodos matemáticos para a solução das equações cúbicas. Ferrari, fiel discípulo de Cardano, saiu em defesa do autor de “*A grande arte*”, afirmando que Cardano havia feito um favor ao matemático de Bréscia, por resgatar a sua fórmula do esquecimento geral.

Apesar da confusão, o livro de Cardano não teve seu destaque com a solução da cúbica, e sim com um método para a solução das equações quárticas. Ferrari utilizou dos resultados obtidos por Tartaglia e del Ferro, fazendo uma extensão dos métodos para as equações elevadas à quarta potência. O método de Ferrari envolvia o uso de raízes quadradas e cúbicas, uma vez que a quarta potência é simplesmente a raiz quadrática elevada a dois. Contudo, o livro de Cardano não tratava de soluções para as equações de quinto grau. De acordo com (STEWART, 2012), o matemático não se preocupou em analisá-las, retomando sua atenção para outros assuntos pessoais, dedicando o resto de sua vida para a medicina.

2.3 A Contemporaneidade de Galois

Evaristé Galois (1811-1832) não construiu suas ideias revolucionárias apenas com seus conhecimentos próprios. Foi preciso que grandes matemáticos de sua época discorressem sobre a solução das equações para que Galois desenvolvesse suas teorias. Preocupado com a solução das equações de quinto grau ou graus maiores, Joseph-Louis Lagrange (1736-1813), matemático italiano, publicou seu primeiro trabalho sobre o assunto "*Réflexions sur la résolution algébrique des équations*" entre 1770 e 1771. De acordo com (KIERNAN, 1971), seu trabalho, além de se preocupar com uma forma para solucionar as equações de quinto grau, Lagrange apresentou procedimentos mais detalhados para a resolução das equações de segundo, terceiro e quarto graus.

> "Lagrange estava ainda principalmente preocupado com o atual processo computacional, ele fez duas contribuições significativas para as técnicas da teoria geral. Primeiro, ele introduziu símbolos para as raízes, e computou diretamente com essas quantidades da forma como elas eram conhecidas. Ele observou como essas e outras quantidades não conhecidas interagiam com as únicas quantidades realmente conhecidas..." (KIERNAN, 1971, p. 45, tradução nossa). [1]

É importante destacar que Lagrange forneceu ferramentas essenciais para a área das soluções das equações algébricas em sua época, a começar pela simbologia para as raízes. Ainda, ao verificar a interação entre os valores conhecidos e desconhecidos, possibilitou uma infinidade de contribuições para a construção das provas aos problemas algébricos da época, uma vez que seria possível manipular aquilo que se conhece para chegar a soluções que não estão claras.

O matemático italiano se preocupou em estudar o comportamento das raízes de uma equação, se atentando como elas se portavam ao serem permutadas entre si, ou seja, se as raízes eram simétricas em uma equação totalmente simétrica, então as soluções poderiam ser rearranjadas de forma a encontrar valores conhecidos. Todo o trabalho de Lagrange se iniciou então com as equações cúbicas e quárticas. Ele acreditava que se essa técnica funcionasse para estas equações, então seria possível resolver as equações quínticas.

---

[1] No original: "[...] Lagrange is still primarily concerned with the actual computational process, he makes two significant contributions to the techniques of the general theory. First, he introduces symbols for the roots, and computes directly with these quantities as though they were known. He observes how these and the other actually unknown quantities interact with the only truly known quantities..." (KIERNAN, 1971, p. 45).

Através do rearranjo (exemplo na figura 2.3), o italiano conseguia reduzir as equações de graus maiores a equações chamadas de auxiliares ou resolventes; essas equações mais simples dariam um suporte para que as raízes da equação de grau maior fossem determinadas. Por exemplo, uma equação cúbica poderia ser reduzida a uma equação quadrática, que possuía uma fórmula para sua resolução; o caminho parecia claro para Lagrange, que acreditava na solução da quíntica ao reduzi-la a equações de graus menores. Logo poderia exibir resultados apoiados nas ideias de del Ferro, Cardano, Tartaglia e Ferrari.

Figura 2.3 – Permutação das raízes.

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_1 & x_4 & x_3 \end{pmatrix} \rightarrow \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_3 & x_2 & x_1 & x_4 \end{pmatrix}$$

Fonte: Do autor (2023).

Contudo, ao seguir o caminho de seu novo método, o italiano encontrou uma grande decepção. Ao aplicar a técnica, percebeu que não obteria uma quártica fácil para resolver, mas encontrou uma equação resolvente do sexto grau, o que tornou a solução bastante complicada. Lagrange chegou a acreditar que as equações quínticas possivelmente não possuíam soluções algébricas, entretanto seu trabalho viria a servir de base para outros matemáticos da época.

Paolo Ruffini (1765-1822), médico e matemático italiano, pela influência dos resultados de Lagrange publicou diversos trabalhos com o intuito de demonstrar que as equações gerais de graus maiores que o quarto grau não podiam ser resolvidas por radicais. Ruffini também utilizou das permutações, seguindo os passos de Lagrange para desenvolver suas provas. De acordo com (KIERNAN, 1971), Ruffini exibiu diversos sistemas para os rearranjos através de suas provas, porém, não os conseguiu traduzir para a terminologia matemática moderna e, com suas demonstrações, apresentou uma noção de grupos ao analisar os rearranjos de forma individual que poderiam ser escritos como permutações.

Ruffini determinou uma permutação específica para as equações simétricas solúveis e provou que esse rearranjo só funcionava para expressões com grau menor ou igual a quatro. Entretanto, todo trabalho do matemático não foi bem recebido por seus contemporâneos, uma vez que os matemáticos antigos acreditavam na solução das equações quínticas algebricamente. Porém, mesmo sem o reconhecimento de sua obra, o trabalho de Ruffini viria a se tornar o ponto de partida para a construção que revolucionaria a Álgebra.

Lagrange e Ruffini se apoiaram no conceito das permutações para desenvolverem suas ideias, entretanto, a base teórica para essa ferramenta viria de Augustin-Louis Cauchy (1789-1857), matemático francês. Cauchy trabalhou criteriosamente na construção das permutações que contribuiria de forma significativa para a Teoria de Galois posteriormente. Em sua obra de 1815, "*Mémoire sur le nombre des valeurs qu'une fonction peut acquérir, lorsqu'on y permute de toutes les manières possibles les quantités qu'elle renferme*", o matemático francês dedicou-se a provar a quantos valores diferentes uma equação não simétrica poderia exibir. Estes resultados viriam a generalizar os trabalhos de Ruffini e, com esses resultados, Cauchy viria a construir com sofisticação as intuições de permutação.

> "Cauchy define o produto de duas permutações, e reconhece a permutação identidade como uma permutação; ele definiu a ordem de uma permutação, uma permutação cíclica e sua potência, e uma transposta. Também nesse artigo, Cauchy introduz e define os termos "permutação" e "substituição" que permaneceram em uso comum durante o século 19." (KIERNAN, 1971, p. 65, tradução nossa). [2]

Com esses resultados sofisticados de Cauchy, mais tarde Galois, ao consultar os manuscritos do matemático francês, viria a pontuar os grupos de permutações, considerando os arranjos que poderiam ser feitos com as raízes das equações. Mas, os interesses de Cauchy logo mudaram para outras questões e, por trinta anos, não se preocupou com a questão das permutações e as equações algébricas.

Contudo, após os resultados exibidos por matemáticos como Ruffini e Lagrange, embora inconclusos, outro grande matemático viria a surgir, acreditando resolver o problema das soluções das equações algébricas. O matemático alemão Niels Henrik Abel (1802-1829) durante sua adolescência acreditava ter provado que a equação quíntica geral poderia ser resolvida, entretanto, logo percebeu erros em suas demonstrações e, no ano de 1824, publicou o panfleto "*Mémoire sur les équations algébriques, où l'on démontre l'impossibilité de la résolution de l'équation générale du cinquème degré*". Abel enviou esses resultados a Gauss, na esperança de que obtivesse um retorno quanto a veracidade de suas provas, porém, nunca obteve retorno do matemático.

O método de Abel consistia em encontrar uma forma mais geral para a equação resolvente, tendo base na equação geral de Lagrange, a saber:

[2] No original: "Cauchy defines the product of two permutations, and recognizes the identity permutation as a permutation; he defines the order of a permutation, a cyclic permutation and its powers, and a transposition. Also in this paper, Cauchy introduces and defines the terms "permutation"and "substitution"which were to remain in common usage through the 19^{th} century." (KIERNAN, 1971, p. 65).

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0,$$

onde $a_1, a_2, \cdots, a_{n-1}, a_n \in \mathbb{R}$. De acordo com (KIERNAN, 1971), Abel então fez uma construção de sucessivas resolventes, com base em Ruffini, e analisou que seria necessário mais de uma resolvente para determinar a solução das raízes desta equação. Dessa forma, com os resultados do matemático alemão, a forma da última resolvente deveria ser

$$x = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \cdots + q_{n-1} p^{\frac{n-1}{n}},$$

onde n é primo e $p, q_0, q_2, ..., q_{n-1}$ são expressões algébricas dos coeficientes da equação geral.

Além disso, Abel se determinou a elaborar classificações para as equações seguindo alguns critérios como a ordem e o grau, considerando o número de radicais que poderiam ser expressos para a resolução geral. Então,

> “[...] Abel conclui que se a equação geral é algebricamente solúvel, então cada uma das raízes da equação geral pode ser colocada numa fórmula de tal modo que cada expressão algébrica envolvida é racional nessas raízes. Apropriadamente, Abel deveria ter dito, “racional nessas raízes e nas raízes da unidade” [...]. Esse resultado é frequentemente referido como “Teorema de Abel”.” (KIERNAN, 1971, p.68, tradução nossa). [3]

Portanto, Abel forneceu condições necessárias para que a equação quíntica de fato pudesse ser resolvida, refutando aquilo que Ruffini afirmou ser insolúvel. A partir dessas concepções, o matemático alemão passou a contribuir de maneira significativa para a Álgebra. Outra questão desenvolvida por Abel foi quanto à comutatividade de duas raízes, de acordo com suas provas, se duas raízes $\theta x, \theta_1 x$ podem ser relacionadas da seguinte forma

$$\theta\theta_1 x = \theta_1\theta x,$$

então a equação pode ser solúvel. A partir deste resultado, começou-se a atribuir a comutatividade a Abel que posteriormente nomeia os grupos comutativos, sendo os Grupos Abelianos.

Somente após a morte de Abel que seus resultados sobre as solubilidades de algumas quínticas vieram a ser afamados. De acordo com (STEWART, 2012), a pergunta que revolucionaria a matemática seria ”Se algumas quínticas podem ser resolvidas e outras não, o que diferenciava um tipo do outro?”. Quem viria a responder de forma sucinta a essa questão seria o matemático francês Evaristé Galois.

[3] No original: “[...] Abel concludes that if the general equation is solvable algebraically, then each of the roots of the general equation can be put into a form such that each algebraic expression involved is rational in those roots. Properly, Abel should have said, “rational in those roots and in the roots of unity” [...]. This result is often referred to as “Abel’s Theorem”.”(KIERNAN, 1971, p.68).

Galois (1811-1832) iniciou seus estudos no colégio Louis-le-Grand em Paris, lá obteve seu primeiro contato com a matemática. Segundo (STEWART, 2012), Galois iniciou seus estudos indo direto aos clássicos matemáticos como os "*Elementos de Geometria*" de Legendre. Logo o francês buscou as leituras dos manuscritos de Abel e Lagrange, contudo, Galois sempre obtinha resultados mas não os demonstrava de maneira sucinta, o que irritava seus professores.

Era do desejo de Galois ingressar na maior formadora de matemáticos na França, a École Polytechnique. Como ignorava quaisquer orientações para sistematizar suas soluções, o garoto francês foi reprovado na prova para ingresso na instituição. Mais tarde, um professor chamado Louis-Paul Richard vendo o potencial de Evaristé, o matriculou num curso de matemática avançada, sendo o orientador de Galois.

Nesse contexto, escreveu seu primeiro artigo sobre frações contínuas e os enviou a Academia de Ciências da França com a esperança de que fosse publicado. Entretanto, como quaisquer processos para reconhecimento naquela época, o artigo do jovem francês deveria passar pela avaliação de membros da área, logo seus escritos foram para Cauchy, que não lhe retornou.

Contudo, Galois foi admitido na École Normal e por lá se formou no ano de 1829 em Ciências e Letras. De acordo com (STEWART, 2012), em 1830, Galois entregou à Academia seus manuscritos sobre a Teoria das Equações para o Grande Prêmio. Joseph Fourier ficaria responsável por analisar seu trabalho, porém, para o descontentamento de Evaristé, Fourier morreu antes mesmo de ler seu escrito.

Marcado pela falta de reconhecimento da Academia, Galois se alistou na Artilharia da Guarda Nacional. Algum tempo depois, Galois se veria num duelo afim de conquistar o coração daquela em que estava apaixonado. Ainda, de acordo com (STEWART, 2012), "o duelo foi com pistolas. O relatório póstumo afirma que foram disparadas a 25 passos [...]". Ali, Evaristé Galois veria o fim de sua vida em 1832, mas deixaria um legado escondido. Às vésperas de sua morte, Galois teria escrito a Auguste Chevalier esboçando sobre suas descobertas que estabelecia a relação entre grupos e equações polinomiais.

Foi através de Joseph-Louis Liouville que os escritos de Galois se tornaram famosos perante a Academia. Por isso, com essas descobertas do matemático francês que fora tragicamente morto, a matemática sofreu uma grande revolução.

> "Com Galois, a matemática deixou de ser o estudo dos números e das formas - arimética, geometria e ideias desenvolvidas a partir daí como álgebra e trigonometria. Tornou-se o estudo de estruturas. O que começou como um estudo de coisas se transformou num estudo de processos." (STEWART, 2012, p.136).

Galois então começou a trabalhar com os grupos de permutações. Vejamos o exemplo examinado por (STEWART, 2012). Considerando uma equação genérica cúbica, temos três raízes a, b e c. Logo, há seis maneiras de permutar essas raízes; chamemos as permutações de $I = abc$, $R = acb$, $Q = bac$, $V = bca$, $U = cab$ e $P = cba$. Então teremos a tabela de multiplicação, conforme o quadro 2.1..

Quadro 2.1 – Tabela de multiplicação para as seis permutações das raízes da equação cúbica.

	I	U	V	P	Q	R
I	I	U	V	P	Q	R
U	U	V	I	R	P	Q
V	V	I	U	Q	R	P
P	P	Q	R	I	U	V
Q	Q	R	P	V	I	U
R	R	P	Q	U	V	I

Fonte: Adaptada de Stewart (2012).

O matemático francês logo percebeu que o produto entre duas permutações também é uma permutação. Há uma propriedade interessante a ser analisada, pois o produto de duas permutações, neste conjunto, continua a pertencer a ele. Galois passou a chamar estas permutações de *permutações de um grupo* e, neste caso, quando conseguimos criar subconjuntos do grupo geral, em que este subconjunto é um grupo, o chamamos de *subgrupo*, como é o caso do conjunto $\{I, U, V\}$:

Quadro 2.2 – Tabela de multiplicação do subconjunto de três permutações.

	I	U	V
I	I	U	V
U	U	V	I
V	V	I	U

Fonte: Adaptada de Stewart (2012).

Partindo dessa teoria, Galois então afirmou que qualquer equação algébrica possui um grupo associado a ela, este grupo recebe o nome de grupo de simetria da equação ou Grupo de Galois. Com essas ideias, o problema da resolução das equações algébricas tomou um novo panorama, sob a perspectiva da teoria recém-nascida. De acordo com (STEWART, 2012), podemos construir uma árvore para visualizarmos as ideias propostas pelo francês.

> "O tronco é o grupo das equações de Galois. Os galhos, gravetos e folhas são os vários subgrupos. Os subgrupos surgem naturalmente assim que começamos a pensar sobre como as simetrias das equações mudam quando começamos a pensar radicais. [...] Galois mostrou que se temos a $p-ésima$ raiz, então o grupo de simetria pode ser subdividido em p blocos distintos do mesmo tamanho [...]. Então, por exemplo, um grupo de 15 permutações poderia se dividir em 5 grupos de 3, ou 3 grupos de 5[...], uma delas deve formar por conta própria um subgrupo de um tipo especial conhecido como "subgrupo normal de índice p"." (STEWART, 2012, p.139)

Ao observar a condição imposta quanto ao subgrupo normal de índice p, Galois conseguiu identificar que, para as equações quínticas, não existe qualquer subgrupo normal de índice 5. E aqui, a chave para a questão discutida por séculos parece encontrar sua resposta, entretanto, alguns matemáticos como Sylvestre François Lacroix, Siméon Denis Poisson e Augustin-Louis Cauchy não ficaram entusiasmados com a descoberta.

É interessante analisar que os grupos de Galois nos dizem respeito a soluções das equações algébricas, entretanto, se analisarmos estritamente somente pela equação dada, não conseguiremos verificar se a equação é solúvel ou não. Isso ocorre pelo fato de que a Teoria de Galois consiste na análise das raízes num grupo e não considera os coeficientes, logo, o seu desenvolvimento se dá com o que é desconhecido e não com o que conhecemos. Contudo, Evaristé Galois abriu uma porta de inúmeras possibilidades para o desenvolvimento da Álgebra, e seus sucessores fizeram inúmeras contribuições apoiando-se nas suas teorias.

2.4 Jordan e os Grupos de Simetria

Após a publicação das descobertas de Galois, inúmeros matemáticos puderam se apoiar nos manuscritos do francês para construir novos ramos da Álgebra Moderna, bem como para estender e aprofundar os resultados já publicados. No ano de 1866, surge a terceira edição do curso de Álgebra desenvolvido pelo matemático francês Joseph Alfred Serret. De acordo com (KIERNAN, 1971), o manuscrito de Serret traz consigo algumas novas terminologias como o conceito de "grupos de equações". Além disso, contribui para a reformulação de algumas demonstrações esboçadas por Galois.

> "A principal contribuição de Serret é notacional. A primeira representação dele aparece no que pode ser reconhecida como notação moderna. Isso resulta principalmente do fato de que sua notação reconhece que o conjunto de permutações e não o conjunto de arranjos, esses conceitos são o objeto de prin-

> cipal preocupação no desenvolvimento." (KIERNAN, 1971, p.111, tradução nossa). [4]

Dentre essas inúmeras contribuições realizadas por Serret, as notações propostas por ele puderam aprimorar o estudo das estruturas algébricas, como é o caso considerado para o conjunto das permutações, antes notados como arranjos:

$$\phi_n = \{1, S_1, S_2, ..., S_{n-1}\},$$

passando então a considerar a notação dos grupos de permutação:

$$\phi = \{1, TS_1, T^{-1}, TS_2T^{-1}, ..., T_{S_{n-1}}T^{-1}\},$$

sendo esta a notação moderna para um agrupamento de permutações ou um grupo de permutações.

O curso de Serret se difundiu entre diversos espaços acadêmicos da época, tornando-se uma das bases para a álgebra dos grupos. Um de seus alunos, o matemático francês Camille Jordan, foi o responsável por contribuir significativamente para o progresso das teorias de Galois. Em 1870, influenciado por Serret, Jordan publica seu primeiro manuscrito a respeito das permutações e as equações algébricas intitulado *Traité des substitutions et des équations algébriques*. Segundo Kiernan (1971, p. 114),[5] "seu trabalho serve como um ponto alto da matemática francesa, pelo menos na álgebra, no final do século XIX."

Jordan foi responsável por revolucionar o conceito de grupo, trazendo consigo alguns conceitos antes tratados por Lagrange. O matemático francês deu notoriedade e formalismo a muitos teoremas desde Galois. Segundo Kiernan (1971), seu trabalho foi tão revolucionário quanto o de Evaristé Galois, sendo o trabalho de Jordan considerado tão original quanto os manuscritos divulgados por Liouville.

> "O envolvimento de Jordan com a teoria dos grupos começou em 1867, quando exibiu o profundo elo com a geometria de maneira bem explícita, classificando os tipos básicos de movimentos de um corpo rígido no espaço euclidiano. Mais importante, fez uma excelente tentativa de classificar como esses movimentos podiam ser combinados em grupos." (STEWART, 2014, p. 240).

---

[4] No original: "Serret's main contribution is notational. His is the first presentation which appears in what can be recognized as modern notation. This principally results from the fact that his notation recognizes that the set of permutations and not the set os arrangements is the object of chief concern in the development." (KIERNAN, 1971, p.111).

[5] No original: "[...] which serves as the high point of French mathematics, at least in algebra, in the later part of the 19^{th} century." (KIERNAN, 1971, p. 114)

Os estudos de Jordan, por certo período, se concentraram em generalizar as pesquisas realizadas por Auguste Bravais, físico francês. A pesquisa de Bravais estava relacionada com as simetrias das estruturas cristalinas. Camille se dedicou a explorar os grupos ditos fechados, ou seja, quando realizados movimentos deste grupo, resultam em elementos do próprio grupo.

Ao considerar o estudo destes grupos, segundo (STEWART, 2014), Jordan estabeleceu os movimentos de translação, rotação, reflexão e a reflexão deslizada, que consiste na composição de uma reflexão e uma translação. Além disso, no espaço em três dimensões, considerou o movimento chamado de parafuso, quando é fixado um eixo e o objeto gira em torno de si e ao redor deste eixo. Ele observou as translações em que as distâncias de movimento são fixas e as em quaisquer distância e pôde listar dez ao considerar todas.

De acordo com Stewart (2014, p. 242), Jordan "listou também os principais grupos finitos de rotações e reflexões: cíclico, diédrico, tetraédrico, octaédrico e icosaédrico". Seu trabalho perpassou dois espaços euclidianos, sendo em duas dimensões e três dimensões, o que revelou um grande escopo para o trabalho do matemático. Jordan utilizou das noções de permutações para verificar esses movimentos, que posteriormente seriam associados a transformações no plano e no espaço.

Com Camille Jordan, a Álgebra buscou novas interseções, como é o caso da Geometria, tornando-se uma área que transita entre diversos campos da Matemática, passando a constituir uma grande área e uma importante linha de pesquisa para diversos estudiosos ao longo dos tempos, aprimorando aquilo que Galois propôs com simplicidade.

3 NOÇÕES DE ÁLGEBRA LINEAR

Neste capítulo apresentaremos algumas estruturas, propriedades e conceitos importantes da Álgebra Linear com base em (COELHO; LOURENÇO, 2020) e (CURTIS, 1984). Essa revisão teórica nos fornecerá ferramentas importantes para descrever as estruturas dos grupos de simetria no espaço euclidiano de dimensão dois e três.

3.1 Espaços Vetoriais

Definição 3.1. *Um conjunto não-vazio V é um espaço vetorial sobre $\mathbb{R}$ se, em seus elementos, denominados vetores, estiverem definidas as seguintes operações:*

(Adição) A cada par $(u,v) \in V \times V$ corresponde um vetor $u+v \in V$, chamado soma de u e v, de modo que:
(A1) $u+v = v+u$, para todo $u,v \in V$ (propriedade comutativa);
(A2) $(u+v)+w = u+(v+w)$, para todo $u,v,w \in V$ (propriedade associativa);
(A3) exista em V um vetor denominado vetor nulo – e denotado por 0 – tal que $0+v = v$, para todo $v \in V$ (elemento neutro);
(A4) a cada vetor $v \in V$, exista um vetor em V, denotado por $-v$, tal que $v+(-v) = 0$ (elemento simétrico).

(Multiplicação por escalar) A cada par $(\alpha,v) \in \mathbb{R} \times V$ corresponde um vetor $\alpha \cdot v \in V$ denominado produto por escalar de α por v, de modo que:
(M1) $(\alpha\beta) \cdot v = \alpha \cdot (\beta \cdot v)$, para todo $\alpha,\beta \in \mathbb{R}$ e para todo $v \in V$ (propriedade associativa);
(M2) $1 \cdot v = v$, para todo $v \in V$ (1 é o elemento identidade de $\mathbb{R}$).

Além disso, as operações de Multiplicação e Adição podem se distribuir, gerando outras duas propriedades:
(D1) $\alpha \cdot (u+v) = \alpha \cdot u + \alpha \cdot v$, para todo $\alpha \in \mathbb{R}$ e para todo $u,v \in V$;
(D2) $(\alpha+\beta) \cdot v = \alpha \cdot v + \beta \cdot v$, para todo $\alpha,\beta \in \mathbb{R}$ e para todo $v \in V$.

Exemplo 3.1. *Seja o conjunto $\mathbb{R}^n = \{(v_1,v_2,...,v_n) | v_1,v_2,\cdots,v_n \in \mathbb{R}\}$ munido com a operação de adição dada por*

$$u+v = (u_1,...,u_n)+(v_1,...,v_n) = (u_1+v_1,...,u_n+v_n)$$

e com a operação de multiplicação de um vetor por escalar dada por

$$\alpha \cdot v = (\alpha v_1, ..., \alpha v_n).$$

Vamos verificar que o conjunto $\mathbb{R}^n$ é um espaço vetorial sobre $\mathbb{R}$.

Vamos iniciar provando as propriedades de (A1) a (A4). Sejam $u = (u_1, ..., u_n)$, $v = (v_1, ..., v_n)$ e $w = (w_1, ..., w_n)$ elementos de $\mathbb{R}^n$. Como $u_i, v_i, w_i \in \mathbb{R}$, para todo $i = 1, ..., n$, vale que $u_i + v_i = v_i + u_i$ e $(u_i + v_i) + w_i = u_i + (v_i + w_i)$, para todo $i = 1, ..., n$. Logo,

$$u + v = (u_1 + v_1, ..., u_n + v_n) = (v_1 + u_1, ..., v_n + u_n) = v + u,$$

provando (A1) e

$$\begin{aligned} (u+v)+w &= ((u_1+v_1)+w_1, ..., (u_n+v_n)+w_n) \\ &= (u_1+(v_1+w_1), ..., u_n+(v_n+w_n)) \\ &= u+(v+w), \end{aligned}$$

provando (A2).

Seja $v = (v_1, ..., v_n) \in \mathbb{R}^n$. Vamos encontrar um vetor $\bar{v} = (\bar{v}_1, ..., \bar{v}_n) \in \mathbb{R}^n$ tal que $v + \bar{v} = v$. Temos que

$$v + \bar{v} = v \Rightarrow (v_1, ..., v_n) + (\bar{v}_1, ..., \bar{v}_n) = (v_1, ..., v_n) \Rightarrow (v_1 + \bar{v}_1, ..., v_n + \bar{v}_n) = (v_1, ..., v_n).$$

Esta última igualdade é válida se, e somente se, $v_i + \bar{v}_i = v_i$, para todo $i = 1, ..., n$. Como esses elementos são números reais, segue que $\bar{v}_i = 0$, para todo $i = 1, ..., n$, e assim $\bar{v} = (0, ..., 0)$. Logo, segue (A3).

Seja $v = (v_1, ..., v_n) \in \mathbb{R}^n$. Como $v_i \in \mathbb{R}$, existe $-v_i \in \mathbb{R}$, tal que $v_i + (-v_i) = 0$, para todo $i = 1, ..., n$. Denotemos por $-v$ o vetor $-v = (-v_1, ..., -v_n)$. Portanto,

$$v + (-v) = (v_1 + (-v_1), ..., v_n + (-v_n)) = (0, ..., 0) = 0,$$

demonstrando (A4).

Vamos mostrar, a seguir, a validade das propriedades da multiplicação por escalar.

Sejam $\alpha, \beta \in \mathbb{R}$ e $v = (v_1, ..., v_n) \in \mathbb{R}^n$. Sendo $\alpha, \beta \in \mathbb{R}$ *e* $v_i \in \mathbb{R}$, para todo $i = 1, ..., n$, segue que $(\alpha\beta) \cdot v_i = \alpha(\beta \cdot v_i)$, para todo $i = 1, ..., n$, e assim

$$\begin{aligned}(\alpha \cdot \beta) \cdot v &= ((\alpha \cdot \beta) \cdot v_1, ..., (\alpha \cdot \beta) \cdot v_n) \\ &= (\alpha \cdot (\beta \cdot v_1), ..., \alpha \cdot (\beta \cdot v_n)) \\ &= \alpha \cdot (\beta \cdot v),\end{aligned}$$

provando (M1).

Para mostrar (M2), basta mostrar que $1v_i = v_i$, para todo $i = 1, ..., n$. Logo,

$$1 \cdot v = (1v_1, ..., 1v_n) = (v_1, ..., v_n) = v.$$

Para finalizar, a seguir demonstraremos que valem as propriedades (D1) e (D2).

Sejam $u = (u_1, ..., u_n)$, $v = (v_1, ..., v_n) \in \mathbb{R}^n$. Como $\alpha, u_i, v_i \in \mathbb{R}$, temos que $\alpha(u_i + v_i) = \alpha u_i + \alpha v_i$, para todo $i = 1, ..., n$, e assim

$$\begin{aligned}\alpha \cdot (u + v) &= (\alpha(u_1 + v_1), ..., \alpha(u_n + v_n)) \\ &= (\alpha u_1 + \alpha v_1, ..., \alpha u_n + \alpha v_n) \\ &= (\alpha u_1, ..., \alpha u_n) + (\alpha v_1, ..., \alpha v_n) \\ &= \alpha \cdot u + \alpha \cdot v.\end{aligned}$$

Seja $v = (v_1, ..., v_n) \in \mathbb{R}^n$ e $\alpha, \beta \in \mathbb{R}$. Sabendo que $(\alpha + \beta)v_i = \alpha v_i + \beta v_i$, para todo $i = 1, ..., n$, temos que

$$\begin{aligned}(\alpha + \beta) \cdot v &= ((\alpha + \beta)v_1, ..., (\alpha + \beta)v_n) \\ &= (\alpha v_1 + \beta v_1, ..., \alpha v_n + \beta v_n) \\ &= \alpha \cdot v + \beta \cdot v.\end{aligned}$$

Portanto, o conjunto $\mathbb{R}^n$ é um espaço vetorial sobre $\mathbb{R}$.

3.2 Base de um espaço vetorial

Definição 3.2. *Seja V um espaço vetorial sobre $\mathbb{R}$.*

1. Um vetor $v \in V$ é uma combinação linear dos vetores $v_1, \cdots, v_n \in V$ se existirem escalares

$\alpha_1, \cdots, \alpha_n \in \mathbb{R}$ tais que $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$.

2. Seja $\mathscr{B}$ um subconjunto de V. Dizemos que $\mathscr{B}$ é um conjunto gerador de V se todo elemento de V for uma combinação linear de um número finito de elementos de $\mathscr{B}$.

Exemplo 3.2. *Consideremos o espaço vetorial $\mathbb{R}^3$ sobre $\mathbb{R}$. Podemos observar que o conjunto $\{(1,0,0),(0,1,0),(0,0,1)\}$ é um conjunto gerador de $\mathbb{R}^3$, pois se $(x,y,z) \in \mathbb{R}^3$, então*

$$(x,y,z) = x(1,0,0) + y(0,1,0) + z(0,0,1), \text{ com } x,y,z \in \mathbb{R}.$$

Definição 3.3. *Sejam V um espaço vetorial sobre $\mathbb{R}$ e $\mathscr{B}$ um subconjunto de V.*

1. Dizemos que $\mathscr{B}$ é linearmente independente (l.i.) se $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$, para $v_i \in \mathscr{B}$ e $\alpha_i \in \mathbb{R}$, $i = 1, ..., n$, então $\alpha_1 = \cdots = \alpha_n = 0$.

2. O conjunto $\mathscr{B}$ é chamado linearmente dependente (l.d.) se não for linearmente independente.

Exemplo 3.3. *Considere o conjunto $\{(1,2),(4,3)\} \subset \mathbb{R}^2$. Vamos provar que este conjunto é linearmente independente.* Sendo $\alpha_1, \alpha_2 \in \mathbb{R}$, temos que

$$\alpha_1(1,2) + \alpha_2(4,3) = (\alpha_1, 2\alpha_1) + (4\alpha_2, 3\alpha_2) = (\alpha_1 + 4\alpha_2, 2\alpha_1 + 3\alpha_2) = (0,0).$$

Obtendo o sistema de equações

$$\left\{\begin{array}{r} \alpha_1 + 4\alpha_2 = 0 \\ 2\alpha_1 + 3\alpha_2 = 0 \end{array}\right. \Rightarrow \left\{\begin{array}{r} \alpha_1 = -4\alpha_2 \\ 2\alpha_1 + 3\alpha_2 = 0 \end{array}\right. ,$$

teremos

$$2(-4\alpha_2) + 3\alpha_2 = 0 \Rightarrow -8\alpha_2 + 3\alpha_2 = 0 \Rightarrow -5\alpha_2 = 0 \Rightarrow \alpha_2 = 0.$$

Logo, da primeira equação, segue que $\alpha_1 = 0$ e, portanto, mostrando o que queríamos.

Definição 3.4. *Seja V um espaço vetorial sobre $\mathbb{R}$. Dizemos que um subconjunto $\mathscr{B}$ de V é uma base de V se*

(I) $\mathscr{B}$ é um conjunto gerador de V e

(II) $\mathscr{B}$ é linearmente independente.

Exemplo 3.4. *Vamos provar que $\mathscr{B} = \{(1,0,0),(0,1,0),(0,0,1)\} \subset \mathbb{R}^3$ é uma base de $\mathbb{R}^3$.*

Mostramos no Exemplo 3.2 que $\mathscr{B}$ gera o $\mathbb{R}^3$. Resta-nos provar que $\mathscr{B}$ é linearmente independente. Sejam $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ tais que

$$\alpha_1(1,0,0) + \alpha_2(0,1,0) + \alpha_3(0,0,1) = (0,0,0).$$

É fácil notar que $\alpha_1 = \alpha_2 = \alpha_3 = 0$, provando assim que $\mathscr{B}$ é linearmente independente. Portanto, $\mathscr{B}$ é uma base de $\mathbb{R}^3$ e é conhecida como *base canônica* de $\mathbb{R}^3$.

3.3 Subespaço vetorial

Definição 3.5. *Seja V um espaço vetorial sobre $\mathbb{R}$. Um subconjunto W de V é um subespaço vetorial de V se a restrição das operações de V a W torna esse conjunto um espaço vetorial sobre $\mathbb{R}$.*

Proposição 3.1. *Sejam V um espaço vetorial sobre $\mathbb{R}$ e $W \subseteq V$ um subconjunto. São equivalentes as seguintes afirmações:*
(a) W é um subespaço vetorial de V sobre $\mathbb{R}$.
(b) (I) $0 \in W$;
(II) se $v_1, v_2 \in W$, então $v_1 + v_2 \in W$.
(III) se $\lambda \in \mathbb{R}$ e $v \in W$, então $\lambda \cdot v \in W$.

Demonstração. Seja W um subespaço vetorial de V sobre $\mathbb{R}$. Vamos provar a afirmação (b).

Sejam $v_1, v_2 \in W$. Como W é subespaço vetorial sobre $\mathbb{R}$, segue que $v_1 + v_2 \in W$ e, também, vale a propriedade (A1), ou seja, existe $0 \in W$ tal que $v + 0 = v$, para todo $v \in W$. Logo, provamos (I) e (II).

Seja $\lambda \in \mathbb{R}$ e $v \in W$. Como W é um espaço vetorial sobre $\mathbb{R}$, segue que $\lambda \cdot v \in W$, e assim mostramos (III).

Vamos provar agora a recíproca. Seja W um subconjunto de V cujos elementos satisfazem (I), (II) e (III). Note que, de (II) e (III), as propriedades do fechamento da Adição e Multiplicação são satisfeitas; de (I) segue a propriedade (A3). Como W é um subconjunto de V, temos que todo elemento $v \in W$ é um elemento $v \in V$. Assim seguem as propriedades (A1), (A2), (A4), (M1), (M2), (D1) e (D2) mostrando o que queríamos.■

Definição 3.6. *Sejam W_1 e W_2 subespaços vetoriais de um espaço vetorial V sobre $\mathbb{R}$. A soma dos subespaços W_1 e W_2 é dada por*

$$W_1 + W_2 = \{v \in V | v = w_1 + w_2, w_1 \in W_1 \text{ e } w_2 \in W_2\}.$$

Definição 3.7. *Sejam W_1 e W_2 subespaços vetoriais de um espaço vetorial V sobre $\mathbb{R}$. Dizemos que a soma $W_1 + W_2$ é direta se $W_1 \cap W_2 = \{0\}$ e, neste caso, escrevemos $W_1 \oplus W_2$.*

Exemplo 3.5. *Sejam W_1 e W_2 subespaços de $\mathbb{C}^4$ sobre $\mathbb{R}$ com as bases $\{(1,2,0,i),(i,0,0,1)\}$ e $\{(0,0,3,1)\}$, respectivamente. Vamos provar que a soma de W_1 e W_2 é direta.*

Em primeiro lugar, mostraremos que $W_1 \cap W_2 = \{(0,0,0,0)\}$.

Como W_1 e W_2 são subespaços de $\mathbb{C}^4$, temos que $(0,0,0,0) \in W_1$ e $(0,0,0,0) \in W_2$. Logo, $(0,0,0,0) \in W_1 \cap W_2$, e assim $\{(0,0,0,0)\} \subset W_1 \cap W_2$.

Agora, vamos provar que $W_1 \cap W_2 \subset \{(0,0,0,0)\}$.

Seja $(x,y,z,w) \subset W_1 \cap W_2$. Como $(x,y,z,w) \in W_1$ e $\{(1,2,0,i),(i,0,0,1)\}$ é uma base de W_1 sobre $\mathbb{R}$, existem $\alpha, \beta \in \mathbb{R}$ tais que

$$(x,y,z,w) = \alpha(1,2,0,i) + \beta(i,0,0,1);$$

Como $(x,y,z,w) \in W_2$ e $\{(0,0,3,1)\}$ é uma base de W_2 sobre $\mathbb{R}$, existe $\lambda \in \mathbb{R}$ tal que

$$(x,y,z,w) = \lambda(0,0,3,1).$$

Logo:

$$\alpha(1,2,0,i) + \beta(i,0,0,1) = \lambda(0,0,3,1)$$

ou seja,

$$(\alpha + \beta i, 2\alpha, -3\lambda, \alpha i + \beta - \lambda) = (0,0,0,0),$$

e assim $\alpha = \beta = \lambda = 0$. Portanto, $(x,y,z,w) = (0,0,0,0)$, provando o que queríamos.

Definição 3.8. *Seja V um espaço vetorial sobre $\mathbb{R}$ e sejam W_1 e W_2 subespaços de V. Dizemos que V é a soma direta de W_1 e W_2 se $V = W_1 \oplus W_2$.*

Exemplo 3.6. *Seja $W_1 = \mathbb{R}$, sendo $\mathbb{R}$ gerado por $\{(1,0)\}$ e seja $W_2 = \mathbb{R}$, neste caso gerado por $\{(1,1)\}$. Mostraremos que $\mathbb{R}^2 = W_1 \oplus W_2$.*

Antes de mais nada, iremos provar que, se $(a,b) \in \mathbb{R}^2$, então

$$(a,b) = \alpha w_1 + \beta w_2$$

sendo $w_1 \in W_1$, $w_2 \in W_2$ e $\alpha, \beta \in \mathbb{R}$, ou seja, $(a,b) = \alpha(1,0) + \beta(1,1)$. Fazendo os cálculos, obtemos $\alpha = a - b$ e $\beta = b$. Logo,

$$(a,b) = (a-b) \cdot (1,0) + b \cdot (1,1).$$

Agora, provaremos que $W_1 \cap W_2 = \{(0,0)\}$.

Como W_1 e W_2 são subespaços de $\mathbb{R}^2$, temos que $(0,0) \in W_1$ e $(0,0) \in W_2$, e assim $(0,0) \in W_1 \cap W_2$. Portanto, $\{(0,0)\} \subset W_1 \cap W_2$.

Seja $(a,b) \in W_1 \cap W_2$. Então, $(a,b) \in W_1$ e $(a,b) \in W_2$, e assim existem $\lambda_1, \lambda_2 \in \mathbb{R}$ tais que $(a,b) = \lambda_1 \cdot (1,0) = (\lambda_1, 0)$ e $(a,b) = \lambda_2 \cdot (1,1) = (\lambda_2, \lambda_2)$. Logo, $(a,b) = (\lambda_1, 0) = (\lambda_2, \lambda_2)$, seguindo que $\lambda_1 = \lambda_2 = 0$. Portanto, $(a,b) = (0,0)$, provando que $W_1 \cap W_2 \subset \{(0,0)\}$.

Proposição 3.2. *Seja V um espaço vetorial sobre $\mathbb{R}$ e sejam W_1 e W_2 dois subespaços de V. São equivalentes as afirmações:*

(a) $V = W_1 \oplus W_2$.

(b) cada elemento $v \in V$ se escreve de maneira única como uma soma $w_1 + w_2$ com $w_1 \in W_1$ e $w_2 \in W_2$.

Demonstração. Vamos supor que $V = W_1 \oplus W_2$. Segue então que cada elemento de $v \in V$ se escreve como a soma de um elemento de W_1 e um elemento de W_2. Suponhamos agora que $v = x_1 + x_2 = y_1 + y_2$ com $x_1, y_1 \in W_1$ e $x_2, y_2 \in W_2$. Daí segue que $x_1 - y_1 = y_2 - x_2$, sendo $x_1 - y_1 \in W_1$ e $y_2 - x_2 \in W_2$, pois W_1 e W_2 são subespaços de V. Logo, $x_1 - y_1 \in W_1 \cap W_2 = \{0\}$ e $y_2 - x_2 \in W_1 \cap W_2 = \{0\}$. Logo, $x_1 = y_1$ e $x_2 = y_2$, provando que (a) implica (b).

De (b) temos que cada elemento de V pode ser escrito como uma soma de elementos de W_1 e W_2, logo $V = W_1 + W_2$. Agora suponhamos que $W_1 \cap W_2 \neq \{0\}$, ou seja, que exista $w \in W_1 \cap W_2$ sendo $w \neq 0$. Então existe $w_1 \in W_1$, $w_1 \neq 0$, tal que $w = w_1 + 0$; existe $w_2 \in W_2$, $w_2 \neq 0$, tal que $w = 0 + w_2$. Dessa forma, podemos escrever w de duas maneiras distintas, mas isso contradiz a nossa hipótese de unicidade. Logo $W_1 \cap W_2 = \{0\}$ mostrando que (b) implica (a). ■

3.4 Transformações lineares

Definição 3.9. *Sejam U e V espaços vetoriais sobre $\mathbb{R}$. Uma função $T : U \to V$ é uma transformação linear se são verdadeiras as afirmações:*

(I) $T(u_1 + u_2) = T(u_1) + T(u_2)$, para todo $u_1, u_2 \in U$.

(II) $T(\lambda u) = \lambda T(u)$, para todo $\lambda \in \mathbb{R}$ e todo $u \in U$.

Proposição 3.3. *Sejam U e V espaços vetoriais sobre $\mathbb{R}$. São equivalentes as seguintes afirmações:*

(a) $T : U \to V$ é linear.

(b) $T(\lambda_1 u_1 + \lambda_2 u_2) = \lambda_1 T(u_1) + \lambda_2 T(u_2)$, para todo $u_1, u_2 \in U$ e para todo $\lambda_1, \lambda_2 \in \mathbb{R}$.

Proposição 3.4. *Sejam U e V espaços vetoriais sobre $\mathbb{R}$ e $T : U \to V$ uma transformação linear. São verdadeiras as seguintes afirmações:*

(i) $T(0_U) = 0_V$, 0_U, 0_V são os vetores nulos de U e V, respectivamente.

(ii) $T(-u) = -T(u)$, para cada $u \in U$.

(iii) $T(\alpha_1 u_1 + \cdots + \alpha_n u_n) = \alpha_1 T(u_1) + \cdots + \alpha_n T(u_n)$, para todo $u_1, \ldots, u_n \in U$ e $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$.

Exemplo 3.7. *Considere os espaços vetoriais $\mathbb{R}^2$ e $\mathbb{R}^3$ sobre $\mathbb{R}$ e seja $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ definida por $T(x,y,z) = (2x, 3y-z)$. Vamos verificar que T é uma transformação linear.*

Sejam $u = (x_1, y_1, z_1), v = (x_2, y_2, z_2) \in \mathbb{R}^3$ e $\lambda_1, \lambda_2 \in \mathbb{R}$. Então

$$\begin{aligned}
T(\lambda_1 u + \lambda_2 v) &= T(\lambda_1 x_1 + \lambda_2 x_2, \lambda_1 y_1 + \lambda_2 y_2, \lambda_1 z_1 + \lambda_2 z_2) \\
&= (2(\lambda_1 x_1 + \lambda_2 x_2), 3(\lambda_1 y_1 + \lambda_2 y_2) - (\lambda_1 z_1 + \lambda_2 z_2)) \\
&= (\lambda_1(2x_1) + \lambda_2(2x_2), \lambda_1(3y_1 - z_1) + \lambda_2(3y_2 - z_2)) \\
&= (\lambda_1(2x_1), \lambda_1(3y_1 - z_1)) + (\lambda_2(2x_2), \lambda_2(3y_2 - z_2)) \\
&= \lambda_1(2x_1, 3y_1 - z_1) + \lambda_2(2x_2, 3y_2 - z_2) \\
&= \lambda_1 T(x_1, y_1, z_1) + \lambda_2 T(x_2, y_2, z_2) \\
&= \lambda_1 T(u) + \lambda_2 T(v).
\end{aligned}$$

Logo, pela Proposição 3.3, temos que T é linear.

Definição 3.10. *Sejam U e V espaços vetoriais sobre $\mathbb{R}$ e considere $\mathscr{B} = \{u_1, u_2, ..., u_n\}$ uma base de U e $\mathscr{C} = \{v_1, v_2, ..., v_m\}$ uma base de V. Seja $T : U \to V$ uma transformação linear. Os elementos $T(u_1), T(u_2), ..., T(u_n) \in V$ e, desse modo, podemos escrever*

$$\begin{aligned}
T(u_1) &= \alpha_{11} \cdot v_1 + \alpha_{21} \cdot v_2 + ... + \alpha_{m1} \cdot v_m \\
T(u_2) &= \alpha_{12} \cdot v_1 + \alpha_{22} \cdot v_2 + ... + \alpha_{m2} \cdot v_m \\
&\vdots \\
T(u_n) &= \alpha_{1n} \cdot v_1 + \alpha_{2n} \cdot v_2 + ... + \alpha_{mn} \cdot v_m.
\end{aligned}$$

Desse modo, a matriz de T é dada por

$$[T] = \begin{bmatrix} \alpha_{11} & \alpha_{12} & ... & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & ... & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{m1} & \alpha_{m2} & ... & \alpha_{mn}. \end{bmatrix}.$$

Proposição 3.5. *Seja U um espaço vetorial sobre $\mathbb{R}$ e considere $\mathscr{B} = \{u_1, ..., u_n\}$ uma base de U. Sejam $S, T : U \to U$ transformações lineares tais que $T(U) \subset U$. Então, $S \circ T$ é linear e a matriz de $S \circ T$, na base $\mathscr{B}$, é*

$$[S \circ T] = [S] \cdot [T].$$

3.5 Espaços vetoriais com produto interno

Definição 3.11. *Seja V um espaço vetorial sobre $\mathbb{R}$. Um produto interno em V é uma aplicação $\langle \cdot, \cdot \rangle : V \times V \longrightarrow \mathbb{R}$ que, a cada par $(u,v) \in V \times V$, associa um número real $\langle u,v \rangle$, e para todo $u,v,w \in V$ e para todo $\lambda \in \mathbb{R}$, satisfaz as seguintes propriedades:*

(I) $\cdot$ $\langle u+v, w\rangle = \langle u,w\rangle + \langle v,w\rangle$

$\cdot$ $\langle u, w+v\rangle = \langle u,w\rangle + \langle u,v\rangle$ *(distributiva);*

(II) $\langle u,v\rangle = \langle v,u\rangle$ *(simetria);*

(III) $\langle u,u\rangle \geq 0$ *e* $\langle u,u\rangle = 0$ *se, e somente se,* $u = 0_v$ *(positividade);*

(IV) $\cdot$ $\langle \lambda u, v\rangle = \lambda \langle u,v\rangle$

$\cdot$ $\langle u, \lambda v\rangle = \lambda \langle u,v\rangle$ *(homogeneidade).*

Exemplo 3.8. *Seja $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$ a função dada por*

$$\langle u,v\rangle = u_1v_1 + u_2v_2 + ... + u_nv_n$$

sendo $u = (u_1,u_2,...,u_n)$ e $v = (v_1,v_2,...,v_n)$. Mostraremos que esta função é um produto interno em $\mathbb{R}^n$.

De fato, sejam $u = (u_1,u_2,...,u_n), v = (v_1,v_2,...,v_n)$ e $w = (w_1,...,w_n)$ elementos de $\mathbb{R}^n$. Como $u_i, v_i, w_i \in \mathbb{R}$, para todo $i = 1,2,...,n$, as propriedades (I) e (II) seguem do fato de que, em $\mathbb{R}$, valem as propriedades distributiva e associativa (da soma e do produto).

Notemos que

$$\langle u,u\rangle = u_1^2 + u_2^2 + ... + u_n^2 \geq 0,$$

pois é uma soma formada apenas por elementos maiores ou iguais a zero. Logo,

$$\langle u,u\rangle = u_1^2 + u_2^2 + ... + u_n^2 = 0,$$

se, e somente se, $u_1 = u_2 = ... = u_n = 0$, provando (III).

Para finalizar, seja $\lambda \in \mathbb{R}$. Como $u_i, v_i \in \mathbb{R}$, para todo $i = 1, 2, ..., n$, e valem as propriedades associativa e distributiva do produto em relação a adição em $\mathbb{R}$, temos que

$$\begin{aligned} \langle \lambda u, v \rangle &= (\lambda u_1)v_1 + (\lambda u_2)v_2 + ... + (\lambda u_n)v_n \\ &= \lambda(u_1v_1) + \lambda(u_2v_2) + ... + \lambda(u_nv_n) \\ &= \lambda(u_1v_1 + u_2v_2 + ... + u_nv_n) \\ &= \lambda\langle u, v \rangle \end{aligned}$$

e

$$\begin{aligned} \langle u, \lambda v \rangle &= u_1(\lambda v_1) + u_2(\lambda v_2) + ... + u_n(\lambda v_n) \\ &= \lambda(u_1v_1) + \lambda(u_2v_2) + ... + \lambda(u_nv_n) \\ &= \lambda(u_1v_1 + u_2v_2 + ... + u_nv_n) \\ &= \lambda\langle u, v \rangle, \end{aligned}$$

mostrando o que queríamos.

Da propriedade (III) da Definição 3.11 temos que $\langle u, u \rangle \geq 0$. Logo, faz sentido definir a norma.

Definição 3.12. *Seja V um espaço vetorial sobre $\mathbb{R}$ e seja $\langle \cdot, \cdot \rangle$ um produto interno em V. Definimos a norma de u, denotada por $\|u\|$, por $\|u\| = \sqrt{\langle u, u \rangle}$.*

Notemos que $\|u\| \geq 0$, e $\|u\| = 0$ se, e somente se $u = 0$; $\|u\|^2 = \langle u, u \rangle$ e $\|\lambda u\| = |\lambda| \cdot \|u\|$.

Lema 3.1. *Seja V um espaço vetorial sobre $\mathbb{R}$ e sejam $u, v \in V$ tais que $\|u\| = \|v\| = 1$, então $|\langle u, v \rangle| \leq 1$.*

Demonstração. Sejam $u, v \in V$ tais que $\|u\| = \|v\| = 1$. Vamos provar que $\langle u, v \rangle \leq 1$ e $\langle u, v \rangle \geq -1$ (pois $|\langle u, v \rangle| \leq 1$ é equivalente a $-1 \leq \langle u, v \rangle \leq 1$).

Da propriedade (III) da Definição 3.11 temos que $\langle u-v, u-v\rangle \geq 0$ e $\langle u+v, u+v\rangle \geq 0$. Notemos que

$$\begin{aligned}
0 \leq \langle u-v, u-v\rangle &= \langle u,u\rangle - \langle u,v\rangle - \langle v,u\rangle + \langle v,v\rangle \\
&= \langle u,u\rangle - \langle u,v\rangle - \langle u,v\rangle + \langle v,v\rangle \\
&= \|u\|^2 - 2\langle u,v\rangle + \|v\|^2 \\
&= 2 - 2\langle u,v\rangle,
\end{aligned}$$

e assim $\langle u,v\rangle \leq 1$; e que

$$\begin{aligned}
0 \leq \langle u+v, u+v\rangle &= \langle u,u\rangle + \langle u,v\rangle + \langle v,u\rangle + \langle v,v\rangle \\
&= \langle u,u\rangle + \langle u,v\rangle + \langle u,v\rangle + \langle v,v\rangle \\
&= \|u\|^2 + 2\langle u,v\rangle + \|v\|^2 \\
&= 2 + 2\langle u,v\rangle,
\end{aligned}$$

e assim $\langle u,v\rangle \geq -1$, seguindo o que queríamos demonstrar. ■

Teorema 3.1 (Desigualdade de Cauchy-Schwarz)**.** *Seja V um espaço vetorial sobre $\mathbb{R}$ e seja $\langle \cdot,\cdot\rangle$ um produto interno em V. Para todo $u,v \in V$ tem-se*

$$|\langle u,v\rangle| \leq \|u\|\|v\|.$$

Demonstração. Sejam $u,v \in V$. Se $u=0$ ou $v=0$, a desigualdade estará provada. Suponhamos, então, $u \neq 0$ e $v \neq 0$, e consideremos $\bar{u} = \dfrac{1}{\|u\|}\cdot u$ e $\bar{v} = \dfrac{1}{\|v\|}\cdot v$. Notemos que $\bar{u},\bar{v} \in V$ e $\|\bar{u}\| = \|\bar{v}\| = 1$. Logo, pelo Lema 3.1, temos que $|\langle \bar{u},\bar{v}\rangle| \leq 1$, ou seja,

$$\begin{aligned}
|\langle \bar{u},\bar{v}\rangle| &= \left|\left\langle \frac{1}{\|u\|}\cdot u, \frac{1}{\|v\|}\cdot v\right\rangle\right| \\
&= \left|\frac{1}{\|u\|}\left\langle u, \frac{1}{\|v\|}\cdot v\right\rangle\right| \\
&= \left|\frac{1}{\|u\|\|v\|}\langle u,v\rangle\right| \\
&= \frac{1}{\|u\|\|v\|}|\langle u,v\rangle| \leq 1.
\end{aligned}$$

Portanto, $|\langle u,v\rangle| \leq \|u\|\|v\|$. ■

Corolário 3.1 (Desigualdade triangular)**.** *Seja V um espaço vetorial sobre* $\mathbb{R}$*. Para todo* $u, v \in V$ *tem-se* $\|u+v\| \leq \|u\| + \|v\|$.

Demonstração. Para demonstrar essa desigualdade, iremos provar que

$$\|u+v\|^2 \leq (\|u\| + \|v\|)^2$$

pois, ao extrair a raiz quadrada dos dois lados, obteremos a desigualdade desejada. Temos que

$$\begin{aligned}
\|u+v\|^2 &= \langle u+v, u+v\rangle \\
&= \langle u,u\rangle + \langle u,v\rangle + \langle v,u\rangle + \langle v,v\rangle \\
&= \langle u,u\rangle + \langle u,v\rangle + \langle u,v\rangle + \langle v,v\rangle \\
&= \|u\|^2 + 2\langle u,v\rangle + \|v\|^2.
\end{aligned}$$

Pela desigualdade de Cauchy-Schwarz, temos que $|\langle u,v\rangle| \leq \|u\|\|v\|$. Como $\langle u,v\rangle \leq |\langle u,v\rangle|$ segue que

$$\begin{aligned}
\|u+v\|^2 &\leq \|u\|^2 + 2\|u\|\|v\| + \|v\|^2 \\
&= (\|u\| + \|v\|)^2,
\end{aligned}$$

e, portanto, $\|u+v\| \leq \|u\| + \|v\|$. ∎

3.6 Bases ortonormais

Definição 3.13. *Seja V um espaço vetorial sobre* $\mathbb{R}$ *e seja* $\langle\cdot,\cdot\rangle$ *um produto interno em V. A medida* θ *do ângulo entre dois vetores não-nulos* $u, v \in V$*,* $0 \leq \theta \leq \pi$*, é dada por* $\cos(\theta) = \dfrac{\langle u,v\rangle}{\|u\|\|v\|}$.

Definição 3.14. *Seja V um espaço vetorial sobre* $\mathbb{R}$ *e seja* $\langle\cdot,\cdot\rangle$ *um produto interno em V. Dizemos que* $u, v \in V$ *são ortogonais se* $\langle u,v\rangle = 0$.

Definição 3.15. *Seja V um espaço vetorial de dimensão n sobre* $\mathbb{R}$ *e seja* $\langle\cdot,\cdot\rangle$ *um produto interno em V. Dizemos que uma base* $\mathscr{B} = \{u_1, \ldots, u_n\}$ *de V é ortonormal se são verdadeiras as seguintes afirmações:*

(i) $\|u_k\| = 1$*, para todo* $k = 1, \ldots, n$.

(ii) $\langle u_j, u_k\rangle = 0, k \neq j,\ j,k = 1, \ldots, n$.

Apresentaremos, a seguir, o processo de ortogonalização de Gram-Schmidt e nele aparece uma notação que iremos explicar o seu significado.

A notação $S[z_1,...,z_s]$ significa que S é gerado pelo conjunto $\{z_1,...,z_s\}$.

Teorema 3.2 (Gram-Schmidt)**.** *Seja V um espaço vetorial de dimensão n sobre $\mathbb{R}$ e seja $\langle\cdot,\cdot\rangle$ um produto interno em V. Seja $\{w_1,...,w_n\}$ uma base de V e suponhamos que $\{u_1,...,u_r\}$ seja uma base ortonormal do subespaço $S[w_1,...,w_r]$ de V. Definindo*

$$u_{r+1} = \frac{w}{\|w\|},$$

onde

$$w = w_{r+1} - \sum_{k=1}^{r} \langle w_{r+1}, u_k\rangle \cdot u_k$$

Então, $\{u_1,...,u_r,u_{r+1}\}$ é uma base ortonormal de $S[w_1,...,w_{r+1}]$.

Demonstração. Precisamos mostrar que

(a) $S[w_1,...,w_r,w_{r+1}] = S[u_1,...,u_r,u_{r+1}]$;

(b) $\{u_1,...,u_r,u_{r+1}\}$ é linearmente independente;

(c) $\|u_j\| = 1$, para todo $j = 1,...,r,r+1$ e

(d) $\langle u_j,u_k\rangle = 0$, para todo $k \neq j$, $j,k = 1,...,r+1$.

Sabemos que $\{u_1,...,u_r\}$ é uma base de $S[w_1,...,w_r]$. Logo, $\{u_1,...,u_r\}$ gera $S[w_1,...,w_r]$. Além disso, como

$$u_{r+1} = w_{r+1} - \sum_{k=1}^{r} \langle w_{r+1}, u_k\rangle u_k$$

temos que $\{u_1,...,u_r,u_{r+1}\}$ gera $S[w_1,...,w_r,w_{r+1}]$, provando (a).

A seguir, provaremos (b).

A afirmação (b) segue do fato de que $\{u_1,...,u_{r+1}\}$ está contido em V e $\{w_1,...,w_n\}$ é uma base de V.

Pelo fato de $\{u_1,...,u_r\}$ ser ortonormal, temos que $\|u_k\| = 1$, para todo $k = 1,...,r$. Sabendo que

$$u_{r+1} = \frac{w}{\|w\|},$$

segue que $\|u_{r+1}\| = 1$, e assim segue (c).

Por fim, provaremos (d).

É sabido que $\{u_1,...,u_r\}$ é ortonormal. Logo, $\langle u_j,u_k\rangle = 0$, para todo $j \neq k$, $j,k = 1,...,r$. Desse modo, basta verificarmos que $\langle u_j,u_{r+1}\rangle = 0$, para todo $j = 1,...,r$, ou seja, $\langle u_j,w\rangle = 0$, para todo $j = 1,...,r$. Temos que

$$\begin{aligned}\langle u_j,w\rangle &= \langle u_j,w_{r+1}\rangle - \sum_{k=1}^{r}\langle w_{r+1},u_k\rangle u_k \\ &= \langle u_j,w_{r+1}\rangle - \sum_{k=1}^{r}\langle w_{r+1},u_k\rangle\langle u_j,u_k\rangle.\end{aligned}$$

Notemos que

$$\begin{aligned}\sum_{k=1}^{r}\langle w_{r+1},u_k\rangle\langle u_j,u_k\rangle &= \langle w_{r+1},u_1\rangle\langle u_j,u_1\rangle + \langle w_{r+1},u_2\rangle\langle u_j,u_2\rangle + ... + \langle w_{r+1},u_r\rangle\langle u_j,u_r\rangle \\ &= \langle w_{r+1},u_j\rangle,\end{aligned}$$

para todo $j = 1,...,r$, pois $\langle u_j,u_k\rangle = 0$, para todo $j \neq k$, $j,k = 1,...,r$, e $\langle u_j,u_j\rangle = \|u_j\|^2 = 1$, para todo $j = 1,...,r$. Portanto,

$$\langle u_j,w\rangle = \langle u_j,w_{r+1}\rangle - \langle u_j,w_{r+1}\rangle = 0$$

para todo $j = 1,...,r$, demonstrando o que queríamos. ■

Exemplo 3.9. *Considere um subespaço S do* $\mathbb{R}^4$ *gerado pelo conjunto* $\{(1,1,1,0),(-1,1,2,1)\}$. *Vamos determinar uma base ortonormal desse subespaço utilizando o processo de Gram-Schmidt.*

Antes de mais nada, notemos que $\{(1,1,1,0),(-1,1,2,1)\}$ é linearmente independente. Como este conjunto é l.i. e gera o subespaço S de $\mathbb{R}^4$, temos que $\{(1,1,1,0),(-1,1,2,1)\}$ é uma base de S e, portanto, a dimensão de S sobre $\mathbb{R}$ é igual a 2. Denotemos $u_1 = (1,1,1,0)$ e $u_2 = (-1,1,2,1)$.

Seja $\{u_1,\bar{u_2}\}$ uma base de S. Façamos

$$\bar{u_2} = u_2 - \frac{\langle u_1,u_2\rangle}{\|u_1\|^2}\cdot u_1.$$

Sabendo que $\langle u_1,u_2\rangle = 2$ e $\|u_1\|^2 = 3$, segue que

$$\bar{u_2} = \left(-\frac{5}{3},\frac{1}{3},\frac{4}{3},1\right).$$

Por construção, $\langle u_1,\bar{u_2}\rangle = 0$, então $\left\{\frac{u_1}{\|u_1\|},\frac{\bar{u_2}}{\|\bar{u_2}\|}\right\}$ é uma base ortonormal de S.

3.7 Transformações Ortogonais

Definição 3.16. *Seja V um espaço vetorial sobre $\mathbb{R}$ munido de um produto interno $\langle \cdot, \cdot \rangle$ e seja $\|\cdot\|$ a norma proveniente desse produto interno. Uma transformação linear $T : V \to V$ é chamada transformação ortogonal se T preserva as distâncias, ou seja, $\|T(v)\| = \|v\|$, para todo $v \in V$.*

Definição 3.17. *Uma matriz A $n \times n$ é dita ortogonal se $A \cdot A^t = I_n$, sendo A^t a matriz transposta de A e I_n a matriz identidade de ordem n.*

Teorema 3.3. *Seja V um espaço vetorial de dimensão n sobre $\mathbb{R}$ e seja $\langle \cdot, \cdot \rangle$ um produto interno em V. Considere $T : V \to V$ uma transformação linear. São equivalentes as seguintes afirmações:*
(a) T é uma transformação ortogonal.
(b) $\langle T(u), T(v) \rangle = \langle u, v \rangle$, para todo $u, v \in V$.

Demonstração. Inicialmente, vamos mostrar que (a) implica (b).

Sejam $u, v \in V$. Como T é ortogonal, temos que

$$\|T(u+v)\| = \|u+v\|,$$

isto é,

$$\|T(u+v)\|^2 = \|u+v\|^2.$$

Notemos que

$$\begin{aligned}
\|T(u+v)\|^2 = \langle T(u+v), T(u+v) \rangle &= \langle T(u) + T(v) \rangle, T(u) + T(v) \rangle \\
&= \langle T(u), T(u) \rangle + \langle T(v), T(u) \rangle + \langle T(u), T(v) \rangle + \langle T(v), T(v) \rangle \\
&= \|T(u)\|^2 + \langle T(u), T(v) \rangle + \langle T(u), T(v) \rangle + \|T(v)\|^2 \\
&= \|T(u)\|^2 + 2\langle T(u), T(v) \rangle + \|T(v)\|^2.
\end{aligned}$$

Como, $\|T(u)\| = \|u\|$ e $\|T(v)\| = \|v\|$, segue que

$$\|T(u+v)\|^2 = \|u\|^2 + 2\langle T(u), T(v) \rangle + \|v\|^2.$$

Por outro lado:

$$\begin{aligned} \|u+v\|^2 &= \langle u+v, u+v\rangle \\ &= \langle u,u\rangle + \langle v,u\rangle + \langle u,v\rangle + \langle v,v\rangle \\ &= \|u\|^2 + \langle v,u\rangle + \langle u,v\rangle + \|v\|^2 \\ &= \|u\|^2 + 2\langle u,v\rangle + \|v\|^2. \end{aligned}$$

De $\|T(u+v)\|^2 = \|u+v\|^2$ segue que $\langle T(u), T(v)\rangle = \langle u,v\rangle$, provando (b).

Reciprocamente, seja $v \in V$. Iremos provar que $\|T(v)\| = \|v\|$. Para isso, basta provar que $\|T(v)\|^2 = \|v\|^2$, mas essa afirmação segue diretamente de (b), pois

$$\|T(v)\|^2 = \langle T(v), T(v)\rangle = \langle v,v\rangle = \|v\|^2,$$

demonstrando o que queríamos. ■

3.8 Complemento ortogonal

Definição 3.18. *Seja V um espaço vetorial sobre $\mathbb{R}$ munido de um produto interno $\langle\cdot,\cdot\rangle$. Seja S um subconjunto de V não-vazio. Definimos o complemento ortogonal de S em V como sendo o conjunto*

$$S^\perp = \{v \in V \,|\, \langle v,s\rangle = 0, \textit{ para todo } s \in S\}.$$

Lema 3.2. *Seja V um espaço vetorial sobre $\mathbb{R}$ munido de um produto interno $\langle\cdot,\cdot\rangle$. Seja S um subconjunto não-vazio de V. Então $S^\perp$ é um subespaço vetorial de V.*

Demonstração. Pela Proposição 3.1., precisamos mostrar que
(i) $0 \in S^\perp$;
(ii) se $v_1, v_2 \in S^\perp$, então $v_1 + v_2 \in S^\perp$ e
(iii) se $\lambda \in \mathbb{R}$ e $v \in S^\perp$, então $\lambda \cdot v \in S^\perp$.

É válido que $0 \cdot v = 0$, para todo $v \in V$. Dessa forma, para todo $v \in V$ e para todo $s \in S$,

$$\langle 0, s\rangle = \langle 0 \cdot v, s\rangle = 0\langle v,s\rangle = 0,$$

isto é, $0 \in S^\perp$.

Sejam $v_1, v_2 \in S^\perp$. Então $\langle v_1, s\rangle = 0$ e $\langle v_2, s\rangle = 0$, para todo $s \in S$. Logo,

$$\langle v_1 + v_2, s\rangle = \langle v_1, s\rangle + \langle v_2, s\rangle = 0,$$

para todo $s \in S$, isto é, $v_1 + v_2 \in S^{\perp}$, provando (ii).

Sejam $\lambda \in \mathbb{R}$, $v \in S^{\perp}$. Então, para todo $s \in S$, $\langle v, s\rangle = 0$. Desse modo,

$$\langle \lambda v, s\rangle = \lambda \langle v, s\rangle = \lambda \cdot 0 = 0,$$

provando que $\lambda v \in S^{\perp}$. ■

Teorema 3.4. *Seja V um espaço vetorial sobre $\mathbb{R}$ munido de um produto interno $\langle \cdot, \cdot \rangle$ e seja S um subespaço de dimensão finita de V. Então, $V = S \oplus S^{\perp}$.*

Demonstração. Em primeiro lugar, vamos mostrar que $V = S + S^{\perp}$, isto é, todo elemento de $v \in V$ é uma soma de um elemento de S com um elemento de $S^{\perp}$.

Sabendo que S tem dimensão finita, seja $\mathscr{B} = \{s_1, ..., s_n\}$ uma base ortonormal de S. Seja $v \in V$ qualquer e considere

$$\begin{aligned}\bar{s} &= \sum_{i=1}^{n} \langle v, s_i\rangle \cdot s_i \\ &= \langle v, s_1\rangle \cdot s_1 + ... + \langle v, s_n\rangle \cdot s_n.\end{aligned}$$

Note que $\bar{s} \in S$, pois $\langle v, s_i\rangle \in \mathbb{R}$ e $s_i \in S$, para todo $i = 1, ..., n$, e S é subespaço vetorial de V.

Vamos verificar que $v - \bar{s} \in S^{\perp}$. Para isso, devemos mostrar que $\langle v - \bar{s}, s\rangle = 0$, para todo $s \in S$.

Seja $s \in S$ qualquer. Então, existem $\lambda_1, ..., \lambda_n \in \mathbb{R}$ tais que

$$s = \lambda_1 s_1 + ... + \lambda_n s_n.$$

Logo, bastará provar que $\langle v - \bar{s}, s_j\rangle = 0$, para todo $j = 1, ..., n$.

Seja $j_0 \in \{1, ..., n\}$. Como $\mathscr{B}$ é uma base ortonormal, temos que $\langle s_i, s_j\rangle = 0$, para $i \neq j$, $i, j = 1, ..., n$, e $\langle s_{j_0}, s_{j_0}\rangle = 1$. Dessa forma,

$$\begin{aligned}\langle v - \bar{s}, s_{j_0}\rangle &= \langle v, s_{j_0}\rangle - \langle \bar{s}, s_{j_0}\rangle \\ &= \langle v, s_{j_0}\rangle - \sum_{i=1}^{n} \langle v, s_i\rangle \langle s_i, s_{j_0}\rangle \\ &= \langle v, s_{j_0}\rangle - \langle v, s_{j_0}\rangle = 0.\end{aligned}$$

Portanto, $v-\bar{s}\in S^{\perp}$, e assim $v=\bar{s}+(v-\bar{s})$ com $\bar{s}\in S$ e $v-\bar{s}\in S^{\perp}$.

Verificaremos, agora, que $S\cap S^{\perp}=\{0\}$.

Notemos que $0\in S$ e $0\in S^{\perp}$ pois S e $S^{\perp}$ são subespaços vetoriais de V. Logo, $0\in S\cap S^{\perp}$, e assim $\{0\}\subset S\cap S^{\perp}$.

Seja $v\in S\cap S^{\perp}$. Então, $v\in S$ e $v\in S^{\perp}$. Como $v\in S^{\perp}$, temos que $\langle v,s\rangle=0$, para todo $s\in S$. Em particular, $\langle v,v\rangle=0$, e assim $v=0$. Portanto, $S\cap S^{\perp}\subset\{0\}$. ■

Observação 3.5. Se $v\in V$, $v\neq 0$, tem-se

$$v^{\perp}=\{u\in V|\langle u,\alpha v\rangle=0,\alpha\in\mathbb{R}\}.$$

4 NOÇÕES DE GRUPOS

Neste capítulo trataremos do conceito de grupo, suas propriedades e de outros conceitos pertinentes à Teoria de Grupos. Nos embasaremos nesses conceitos para, posteriormente, construirmos os conceitos de grupos de simetrias no plano e no espaço. Neste primeiro momento adotaremos a conceituação segundo (DOMINGUES; IEZZI, 2003).

4.1 O conceito de grupo

Definição 4.1. *Seja um conjunto não-vazio G constituído de uma operação*

$$\begin{aligned} * : G \times G &\longrightarrow G \\ (a,b) &\longmapsto a * b. \end{aligned}$$

*Dizemos que G é um **grupo** se $*$ satisfaz as seguintes propriedades:*
(I) Associatividade: $(a*b)*c = a*(b*c)$, para todo $a,b,c \in G$.
(II) Existência do elemento neutro: existe um $e \in G$ tal que $a*e = e*a = a$, para todo $a \in G$.
(III) Existência do elemento simétrico: para todo $a \in G$, existe $a' \in G$ tal que $a*a' = a'*a = e$.

Denotaremos o par $(G,*)$ para referirmos ao grupo G munido da operação $*$.

Definição 4.2. *Seja $(G,*)$ um grupo. Dizemos que G é um grupo abeliano se $a*b = b*a$, para todo $a,b \in G$.*

Mostraremos, a seguir, algumas propriedades imediatas relacionadas a grupo.

Proposição 4.1. *Seja $(G,*)$ um grupo. Existe um único elemento neutro $e \in G$ tal que $a*e = a$, para todo $a \in G$.*

Demonstração. Suponhamos que existam e_1, e_2 tais que $a*e_1 = a$ e $a*e_2 = a$, para todo $a \in G$. Provaremos que $e_1 = e_2$.

Seja $a \in G$. Como G é grupo, existe $a' \in G$ tal que $a*a' = a'*a = e_1$ e $a*a' = a'*a = e_2$. Operando os dois lados da equação, à esquerda, por a' obtemos

$$a'*(a*e_1) = a'*(a*e_2).$$

Pela associatividade segue que

$$(a' * a) * e_1 = (a' * a) * e_2$$
$$e_1 * e_1 = e_2 * e_2$$
$$e_1 = e_2,$$

como queríamos. ■

Proposição 4.2. *Seja $(G, *)$ um grupo e $a \in G$. Existe um único elemento simétrico $a' \in G$ que satisfaz $a * a' = a' * a = e$.*

Demonstração. Seja $a \in G$. Suponhamos que existam a'_1, a'_2, tais que $a * a'_1 = a'_1 * a = e$ e $a * a'_2 = a'_2 * a = e$. Mostraremos que $a'_1 = a'_2$.

Como $a * a'_1 = e$ e $a * a'_2 = e$, temos que $a * a'_1 = a * a'_2$. Operando dos dois lados, à esquerda, por a'_1 obtemos que

$$a'_1 * (a * a'_1) = a'_1 * (a * a'_2).$$

Pela associatividade segue que

$$(a'_1 * a) * a'_1 = (a'_1 * a) * a'_2$$
$$e * a'_1 = e * a'_2$$
$$a'_1 = a'_2,$$

provando o que queríamos. ■

Proposição 4.3. *Seja $(G, *)$ um grupo. Então, para todo $a, b \in G$ tem-se que $(a * b)' = b' * a'$.*

Demonstração. Sejam $a, b \in G$. Vamos mostrar que $(a * b) * (b' * a') = e$ e $(b' * a') * (a * b) = e$ pois, pela unicidade do elemento simétrico, teremos $b' * a' = (a * b)'$.

Pela propriedade associativa temos que

$$\begin{aligned}(b' * a') * (a * b) &= b' * (a' * a) * b \\ &= b' * e * b \\ &= b' * b \\ &= e,\end{aligned}$$

e

$$\begin{aligned}(a*b)*(b'*a') &= a*(b*b')*a' \\ &= a*e*a' \\ &= a*a' \\ &= e.\end{aligned}$$

seguindo o que desejávamos provar. ■

Proposição 4.4. *Seja $(G,*)$ um grupo. Para todo $a \in G$ tem-se $(a')' = a$.*

Demonstração. Seja $a \in G$. Sabemos que $a*a' = e$. Pelo fato de $e' = e$ e pela Proposição 4.3 segue que $(a')'*a' = e$. Operando os dois lados, à direita, por a e usando a associatividade obteremos

$$\begin{aligned}(a')'*a' &= e \\ ((a')'*a')*a &= e*a \\ (a')'*(a'*a) &= e*a \\ (a')'*e &= e*a \\ (a')' &= a,\end{aligned}$$

mostrando o que desejávamos. ■

Proposição 4.5. *Seja $(G,*)$ um grupo. Se $a*x = a*y$, para todo $a \in G$, então $x = y$.*

Demonstração. Seja $a \in G$. Se $a = e$ segue a tese pelo fato de e ser o elemento neutro da operação $*$. Suponhamos que $a \neq e$. Logo, existe $a' \in G$ tal que $a*a' = a'*a = e$. Operando os dois lados, à esquerda, por a' e usando a associatividade temos que

$$\begin{aligned}a'*(a*x) &= a'*(a*y) \\ (a'*a)*x &= (a'*a)*y \\ e*x &= e*y \\ x &= y,\end{aligned}$$

provando o que pretendíamos. ■

Definição 4.3. *Seja $(G,*)$ um grupo e H um subconjunto não-vazio de G. Dizemos que H é um subgrupo de G se são satisfeitas as seguintes asserções:*
(I) para todo $a,b \in H$, $a*b \in H$.
(II) H, munido da operação $*$ restrita a H, é um grupo.

4.2 Grupos finitos, de permutação e cíclicos

Definição 4.4. *Seja $(G,*)$ um grupo. Dizemos que G é finito se o número de seus elementos é finito. Esse número chamamos de ordem de G e denotamos por $|G|$.*

Definição 4.5. *Seja E um conjunto não-vazio. Uma permutação dos elementos de E é uma função $f : E \to E$ bijetora.*

Seja E um conjunto não-vazio. Denotemos por $S(E)$ o conjunto de todas as permutações de E.

Proposição 4.6. *Seja E um conjunto não-vazio. Se $f,g \in S(E)$, então $f \circ g \in S(E)$.*

Demonstração. Sejam $f,g \in S(E)$. Vamos provar que $f \circ g \in S(E)$, isto é, que $f \circ g$ é injetora e sobrejetora.

Sejam $x,y \in E$ tais que $f(g(x)) = f(g(y))$. Como f é injetora, segue que $g(x) = g(y)$ e, como g é injetora, temos que $x = y$, provando que $f \circ g$ é injetora.

A seguir, mostraremos que $f \circ g$ é sobrejetora, isto é, $E \subset f(g(E))$.

Seja $z \in E$. Como f é sobrejetora, existe $y \in E$ tal que $z = f(y)$; como g é sobrejetora, existe $x \in E$, tal que $y = g(x)$. Logo, existe $x \in E$ tal que $z = f(y) = f(g(x))$, provando o que queríamos. ■

Proposição 4.7. *Seja E um conjunto não-vazio. O par $(S(E),\circ)$ é um grupo, sendo $\circ$ a composição de funções.*

Demonstração. Sejam $f,g,h \in S(E)$. Em primeiro lugar, mostraremos a propriedade associativa. Para todo $x \in E$ temos que

$$(f \circ (g \circ h))(x) = f(g(h(x))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x),$$

e assim segue a associatividade.

Considere $i_E : E \to E$ a função identidade. Vamos mostrar que i_E é o elemento neutro de $S(E)$. De fato, para todo $x \in E$, temos

$$(f \circ i_E)(x) = f(i_E(x)) = f(x)$$

e

$$(i_E \circ f)(x) = i_E(f(x)) = f(x).$$

Por fim, demonstraremos a existência do elemento simétrico.

Como $f \in S(E)$, temos que f é bijetora. Logo, existe $f^{-1} \in S(E)$. Desse modo, para todo $x \in E$, segue que

$$(f \circ f^{-1})(x) = i_E(x) = (f^{-1} \circ f)(\text{x})$$

Portanto, f^{-1} é o elemento simétrico em $S(E)$. ■

Definição 4.6. *Seja $(G, *)$ um grupo. Dizemos que G é um grupo cíclico se existe $a \in G$ tal que G é gerado por a, isto é, todos os elementos de G podem ser escritos como uma potência de a.*

4.3 Homomorfismo e isomorfismo de grupos

Nesta seção verificaremos apenas as definições de homomorfismo e isomorfismo de grupos que serão necessárias posteriormente.

Definição 4.7. *Sejam $(G, *)$ e $(H, \circ)$ grupos. Dizemos que uma aplicação $f : G \longrightarrow H$ é um homomorfismo se, para todo $a, b \in G$, tem-se*

$$f(a * b) = f(a) \circ f(b).$$

Exemplo 4.1. *Seja $(GL_n(\mathbb{R}), \cdot)$ o grupo das matrizes de ordem n inversíveis com a operação de multiplicação de matrizes e $(\mathbb{R}^*, \cdot)$ o grupo dos números reais sem o 0 com a operação de multiplicação usual. A aplicação*

$$\begin{aligned} det : GL_n(\mathbb{R}) &\longrightarrow \mathbb{R}^* \\ A &\longmapsto det(A) \end{aligned}$$

é um homomorfismo. De fato, da propriedade de determinante, $det(A \cdot B) = det(A) \cdot det(B)$, para toda $A, B \in GL_n$.

Definição 4.8. *Sejam* $(G,*)$ *e* $(H,\circ)$ *grupos. Dizemos que uma aplicação* $f : G \longrightarrow H$ *é um isomorfismo se* f *é um homomorfismo bijetor, ou seja,* f *é um homomorfismo e é bijetora.*

Exemplo 4.2. *Sejam* $(\mathbb{Z},+)$ *e* $(2\mathbb{Z},+)$ *grupos. A aplicação*

$$\begin{aligned} f :& \mathbb{Z} \longrightarrow 2\mathbb{Z} \\ & n \longmapsto 2n \end{aligned}$$

é um isomorfismo.

Sejam $m,n \in (\mathbb{Z},+)$. Temos que

$$f(m+n) = 2(m+n) = 2m+2n = f(m)+f(n),$$

mostrando que f é um homomorfismo.

Provaremos, a seguir, que f é injetora. Sejam $m,n \in \mathbb{Z}$ tais que $f(m) = f(n)$, isto é, $2m = 2n$, e assim $m = n$.

Para finalizar, iremos mostrar que f é sobrejetora. Seja $k \in 2\mathbb{Z}$, isto é, k é um número par. Logo, existe $n \in \mathbb{Z}$ tal que $k = 2n$, ou seja, existe $n \in \mathbb{Z}$ tal que $k = f(n)$, concluindo nossa demonstração.

5 OS GRUPOS DE SIMETRIAS

Neste capítulo veremos o conceito dos grupos de simetria nos espaços euclidianos $\mathbb{R}^2$ e $\mathbb{R}^3$. A apresentação desses grupos será feita sob a perspectiva de (CURTIS, 1984), logo, as definições, teoremas e propriedades terão uma perspectiva que irá além da Álgebra Abstrata, percorrendo a Álgebra Linear, além disso, alguns resultados serão enunciados de acordo com (MARTIN, 1982). Neste capítulo consideraremos o produto interno canônico do $\mathbb{R}^n$ e iremos considerar como a distância, a distância euclidiana entre dois pontos (a distância mais usual).

5.1 Os grupos de simetrias em $\mathbb{R}^2$

Nesta seção iremos considerar dois tipos de simetrias, segundo (CURTIS, 1984): rotação e reflexão.

Definição 5.1. *Seja uma figura X um conjunto de pontos no plano. Uma simetria dessa figura é uma transformação T no plano que satisfaz as seguintes condições:*
(I) $T(X) = X$, ou seja, a transformação T leva cada ponto de X em X e, cada um desses pontos, é a imagem de algum outro ponto de X.
(II) T preserva as distâncias, ou seja,

$$d(T(p), T(q)) = d(p,q).$$

Definição 5.2. *Seja $R : \mathbb{R}^2 \to \mathbb{R}^2$ uma transformação linear que preserva distâncias. Dizemos que R é uma rotação em torno da origem se $R(x,y) = (x',y')$, sendo $v = (x',y')$ o vetor obtido da rotação, em graus, no sentido anti-horário, do vetor $u = (x,y)$.*

Definição 5.3. *Seja $S : \mathbb{R}^2 \to \mathbb{R}^2$ uma transformação linear que preserva distâncias.*
(i) Dizemos que S é uma reflexão em torno do eixo x se $S(x,y) = (x,-y)$.
(ii) Dizemos que S é uma reflexão em torno do eixo y se $S(x,y) = (-x,y)$.
(iii) Dizemos que S é uma reflexão em torno de $(0,0)$ se $S(x,y) = (-x,-y)$.

Observação 5.1. Note que a reflexão descrita na afirmação (iii) da definição acima é um caso de uma rotação de 180 graus, estando o vetor u sobre a reta $y = x$.

O resultado a seguir nos será útil para o que faremos ao longo dessa seção.

Proposição 5.1. *Seja $T : \mathbb{R}^2 \to \mathbb{R}^2$ uma transformação ortogonal. Então, a matriz $[T]$ associada a T, na base canônica $\mathscr{B} = \{e_1, e_2\}$, onde $e_1 = (1,0)$ e $e_2 = (0,1)$, tem somente uma das* *seguintes formas:*

1. $[T] = \begin{bmatrix} cos(\theta) & -sen(\theta) \\ sen(\theta) & cos(\theta) \end{bmatrix}$*, que é a matriz da rotação centrada na origem e ângulo* $\theta \in [0, 2\pi[$*;*

2. $[T] = \begin{bmatrix} cos(\theta) & sen(\theta) \\ sen(\theta) & -cos(\theta) \end{bmatrix}$*, que é a matriz da reflexão na reta que passa pela origem e faz um ângulo de* $\frac{\theta}{2}$ *com o eixo x positivo.*

Demonstração. Ver (BACALHAU, 2012).

Teorema 5.2. *Sejam* $R, S : \mathbb{R}^2 \to \mathbb{R}^2$ *transformações lineares que preservam a distância. São verdadeiras as seguintes afirmações:*

(a) Se R_1 *é uma rotação de ângulo* θ_1 *e* R_2 *é uma rotação de ângulo* θ_2*, então* $R_1 \circ R_2$ *é uma rotação de ângulo* $\theta_1 + \theta_2$*.*

(b) Se S_1 *e* S_2 *são reflexões, então* $S_1 \circ S_2$ *é uma rotação.*

(c) Se R *é uma rotação e* S *é uma reflexão, então* $R \circ S$ *é uma reflexão.*

Demonstração. Seja R_1 uma rotação de ângulo θ_1 e R_2 uma rotação de ângulo θ_2. Então,

$$[R_1] = \begin{bmatrix} cos(\theta_1) & -sen(\theta_1) \\ sen(\theta_1) & cos(\theta_1) \end{bmatrix}$$

e

$$[R_2] = \begin{bmatrix} cos(\theta_2) & -sen(\theta_2) \\ sen(\theta_2) & cos(\theta_2) \end{bmatrix}.$$

Então:

$$\begin{aligned} [R_1 \circ R_2] &= [R_1] \cdot [R_2] \\ &= \begin{bmatrix} cos(\theta_1) & -sen(\theta_1) \\ sen(\theta_1) & cos(\theta_1) \end{bmatrix} \cdot \begin{bmatrix} cos(\theta_2) & -sen(\theta_2) \\ sen(\theta_2) & cos(\theta_2) \end{bmatrix} \\ &= \begin{bmatrix} cos(\theta_1 + \theta_2) & -sen(\theta_1 + \theta_2) \\ sen(\theta_1 + \theta_2) & cos(\theta_1 + \theta_2) \end{bmatrix}, \end{aligned}$$

provando (a).

Sejam S_1 e S_2 reflexões, excetuando a reflexão descrita na afirmação (iii) da Definição 5.3. Pela Proposição 5.1, temos que

$$[S_1] = \begin{bmatrix} cos(\alpha_1) & sen(\alpha_1) \\ sen(\alpha_1) & -cos(\alpha_1) \end{bmatrix}$$

e

$$[S_2] = \begin{bmatrix} cos(\alpha_2) & sen(\alpha_2) \\ sen(\alpha_2) & -cos(\alpha_2) \end{bmatrix}.$$

Então:

$$\begin{aligned} [S_1 \circ S_2] &= [S_1] \cdot [S_2] \\ &= \begin{bmatrix} cos(\alpha_1) & sen(\alpha_1) \\ sen(\alpha_1) & -cos(\alpha_1) \end{bmatrix} \cdot \begin{bmatrix} cos(\alpha_2) & sen(\alpha_2) \\ sen(\alpha_2) & -cos(\alpha_2) \end{bmatrix} \\ &= \begin{bmatrix} cos(\alpha_1 - \alpha_2) & -sen(\alpha_2 - \alpha_1) \\ sen(\alpha_1 - \alpha_2) & cos(\alpha_1 - \alpha_2) \end{bmatrix}. \end{aligned}$$

Logo, pela Proposição 5.1, temos que $S_1 \circ S_2$ é uma rotação.

Por fim, vamos provar a afirmação (c).

Sejam R uma rotação e S uma reflexão, exceto a reflexão indicada na afirmação (iii) da Definição 5.3. Pela Proposição 5.1, as matrizes associadas a R e a S podem ser escritas como

$$[R] = \begin{bmatrix} cos(\theta) & -sen(\theta) \\ sen(\theta) & cos(\theta) \end{bmatrix}$$

e

$$[S] = \begin{bmatrix} cos(\alpha) & sen(\alpha) \\ sen(\alpha) & -cos(\alpha) \end{bmatrix}.$$

Então:

$$\begin{aligned} [R \circ S] &= [R] \cdot [S] \\ &= \begin{bmatrix} cos(\theta) & -sen(\theta) \\ sen(\theta) & cos(\theta) \end{bmatrix} \cdot \begin{bmatrix} cos(\alpha) & sen(\alpha) \\ sen(\alpha) & -cos(\alpha) \end{bmatrix} \\ &= \begin{bmatrix} cos(\alpha + \theta) & sen(\alpha + \theta) \\ sen(\alpha + \theta) & -cos(\alpha + \theta). \end{bmatrix} \end{aligned}$$

Logo, pela Proposição 5.1, segue que $R \circ S$ é uma reflexão. ■

Ao descrevermos as rotações e reflexões de uma figura X do plano euclidiano $\mathbb{R}^2$, faz sentido considerarmos o conjunto formado por todas as simetrias no plano dessa figura X.

Teorema 5.3. *Seja X uma figura no plano euclidiano $\mathbb{R}^2$ e seja G o conjunto formado por todas as simetrias de X. Então, o par $(G,\circ)$ é um grupo, sendo $\circ$ a operação composição de funções.*

Demonstração. Sejam $T,S \in G$. Em primeiro lugar, vamos provar que $S \circ T \in G$. Seja X uma figura do plano. Como $S(X) = X$ e $T(X) = X$, temos que

$$(S \circ T)(X) = S(T(X)) = S(X) = X.$$

Sejam $p,q \in X$. Iremos mostrar que

$$d((T \circ S)(p),(T \circ S)(q)) = d(p,q).$$

Pelo fato de $T,S \in G$, temos que $d(T(S(p)),T(S(q))) = d(S(p),S(q))$ e $d(S(p),S(q)) = d(p,q)$. Logo,

$$d((T \circ S)(p),(T \circ S)(q)) = d(T(S(p)),T(S(q))) = d(S(p),S(q)) = d(p,q).$$

Desse modo, provamos que $(T \circ S)(X) = X$ e $d((T \circ S)(q),(T \circ S)(p)) = d(p,q)$, isto é, $T \circ S \in G$.

Sejam $R,S,T \in G$. Iremos provar que a operação $\circ$ é associativa.

Sejam X uma figura no plano. Então:

$$(R \circ (S \circ T))(X) = R((S \circ T)(X)) = R(S(T(X))) = (R \circ S)(T(X)) = ((R \circ S) \circ T)(X).$$

Seja $I_G(p) = p$ a simetria tal que $I(X) = X$, para qualquer figura X no plano, e $I_G(p) = p$, para todo $p \in X$. Mostraremos que I_G é o elemento neutro de G.

Para começar notemos que $I_G \in G$, pois $I_G(X) = X$, para qualquer figura X do plano, e $d(I_G(p),I_G(q)) = d(p,q)$, para todo $p,q \in X$.

Seja $T \in G$. Para toda figura X do plano segue que

$$(T \circ I_G)(X) = T(I_G(X)) = T(X)$$

e

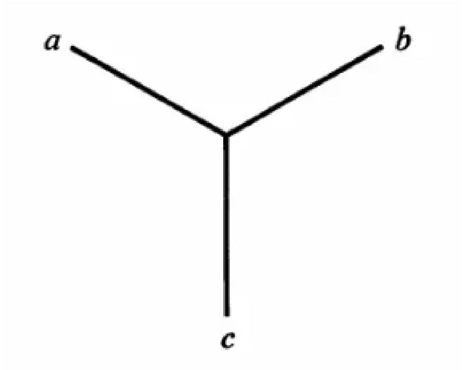
$$(I_G \circ T)(X) = I_G(T(X)) = T(X).$$

Para finalizar, provaremos a existência do elemento simétrico. Seja $T \in G$. Existe $T^{-1} \in G$ tal que $(T \circ T^{-1})(p) = (T^{-1} \circ T)(p) = p$ para todo $p \in X$, sendo X uma figura do plano qualquer, provando o que queríamos. ■

Dada uma figura X no plano euclidiano $\mathbb{R}^2$, podemos nos questionar sobre a quantidade de simetrias que essa figura possui.

Considere a figura 5.1 abaixo.

Figura 5.1 – Simetria I.



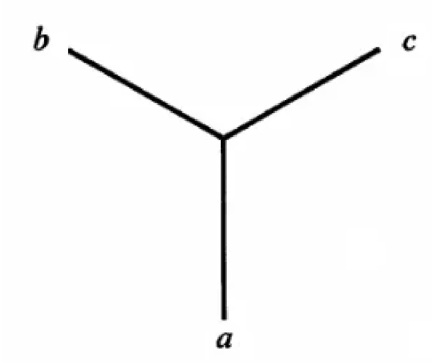
Fonte: Adaptada de Curtis (1984).

Essa figura consiste de três segmentos, a, b e c de mesmo tamanho e unidos por um único ponto, como na figura.

Seja R a rotação de $120°$, no sentido anti-horário, centrada no ponto de união dos segmentos a, b e c, e seja S a reflexão em relação ao segmento a. Vejamos as simetrias que podemos obter.

- A simetria identidade I, que corresponde à figura 5.1.
- Rotacionando a figura 5.1, em $120°$, no sentido anti-horário, e centrada no ponto de união dos segmentos a, b e c, teremos a figura 5.1 rotacionada:

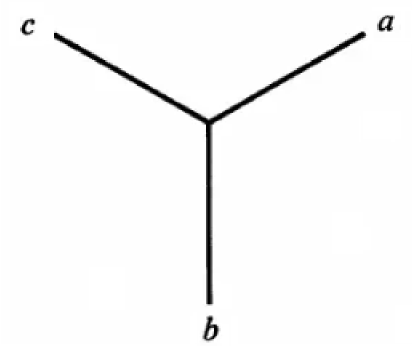
Figura 5.2 – Simetria R.



Fonte: Adaptada de Curtis (1984).

- Aplicando a rotação R na Figura 5.2 acima, teremos a função $R^2 = R \circ R$ e a figura 5.3 abaixo.

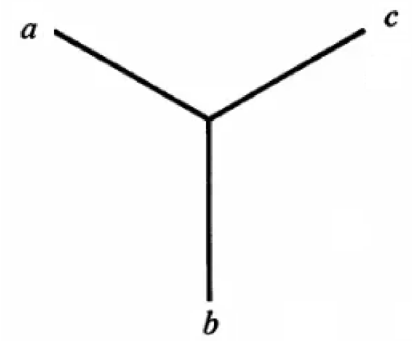
Figura 5.3 – Simetria R^2.



Fonte: Adaptada de Curtis (1984).

- Aplicando a rotação R na figura 5.3, obteremos a figura 5.1. Logo, $R^3 = R \circ R \circ R = I$.
- Agora, aplicando a reflexão S à figura 5.1, obteremos a figura

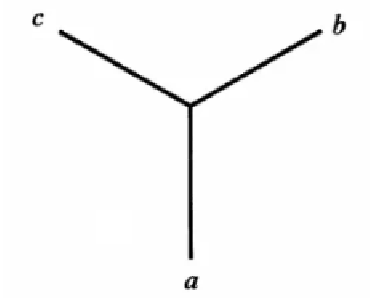
Figura 5.4 – Simetria S.



Fonte: Adaptada de Curtis (1984).

- Tomando como base a figura 5.1, podemos aplicar a rotação R e depois a reflexão S em relação ao segmento a, obtendo a figura

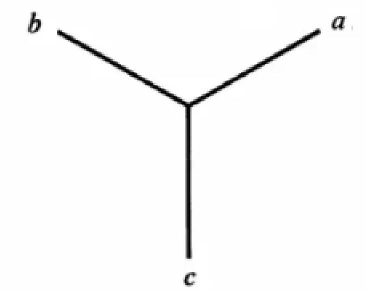
Figura 5.5 – Simetria SR.



Fonte: Adaptada de Curtis (1984).

- Por fim, tomando como base a figura 5.1 e aplicando a rotação R^2 e depois a reflexão S em relação ao segmento a, obteremos.

Figura 5.6 – Simetria SR^2.



Fonte: Adaptada de Curtis (1984).

Notemos que $S^2 = S \circ S = I$ e $R^3 = R \circ R \circ R = I$. Logo, o grupo de simetrias da figura 5.1 é

$$G = \{I, R, R^2, S, SR, SR^2\}.$$

Considere, agora, uma figura no plano formada por n segmentos. O grupo composto pelas simetrias de rotação e reflexão dessa figura denotaremos por D_n, a saber:

$$D_n = \{I, R, R^2, ..., R^{n-1}, S, SR, ..., SR^{n-1}\}.$$

Esse grupo é chamado de **grupo diedral.** O grupo formado pelas rotações $I, R, R^2, ...R^{n-1}$ da mesma figura denotaremos por C_n, a saber:

$$C_n = \{I, R, R^2, ..., R^{n-1}\}.$$

Esse grupo é chamado **grupo cíclico**.

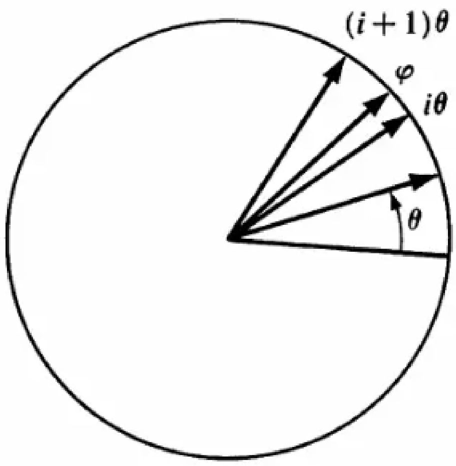
Com essas considerações, vejamos o seguinte teorema:

Teorema 5.4. *Seja G um grupo finito de transformações no plano que preservam a distância. São verdadeiras as seguintes afirmações:*
(a) G é isomorfo ao grupo diedral D_n.
(b) G é isomorfo ao grupo cíclico C_n.

Demonstração. Suponhamos $G \neq \{I\}$ e todo $R \in G$ seja uma rotação. Seja R uma rotação com ângulo de rotação sendo o menor número positivo possível e considere o conjunto $\{I, R, R^2, ..., R^s\}$ formado pelas rotações que possam ser realizadas.

Suponhamos que exista $T \in G$, com T rotação, tal que T não seja nenhuma das rotações possíveis. Se T é uma rotação com ângulo φ e R é uma rotação com ângulo θ, existe i, $i\theta < \varphi < (i+1) \cdot \theta$ (figura 5.7) tal que G contém uma transformação TR^i que é uma rotação em G com ângulo $\varphi - i\theta$, mas $\varphi - i\theta < \theta$, o que contradiz o fato de θ ser o menor ângulo positivo de rotação possível. Portanto, G é um grupo cíclico gerado pelas rotações de ângulo θ, provando (b).

Figura 5.7 – Círculo das rotações com ângulo θ.



Fonte: Curtis (1984).

Vamos, agora, provar (a).

Suponhamos que exista pelo menos uma $S \in G$, com S sendo uma reflexão.

Seja H o conjunto formado por todas as rotações contidas em G, isto é,

$$H = \{I, R, R^2, ..., R^{n-1}\}.$$

Estamos considerando $R^n = I$.

Suponhamos que G possua uma reflexão S. Então, $S \in H$ ou $S \in G - H$. Se $S \in H$, então $SR \in H$ (a composição de rotações é uma rotação), e assim existe $i = 1, ..., n-1$ tal que $SR = R^i$. Então teremos

$$G = \{1, R, ..., R^{n-1}, S, SR, ..., SR^{n-1}\}.$$

Se $S \in G - H$, então SR é uma reflexão e $(SR)^2 = I$. Portanto, G é isomorfo a D_n. ■

Portanto, construímos o grupo das simetrias das figuras no espaço euclidiano $\mathbb{R}^2$.

5.2 Os grupos de simetrias em $\mathbb{R}^3$

Nosso objetivo nessa seção é apresentar o grupo de simetrias em $\mathbb{R}^3$ e, o que faremos a seguir, nos será útil em resultados que iremos demonstrar.

Seja V um espaço vetorial sobre $\mathbb{R}$, munido de um produto interno $\langle \cdot, \cdot \rangle$, e de dimensão n. Seja $v \in V$, $v \neq 0$ e consideremos o subespaço $v^\perp$ de V. Podemos escrever $V = S[v] \oplus v^\perp$.

Seja $T : V \to V$ a transformação ortogonal dada por $T(u) = -u$ se $u \in S[v]$ e $T(u) = u$, se $u \in v^\perp$. T é uma reflexão em relação ao subespaço $v^\perp$. Notemos que $T \circ T = T^2 = I$, sendo I a identidade. De fato, se $u \in S[v]$, então $T(u) = -u$ e $(T \circ T)(u) = T(T(u)) = T(-u) = u$ e segue facilmente que $(T \circ T)(u) = u$.

Teorema 5.5. *Seja V um espaço vetorial sobre $\mathbb{R}$, munido de um produto interno $\langle \cdot, \cdot \rangle$, de dimensão n e seja $T : V \to V$ uma transformação ortogonal. Então T é produto de, no máximo, n reflexões.*

Demonstração. Vamos provar esse resultado por indução em n.

Para $n = 1$, a afirmação é verdadeira. Agora, seja $n \in \mathbb{N}$, $n > 1$, e suponha que a tese seja válida para as transformações ortogonais sob o espaço V com dimensão $n-1$. Seja $T : V \to V$ uma transformação ortogonal e seja $w \in V$, $w \neq 0$.

Caso 1. Suponhamos $T(v) = v$. Se $u \in v^\perp$, então

$$\langle T(u), w \rangle = \langle T(u), T(w) \rangle = \langle u, w \rangle = 0,$$

e assim T é uma transformação ortogonal em $w^\perp$ de dimensão $n-1$. Por hipótese de indução, existem $T_1, ..., T_s$ reflexões de $w^\perp$, com $s \leq n-1$ tais que

$$T(u) = T_1 \cdots T_s(u).$$

Estendendo cada T_i para uma transformação T_i' em V dada por $T_i'(v) = -v$ e $T_i'(u) = T_i(u)$, $u \in v^\perp$, $i = 1, ..., s$, $v \in S[v]$ teremos que T_i' é uma reflexão em V, $i = 1, ..., s$.

Existe um subespaço $H_i \subset v^\perp$, sendo $n-2$ a dimensão de H_i e com $1 \leq i \leq s$ cujos elementos estão fixados por T_i. Então T_i' também fixa os elementos de $H_i' = H_i + S[v]$. Se v_i gera $H_i^\perp$, então $v_i \in (H_i')^\perp$ e $T_i'(v_i) = T_i(v_i) = -v_i$. Logo, pela definição das transformações T_i' segue que

$$T = T_1' \cdots T_s'.$$

Isso mostra que uma transformação ortogonal é um produto de no máximo $n-1$ reflexões.

Caso 2. Suponhamos que $T(v) \neq v$, e assim $u = T(v) - v \neq 0$. Consideremos $u^\perp$ e seja U a reflexão em torno de $u^\perp$. Temos que

$$\langle T(v) - v, T(v) + v \rangle = \langle T(v), T(v) \rangle + \langle T(v), v \rangle - \langle v, T(v) \rangle - \langle v, v \rangle = 0,$$

pois T é uma transformação ortogonal. Logo, $T(v) + v \in u^\perp$ e, pela definição de U ser uma reflexão, segue que

$$U(T(v) + v) = T(v) + v$$

e

$$U(T(v) - v) = -(T(v) - v) = v - T(v).$$

Logo,

$$U(T(v) + v) + U(T(v) - v) = 2v,$$

isto é,

$$U(T(v)) + U(v) + U(T(v)) - U(v) = 2v,$$

ou seja

$$U(T(v)) = v.$$

Pelo Caso 1, sabemos que existem $T_1, ..., T_s$ reflexões tais que

$$U \circ T = T_1 \cdots T_s.$$

Sabendo que $U^2 = I$, segue que

$$T = U^2 T = U(UT) = UT_1 \cdots T_s,$$

completando a prova.■

Corolário 5.1. *Seja $T : \mathbb{R}^3 \to \mathbb{R}^3$ uma rotação. Então, existe $v \in \mathbb{R}^3$, $v \neq 0$, tal que $T(v) = v$.*

Demonstração. Se $T = I$, segue o resultado. Suponhamos $T \neq I$. Como T é uma transformação ortogonal e a $dim_{\mathbb{R}} = 3$ temos, pelo Teorema 5.5, que T é o produto de no máximo três reflexões. Como T é uma rotação, T não pode ser o produto de uma reflexão e nem o produto de três reflexões pois, em ambos os casos, o resultado seria uma reflexão. Então, $T = T_1 \cdot T_2$ onde T_i é uma reflexão a um espaço H_i de dimensão dois, $i = 1, 2$. Sabemos que

$$dim_{\mathbb{R}}(H_1 + H_2) + dim_{\mathbb{R}}(H_1 \cap H_2) = dim_{\mathbb{R}} H_1 + dim_{\mathbb{R}} H_2 = 4.$$

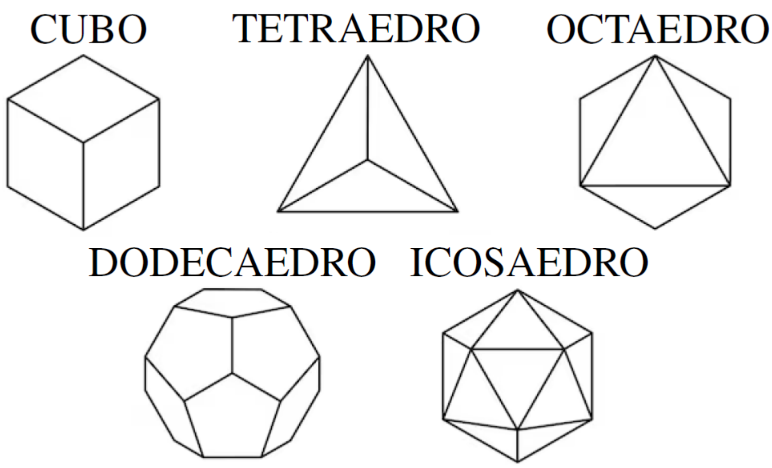
Mas, se tivermos que $dim_{\mathbb{R}}(H_1 + H_2) \leq 3$, então $dim_{\mathbb{R}}(H_1 \cap H_2) \geq 1$. Seja então $v \neq 0$, onde $v \in H_1 \cap H_2$, então só existe uma transformação tal que $T(v) = v$. ■

Para constituirmos as propriedades a respeito dos grupos de simetrias no $\mathbb{R}^3$, será necessário fazermos algumas considerações:

- Pelo Corolário 5.1, toda rotação ocorre em torno de um eixo fixado. Isso será a chave fundamental para a classificação dos grupos finitos de simetria em $\mathbb{R}^3$;
- Por grupo finito de simetria em $\mathbb{R}^3$, entendemos ser o grupo finito de todas as transformações ortogonais em três dimensões.
- Por ordem desse grupo, entendemos a quantidade de elementos que o compõe, como o caso do grupo diedral D_n que, pela seção anterior, temos que sua ordem é $2n$.
- A partir dessa seção, trataremos o grupo D_n como o grupo de simetria dos polígonos regulares de n lados. Além disso, é importante destacar que sendo S a transformação em D_n em torno de um eixo de simetria, S é uma reflexão quando vista do plano, entretanto se vista do espaço, é uma rotação.

Neste trabalho analisaremos especificamente os grupos de simetrias dos sólidos platônicos (figura 5.8).

Figura 5.8 – Sólidos Platônicos.



Fonte: Do autor (2023).

Podemos analisar, também, quais as componentes desses sólidos (Quadro 5.1), estes elementos são essenciais para verificarmos as simetrias. Quanto às faces dos sólidos, encontramos polígonos regulares, no cubo temos quadrados, no tetraedro, no octaedro e no icosaedro temos triângulos e no dodecaedro pentágonos.

Quadro 5.1 – Sólidos Platônicos e suas componentes.

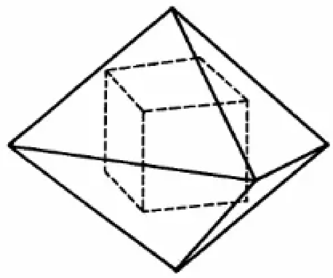
Nome	Vértices	Arestas	Faces
Tetraedro	4	6	4
Cubo	8	12	6
Octaedro	6	12	8
Dodecaedro	20	30	12
Icosaedro	12	30	20

Fonte: Do autor (2023).

Definição 5.4. *Dizemos que dois sólidos são duais quando, partindo do centro de cada uma das faces de um sólido, podemos construir os vértices do outro sólido. Logo podemos inscrever um sólido no outro.*

Exemplo 5.1. O cubo é dual do octaedro, assim como o octaedro é dual do cubo. (Figura 5.9)

Figura 5.9 – Sólidos duais.



Fonte: Curtis (1984).

Observação 5.6. O icosaedro é dual do dodecaedro, assim como o dodecaedro é dual do icosaedro.

Assim como nos grupos de simetrias em duas dimensões, aparentemente teríamos um grupo das simetrias para cada uma dessas formas geométricas. Entretanto, note que como conseguimos inscrever um sólido no outro, por exemplo, quando rotacionarmos o cubo também estaremos rotacionando o octaedro e vice-versa, logo a simetria de ambos será a mesma. E portanto, teremos apenas **três grupos** de simetrias dos sólidos platônicos:

- O grupo de rotações do tetraedro ($\mathscr{T}$);
- O grupo de rotações do octaedro ($\mathscr{O}$);
- O grupo de rotações do icosaedro ($\mathscr{I}$).

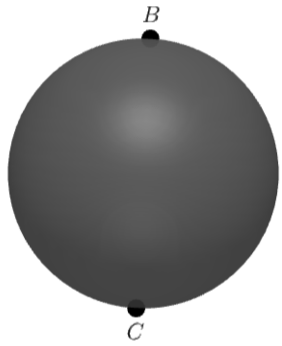
Para construirmos as propriedades desses grupos, faremos uma discussão e apresentaremos algumas definições que nos fornecerão ferramentas para demonstrar alguns resultados.

Sejam

$$S = \{x \in \mathbb{R}^3 | \|x\| = 1\}$$

a esfera unitária em $\mathbb{R}^3$ e $\mathscr{G}$ um grupo finito de rotações em $\mathbb{R}^3$. Notamos que se $T \in \mathscr{G}$, então $T(x) \in S$, para todo $x \in S$, e T é determinada por suas ações sob os elementos de S, pois S contém a base canônica $\mathscr{B} = \{(1,0,0),(0,1,0),(0,0,1)\}$ do $\mathbb{R}^3$. Toda transformação $T \in \mathscr{G}$, tal que $T \neq I_{\mathscr{G}}$, pelo Corolário 5.1 deixa dois pontos, chamados antipodais, fixos na esfera, isto é, $T(p) = p$ (Figura 5.10). Esses pontos são chamados polos de T. Na figura são indicados por B e C.

Figura 5.10 – Esfera S, com pontos antipodais B e C.



Fonte: Do autor (2023).

Considere um número finito de rotações $T : S \to S$, $T \neq I_{\mathscr{G}}$. O conjunto formado por todos os pontos $p \in S$ tais que $T(p) = p$, para algum $T \in \mathscr{G}$, é um subconjunto finito de S.

Teorema 5.7. *Seja p um polo em S. O conjunto $\mathscr{H}$ de todos os elementos $T \in \mathscr{G}$ tal que p é um polo de T, também com o elemento $I_{\mathscr{G}}$, é um subgrupo de $\mathscr{G}$.*

Demonstração. Sejam $T, S \in \mathscr{H}$. Vamos provar que $T \circ S \in \mathscr{H}$. Sabendo que $T(p) = S(p) = p$, segue que

$$(T \circ S)(p) = T(S(p)) = T(p) = p,$$

portanto, $T \circ S \in \mathscr{H}$.

Seja $I_{\mathscr{G}} \in \mathscr{G}$, então $I_{\mathscr{G}}(p) = p$, logo $I_{\mathscr{G}} \in \mathscr{H}$.

Seja $T \in \mathscr{H}$. Então $T(p) = p$, e assim

$$(I_{\mathscr{G}} \circ T)(p) = I_{\mathscr{G}}(T(p)) = T(p) = p$$

e

$$(T \circ I_{\mathscr{G}})(p) = T(I_{\mathscr{G}}(p)) = T(p) = p,$$

portanto, $\mathscr{H}$ possui elemento neutro.

Seja $T \in \mathscr{H}$. Então $T(p) = p$ e existe T^{-1} tal que $T^{-1}(p) = p$. Assim,

$$(T \circ T^{-1})(p) = T(T^{-1}(p)) = T(p) = p = I_{\mathscr{G}}(p)$$

e

$$(T^{-1} \circ T)(p) = T^{-1}(T(p)) = T^{-1}(p) = p = I_{\mathscr{G}}(p),$$

provando que T possui elemento simétrico em $\mathscr{H}$.

Por fim, resta-nos mostrar a associatividade. Sejam $T,S,W \in \mathscr{H}$ tais que $T(p) = S(p) = W(p) = p$. Dessa forma

$$(R \circ (S \circ W))(p) = R((S \circ W)(p)) = R(S(W(p))) = (R \circ S)(W(p)) = ((R \circ S) \circ W)(p)$$

concluindo a prova. ■

Observação 5.8. A ordem desse subgrupo é chamada de *ordem do polo p* e é denotada por v_p.

Definição 5.5. *Dizemos que dois polos p e p' são equivalentes - escrevemos $p \sim p'$ - se $T(p') = p$, para alguma $T \in \mathscr{G}$.*

Observação 5.9. Como existe uma relação de equivalência entre os polos p e p', chamamos o conjunto de todos os polos equivalentes a p de *classe equivalente de p*.

Os próximos resultados serão importantes para constituirmos a forma dos grupos dos sólidos platônicos.

Lema 5.1. *Polos equivalentes possuem a mesma ordem.*

Demonstração. Sejam $\mathscr{H}$ e $\mathscr{H}'$ como no enunciado do Teorema 5.7, sendo $\mathscr{H}$ correspondente a p e $\mathscr{H}'$ correspondente a p'. Como $p \sim p'$, existe $T \in \mathscr{G}$ tal que $p = T(p')$. Considere a aplicação

$$\begin{aligned} \Phi : \mathscr{H}' &\longrightarrow \mathscr{H} \\ X &\longmapsto T \circ X \circ T^{-1} \end{aligned}$$

Vamos provar que Φ é bijetora e, com isso, $|H| = |H'|$, isto é, $v_p = v_{p'}$.

Antes de mais nada, mostraremos que se $X \in \mathscr{H}'$, então $T \circ X \circ T^{-1} \in \mathscr{H}$. Se $X \in \mathscr{H}'$, então $X(p') = p'$. Então,

$$(T \circ X \circ T^{-1})(p) = T(X(T^{-1}(p))) = T(X(p')) = T(p') = p,$$

ou seja, $TXT^{-1} \in \mathscr{H}$.

Mostraremos, a seguir, a injetividade de Φ. Sejam $X,Y \in \mathscr{H}'$ tais que $\Phi(X) = \Phi(Y)$, isto é $T \circ X \circ T^{-1} = T \circ Y \circ T^{-1}$. Aplicando T, à direita, em ambos os lados da igualdade, obtemos

$$
\begin{aligned}
(T \circ X \circ T^{-1}) \circ T &= (T \circ Y \circ T^{-1}) \circ T \\
(T \circ X) \circ (T^{-1} \circ T) &= (T \circ Y) \circ (T^{-1} \circ T) \\
(T \circ X) \circ I_{\mathscr{G}} &= (T \circ Y) \circ I_{\mathscr{G}} \\
T \circ X &= T \circ Y.
\end{aligned}
$$

Aplicando T^{-1} à esquerda, dos dois lados da última igualdade obtemos

$$
\begin{aligned}
T^{-1} \circ (T \circ X) &= T^{-1} \circ (T \circ Y) \\
(T^{-1} \circ T) \circ X &= (T^{-1} \circ T) \circ Y \\
I_{\mathscr{G}} \circ X &= I_{\mathscr{G}} \circ Y \\
X &= Y,
\end{aligned}
$$

provando o desejado.

Agora provaremos que Φ é sobrejetora, ou seja, que dado $Y \in \mathscr{H}$, existe $X \in \mathscr{H}'$ tal que $Y = \Phi(X)$.

Seja $X = T^{-1} \circ Y \circ T$. Notemos que $X \in \mathscr{H}'$. De fato:

$$X(p') = T^{-1}(Y(T(p'))) = T^{-1}(Y(p)) = T^{-1}(p) = p'.$$

Além disso, $Y = \Phi(X)$, que é verificado facilmente. Logo, Φ é sobrejetiva e, portanto, os polos equivalentes possuem a mesma ordem. ■

Lema 5.2. *Seja $X : \mathbb{R}^3 \to \mathbb{R}^3$ uma transformação ortogonal pertencente a $\mathscr{G}$ e $X\mathscr{H} = \{Y \in \mathscr{G} | Y = XT,\ T \in \mathscr{H}\}$. Seja n_p o número de polos equivalentes a p. São verdadeiras as seguintes afirmações:*

(i) $X(p)$ é um polo, para todo $X \in \mathscr{G}$.

(ii) Para todo $X, X' \in \mathscr{G}$, as seguintes afirmações são equivalentes:

(a) $X(p) = X'(p)$.

(b) $X' \in X\mathscr{H}$.

(iii) $n_p = K$, onde K é o número de conjuntos disjuntos da forma $X\mathscr{H}$.

(iv) Cada $X \in \mathscr{G}$ pertence a uma e apenas uma classe lateral.

(v) $|X\mathscr{H}| = v_p$, onde $|X\mathscr{H}|$ é a ordem de $X\mathscr{H}$.

(vi) $n_p \cdot v_p = N$, onde N é a ordem de $\mathscr{G}$.

Demonstração. Vamos provar, a seguir, a afirmação (i).

Seja $X \in \mathscr{G}$ tal que $X(p) = p'$. Logo, $p = X^{-1}(p')$. Seja $S \in \mathscr{H}$, e assim

$$p = S(p) = S(X^{-1}(p')) = S(X^{-1}(X(p))).$$

Portanto,

$$X(p) = X(S(X^{-1}(X(p)))) = (X \circ S \circ X^{-1})(X(p)).$$

ou seja, $X(p)$ é um polo.

Vamos mostrar a afirmação (ii).

Se $X' \in X\mathscr{H}$, então $X' = XT$, $T \in \mathscr{H}$. Logo, $T(p) = p$ e $X'(p) = X(T(p)) = X(p)$, mostrando que (b) implica (a).

Agora consideremos $X, X' \in \mathscr{G}$ e $X(p) = X'(p)$. Sabendo que $X^{-1} \in \mathscr{G}$, temos que $X^{-1}(X(p)) = X^{-1}(X'(p))$, ou seja, $p = (X^{-1} \circ X')(p)$. Daí segue que $X^{-1} \circ X' \in \mathscr{H}$, então existe $T \in \mathscr{H}$ tal que $X^{-1} \circ X' = T$. Assim, $X' = X \circ T$, ou seja, $X' \in X\mathscr{H}$ provando que (a) implica (b).

Note que a afirmação (iii) segue do fato que como p é polo, pela afirmação (i) temos que $X(p)$ é polo. Logo, pela relação de equivalência definida em p, o número de polos equivalentes a p é igual ao número dos conjuntos disjuntos $X\mathscr{H}$, onde $X\mathscr{H}$ é a classe lateral de $\mathscr{H}$ contendo X, pois $X = XI_{\mathscr{G}}$.

A seguir provaremos (iv).

Vamos supor que $X \in X'\mathscr{H} \cap X''\mathscr{H}$. Vamos ver que $X'\mathscr{H} = X''\mathscr{H}$. Temos que se $Y \in X'\mathscr{H}$, então $Y = X'T, T \in \mathscr{H}$. Mas se $X \in X'\mathscr{H} \cap X''\mathscr{H}$, então

$$X = X'T' = X''T'', (1)$$

$T', T'' \in \mathscr{H}$. Logo, existe uma $(T')^{-1}$, onde $X(T')^{-1} = X'$, assim,

$$Y = X'T = X(T')^{-1}T,$$

mas, de (1), teremos que,

$$X(T')^{-1}T = X''T''(T')^{-1}T \in X''\mathscr{H}.$$

Logo, $X'\mathscr{H} \subset X''\mathscr{H}$ e, de maneira similar, $X''\mathscr{H} \subset X'\mathscr{H}$. Portanto, $X'\mathscr{H} = X''\mathscr{H}$, e assim provamos que cada elemento em $\mathscr{G}$ pertence a uma única classe lateral $\mathscr{H}$ contendo X.

Seja

$$\varepsilon : \mathscr{H} \longrightarrow X\mathscr{H}$$
$$T \longmapsto XT.$$

Vamos mostrar que ε é bijetora.

Sejam $T, T' \in \mathscr{H}$ tais que $\varepsilon(T) = \varepsilon(T')$, isto é, $X \circ T = X \circ T'$. Como $X \in X\mathscr{H}$ e $\mathscr{H}$ é subgrupo de $\mathscr{G}$, existe $X^{-1} \in X\mathscr{H}$. Logo, $X^{-1} \circ (X \circ T) = X^{-1} \circ (X \circ T')$, isto é, $T = T'$, provando que ε é injetora.

Vejamos a sobrejetividade.

Seja $Y \in X\mathscr{H}$. Vamos provar que existe $T \in \mathscr{H}$ tal que $\varepsilon(T) = Y$.

Seja $T = X^{-1} \circ Y$. Em primeiro lugar, mostraremos que $T \in \mathscr{H}$. Como $Y \in X\mathscr{H}$, temos que $Y = X \circ U$, $U \in \mathscr{H}$. Logo $Y(p) = X(U(p)) = X(p)$, e assim $T(p) = X^{-1}(Y(p)) = X^{-1}(X(p)) = p$, provando que $T \in \mathscr{H}$. É fácil verificar que $\varepsilon(T) = Y$.

Sabendo que ε é bijetora e que $|\mathscr{H}| = v_p$, segue que $|X\mathscr{H}| = |\mathscr{H}| = v_p$, provando (v).

A afirmação (vi) segue de que, pela afirmação (iii), temos que n_p é o número de classes laterais, $X\mathscr{H}$ e, dessa forma, pela afirmação de que cada classe lateral tem v_p elementos e de que cada $Y \in \mathscr{G}$ pertence a somente uma classe lateral, temos que

$$\mathscr{G} = \bigcup_{Y \in \mathscr{G}} Y\mathscr{H}.$$

Portanto, $card(\mathscr{G}) = \sum_{Y\mathscr{H}} (card(Y\mathscr{H})) = \sum v_p = n_p \cdot v_p = N$, sendo $card(\cdot)$ a cardinalidade. ■

Teorema 5.10. *Sejam $\mathscr{T}$, $\mathscr{O}$ e $\mathscr{I}$ os grupos de simetrias do Tetraedro, do Octaedro e o Icosaedro, respectivamente. São verdadeiras as seguintes afirmações:*

(i) A ordem de $\mathscr{T}$ é 12.

(ii) A ordem de $\mathscr{O}$ é 24.

(iii) A ordem de $\mathscr{I}$ é 60.

Demonstração. Vamos mostrar a afirmação (i).

Seja $T \in \mathscr{T}$ uma transformação que preserva a simetria do Tetraedro e seja $p \in S$ um vértice do Tetraedro. Note que existe $T(p) = p$, logo, pelo Quadro 5.1, temos que existem quatro subgrupos, $\mathscr{H}_{\mathscr{T}}$, associados a cada um dos vértices. Além disso, considere que $I_{\mathscr{G}} \in \mathscr{H}_{\mathscr{T}}$.

Tomando uma simetria em relação a $p \in S$, vértice do Tetraedro, teremos $T_1, T_2 \in \mathscr{H}_{\mathscr{T}}$, com $T_i \neq I_{\mathscr{G}}$, $i = 1,2$. Dessa forma, $v_p = 3$.

Analogamente, seja $T(p) = p'$ a relação de equivalência entre dois vértices $p \in S$, note que existe $T \in \mathscr{G}$ tal que $T(s) = s'$, com $s, s' \in S$ vértices do Tetraedro para cada vértice, também considerando a transformação $I_{\mathscr{G}}$, logo $n_p = 4$.

Seja $N_{\mathscr{T}}$ a ordem do grupo de simetrias do Tetraedro, então, pelo Lema 5.2, temos que

$$N_{\mathscr{T}} = n_p \cdot v_p$$

ou seja,

$$N_{\mathscr{T}} = 4 \cdot 3 = 12.$$

Agora, vamos provar a afirmação (ii).

Seja $P \in \mathscr{G}$ uma transformação que preserva a simetria do Octaedro e seja $q \in S$ um vértice do Octaedro. Note que, para cada vértice existe $P(q) = q$. Dessa forma, pelo Quadro 5.1, temos que existem seis subgrupos, $\mathscr{H}_{\mathscr{O}}$, associados a cada vértice. Note que para cada vértice, existem $P_1, P_2, P_3 \in \mathscr{H}_{\mathscr{O}}$ tais que $P_i(q) = q$, $i = 1,2,3$ e $I_{\mathscr{G}} \in \mathscr{H}_{\mathscr{O}}$. Dessa forma, $v_p = 4$.

De forma similar, seja $P(s) = s'$ a relação de equivalência entre dois vértices $s, s' \in S$. Note que existe $P \in \mathscr{G}$ tal que $P(r) = r'$ com $r, r' \in S$ vértices do Octaedro, para cada vértice, também considerando a transformação $I_{\mathscr{G}}$. Logo $n_p = 6$.

Seja $N_{\mathscr{O}}$ a ordem do grupo de simetrias do Octaedro, então, pelo Lema 5.2, temos que $N_{\mathscr{O}} = n_p \cdot v_p = 6 \cdot 4 = 24$.

Por fim, resta-nos mostrar a afirmação (iii).

Seja $S \in \mathscr{G}$ uma transformação que preserva a simetria do Icosaedro e seja $r \in S$ um vértice do Icosaedro. Note que para cada vértice existe $S(r) = r$. Dessa forma, pelo Quadro 5.1, temos que existem doze subgrupos, $\mathscr{H}_{\mathscr{I}}$, associados a cada vértice. Note que para cada vértice, existem $S_1, S_2, S_3, S_4 \in \mathscr{H}_{\mathscr{I}}$ tal que $S_i(q) = q$, $i = 1,2,3,4$ e $I_{\mathscr{G}} \in \mathscr{H}_{\mathscr{I}}$, dessa forma, $v_p = 5$.

De forma similar, seja $S(t) = t'$ a relação de equivalência entre dois vértices $t, t' \in S$. Note que existe $S \in \mathscr{G}$ tal que $S(r) = r'$, com $r, r' \in S$ vértices do Icosaedro, para cada vértice, também considerando a transformação $I_{\mathscr{G}}$. Logo $n_p = 12$.

Seja $N_{\mathscr{I}}$ a ordem do grupo de simetrias do Icosaedro, então, pelo Lema 5.2, temos que $N_{\mathscr{I}} = n_p \cdot v_p = 12 \cdot 5 = 60$. ■

O próximo resultado determina a estrutura dos grupos de simetrias dos sólidos platônicos através do isomorfismo de grupos, uma vez que conhecemos a estrutura do grupo $\mathscr{G}$, podemos determinar uma relação com os outros grupos.

Teorema 5.11. *Seja $\mathscr{G}$ um grupo finito das rotações em $\mathbb{R}^3$. Então,*
(i) $\mathscr{G}$ é isomorfo ao grupo cíclico $\mathscr{C}_n$, $n \in \mathbb{N}^*$ ou
(ii) $\mathscr{G}$ é isomorfo ao grupo diedral $\mathscr{D}_n$, $n \in \mathbb{N}^*$ ou
(iii) $\mathscr{G}$ é isomorfo ao grupo $\mathscr{T}$ ou
(iv) $\mathscr{G}$ é isomorfo ao grupo $\mathscr{O}$ ou
(v) $\mathscr{G}$ é isomorfo ao grupo $\mathscr{I}$.

Demonstração. Consideremos o conjunto de todos os pares (T, p) com $T \in \mathscr{G}$, $T \neq I_{\mathscr{G}}$, e p é um polo de T. Contando os pares de duas maneiras diferentes, considerando que $T \neq I_{\mathscr{G}}$ é associado a dois polos e, em seguida, que cada polo está associado a $(v-1)$ elementos $T \in \mathscr{G}$, com $T \neq I_{\mathscr{G}}$, teremos

$$2(N-1) = \sum_p (v_p - 1)$$

e considerando os termos à direita de acordo com a classe de equivalência dos polos, C, nós temos

$$2(N-1) = \sum_c n_c(v_c - 1)$$

onde n_c é o número de polos na classe de equivalência C, v_c é a ordem de um polo em C e a soma toma as diferentes classes de equivalência dos polos, mas pelo Lema 5.2, nós temos que,

$$2(N-1) = \sum_c (n_c v_c - n_c) = \sum_c (N - n_c) = \sum_c \left(N - \frac{N}{v_c}\right).$$

Dividindo por N, teremos

$$\frac{2N-2}{N} = \sum_c \frac{\left(N - \frac{N}{v_c}\right)}{N}$$
$$\Rightarrow 2 - \frac{2}{N} = \sum_c \left(1 - \frac{1}{v_c}\right).$$

Note que o lado esquerdo está entre $1 < \left(2 - \frac{2}{N}\right) < 2$ e, portanto,

$$1 < \sum_c \left(1 - \frac{1}{v_c}\right) < 2.$$

Vamos verificar as possibilidades para o número de classes. Note que se $c = 1$, temos

$$\begin{aligned} 1 &< 1 - \frac{1}{v_1} < 2 \\ \Rightarrow 0 &< -\frac{1}{v_1} < 1, \end{aligned}$$

o que é um absurdo, pois $-\dfrac{1}{v_1} < 0$. Consideremos o número de classes maior ou igual a 4. Como $v_i \geq 2$, pois cada classe possui o elemento identidade $(I_{\mathscr{G}})$ e $T \neq I_{\mathscr{G}}$, então $\dfrac{1}{v_i} \leq \dfrac{1}{2}$, para todo $i = 1, 2, ..., k$. Daí, temos que

$$\begin{aligned} 1 &< 1 - \frac{1}{v_1} + 1 - \frac{1}{v_2} + ... + 1 - \frac{1}{v_k} < 2 \\ \Rightarrow 0 &< (k-1) - \sum_{i=1}^{k} \frac{1}{v_i} < 1 \\ \Rightarrow \sum_{i=1}^{k} \frac{1}{v_i} &> (k-1) - 1 = k - 2, \end{aligned}$$

mas

$$\sum_{i=1}^{k} \frac{1}{v_i} \leq \sum_{i=1}^{k} \frac{1}{2} = \frac{k}{2}.$$

Logo,

$$k - 2 < \sum \frac{1}{v_i} \leq \frac{k}{2},$$

ou seja,

$$\begin{aligned} k - \frac{k}{2} &< 2 \\ \Rightarrow \frac{k}{2} &< 2, \end{aligned}$$

ou seja, $k < 4$. Dessa forma, existem duas ou três classes de equivalência. Assim, teremos dois casos.

No primeiro caso consideremos duas classes de equivalência com ordem v_1 e v_2, assim teremos

$$\begin{aligned} 2-\frac{2}{N} &= 1-\frac{1}{v_1}+1-\frac{1}{v_2} \\ \Rightarrow \frac{2}{N} &= \frac{1}{v_1}+\frac{1}{v_2} \\ \Rightarrow 2 &= \frac{N}{v_1}+\frac{N}{v_2}. \end{aligned}$$

Note que $\frac{N}{v_i} > 0$, pois N é a ordem do grupo e v_i é a ordem de cada subgrupo de $\mathscr{G}$. Pelo Lema 5.2, temos que $\frac{N}{v_p} = n_p$, ou seja, $\frac{N}{v_i} \in \mathbb{Z}$.

Como $2 = \frac{N}{v_1}+\frac{N}{v_2}$, segue que $\frac{N}{v_1} = \frac{N}{v_2} = 1$. Ou seja, $N = v_i$, portanto, a ordem dos subgrupos de N é igual a ordem do grupo todo, neste caso só há um eixo de simetria. Logo, $\mathscr{G}$ é cíclico.

No segundo caso, consideraremos três classes de equivalência com ordens v_1, v_2 e v_3, com $v_1 \leq v_2 \leq v_3$. Vamos considerar $v_1 = v_2 = 2$. Então:

$$\begin{aligned} \frac{1}{v_1}+\frac{1}{v_2}+\frac{1}{v_3} &= 1+\frac{2}{N} \\ \Rightarrow \frac{1}{2}+\frac{1}{2}+\frac{1}{v_3} &= 1+\frac{2}{N} \\ \Rightarrow \frac{1}{v_3} &= \frac{2}{N} \\ 2v_3 &= N. \end{aligned}$$

Note que v_3 pode corresponder ao número de vértices da forma geométrica deste grupo. Logo $\mathscr{G}$ é o grupo diedral.

Agora, tomemos $v_1 = 2, v_2 = 3$, assim

$$\begin{aligned} \frac{1}{v_1}+\frac{1}{v_2}+\frac{1}{v_3} &= 1+\frac{2}{N} \\ \Rightarrow \frac{1}{2}+\frac{1}{3}+\frac{1}{v_3} &= 1+\frac{2}{N} \\ \Rightarrow \frac{1}{v_3} &= \frac{1}{2}-\frac{1}{3}+\frac{2}{N} = \frac{1}{6}+\frac{2}{N} \\ \Rightarrow \frac{1}{v_3} &= \frac{N+12}{6N}. \end{aligned}$$

Tomemos $v_3 \geq 3$, pois $v_3 \geq v_2 = 3$. Logo, se $v_3 = 3$, teremos

$$\begin{aligned}
\frac{1}{3} &= \frac{N+12}{6N} \\
\Rightarrow 3(N+12) &= 6N \\
\Rightarrow 3N+36 &= 6N \\
\Rightarrow 3N &= 36 \\
\Rightarrow N &= 12.
\end{aligned}$$

Dessa forma, $\mathscr{G}$ tem ordem 12 e, pelo Teorema 5.10, é o grupo de simetrias do Tetraedro.

Seja $v_3 = 4$, temos

$$\begin{aligned}
\frac{1}{4} &= \frac{N+12}{6N} \\
\Rightarrow 4(N+12) &= 6N \\
\Rightarrow 4N+48 &= 6N \\
\Rightarrow 2N &= 48 \\
\Rightarrow N &= 24,
\end{aligned}$$

assim $\mathscr{G}$ possui ordem 24 e, pelo Teorema 5.10, é o grupo de simetria do Octaedro.

Seja $v_3 = 5$, temos

$$\begin{aligned}
\frac{1}{5} &= \frac{N+12}{6N} \\
\Rightarrow 5(N+12) &= 6N \\
\Rightarrow 5N+60 &= 6N \\
\Rightarrow N &= 60,
\end{aligned}$$

logo, $\mathscr{G}$ possui ordem 60, pelo Teorema 5.10, é o grupo de simetria do Icosaedro.

Note que se $v_3 > 5$, temos

$$\begin{aligned}
&6 \leq v_3 = \frac{6N}{N+12} \\
&6N \geq 6(N+12) = 6N+72 \\
&0 \geq 72,
\end{aligned}$$

o que é um absurdo. Logo, v_3, só pode assumir os valores 3,4 e 5, concluindo a demonstração.

■

6 CONCLUSÃO

Neste trabalho, ao apresentarmos uma parte da História da Matemática, foi possível compreender como alguns conceitos matemáticos podem ser desenvolvidos durante o tempo. Além disso, é notório que o processo para a construção do conhecimento na Matemática nem sempre percorre um caminho cumulativo e linear, mas, depende de inúmeras intervenções e diversos personagens envolvidos para que se chegue a uma só conclusão.

Além disso, com a história da busca pelas soluções das equações algébricas, vimos que o trabalho associativo de diversos matemáticos foi o ponto fundamental para que o conceito de simetria pudesse tomar forma. Também pudemos observar que as dificuldades pessoais de cada matemático os mostraram também como humanos, quebrando o preceito de que os grandes gênios das Ciências Exatas são perfeitos e sem mazelas em seus cotidianos.

Através da história de Evaristé Galois, foi possível analisar que nem sempre as teorias matemáticas são aceitas de imediato, necessitando de diversos aperfeiçoamentos. Com Camille Jordan, temos que os aperfeiçoamentos na matemática nascem da necessidade de resolver situações específicas, como é o caso dos grupos de simetrias para classificar os cristais.

Adentrando na Teoria de Grupos, notamos que a definição do conceito de grupo se ampliou para além das raízes de uma equação. Desse modo, com diversos resultados que foram além dessas fronteiras, pudemos construir os grupos de simetrias no $\mathbb{R}^2$ e $\mathbb{R}^3$, considerando as transformações de rotação e reflexão e suas composições. Na construção desses grupos, pudemos analisar toda a teoria em torno das simetrias dos sólidos platônicos, bem como as generalizações para quaisquer figuras regulares que possam ser definidas no espaço e no plano.

REFERÊNCIAS BIBLIOGRÁFICAS

BACALHAU, F. M. **Isometrias do Plano e Simetria**. 54 p. Dissertação (Mestrado em Matemática para professores) — Universidade de Lisboa, Lisboa, 2012.

COELHO, F. U.; LOURENÇO, M. L. **Um curso de Álgebra Linear**. São Paulo: Editora da Universidade de São Paulo, 2020. v. 2.

CURTIS, C. W. **Linear Algebra: An Introductory Approach**. New York: Springer-Verlag, 1984. v. 2.

DOMINGUES, H. H.; IEZZI, G. **Álgebra Moderna**. São Paulo: Atual, 2003. v. 4.

KIERNAN, B. M. **The Development of Galois Theory from Lagrange to Artin**. **Archive for History of Exact Sciences**, v. 8, p. 40–154, 1971.

LIVIO, M. **A Equação que ninguém conseguia resolver**. Rio de Janeiro: Record, 2005. v. 3.

MARTIN, G. E. **Transformation Geometry: An Introduction to Symmetry**. [S.l.]: Springer, 1982. (Undergraduate Texts in Mathematics).

STEWART, I. **Uma história da simetria na matemática**. Rio de Janeiro: Zahar, 2012. v. 1.

STEWART, I. **Em busca do infinito: Uma história da matemática dos primeiros números à teoria do caos**. Rio de Janeiro: Zahar, 2014. v. 1.