Gabriel de Souza Cruz

O uso do GAP no estudo da teoria de grupos

Alegre - ES

Agosto de 2024

Gabriel de Souza Cruz

O uso do GAP no estudo da teoria de grupos

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática Pura e Aplicada da Universidade Federal do Espírito Santo como parte dos requisitos para a obtenção do título de Licenciado Pleno em Matemática.

Universidade Federal do Espírito Santo – UFES

Centro de Ciências Exatas, Naturais e da Saúde

Departamento de Matemática Pura e Aplicada

Orientador: Victor do Nascimento Martins

Alegre - ES

Agosto de 2024

Gabriel de Souza Cruz

O uso do GAP no estudo da teoria de grupos

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática Pura e Aplicada da Universidade Federal do Espírito Santo como parte dos requisitos para a obtenção do título de Licenciado Pleno em Matemática.

Trabalho aprovado. Alegre - ES, 13 de agosto de 2024.

Banca examinadora:

Prof. Dr. Victor do Nascimento Martins
(DMPA/CCENS - UFES)

Profa. Dra. Patricia Elaine Desideri
(DMPA/CCENS - UFES)

Profa. Dra. Fabiana Maria Ferreira
(DMPA/CCENS - UFES)

Orientador(a):

gov.br
Documento assinado digitalmente
VICTOR DO NASCIMENTO MARTINS
Data: 07/10/2024 15:14:00-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Victor do Nascimento Martins
(DMPA/CCENS - UFES)

Alegre - ES
Agosto de 2024

Esse trabalho dedico à minha esposa (Thamires) e aos meus pais (Leonor e Marino).

Agradecimentos

Primeiramente, quero agradecer a Deus pelo fato de me abençoar com a oportunidade de realizar um trabalho de conclusão de curso na área que me fez querer ser professor de matemática. Também quero demonstrar a gratidão com as pessoas mais importantes da minha vida, que são minha esposa (Thamires), meu pai (Marino), minha mãe (Leonor), meu irmão de coração (Saulo), minha irmã (Valéria), meu sogro (Raul), minha sogra (Elizabeth), meus amigos de república que era minha segunda casa (Dardengo, Fernando, Lucas, Mello, Miquéias), meu orientador e amigo Víctor, meus demais colegas da UFES e meus amigos da igreja (Rafael, Samuel, Danilo, Lauriany, Marim, Nathália, entre outros que estão no meu coração). Quero também agradecer à todos os professores do DMPA que tive a honra de cursar alguma disciplina, os senhores ajudaram a formar meu caráter de professor de matemática, me deram inúmeras oportunidades para prosseguir mesmo com minha rotina completamente corrida!

Sem todos vocês eu não teria chegado aqui, pois ainda que haja em mim certa resiliência, se não fosse Deus tê-los colocado em minha vida, eu ainda não estaria apto para vivenciar tal etapa da graduação, ou nem mesmo chegaria nela, pois sempre que eu me encontrava desanimado ou cansado vocês, de forma direta ou indireta, me davam força e oportunidade para continuar na progressão de realizar meus sonhos.

De todo meu coração, muito obrigado!

Quero agrader, em especial, às professoras Patrícia Desideri e Fabiana Ferreira pelo fato de terem aceitado o convite para composição da banca examinadora do presente trabalho.

Resumo

Este trabalho teve como objetivo a elaboração de um material didático-aplicado para o ensino da teoria algébrica de grupos, conciliando os assuntos teóricos tradicionais abordados no estudo dessa estrutura algébrica com a utilização do software GAP. Atribuiu-se aos tópicos selecionados uma dupla visão, utilizando-se dessa tecnologia de informação como uma ferramenta para contribuir, de forma eficiente, no processo de ensino e aprendizagem sobre grupos. Para isso, foram realizadas diversas pesquisas bibliográficas que culminaram no desenvolvimento de uma ementa contendo tópicos essenciais a serem estudados, tanto por licenciandos quanto por bacharelandos em matemática, visto que o desenvolvimento do pensamento algébrico é um pilar essencial na formação do matemático.

Palavras-chave: Grupos; Processo de ensino e aprendizagem; Matemática; GAP.

Abstract

This work aimed to develop an applied didactic material for teaching the algebraic theory of groups, combining the traditional theoretical topics addressed in the study of this algebraic structure with the use of the GAP software. The selected topics were given a dual perspective, utilizing this information technology as a tool to efficiently contribute to the teaching and learning process about groups. To achieve this, extensive bibliographic research was conducted, culminating in the development of a syllabus containing essential topics to be studied by both mathematics undergraduates and graduates, considering that the development of algebraic thinking is a fundamental pillar in the formation of a mathematician.

Key-words: Groups; Teaching and learning process; Mathematics; GAP.

Sumário

Introdução

A álgebra é considerada uma das grandes áreas de pesquisa em matemática, de modo que a teoria básica de grupos pode ser vista como um alicerce para o desenvolvimento de diversas teorias de natureza algébrica, tais como os espaços vetoriais, anéis e corpos. Consoante a tais aspectos compreende-se a importância de tal teoria algébrica ser discutida nos cursos de matemática, tanto no bacharelado quanto na licenciatura, pois trabalhando aspectos da teoria de grupos é possível munir os futuros profissionais de um pensamento crítico matemático vindo, especialmente, das abstrações que envolvem o estudo de diversos conceitos algébricos.

Outro aspecto importante que tem emergido é a utilização de tecnologias de informação e comunicação, denominadas TIC's, em diversos contextos sociais, e um desses é a utilização nas áreas de pesquisa, onde softwares são usados para auxiliar na produção e compartilhamento de informações de dados e implicações de pesquisas científicas. Além disso, temos as discussões voltadas para áreas de ensino, trazendo argumentações acerca da implementação dessas tecnologias em sala de aula de forma que colabore eficaz e eficientemente no processo de ensino-aprendizagem de diversas áreas de conhecimento.

Mediante aos aspectos elencados, o objetivo desse Trabalho de Conclusão de Curso foi o desenvolvimento de um material que aborda tópicos essenciais da teoria básica de grupos com a utilização de uma tecnologia de informação, que é conhecido como "GAP" (Groups, Algorithms and Programming). Tal material foi fundamentado na ementa também formalizada no escopo desse trabalho. Para construção da ementa utilizada como referência no material desenvolvido, foram feitas pesquisas sobre o plano de ensino da teoria de grupos em alguns centros de pesquisa e ensino, com intuito de investigar quais seriam os "tópicos chave" que deveriam ser abordados numa disciplina básica de grupos, para que tal fosse relevante para o aprendizado de noções de álgebra abstrata na formação do matemático, tanto o licenciado quanto o bacharel.

Todos os assuntos abordados no escopo do trabalho visam expressar quão relevante é o aprendizado sobre a teoria de grupos na graduação em matemática, em particular, na esfera da licenciatura, em prol de que o desenvolvimento do pensamento algébrico venha munir os futuros professores de matemática para atuarem na educação básica de forma coerente e concisa na explicação de tópicos de álgebra nesse nível de educação. Por outro lado, o material desenvolvido no trabalho possui também o potencial de fundamentar conceitos relevantes da estrutura algébrica de grupos para pesquisadores em matemática, visto que a tal teoria é o cerne do desenvolvimento de inúmeros tópicos algébricos.

O trabalho está organizado em 3 capítulos. No primeiro, descrevemos o referencial

teórico, nele estão fundamentados argumentos que justificam a importância de se abordar assuntos sobre a teoria básica de grupos, tanto no âmbito de pesquisa quanto no aspecto de preparação do professor de matemática. No segundo capítulo elencamos diversos aspectos sobre a inserção de tecnologias de informação, em particular o GAP, no processo de ensino e aprendizagem de tal estrutura algébrica na graduação em matemática. Além do mais, nesta parte do trabalho abordamos algumas funções e codificações usadas no software e comentamos como elas se comportam na interface do GAP. Por fim, no terceiro capítulo desenvolvemos uma sequência didática para trabalhar tópicos da teoria de grupos na graduação, culminando na preparação de um material didático com uma dupla visão sobre os tópicos de tal estrutura, de modo que grande parte dos assuntos são abordados conciliando a teoria clássica com a utilização do software.

1 Referencial teórico

1.1 Sobre a teoria básica de grupos

A primeira definição de grupos foi apresentada por Arthur Cayley em um trabalho no ano de 1854, sendo a tal matemático atribuída a frase *"Um grupo é definido por meio de leis que combinam seus elementos"*. Sua definição é um pouco diferente da usada nos dias atuais, mas sendo ambas equivalentes. A definição usada hoje foi descrita por Walther von Dyck, no ano de 1882, onde diz-se que um conjunto não vazio G, com uma operação * é um **grupo** se essa operação for associativa, se existir elemento neutro para tal operação em G e se para todo elemento em G existir um elemento inverso. Se a operação * do grupo G for comutativa, então G é um **grupo abeliano**, nome dado em homenagem ao matemático N. H. Abel.

A teoria de grupos surgiu a partir do estudo das permutações cujo objetivo era obter a solubilidade de equações polinomiais. Sabia-se que equações polinomiais de até quarto grau eram solúveis por meio de radicais, mas somente em 1824, através de trabalhos dos matemáticos Lagrange, P. Ruffini e Abel comprovou-se que as equações de quinto grau não possuíam soluções por meio de radicais. A determinação de quando uma equação algébrica de grau maior que cinco era solúvel por radicais foi dada por Évariste Galois, fundamentada na teoria de *grupos solúveis*, que fora um conceito introduzido pelo próprio Évariste, onde tais resultados foram, a priori, esboçados em uma carta enviada ao seu amigo Auguste Chevalier. No entanto, tais descobertas foram expostas a academia através de Chevalier em *Revue Enciclopédique*. Além do mais, outros resultados foram apresentados por Liouville, no ano de 1846.

Logo nas primeiras décadas do século XX houve uma expansão acerca do estudo sobre a teoria de grupos finitos, onde grandes matemáticos como Frobenius, Burnside, Schur desenvolveram pesquisas relacionadas sobre a classificação e representação de grupos finitos. Em meados de tal século, Hall, Wielandt e Brauer contribuíram para avanços nessa linha de pesquisa, até que em 1982 tal classificação foi completada, com ajuda de inúmeros matemáticos liderados por Gorenstein.

Um fator importante atrelado a teoria de grupos é o estudo entre dois entes matemáticos fundamentais, que é a Álgebra e a Geometria, de modo que, através do estudo da teoria básica de tal estrutura podemos interpretar alguns objetos geométricos utilizando o panorama de grupos, tal aspecto está relacionado com a simetria de figuras planas.

Por mais que a estrutura algébrica de grupo seja considerada simples, visto que

possui uma única operação, sua teoria fundamenta o estudo em diversas áreas da física, química e computacão. Uma aplicação para tais conceitos fundamentais está ligada aos códigos de grupo, que são uma ramificação da área de códigos corretores de erro que têm por base a estrutura algébrica de um anel de grupo, estrutura híbrida de anel e grupo.

Outro aspecto relevante a ser destacado é a abordagem da teoria de grupos em áreas aplicadas da química, especialmente no ramo de cristalografia, alicerçando os estudos acerca dos grupos de simetria e grupos cristalográficos.

1.2 A teoria de grupos na formação do matemático

A priori, temos que a álgebra, de forma inexorável, é um dos grandes eixos de estudo da matemática científica e acadêmica, possuindo inúmeras ramificações provenientes de aplicações. Seguindo nesse panorama temos que a teoria de grupos se destaca por ser umas das primeiras teorias algébricas abstratas que foram estudadas e definidas, sendo que todas as estruturas algébricas que são vistas de forma geral, tanto na licenciatura quanto no bacharelado em matemática, como os espaços vetorias, anéis, corpos finitos, possuem em sua essência o alicerce da teoria de grupos, isto é, tais estruturas, primeiramente, são grupos que possuem uma outra operação que satisfaz algumas outras propriedades. Portanto, vale destacar que ao se estudar a teoria de grupos tanto na licenciatura quanto no bacharelado o aluno estará munido de um conhecimento algébrico que alicerçará seu progresso nos fundamentos de teorias algébricas abstratas em geral.

Outro aspecto importante que vale ser salientado é que através da definição de grupo dada por Cayley/ Von Dick, tal teoria extrapolou os limites da álgebra abstrata e hoje permeia diversas grandes áreas da ciência, dentro e fora da matemática. A teoria de grupos elenca um tópico importante para diversos ramos científicos, que é a simetria interna de uma estrutura, ou seja, busca-se analisar propriedades invariantes dentro de um conjunto, que fundamenta-se no conjunto de transformações realizadas sobre seus elementos que o preservam como grupo, sendo denominado por *grupo de simetria*. Nesse sentido, diversos ramos de pesquisa, que estão relacionados diretamente ou indiretamente com matemática pura ou aplicada, tem se alicerçado em tal teoria da álgebra, como a Teoria de Lie e os grupos topológicos, a Teoria de Gauge e os grupos de laços, dentre outros, que podem ser visto em (SOUZA, 2012). Portanto, é imprescindível o estudo acerca de tal teoria algébrica para formação do matemático, com intuito de muní-lo com as ferramentas matemáticas presentes nesse ente matemático para que o mesmo possa trabalhar tais pilares teóricos em diversas áreas da ciência.

1.3 A teoria de grupos na formação do professor de matemática

No início do século XXI o Ministério da Educação elaborou um parecer acerca de Diretrizes Nacionais para Formação de Professores da Educação Básica, e através dessa nova legislação a licenciatura disvenciliou-se do bacharelado, possuindo projetos e metas específicas, fundamentados em possuírem curriculos próprios e também não estarem mais atrelados a formação de professores do molde "$3 + 1$". Particularmente, no ramo da matemática, tal projeto veio esclarecer o fato de que tanto licenciados quanto bacharéis em matemática trabalham com o mesmo objeto, entretanto possuem objetivos completamente diferentes. Doravante a tal posicionamento, muito bem elencado por (SOARES; BIANCHINI, 2019), emerge uma questão importante: **"Qual a profundidade da abordagem de disciplinas de álgebra no currículo do professor no ensino básico?"**.

Para elencarmos fundamentações que respondam a tal indagação já destacamos que a Teoria de Grupos é a estrutura mais simples dentre as que são comumentes abordadas em cursos de bacharelado ou licenciatura em matemática, visto que possui uma única operação e devem ser satisfeitas três propriedades para que um conjunto não vazio seja um grupo. No entanto todas as demais estruturas algébricas (como os espaços vetoriais, anéis, corpos, entre outras) vistas em tais cursos são, em particular, grupos.

Um outro ponto importante é a defesa de se abordar disciplinas de cunho algébrico nos cursos de licenciatura, pois tais estruturas fundamentam grande parte do conteúdo visto na educação básica. Através das disciplinas de álgebra na graduação o futuro professor estará munido para elencar os tópicos oriundos dessa área da matemática de uma forma com que tais assuntos façam sentido para os aluno, pelo fato da álgebra trabalhar pilares fundamentais como a definição de operações e propriedades atribuídas a cada estrutura, refinando assim a visão como a matemática é construída e permitindo a compreensão de como é organizado o pensamemnto matemático que alicerça as operações vistas na educação básica. Através disso, os futuros docentes terão ferramentas matemáticas que os permitam moldar suas atuações práticas integrando tal conhecimento teórico com a realidade e profundidade necessária para abordar tópicos matemáticos na educação básica. Pois através desse processo os professores serão capazes de trabalhar de forma mais eficiente e eficaz conteúdos matemáticos que exigem maior abstração matemática, como a álgebra. E com isso conseguirão desenvolver, mesmo que em uma esfera mais simplória, o pensamento abstrato matemático, que é de suma importância para compreensão da matemática como linguagem e ciência. Tal parte da discussão está fundamentada por (MONDINI; BICUDO, 2010) como citado abaixo.

> [...] sem esta disciplina o aluno sai do curso sem o alicerce básico para ensinar os princípios fundamentais da matemática. Faz-se necessário, porém, uma apresentação destes princípios, mostrando ao aluno a impor-

> tância da mesma, chamando a atenção para os pontos relevantes e não apenas cumprir currículo e apresentar a teoria de forma vazia e abstrata. Assim como qualquer outra disciplina, a Álgebra deve ser apresentada de maneira a fazer sentido ao aluno o porquê que ela faz parte de seu currículo. (SOUZA,2008 apud MONDINI; BICUDO, 2010, p.51)

Sendo assim, a Teoria de Grupos apresenta-se como uma solução para questão proposta, pois além de sua definição "simples", ressaltamos o fato de tal teoria munir os futuros professores com os princípios fundamentais trabalhados em tópicos algébricos, que envolvem estudo sobre conjuntos, definições sobre operações, entre outros. Ou seja, os futuros profissionais da educação trabalham conteúdos com maior abstração matemática, dando-lhes subsídios para conseguirem abordar tópicos de álgebra vistos no ensino básico, de forma eficaz e eficiente. Portanto, os futuros docentes estarão munidos teoricamente para desenvolverem o pensamento abstrato matemático nos alunos, que é indispenável para fundamentar o conhecimento matemático.

2 Desenvolvimento

2.1 Um breve panorama sobre o ensino de grupos na graduação

Nosso intuito está pautado no desenvolvimento de novas perspectivas de estudo acerca da teoria de grupos na graduação, doravante a essa causa central buscamos entender como tais tópicos algébricos são vistos em cursos de matemática, tanto da licenciatura quanto do bacharelado em universidades e institutos federais dentro do estado do Espírito Santo. Para isso, fizemos um levantamento de projetos pedagógicos de cursos de matemática em páginas eletrônicas de algumas universidades e institutos federais presentes nesse estado, a fim de visualizar os principais assuntos que envolvem a teoria de grupos e como tais são discutidos nesses centros acadêmicos, ou seja, a busca possui o intuito de encontrar subtópicos comuns sobre grupos entre as instituições e assim desenvolver o escopo do trabalho, para que o mesmo agregue a utilização de tecnologias, como o GAP, nos tópicos comumente encontrados nas ementas dos cursos pesquisados, tendo a finalidade de auxiliar o processo de ensino-aprendizagem sobre tal estrutura algébrica nos cursos de matemática.

Para organização dos dados coletados construímos uma tabela que traz elementos como:

i) Nome da instituição e cidade em que está localizada;

ii) Curso e modalidade (bacharelado ou licenciatura);

iii) Nome da disciplina e se é obrigatória ou optativa;

iv) Carga horária (destinada a teoria de grupos);

v) Ementa acerca do tópico de grupos.

Algo que queremos salientar é o fato de que trouxemos as cargas horárias referentes ao assunto da teoria de grupos abordada em cada disciplina descrita na tabela, visto que algumas possuem em seu plano de curso tópicos voltados a outras estruturas algébricas ou que envolvam tópicos sobre teoria dos números. Para atender o objetivo de nosso trabalho descrevemos a carga horária referente a estrutura que iremos abordar, que é a estrutura de grupo.

A seguinte tabela foi construída com o objetivo de resumir os dados obtidos em nossa pesquisa e facilitar a compreensão acerca dos principais assuntos sobre teoria de grupos que são abordados nas instituições pesquisadas, dessa forma fica evidente quais assuntos são comumente abordados sobre tal estrutura algébrica, qual carga horária é

atribuída para tais assuntos e além do mais, conseguimos visualizar a abordagem do conteúdo nos cursos de bacharelado e licenciatura citados, realizando assim, uma análise qualitativa desses dados elencados.

Instituição	**Curso**	**Nome da disciplina**	**Carga horária**	**Ementa (teoria de grupos)**
UFES (Alegre)	Matemática (Licenciatura)	Introdução à Teoria de grupos (Optativa) (UFES, 2017)	60h	Grupos: subgrupos, classes laterais, subgrupos normais, grupos quocientes, grupos cíclicos, grupos de permutações; Teoremas de homomorfismos; Grupos de Sylow.
UFES (Vitória)	Matemática (Bacharelado)	Álgebra 1 (Obrigatória) (UFES, 2018b)	30h	Grupos, Exemplos simples , de grupos e suas estruturas, raízes n-ésimas da unidade, grupo das permutações; grupos de rotações;
UFES (Vitória)	Matemática (Licenciatura)	Álgebra 1 (Obrigatória) (UFES, 2018c)	30h	Grupos, Exemplos simples , de grupos e suas estruturas, raízes n-ésimas da unidade, grupo das permutações; grupos de rotações;

Instituição	**Curso**	**Nome da disciplina**	**Carga horária**	**Ementa (teoria de grupos)**
UFES (Vitória)	Matemática (licenciatura)	Teoria de Grupos (Optativa) (UFES, 2018c)	90h	Grupos, grupos quocientes, teoremas de homomorfismos de grupos. O grupo de permutações; Teoremas de representação; Os teoremas de Sylow.
UFES (Vitória)	Matemática (bacharelado)	Teoria de Grupos (Optativa) (UFES, 2018b)	90h	Grupos, grupos quocientes, teoremas de homomorfismos de grupos; O grupo de permutações; Teoremas de representação; Os teoremas de Sylow.

Instituição	**Curso**	**Nome da disciplina**	**Carga horária**	**Ementa (teoria de grupos)**
UFES (São Mateus)	Matemática (licenciatura)	Elementos de Álgebra (Obrigatória) (UFES, 2018a)	30h	Grupos, Subgrupos, Classes Laterais, Teorema de Lagrange; Homomorfismos de Grupos.
UFES (São Mateus)	Matemática Industrial (Bacharelado)	Álgebra II (Optativa) (UFES, 2013)	30h	Grupos, Subgrupos, Classes Laterais, Teorema de Lagrange, Homomorfismos de Grupos.
IFES (Cachoeiro)	Matemática (Licenciatura)	Álgebra (obrigatória) (IFES, 2020a)	12h	Grupos, subgrupos, grupo quociente.
IFES (Vitória)	Matemática (Licenciatura)	Álgebra II (Obrigatória) (IFES, 2020b)	16h	Grupos e propriedades. Subgrupos e Propriedades. Grupos de Simetria, de Permutação. Grupos Cíclicos. Teorema de Lagrange. Classes Laterais. Grupo Quociente.

Um fator importante a ser destacado é a marcante presença de disciplinas que abordem a teoria de grupos, ou em caráter obrigatório ou de natureza optativa nas instituições pesquisadas, visto que, podemos considerá-la como uma *estrutura clássica* quando discutidos assuntos relacionados a álgebra abstrata e portanto se faz presente na maioria (talvez todos) os cursos de graduação em matemática. Portanto, reafirma-se a importância de compreender como essa teoria vem sendo abordada e quais os principais assuntos que são discutidos, para que possamos determinar uma ementa tal qual supra, de forma efetiva, a necessidade da abordagem da estrutura de grupos nos cursos de matemática.

Através dos dados coletados percebe-se que tópicos da teoria de grupos tais como a definição da estrutura, seguida de exemplos importantes como o grupo de permutações, grupos cíclicos, entre outros, subgrupos, classes laterais, grupos quocientes, teorema de lagrange e homomorfismo de grupos são elementos bastante presentes nas ementas das disciplinas. A partir dessa observação buscamos sugerir uma disciplina que contenha esses conhecimentos comumente trazidos nas ementas dos cursos analisados, que visam cumprir com as propstas elencadas no escopo do trabalho.

i) Nome: **Teoria básica de grupos**

ii) Carga horária: **30h**

iii) Ementa: **Definição de grupo, exemplos de grupos (grupo de permutação, grupo diedral, grupos cíclicos, entre outros), subgrupos, classes laterais, grupos quocientes, teorema de lagrange, homomorfismo de grupos.**

2.2 O uso de tecnologias no ensino de grupos

Um fator inerente a sociedade moderna é a busca pelo avanço tecnológico, em particular, das tecnologias de informação. Diante disso, emergiram diversas implementações de tais tecnologias ao dia a dia para realização de grande parte das atividades humanas. No âmbito educacional tal perspectiva é análoga, pois um grande ponto de discussão de pesquisadores da área da educação está centrada na utilização dessas tecnologias de informação e comunicação (TIC's) com a finalidade de contribuir no processo de ensino e aprendizagem nos diversos níveis de educação, ou seja, utlizar as TIC's como ferramenta no processo educacional de modo que através do uso de tecnologias sejam expandidas as possibilidades do professor ensinar e também do aluno aprender. Note que tal discussão está alicerçada por (PEREIRA, 2010), na citação abaixo.

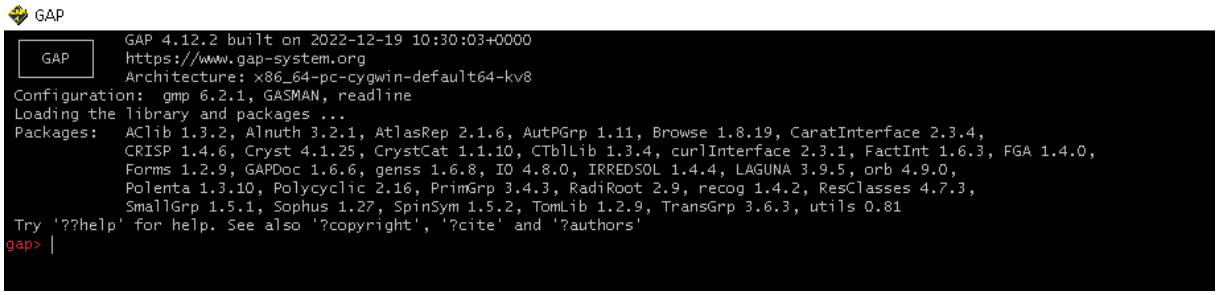
> Devemos considerar como ideal um ensino usando diversos meios, um ensino no qual todos os meios deveriam ter oportunidade, desde os mais modestos até os mais elaborados: desde o quadro, os mapas e as transparências de retroprojetor até as antenas de satélite de televisão. Ali deveriam ter oportunidade também todas as linguagens: desde a palavra falada e escrita até as imagens e sons, passando pelas linguagens matemáticas, gestuais e simbólicas. (SANCHO, 2001, p. 136 apud PEREIRA, p.6).

Sendo assim, o software GAP (GAP, 2011) emerge como uma possibilidade latente de aplicação de toda a discussão teórica acima, pelo fato de que é um recurso computacional que visa contribuir no estudo e pesquisa vinculada a tópicos de álgebra abstrata. Para maior detalhes indicamos (SANTOS; SANTOS,), que mostrou como tal ferramenta computacional contribui para o processo de ensino e aprendizagem em disciplinas de

álgebra, e com isso, direcionamos o escopo de nosso trabalho focados em abordar a temática da estrutura algébrica de Grupos aplicada no GAP, visto que, como discutido anteriormente, é um tópico essencial para formação do professor de matemática.

2.2.1 GAP: Groups, Algorithms and Programming

O software GAP, (GAP, 2011), é um recurso computacional (software) livre, que pode ser instalado direto de sua página inicial (GAP, 2011), e que é voltado para o estudo de álgebra cujo intuito é o de facilitar a pesquisa e o ensino de teorias relacionadas com contextos mais abstratos, de modo que os algoritmos do programa efetuem cálculos que por muitas vezes são trabalhosos e possibilitem a visualização de diversas estruturas, tais como: Espaços vetoriais, Anéis, Grupos, Corpos finitos. Esta subseção, bem como a motivação para utilização do GAP em nosso trabalho, surgiu a partir da leitura de (ALTOE, 2017), onde o autor propõe aplicações das teorias de grupos e corpos no GAP. Abaixo trazemos uma imagem do GAP já instalado no Windows.



2.2.1.1 Preceitos básicos da linguagem GAP

O primeiro elemento a ser destacado é o operador (#), pois qualquer informação que venha após ele é entendida pelo programa como comentário, isto é, não é compilado como parte do código descrito.

O segundo ponto importante é relacionado a atribuição para uma variável utilizando o operador (:=). Outro fator acerca do GAP é que todo comando informado deve ser finalizado com (;), pois caso tal operador não esteja presente ao final do comando o mesmo não é reconhecido pelo programa, ou seja, não há prosseguimento na compilação do código até que o operador esteja presente.

Após cada comando compilado o GAP descreve informações acerca do que foi interpretado, caso isso não seja necessário para o programador, basta finalizar o código utilizando o operador (;;).

2.2.1.2 Alguns comandos

Como comentado anteriormente, o GAP é um software que busca auxiliar nos estudos e pesquisas relacionados a estruturas algébricas como grupos, espaços vetoriais, anéis, dentre outras. Para que isso seja almejado existem diversos comandos em seu menu que visam contribuir para sua utilização de forma eficaz e eficiente em prol de realizar estudos sobre tais áreas da matemática. Nesta seção comentaremos sobre alguns desses comandos que munem o usuário do software com ferramentas computacionais que representam os processos matemáticos utilizados em tais entes de estudo.

2.2.1.3 Funções

O GAP já possui diversas funções integradas, como a função "*IsPrime*" onde o software analisa se um número inteiro é primo ou não, com um caráter de análise booleana.

Exemplo 2.1. Indicar se um inteiro é primo ou não:

```
gap> IsPrime (7);
True
```

No entanto, o usuário pode definir novas funções dentro do software, para isso, basta utilizar o sinal de menos"$(-)$" e o sinal de maior "$(>)$" juntos, assim teremos "$(->)$", que representa a ideia de implicação lógica matemática. Outro aspecto que precisa ser comentado é que para nomearmos a função, atribuímos seu nome e depois usamos o argumento "$(:=)$" para indicar qual função tal nome descreve.

Exemplo 2.2. Elevar um inteiro ao cubo.

```
gap> cub := (x -> x^3);
function (x) ... end
gap> cub (3);
27
```

2.2.1.4 Listas

No GAP podemos agrupar vários elementos num pacote e com isso criar uma lista, pois ele consegue indicar qual a posição de cada elemento listado. Inicia-se uma lista com o colchete esquerdo e finalizada com o direito. As entradas da lista definida são separadas por vírgula. Outro aspecto importante a ser destacado é o comando "*Length*", pois descreve o número de entradas da lista atribuída. Se quisermos saber qual elemento está numa determinada posição da lista basta descrever o nome da lista e colocar a posição almejada dentro de colchetes, e se quisermos avaliar qual posição de um objeto na lista basta utilizar o comando "*Position*", como mostrado abaixo.

Exemplo 2.3. Criar uma lista L.

$gap > L := [4, 2, 14, 27, 1];$
$[4, 2, 14, 27, 1]$
$gap > Length(L);$
5
$gap > L[4];$
27
$gap > Position(L, 27);$
4

Ainda em relação a estruturação de listas no GAP, podemos substituir elementos ou adicioná-los a listas já existentes. Para substituir um elemento, indicamos o nome da lista depois colocamos entre colchetes a posição a ser substuído, depois atribuímos o argumento "(:=)" e descrevemos qual elemento será descrito no local. Para adicionarmos um elemento utilizamos o comando "*Add*", que adicionará tal elemento a última posição da lista já existente, já o comando "*Append*" adiciona toda uma segunda lista a já existente. Vejamos isso no exemplo abaixo.

Exemplo 2.4. Adicionando e substituindo elementos na lista L.

$gap > L := [4, 2, 14, 27, 1];$
$[4, 2, 14, 27, 1]$
$gap > Add(L, 37);$
$gap > L;$
$[4, 2, 14, 27, 1, 37]$
$gap > Append(L, [98, 0, 54]);$
$gap > L;$
$[4, 2, 14, 27, 1, 37, 98, 0, 54]$

2.2.1.5 Vetores e matrizes

De forma geral, podemos pensar no GAP os vetores como listas dos elementos e as matrizes como listas de seus vetores colocadas na mesma linha. Cabe salientar que o comando "*Display*"formata a matriz atribuída próxima a forma canônica da estruturação do ente matemático, trazendo familiaridade e compreenssão de como se comportam os comandos do software em relação aos objetos matemáticos, e para localizar as entradas utilizamos dentro de dois colchetes a coordenada da entrada na matriz. Vejamos abaixo como tais implementações são feitas no GAP.

Exemplo 2.5. Vetores e matrizes

$gap > v := [1, 3, 5];$
$[1, 3, 5]$
$gap > M := [[2, 3, 4], [7, 9, 3], [2, 3, 5]];$
$[[2, 3, 4], [7, 9, 3], [2, 3, 5]]$
$gap > Display(M);$
$[[2, 3, 4],$
$[7, 9, 3],$
$[2, 3, 5]]$
$gap > M * v;$
$[31, 49, 36]$
$gap > M[2][2];$
9

Vale ressaltar que os vetores e as matrizes não podem ter suas entradas alteradas depois de compiladas com intuito de evitar que o software use propriedades de forma errada nos implementos alterados, todavia caso haja necessidade de alterar algo nas matrizes o GAP possui os comandos "(*ShallowCopy*(vetor))" e "(*MutableCopyMat*(matriz))", assim retornam o vetor e a matriz, respectivamente, duplicadas e possíveis de alteração.

2.2.1.6 Conjuntos e listas ordenadas

No GAP, dada uma lista L, o comando "(*Set*)" retorna uma cópia ordenada de tal lista. Outros aspectos importantes que envolvem tais assuntos, são os comandos "(*AddSet*)" que adiciona um elemento na lista já atribuída preservando a classificação do conjunto, além dos comandos "(*Union*)", "(*Intersection*)" e "(*Difference*)", que definem as operações fundamentais sobre conjuntos, que são a união, interseção e diferença, respectivamente. Abaixo veremos como tais comandos são expostos no GAP.

Exemplo 2.6. Lista ordenada e relação entre conjuntos.

$gap > L := Set([-4, 7, -2, 3, 0]);$
$[-4, -2, 0, 3, 7]$
$gap > AddSet(L, 1); L;$
$[-4, -2, 0, 1, 3, 7]$
$gap > Union(L, [2, 5, 15]);$
$[-4, -2, 0, 1, 2, 3, 5, 7, 15]$
$gap > Intersection(L, [-1, 0, 1]);$
$[0, 1]$
$gap > Difference(L, [-1, 0, 1]);$
$[-4, -2, 3, 7];$

2.2.1.7 GAP e a teoria de grupos

Conforme já discutido anteriormente, a álgebra é tratada como um pilar na formação tanto do matemático quanto do licenciado em matemática. Um outro aspecto que já foi elencado é o fato da contribuição da utilização de tecnologias de informação e comunicação no processo de ensino e aprendizagem no ensino de matemática, nas diversas esferas de ensino, desde a educação básica ate o nível superior. Fundamentados nesses entes de discussão, desenvolvemos um material que trabalha a estrutura algébrica de Grupos conciliada com a utilização do GAP em prol de contribuir no processo de ensino e aprendizagem desse assunto, de modo que o GAP ajude a tornar "mais palpável" assuntos que normalmente são vistos como "puramente abstratos".

Nesse naterial desenvolvido para ser aplicado em cursos de matemática, a nível superior, visamos correlacionar os conceitos provenientes do tópico de Grupos, como são comumente abordados, com a forma como os mesmos assuntos são apresentados no software, criando assim, em grande parte do material desenvolvido, uma "dupla visão" dos mesmos tópicos. Criando assim um novo caminho para se estudar os assuntos dessa estrutura algébrica, munindo o docente com ferramentas para utilizar o software como "coadjuvante" no processo de ensino e sendo um potencial facilitador do processo de compreensão dos assuntos abordados aos discentes.

Queremos destacar que a parte aplicada dos assuntos de Grupos no software foram elencados a luz de (HULPKE, 2011), que denvolveu um material bastante completo relacionado a diversas estruturas algébricas, e também, a estrutura algébrica fundamental do escopo de nosso trabalho.

3 Uma proposta de sequência didática

3.1 Introdução

Nesta seção pretendemos descrever uma sequência didática que contemple a teoria básica de grupos segundo a proposta base apresentada na Seção 2.1.

A ideia central está alicerçada em preparar alunos de graduação em matemática tanto para o âmbito de pesquisa na área de álgebra quanto na formação de professores que atuarão no ensino básico, dando-lhes ferramentas para abordar tópicos de álgebra. Sendo assim, buscamos criar uma sequência didático-aplicada que permitirá que pesquisadores e professores utilizem tais tecnologias para avanço dos tópicos matemáticos vinculados a álgebra.

Acerca da relação entre o software com referncial teórico escolhido para ser trabalhado na disciplina proposta, queremos destacar dois grandes aspectos. O primeiro está relacionado com o fato de o GAP ser uma ferramenta que tornará o aprendizado acerca da teoria de grupos mais eficiente e até mesmo atrativo, onde o professor conseguirá discutir, com maior eficiência os assuntos abordados, visto que o docente pode explicar como são realizados os cálculos de cada grande eixo estudado nessa ementa (subgrupos, Teorema de lagrange, classes ded conjugação, dentre outros) para algum exemplo específico e depois utilizar o software para visualizar como seriam as generalizações desses resultados, e com isso tornando o processo de ensino e aprendizagem mais dinâmico e menos exaustivo para docentes e discentes, onde tal generalização não precisará ssr calculada "a mão", mas discutida e compreendida através da interpretação do resultado descrito pelo GAP.

O segundo aspecto a ser destacado é o fato de não trabalharmos com o software os resultados da parte de *grupos quocientes* e de *homomorfismo de grupos*. isso se deve ao fato dos comandos exigirem implementações mais avançadas, ou seja, as funções que seriam relacionadas em tais assuntos envolvem a combinação de diversos comandos, que muitas vezes não são intuitivos da linguagem matemática, como os abordados no escopo do trabalho. Assim, o material proposto continua a contemplar a ideia inicial de ser uma referência para o ensino da teoria de grupos, cabendo ao professor nesse trecho, de estudar e implementar, caso ache válido, a utilização do software nessa parte do trabalho. Caso haja interesse, indicamos (HULPKE, 2011).

No que diz respeito a teoria de grupos básica, a próxima seção foi elaborada baseando-se em (GARCIA; LEQUAIN, 2008) e (GONCALVES, 2006), que são duas referências básicas presentes nas ementas das disciplinas de álgebra que possuíam tópicos da teoria de grupos e que foram pesquisadas para elaboração da Seção 2.1 deste projeto.

3.2 Teoria de grupos

Um **grupo** G é um conjunto não vazio munido de uma operação

$$* : G \times G \to G$$

$$(a, b) \mapsto a * b,$$

satisfazendo as seguintes propriedades:

i) Associatividade:

$$(a * b) * c = a * (b * c);\ \forall\ a, b, c \in G$$

ii) Elemento neutro:

Existe $e \in G$ tal que

$$e * a = a * e = a, \quad \forall\ a \in G$$

iii) Elemento inverso:

$\forall\ g \in G$ existe $g^{-1} \in G$ tal que

$$g * g^{-1} = e = g^{-1} * g$$

Proposição 3.1. *Seja G um grupo com a operação $*$, onde e é o elemento neutro, então:*

a) O elemento neutro é único;

b) O elemento inverso é único;

Demonstração:

a) Sejam e, e_1 elementos neutros de G, daí

$e = e * e_1 = e_1 * e$ e $e_1 = e_1 * e = e * e_1$ logo $e = e_1$;

Observação 3.1. *É usual denotarmos o único elemento neutro de G por e.*

b) Sejam $g \in G$ e $g_1, g_2 \in G$ elementos inversos de g, daí

$g_1 = g_1 * e = g_1 * (g * g_2) = (g_1 * g) * g_2 = e * g_2 = g_2$;

Observação 3.2. *É usual denotarmos o único inverso de $g \in G$ por g^{-1}.*

■

Definição 3.1. Um grupo G é denominado **comutativo** (ou **abeliano**) se

$$g * h = h * g, \ \forall \ g, h \in G$$

Exemplo 3.1. $(\mathbb{C}, +)$ e $(\mathbb{R}, +)$ são grupos aditivos abelianos.

Exemplo 3.2. Considere um conjunto G não vazio e defina

$$G' = \{f : G \to G, f \text{ é bijetora}\}.$$

A operação que definiremos para G' será a composição de funções, isto é:

$$\circ : G' \times G' \to G'$$
$$(g, f) \mapsto g \circ f$$

Temos que $(G', \circ)$ é um grupo onde seu elemento neutro é a aplicação identidade dada por

$$I_G : G \to G$$
$$x \mapsto x.$$

Esse grupo G' que acabamos de definir é chamado **grupo das permutações do conjunto** G. Se $G = 1, 2, 3, ..., n$, denotamos as permutações de G por G_n e tal grupo possui $n!$ elementos.

Usualmente, denotamos os elementos do grupo G_n da seguinte forma:

$$\begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}$$

Vamos considerar o seguinte exemplo

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Temos que $f(1) = 2, f(2) = 3, ef(3) = 1$. Podemos utilizar a notação cíclica (123), para representar essa permutação, onde o elemento seguinte é a imagem do anterior. Temos que o grupo G_3 é formado pelos seguintes elementos:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \ f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Agora, para representarmos o grupo G_3 acima abordado utilizaremos os comandos $G_3 := SymmetricGroup(3)$, que caracteriza um grupo de permutação de ordem 3 no GAP, e através do comando $Elements(G_3)$; o software descreve todos as permutações resultantes. Abaixo mostraremos como tais comandos ficam dispostos no GAP.

Grupo das permutações de ordem 3 (G_3)

$gap > G_3 := SymmetricGroup(3);$
$Sym([1..3])$
$gap > Elements(G_3);$
$[(), (2,3), (1,2), (1,2,3), (1,3,2), (1,3)]$

Vale salientar que o GAP utiliza as notações cíclicas, ou seja, na representação do elemento $(1,2)$ temos que a permutação leva 1 no 2, 2 no 1 e 3 no 3, e de modo análogo, em $(1,2,3)$ temos que 1 é levado no 2, 2 é levado no 3 e 3 é levado no 1. Assim, temos as seguintes identificações no grupo G_3, utilizando essa notação:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \longleftrightarrow ();$$
$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \longleftrightarrow (12);$$
$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \longleftrightarrow (23);$$
$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \longleftrightarrow (13);$$
$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \longleftrightarrow (123);$$
$$f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \longleftrightarrow (132).$$

Definição 3.2. Seja G um grupo e $g \in G$, se $n \in \mathbb{Z}$ definimos g^n como

$$g^n = \begin{cases} e & se \quad n = 0 \\ g^{n-1} * g & se \quad n > 0 \\ (g^{-n})^{-1} & se \quad n < 0. \end{cases}$$

Se $m, n \in \mathbb{Z}$ valem as seguintes propriedades:

i) $g^m * g^n = g^{m+n}$

ii) $(g^m)^n = g^{mn}$

Denotando $< g >= \{g^n : n \in \mathbb{Z}\} \subset G$ então temos que $g^0 = e$, $(g^n)^{-1} = g^{-n}$ e $g^m * g^n = g^{m+n}$ segue de imediato que $< g >$ é um grupo abeliano. Tal grupo é denominado **grupo cíclico** gerado pelo elemento $g \in G$.

Exemplo 3.3. Se $n \geq 1$, onde $n \in \mathbb{Z}$ então o conjunto $\mathbb{Z}_n$ dos inteiros módulo n é um grupo aditivo contendo exatamente n elementos.

Agora, traremos a abordagem do software para construção de grupos cíclicos gerados por um elemento, corroborando com o exemplo acima. No exemplo abaixo, do grupo G, temos a representação do grupo aditivo $\mathbb{Z}_6$, onde tal é gerado pela classe $\overline{1}$ e que é representado pelo GAP por "a".

No GAP, para obtermos tal grupo com um gerador único utilizamos a função "*isFpGroup*". Agora, para construírmos um código que represente um grupo cíclico G de ordem 6 com um único gerador basta tomarmos o comando "*CyclicGroup(IsFpGroup,6)*" e através do comando "*Elements*" todos os elementos de G são descritos.

Grupo cíclico G gerado por "a", de ordem 6

$gap > G := CyclicGroup(IsFpGroup, 6);$
$< fpgroupofsize6onthegenerators[a] >$
$gap > Elements(G);$
$[< identity... >, a, a^2, a^3, a^4, a^5]$

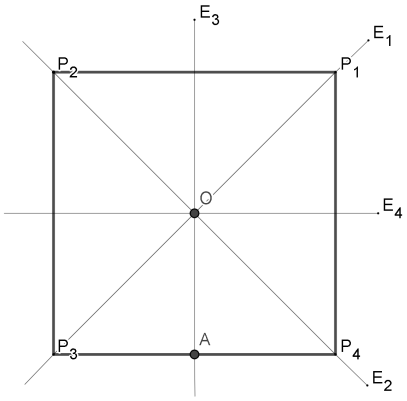
Para melhor compreensão do exemplo a seguir traremos duas definições fundamentais no estudo da teoria básica de grupo.

Definição 3.3. O *grupo de simetria de um objeto geométrico* é o grupo de todas as transformações sob as quais o objeto é invariante, tendo como operação do grupo a composição.

Definição 3.4. Um *grupo diedral* é o grupo de simetrias de um polígono regular de n lados qualquer.

Exemplo 3.4. Grupo de simetrias espaciais do quadrado (C)

Seja $P_1P_2P_3P_4$ um quadrado. Consideramos o centro de gravidade do quadrado como "O" e denominamos por E_1, E_2, E_3, E_4 as retas do espaço determinadas pelas diagonais e mediatrizes do quadrado, respectivamente.



As transformações espaciais que preservam o quadrado são:

i) $id, R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3\pi}{2}}$ as rotações planas centradas na interseção de "O", no sentido anti-horário, de ângulo zero, $\frac{\pi}{2}$, π e $\frac{3\pi}{2}$.

ii) R_1, R_2, R_3, R_4 as rotações espaciais de ângulo π com eixos E_1, E_2, E_3, E_4, respectivamente.

Assim temos que $C := \{id, R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3\pi}{2}} R_1, R_2, R_3, R_4\}$ com a composição de funções é um grupo não abeliano, pois $R_1 \circ R_3 = R_{\frac{3\pi}{2}}$ e $R_3 \circ R_1 = R_{\frac{\pi}{2}}$

No GAP, para trabalharmos os Grupos Diedrais utilizamos funções auxiliares para relacionar as rotações que preservam o quadrado nas transformações espaciais, separando em dois grandes eixos, das rotações em torno do centro de gravidade "O" e das rotações feitas de um ângulo π sobre as diagonais e sobre as mediatrizes do quadrado. Observe que o software utiliza as notações cíclicas, que são análogas ao utilizado no grupo das permutações. Relacionam-se as notações do GAP com as do exemplo do seguinte modo:

$P_2 = 1$, $P_3 = 2$, $P_4 = 3$, $P_1 = 4$;

$R0 = () = id$, $R90 = (1234) = R_{\frac{\pi}{2}}$, $R180 = (13)(24) = R_{\pi}$, $R270 = (1432) = R_{\frac{3\pi}{2}}$,

$H = (12)(34) = R_4$, $D = (13) = R_1$, $V = (14)(23) = R_3$, $N = (24) = R_2$.

Grupo das simetrias espaciais do quadrado (C)

$gap > R90 := (1,2,3,4);; R180 := R90^2;; R270 := R90^3;; R0 := ();;$
$gap > H := (1,2)(3,4);; D := H * R90;; V := H * R180;; N := H * R270;;$
$gap > C := Group(R90, H);$
$Group([(1,2,3,4),(1,2)(3,4)])$
$gap > Elements(C);$
$[(), (2,4), (1,2)(3,4), (1,2,3,4), (1,3),$
$(1,3)(2,4), (1,4,3,2), (1,4)(2,3)]$

3.2.1 Subgrupos

Seja G um grupo e H um subconjunto não vazio de G. Diz-se que H é **subgrupo** de G se e só se H for um grupo com a operação herdada de G.

Proposição 3.2. *Seja $(G, *)$ um grupo com elemento neutro e, e H um subconjunto não vazio de G. H é subgrupo de G se, e somente se, são válidas as seguintes condições*

i) $e \in H$;

ii) $\forall h_1, h_2 \in H$ *tem-se* $h_1 * h_2 \in H$;

iii) $\forall h \in H$ *tem-se* $h^{-1} \in H$;

Demonstração:

($\Rightarrow$) De fato, segue imediatamente das definições de grupo, da unicidade do elemento neutro e da unicidade do inverso de cada elemento do grupo G.

($\Leftarrow$) Basta observar que a condição (ii) (H é fechado para a operação de G) mostra que a operação de G induz a operação em H e essa operação será também associativa já que a operação é associativa em G.

■

Observação 3.3. *Se H for subgrupo do grupo G então denota-se $H \leq G$.*

Exemplo 3.5. Se G é grupo, então $\{e\}$ e G são subgrupos de G, ditos **subgrupos triviais**.

Exemplo 3.6. Seja $n \in \mathbb{Z}$. Temos que $(n\mathbb{Z}, +)$ é subgrupo de $(\mathbb{Z}, +)$.

Exemplo 3.7. Seja G um grupo e $x \in G$. Então

$$C_g(x) = \{y \in G : y * x = x * y\}$$

é um subgrupo de G denominado **centralizador de** x **em** G.

Exemplo 3.8. Seja G um grupo. Então

$$Z(G) = \{a \in G : ax = xa, \forall x \in G\};$$

é um subgrupo de G denominado de **centro do grupo** G.

Exemplo 3.9. Grupo das permutações pares (A_n).

Seja $P = P(x_1, ..., x_n)$ o seguinte polinômio nas variáveis $x_1, ..., x_n$, onde $x_i x_j = x_j x_i, \forall i, j \in \{1, 2, ..., n\}$,

$$P = (x_1 - x_2)(x_1 - x_3)...(x_1 - x_n)(x_2 - x_3)...(x_2 - x_n)...(x_{n-1} - x_n),$$

o qual denotaremos por

$$P = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Se $\gamma \in G'$, denotaremos por P^γ o seguinte polinômio,

$$P^\gamma = \prod_{1 \leq i < j \leq n} (x_{\gamma(i)} - x_{\gamma(j)}),$$

e assim temos que

$$P^\gamma = \pm P.$$

Se $P^\gamma = P$ dizemos que γ é uma **permutação par**, e se $P^\gamma = -P$, diz-se que é uma **permutação ímpar**.

Observe que se $\alpha, \beta \in G_n$ então

$$(P^\alpha)^\beta = P^{\beta \circ \alpha}$$

e disso segue que o conjunto A_n de todas as permutações pares é um subgrupo de G'.

Por exemplo, $A_3 = \{e, f, f^{-1}\}$, onde $e = (), f = (123), f^{-1} = (132)$.

De fato, $P = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ então $P^f = (x_{f(1)} - x_{f(2)})(x_{f(1)} - x_{f(3)})(x_{f(2)} - x_{f(3)}) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1)$, ou seja, $P^f = P$. Analogamente, $P^{f^{-1}} = P$.

Exemplo 3.10. Um conjunto gerador de um grupo é um subconjunto, tal que todo elemento do grupo pode ser expresso como a combinação (sob a operação do grupo) de elementos finitos deste subconjunto e de seus inversos. Dentre eles, temos em G_3 que os elementos $\alpha = (123)$ e $\beta = (23)$ geram todo o grupo. Note que:

$$G_3 = \{\alpha; \beta; \alpha.\beta; \alpha^2; \beta^2; \alpha^2.\beta\}$$

Observação 3.4. *Algo que deve ser salientando nesse trecho do trabalho são os* ***reticulados de subgrupos****, que serão vistos já no próximo exemplo, esses tipos de organogramas descrevem todos os subgrupos segundo as respectivas cardinalidades, onde subgrupos de maior cardinalidade vão ficando próximos ao grupo, os demais com menor cardinalidade vão sendo descrtios, horizontalmente, abaixo dos outros subgrupos, até chegarmos no subgrupo formado somente pelo elemento neutro do grupo atribuído. Além do mais, subgrupos de mesma cardinalidade ficam alinhados horizontalmente e cada subgrupo poosui um "segmento de reta"o liga ao grupo no qual está vinculado.*

Exemplo 3.11. Subgrupos do grupo das permutações de ordem 3 (G_3);
Um exemplo de subgrupo de G_3 é o grupo $H = \{f_2 = (2,3); f_2^{-1} = (3,2); e = ()\}$, visto que satisfaz a Proposição 3.2 pois:

i) $e = () \in H$, por construção;

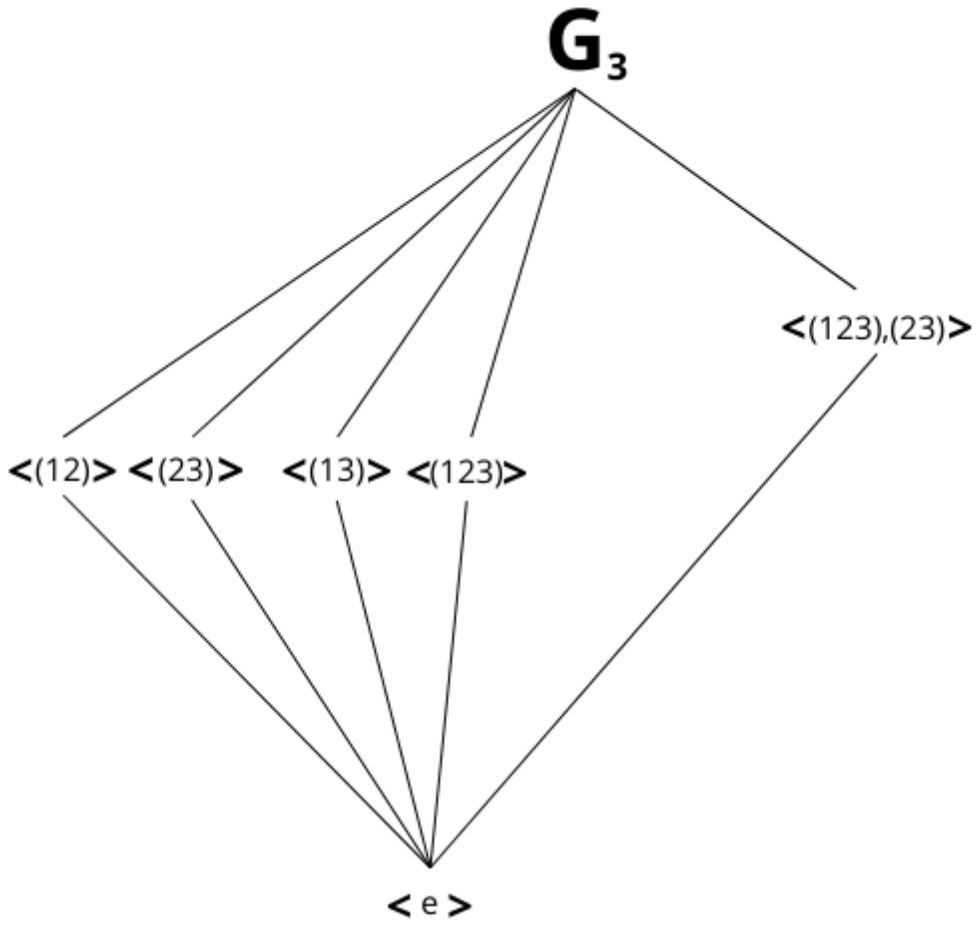
ii) Tomando $f_2 = (2,3), f_2^{-1} = (3,2)$ temos $f_2 \circ f_2^{-1} = f_2^{-1} \circ f_2 = e$, onde $e \in H$;

iii) $f_2 = f_2^{-1}$, $e = e^{-1}$;

Para descrevermos todos os subgrupos utilizando o GAP basta utilizarmos a função "*AllSubgroups*". Em particular, o exemplo acima é descrito no software como "*Group([2,3])*", isto é, o grupo gerado por $(2,3)$.

$gap > G_3 := SymmetricGroup(3);$
$Sym([1..3])$
$gap > Elements(G_3);$
$[(), (2,3), (1,2), (1,2,3), (1,3,2), (1,3)]$
$gap > F := AllSubgroups(G_3);$
$[Group(()), Group([(2,3)]), Group([(1,2)]), Group([(1,3)]), Group([(1,2,3)]),$
$Group([(1,2,3),(2,3)])]$

Imagem 1: Reticulado do grupo G_3



Fonte: próprio autor.

Exemplo 3.12. Subgrupos do grupo cíclico G gerado por a de ordem 6;

Um exemplo de subgrupo de G é $S = \{a^2; a^4, e\}$ pois:

i) $e \in S$, por construção;

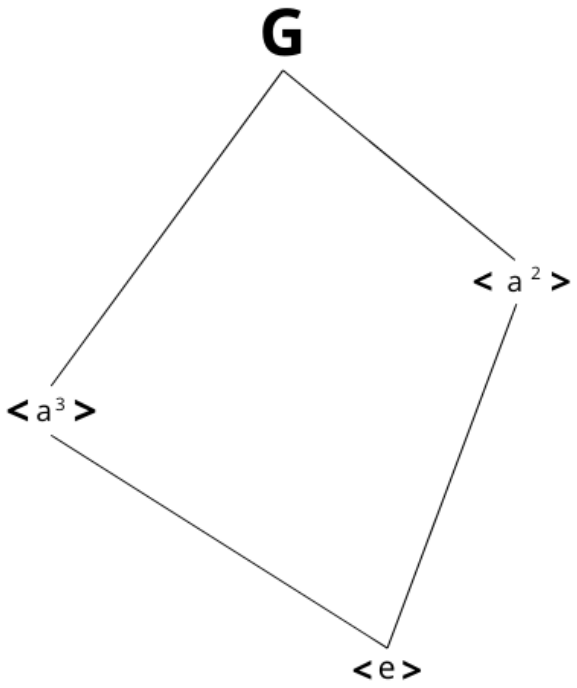
ii) $a^2.a^2 = a^4$; $a^4.a^4 = a^2$; $a^2.a^4 = a^6 = e$;

iii) $a^{-2} = (a^2)^{-1}$, $e = e^{-1}$.

No software GAP tal sugrupo está descrito como "$Group([a^2])$", como será visto abaixo.

$gap > G := CyclicGroup(IsFpGroup, 6);$
$< fpgroupofsize6onthegenerators[a] >$
$gap > Elements(G);$
$[< identity... >, a, a^2, a^3, a^4, a^5]$
$gap > K := AllSubgroups(G);$
$[Group([]), Group([a^3]), Group([a^2]), Group([a])]$
$gap > Elements(K);$
$[Group([]), Group([a]), Group([a^2]), Group([a^3])]$

Imagem 2: Reticulado do grupo G



Fonte: próprio autor.

Exemplo 3.13. Subgrupos do grupo de simetrias do quadrado (**C**);

Um exemplo de subgrupo de (**C**) é $K = \{Id, R_\pi\}$pois:

i) $id \in K$, por construção;

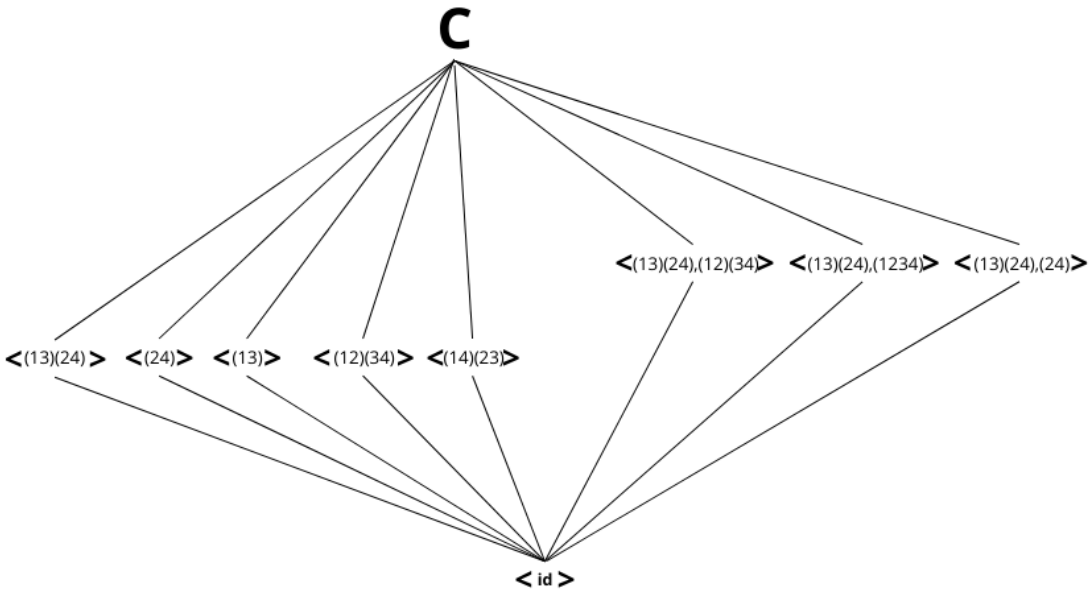
ii) Tomando R_π, R_π^{-1} temos $R_\pi \circ R_\pi^{-1} = R_\pi^{-1} \circ R_\pi = id$, onde $id \in K$;

iii) $R_\pi^{-1} = R_\pi$ e $id^{-1} = id$.

No software tal subgrupo (K) é descrito como "**Group([(13)(24)])**" e, de forma geral, ele nos apresenta os subgrupos da seguinte maneira:

$gap > R90 := (1,2,3,4);; R180 := R90^2;; R270 := R90^3;; R0 := ();;$
$gap > H := (1,2)(3,4);; D := H * R90;; V := H * R180;; N := H * R270;;$
$gap > C := Group(R90, H);$
$Group([(1,2,3,4),(1,2)(3,4)])$
$gap > Elements(C);$
$[(), (2,4), (1,2)(3,4), (1,2,3,4), (1,3),$
$(1,3)(2,4), (1,4,3,2), (1,4)(2,3)]$
$gap > T := AllSubgroups(C);$
$[Group(()), Group([(1,3)(2,4)]), Group([(2,4)]), Group([(1,3)]),$
$Group([(1,2)(3,4)]), Group([(1,4)(2,3)]), Group([(1,3)$
$(2,4),(2,4)]), Group([(1,3)(2,4),(1,2,3,4)]), Group([(1,3)(2,4),(1,2)(3,4)]),$
$Group([(1,3)(2,4),(2,4),(1,2,3,4)])]$

Imagem 3: Reticulado do grupo C



Fonte: próprio autor.

3.2.2 Classes laterais e Teorema de Lagrange

Consideremos G um grupo e $H \leq G$. Nesta seção, iremos definir uma relação de equivalência em G que dependerá do subgrupo H fixado e estudaremos as classes de equivalência dessa relação.

Para cada par $x, y \in G$ diremos que x é congruente a y módulo H se $x * y^{-1} \in H$, isto é,

$$x \equiv y(modH) \Leftrightarrow x * y^{-1} \in H.$$

A relação definida acima é uma relação de equivalência. De fato,

i) $x \equiv x(modH)$, para todo $x \in G$ pois $e = x * x^{-1} \in H$. Logo a relação é simétrica;

ii) Se $x \equiv y(modH)$ então $y \equiv x(modH)$, pois se $x * y^{-1} \in H$ então $x * y^{-1} = h_1 \in H$. Daí, $h_1^{-1} = y * x^{-1} = (x * y^{-1})^{-1} \in H$. Logo a relação é reflexiva;

iii) Se $x \equiv y(modH)$ e $y \equiv z(modH)$ então $x \equiv z(modH)$ pois, $x * y^{-1} \in H$ e $y * z^{-1} \in H$. Logo $(x * y^{-1}) * (y * z^{-1}) = (x * z^{-1}) \in H$ e daí que a relação é transitiva.

As classes de equivalência da relação definida acima são dadas por

$$\overline{x} = \{y \in G : y \equiv x(modH)\}.$$

Ou seja, se $y \in \overline{x}$ então $y * x^{-1} \in H$, isto é, $y * x^{-1} = h \in H$ e consequentemente $h * x = y$. Segue que

$$\overline{x} = \{h * x : h \in H\} = Hx,$$

onde Hx será denominada **uma classe lateral a direita de H em G** e de forma análoga constrói-se o conjunto $xH = \{x * h : h \in H\}$ denominado **uma classe lateral a esquerda de H em G**.

O conjunto quociente, que contém todas as classes laterais a direita da relação dada, será representado por

$$G/H = \{Hx : \ x \in G\}$$

e de forma análoga

$$G/H = \{xH : \ x \in G\}$$

descreve o conjunto para as classes laterais a esquerda.

Proposição 3.3. *Todas as classes laterais de H em G possuem a mesma cardinalidade de H.*

Demonstração:

Note que a função

$$f : H \to Hx$$

$$h \mapsto hx$$

é claramente sobrejetiva e tomando $h_1, h_2 \in H$ de modo que

$$h_1 * x = h_2 * x$$

logo

$$h_1 = h_2$$

e com isso temos que a função é também injetiva, ou seja, é bijetiva e daí $|H| = |Hx|$.

■

Dado um grupo G, dizemos que a **ordem** de G é n e escrevemos $|G| = n$ se G possui exatamente n elementos. Neste caso, dizemos que G é um grupo finito. No caso de grupos finitos um importante resultado, o Teorema de Lagrange, garante que qualquer subgrupo de um grupo finito tem ordem que divide a ordem do grupo.

Teorema 3.1 (Teorema de Lagrange)**.** *Se G é um grupo finito e H é um subgrupo de G então $|H|$ é um divisor de $|G|$, ou seja, a ordem de H é um divisor da ordem de G.*

Demonstração:
Considerando G um grupo finito e definida sobre G a relação de equivalência $\equiv (modH)$ temos que o conjunto quociente G/H é finito, daí

$$G/H = n \qquad \text{e} \qquad G/H = \{Hx_1, Hx_2, ..., Hx_n\}$$

Observe que $G = Hx_1 \dot{\cup} Hx_2 \dot{\cup} ... \dot{\cup} Hx_n$ e com isso $|G| = |Hx_1| + |Hx_2| + ... + |Hx_n|$
Segue da proposição anterior que $|G| = n|H|$, e portanto segue o resultado. ■

Segue do Teorema de Lagrange que a cardinalidade (ordem) de cada subgrupo do grupo dado é um divisor inteiro da cardinalidade do grupo. O GAP nos permite analisar todas as ordens, tanto do grupo quanto dos subgrupos com o comando "*Order*" e *List("grupo escolhido", "Order")*, respectivamente. Assim conseguimos observar tal relação descrita pelo teorema, observe os exemplos a seguir.

Exemplo 3.14. Ordem do grupo G_3 e de seus subgrupos visualizadas no GAP

$gap > G_3 := SymmetricGroup(3);$
$Sym([1..3])$
$gap > Order(G_3);$
6
$gap > L := AllSubgroups(G_3);$
$[Group(()), Group([(2,3)]), Group([(1,2)]), Group([(1,3)]), Group([(1,2,3)]),$
$Group([(1,2,3),(2,3)])]$
$gap > List(L, Order);$
$[1,2,2,2,3,6]$

Observe que o subgrupo "$Group([(1,2,3),(2,3)])$" tem a mesma cardinalidade de G_3, ou seja, ele coincide com G_3. Portanto G_3 é gerado pelos elementos (123) e (23).

Exemplo 3.15. Ordem do grupo G e de seus subgrupos visualizadas no GAP

$gap > G := CyclicGroup(IsFpGroup, 6);$
$< fpgroupofsize6onthegenerators[a] >$
$gap > Order(G);$
6
$gap > K := AllSubgroups(G);$
$[Group([]), Group([a^3]), Group([a^2]), Group([a])]$
$gap > List(K, Order);$
$[1,2,3,6]$

Exemplo 3.16. Ordem do grupo C e de seus subgrupos descritas no GAP

$gap > C := Group(R90, H);$
$Group([(1,2,3,4),(1,2)(3,4)])$
$gap > Elements(C);$
$[(), (2,4), (1,2)(3,4), (1,2,3,4), (1,3),$
$(1,3)(2,4), (1,4,3,2), (1,4)(2,3)]$
$gap > Order(G);$
8
$T := AllSubgroups(G);$
$[Group(()), Group([(1,3)(2,4)]), Group([(2,4)]), Group([(1,3)]),$
$Group([(1,2)(3,4)]), Group([(1,4)(2,3)]),$
$Group([(1,3)(2,4),(2,4)]),$
$Group([(1,3)(2,4),(1,2,3,4)]),$
$Group([(1,3)(2,4),(1,2)(3,4)]),$
$Group([(1,3)(2,4),(2,4),(1,2,3,4)])]$
$gap > List(T, Order);$
$[1,2,2,2,2,2,4,4,4,8]$

3.2.3 Classes de Conjugação

Se G é um grupo, vamos definir uma relação de equivalência em G como segue:

$$x, y \in G, x \sim y \Leftrightarrow \exists g \in G \text{ tal que } y = g^{-1}xg$$

Proposição 3.4. *Seja G um grupo. A relação "$\sim$" define uma relação de equivalência em G.*

Demonstração:

i) $x \sim x, \forall x \in G$, pois $x = e^{-1}xe$;

ii) Se $x \sim y$ então $y \sim x$.

Se $x \sim y$ existe $g \in G$ tal que $y = g^{-1}xg$. Assim, se $u = g^{-1}$ temos $x = u^{-1}yu$, isto é, $y \sim x$;

iii) Se $x \sim y$ e $y \sim z$ então $x \sim z$.

De fato, se $y = g^{-1}xg$ e $z = h^{-1}yh$, onde $g, h \in G$ temos $z = u^{-1}xu$, onde $u = gh$.

■

Se $x \sim y$ dizemos que x e y são **elementos conjugados** em G. Se denotarmos $g^{-1}xg = x^g$ são válidas as seguintes propriedades:

i) $x^e = x, \forall x \in G$;

ii) $y = x^g \Rightarrow x = y^{(g^{-1})}, \forall x, y, g \in G$;

iii) $(x^g)^h = x^{(gh)}, \forall x, g, h \in G$.

A classe $\overline{x} = \{y : x \sim y\} = \{x^g; g \in G\}$ é chamada **classe de conjugação (em G)** determinada pelo elemento $x \in G$. Vamos denotar a classe $\overline{x}$ por C_x.

Se G é um grupo finito e existem n classes de conjugação em G com representantes $x_1, x_2, ..., x_n$ então temos a união disjunta

$$G = C_{x_1} \dot{\cup} C_{x_2} \dot{\cup} ... \dot{\cup} C_{x_n}$$

e assim chegamos a chamada equação de classes:

$$|G| = |C_{x_1}| + |C_{x_2}| + ... + |C_{x_n}|$$

Exemplo 3.17. Classes de conjugação do grupo das permutações de ordem 3 (G_3). Observe que $C_{(1,2)} = \{(1,2), (2,3), (1,3)\}$, é uma classe de conjugação de G_3, sendo sua principal característica a relação de permutação de dois elementos. Note que:

i) $e\ (1,2)\ e = (1,2)$.

ii) $(2,3)(1,2)(2,3) = (1,3) \Rightarrow C_{(1,2)} = C_{(1,3)}$.

iii) $(1,3)(1,2)(1,3) = (2,3) \Rightarrow C_{(1,2)} = C_{(2,3)}$.

iv) $(1,2,3)(1,2)(1,2,3) = (1,2)$.

v) $(1,3,2)(1,2)(1,3,2) = (1,2)$.

vi) $(1,2)(1,2)(1,2) = (1,2)$.

Para obtermos todas as classes de conjugação de um grupo atribuído no GAP utilizamos a função "*Conjugacyclasses*". E como as classes de conjugação são classes de equivalência, mostramos que $C_{(1,2)} = \{(1,2), (2,3), (1,3)\}$. No GAP, tal classe de conjugação é descrita por "$(1,2)^G$". Vejamos abaixo como são descritas todas as classes de G_3.

$gap > G_3 := SymmetricGroup(3);$
$Sym([1..3])$
$gap > Elements(G_3);$
$[(), (2,3), (1,2), (1,2,3), (1,3,2), (1,3)]$
$gap > D := ConjugacyClasses(G_3);$
$[()^G, (1,2)^G, (1,2,3)^G]$

Exemplo 3.18. Classes de conjugação do grupo cíclico G gerado por a de ordem 6. Observe que C_{a^2} é uma classe de conjugação do grupo G. Lembremos que $G = \langle a \rangle$ pode ser identificado com o grupo $(\mathbb{Z}_6, +)$, de modo que com um abuso de notação, podemos fazer as seguintes identificações $\overline{0} = e; \overline{1} = a; \ldots; \overline{5} = a^5$. O elemento a^2 pode ser identificado com o elemento $\overline{2}$ no grupo aditivo $\mathbb{Z}_6$ e com isso, podemos determinar qual a classe de conjugação de $\overline{2}$, em particular. Vamos então analisar quais os elementos estão conjugados ao $\overline{2}$. Note que se

$$\overline{y} = \overline{g^{-1}} + \overline{2} + \overline{g}, \text{ onde } \overline{g} \in \mathbb{Z}_6$$

Temos

$$\overline{y} = \overline{g^{-1} + 2 + g}, \text{ onde } g^{-1} = -g$$

Portanto,

$$\overline{y} = \overline{2}.$$

Ou seja, $C_{\overline{y}} = C_{\overline{2}} = \{\overline{2}\}$ e com isso vemos que as classes de equivalência de $\mathbb{Z}_6$ na relação de equivalência determinada em $\mathbb{Z}$ pelo resto da divisão por 6 são as classes de conjugação de $\mathbb{Z}_6$ como grupo aditivo. No GAP tal classe de conjugação acima abordada é descrita por "a^{2^G}".

$gap > G := CyclicGroup(IsFpGroup, 6);$
$< fpgroupofsize6onthegenerators[a] >$
$gap > Elements(G);$
$[< identity... >, a, a^2, a^3, a^4, a^5]$
$gap > F := ConjugacyClasses(G);;$
$[< identity... >^G, a^G, a^{2^G}, a^{3^G}, a^{4^G}, a^{5^G}]$

Exemplo 3.19. Classes de conjugação do grupo das simetrias espaciais do quadrado (C)

Observe que $C_{(24)} = \{(12), (13)\}$ é uma classe de conjugação do grupo C, visto que:

i) $id\ (24)\ id = (24)$;

ii) $(24)(24)(24) = (24)$;

iii) $(1432)(24)(1234) = (13) \Rightarrow C_{(24)} = C_{(13)}$;

iv) $((12)(34))(24)((12)(34)) = (13) \Rightarrow C_{(24)} = C_{(13)}$;

v) $(13)(24)(13) = (24)$;

vi) $(1234)(24)(1432) = (13) \Rightarrow C_{(24)} = C_{(13)}$;

vii) $((13)(24))(24)((13)(24)) = (24)$;

viii) $((14)(23))(24)((14)(23)) = (13) \Rightarrow C_{(24)} = C_{(13)}$.

No GAP, tal classe de conjugação é representada pela notação "$(2,4)^G$". Vejamos como estão descritas as classes de conjugação do grupo C no software.

$gap > R90 := (1,2,3,4);; R180 := R90^2;; R270 := R90^3;; R0 := ();;$
$gap > H := (1,2)(3,4);; D := H * R90;; V := H * R180;; N := H * R270;;$
$gap > C := Group(R90, H);$
$Group([(1,2,3,4),(1,2)(3,4)])$
$gap > Elements(C);$
$[(), (2,4), (1,2)(3,4), (1,2,3,4), (1,3),$
$(1,3)(2,4), (1,4,3,2), (1,4)(2,3)]$
$gap > P := ConjugacyClasses(C);$
$[()^G, (2,4)^G, (1,2)(3,4)^G, (1,2,3,4)^G, (1,3)(2,4)^G]$

3.2.4 Subgrupos normais e grupos quocientes

Sejam G um grupo e H um subgrupo de G. Para cada $g \in G$, define-se a função γ_g (**conjugação pelo elemento** $g \in G$) por

$$\gamma_g : G \to G$$
$$x \mapsto \gamma_g(x) = g^{-1} * x * g$$

Note que $\gamma_g(H) = \{\gamma_g(h) : h \in H\} = \{g^{-1} * h * g : h \in H\}$. Vamos denotar a conjugação de um elemento h por g por h^g, isto é

$$\gamma_g(h) = h^g = g^{-1} * h * g.$$

Daí faz sentido denotarmos por H^g ou $g^{-1} * H * g$ o conjunto $\gamma_g(H) = \{\gamma_g(h) : h \in H\}$.

Vejamos que H^g é um subgrupo de G:

i) $e = e^g \in H^g$;

De fato, $\gamma_g(e) = g^{-1} * e * g = e$

ii) $h^g * h_1^g \in H^g, \ \forall \ h^g, h_1^g \in H^g$;

De fato $h^g * h_1^g = (g^{-1} * h * g) * (g^{-1} * h_1 * g) = g^{-1} * (h * h_1) * g \in H^g$

iii) $(h^g)^{-1} \in H^g,\ \forall\ h^g \in H^g$;

De fato, dado que $h^g \in H^g$ como $h \in H$, $h^{-1} \in H$ logo $(h^{-1})^g \in H^g$. Note que $(h^g) * (h^{-1})^g = (g^{-1} * h * g) * (g^{-1} * h^{-1} * g) = e$, ou seja, $(h^{-1})^g = (h^g)^{-1} \in H^g$

Observe que a função γ_g transforma subgrupos de G em subgrupos de G.

Definição 3.5. Diz-se que um subgrupo H em G é **normal** se $\gamma_g(H) = H^g \subseteq H,\ \forall g \in G$.

Suponhamos que $H^g \subseteq H, \forall g \in G$, vamos mostrar que $H \subseteq H^g, \forall g \in G$. De fato, dados $h \in H$ e $g \in G$, temos

$$h = g^{-1}(ghg^{-1})g \in g^{-1}(gHg^{-1})g \subseteq g^{-1}Hg.$$

Portanto, se H é um subgrupo normal de G, então $H^g = H$, para todo $g \in G$.

Observação 3.5. *Se H é um subgrupo normal de G denotaremos "$H \trianglelefteq G$".*

Exemplo 3.20. $\{e\}$ e G são subgrupos normais do grupo G;

Exemplo 3.21. Se G é um grupo abeliano então qualquer subgrupo H de G é normal.

Definição 3.6. Diz-se que um grupo $G \neq \{e\}$ é **simples** se e só se os únicos subgrupos normais de G são $\{e\}$ e G.

Algo que cabe ressaltar é o fato de que o GAP nos descreve quais são os subgrupos normais dos grupos estudados através da utilização do comando *"NormalSubgroups"*. Outro aspecto bastante importante trazido pelo software é o comando *"LatticeSubgroups"*, pois informa qual o número de classes de conjugação do grupo atribuído e também descreve o número de subgrupos atrelados, com isso alguns resultados podem ser obtidos mais rápidos graças a tal função, visto que alguns elementos estudados sobre teoria de grupos dependem exclusivamente da ordem do objeto analisado, como por exemplo o Teorema de Lagrange, e com essa função há a possibilidade de analisar informações diretas sobre o número de classes de conjugação e de subgrupos existentes, o que serve como catalisador para o processo de ensino-aprendizagem para formalizar inúmeras conjecturas propostas sobre a teoria de grupos.

Exemplo 3.22. Subgrupos normais do grupo das permutações de ordem 3 (G_3);

Observe que o subgrupo $A_3 = \{\mathrm{e}; (123); (132)\} = Alt([123])$ é subgrupo normal de G_3, pois:

i) $e\ (123)\ e = (123)$;

ii) $(132)(123)(123) = (123)$;

iii) $(12)(123)(12) = (132)$;

iv) $(13)(123)(13) = (132)$;

v) $(123)(123)(132) = (123)$;

i) $e\ (132)\ e = (132)$;

ii) $(132)(132)(123) = (132)$;

iii) $(12)(132)(12) = (123)$;

iv) $(13)(132)(13) = (123)$;

v) $(123)(132)(132) = (132)$;

O outro elemento de A_3 a ser analisado é e, no entanto, é fácil ver que o resultado da conjugação é o próprio e. Portanto $A_3 \trianglelefteq G_3$. Abaixo mostramos como o software nos apresenta os demais subgrupos normais de G_3.

$gap > G_3 := SymmetricGroup(3);$
$Sym([1..3])$
$gap > F := AllSubgroups(G_3);$
$[Group(()), Group([(2,3)]), Group([(1,2)]), Group([(1,3)]),$
$Group([(1,2,3)]), Group([(1,2,3),(2,3)])]$
$gap > D := ConjugacyClassesSubgroups(G_3);$
$[Group(())^G, Group([(2,3)])^G, Group([(1,2,3)])^G, Group([(1,2,3),(2,3)])^G]$
$gap > NormalSubgroups(G_3);$
$[Sym([1..3]), Alt([1..3]), Group(())]$
$gap > LatticeSubgroups(G_3);$
$< subgrouplatticeofSym([1..3]), 4classes, 6subgroups >$

Exemplo 3.23. Subgrupos normais do grupo cíclico G gerado por a de ordem 6.

Observe que o subgrupo $J = Group([a^3]) = \{a^3, e\}$ é subgrupo normal de G. De fato, utilizando a identificação de G com $(\mathbb{Z}_6, +)$, temos:

i) $\overline{0} + \overline{3} + \overline{0} = \overline{0 + 3 + 0} = \overline{3}$;

ii) $\overline{1} + \overline{3} + \overline{5} = \overline{1 + 3 + 5} = \overline{3}$;

iii) $\overline{2} + \overline{3} + \overline{4} = \overline{2 + 3 + 4} = \overline{3}$;

iv) $\overline{3} + \overline{3} + \overline{3} = \overline{3 + 3 + 3} = \overline{3}$;

v) $\overline{4}+\overline{3}+\overline{2}=\overline{4+3+2}=\overline{3}$;

vi) $\overline{5}+\overline{3}+\overline{1}=\overline{5+3+1}=\overline{3}$.

Portanto, $J \trianglelefteq G$. Abaixo, trazemos como o GAP nos descreve todos os subgrupos normais de G.

$gap > G := CyclicGroup(IsFpGroup, 6);$
$< fpgroupofsize6onthegenerators[a] >$
$gap > K := AllSubgroups(G);$
$[Group([]), Group([a^3]), Group([a^2]), Group([a])]$
$gap > C := ConjugacyClassesSubgroups(G);$
$[Group(< identity... >)^G, Group([a^3])^G, Group([a^2])^G, Group([a])^G]$
$gap > L := NormalSubgroups(G);$
$[Group(< fp, nogeneratorsknown >), Group(< fp, nogeneratorsknown >),$
$Group(< fp, nogeneratorsknown >), Group(< fp, nogeneratorsknown >)]$
$gap > Elements(L);$
$[Group([]), Group([a]), Group([a^{-2}]), Group([a^3])]$
$gap > LatticeSubgroups(G);$
$< subgroupplatticeof < fpgroupofsize6onthegenerators[a] >$
$, 4classes, 4subgroups >$

No exemplo anterior, ao calcularmos os subgrupos normais tivemos a frase *"no generators know"*, onde o software retornou os subgrupos, entretanto não descreveu os geradores de tais, para visualização mais precisa dos subgrupos normais utilizamos o comando *"Elements(L)"* e através disso o gerador de cada um foi descrito.

Exemplo 3.24. Subgrupos normais do grupo C.

Observe que o subgrupo $F = [(13)(24), (24)] = \{(), (13)(24), (13), (24)\}$ é subgrupo normal de C, pois:

i) $id\ (24)\ id = (24)$;

ii) $(24)(24)(24) = (24)$;

iii) $(1432)(24)(1234) = (13)$;

iv) $((12)(34))(24)((12)(34)) = (13)$;

v) $(13)(24)(13) = (24)$

vi) $(1234)(24)(1432) = (13)$;

vii) $((13)(24))(24)((13)(24)) = (24)$;

viii) $((14)(23))(24)((14)(23)) = (13)$.

i) $id\ (13)\ id = (13)$;

ii) $(24)(13)(24) = (13)$;

iii) $(1432)(13)(1234) = (24)$;

vi) $((12)(34))(13)((12)(34)) = (24)$;

v) $(13)(13)(13) = (13)$;

vi) $(1234)(13)(1432) = (24)$;

vii) $((13)(24))(13)((13)(24)) = (13)$;

viii) $((14)(23))(13)((14)(23)) = (24)$.

i) $id\ ((13)(24))\ id = ((13)(24))$;

ii) $(24)((13)(24))(24) = (13)(24)$;

iii) $(1432)((13)(24))(1234) = (13)(24)$;

vi) $((12)(34))((13)(24))((12)(34)) = ((13)(24))$;

v) $(13)((13)(24))(13) = (13)(24)$;

vi) $(1234)((13)(24))(1432) = (13)(24)$;

vii) $((13)(24))((13)(24))((13)(24)) = (13)(24)$;

viii) $((14)(23))((13)(24))((14)(23)) = (13)(24)$.

Observe que o último elemento de F a ser analisado é (), mas que claramente a conjugação resulta nele mesmo, portanto $F \trianglelefteq C$. Abaixo mostramos como o GAP nos descreve todos os subgrupos normais de C.

$gap > R90 := (1,2,3,4);; R180 := R90^2;; R270 := R90^3;; R0 := ();;$
$gap > H := (1,2)(3,4);; D := H * R90;; V := H * R180;; N := H * R270;;$
$gap > C := Group(R90, H);$
$Group([(1,2,3,4),(1,2)(3,4)])$
$gap > Elements(C);$
$[(), (2,4), (1,2)(3,4), (1,2,3,4), (1,3),$
$(1,3)(2,4), (1,4,3,2), (1,4)(2,3)]$
$gap > J := AllSubgroups(C);$
$[Group(()), Group([(1,3)(2,4)]), Group([(2,4)]), Group([(1,3)]),$
$Group([(1,2)(3,4)]), Group([(1,4)(2,3)]),$
$Group([(1,3)(2,4),(2,4)]), Group([(1,3)(2,4),(1,2,3,4)]), Group([(1,3)(2,4),$
$(1,2)(3,4)]), Group([(1,3)(2,4),(2,4),(1,2,3,4)])]$
$gap > T := ConjugacyClassesSubgroups(C);$
$[Group(())^G, Group([(1,3)(2,4)])^G, Group([(2,4)])^G, Group([(1,2)(3,4)])^G,$
$Group([(1,3)(2,4),(2,4)])^G, Group([(1,3)(2,4),(1,2,3,4)])^G,$
$Group([(1,3)(2,4),(1,2)(3,4)])^G, Group([(1,3)(2,4),(2,4),(1,2,3,4)])^G]$
$gap > NormalSubgroups(C);$
$[Group([(1,2,3,4),(1,2)(3,4)]), Group([(1,2,3,4),(1,3)(2,4)]),$
$Group([(1,4)(2,3),(1,3)(2,4)]), Group([(2,4),(1,3)(2,4)]),$
$Group([(1,3)(2,4)]), Group(())]$
$gap > LatticeSubgroups(C);$
$< subgrouplatticeofGroup([(1,2,3,4),(1,2)(3,4)]), 8classes, 10subgroups >$

Proposição 3.5. *Seja G um grupo, então:*

i) $N \trianglelefteq G \Leftrightarrow Ng = gN, \forall g \in G$ *onde* $gN = \{gn : n \in N\}$ *é uma classe lateral (à esquerda) de* N *em* G*;*

ii) $N, N_1 \trianglelefteq G \Rightarrow N \cap N_1 \trianglelefteq G$*;*

iii) $H \leq G$ *e* $N \trianglelefteq G \Rightarrow HN = \{h * n : h \in H, n \in N\}$ *é um subgrupo de* G*;*

iv) $N \trianglelefteq G, N_1 \trianglelefteq G \Rightarrow NN_1 \trianglelefteq G$*;*

v) $H \leq G, N \trianglelefteq G \Rightarrow H \cap N \trianglelefteq H$*.*

Demonstração:

i) Basta observar que $N^g = g^{-1} * N * g = N \Leftrightarrow Ng = gN, \forall g \in G$.

ii) Se x $\in N \cap N_1$ e $g \in G$ então $x \in N$ e $x \in N_1$. Daí, se $x^g \in (N \cap N_1)^g$, então $x^g \in N^g = N$ e $x^g \in N_1^g = N_1$, ou seja, $x^g \in N \cap N_1$. Assim $(N \cap N_1)^g = N \cap N_1, \forall g \in G$.

iii) Seja $H \leq G$ e $N \trianglelefteq G$, queremos provar que $HN = \{h * n : h \in H, n \in N\}$ é um subgrupo de G.
De fato,

a) $e \in H$, $e \in N \Rightarrow e * e = e \in HN$.

b) Considerando h_0n_0 e $h_1n_1 \in HN \Rightarrow (h_0n_0)(h_1n_1) = h_0(h_1h_1^{-1})(n_0h_1)n_1 \Rightarrow (h_0n_0)(h_1n_1) = (h_0h_1)(h_1^{-1}n_0h_1)n_1$, e se denotarmos $h = h_0h_1, n = n_0^{h_1} * n_1$ teremos $h \in H, n = n_0^{h_1} * n_1 \in N^{h_1} = N$ e assim,

$$(h_0n_0)(h_1n_1) = hn \in HN.$$

c) Tomando $r = hn \in HN \Rightarrow r^{-1} = n^{-1}h^{-1} = h^{-1}(h * n^{-1} * h^{-1})$, mas $h^{-1} \in H$ e $h * n^{-1} * h^{-1} = (n^{-1})^{h^{-1}} \in N^{h^{-1}} = N$, ou seja, $r^{-1} \in HN$.

iv) Basta observar que $\forall g \in G$ temos

$$(NN_1)^g = g^{-1} * (NN_1)g = (g^{-1}Ng)(g^{-1}N_1g) = N^gN_1^g$$

e como $N^g = N$ e $N_1^g = N_1, \forall g \in G$, segue que $(NN_1)^g = NN_1, \forall g \in G$.

v) Considerando $x \in H \cap N$ e $h \in H \Rightarrow x \in N$ e $x^h \in N^H = N$, como $x, h \in H$ segue imediatamente que $x^h \in H \cap N, \forall h \in H$.

■

Vamos utilizar a relação de equivalência definida anteriormente para trabalhar com o conjunto quociente daquela relação que poderemos, sob certa circunstância, muní-lo com estrutura de grupo. Este será chamado **grupo quociente**.

Seja G um grupo e $N \trianglelefteq G$. Sabe-se que

$$x, y \in G,\ x \equiv y(modN) \Leftrightarrow x * y^{-1} \in N$$

define uma relação de equivalência sobre G de modo que $G/N = \{\overline{g} : g \in G\}$ é o conjunto quociente de G por N e $\overline{g} = Ng = \{n * g : n \in N\}$ são as classes de equivalência da relação $\equiv (modN)$.

A proposição abaixo definirá uma operação no conjunto das classes G/N de modo que G/N seja um grupo com essa operação atribuída, sendo esse denominado **grupo quociente**.

Proposição 3.6. *Seja G um grupo e $N \trianglelefteq G$ então para quaisquer $x, y \in G$,*

$$\overline{x} * \overline{y} = \overline{x * y}$$

define uma operação no conjunto quociente G/N. Com essa operação, G/N é um grupo.

Demonstração:

Primeiramente provar-se-á que a operação está bem definida, isto é, não depende da escolha do representante da classe.

Dados $\overline{x} = \overline{a}$ e $\overline{y} = \overline{b}$, queremos mostrar que $\overline{x * y} = \overline{a * b}$, ou seja, queremos mostrar que

$$(x * y) \equiv (a * b)(mod N) \Leftrightarrow (x * y) * (a * b)^{-1} \in N \Leftrightarrow x * y * b^{-1} * a^{-1} \in N.$$

Mas note que, como $\overline{x} = \overline{a}$ e $\overline{y} = \overline{b}$ então

$$x * a^{-1} \in N, y * b^{-1} \in N.$$

Entretanto, se $x * a^{-1} = n_0 \in N$ e $y * b^{-1} = n_1 \in N$ então temos

$$x * n_1 * a^{-1} = (n_0 * a) * (n_1) * a^{-1} = n_0 * (a * n_1 * a^{-1})$$

E como $n_0 \in N$ e $a * n_1 * a^{-1} \in N^{a^{-1}} = N$. Segue de imediato que

$$x * n_1 * a^{-1} = x * y * b^{-1} * a^{-1} = (x * y) * (a * b)^{-1} \in N$$

.

i) Elemento neutro de G/N;

Tomando e elemento neutro de G tem-se que $\overline{e} * \overline{x} = \overline{e * x} = \overline{x} = \overline{x * e} = \overline{x} * \overline{e}$, para todo $\overline{x} \in G/N$.

ii) Associatividade em G/N;

Considerando $\overline{g}, \overline{h}, \overline{i} \in G/N$ tem-se que $\overline{g} * (\overline{h * i}) = \overline{g * (h * i)} = \overline{(g * h) * i} = \overline{g * h} * \overline{i}$.

iii) Elemento inverso em G/N;

Considerando $\overline{x} \in G/N \Rightarrow \overline{x} * \overline{x^{-1}} = \overline{x * x^{-1}} = \overline{e} = \overline{x^{-1} * x} = \overline{x^{-1}} * \overline{x}$.

Portanto, G/N com a operação atribuída é um grupo.

■

Exemplo 3.25. Conjunto quociente G_3/A_3

Seja

$$A_3 = \{e; (123); (132)\}, \text{ onde } A_3 \trianglelefteq G_3.$$

Note que $e^{-1} = e$, assim:

i) $e\ e = e$;

ii) $(123)\ e = (123)$;

iii) $(132)\ e = (132)$;

Logo:

$$\overline{e} = \{e; (123); (132)\};$$

Observe que $(12)^{-1} = (12)$, assim:

i) $(12)(12) = e$;

ii) $(13)(12) = (132)$;

iii) $(23)(12) = (123)$;

Logo:

$$\overline{(12)} = \{(12); (13); (23)\}$$

Portanto,

$$G_3/A_3 = \{\overline{e}; \overline{(12)}\}$$

Exemplo 3.26. Conjunto quociente G/V.

Seja

$V = \{\overline{2}; \overline{4}; \overline{0}\}$, onde $V \trianglelefteq G$ e considerando por abuso de notação $G = \mathbb{Z}_6$.

Note que $(a)^{-1} = (-a) = a^5$, assim:

i) $\overline{1} + \overline{5} = \overline{0}$;

ii) $\overline{3} + \overline{5} = \overline{2}$;

iii) $\overline{5} + \overline{5} = \overline{4}$;

Logo:

$$\overline{1} = \{\overline{1}; \overline{3}; \overline{5}\};$$

Observe que $(a^2)^{-1} = (-a^2) = a^4$, assim:

i) $\overline{2} + \overline{4} = \overline{0}$;

ii) $\overline{4} + \overline{4} = \overline{2}$;

iii) $\overline{0} + \overline{4} = \overline{4}$;

Logo:

$$\overline{2} = \{\overline{0}; \overline{2}; \overline{4}\};$$

Portanto,

$$G/V = \{\overline{1}, \overline{2}\}$$

Exemplo 3.27. Conjunto quociente C/F.

Seja

$$F = [(13)(24)] = \{\text{id}; (13)(24); (13); (24)\}, \text{ onde } F \trianglelefteq C.$$

Note que $id^{-1} = id$, assim:

i) $id\ id = id$;

ii) $((13)(24))\ id = (13)(24)$;

iii) $(13)\ id = (13)$;

iv) $(24)\ id = (24)$;

Logo:

$$\overline{id} = \{id; (13)(24); (13); (24)\};$$

Observe que $((12)(34))^{-1} = (12)(34)$, assim:

i) $((12)(34))((12)(34)) = id$;

ii) $(1234)((12)(34)) = (24)$;

iii) $(1432)((12)(34)) = (13)$;

iv) $((14)(23))((12)(34)) = (13)(24)$;

Logo:

$$\overline{(12)(34)} = \{(12)(34); (1234); (1432); (13)(24)\};$$

Portanto,

$$C/F = \{\overline{id}, \overline{(12)(34)}\}$$

Observe que cada um dos conjuntos quocientes (G_3/A_3, G/V e C/F) com a operação entre classes de equivalência definida na Proposição 3.6 é um grupo. Tal característica é bastante intuitiva pois podemos compreender que a operação entre as classes de equivalência se comportam com a dinâmica de "passarmos uma barra única" quando operamos dois elementos de cada grupo, resultando assim em algum elemento contido em cada grupo. Logo, pela relação de equivalência ($\equiv (modA_3)$, $\equiv (modV)$ e $\equiv (modF)$), sabemos que tais resultados estão contidos em alguma das classes de equivalência descritas anteriormente nos exemplos acima.

3.2.5 Homomorfismos de grupos

Sejam $(G, \bullet)$ e $(G', *)$ grupos e $\gamma : G \to G'$ uma aplicação de G em G'. Dizemos que γ é um **homomorfismo** se

$$\gamma(x \bullet y) = \gamma(x) * \gamma(y), \ \forall \ x, y \in G.$$

Se o homomorfismo $\gamma : G \to G'$ for bijetivo então γ é um **isomorfismo**. Neste caso diz-se que G é **isomorfo** a G', denotando-se $G \simeq G'$. E um isomorfismo $\gamma : G \to G$ é denominado **automorfismo** de G. O conjunto de todos os automorfismos de G é denotado por Aut$G$.

Exemplo 3.28. A aplicação

$$Id : G \to G$$

$$x \mapsto id(x) = x.$$

é, claramente, um homomorfismo de G

Exemplo 3.29. A função

$$e : G \to G^{'}$$

$$x \mapsto e(x) = e^{'}, \forall x \in G$$

.

chama-se **homomorfismo trivial**.

Demonstração:

Dados $x, y \in G$, temos $x \bullet y \in G$. Assim, $e(x \bullet y) = e^{'} = e^{'} * e^{'} = e(x) * e(y)$. ■

Exemplo 3.30. Seja $n \in \mathbb{Z}$ fixo. Então

$$\gamma_n : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$$

$$z \quad \mapsto \quad \gamma_n(z) = nz,$$

é um homomorfismo de G

Demonstração:

De fato, pois dado $x, y \in (\mathbb{Z}, +)$ temos:

$$x + y \in (\mathbb{Z}, +) \Rightarrow \gamma_n(x + y) = n(x + y) = \underbrace{(x + y) + \cdots + (x + y)}_{n \quad vezes} =$$

$$\underbrace{(x + x + \cdots + x)}_{n \quad vezes} + \underbrace{(y + y + \cdots + y)}_{n \quad vezes} = nx + ny$$

. ■

Exemplo 3.31. Seja $H \trianglelefteq G$. Então

$$\pi : G \to G/H$$

$$g \mapsto \pi(g) = gH$$

é um homomorfismo denominado **projeção canônica**.

Demonstração:

De fato, dados $x, y \in G$ temos:

$$xy \in G \Rightarrow \pi(xy) = xyH = \overline{x * y} = \overline{x} * \overline{y} = xHyH$$

■

Exemplo 3.32. Seja $g \in G$ fixo. Então

$$I_g : G \to G$$

$$x \mapsto I_g(x) = gxg^{-1}$$

é um automorfismo de G

Demonstração:

A priori, a função é claramente bijetiva, pois:

i) Dados $y, z \in G$ onde $gyg^{-1} = gzg^{-1}$ segue que $y = z$, tomando os inversos pela direita e pela esquerda.

ii) É sobrejetiva pelo fato de I_g ser injetiva e pelo fato do *contradomínio* de (I_g) ser o próprio G, logo o *contradomínio* de (I_g) é igual a *imagem* de (I_g).

Por fim, note que I_g é um homomorfismo pois, dados $y, z \in G$ temos:

$$yz \in G \Rightarrow I_g(yz) = g(yz)g^{-1} = (gyg^{-1})(gzg^{-1}) = I_g(y)I_g(z)$$

. ■

Exemplo 3.33. Considere os elementos $\alpha_1 = (\overline{0}; \overline{1})$, $\alpha_2 = (\overline{1}; \overline{0})$, $\alpha_3 = (\overline{1}; \overline{1})$, onde $\alpha_1, \alpha_2, \alpha_3 \in (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Então:

$$\begin{array}{ccc} f_i : (\mathbb{Z}/2\mathbb{Z}) & \to & (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\ \overline{0} & \mapsto & (\overline{0}; \overline{0}) \\ \overline{1} & \mapsto & \alpha_i \end{array}$$

é um homomorfismo injetivo, $\forall i = 1, 2, 3$.

Demonstração:
A priori, mostraremos que f_i é homomorfismo.

i) $\overline{0} + \overline{1} \in (\mathbb{Z}/2\mathbb{Z}) \Rightarrow f_1(\overline{0} + \overline{1}) = f_1(\overline{1}) = \alpha_1 = (\overline{0}; \overline{1}) = (\overline{0}; \overline{0}) + (\overline{0}; \overline{1}) = f_1(\overline{0}) + f_1(\overline{1})$;

ii) $\overline{0} + \overline{1} \in (\mathbb{Z}/2\mathbb{Z}) \Rightarrow f_2(\overline{0} + \overline{1}) = f_2(\overline{1}) = \alpha_2 = (\overline{1}; \overline{0}) = (\overline{0}; \overline{0}) + (\overline{1}; \overline{0}) = f_2(\overline{0}) + f_2(\overline{1})$;

iii) $\overline{0} + \overline{1} \in (\mathbb{Z}/2\mathbb{Z}) \Rightarrow f_3(\overline{0} + \overline{1}) = f_3(\overline{1}) = \alpha_3 = (\overline{1}; \overline{1}) = (\overline{0}; \overline{0}) + (\overline{1}; \overline{1}) = f_3(\overline{0}) + f_3(\overline{1})$.

Agora, provaremos que f_i é injetiva.

Sejam $x, y \in (\mathbb{Z}/2\mathbb{Z})$ tais que

$$f_i(x) = f_i(y),$$

onde $i = \{1, 2, 3\}$.

Tomando $i = 1$, sem perda de generalidade, temos:

$$f_1(x) = f_1(y) \Rightarrow f_1(x) - f_1(y) = (\overline{0}; \overline{0}) \Rightarrow f_1(x + (-y)) = (\overline{0}; \overline{0}) \Rightarrow x - y = 0 \Rightarrow x = y.$$

■

Proposição 3.7. *Seja G um grupo e f_1, $f_2 \in AutG$ então*

i) $f_1 \circ f_2 \in AutG$;

ii) $f_1^{-1} \in AutG$, sendo f_1^{-1} a aplicação inversa de f_1.

Demonstração:

i) Basta mostrar que a composição de aplicações que estão em Aut$G$ descreve um homomorfismo. De fato,

$$f_1 \circ f_2(x * y) = f_1(f_2(x * y)) = f_1(f_2(x) * f_2(y)) = f_1(f_2(x)) * f_1(f_2(y)) = f_1 \circ f_2(x) * f_1 \circ f_2(y),$$

logo $f_1 \circ f_2 \in$ Aut$G$, pois a composição de aplicações bijetivas é também bijetiva.

ii) Considerando que $f_1 \in$ Aut$G$ então $\forall x', y' \in G$ existem $x, y \in G$ de modo que $f_1(x) = x'$ e $f_1(y) = y'$. Como f_1 é bijetiva, então existe f_1^{-1} tal que

$$f_1^{-1}(x' * y') = f_1^{-1}(f_1(x) * f_1(y)) = f_1^{-1}(f_1(x * y)) = (f_1^{-1} \circ f_1)(x * y) = x * y = f_1^{-1}(x') * f_1^{-1}(y').$$

Portanto $f_1^{-1} \in$ Aut$G$.

■

Teorema 3.2 (Teorema do Homomorfismo)**.** *Sejam G e G' grupos com identidades e,e' respectivamente e $\gamma : G \to G'$ um homomorfismo. Então*

i) $Im(\gamma) = \gamma(G) = \{\gamma(g) : g \in G\}$ *é um subgrupo de* G'*;*

ii) $N(\gamma) = \{g \in G : \gamma(g) = e'\}$ *é um subgrupo normal de* G *chamado* ***núcleo*** *do homomorfismo* γ*, e mais*

$$\gamma \text{ é injetiva} \iff N(\gamma) = \{e\};$$

iii) $G/N(\gamma) \simeq Im(\gamma)$.

Demonstração:

i) $e' = \gamma(e) \in \mathrm{Im}(\gamma)$ pois $e \bullet e = e \Rightarrow \gamma(e) * \gamma(e) = \gamma(e) \Rightarrow \gamma(e) = e^{'} \in \mathrm{Im}(\gamma)$, logo $\mathrm{Im}(\gamma) \neq \varnothing$.

Observe que $\gamma(g_1), \gamma(g_2) \in \mathrm{Im}(\gamma) \Rightarrow \gamma(g_1) * \gamma(g_2)^{-1} \in \mathrm{Im}(\gamma), \forall g \in G$.
E isto demonstra que $\mathrm{Im}(\gamma)$ é subgrupo de G, visto que satisfaz de forma sintática a definição de subgrupo.

ii) Note que $e \in N(\gamma)$, pois $\gamma(e) = e'$.

Dados $g_1, g_2 \in \mathrm{N}(\gamma)$, temos que

$$\gamma(g_1 \bullet g_2) = \gamma(g_1) * \gamma(g_2) = e' * e' = e' \Rightarrow g_1 \bullet g_2 \in N(\gamma).$$

Temos que se $g \in \mathrm{N}(\gamma)$ então

$$\gamma(g^{-1}) = \gamma(g)^{-1} = (e')^{-1} = e' \Rightarrow g^{-1} \in N(\gamma).$$

Considere $n \in N(\gamma)$ e $g \in G$, daí

$$\gamma(g^{-1} \bullet n \bullet g) = \gamma(g^{-1}) * \gamma(n) * \gamma(g) = \gamma(g^{-1}) * e' * \gamma(g) = e'$$

isto é, $g^{-1} \bullet n \bullet g \in \mathrm{N}(\gamma)$, para todo $n \in N(\gamma)$ e para todo $g \in G$.

Portanto $\mathrm{N}(\gamma)$ é um subgrupo normal de G.
Agora, se $g_1, g_2 \in G$

$$\gamma(g_1) = \gamma(g_2) \Leftrightarrow \gamma(g_1) * \gamma(g_2)^{-1} = e' \Leftrightarrow \gamma(g_1 \bullet g_2^{-1}) = e^{'} \Leftrightarrow g_1 \bullet g_2^{-1} \in N(\gamma),$$

e dai segue de imediato o item (ii) do Teorema 3.2.

iii) Consideremos $\overline{G} = G/\ \mathrm{N}(\gamma)$ e $N = \mathrm{N}(\gamma) \trianglelefteq G$ defina a função

$$\begin{aligned} \overline{\gamma} : \overline{G} &\to \mathrm{Im}\gamma \\ \overline{g} &\mapsto \gamma(g) \end{aligned}$$

Primeiramente, veremos que $\overline{\gamma}$ está bem definida, basta observar que

$$\overline{g} = \overline{h} \Rightarrow Ng = Nh,$$

e daí

$$g \bullet h^{-1} \in N \Rightarrow \gamma(g \bullet h^{-1}) = e' \Rightarrow \gamma(g) * \gamma(h)^{-1} = e',$$

ou seja, $\gamma(g) = \gamma(h)$.

A função é claramente sobrejetiva, pois $\mathrm{Im}\overline{\gamma} = \mathrm{Im}(\gamma)$.

Observe que $\overline{\gamma}$ é homomorfismo, pois

$$\overline{\gamma}(\overline{x} \bullet \overline{y}) = \overline{\gamma}(\overline{x \bullet y}) = \gamma(x \bullet y) = \gamma(x) * \gamma(y) = \overline{\gamma}(\overline{x}) * \overline{\gamma}(\overline{y}).$$

Note que

$$\overline{\gamma}(\overline{x}) = e^{'} \Rightarrow \gamma(x) = e^{'} \Rightarrow x \in N \Rightarrow \overline{x} = \overline{e},$$

ou seja, $\mathrm{N}(\overline{\gamma}) = \overline{e}$ e com isso $\overline{\gamma}$ é injetiva e portanto $\overline{G} \simeq \mathrm{Im}\gamma$.

■

Considerações finais

O material desenvolvido teve como objetivo fomentar um maior uso de tecnologias de informação, em particular o GAP, em disciplinas de matemática com caráter mais abstrato, como a álgebra e, consequentemente, a teoria de grupos. A utilização de tecnologias de informação no processo de ensino e aprendizagem tem se tornado um tema substancial e necessário para ser abordado e estudado, com o intuito de efetivar tais aplicações no cotidiano educacional. Nesse contexto, nosso trabalho de conclusão de curso surge como um "ponto de partida" para incrementar essa nova tendência de processo educacional, possibilitando o desenvolvimento de novos horizontes e a elaboração de novos materiais.

Outro aspecto relevante a ser salientado é o fato de tal material também servir como uma "introdução" para pesquisadores matemáticos, visto que o software abordado possui uma biblioteca extensa que permite realizar estudos sobre diversas estruturas algébricas, conforme bem desenvolvido por (HULPKE, 2011). Assim, através do que foi apresentado no escopo deste trabalho, o leitor estará munido dos preceitos fundamentais presentes nos comandos dos algoritmos gerados no GAP.

Esperamos, portanto, que este trabalho possa contribuir de forma eficaz e eficiente para o processo de ensino e aprendizagem de álgebra na formação do matemático, fornecendo-lhe os fundamentos teóricos e tecnológicos necessários para desenvolver-se na área da matemática em que decidir atuar. O material desenvolvido, com sua "dupla visão" (teórico-prática), visa contribuir para o desenvolvimento do pensamento algébrico no estudante e, como consequência, melhorar a vida das pessoas que serão atendidas por esse profissional.

Referências

ALTOE, T. J. *Grupos e corpos com aplicações em GAP*. 2017. Trabalho de conclusão de curso (bacharelado em matemática), Instituto de Ciências Exatas, Universidade Federal Fluminense, Volta Redonda, Brasil. 19

GAP. *Groups, Algorithms, Programming - a System for Computational Discrete Algebra*. 2011. Disponível em: <https://www.gap-system.org>. 18, 19

GARCIA, A.; LEQUAIN, Y. *Elementos de álgebra*. Rio de Janeiro: Projeto Euclides. 5. ed. IMPA, 2008. 24

GONCALVES, A. *Introdução à Álgebra*. Rio de Janeiro: Projeto Euclides, IMPA, 2006. 24

HULPKE, A. Abstract algebra in gap. *United States: CreativeCommon*, 2011. 23, 24, 58

IFES. *Disciplina "Álgebra"*. 2020. Disponível em: <https://www.ifes.edu.br/images/stories/-publicacoes/cursos/graduacao/Cachoeiro/ppc-lic-matematica-cachoeiro-vigente-a-partir-de-2020.pdf>. 17

IFES. *Disciplina "Álgebra 2"*. 2020. Disponível em: <https://www.ifes.edu.br/images/stories/-publicacoes/cursos/graduacao/Vitoria/PPC-matem%C3%A1tica-vitoria-vigente-2020.pdf>. 17

MONDINI, F.; BICUDO, M. A. A presença da Álgebra nos cursos de licenciatura em matemática no estado do rio grande do sul. *Acta Scientiae, p. 51*, 2010. 12

PEREIRA, B. T. O uso das tecnologias da informação e comunicação na prática pedagógica da escola. *Curitiba: Secretária da Educação*, 2010. 18

SANTOS, A. R. d.; SANTOS, P. C. S. d. O programa gap como ferramenta de ensino e aprendizagem de Álgebra e uma reflexão das dificuldades da disciplina Álgebra i. *Universidade Federal de Goiás/Regional Catalão*. 18

SOARES, N. C.; BIANCHINI, B. L. Tópicos de teoria de grupos nos cursos de licenciatura em matemática. *Rev. Prod. Educ. Matem., São Paulo, v.8, n.1, pp. 87-95*, 2019. 12

SOUZA, J. A. Uma nota sobre a teoria dos grupos: da teoria de galois à teoria de gauge. *Rev. Bra. de Hist. da Mat.- vol. 12 nº24 - pág 71-81*, 2012. 11

UFES. *Disciplina "Álgebra II"*. 2013. Disponível em: <https://matematicaindustrial.saomateus.ufes.br/sites/matematicaindustrial.saomateus.ufes.br/files/field/anexo/matematica_industrial_ufes_-_ppc_2013.pdf>. 17

UFES. *Disciplina "Introdução a teoria de grupos"*. 2017. Disponível em: <https://matematica.alegre.ufes.br/sites/matematica.alegre.ufes.br/files/field/file/ppc-matematica-lic-ufes-ccens-alegre-versao-2017.pdf>. 15

UFES. *Disciplina "Elementos de álgebra"*. 2018. Disponível em: <https://prograd.ufes.br/sites/prograd.ufes.br/files/field/anexo/ppc_matematica_lic_ceunes.pdf>. 17

UFES. *Disciplina "Álgebra I"*. 2018. Disponível em: <https://matematica.ufes.br/sites/matematica.ufes.br/files/field/anexo/ppc_bach_matem_cce_2017_versao_colmat_0.pdf>. 15, 16

UFES. *Disciplina "Álgebra I"*. 2018. Disponível em: <https://matematica.ufes.br/sites/matematica.ufes.br/files/field/anexo/resolucao_e_anexo_de_resolucao_matematicalicenccce_2018_finalizado.pdf>. 15, 16