ELEMENTOS

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

Edufac

Ano - 2011

ELEMENTOS: REVISTA DE ENSINO E PESQUISA EM CLASSES, OPERAÇÕES E PROPRIEDADES DE ESTRUTURAS ALGÉBRICAS. Rio Branco: Edufac, 2011- Anual. ISSN

Ficha catalográfica elaborada pela Biblioteca Central da UFAC.

B546e

Elementos: Revista de Ensino e Pesquisa em Classes, Operações e Propriedades de Estruturas Algébricas.
V. 1, Nº. 1 (jan./dez. 2011) – Rio Branco: Edufac, 2011.

Anual
ISSN: 0000.0000(on line)

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

CDD: 512
CDU: 512

Marcelino G. M. Monteiro CRB/11 - 258

Associação Brasileira
das Editoras Universitárias

Edufac

Editora da Universidade Federal do Acre

Revista
ELEMENTOS

Objetivo e Política Editorial

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

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

APRESENTAÇÃO

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

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

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

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

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

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

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

Os Editores
e-mail: elementos@ufac.br

Editorial

A Universidade Federal do Acre (UFAC), através de sua Editora, tem incentivado a criação das revistas eletrônicas, como forma de divulgar a produção de conhecimentos gerados no âmbito da Instituição. Dessa forma, os registros de trabalhos já realizados podem ser colocados para a comunidade acadêmica de forma mais imediata, evitando, por exemplo, os custos de impressão.

O Comitê Científico da revista *ELEMENTOS*, que tem a maior parte de seus representantes dentro do GEPCOPEA, entendeu que esse seria o momento oportuno de criação da revista. Entendendo também que a regularidade de suas edições e a responsabilidade com seus conteúdos poderão, no futuro, fazer com que a mesma receba pareces favoráveis à sua manutenção.

A divulgação da pesquisa em Matemática não pode deixar de considerar a forma séria e responsável com que devem ser tratados os objetos e conceitos já estabelecidos, que se acumulam de maneira compatível e organizada durante décadas e décadas.

Na Álgebra, podemos encontrar uma riqueza incomensurável de caminhos para o raciocínio lógico. A compreensão de que qualquer argumentação deva se pautar nas características dos objetos manipulados é uma forte aliada a quem se dispõe a escrever sobre esses assuntos.

A edição "Ano 2011" desta revista traz algumas notas relacionadas com estudos bastante significativos. A entrevista com um pensador, ex-professor de nossa Instituição, se constitui numa agradável leitura que dá uma idéia de sua atuação frente à sala de aula, de como o mesmo vê o mundo e a relação entre a academia e a comunidade a qual ela serve.

José Ivan da Silva Ramos

(Professor efetivo do CCET/UFAC)

SEÇÕES

I - ENTREVISTA

Professor João Batista de O. Sobrinho

A OPÇÃO POR MATEMÁTICA

Eu queria ser um astrônomo. Mas na minha tão pequenina e tão distante cidade restou-me estudar matemática, física, química e biologia. Sou portador da síndrome do autismo, mais precisamente da sua particularidade, síndrome de Asperger. Por esse motivo tenho forte deficiência com a minha comunicação. Por mais que eu escreva uma palavra ou uma frase de maneira correta, no dia seguinte volto a me perder nas regras gramaticais. Autismo é um desenvolvimento atípico onde regiões do cérebro parecem auto dinamizar-se, e, regiões, parecem não se complementarem. A minha mãe dizia que as minhas frases iniciais eram do tipo: "O meu irmã está vindo pegar mim". Tenho certeza que leio o universo em uma linguagem diferenciada. As interpretações de um autista fizeram os estudiosos entenderem melhor o quanto uma comunicação trata da subjetividade de uma idéia. E a matemática, o que tem a ver com isso? Por que os autistas, quase todos têm um bom relacionamento com os números? Consigo responder que é por se tratar da linguagem mais primitiva, mais intuitiva e mais simples das nossas inter-relações com o próprio universo. A matemática é a naturalidade dos nossos próprios sentidos. No silêncio do meu mundo ela foi sempre as palavras da minha estrada. Não pode! Estudar matemática a partir das suas regras faz nossa vida se tornar ingrata e reversa.

A ESCOLA, A VIDA DO ALUNO E O MÉTODO ADEQUADO DE ENSINO

Nos anos 70, li um livro escrito pelo pedagogo mais importante dos EUA, na época. A sua maior ênfase era sobre o quanto o ambiente de uma sala de aula não condiz com o bem estar de um aluno. Ele fazia comparações sobre o cansativo conforto de uma criança em sala de aula e sobre o seu prazeroso esforço em um jogo de futebol. É a escola distante dos sentidos da própria vida. Isto me chama muita atenção porque, no meu mundo as salas de aulas muito me torturavam. O mundo do autismo é um lugar sem as pessoas e, numa sala de aula, eu restava sem as pessoas e sem o meu próprio lugar. Eu restava sem mais nada. Escrevi um livro, ainda não publicado, formado por 40 textos.

Creio que com ele eu faça entender o quanto a escola é imprópria para pessoas com os meus problemas, por exemplo. Entendo que a própria genética teve o devido cuidado de dar a cada pessoa o seu particular autismo. Não quero jamais esquecer: Entre tantas contradições, foi na escola onde encontrei guarida e complementação para o meu desenvolvimento. Em meio as minhas dificuldades, as professoras e a minha mãe, que também me ensinava as lições, elas se admiravam com a facilidade que eu operava os cálculos matemáticos. Quando eu leio o número como, por exemplo, o número 753, imediatamente, na minha mente eu o decomponho nas unidades de centenas, unidades de dezenas e unidades simples. De imediato, no seu devido sistema decimal, eu passo a visualizá-lo em formas e cores. Uma representação numeral quando compilada assim, em uma apresentação material, mesmo que imaginária, os cálculos matemáticos tornam-se mais compreensivos e muito mais seguros.

Somente quando eu tinha 19 anos de idade, estudando ainda a sétima série do ensino básico, tive a compreensão de que deveria ler e resolver todos os livros didáticos, a partir do primeiro aninho escolar. E assim, passei a me entender com os professores. Antes, tudo foi uma história de reprovações, suspensões e expulsões, apesar da minha característica de calmo. Passei a ser um ótimo e respeitado aluno. É claro que ao assumir a posição de professor, essa minha nova estrada me encaminhou para me tornar um profissional tolerante e compreensivo. Talvez os nossos sofrimentos aqui nesta nossa Terra sejam apenas uma leitura para uma melhor compreensão do que seja o céu.

Um professor tem muito o que contar. Talvez pessoas como eu, que um dia conseguiu chegar à academia, tenham muito mais o que falar. Será que esses meus alunos, hoje tão importantes Doutores da UFAC, que voltam e procuram este velho aposentado, será que eles precisaram mesmo dos meus recados? Senhores Doutores, quero vos dizer que muito mais ficaram comigo aqueles que, eu e eles, não conseguimos. Eles ainda são meus amigos. Alguns se tornaram alcoólatras e, quando nos encontramos por aí, pelos bairros, pelas beiras dos mercados, ainda conversamos e ainda filosofamos. Peço a vocês que, com muito carinho e cuidado, olhem para os seus alunos chamados de reprovados.

Mesmo que se trate de alguém fracassado, ele ainda é uma pessoa. Quando tudo já nos parece perdido, na verdade, apenas temos o mundo a nos oferecer uma oportunidade sagrada para participarmos da reconstrução da vida. Não existe prova para quem ainda nada sabe. Nunca olhei para um aluno como reprovado. Em cada vez que assim eu fui classificado nunca acreditei que as portas do mundo pudessem ser fechadas.

Infelizmente a metodologia de ensino adotada pela escola fundamenta-se no sucesso ou fracasso das notas das provas. As notas, o retrato da construção erguida pelo próprio sistema, quando feias, são pechadas ao próprio aluno. No Mundo dos passarinhos não existe culpa aos seus filhinhos por eles não chegarem voando aos seus ninhos. Muito menos, os passarinhos inventaram a construção do "diabo" pela culpa dos seus pecados. Quem sabe, talvez tudo nosso tenha ainda a ver com a nossa dificílima "competição espermatozóica". A sobrevivência escolar não tem sido tão diferente. Talvez seja preciso aprender um pouco mais com o dom materno na sua proteção ímpar para com o que seja apenas um único e tão querido ovo.

Quem sabe, esses meus alunos: Ivan, Ronaldo, Sergio e demais, tenham apenas a me agradecer pelas nossas muitas e muitas conversas e, de principal, eu tenha apenas lhes oportunizado e exigido que eles lessem e resolvessem os livros didáticos.

Esse importante pedagogo ao qual eu me referi anteriormente, assim com também Carl Sagan, o afamado astrônomo do projeto "Cosmos", fazem, nos seus trabalhos, fortes referências ao pai da imprensa, João Gutenberg, que nos oportunizou o livro ao alcance de todos. Foi a luz em que a humanidade iluminou-se no "RENASCIMENTO".

Muito mais do que a explosão do Renascimento, hoje estamos no olho do hiperfuracão chamado Internet. Agora, os terráqueos simplesmente integraram-se ao universo. Hoje, cada cérebro é uma janela aberta ao infinito. Tudo nosso tornou-se dados integrados ao cosmos. O paciente passou a conhecer a sua doença melhor do que o seu próprio médico.

Tive a sorte de ser professor da Senadora Marina, do Ex-Governador Arnóbio Marques, do Governador Tião Viana, da Médica Célia Mendes e de muitas outras pessoas queridas da nossa comunidade. Apesar de tudo, muito mais perto do coração da gente, restaram aqueles que se atrapalharam e, com os quais precisamos, por demais, conversar sobre as suas vidas quase sempre tão carentes.

A DOCÊNCIA NA UNIVERSIDADE E A POSSIBILIDADE DE ESTUDOS APROFUNDADOS

Ao concluir a licenciatura em matemática fui contratado pela UFAC como professor, contudo, condicionado a fazer uma especialização em Manaus, dentro de um projeto oferecido pela Universidade Federal do Amazonas, administrado pelos irmãos Tribuzi. Na época, no Estado do Acre, não tínhamos Doutores para a realização de projetos desse porte. Como aluno dos Professores Tribuzi eu tive a oportunidade de obter respostas para muitas das minhas curiosidades.

Me lembro das várias vezes em que o professor Ivan Tribuzi parou a aula para responder perguntas minhas. Me lembro depois de algumas delas ele falou: "Esta eu vou responder regada a Champanhe". Uma dessas perguntas foi querer saber quais eram os princípios da própria matemática, já que as suas particularidades eram axiomáticas (quando tudo é provado a partir de princípios intuitivos). Gostei muito de tudo que ouvi do Doutor Tribuzi. Ele expôs que a matemática se sustenta sobre três esteios: O probabilístico, o algébrico e o geométrico. Nesse curso tive a oportunidade de entender melhor o quanto a linguagem das funções é uma comunicação para a compreensão do próprio universo. Que, na última série do ensino fundamental, com o estudo das funções, o aluno tem a oportunidade de iniciar a alfabetização da comunicação e que somente com ela é possível entender o nosso modernismo científico.

Infelizmente a própria escola insinua que a matemática seja apenas as quatro operações. Fico preocupado e triste pelos alunos não serem orientados de que, sem o estudo da matemática do ensino médio, seja impossível entender o que seja “um computador” em sua máquina e em sua linguagem. No estudo das funções, junto aos isomorfismos, com a teoria de Galoi é possível a gente ler sobre o nosso universo quântico e entender o quanto somos as mesmas propriedades das demais dimensões. É uma oportunidade para um melhor contato com Deus. É bem natural que a partir daqui um matemático seja chamado de louco.

A ESTRUTURA EDUCACIONAL

Um dia conversando com um velho amigo ele me reclamou sobre o quanto tudo está por aí tão falsificado. Todavia, ele me afirmou que o homem ainda não tinha conseguido corromper uma galinha. Esse amigo me garantiu que um ovo não consegue ser formado sem que nele não esteja presente o mínimo das suas substâncias fundamentais. Um dia, todos nós fomos também um ovo. Para estarmos aqui foi preciso passar por um controle de qualidade. Como professor, fiquei a pensar qual é mesmo a nossa responsabilidade com a qualidade e a integralidade do aluno a partir do jardim de infância até à universidade. A escola é desconexa. Até mesmo o ensino fundamental é formado por um grande abismo entre a quarta e a quinta série. De série para série o conteúdo dos livros didáticos é de excelentíssima qualidade. Todavia, a escola não tem conseguido um bom resultado com a sua aplicabilidade.

O PROFESSOR UNIVERSITÁRIO

Eu imaginava que a universidade, em si, fosse um centro dinâmico e contagiante da seletividade dos conhecimentos. Tudo que nela encontrei foi um lugar de profundo silêncio. Perguntava-me: Aonde vou conversar com os sábios de ontem e os sábios de hoje? Perguntava: Em qual é a sala na qual estarei bem informado? A biblioteca era algo impróprio, quente, quando não, barulhento, burocrático ou interditado. Digo, sem um pingo de medo: As esquinas dos botecos eram lugares muito mais aconchegantes e muito mais intelectualizados, mesmo para mim que não fumava e nem bebia! Apesar de tudo, peço desculpas à escola porque, mesmo assim, foi com ela que eu tive todas as minhas vitórias. Foi com ela que eu aprendi a ter coragem de falar dos sentimentos da minha alma. Quando se reclama por uma melhora não se merece uma degola.

A UNIVERSIDADE HOJE

Quando cheguei à universidade, tanto como aluno ou como professor, fiquei surpreso o quanto o seu modelo está muito mais para encapsulação do conhecimento do que para a integração com a comunidade.

A palavra universidade, aqui em seu amplo contexto, se tornou bem diferente do seu histórico lugar dos discursos e dos conhecimentos. Ainda bem que o próprio universo é semântico, enquanto entendemos que "semânticas" sejam as nossas palavras. É assim que o próprio conhecimento iluminou-se nas frestas da internet. As portas dos nossos mosteiros tornaram-se transparentes à luz e ao vento. Os cursos não mais serão provas de medo e sacrifícios. É muito curioso observar que a expansão do ensino que acontece agora no Brasil, tenha sido providência de alguém que não teve oportunidade, mas que, muito mais acreditou na universidade.

CONSIDERAÇÕES FINAIS

Eu esperava encontrar, na universidade, um discurso integrado com a sua característica de universalidade. Mas, tudo que vi foi uma distância muito grande para com o próprio homem. Encontrei a escola muito mais distante da realidade. Não se pode esperar que uma escola infantil revolucione a nossa apatia. O ensino é algo atípico. É uma construção que se ergue de cima para baixo. A universidade precisa descer do seu pedestal ao encontro de si mesma, enquanto ela é uma criança e, muito mais ao encontro de si mesma, enquanto, lá muito longe, a universidade não é nem mesmo alfabetizada. Como professor, muitas vezes eu tenho inveja dos engenheiros que são presos quando deixam ruir um prédio que se propuseram a construir.

É uma questão de felicidade esta revista poder quebrar um pouco desse nosso tão ensurdecedor silêncio.

Quase Vazios mas Puros de Raciocínio

(Dedicado ao meu filho Emanuel)

por

José Ivan da Silva Ramos

(Doutor em Álgebra e membro efetivo do Centro de Ciências Exatas e Tecnológicas da Universidade Federal do Acre)

Resumo

As experiências aqui relatadas se baseiam nas observações que fiz durante alguns anos trabalhando com ensino de Matemática. O texto aqui apresentado foi motivado por uma ação junto a escolas de ensinos fundamental e médio da rede pública e pelo acompanhamento que tenho feito no intuito de verificar o quanto uma criança é capaz de se utilizar da abstração para compreender o mundo das formas e das quantidades (números).

Abstract

The experiments reported here are based on observations made during a few years working with the teaching of mathematics. The text presented here was motivated by a complaint to the schools of primary and secondary education in the public and for monitoring I have done in order to chek how much a child is able to use abstraction to understand the world of forms and quantities (numbers).

Palavras Chaves: Extensão, Escola, Alunos, Investigação, Educadores, Aritmética, Equações e Abstração.

Introdução: Justificativa e Objetivos

Desde a década de 90, precisamente, a partir de 1994, tenho acompanhado vários alunos de cursos de graduação, especialmente os alunos do Curso de Matemática. Mais recentemente, preocupado com o desempenho desses alunos, no início de suas graduações, desde 2004, venho, a cada dois anos, trabalhando alguns temas ligados às Estruturas Algébricas, em Cursos de Extensão, planejados para a comunidade acadêmica de Rio Branco. O primeiro curso intitulado *Grupos Cíclicos*, foi ministrado em 2004, quando atuei como coordenador e professor. Em 2006, movido pelo fato de um dos alunos desse curso ter atingido a motivação suficiente para continuar estudando, sob minha orientação, e conseguir a aprovação na seleção do Mestrado em Matemática da Universidade Federal do Ceará-UFC, mesmo não tendo concluído o 4º período de sua graduação de Licenciatura, elaborei uma nova proposta para desenvolver outra ação mais direcionada para alunos do Ensino Médio. O segundo curso, *A Influência da Teoria dos Conjuntos no Desenvolvimento de Alguns Conceitos Matemáticos*, recebeu um número satisfatório de inscrições, e uma quantidade razoável de alunos do ensino médio, que conseguiu permanecer até o seu encerramento.

No início de 2008, examinando os relatórios que enviei para a Pró-Reitoria de Extensão da Universidade Federal do Acre, lembrei-me de que poucos alunos declararam ter interesse em ingressar em um curso superior de Matemática. Esse fato me intrigou bastante. Havia realizado um debate intensivo de 4 meses, apresentando muitas curiosidades, fundamentando os conceitos abordados e estudando, com eles, sem o fantasma das avaliações formais. Esperava, com isso, despertar o interesse da maioria deles para a área de Matemática.

Paralelamente a isso, tenho acompanhado, de perto, o desenvolvimento de meu filho Emanuel e, algumas vezes, fico olhando para ele e me pergunto quando e como poderei avaliar sua capacidade de abstração de maneira formalizada.

Nos longos diálogos noturnos, com esse menino de 4 anos, muitas vezes dormi ao seu lado, imaginando como poderia estender as pequenas idéias que ele tem de *grande*, *pequeno* e das *formas geométricas*. Para mim, confesso ser uma tarefa árdua e que muito me incomoda.

Não consigo avaliar que efeito teria uma intervenção nos sonhos coloridos que ele vivencia, em sua sala de aula, junto com seus colegas.

Hoje as formas geométricas são reconhecidas por ele, com muita facilidade. Constantemente pede que suas fatias de pão sejam cortadas em forma de triângulos, quadrados, retângulos e tem uma verdadeira adoração pelo hexágono. Pode ser uma "birra" com sua mãe, minha adorável Wirla, que sempre demora mais nessa construção, mas pode ser uma paixão prematura por desafios, já que até agora suas tentativas de desenhar esse polígono falharam.

Se eu lhe apontasse as 2 diagonais de um quadrado, marcando-as no pedaço de pão, certamente ele poderia perguntar sobre as do hexágono, que ele tanto pede para fatiar. E ali, sobre o pão, seria difícil visualizá-las.

A associação dos conceitos de *muito*, *pouco*, *grande* e *pequeno* com os "números" começam a ser estabelecidas, muito embora para ele e seus coleguinhas, 1, 2, 3, 4, 5, 6, 7, 8 e 9, tenham um significado mais figurativo do que quantitativo.

Esse assunto poderia ser explorado em pequenas "doses". Mas até que ponto? Onde isso começa a ser uma transgressão à pureza do raciocínio desses meninos?

Acompanhando, também, alguns trabalhos, nas séries iniciais do Ensino Fundamental, deparei-me com questões interessantes. Um procedimento que sempre me chamou a atenção é o de se tentar passar a idéia de número racional, aquele que é um possível quociente de números inteiros.

Associando a metade de uma maçã ao número $\frac{1}{2}$ e ao número $\frac{3}{4}$, os três visíveis pedaços de uma barra de chocolate, após retirar-se um deles, podem surgir questionamentos, ao evidenciarmos a adição desses números. Certamente $\frac{1}{2} + \frac{3}{4} = \frac{5}{4}$, não pode significar algo que possa ser obtido com a mistura desses alimentos. Claro que as representações são úteis para dar significado aos números $\frac{1}{2}$ e $\frac{3}{4}$. No entanto, essa construção não acompanha, por exemplo, as propriedades da adição em $\mathbb{Q}$.

O porquê da regra de divisão, no conjunto $\mathbb{Q}$: $\frac{a}{b} \div \frac{c}{d} = \frac{ad}{bc}$, "repete-se a primeira fração e multiplica-se pelo inverso da segunda", a regra de obtenção da fração geradora de uma dízima periódica, o caso 0,999..., e o significado de – x, que dá sentido às regras dos sinais, na multiplicação dos números inteiros, poderiam ser explicados de forma mais "honesta". Mas essas coisas, algumas vezes, me parecem mal abordadas, em nome de uma melhor didática que, a meu ver, compromete o entendimento do que de fato deveria ser colocado. A questão, me parece, está em se descobrir o ponto em que podemos abandonar algumas dessas ligações e usar da abstração e do formalismo.

Os constantes questionamentos que tenho feito, ao longo de minha carreira de professor de Matemática já me levaram a desenvolver outros tipos de orientações e a mudar, freqüentemente, minhas estratégias de ensino. Pensando em quebrar uma provável resistência ao estudo da Matemática, e na certeza de que podemos formalizar algumas idéias desde cedo, decidi dar um passo na direção do Ensino Fundamental. Não devia avançar muito para baixo. Era na 8ª série do ensino fundamental, antiga 7ª série do extinto ensino ginasial, em que eu devia começar essa investigação. A pouca idade, embalada pela curiosidade e a pureza do raciocínio lógico e a Álgebra, comumente apresentada ali, podiam se constituir no ponto de partida de um interessante estudo e caça de jovens talentos. Se existia uma possibilidade de descer até o nível dos menores eu não queria arriscar. Um grupo de trabalho envolvendo fraldas, e auxílio a possíveis idas ao banheiro, poderia ser difícil para eu coordenar.

O curso, *Decisões à Luz do Algoritmo de Euclides*, foi formatado quase que, simultaneamente, quando da escolha desse nome. Alguns assuntos, já "batidos" nos outros dois cursos, seriam discutidos com os "meninos" que seriam selecionados. O trabalho a ser desenvolvido se constituía em um desafio, tanto da capacidade de abordagem do professor, quanto da capacidade de entendimento dos conceitos que abordaríamos. Usaríamos o máximo de rigor que, por ventura, fosse suportável.

Depois dos axiomas e dos elementos da Geometria Plana, abordaríamos vários problemas diretamente ligados à aritmética dos números inteiros, terminando pela construção de corpos finitos, fazendo-se partições adequadas no conjunto $\mathbb{Z}$. Alguns importantes resultados deveriam ser justificados pelo Algoritmo da Divisão de Euclides.

Embora o mergulho não fosse mais profundo e essa discussão ainda estivesse longe das minhas angústias de como abordar os aspectos da abstração, nas primeiras séries do Ensino Fundamental, essa experiência serviria para medir a intensidade dos parâmetros: *entusiasmo* e *pureza de raciocínio* e revelar até que ponto o uso do formalismo técnico e científico auxilia na compreensão de certas questões, que comumente, são consideradas prematuras, nesse nível de ensino.

Caso conseguíssemos programar um fluxo contínuo de conversação, e, em certos momentos dos encontros, abordarmos alguns problemas sem os recursos didáticos, restaria verificar uma última coisa: *Produzir textos satisfatórios a cerca de determinados temas, usando somente a folha de papel em branco e um lápis*.

Nesse caso, nossos relatos serviriam para orientar novos trabalhos. Talvez surgisse a idéia de desenvolver alguma ação mais para baixo, no sentido das séries inicias.

5. Fundamentos Teóricos - Metodológicos

Podemos caracterizar a História da Matemática como uma forma de representar o que é real e os fenômenos decorrentes dos desafios impostos pelas condições de nossa existência. É inegável a universalidade da Matemática e sua importância para o desenvolvimento da humanidade.

Os registros dos pensamentos, das descobertas e dos conceitos matemáticos, acumularam-se de forma sistematizada, implicando em quase tudo o que se pensa fazer hoje dentro do campo das ciências exatas. Podemos entender esse fato como o ponto vital para a uniformização de uma linguagem universal que hoje está posta.

Alinhada com o sentido do termo *filosofia*: amor pela sabedoria, experimentado, apenas, pelo ser humano, consciente de sua própria ignorância, assim definido, originalmente, por Pitágoras (Século VI a.C), a Matemática sofre, até hoje, a influência de diversas correntes filosóficas no pensamento matemático. Cercadas pela subjetividade, essas correntes são questionadas desde a Antiga Grécia, podendo inclusive ser alvos da ignorância de seus questionadores.

Lembremos, aqui, as afirmações de Aristóteles (384-322 a.C):

– "A mulher é um homem inacabado".

– "O ser humano nasce sem ter dentro de si nenhum conhecimento e aprende ao apropriar-se do conhecimento dos outros".

O pensamento de Sócrates (470-399 a.C):

– "O ser humano, ao nascer, traz consigo conhecimentos que aparecem na medida em que ele for estimulado.

Ainda que, distante dessa época, e, embora os avanços da ciência, como um todo, tenham sido grandes, podemos ver, nitidamente, que muitos traços desses pensamentos suscitam discussões até hoje. Ainda na academia, estando organizada, é muito difícil obtermos um padrão único de respostas às inerentes dificuldades que encontramos ao entrarmos no mundo da Matemática. Isso contribui para o surgimento e estabelecimento de algumas correntes filosóficas no pensamento matemático. Podemos citar, dentre outras: o Platonismo, o Racionalismo, o Empirismo, o Construtivismo, o Formalismo, o Historicismo e o Logicismo.

O processo de ensino e aprendizagem de conhecimento não cabe em "pacotes". Os seres humanos, intrinsecamente ávidos de conhecimento, sujeitos às diversas variantes de suas condições existenciais, constituem-se em peças de um processo em que os métodos e técnicas precisam variar.

Os conhecimentos espontâneos e científicos, segundo Vygotsky, se desenvolvem de formas diferentes; os espontâneos se desenvolvem na prática cotidiana, a partir de situações empíricas, os científicos se desenvolvem a partir da aprendizagem sistematizada de propriedades mais complexas dos objetos matemáticos, mas esses dois processos se interligam fortemente.

Nesse contexto, se faz necessário possibilitar ao aluno a apropriação da forma sistematizada de pensamento e de linguagem, partindo das experiências vividas para níveis mais complexos de abstração.

O poder dos conceitos científicos se manifesta em uma área que está bem determinada pelas suas propriedades: o caráter consciente e a voluntariedade, e continua adiante, na direção da experiência pessoal e de situações concretas. O desenvolvimento dos conceitos espontâneos começa na esfera das situações concretas e do empírico e se move na direção daquelas propriedades.

Compreender essa relação é fundamental para o processo de aprendizagem dos conceitos matemáticos, a inter-relação das situações contextualizadas e não contextualizadas, principalmente nas séries iniciais, deve ser administrada, de tal forma, que as marcas do verdadeiro conceito possam ser, efetivamente, exercitadas pelo aluno, a saber: a generalização, a abstração e a aplicação a novas situações. Além disso, é necessário considerar as múltiplas dimensões, dentre elas, a cognitiva, a social, a emocional e a biológica, a partir das perspectivas clássicas do desenvolvimento, inatismo e empirismo, classificadas como unidimensionais, e as abordagens interacionistas, representadas pelo construtivismo de Piaget, o sócio-interacionismo de Vigotsky e o desenvolvimento emocional de Wallon, classificadas como multidimensionais.

O Inatismo é uma tendência naturalista, acerca do desenvolvimento humano, que acredita que o homem nasce pré-determinado pela hereditariedade. Portando, em sua inteligência, algumas idéias verdadeiras, inatas, além dos princípios racionais, ou até por vontade divina.

O empirismo, palavra decorrente do termo grego "*empiria*", sustenta o contrário, afirma que a razão, vista como uma folha em branco, onde nada foi escrito, é adquirida através da experiência.

O construtivismo é uma das correntes teóricas dedicadas a explicar como a inteligência humana evolui, partindo do princípio de que o desenvolvimento da inteligência é determinado pelas ações mútuas entre o indivíduo e o meio. A idéia é que o ser humano não nasce inteligente, mas também não é passivo sob a influência do meio, isto é, ele responde aos estímulos externos, agindo sobre eles para construir e organizar o seu próprio conhecimento, de uma forma cada vez mais elaborada.

Segundo o suíço Jean Piaget, o principal objetivo da educação é criar indivíduos capazes de fazer coisas novas e não simplesmente repetir o que as outras gerações fizeram. Em oposição às perspectivas do inatismo, afirma, ainda, que as estruturas operatórias da inteligência não são inatas.

Segundo o russo Lev Semenovich Vigotsky, a aprendizagem deflagra vários processos internos de desenvolvimento mental, que tomam corpo somente quando o sujeito interage com objetos e sujeitos em cooperação. Uma vez internalizados, esses processos tornam-se parte das aquisições do desenvolvimento.

A teoria do desenvolvimento emocional (ou cognitivo) do francês Henri Wallon é centrada na psicogênese da pessoa completa, que estuda o desenvolvimento humano a partir do desenvolvimento psíquico da criança.

No pensamento de Gramsci, Vygotsky e outros, o conhecimento é muito mais que meramente utilitário, mas um patrimônio ao qual todo cidadão tem direito e que lhe propicia sabedoria e serenidade de espírito, dando-lhe ânimo e humor frente às adversidades.

Seguindo ou não uma dessas correntes de pensamento, uma dificuldade que está posta, para quem deseja ensinar Matemática, é a escolha certa de um método de ensino. É necessário perceber a relação entre os ensinamentos e a vida dos indivíduos, pois as pessoas são diferentes umas das outras e aprendem de maneiras diversas. Assim, mesmo que um professor utilize sempre um único método de ensino, é de fundamental importância que ele esteja atento às circunstâncias, adaptando seus procedimentos conforme a situação e as pessoas envolvidas.

Ações Desenvolvidas

Durante todo esse tempo, os trabalhos foram desenvolvidos com a filosofia de desmistificar e divulgar a Matemática e ampliar o número de pensadores nessa área de conhecimento. Embora as intervenções tenham ocorrido nos diversos níveis de ensino, o principal resultado foi à manutenção de um grupo de pessoas conversando sobre assuntos relacionados com a Matemática.

As fases de visitações às escolas de ensino fundamental e médio me trouxeram muitas lembranças do início de minha carreira como professor. Ali está a energia, em suas mais variadas formas. Uma oportunidade de refletirmos sobre o nosso papel no "andar de cima" no sentido de respeitar as aptidões, preferências e filosofia de vida. Ainda, no sentido de dentro para fora da Universidade, vale a pena mencionar a interação direta com coordenadores, diretores de escolas e professores de Matemática, resultando em discussões sobre as oportunidades que a Universidade propicia.

Em outro sentido, ocorreu que centenas de pessoas, que só ouviam falar de nossa Instituição, viessem conhecer os espaços das salas de aula, biblioteca e o restaurante universitário. Uma sublime integração.

Esses projetos, elaborados, aprovados e executados, ajudaram a divulgar o papel de nossa Instituição junto à nossa sociedade. Além das bolsas de ensino, criamos oportunidades para que os alunos dos cursos de licenciatura adquirissem créditos para o cumprimento da carga horária de sua grade curricular, destinada aos seminários. Isso fez com que espaços fossem cedidos para palestrantes que, mesmo atuando fora da Universidade, tiveram a oportunidade de falar, de forma mais madura, sobre certos objetos matemáticos com que lidam diariamente.

Ao submetermos os debates a ex-alunos do curso de Matemática, professores e alunos da rede municipal e da rede estadual de ensino, alunos dos cursos de graduação e professores da UFAC, hábitos de leitura e emprego de linguagem matemática correta foram restabelecidos.

As oficinas, os almoços coletivos no restaurante universitário, o uso dos espaços da Biblioteca acabaram por despertar entusiasmo pelo ensino superior. De certa forma, incluímos, em nossos espaços, as vontades e as idéias de quem, embora muito jovem para estudos superiores, pode apontar saídas para a retenção de alunos e para o avanço substancial no meio científico.

Discussão dos Resultados

Ando assistindo pequenas aulas sobre paralelas cortadas por transversais. Um menino que acaba de completar 4 anos de idade faz questão de incluir no seu passeio visitas às salas de aula de minha Universidade, nos fins de semana. Indo ao quadro, desenha e fala desses conceitos com bastante propriedade. Em seu cotidiano, consegue perceber que, em geral os cortes sucessivos numa “peça” de picanha, no preparo para assá-la, são paralelos.

Percebe ainda, se na letra “A”, em caixa alta, descemos um “pauzinho”, temos um triângulo! E nisso, um “perigo momentâneo”, admitir a igualdade: 0 + 0 = 8, pois ele acha simples a posição de dois círculos, um sobre o outro, formando esse número.

Por considerar de fundamental importância perceber os pequenos sinais do desenvolvimento do raciocínio da criança, é que incluo, aqui, o que venho descobrindo com Emanuel. Pode ser que, em algum momento, eu consiga descobrir uma boa oportunidade para que eu possa direcioná-lo melhor para os assuntos da Matemática. Embora exista uma grande probabilidade dele ser um historiador ou outra coisa de sentido inverso a essa discussão.

Em outro nível, o que levou o jovem Cleber, de família humilde, e que sempre estudou na zona rural, até chegar à Universidade, a conseguir aprovação na seleção do mestrado Institucional em Matemática, na Universidade Federal do Ceará, mesmo antes de concluir seu 4º período de graduação? Certamente aquele era o aluno mais prematuro que eu orientava, com vistas a uma pós-graduação. Acontece que a absorção da simbologia e o treino das conversações fizeram com que, em pouco tempo, ele passasse a ser um “questionador” nato, uma das mais importantes características do estudioso. Logo depois de eu ensinar as *noções dos conjuntos*, no 1º período de sua graduação, convidei-o para participar do curso sobre os *Grupos Cíclicos*. Muito curioso e interessado pelas relações que eu discutia com alunos mais maduros, investiu muito do seu tempo em seus estudos. O trabalho que eu comecei a fazer, desde 1994, de maneira informal, transformou-se mais uma vez em um desafio. Tínhamos que estabelecer as notações, entender os principais fundamentos da Álgebra Linear e aprender a conversar, fluentemente, sobre os assuntos, mesmo sem os recursos primários da caneta e papel. Era 2005, meu filho havia acabado de nascer. Se, por um lado o aluno estava encantado com os estudos e suficiente motivado, eu estava no ápice do meu entusiasmo.

Hoje o professor Cleber faz parte do quadro de professores efetivo do CCET-UFAC. Já está participando nos cursos de extensão, que nossa Instituição promove, e, também na orientação dos estudos de pequenos grupos de alunos do ensino médio.

O 2º curso, formalmente proposto, *A Influência da Teoria dos Conjuntos no Desenvolvimento de Alguns Conceitos Matemáticos*, embora tenha nascido para se contrapor a idéia de que a Teoria dos Conjuntos não deve ser considerada como assunto essencial, também teve respostas muito boas. Incorporou ex-alunos do antigo curso de Matemática que continuam atuando como professores em meu Estado e ex-alunos do 1º curso de extensão, hoje alunos dos cursos de Matemática, Engenharia, Economia e até de História.

Questionamos a semestralidade, concentração de determinadas disciplinas no primeiro semestre e de outras no segundo semestre, do ano letivo, do ensino médio. A Matemática não poderia suportar essa interrupção. Nossos questionamentos eram sobre a seqüência dos conteúdos na formalização dos conceitos e dos argumentos em cada nível de ensino.

Os próximos parágrafos contêm lembranças do curso mais recente: *Decisões à Luz do Algoritmo de Euclides*.

Os pequeninos se encantaram com os axiomas da Geometria Plana. A problemática sobre o triângulo retângulo de catetos iguais a 1 e hipotenusa $\sqrt{2} = 1{,}414213562\cdots$ mexeu muito com eles. Lembramos que isso é, em princípio, assunto de gente grande, mas suportaríamos a discussão daquele momento. Usando de uma calculadora, viram que o espaço da tela era todo preenchido com uma seqüência de números que, sabidamente, não termina. Como é que podemos ligar a hipotenusa que tem essa medida às extremidades dos dois catetos? A questão foi tratada com rigor e filosoficamente.

Um teste com várias folhas de papel cartão foi feito. Construímos várias caixas, usando sempre o mesmo tanto de papel. Muitas que pareciam ter volume maior que outra acabava se mostrando com capacidade menor. Então, discutimos o porquê do formato de uma lata de sardinha. Quase tocamos no Cálculo Diferencial!

Métricas e Volumes ficaram rondando suas cabeças, por muito tempo, numa clara evidência de que a Matemática Aplicada, para os "amadores", sempre será vista como um caminho mais atrativo do que o caminho da Abstração.

Uma observação cuidadosa mostrou que a adição de duas frações de denominadores diferentes pode significar um problema de mesma intensidade, comparado ao da construção que mostra que, num corpo finito, podemos ter $2 + 2 = 0$. Isso depende do grupo onde essas coisas são trabalhadas.

Os corpos finitos foram apresentados. Ali estavam alunos da 7ª série e, estabelecendo uma relação de equivalência conveniente sobre $\mathbb{Z}$, eles logo adquiriram habilidade em somar e multiplicar "módulo" um inteiro n positivo.

O respeito pela Universidade, os professores e seus títulos, embora para muitos, sem muito sentido, impuseram um ambiente mais propício para a realização do estudo. Muitos meninos mudaram o jeito de vestir e o corte de cabelo. Um deles veio de uma vila próxima à cidade de Rio Branco. Meio "rippie" e de andar balançado, durou pouco para que ele começasse a aparecer de banho tomado, andando ereto. Um exemplo de adaptação e dedicação ao que se propôs fazer junto com a equipe do curso.

Outro acostumado a passar nas peneiras dos clubes locais de futebol, ameaçando abandonar os estudos, torrando a paciência de sua mãe, trocou o uso constante das chuteiras pelos almoços e lanches na Universidade, imitando o seu irmão que, já tendo participado de uma dessas extensões, forma o grupo dos primeiros alunos do curso de Engenharia e se prepara para enfrentar um mestrado daqui a dois anos.

As meninas, sem o uso da farda, pareciam pequenas senhoras, ostentando uma pasta e "aparelhos" de medição, que constantemente, eram exigidos nos debates. Uma delas, uma menina magrela e bela, muito tímida, nem aparentava que havia adquirido uma medalha nas Olimpíadas que o Instituto de Matemática Pura e Aplicada - IMPA promove em nosso país. Seus estudos ficaram sendo orientados pelos professores Cleber e Felipe, que conduziram os trabalhos nesse curso, o que faz com que ela venha constantemente à nossa Universidade, ainda longe de poder aqui conseguir uma matrícula.

Conclusão

Para mim, acostumado a lidar com problemas extremamente abstratos, a manutenção da boa relação com a sala de aula se constitui num exercício que espanta a rotina. Entendo que os diferentes níveis de ensino de Matemática devem ser conhecidos e experimentados por cada pessoa que pretenda trabalhar com essa área de conhecimento.

Tenho o privilégio de conviver com ex-alunos do antigo 2º grau e do curso de Matemática de minha universidade. Mesmo trabalhando, informalmente, consegui direcioná-los para estudos mais avançados, contrariando o jogo político e o uso inadequado de "controle" de certas "autoridades" acadêmicas.

Sem causar danos ao auto-conceito, impedir o acesso ao conhecimento sistematizado e, portanto, sem restringir as oportunidades de participação social, seremos responsáveis diretos pelo sucesso profissional desses jovens, a quem devemos todo nosso respeito.

Se a verdadeira missão da Universidade se revela sempre que as ações se voltam para a comunidade, em outro sentido, a comunidade, "das janelas", espera muito de seus filhos, de seus profissionais e de seus pensadores.

Bibliografia

BICUDO, Maria Aparecida. **Educação matemática**. São Paulo: Moraes, 1995.

BIGODE, Antonio Lopes. **Matemática atual**. São Paulo: Atual, 1994.

BOYER, C. B.. **História da Matemática**. São Paulo: Edgar Blücher, 1974.

CARRAHER, T. et. Alii. (org.). **Aprender pensando - contribuições da psicologia cognitiva para a educação**. Petrópolis: Vozes, 1982.

_____. **Na vida dez na escola zero**. São Paulo: Cortez, 1988.

DAMÁZIO, Ademir. **A prática docente do professor de matemática: a pedagogia que fundamenta o planejamento e a execução do ensino**. Dissertação (Mestrado em Educação e Ciência). Florianópolis: UFSC, 1991.

D'AMBRÓSIO, Ubiratã. **Etnomatemática**. São Paulo: Ática, 1990.

_____. **Educação matemática**. Campinas, São Paulo: Papirus, 1996.

DURAM, Will. **História da Filosofia - A vida e as Idéias dos Grandes Filósofos**. São Paulo, Editora Nacional, 1ª edição, 1926.

IMENES, L. M. P.. **Um estudo sobre o fracasso do ensino e da aprendizagem da matemática**. Dissertação de Mestrado. Rio Claro: IGCE – UNESP, 1989.

LA TAILLE, Yves de. OLIVEIRA, Martha Kohl, DANTAS, Heloysa. **Piaget, Vygostky, Wallon: teorias psicogenéticas em discussão**. Summus Editorial, São Paulo, 1992.

NETO, Ernesto Rosa. **Didática da matemática**. São Paulo, Ática, 1988.

PIAGET, Jean. **Fazer e Compreender**. São Paulo: Melhoramentos. Editora Universidade de São Paulo, 1978.

_____. **A formação do símbolo na criança: imitação, jogo e sonho, imitação e representação**. Rio de Janeiro: LTC, 1990.

_____. **O Nascimento da Inteligência na Criança**. Rio de Janeiro: Guanabara, 1991.

RAMOS, Luzia Faraco. **Aventura decimal**. São Paulo: Ática, 1991.

SOUZA, Clarilza Prado de. **Avaliação escolar - limites e possibilidades**. Série Idéias nº. 22 - São Paulo: FDE, 1994; p. 89-90.

VYGOTSKY, Lev Semenovich. **Pensamento e Linguagem**. São Paulo, Martins Fontes, 3ª edição, 1991.

_____. **A formação social da mente**. 6. Ed. São Paulo: Martins Fontes, 1998.

WALLON, H.. **L' évolution psychologique de l' enfant (Evolução Psicológica da Criança)**. PUF, Paris, 1941, reed. 1974 (Andes, Rio de Janeiro, s. d.).

_____. **Les origenes de la pensée chez l' enfant (Origens do Pensamento da Criança)**. PUF, Paris, 1945, reed. 1963 (Manole. São Paulo. 1989).

José Ivan da Silva Ramos

Rua Maranhão, nº 133 – Bairro Bosque – Rio Branco – Acre

CEP: 69908-240

ivanr@ufac.br

Tels.: 0xx68-3224-5054 e 0xx68-84132219

ALGUMAS OBSERVAÇÕES ACERCA DA DEFINIÇÃO DE ANEL A PARTIR DAS BIBLIOGRAFIAS COMUMENTE UTILIZADAS NOS CURSOS DE MATEMÁTICA DA UFAC

Sérgio Brazil Júnior
Professor Adjunto da Universidade Federal do Acre

Resumo

A teoria de anéis estuda estruturas algébricas com duas operações binárias, adição $(+)$ e multiplicação $(\cdot)$, que possuem propriedades (de certa forma) similares às dos números inteiros. Não é difícil notar as diversas formas com que alguns autores definem essa tão importante estrutura algébrica. Dependendo do autor, um conjunto pode ser ou não um anel. No presente texto, realiza-se um estudo comparativo da definição dessa estrutura colocada por alguns importantes autores, cujos livros são utilizados nos cursos de Matemática da Universidade Federal do Acre – UFAC.

Abstract

The ring theory study algebraic structures with two binary operations: addition $(+)$and multiplication $(\cdot)$ that they possess properties (of certain form) similar to the integers number. It is not difficult to notice the diverse forms that some authors define this so important algebraic structure. Depending on the author, a set can be or not a ring. In the present text we carry through a comparative study of the definition of this structure carried through for some important authors whose books are used in the course of mathematics of the Federal University of Acre – UFAC.

Palavras chaves: Definição de Anel, Exemplos de Anéis.

1. INTRODUÇÃO: Justificativa e Objetivos

Em Álgebra Abstrata, uma estrutura algébrica consiste num conjunto associado a uma ou mais operações sobre o mesmo que satisfazem certos axiomas (ou propriedades). A teoria de anéis estuda estruturas algébricas com duas operações binárias, adição $(+)$ e multiplicação $(\cdot)$, que possuem propriedades (de certa forma) similares às dos inteiros. O estudo de anéis originou-se a partir do estudo de polinômios e da teoria de inteiros algébricos.

Segundo Picado (2009: 3), a teoria moderna de anéis originou-se no século XIX, a partir da introdução da noção de ideal feita por Richard Dedekind (1831-1916), em 1871, em trabalho que visava a generalizar o Teorema Fundamental da Aritmética, aplicando-o a contextos mais abstratos; bem como, em decorrência do trabalho com anéis de polinômios de David Hilbert (1862-1945), Edmund Lasker (1868-1941) e F. S. Macaulay (1862-1927). Foi Adolf Fraenkel (1891-1965) o pioneiro no tratamento abstrato da teoria dos anéis, tendo feito a primeira caracterização axiomática da noção de anel, a qual não é utilizada atualmente em decorrência da nova definição introduzida pelo matemático japonês Masazo Sono, em 1917.

Os maiores avanços nos estudos dessa teoria estão relacionados com os trabalhos de Emmy Noether (1882-1935) que, no artigo "*Ideal theory in rings*", de 1921, propõe uma teoria abstrata dos anéis, na qual o trabalho de Hilbert, Lasker e Macaulay, em anéis de polinômios, é estendido a anéis mais gerais.

É comum, em qualquer curso introdutório de álgebra abstrata, o estudo de estruturas algébricas, tais como grupos, anéis e corpos. Alguns livros comumente usados nessa área de conhecimento matemático, geralmente, realizam um estudo preliminar dessas estruturas apresentando definições, propriedades e vários exemplos (na maioria dos casos). Particularmente, quando abordam a estrutura anel, apresentam, além disso, algumas qualidades dessa estrutura.

Não é difícil notar as diversas formas que os autores desses livros definem a estrutura anel. É claro que isso pode não causar prejuízo, tendo em vista que tal abordagem depende do enfoque ou objetivo a que se propõem. No entanto, para um leitor inexperiente, isso pode ser motivo de conflito e até mesmo fazer com que ele desista de investigar esse assunto. É comum encontrar alunos que, depois de comparar algumas dessas bibliografias, tenham dúvidas sobre essas formas de definir essa tão importante estrutura.

Destarte, o estudo proposto resulta de experiências acumuladas em 21 anos de magistério de Matemática, dos quais 18 foram na Universidade Federal do Acre, predominantemente na área de Álgebra. Em tal período, foram ministradas diversas disciplinas cujos conteúdos englobam tópicos da estrutura algébrica anel, ocasiões em que se observou variação na definição de anel, a depender do enfoque do respectivo autor, por vezes exigindo-se mais axiomas para o enquadramento no conceito algébrico em estudo, e implicando na diminuição qualitativa dos exemplos.

No presente texto, realizar-se-á, na medida do possível, um estudo comparativo das definições de anel realizadas por alguns importantes autores cujos livros são utilizados nos cursos de matemática da UFAC, bem como será feita uma análise dos exemplos à luz dessas definições.

2. FUNDAMENTOS TEÓRICO-METODOLÓGICOS

A metodologia utilizada para a realização do estudo, que consistiu em pontuar algumas observações acerca da definição de anel, foi a comparação das definições e análise dos exemplos apresentados pelos autores cujos livros são regularmente utilizados nos cursos de Matemática da UFAC: Gonçalves (1999); Domingues e Iezzi (2003); Hefez (1993); Garcia e Lequain (2002); Monteiro (1971); e Alencar Filho (1990).

3. AÇÕES DESENVOLVIDAS

O presente relato de experiências consiste em análise das ocorrências e empregos de diversos autores nas disciplinas da área de Álgebra em cursos de graduação em Matemática da Universidade Federal do Acre, para o que foram desenvolvidas as seguintes ações: 1) seleção das referências e análise das definições; 2) estudo minucioso e comparativo dos axiomas componentes das definições de anéis; 3) identificação das principais dificuldades enfrentadas por alunos de graduação para a compreensão de uma ideia ou definição geral de anéis; e 4) discussão dos resultados e proposição de um conceito menos rígido da estrutura algébrica, de forma a contemplar a maior parte das referências bibliográficas sobre o assunto, sem prejuízo de enfoques especiais.

O que segue são transcrições dos livros desses autores, nas quais são omitidas, sem prejuízo ao estudo, partes de texto original, e, por vezes, adicionadas informações consideradas pertinentes para a melhor compreensão do propósito do presente texto.

4. DEFINIÇÃO E EXEMPLOS DE ANÉIS

As definições e os exemplos a seguir foram todos retirados dos textos originais, no entanto, os exemplos foram organizados para uma melhor visualização. Considere-se, também, que quando as operações de adição e multiplicação não estiverem explícitas, admitir-se-á que essas são as usuais.

4.1. Definição de Anel, segundo Gonçalves (1999: 34-39)

Seja A um conjunto não vazio no qual estejam definidas duas operações, as quais serão denominadas soma e produto em A, denotadas (como em $\mathbb{Z}$) $+$ e $\cdot$, da seguinte forma:

$$+ : A \times A \to A \quad (a,b) \rightsquigarrow a+b \qquad \text{e} \qquad \cdot : A \times A \to A \quad (a,b) \rightsquigarrow a \cdot b$$

Chamar-se-á $A, +, \cdot$ um anel se as seguintes 6 propriedades são verificadas quaisquer que sejam $a, b, c \in A$:

A1) $(a+b)+c = a+(b+c)$ (associatividade da soma);

A2) $\exists\ 0 \in A$, tal que $a+0 = 0+a = a$ (existência do elemento neutro para a soma);

A3) $\forall\, x \in A$ existe um único $y \in A$, denotado por $y = -x$, tal que $x+y = y+x = 0$ (existência do inverso aditivo);

A4) $a+b = b+a$ (comutatividade da soma);

A5) $(a\,.\,b)\,.\,c = a\,.\,(b\,.\,c)$ (associatividade do produto);

A6) $a\,.\,(b+c) = a\,.\,b + a\,.\,c$; $(a+b)\,.\,c = a\,.\,c + b\,.\,c$ (distributividade à esquerda e à direita);

Se um anel $A, +, \cdot$ satisfaz a propriedade:

A7) $\exists\ 1 \in A,\ 0 \neq 1$, tal que $x\,.\,1 = 1\,.\,x = x\ \ \forall\ x \in A$, diz-se que $A, +, \cdot$ é um anel com unidade 1.

Se um anel $A, +, \cdot$ satisfaz a propriedade:

A8) $\forall\, x, y \in A,\ x.y = y.x$, diz-se que $A, +, \cdot$ é um anel comutativo.

Se um anel $A, +, \cdot$ satisfaz a propriedade:

A9) $x, y \in A,\ x.y = 0 \Longrightarrow x = 0$ ou $y = 0$, diz-se que $A, +, \cdot$ é um anel sem divisores de zero.

Se $A, +, \cdot$ é um anel comutativo, com unidade e sem divisores de zero, diz-se que $A, +, \cdot$ é um domínio de Integridade.

E, finalmente, se um domínio de Integridade $A, +, \cdot$ $s$atisfaz a propriedade:

A10) $\forall\, x \in A,\ x \neq 0, \exists\, y \in A$, tal que $x.y = y.x = 1$, diz-se que $A, +, \cdot$ é um corpo.

Exemplos:

(1) Anéis Comutativos: $\mathbb{Z}$, $n.\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$,

$\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} \mid a, b \in \mathbb{Z},\ p\, primo\}$ e $\mathbb{Q}[\sqrt{p}]$, p primo

(2) Anéis Comutativos que não possuem unidade são os $n.\mathbb{Z}$, em que $n \geq 2$.

(3) Anéis Comutativos que possuem divisores de zero da lista acima são os anéis $A = \mathbb{Z}_n$, nos quais $n \geq 2$ não é um número primo.

(4) Domínios de Integridade que não são corpos: $\mathbb{Z}$, $\mathbb{Z}[\sqrt{p}]$, p primo e $\mathbb{Z}[i\,] = \{a + bi \mid a, b \in \mathbb{Z},\ i = \sqrt{-1} \in \mathbb{C}\}$

(4) Corpos: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}[\sqrt{p}]$, $\mathbb{Q}[i\,]$ e $\mathbb{Z}_p$, p primo.

(5) Anel comutativo com unidade e com divisores de zero**:** $\mathcal{F}(\mathbb{R})$ o conjunto de todas as funções $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ é um com relação às seguintes operações:

$$\begin{aligned} + : A \times A &\rightarrow A \\ (f, g) &\rightsquigarrow f + g \end{aligned}$$, em que $(f + g)(x) = f(x) + g(x)\ \forall\, x \in \mathbb{R}$ e

$$\begin{aligned} \cdot : A \times A &\rightarrow A \\ (f, g) &\rightsquigarrow f \cdot g \end{aligned}$$, em que $(f \cdot g)(x) = f(x) \cdot g(x)\ \forall\, x \in \mathbb{R}$

Analogamente, $\mathcal{C}(\mathbb{R})$ (respectivamente $\mathcal{D}(\mathbb{R})$), o conjunto de todas as funções contínuas (respectivamente deriváveis) $f\colon \mathbb{R} \longrightarrow \mathbb{R}$, é um anel comutativo com unidade e com divisores de zero.

(6) Anéis não comutativos com unidade e com divisores de zero: $Mat_2(\mathbb{R}) = A = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}\right\}$.

(7) Anéis não comutativos com unidade e sem divisores de zero: $Quat = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$, em que $i^2 = j^2 = k^2 = -1$, $i.j = k$, $j.i = -k, j.k = i$, $k.j = -i$, $k.i = j$, $i.k = -j$

4.2. Definição de Anel, conforme Domingues e Iezzi (2003: 210-223)

Um sistema matemático constituído de um conjunto não vazio A e um par de operações sobre A, respectivamente uma adição $(x, y) \longmapsto x + y$ e uma multiplicação $(x, y) \longmapsto xy$ (ou $x.y$), é chamado anel se:

(i) $(A, +)$ é um grupo abeliano, ou seja:

(a) Se $a, b, c \in A$, então $a + (b + c) = (a + b) + c$ (associatividade);

(b) Se $a, b \in A$, então $a + b = b + a$ (comutatividade);

(c) Existe um elemento $0_A \in A$, tal que qualquer que seja $a \in A$, $a + 0_A = 0_A + a$ (existência de elemento neutro);

(d) Qualquer que seja $a \in A$, existe um elemento em A, indicado genericamente por $-a$, tal que $a + (-a) = 0_A$ (existência de opostos).

(ii) A multiplicação goza da propriedade associativa, isto é, se $a, b, c \in A$, então $a(bc) = (ab)c$;

(iii) A multiplicação é distributiva em relação à adição, vale dizer: Se $a, b, c \in A$, então $a(b + c) = ab + ac$ e $(a + b)c = ac + bc$.

Exemplos:

(1) Anéis numéricos: $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$.

(2) Anel das classes de resto módulo m: para todo inteiro $m > 1$, é o conjunto $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m - 1}\}$.

(3) Anéis de matrizes: para qualquer inteiro $n > 0$, são anéis: $(M_n(\mathbb{Z}), +, \cdot), (M_n(\mathbb{Q}), +, \cdot), (M_n(\mathbb{R}), +, \cdot), (M_n(\mathbb{C}), +, \cdot)$.

Se A é um anel, o conjunto $(M_n(A), +, \cdot)$ das matrizes $n \times n$ sobre A, para todo $n \geq 1$, é o anel das matrizes sobre A de ordem n.

(4) Anéis de funções: seja $A = \mathbb{Z}^{\mathbb{Z}} = \{f \mid f: \mathbb{Z} \longrightarrow \mathbb{Z}\}$. Se $f, g \in A$, define-se a soma $f + g$ e o produto fg dessas funções da seguinte maneira:

$f + g: \mathbb{Z} \longrightarrow \mathbb{Z}$ e $(f + g)(x) = f(x) + g(x)$, para todo $x \in \mathbb{Z}$;

$fg: \mathbb{Z} \longrightarrow \mathbb{Z}$ e $(fg)(x) = f(x)g(x)$, para todo $x \in \mathbb{Z}$.

Anéis comutativos

Seja A um anel. Se a multiplicação de A goza da propriedade comutativa, isto é, se $ab = ba$, para quaisquer $a, b \in A$, então se diz que A é um anel comutativo.

Exemplos:

(5) Os anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$.

(6) Os anéis $\mathbb{Z}_m$ das classes de resto módulo m.

(7) Os anéis de funções A^X, sempre que A é um anel comutativo.

(8) Não são comutativos os anéis $M_n(A)$, em que A é um dos anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.

Anéis com unidade

Seja A um anel. Se A conta com elemento neutro para a multiplicação, isto é, se existe um elemento $1_A \in A$, $1_A \neq 0_A$, tal que $a \,.\, 1_A = 1_A . a = a$, qualquer que seja $a \in A$, então se diz que 1_A é a unidade de A e que A é um anel com unidade.

Exemplos:

(9) Os anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ cuja unidade é o número 1.

(10) Os anéis $\mathbb{Z}_m$ das classes de resto módulo m. A unidade é a classe $\overline{1}$.

(11) Os anéis $M_n(A)$, em que A é um dos anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$. A unidade é a matriz $n \times n$ abaixo:

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

(12) Se A é um conjunto com unidade, então a aplicação constante $u: X \longrightarrow A$, $u(x) = 1_A$, é a unidade do anel A^X.

(13) Os anéis $n\mathbb{Z}$ não possuem unidade quando $n \neq \pm 1$.

Anéis comutativos com unidade

Um anel cuja multiplicação é comutativa e que possui unidade chama-se anel comutativo com unidade.

Exemplos:

(14) Os anéis numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$.

Se A é um anel comutativo com unidade, o mesmo se pode dizer de A^X, qualquer que seja o conjunto $X \neq \emptyset$.

Anéis de integridade

Seja A um anel comutativo com unidade. Se para esse anel vale a lei do anulamento do produto, ou seja, se uma igualdade do tipo $ab = 0_A$, em que $a, b \in A$, só for possível para $a = 0_A$ ou $b = 0_A$, então se diz que A é um anel de integridade ou domínio.

(15) Todos os anéis numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são anéis de integridade.

(16) Considere-se o anel de integridade $\mathbb{Z}$ e um conjunto unitário $X = \{a\}$. Então $A = \mathbb{Z}^X$ é um anel de integridade.

No entanto, se X possuir mais do que um elemento, então $A = \mathbb{Z}^X$ não é um anel de integridade.

(17) Se $m > 1$ é um inteiro composto, então sempre há divisores próprios do zero no anel $\mathbb{Z}_m$.

4.3. Definição de Anel, segundo Hefez (1993: 23-25)

Sejam A um conjunto e $(+)$ e $(\cdot)$ duas operações em A, chamadas de adição e multiplicação. A terna $(A, +, \cdot)$ será chamada de anel se as operações gozarem das seguintes propriedades:

A1) **(A adição é associativa)** Quaisquer que sejam $a, b, c \in$ A, tem-se que: $(a + b) + c = a + (b + c)$;

A2) **(A adição é comutativa)** Quaisquer que sejam $a, b \in A$, tem-se que: $a + b = b + a$;

A3) **(Existe um elemento neutro para a adição)** Existe α ∈ A, tal que $\alpha + x = x$, para todo $x \in A$;

A4) **(Todo elemento de A possui um simétrico)** Para todo $a \in A$ existe $a' \in A$, tal que $a + a' = \alpha$;

M1) **(A multiplicação é associativa)** Quaisquer que sejam $a, b, c \in$ A, tem-se que $(a \,.\, b) \,.\, c = a \,.\, (b \,.\, c)$;

M2) **(A multiplicação é comutativa)** Quaisquer que sejam $a, b \in A$, tem-se que $a \,.\, b = b \,.\, a$;

M3) **(Existe um elemento neutro para a multiplicação)** Existe $e \in$ A, com $e \neq 0$, tal que $x \,.\, e = x$, para todo $x \in A$;

AM) **(A multiplicação é distributiva com relação à adição)** Quaisquer que sejam $a, b, c \in$ A, tem-se que $a \,.\, (b + c) = a \,.\, b + a \,.\, c$.

Um anel A será chamado de domínio de integridade ou simplesmente de domínio se for verificada a seguinte propriedade:

M4) **(Integridade)** Dados $a, b \in A$, se $a \neq 0$ e $b \neq 0$, então $a \,.\, b \neq 0$.

Exemplo: $(\mathbb{Z}, +, \cdot)$ é um domínio de integridade.

Um anel A em que todo elemento não nulo (i.e., diferente de zero) é invertível é chamado de corpo.

4.4. Definição de Anel, segundo Garcia e Lequain (2002: 7-12)

Um anel ou anel comutativo $(A, +, \cdot)$ é um conjunto A com pelo menos dois elementos, munido de uma operação denotada por $+$ (chamada de adição) e de uma operação denotada por $\cdot$ (chamada multiplicação) que satisfazem as condições seguintes:

A.1) A adição é associativa, isto é, $\forall\, x, y, z \in A,\ (x + y) + z = x + (y + z)$;

A.2) Existe um elemento neutro com respeito à adição, isto é, $\exists\, 0 \in A$, tal que, $\forall\, x \in A,\ 0 + x = x$ e $x + 0 = x$;

A.3) Todo elemento de A possui um inverso com respeito à adição, isto é $\forall\, x \in A$, $\exists\, z \in A$, tal que $x + z = 0$ e $z + x = 0$;

A.4) A adição é comutativa, isto é, $\forall\, x, y \in A,\ x + y = y + x$;

M.1) A multiplicação é associativa, isto é, $\forall\, x, y, z \in A,\ (x \,.\, y) \,.\, z = x \,.\, (y \,.\, z)$;

M.2) Existe um elemento neutro com respeito à multiplicação, isto é, $\exists\ 1 \in A$, tal que $\forall\ x \in A,\ 1 . x = x$ e $x . 1 = x$;

M.3) A multiplicação é comutativa, isto é, $\forall\ x, y \in A,\ \ x\ .\ y = y\ .\ x$;

AM) A adição é distributiva relativamente à multiplicação, isto é, $\forall\ x, y, z \in A, \quad x . (y + z) = x . y + x . z$).

Se todas as condições são satisfeitas, com exceção de M.3), então $(A, +, \cdot)$ é chamado de anel não-comutativo.

Um anel $(D, +, \cdot)$ é chamado domínio ou domínio de integridade se ele satisfaz a seguinte condição:

M.4) O produto de quaisquer dois elementos não nulos de D é um elemento não nulo, isto é, $\forall\ x, y \in D \setminus \{0\},\ \ x\ .\ y \neq 0$.

Um anel $(K, +, \cdot)$ é chamado corpo se ele satisfaz a seguinte condição:

M.4') Todo elemento diferente de zero de K possui um inverso com respeito à multiplicação, isto é, $\forall\ x \in K \setminus \{0\},\ \exists\ y \in K$, tal que $x\ .\ y = 1$.

Exemplos:

(1) $(\mathbb{Z}, +, \cdot)$ é um domínio.

(2) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ são corpos.

(3) Seja $\mathbb{Z}[i\,] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Então $(\mathbb{Z}[i\,], +, \cdot)$ é um domínio chamado anel dos inteiros de Gauss.

(4) $(\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}, +, \cdot)$ e $(\{a + bi\sqrt{3} \mid a, b \in \mathbb{Z}\}, +, \cdot)$ são domínios.

(5) Mais geralmente, se n é um inteiro positivo, tem-se que $(\{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}, +, \cdot)$ e $(\{a + bi\sqrt{n} \mid a, b \in \mathbb{Z}\}, +, \cdot)$ são domínios.

(6) $\{a + bi \mid a, b \in \mathbb{Q}\}$ é um corpo. Esse corpo será denotado por $\mathbb{Q}[i\,]$.

(7) Dados dois anéis $(A_1, +_1, \cdot_1)$ e $(A_2, +_2, \cdot_2)$, pode-se construir um novo anel da maneira seguinte: no conjunto $A_1 \times A_2 := \{(a_1,\ a_2) :\ a_1 \in A_1,\ a_2 \in A_2\}$, definem-se as operações:

$$(a_1, a_2) + (a'_1, a'_2) = (a_1 +_1 a'_1, a_2 +_2 a'_2)$$
$$(a_1, a_2) . (a'_1, a'_2) = (a_1 \cdot_1 a'_1, a_2 \cdot_2 a'_2)$$

$(A_1 \times A_2, +, \cdot)$ é um anel, chamado produto direto de A_1 com A_2.

(8) Mais geralmente, dados r anéis $(A_1, +_1, \cdot_1), \ldots, (A_r, +_r, \cdot_r)$, define-se a noção de produto direto $A_1 \times \ldots \times A_r$.

(9) Se $f :\ \mathbb{R} \longrightarrow \mathbb{R}$ e $g :\ \mathbb{R} \longrightarrow \mathbb{R}$ são duas funções de $\mathbb{R}$ em $\mathbb{R}$, define-se:

$$
\begin{array}{rccc}
f \oplus g\colon & \mathbb{R} & \longrightarrow & \mathbb{R} \\
 & x & \longmapsto & f(x) + g(x)
\end{array}
$$

$$
\begin{array}{rccc}
f \odot g\colon & \mathbb{R} & \longrightarrow & \mathbb{R} \\
 & x & \longmapsto & f(x).g(x)
\end{array}
$$

Então, ({funções de $\mathbb{R}$ em $\mathbb{R}$}, $\oplus,\odot$) é um anel comutativo com unidade, mas não é domínio.

(10) $(M_{n\times n}(\mathbb{R}), +,\cdot)$ é um anel não-comutativo se $n \geq 2$.

(11) No exemplo 5) acima, substituindo o anel dos inteiros $\mathbb{Z}$ pelo corpo dos números racionais $\mathbb{Q}$, obtêm-se corpos.

(12) (Anel dos inteiros módulo n): Seja n um número inteiro positivo. $(\mathbb{Z}/n\mathbb{Z}, \oplus_n, \odot_n)$ é um anel.

4.5. Definição de Anel, conforme Monteiro (1971: 166-178)

Seja A um conjunto, e supondo-se que estejam definidas sobre A duas operações $A \times A \overset{+}{\rightarrow} A$ e $A \times A \overset{\cdot}{\rightarrow} A$ denominadas, respectivamente, adição e multiplicação, diz-se que estas operações definem uma estrutura de anel sobre o conjunto A ou que o conjunto A é um anel em relação a estas operações se, e somente se, são válidos os seguintes axiomas:

A: a operação de adição define uma estrutura de grupo comutativo sobre o conjunto A, isto é:

Sejam a, b e c elementos quaisquer de A:

A1: $a + (b + c) = (a + b) + c$;

A2: $a + b = b + a$;

A3: $a + 0 = a$;

A4: $a + (-a) = 0$.

M1: a operação de multiplicação define uma estrutura de semi-grupo sobre o conjunto A, isto é: $(ab)c = a(bc)$.

D: quaisquer que sejam a, b e c em A, tem-se (propriedades distributivas da multiplicação em relação à adição):

$a(b + c) = (ab) + (ac)$ e $(b + c)a = (ba) + (ca)$

Diz-se que um anel A é comutativo se, e somente se, estiver verificado o seguinte axioma:

M2: quaisquer que sejam a e b em A, tem-se $ab = ba$ (propriedade comutativa da multiplicação).

Diz-se que um anel A tem elemento unidade se, e somente se, estiver verificada a seguinte propriedade:

M3: existe um elemento 1 em A, tal que $a.1 = a = 1.a$ para todo a em A (existência do elemento unidade da multiplicação).

Se um anel A satisfaz os axiomas M2 e M3, dir-se-á que A é um anel comutativo com unidade.

Exemplos:

(1) O conjunto $\mathbb{Z}$ dos números inteiros é um anel comutativo com elemento unidade.

(2) O conjunto $2\mathbb{Z}$ dos números inteiros pares é um anel comutativo. Este anel não tem elemento unidade.

(3) O conjunto $\mathbb{Q}$ dos números racionais é um anel comutativo com elemento unidade.

(4) O conjunto $\mathbb{R}$ dos números reais é um anel comutativo com elemento unidade.

(5) Seja A um conjunto unitário, e indicando-se por 0 (zero) seu único elemento; é evidente que só existe uma única operação f sobre A, definida por $0f0 = 0$. Tomando-se $f = + = \cdot$, obtém-se uma estrutura de anel comutativo com elemento unidade $A = \{0\}$. Diz-se, neste caso, que $A = \{0\}$, com estas operações, é um anel nulo.

(6) Seja $(A, +)$ um grupo comutativo, e colocando-se, por definição, $x \,.\, y = 0$ quaisquer que sejam x e y em A, $(A, +, \ \cdot)$ é um anel comutativo, que é chamado anel trivial.

(7) Seja $\mathbb{Z}[\sqrt{2}]$ o conjunto de todos os números reais da forma $a + b\sqrt{2}$, com a e b inteiros. Este conjunto é um anel comutativo com elemento unidade.

(8) Considere-se o conjunto A de todas as funções reais e contínuas definidas sobre o conjunto $\mathbb{R}$ dos números reais. Se f e g são dois elementos quaisquer de A, definir-se-á $f + g$ e $f \cdot g$ por $(f + g)(x) = f(x) + g(x)$ e $(f.g)(x) = f(x) \,.\, g(x)$, para todo x em $\mathbb{R}$. Essas operações definem uma estrutura de anel comutativo com elemento unidade sobre o conjunto A.

(9) Considere-se o conjunto $A = \{a, b, c, d\}$ com quatro elementos e definam-se as operações de adição e de multiplicação pelas seguintes tábuas:

$+$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

$\cdot$	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	0	0	0
c	0	a	b	c

Essas operações definem uma estrutura de anel sobre o conjunto A. Note-se que este anel não é comutativo e nem tem elemento unidade.

(10) Seja X um conjunto não vazio e seja A um anel, indique-se por $E = A^X$ o conjunto de todas as aplicações de X em A. Se f e g são dois elementos quaisquer de E, definir-se-á $f + g$ e fg por $(f + g)(x) = f(x) + g(x)$ e $(fg)(x) = f(x)g(x)$. Para todo x em X, E é um anel em relação a essas operações. E é comutativo (resp., tem elemento unidade) se, e somente se, A é comutativo (resp., tem elemento unidade).

Diz-se que um elemento a, de um anel comutativo não nulo A, é um divisor de zero se, e somente se, existe $b \in A,\ b \neq 0$, tal que $ab = 0$. Se a é divisor do zero e se $a \neq 0$, dir-se-á que a é um divisor próprio de zero.

Chama-se anel de integridade a todo anel comutativo com elemento unidade $1 \neq 0$ que não possui divisores próprios do zero.

Exemplos:

(11) Os anéis considerados nos exemplos 1, 3, 4 e 7 são anéis de integridade.

(12) $2\mathbb{Z}$ não é um anel de integridade, pois este anel não tem elemento unidade.

(13) Sejam A e B dois anéis comutativos com elementos unidades 1_A e 1_B, considerando-se o anel produto $A \times B$ de A por B, tem-se que $A \times B$ é um anel comutativo e tem unidade $(1_A, 1_B)$, bem como $A \times B$ não é um anel de integridade, pois, por exemplo, $(1_A, 0).(0,\ 1_B) = (1_A.0,\ 0.1_B) = (0, 0)$.

(14) Considerando-se o anel A das funções reais e contínuas definido no exemplo 8, e sendo f e g as funções definidas por:

$$f(x) = \begin{cases} x & se \ \ x \geq 0 \\ 0 & se \ \ x < 0 \end{cases}$$

e

$$g(x) = \begin{cases} 0 & se \ \ x \geq 0 \\ -x & se \ \ x < 0 \end{cases}$$

$f \neq 0, g \neq 0$, tem-se que $fg \neq 0$.

(15) Considerando-se o anel $A = \{a, b, c, d\}$ definido no exemplo 9. Conforme tábua de multiplicação desse anel, tem-se, por exemplo, $ba = 0$ com $b \neq 0$.

(16) Considerando-se o anel E definido no exemplo 10, em que se supõe que A seja um anel não nulo e que o conjunto X tenha pelo menos dois elementos x_1 e x_2. Seja a um elemento não nulo de A e sejam f e g as aplicações de X em A definidas por:

$$f(x) = \begin{cases} a & se \ \ x = x_1 \\ 0 & se \ \ x \neq x_1 \end{cases}$$

e

$$g(x) = \begin{cases} a & se \ \ x = x_2 \\ 0 & se \ \ x \neq x_2 \end{cases}$$

$f \neq 0, g \neq 0$ e $fg \neq 0$.

Diz-se que um anel comutativo K, com elemento unidade $1 \neq 0$, é um corpo se, e somente se, todo elemento não nulo de K é inversível para a multiplicação.

4.6. Definição de Anel, segundo Alencar Filho (1990: 209-229)

Seja $(A, \ *, \ \top)$ um conjunto não vazio A $(A \neq \emptyset)$ munido de duas operações * e ⊤.

Diz-se que (A, *, ⊤) é um anel se, e somente se, as operações * e ⊤ possuem as seguintes propriedades:

(A1) A operação * é associativa: $(a * b) * c = a * (b * c), \quad \forall \ a, b, c \ \in A$;

(A2) A operação * admite elemento neutro $e \in A$: $a * e = e * a = a, \ \ \forall \ a \in A$;

(A3) Todo elemento de A é simetrizável para operação * :

$\forall \ a \in A, \ \exists \ a' \in A \mid a * a' = a' * a = e$

(A4) A operação * é comutativa: $a * b = b * a, \ \ \forall \ a, b \in A$;

(A5) A operação ⊤ é associativa: $(a \top b) \top c = a \top (b \top c), \quad \forall \ a, b, c \ \in A$;

(A6) A operação ⊺ é distributiva em relação à operação *:

$$\begin{cases} a \intercal (b * c) = (a \intercal b) * (a \intercal c) \\ (b * c) \intercal a = (b \intercal a) * (c \intercal a) \end{cases}, \quad \forall a, b, c \in A$$

Seja $(A, \ *, \ \intercal)$ um anel. Se a operação ⊺ é comutativa:

(A7) $$a \intercal b = b \intercal a, \ \forall\, a, b \in A$$

Diz-se que $(A, \ *, \ \intercal)$ é um anel comutativo.

Se a operação ⊺ admite elemento neutro $f \in A$:

(A8) $$a \intercal f = f \intercal a = a, \ \ \forall \ a \in A$$

Diz-se que $(A, \ *, \ \intercal)$ é um anel unitário.

As operações * e ⊺ de um anel $(A, \ *, \ \intercal)$ podem ser indicadas pelas notações aditiva e multiplicativa, respectivamente (* = +, ⊺= ·).

Exemplos:

(1) As ternas $(\mathbb{Z}, +, \ \cdot), (\mathbb{Q}, +, \ \cdot), (\mathbb{R}, +, \ \cdot)$ são anéis comutativos com elemento unidade.

(2) A terna $(2\mathbb{Z}, +, \ \cdot)$, em que $2\mathbb{Z}$ denota o conjunto dos números inteiros pares, é um anel comutativo sem elemento unidade.

(3) A terna $(P(E), \ \triangle, \ \cap)$ (na qual $P(E), \ \triangle, \ \cap$ são, respectivamente, o conjunto das partes do conjunto E, a diferença simétrica e interseção) é um anel comutativo unitário.

(4) A terna $(\mathbb{Z}/(n) \ , +, \ \cdot \ )$, em que $m > 1$, é um anel comutativo com elemento unidade.

(5) Seja o conjunto $A = \{a + b\sqrt{3} \,|\, a, b \ \in \mathbb{Z}\,\}$. A terna $(A, +, \ \cdot)$ é um anel comutativo com unidade.

(6) Seja $\mathbb{R}^{\mathbb{R}}$ o conjunto de todas as funções reais de variável real:

$$\mathbb{R}^{\mathbb{R}} = \{f \mid f \colon \mathbb{R} \longrightarrow \mathbb{R}\}$$

A terna $(\mathbb{R}^{\mathbb{R}}, +, \ \cdot)$ é um anel comutativo com elemento unidade.

(7) Seja $M_2(\mathbb{R})$ o conjunto de todas as matrizes reais quadradas de ordem 2. A terna $(M_2(\mathbb{R}), +, \ \cdot \ )$ é um anel não comutativo com elemento unidade.

(8) A terna $(\{0\}, +, \ \cdot \ )$ é um anel comutativo com unidade, denominado anel nulo.

(9) Seja $(A, +)$ um grupo abeliano. Munindo o conjunto A de uma operação de multiplicação ($\cdot$) definida por $a.b = 0,\ \forall a, b \in A$, a terna $(A, +,\ \cdot)$ é um anel comutativo sem elemento unidade, denominado anel trivial.

Chama-se anel de integridade todo anel comutativo $(A, +,\ \cdot)$ com elemento unidade e sem divisores de zero.

Anel de integridade é todo anel comutativo $(A, +,\ \cdot)$ com elemento unidade no qual é verdadeira a proposição: $a \neq 0\ e\ b \neq 0\ \Rightarrow a.b \neq 0,\ \forall\ a, b \in A$, ou seja: $a\,.\,b = 0 \Rightarrow a = 0\ ou\ b = 0, \forall\ a, b \in A$.

Exemplos:

(1) As ternas $(\mathbb{Z}, +,\ \cdot), (\mathbb{Q}, +,\ \cdot), (\mathbb{R}, +,\ \cdot)$ são anéis de integridade.

(2) A terna $(6\mathbb{Z}, +,\ \cdot)$ não é um anel de integridade, pois não possui elemento unidade.

(3) A terna $(\mathbb{Z}/(n)\ , +,\ \cdot\ )$ é um anel de integridade quando o módulo n é um número primo.

5. ANÁLISE DO MATERIAL OBSERVADO: Discussão dos Resultados

Realizando uma leitura nesses transcritos, podem ser feitas algumas observações.

A primeira observação diz respeito às várias formas de apresentação dessa estrutura algébrica. Gonçalves (1999), Domingues e Iezzi (2003), Monteiro (1971) e Alencar Filho (1990) definem a estrutura anel como um conjunto não vazio munido de duas operações, satisfazendo 6 (seis) propriedades e apresentando três qualidades, a saber: 1) comutatividade da multiplicação; 2) existência do elemento unidade; e 3) integridade (sem divisores de zero). Já Hefez (1993), define como um conjunto não vazio (com, no mínimo, dois elementos: veja na definição, as propriedades A3 e M3 com duas operações, satisfazendo 8 (oito) propriedades, isto é, a comutatividade e a existência de unidade, que ao contrário do que preconizam os autores acima citados, são exigências necessárias para uma estrutura algébrica ser um anel. Hefez (1993) apresenta apenas uma qualidade, que é a integridade. Por fim, Garcia (2002) define anel (comutativo) como um conjunto com, no mínimo, dois elementos, munido de duas operações, satisfazendo 8 (oito) propriedades. Esse autor define de modo análogo anel não comutativo com 7 (sete) propriedades. Em ambas as definições existe a necessidade de o conjunto possuir elemento unidade.

Outra observação diz respeito aos exemplos dados por esses autores à luz das respectivas definições. Gonçalves (1999), Domingues e Iezzi (2003) e Alencar Filho (1990) não apresentam, de forma explícita, exemplo de um anel que satisfaça apenas a definição "nua e crua", isto é, não mostram um exemplo de um anel que satisfaça apenas as seis propriedades requeridas pela definição constantes em seus livros. Todos os exemplos dados possuem alguma qualidade. Não obstante, realizando uma leitura mais aprofundada, verifica-se que, implicitamente, os dois últimos autores trazem em listas de exercícios exemplos que poderiam ser explorados nesse sentido (exercício 22 (L_1), página 228, e exercício 9, página 218, respectivamente). Monteiro (1971) exibe um exemplo de uma estrutura que se pode classificar como "pura", isto é, um exemplo de um anel que satisfaz somente as condições da definição, ou seja, não possui qualidade alguma, no entanto, a exemplo das referências citadas no início do parágrafo, o autor não faz essa observação, o que se entende ser muito importante para a compreensão do conceito dessa estrutura.

Ainda na linha das diversas formas de apresentação dessa estrutura, verifica-se que, dependendo do autor, um conjunto pode ter ou não uma estrutura de anel. A forma de definir anel de Hefez (1993) exclui, por exemplo, o anel nulo $\{0\}$ (definição exige no mínimo dois elementos); os múltiplos de um número inteiro maiores que 1(um), $n\mathbb{Z}, n > 1$ (definição exige elemento neutro para multiplicação); as matrizes $M_n(A)$, em que A é um anel (definição exige comutatividade da multiplicação); e os Quatérnios $Quat$ (definição exige comutatividade da multiplicação). Já a definição de Garcia, (2002) exclui, por exemplo, o anel nulo $\{0\}$ (definição exige no mínimo dois elementos) e os múltiplos de um número inteiro maiores que 1 (um), $n\mathbb{Z}, n > 1$ (definição exige elemento neutro para multiplicação). Veja o resumo do exposto no quadro abaixo:

Autor	$\{0\}$	$n\mathbb{Z}, n > 1$	$M_n(A), A$ anel	$Quat$
Gonçalves (1999)	Anel	anel	anel	anel
Domingues e Iezzi (2003)	Anel	anel	anel	anel
Hefez (1993)	não é anel	não é anel	não é anel	não é anel
Garcia (2002)	não é anel	não é anel	anel	anel
Monteiro (1971)	Anel	anel	anel	anel
Alencar Filho (1990)	Anel	anel	anel	anel

6. CONCLUSÃO

Observa-se que as várias formas de abordar a estrutura algébrica anel que os autores mencionados apresentam depende do enfoque, no entanto, se o estudante não for orientado corretamente, a diversidade na conceituação/definição pode confundi-lo e até mesmo fazê-lo pensar que esse estudo não apresenta muita coerência. Dessa forma, alerta-se os docentes sobre a importância da escolha da definição a ser abordada e, consequentemente, dos exemplos escolhidos, ou seja, deve-se fazer um planejamento adequado para o magistério de uma disciplina que tem a estrutura anel como um tópico a ser estudado.

A título de orientação, partindo-se de experiências nos cursos de matemática, entende-se ser mais estimulante apresentar uma definição que abranja a maior quantidade possível de exemplos, isto é, uma definição que exija somente 6 (seis) propriedades, como ocorre em Gonçalves (1999), Domingues e Iezzi (2003), Monteiro (1971) e Alencar Filho (1990).

6.1. Um Exemplo de um anel, digamos, puro, à luz das definições de Gonçalves (1999), Domingues e Iezzi (2003), Monteiro (1971) e Alencar Filho (1990)

Um exemplo de anel que satisfaz somente as seis propriedades requeridas nas definições das referências acima, que poderia ser apresentado de maneira natural, seria o seguinte:

$M_m(n\mathbb{Z}) = \{[a_{ij}] \mid a_{ij} \in n\mathbb{Z}, n > 1\}$, o conjunto das matrizes de ordem m ($m > 1$), com entradas no conjunto $n\mathbb{Z}$.

Esse conjunto é um anel, no entanto, não é comutativo, pois o anel das matrizes não é; não possui unidade, pois o conjunto $n\mathbb{Z}, n > 1$ não tem unidade; e possui divisores de zero. Com isso, acaba-se de construir um exemplo de um anel que não possui qualidade alguma, ou seja, tem-se um exemplo de um anel, pode-se dizer puro, à luz das definições de Gonçalves (1999), Domingues e Iezzi (2003), Monteiro (1971) e Alencar Filho (1990).

REFERÊNCIAS BIBLIOGRÁFICAS

ALENCAR FILHO, Edgard de. **Elementos de Álgebra**. São Paulo: Nobel, 1990.

DOMINGUES, Hygino H.; IEZZI, Gelson. **Álgebra moderna**. 4. ed. São Paulo: Editora Atual, 2003.

GARCIA, Arnaldo. **Elementos de Álgebra**. Rio de Janeiro: Associação Instituto de Matemática Pura e Aplicada, 2002.

GONÇALVES, Adilson. **Introdução à Álgebra**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 1999.

HEFEZ, Abramo. **Curso de Álgebra**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada/CNPq, 1993. 1 v.

MONTEIRO, L. H. Jacy. **Elementos de Álgebra**. Rio de Janeiro: Editora Ao Livro Técnico S.A., 1971.

PICADO, Jorge. **Corpos e Equações Algébricas**. Disponível em: < http://arquivoescolar.org/bitstream/arquivo-e/51/1/CeEA.pdf>. Acesso em: 14 ago. 2011.

Sérgio Brazil Júnior
Centro de Ciências Exatas e Tecnológicas
Universidade Federal do Acre
sbrazil@ufac.br
(68)9984-1922

ÁLGEBRAS NORMADAS ESPECIAIS E OS NÚMEROS OCTÔNIOS

José Kenedy Martins

Resumo

Neste trabalho apresentamos uma abordagem alternativa mais simplificada para a caracterização das álgebras normadas e obtemos os números octônios como uma álgebra normada caracterizada por algumas propriedades algébricas tais como não-associatividade e alternada. Além disso, ilustramos o processo de Cayley-Dickson para construção de novas álgebras e exemplificamos como o grupo de Lie excepcional G_2 pode ser visto como grupo dos automorfismos da álgebra dos octônios.

Abstract

In this piece of work, we introduce a different more direct approach for a characterization of normed algebras. By doing this, the octonions or Cayley numbers are obtained as a particular normed algebra endowed with certain features such as non-associative and alternate multiplicative law. Moreover, the Cayley-Dickson construction process of normed algebras is revisited and the excepcional Lie group G_2 is introduced as the automorphism group of the octonions algebra.

Palavras Chaves: Álgebras normadas, Octônios, Números de Cayley, Grupo de Lie Excepcional G_2.

O processo de Cayley-Dickson para construção das álgebras normadas é bem conhecido. Entretanto fazemos aqui uma apresentação mais objetiva deste processo. Neste caminho naturalmente obtemos os números complexos, quatérnios e octônios como álgebras decorrentes. Algumas das propriedades destas álgebras são revistas. Focalizamos nossa atenção principalmente na multiplicação natural definida para os octônios e vemos como esta induz um produto vetorial em $\mathbb{R}^7$. O grupo de automorfismos G_2 que preserva este produto vetorial é detalhado em algumas de suas propriedades algébricas e geométricas.

Definição 1 *Uma* **algebra** *é um espaço vetorial real V munido de uma operação interna de multiplicação, não necessariamente associativa e com elemento unidade*

$1 \in V$. *Uma* **álgebra normada** B *é uma álgebra dotada de produto interno* $\langle .,. \rangle$ *tal que*

$$|xy| = |x||y| \quad \forall x, y \in B$$

onde $|x| = \sqrt{\langle x, x \rangle}$.

Temos associados à álgebra B, os conjuntos $\Re B = \text{span}\{1\} = \{\lambda.1/\lambda \in \mathbb{R}\} \subseteq B$ e $\Im B = (\Re B)^{\perp}$ que chamaremos respectivamente de parte real e parte imaginária de B. Além disso, para cada elemento $x = \Re x + \Im x$, consideramos o seu elemento conjugado complexo definido por $\overline{x} = \Re x - \Im x$. Desse modo, podemos também escrever:

$$\Re x = \frac{x + \overline{x}}{2} \text{ e } \Im x = \frac{x - \overline{x}}{2}.$$

Observamos que para o caso da álgebra dos números complexos $B = \mathbb{C}$ temos $\Im(x + iy) = iy$ e não o que usualmente consideramos y !.

Uma simples manipulação com as definições acima nos permite obter as seguintes propriedades algébricas elementares relativas aos conjugados em álgebras normadas:

(i) Para cada elemento $x \in B$, tem-se $\overline{\overline{x}} = x$;

(ii) Para quaisquer $x, y \in B$, tem-se $\overline{xy} = \bar{y}\bar{x}$. Em particular para $B = \mathbb{C}$ vale $\overline{zw} = \bar{w}\ \bar{z} = \bar{z}\bar{w}$. Entretanto, é bom ressaltar que álgebras normadas de dimensão maior deixam de ser comutativas;

(iii) Para quaisquer $x, y \in B$ tem-se $\langle x, y \rangle = \Re(x\overline{y}) = \frac{1}{2}(x\overline{y} + y\overline{x})$

Proposição 1 *Considere B uma álgebra normada. Então*

- *Para cada elemento não-nulo $x \in B$ existe um único inverso à esquerda e à direira $x^{-1} = \frac{\overline{x}}{|x|^2}$;*
- *Para quaisquer $x, y \in B$ com $x \neq 0$, as equações $xw = y$ e $wx = y$ podem ser resolvidas de modo único em w com soluções respectivamente iguais a $w = \frac{\overline{x}y}{|x|^2}$ e $w = \frac{y\overline{x}}{|x|^2}$.*
- *A álgebra B é* **fracamente associativa***, ou seja, $(xy)z - x(yz)$ são alternados em x, y, z.*

Vejamos agora um processo bem conhecido de construção de álgebras normadas usualmente chamado de Processo de Cayley-Dickson.

Proposição 2 *Considere uma subálgebra $A \subset B$, $\epsilon \in A^{\perp}$, $|\epsilon| = 1$. Então $A\epsilon \perp A$ e*

$$(a + b\epsilon)(c + d\epsilon) = (ac - \bar{d}b) + (da + b\overline{c})\epsilon \quad \forall a, b, c, d \in A.$$

Exemplo 1 $A = \mathbb{R}$, $B = \mathbb{C}$, $\epsilon = i$,

$$(a + bi)(c + di) = (ac - db) + (da + bc)i.$$

Observação 1 *$\epsilon \in A^{\perp} \subset \Im B$ pois $1 \in A$. Assim, $\overline{\epsilon} = -\epsilon$ e $\epsilon^2 = -1$ uma vez que*

$$1 = |\epsilon|^2 = \epsilon\overline{\epsilon} = \epsilon(-\epsilon) = -\epsilon^2.$$

Definição 2 *Seja A uma álgebra. Considere definida num espaço vetorial $B := A \oplus A$ a seguinte multiplicação*

$$(a,b)(c,d) := (ac - \overline{d}b, da + b\overline{c}).$$

Então isto transforma B em uma álgebra, que dizemos ter sido obtida de A através do **Processo de Cayley-Dickson**.

Observação 2 *Para uma subálgebra $A \subset B$, a álgebra $A + \epsilon A$ é isomorfa a $A \oplus A$.*

Definição 3

- $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}$, **os números complexos**;
- $\mathbb{H} = \mathbb{C} \oplus \mathbb{C}$, **os números quatérnios**;
- $\mathbb{O} = \mathbb{H} \oplus \mathbb{H}$,**os números de Cayley ou Octônios**.

Consideramos os números octônios $\{1, i, j, k, e, ie, je, ke\}$ como uma base canônica para $\mathbb{O}$. Onde, $\mathbb{C} = \mathbb{R} + i.\mathbb{R}$, $\mathbb{H} = \mathbb{C} + j.\mathbb{C}$, $\mathbb{O} = \mathbb{H} + e.\mathbb{H}$.

Observação 3 *Uma álgebra é dita* **alternada** *se o sinal da expressão $(xy)z - x(yz)$ é invertido com a troca das posições das variáveis x, y, z. Uma álgebra normada é alternada e trivialmente álgebras associativas são alternadas.*

Proposição 3 *Considere $B = A \oplus A$, então:*

1. *A álgebra B é comutativa se e somente se $A = \mathbb{R}$;*
2. *A álgebra B é associativa se e somente se A é comutativa;*
3. *A álgebra B é alternada se e somente se A é associativa.*

Exemplo 2 *A álgebra $\mathbb{C}$ é comutativa e associativa. A álgebra $\mathbb{H}$ é associativa e comutativa. A álgebra $\mathbb{O}$ é alternada mas não é associativa ou comutativa. Portanto $\mathbb{O} \oplus \mathbb{O}$ não é alternada e desse modo não pode ser uma álgebra normada.*

Proposição 4 (Hurwitz) *As únicas álgebras normadas sobre $\mathbb{R}$ são $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ e $\mathbb{O}$.*

Demonstração:

Considere uma álgebra normada B. Seja $A_1 = \Re B \cong \mathbb{R}$, então ou $A_1 = B$ ou existe $\epsilon_1 \in \Im B = A_1^{\perp}$ com $|\epsilon_1|^2 = 1$.

Considere $A_2 := A_1 + \epsilon_1 A_1 \subseteq B$. Temos $A_2 \cong A_1 \oplus A_1 \cong \mathbb{R} \oplus \mathbb{R} = \mathbb{C}$, assim se $A_2 = B$, nossa demonstração está completa.

Caso contrário, existe $\epsilon_2 \in A_2^{\perp}$ com $|\epsilon_2|^2 = 1$. Considere $A_3 := A_2 + \epsilon_2 A_2 \cong A_2 \oplus A_2 \cong \mathbf{H}$. Então $B = A_3$ ou existe $\epsilon_3 \in A_3^{\perp}$ com $|\epsilon_3|^2 = 1$.

Finalmente, considere $A_4 := A_3 + \epsilon_3 A_3 \cong A_3 \oplus A_3 \cong \mathbb{O}$. Então $B = A_3 \cong \mathbb{O}$ pois caso contrário o mesmo procedimento produziria uma subalgebra de B isomorfa a $\mathbb{O} \oplus \mathbb{O}$. Mas sabemos que $\mathbb{O} \oplus \mathbb{O}$ não é uma álgebra normada e isto é uma contradição.

$\odot$

Proposição 5 (Artin) *Qualquer subalgebra de $\mathbb{O}$, gerada por dois elementos de $\mathbb{O}$ é associativa.*

Corolário 1 *As álgebras $\mathbb{O}$, $\mathbb{H}$, $\mathbb{C}$ e $\mathbb{R}$ são normadas.*

$$|xy|^2 = (xy)(\overline{xy}) = (xy)(\overline{y}\overline{x}) = xy\overline{y}\overline{x} = |y|^2|x|^2 \quad \forall x, y \in \mathcal{O}.$$

O processo de Cayley-Dickson para construção de novas álgebras pode ser continuado a partir dos octônios produzindo álgebras de dimensão 16, 32, etc. Entretanto, nenhuma delas poderá ser mais de divisão, associativa ou normada. Com efeito, em Baez [BJC] é demonstrado que na álgebra de dimensão 16, obtida pelo processo, tem o conjunto de seus divisores de zero de norma unitária formando um subsespaço isomorfo ao Grupo de Lie excepcional G_2 que apresentamos e discutimos abaixo.

O produto interno de uma álgebra normada B é dado por $(x, y) = \Re x\overline{y}$. Vamos definir um produto cross $\times : B \times B \to \Im B$ em $\mathbb{R}^7$ do seguinte modo:

$$x \times y = \Im(\overline{y}x) = \frac{1}{2}(\overline{y}x - \overline{x}y) = -\frac{1}{2}(\overline{x}y - \overline{y}x) = -\Im(\overline{x}y).$$

Observe que esta aplicação é bilinear e alternada ($x \times x = 0$). Fazendo a restrição deste produto ao subconjunto $\Im B$ obtemos $\times : \Im B \times \Im B \to \Im B$.

Considerando $B = \mathbb{H}$ nós temos $\Im B \cong \mathbb{R}^3$ o qual nos dá $\times : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$, que é o produto vetorial usual de $\mathbb{R}^3$.

Por outro lado, considerando $B = \mathbb{O}$, temos $\Im B \cong \mathbb{R}^7$ produzindo um produto vetorial $\times : \mathbb{R}^7 \times \mathbb{R}^7 \to \mathbb{R}^7$, no espaço vetorial $\mathbb{R}^7$. Este produto vetorial satisfaz a seguinte propriedade fundamental:

$$u \times (v \times w) + (u \times v) \times w = 2(u, w)v - (u, v)w - (w, v)u. \tag{1}$$

e a partir dele, podemos definir um **produto triplo escalar** por $(u \times v, w)$ o qual é anti-simétrico. Em particular, $(u \times v, u) = 0$, ou seja, o vetor $u \times v$ é perpendicular a ambos vetores u e v.

O Grupo de Lie excepcional G_2 pode então ser obtido como o grupo de automorfismos de $\mathbb{O}$, ou seja,

$$G_2 = \{g \in GL_8(\mathbf{R}) : g(xy) = g(x)g(y) \ \ \forall x, y \in \mathcal{O}\}.$$

Observemos que
$$x \in \Im\mathbb{O} \Longleftrightarrow x^2 \in \Re\mathbb{O}^- \cong \mathbb{R}^-.$$
Portanto
$$g(x) \in \Im\mathbb{O} \Longleftrightarrow x \in \Im\mathbb{O}.$$
e assim, por linearidade
$$g(\overline{x}) = \overline{g(x)}.$$
Portanto g é uma isometria, uma vez que
$$|g(x)|^2 = g(x)\overline{g(x)} = g(x)g(\overline{x}) = g(x\overline{x}) = g(|x|^2) = |x|^2 g(1) = |x|^2.$$
Em outras palavras, G_2 é subgrupo de $O(8)$.

Notemos que cada elemento $g \in G_2$ age trivialmente sobre $\mathbb{R} = \Re\mathbb{O} \subset \mathbb{O}$, i.e. $g(r) = r\ \forall r \in \mathbb{R}$. Assim, nós podemos considerar g como uma aplicação de $\Im\mathbb{O}$ em $\Im\mathbb{O}$. E portanto G_2 é um subgrupo do grupo ortogonal $O(7)$ agindo sobre $\Im\mathbb{O} \cong \mathbb{R}^7$.

Por outro lado, uma vez que G_2 é conexo e contém a matriz identidade, temos que G_2 não é apenas subgrupo de $O(7)$ mas sim de $SO(7)$. Disto segue-se que G_2 pode ser considerado como o grupo de automorfismos da estrutura $(\mathbb{R}^7, \times)$ uma vez que $g(ab) = g(a)g(b)$ implica $g(a \times b) = g(a) \times g(b)$.

Definição 4 *Uma* **base-$\mathbf{G_2}$** *de* $\mathbb{R}^7$ *é uma base ortonormal* $\{f_1, \ldots, f_7\}$ *de* $\mathbb{R}^7$ *tal que*
$$f_3 = f_1 \times f_2,\ f_5 = f_1 \times f_4,\ f_6 = f_2 \times f_4,\ f_7 = f_3 \times f_4.$$

Portanto, se f_1, f_2, f_4 são vetores unitários e ortogonais tais que $f_4 \perp f_1 \times f_2$ então f_1, f_2, f_4 determina uma única G_2-base, ou seja a condição extra de ortogonalidade possibilita determinar uma base para o espaço 7-dimensional a partir de 4 vetores cumprindo as condições acima.

Exemplo 3 *A base canônica euclideana* $\{e_1, \ldots, e_7\}$ *of* $\mathbb{R}^7$ *é uma base-*G_2*.*

Proposição 6 *A estrutura* $(\mathbb{R}^7, \times)$ *é gerada pelos vetores* f_1, f_2, f_4 *subordinados às relações:*
$$f_i \times (f_j \times f_k) + (f_i \times f_j) \times f_k = 2\delta_{ik} f_j - \delta_{ij} f_k - \delta_{jk} f_i.$$
Em particular, qualquer subalgebra de $\mathbb{R}^7$ *deve ter dimensão 0,1,3 or 7.*

Uma base-G_2 tem a seguinte tábua de multiplicação:

$$f_i \times f_j \ =$$

$i \backslash j$	1	2	3	4	5	6	7
1	0	f_3	$-f_2$	f_5	$-f_4$	$-f_7$	f_6
2	$-f_3$	0	f_1	f_6	f_7	$-f_4$	$-f_5$
3	f_2	$-f_1$	0	f_7	$-f_6$	f_5	$-f_4$
4	$-f_5$	$-f_6$	$-f_7$	0	f_1	f_2	f_3
5	f_4	$-f_7$	f_6	$-f_1$	0	$-f_3$	f_2
6	f_7	f_4	$-f_5$	$-f_2$	f_3	0	$-f_1$
7	$-f_6$	f_5	f_4	$-f_3$	$-f_2$	f_1	0

Para quaisquer duas bases-G_2, digamos, $\{f_1,\ldots,f_7\}$ e $\{\tilde{f}_1,\ldots,\tilde{f}_7\}$ existe um único elemento $g \in G_2$ tal que $gf_i = \tilde{f}_i$ (simplesmente definimos g pela condição $gf_i = \tilde{f}_i$ e verificamos que este elemento está em G_2).

Também vemos que o elemento $g \in G_2$ que leva a base $\{e_1,\ldots,e_7\}$ na base $\{f_1,\ldots,f_7\}$ pode ser representado, na base canônica, pela matriz

$$(f_1|\ldots|f_7) \in SO(7).$$

Neste ponto é importante perceber que a estrutura algébrica $(\mathbb{R}^7,\times)$ induz uma estrutura adicional na esfera $S^6 \subset \mathbb{R}^7$ do seguinte modo. Para cada ponto $p \in S^6$, consideramos a aplicação $J_p : T_pS^6 \to T_pS^6$ dada por $J_p(v) = p \times v$.

As propriedades do produto $(\mathbb{R}^7,\times)$ mencionadas anteriormente nos dão de imediato que o tensor J cumpre a condição $J_p^2 = -I$ e assim com um pouco mais de geometria diferencial podemos obter (S^6, J) como uma variedade 6-dimensional munida de estrutura quase-complexa e quase khaleriana. Um dos estudos mais belos envolvendo esta estrutura é o das curvas quase-complexas de S^6 que são definidas como superfícies de S^6 cujos planos tangentes são invariantes sob ação de J. Estas curvas juntamente com a estrutura aqui apresentada são estudados em Bolton-Woodward [BW1].

Bibliografia

[BJC] Baez, John C. University of California, Departament of Mathematics - http://math.ucr.edu/home/baez/Octonions/node1.html

[BW1] J.Bolton, L.M.Woodward - Almost complex curves of constant curvature in the nearly K"ahler 6-sphere, Geometry and Topology of Submanifolds V, World Scientific, (1993) 54-67.

[HL] Harvey, Lawson - Calibrated Geometries, Acta Math. **148**, 47-157

[Ward] Ward, J.P. - Quaternions and Cayley numbers, Kluber Academic Publishers, 1997.

Prof. Dr. José Kenedy Martins.
Universidade Federal do Amazonas.
akay333@gmail.com
Fone 55-92-9122-8157

Semigrupos Numéricos e Corpos de Funções Algébricas

THIAGO FILIPE DA SILVA
Professor Assistente do Centro de Ciências Exatas da
Universidade Federal do Espírito Santo.

RESUMO

O estudo sobre o número de pontos racionais de uma curva algébrica não-singular encontra diversas aplicações em Geometria Algébrica, teoria de códigos corretores de erros e criptografia. A uma curva algébrica sobre um corpo associamos o que é chamado corpo de funções, que é uma extensão do corpo onde a curva está definida, e que tem algumas propriedades que serão destacadas neste trabalho. Baseado neste fato, faremos uma introdução à teoria de corpos de funções algébricas destacando os principais conceitos e também uma apresentação da teoria de semigrupos numéricos, que estão ligadas através do Teorema das Lacunas de Weierstrass. Finalmente apresentaremos o conceito de torres de corpos de funções com um exemplo de uma torre assintoticamente boa.

ABSTRACT

The study on the number of rational points of an nonsingular algebraic curve finds many applications in Algebraic Geometry, Algebraic Geometry Codes and Encryption. In an algebraic curve over a field we associate what is called functions fields, which is an extension of the field where the curve is defined, and that has some properties that will be highlighted in this work. Based on this fact will make an introduction to the theory of algebraic functions fields highlighting key concepts and also a presentation of the theory of numerical semigroups, which are linked through the Weierstrass Gap Theorem. Finally we present the concept of towers of functions fields with an example of an asymptotically good tower.

Palavras chaves: Corpos de Funções Algébricas, Semigrupos Numéricos, Torres de Corpos.

1. Introdução

O objetivo deste artigo é motivar os alunos concluintes da graduação, ou mesmo ingressantes no mestrado em Matemática, a prosseguirem na carreira acadêmica. Outro objetivo também é mostrar que alguns conceitos, a princípio bem abstratos que são desenvolvidos em um curso de Álgebra, tem grande importância no desenvolvimento de novas teorias.

A Teoria de Corpos de Funções é muita usada na Geometria Algébrica e veremos também como ela esta intimamente ligada a Teoria de Números, mais especificamente a Teoria de Semigrupos Numéricos.

Neste texto evitamos demonstrações, já que o objetivo é divulgar esta área de estudo, e para que a leitura não seja enfadonha.

O leitor dever estar familiarizado com alguns conceitos e resultados básicos de um primeiro curso de Álgebra.

Detalhes das demonstrações dos resultados exibidos: da seção de semigrupos numéricos podem ser encontrados em [1] e [4], da seção de corpos de funções em [2] e da seção de Torre de Corpos de Funções em [2], [3] e [4].

2. Semigrupos Numéricos

Vamos fazer uma revisão de alguns conceitos básicos sobre a teoria de semigrupos numéricos, dada a grande aplicação que existe na teoria de corpos de funções.

Seja $\mathbb{N}_0$ o conjunto dos números inteiros não-negativos e seja $\mathbb{N} \coloneqq \mathbb{N}_0 - \{0\}$.

Um subconjunto Λ de $\mathbb{N}_0$ é chamado um semigrupo quando $0 \in \Lambda$ e para todos $a, b \in \Lambda$ tem-se $a + b \in \Lambda$. O semigrupo Λ é chamado numérico quando $\mathbb{N}_0 - \Lambda$ for finito. Neste caso o número $g = |\mathbb{N}_0 - \Lambda|$ chama-se o gênero de Λ e $\mathbb{N}_0 - \Lambda$ é chamado o conjunto das lacunas de Λ.

No caso em que Λ é um semigrupo numérico, existe um elemento mínimo $c \in \Lambda$ com a propriedade que para todo $x \in \mathbb{N}_0$ com $x \geq c$ tem-se $x \in \Lambda$. Tal elemento c é chamado de *condutor* de Λ.

Dado H subconjunto não-vazio de $\mathbb{N}_0$ define-se o conjunto $\langle H \rangle = \{a_1x_1 + \cdots + a_mx_m /\ x_1, \dots, x_m \in H, a_1, \dots, a_m \in \mathbb{N}_0 \ e\ m \in \mathbb{N}\}$ que claramente é *um semigrupo de* $\mathbb{N}$ *e é chamado o semigrupo gerado por* H. *Quando* H *é finito e é escrito por* $H = \{\lambda_1, \dots, \lambda_m\}$ *então usamos a notação* $\langle \lambda_1, \dots, \lambda_m \rangle$ *para simbolizar* $\langle H \rangle$.

É conhecido que um semigrupo finitamente gerado é numérico se, e somente se, o máximo divisor comum de seus geradores é igual a 1.

2.1 Definição *Seja* $(a_1, \dots, a_m)$ *uma sequência de números inteiros positivos. Para cada* $i \in \{1, \dots, k\}$ *seja* $d_i = mdc(a_1, \dots, a_i)$. *A sequência* $(a_1, \dots, a_k)$ *é chamada telescópica quando* $d_k = 1$ *e* $\frac{a_i}{d_i} \in \langle \frac{a_1}{d_{i-1}}, \dots, \frac{a_{i-1}}{d_{i-1}} \rangle$, *para todo* $i \in \{2, \dots, k\}$. *Um semigrupo* Λ *de* $\mathbb{N}_0$ *é chamado telescópico quando é gerado por uma sequência telescópica.*

2.2 Exemplos

(1) Seja $\Lambda = \langle 4, 6, 5 \rangle$. Chame $a_1 = 4$, $a_2 = 6$ e $a_3 = 5$. Sendo $d_i = mdc(a_1, \dots, a_i)$, para todo $i \in \{1,2,3\}$, segue que $d_1 = 4$, $d_2 = 2$ e $d_3 = 1$. Observe que $\frac{a_3}{d_3} = 5, \frac{a_1}{d_2} = 2, \frac{a_2}{d_2} = 3$ e $5 = 1 \cdot 2 + 1 \cdot 3$. Portanto Λ é um semigrupo telescópico.

(2) Seja $\Gamma = \langle 34, 4, 62, 97 \rangle$. Chame $a_1 = 34$, $a_2 = 4$, $a_3 = 62$ e $a_4 = 97$ e $d_i = mdc(a_1, \dots, a_i)$, para todo $i \in \{1, 2, 3, 4\}$. Logo, $d_1 = 34$, $d_2 = 2$, $d_3 = 2$ e $d_4 = 1$. Observe que $\frac{a_4}{d_4} = 97$, $\frac{a_1}{d_3} = 17$, $\frac{a_2}{d_3} = 2$, $\frac{a_3}{d_3} = 31$ e $97 = 1 \cdot 17 + 9 \cdot 2 + 2 \cdot 31$. Temos também que $\frac{a_3}{d_3} = 31$, $\frac{a_1}{d_2} = 17$, $\frac{a_2}{d_2} = 2$ e $31 = 1 \cdot 17 + 7 \cdot 2$. Portanto Γ é um semigrupo telescópico.

2.3 Definição *Seja* Λ *um semigrupo numérico de* $\mathbb{N}_0$ *de gênero* g *e condutor* c. *Dizemos que* Λ *é um semigrupo simétrico quando* $c = 2g$.

Sendo Λ um semigrupo numérico com maior lacuna l, é conhecido que Λ é simétrico se, e somente se, para toda lacuna s de Λ tem-se que $l - s$ é uma não lacuna. Daí a nomenclatura "simétrico".

O próximo teorema fornece uma fórmula que expressa o gênero de um semigrupo telescópico em termos de seus geradores, além de provar que todo semigrupo telescópico é simétrico. Esta fórmula será usada na demonstração de um teorema envolvendo torres de corpos de funções.

2.4 Teorema *Sejam* $k \in \mathbb{N}$, $k \geq 2$, $(a_1, \ldots, a_k)$ *uma sequência telescópica,* $\Lambda = \langle a_1, \ldots, a_k \rangle$, $d_i = mdc(a_1, \ldots, a_i)$ *para cada* $i \in \{1, \ldots, k\}$ *e* $g = |\mathbb{N}_0 - \Lambda|$.

a) Se $\Gamma = \langle \frac{a_1}{d_{k-1}}, \ldots, \frac{a_{k-1}}{d_{k-1}} \rangle$ *e* $g' = |\mathbb{N}_0 - \Gamma|$ *então* $g = d_{k-1}g' + \frac{(d_{k-1}-1)(a_k-1)}{2}$;

b) O semigrupo Λ *é simétrico. Em particular*

$$g = \frac{1}{2}\left(1 + \sum_{i=1}^{k}\left(\frac{d_{i-1}}{d_i} - 1\right)a_i\right) \text{ onde } d_0 = 0.$$

Desse modo, os semigrupos telescópicos $\langle 4, 6, 5 \rangle$ e $\langle 34, 4, 62, 97 \rangle$ considerados nos exemplos anteriores têm gênero 4 e 64, respectivamente.

3. Introdução à Teoria de Corpos de Funções

A seguir passamos a introduzir a linguagem básica para a teoria dos corpos de funções algébricas: lugares, divisores, gênero e semigrupos de Weierstrass.

Em todo este texto K é um corpo arbitrário.

3.1 Definição *Seja* F/K *uma extensão de corpos. Dizemos que* F/K *é um corpo de funções algébricas ou simplesmente corpo de funções quando existir* $x \in F$ *transcendente sobre* K *tal que a extensão* $F/K(x)$ *é finita.*

Um exemplo simples de um corpo de funções é o *corpo de funções racional* $K(x)/K$, onde $K(x)$ é o corpo de frações do anel de polinômios $K[x]$.

3.2 Definição *Um anel de valorização de um corpo de funções* F/K *é um subanel* $\mathcal{O} \subset F$ *com as seguintes propriedades:*

a) $K \subsetneq \mathcal{O} \subsetneq F$;

b) Para todo $z \in F - \{0\}$ *tem-se* $z \in \mathcal{O}$ *ou* $z^{-1} \in \mathcal{O}$.

3.3 Exemplo Dado um polinômio mônico e irredutível $p(x) \in K[x]$, o conjunto $\mathcal{O}_{p(x)} = \left\{\frac{f(x)}{g(x)} / f(x), g(x) \in K[x] \text{ e } p(x) \nmid g(x)\right\}$ é um anel de valorização de $K(x)/K$. E ainda, se $q(x) \in K[x]$ é outro polinômio mônico e irredutível, então $\mathcal{O}_{q(x)} \neq \mathcal{O}_{p(x)}$.

Qualquer anel de valorização $\mathcal{O}$ de um corpo de funções F/K é um anel local, ou seja, possui um único ideal maximal P, que será chamado um *lugar* do corpo de funções. Além disso P é um ideal principal, ou seja, existe $t \in \mathcal{O}$ tal que $P = t\mathcal{O}$ (tal elemento t é chamado uniformizante local de P). Desse modo, para cada elemento z em F não-nulo, existe um único inteiro n e um invertível u em $\mathcal{O}$ tal que $z = t^n u$. Tal inteiro não depende da escolha do uniformizante local, e assim é definido como sendo a *valorização* de z por P, e é denotada por $v_P\ (z)$. Definimos $v_P\ (0) = \infty$.

O conjunto dos lugares de um corpo de funções F/K é denotado por $\mathbb{P}_F$.

Sendo P o ideal maximal de um anel de valorização $\mathcal{O}$, segue que o anel quociente $\frac{\mathcal{O}}{P}$ é um corpo que contém um subcorpo que é isomorfo a K, logo $\frac{\mathcal{O}}{P}$ é um espaço vetorial sobre K. É conhecido que este espaço vetorial possui dimensão finita, que será denotada por $degP$ e também será chamada *grau de* P. Dizemos que um lugar P é racional quando $degP = 1$.

Um *divisor* em um corpo de funções é uma soma formal $\sum_{P \in \mathbb{P}_F} n_P P$ onde $n_P \in \mathbb{Z}$ para todo lugar P e $n_P \neq 0$ apenas para uma quantidade finita de lugares.

3.4 Definição *Um lugar* P *é um zero de um elemento* $z \in F$ *se* $v_P\ (z) > 0$, *e* P *é um polo de* z *se* $v_P\ (z) < 0$. *Se* $v_P\ (z) = m > 0$ *então dizemos que* P *é um zero de* z *com ordem* m. *Se* $v_P\ (z) = m < 0$ *então dizemos que* P *é um polo de* z *com ordem* m.

É conhecido que qualquer elemento não-nulo z em um corpo de funções tem apenas uma quantidade finita de zeros e polos. Assim, sendo $x \in F - \{0\}$, Z o conjunto dos zeros de x e N o conjunto dos polos de x definimos os seguintes divisores:

$(x)_0 \coloneqq \sum_{P \in Z} v_P\ (x) P$ como sendo o divisor dos zeros de x;

$(x)_\infty \coloneqq \sum_{P \in N} v_P\ (x) P$ como sendo o divisor dos polos de x e $(x) \coloneqq (x)_0 - (x)_\infty$ como sendo o divisor principal de x.

O semigrupo de Weierstrass de um lugar P é o conjunto $N(P) \coloneqq \{n \in \mathbb{N}_0 / (x)_0 = nP\ para\ algum\ x \in F - \{0\}\}$. É possível mostrar que este conjunto é um semigrupo numérico, ou seja, é fechado para a soma e tem um número finito de lacunas. Não pretendemos dar a definição de *gênero* de um corpo de funções neste texto, mas o Teorema das Lacunas de Weierstrass afirma que o gênero de um corpo de funções é exatamente o gênero do semigrupo de Weierstrass de um lugar racional.

4. Torre de Corpos de Funções

Adiante, passamos a estudar um novo conceito que é muito utilizado na Teoria de Códigos Corretores de Erros que são as torres de corpos de funções. Para a construção de códigos com bons parâmetros, é desejável trabalhar em corpos de funções com um grande número de lugares racionais. Daí se justifica o estudo do comportamento assintótico de torres, a fim de saber se em uma sequência de corpos de funções é possível encontrar um que tenha o número adequado de lugares racionais.

Uma sequência $(F^{(1)}/K, F^{(2)}/K, \dots)$ de corpos de funções é chamada *torre* se $F^{(i)} \subset F^{(i+1)}$, para todo $i \in \mathbb{N}$. Denotamos o corpo finito com q elementos por $\mathbb{F}_q$. É conhecido que um corpo de funções $F/\mathbb{F}_q$ sobre um corpo finito tem uma quantidade finita de lugares racionais. Tal quantidade será denotada por $N(F)$.

Dada uma torre $(F^{(1)}/\mathbb{F}_q, F^{(2)}/\mathbb{F}_q, \dots)$ escrevemos $N^{(i)} = N(F^{(i)})$ e $g^{(i)} = g(F^{(i)})$ (gênero de $F^{(i)}/K$). Dizemos que uma torre de corpos de funções é *assintoticamente boa* quando $\lim_{i\to\infty} g^{(i)} = \infty$ e $\lim_{i\to\infty} inf \frac{N^{(i)}}{g^{(i)}} = k > 0$. Esta segunda condição satisfeita nos diz que o número de lugares racionais é grande em relação ao gênero, que já explode para o infinito à medida que se aumenta o nível da torre.

O próximo resultado faz uma associação entre o conceito de semigrupos telescópicos e a busca por torres assintoticamente boas.

4.1 Teorema *Seja $(F^{(1)}/\mathbb{F}_q, F^{(2)}/\mathbb{F}_q, \dots)$ uma torre de corpos de funções tal que para uma infinidade de índices i tem-se que $F^{(i)}$ possui um lugar racional $P^{(i)}$ com semigrupo de Weierstrass telescópico igual a $\Lambda^{(i)}$. Então a torre $(F^{(1)}/\mathbb{F}_q, F^{(2)}/\mathbb{F}_q, \dots)$ não é assintoticamente boa.*

4.2 Exemplo Sejam $q = l^2$, onde l é uma potência de um primo ímpar, (x_n) uma sequência tal que $x_{n+1}^2 = \frac{1+x_n^2}{2x_n}$ e $F^{(n)} = \mathbb{F}_q(x_0, \dots, x_n)$, para todo $n \in \mathbb{N}_0$, com x_0 transcendente sobre $\mathbb{F}_q$.

Então a torre $\mathcal{F} = (F^{(0)}/\mathbb{F}_q, F^{(1)}/\mathbb{F}_q, \dots)$ é assintoticamente boa.

Referências Bibliográficas

[1] Hoholdt, T., van Lint, J. e Pellikaan, R., *Algebraic Geometry Codes*, V.S. Pless, W. C. huffman (Eds.), Handbook of Coding Theory, vol. 1, Elsevier, Amsterdam, 1998, pp.871-961. (Chapter 10).

[2] Stichtenoth, H., *Algebraic Function Fields and Codes*, (Universitext)(Springer 2009).

[3] Geil, O. e Matsumoto, R., *Bounding the Number of rational places using Weierstrass Semigroups*, Journal of Pure and Applied Algebra, 213, (6), 2009, pp.1152-1156.

[4] da Silva, T. F, *Cotas Superiores para o Número de Pontos Racionais e Aplicações às Torres de Corpos de Funções*, Dissertação de Mestrado, 2010 - UFES

Universidade Federal do Espírito Santo, Vitória - ES, Brasil
E-mail address: thiago.filipe@hotmail.com
URL: www.ufes.br

UMA DEMONSTRAÇÃO ALTERNATIVA DE UM RESULTADO DE HERMANN HEINEKEN SOBRE GRUPOS QUE SATISFAZEM A TERCEIRA CONDIÇÃO DE ENGEL

Sérgio Brazil Júnior

Resumo

Um grupo G é dito grupo Engel se para cada $x, y \in G$ existe $n \in \mathbb{N}$, n dependendo de x e y, tal que $[\underbrace{x, x, \ldots, x}_{n\ vezes}, y] = 1$. Se n pode ser escolhido independente de x e y, dizemos que G é um grupo satisfazendo a n-ésima condição de Engel e o denotaremos por $\mathcal{E}_n$-grupo. Hermann Heineken , em 1961, mostra em seu artigo *Engelsche Elemente der Länge Drei*, além de muitos resultados relevantes sobre os $\mathcal{E}_3$-grupos , que se G é um grupo satisfazendo a terceira condição de Engel, então todo subgrupo gerado por dois elementos é metabeliano e nilpotente de classe no máximo 4. Este não é o principal resultado de Heineken sobre os $\mathcal{E}_3$-grupo, no entanto, nosso objetivo no presente trabalho é apresentar uma demonstração alternativa e bem mais simples desse resultado.

Abstract

A group G is considered an Engel's group if for each $x, y \in G$ exist $n \in \mathbb{N}$, n depending on the x e y , such as $[\underbrace{x, x, \ldots, x}_{n\ times}, y] = 1$. If n can be chosen independent on the x and y, we say that G is a group satisfying the n^{th} condition of Engel and we will denote by $\mathcal{E}_n$-group. Hermann Heineken, in 1961, shows in his article *Engelsche Elemente der Länge Drei*, besides many relevant results about $\mathcal{E}_3$-groups, that if G is a group satisfying Engel's third condition, so all subgroup generated by two elements is metabelian and nilpotent of class at most 4. This is not the main result in Heineken's about the $\mathcal{E}_3$ -groups, nonetheless, our objective in the present work is to present an alternative and even simpler demonstration of this result.

Palavras Chaves: Grupos, 3ª Condição de Engel.

1. Introdução

Um grupo G é dito nilpotente de classe no máximo n se $[x_1, x_2, \dots, x_{n+1}] = 1$, para todo $x_i \in G, i \in \{1, 2, \dots, n+1\}$. Se para todo subconjunto finito X de G o subgrupo $\langle X \rangle$, é nilpotente, dizemos que G é localmente nilpotente. Um grupo G é dito grupo Engel se para cada $x, y \in G$ existe $n \in \mathbb{N}$, n dependendo de x e y, tal que $[\underbrace{x, x, \dots, x}_{nvezes}, y] = 1$. Se n pode ser escolhido independente de x e y, dizemos que G é um grupo satisfazendo a n-ésima condição de Engel e o denotaremos por $\mathcal{E}_n$-grupo. Claramente, grupos localmente nilpotentes são grupos de Engel, assim como grupos nilpotentes de classe no máximo n são $\mathcal{E}_n$-grupo. Dado isto, surgem, naturalmente, três questões:

1) Todo $\mathcal{E}_n$-grupo é nilpotente?
2) Todo grupo de Engel é localmente nilpotente?
3) Todo $\mathcal{E}_n$-grupo é localmente nilpotente?

A resposta para as duas primeiras questões é negativa, veja o exemplo de K. Weston em Brazil (1997), página 16 e Golod (1966), respectivamente. Apesar disto existem classes importantes de grupos onde a condição de Engel implica em nilpotência local. Zorn (1936) mostra esta implicação na classe dos grupos finitos, Gruenberg (1953), na classe dos grupos solúveis e Baer (1957), na classe dos grupos com a condição maximal. Apesar de muito esforço nesta área, a terceira questão, ainda, é um problema em aberto. Porém, para o caso onde o grupo é residualmente finito, esta questão foi respondida positivamente por Wilson (1991). A resposta, para esta questão, também é positiva para os casos onde $n \leq 3$. Brazil (1997) faz um estudo aprofundado sobre os $\mathcal{E}_2$-grupos, $\mathcal{E}_3$-grupos, demonstando os resultados dados por Levi (1942), no caso dos $\mathcal{E}_2$-grupos, e os resultados dados por Heineken (1961) e L. Kappe e W. Kappe (1972), sobre os $\mathcal{E}_3$-grupos. Ainda neste mesmo trabalho, faz um estudo sobre os resultados dados por Traustason (1995), que trata dos $\mathcal{E}_4$-grupos.

Heineken (1961) mostra em seu artigo *Engelsche Elemente der Länge Drei*, além de muitos resultados relevantes, que se G é um $\mathcal{E}_3$-grupo, então todo subgrupo gerado por dois elementos é metabeliano e nilpotente de classe no máximo 4. Nosso objetivo no presente trabalho é apresentar uma demonstração alternativa e bem mais simples desse resultado.

2. Preliminares

Definição 1: Seja G um grupo e x, y elementos de G. Definimos o comutador de x e y como sendo o elemento

$$[x, y] = x^{-1}y^{-1}xy = x^{-1}x^y.$$

O seguinte lema segue imediatamente da definição acima.

Lema 1: Seja G um grupo e x, y, z elementos de G. Então

i) $x^y = x[x,y]$;

ii) $xy = yx[x,y] = [x^{-1}, y^{-1}]yx$;

iii) $[x,y] = [y,x]^{-1} = [y^{-1}, x]^y = [y, x^{-1}]^x$;

iv) $[x,y]^z = [x^z, y^z]$;

v) $[x, yz] = [x,z][x,y]^z$;

vi) $[xy, z] = [x,z]^y[y,z]$;

vii) $[x,[y,z^{-1}]]^z\,[z,[x,y^{-1}]]^y[y,[z,x^{-1}]]^x = 1$ **(Identidade de Hall-Witt)**

O subgrupo

$$G' = [G,G] = \langle [x,y] \mid x, y \in G \rangle$$

é chamado de subgrupo comutador ou derivado de G.
Definimos, também, comutadores simples normado à direita de peso ≥ 2, recursivamente por

$$[x_1, x_2, \dots, x_n] = [x_1, [x_2, \dots, x_n]].$$

Definição 2: Um grupo G é dito nilpotente de classe no máximo n se

$$[x_1, x_2, \dots, x_{n+1}] = 1,$$

para todo $x_i \in G, i \in \{1, 2, \dots, n+1\}$.

Definição 3: Um grupo G é dito metabeliano, se existe N abeliano, $N \lhd G$ com G/N abeliano.
A definição 3 acima, obviamente, implica que G é metabeliano se, e somente se, G' é abeliano.

Definição 4: Um grupo G é dito grupo Engel se para cada $x, y \in G$ existe $n \in \mathbb{N}$, n dependendo de x e y, tal que

$$[\underbrace{x, x, \dots, x}_{n vezes}, y] = 1.$$

Se n pode ser escolhido independente de x e y, dizemos que G é um grupo satisfazendo a n-ésima condição de Engel e o denotaremos por $\mathcal{E}_n$-grupo.

3. Resultados relevantes relacionando os $\mathcal{E}_n$-grupo, $n = 1, 2, 3, 4$ e nilpotência.

O caso em que $n = 1$ é trivial, uma vez que os $\mathcal{E}_1$-grupos são exatamente os grupos abelianos.

No caso $n = 2$, Levi, em 1942, mostrou que os $\mathcal{E}_2$-grupos são nilpotentes de classe no máximo 3.

Para o caso $n = 3$, Heineken, em 1961, deu uma contribuição muito importante, provando que todo $\mathcal{E}_3$-grupo é localmente nilpotente e, ainda, que um $\mathcal{E}_3$-grupo é nilpotente de classe no máximo 4, se este não possuir elementos de ordem 2 ou 5. Em 1971, Bachmuth e Mochizuki construíram exemplos de 2-grupos e 5-grupos, satisfazendo a terceira condição de Engel, que não são nilpotentes. Ainda para $n = 3$, L. Kapper e W. Kapper, em 1972, deram uma caracterização para os $\mathcal{E}_3$-grupos, mostrando que são equivalentes as seguintes afirmações:

(1) Classe de nilpotência de $\langle x^G \rangle$ é no máximo 2, para todo $x \in G$;

(2) $\langle x^G \rangle$ é um $\mathcal{E}_2$-grupo, para todo $x \in G$;

(3) Gé um $\mathcal{E}_3$-grupo.

Demonstrando, com isso, que um $\mathcal{E}_3$-grupo com n geradores possui classe de nilpotência no máximo $2n$.

Os primeiros resultados relevantes sobre os $\mathcal{E}_4$-grupos apareceram em 1994 e são devidos a Vaughan-Lee e Gunnar Traustason. Este último contribuiu com o estudo dos $\mathcal{E}_4$-grupos, mostrando que, se Gé um $\mathcal{E}_4$-grupo, então, os elementos de torção formam um subgrupo, e que o quociente de tal subgrupo pelo seu centro é um produto de p-grupos. Mostrou, ainda, que, se Gé um 2-grupo ou 3-grupo, satisfazendo a quarta condição de Engel, então G é localmente finito. Além disso, se Gé um p-grupo, onde p é um primo diferente de 2 ou 3, e $rad(G)$ é o radical localmente nilpotente de G, então $G/rad(G)$ possui expoente dividindo p. Vaughan-Lee, em 1997, mostra que os $\mathcal{E}_4$-grupos de expoente 5 são localmente finitos.

Para os casos onde $n > 4$, não sabemos se existem resultados relevantes. O que podemos observar é que o nível de dificuldade aumenta quando n cresce.

A seguir apresentaremos uma demonstração alternativa e bem mais simples de um resultado de Heineken sobre o $\mathcal{E}_3$-grupos. Para tanto, seja o seguinte

Lema2: Se Gé um $\mathcal{E}_3$-grupo e $a, b \in G$, então $\big[[a,b],[a,b],a\big] = 1$

Demonstração: Sendo G um $\mathcal{E}_3$-grupo, temos

$$
\begin{aligned}
1 &= [a, a, a, b^{-1}] \\
&= \left[a, a, a^{-1}a^{b^{-1}}\right] \\
&= [a, a, a^{b^{-1}}] && (1)
\end{aligned}
$$

Conjugando por b, obtemos

$$
\begin{aligned}
1 &= [a^b, a^b, a] \\
&= [a^b, [a, b], a] && (2)
\end{aligned}
$$

Porém,

$$
\begin{aligned}
\big[[a, b], [a, b], a\big] &= [a^{-1}a^b, [a, b], a] \\
&= [a^{-1}, [a, b], a]^{a^b}[a^b, [a, b], a] \\
&= [a^{-1}, [a, b], a]^{a^b} && \text{por} \quad (2) \\
&= [a^{-1}, [a, a, b]^{-1}]^{a^b} \\
&= 1
\end{aligned}
$$

■

Uma conseqüência imediata do Lema1 acima é que $[a, b]$comuta com $[a, b]^a$.

Agora estamos em condições de demonstrar o seguinte

Teorema: Se G é um $\mathcal{E}_3$-grupo e $a, b \in G$, então $\langle a, b\rangle$ é metabeliano e nilpotente de classe no máximo 4.

Demonstração: Mostraremos, primeiramente, que

$$\langle a, b\rangle' = \langle [a, b], [a, b]^a, [a, b]^b, [a, b]^{ab}\rangle$$

e é abeliano.

Claramente, $H = \langle [a, b], [a, b]^a, [a, b]^b, [a, b]^{ab}\rangle \leq \langle a, b\rangle'$, uma vez que $[a, b] \in \langle a, b\rangle' \trianglelefteq \langle a, b\rangle$. Já que $\langle a, b\rangle'$ é o fecho normal de $[a, b]$ em $\langle a, b\rangle$, basta mostrar que $H \trianglelefteq \langle a, b\rangle$. Ora, isso é conseqüência das relações abaixo, observando que estas seguem utilizando naturalmente o Lema 1 e usando, algumas vezes, u^{g+h} como notação abreviada para $u^g . u^h$. Isto quer dizer que $u^{(g+h)} . u^{(p+q)} = u^{(g+h)p} . u^{(g+h)q}$ o qual, não necessariamente, é igual a $u^{g(p+q)} . u^{h(p+q)}$.

$$
\begin{aligned}
&[a, b]^{a^{-1}} = [a, b]^{-a+2}; \\
&[a, b]^{b^{-1}} = [a, b]^{-b+2}; \\
&[a, b]^{a^2} = [a, b]^{2a-1}; \\
&[a, b]^{b^2} = [a, b]^{2b-1}; \\
&[a, b]^{ab^{-1}} = [a, b]^{b^{-1}}[a, b][a, b]^{-ab}[a, b]^{-1}[a, b]^{2a}[a, b]^{-b^{-1}};
\end{aligned}
$$

$$[a,b]^{ba} = [a,b][a,b]^{ab}[a,b]^{-1};$$
$$[a,b]^{ba^{-1}} = [a,b]^{-a^{-1}}[a,b]^{-ab}[a,a^b]^{2b}[a,b]^{a^{-1}};$$
$$[a,b]^{aba} = [a,b][a,b]^{2ab}[a,b]^{-b}[a,b]^{-1};$$
$$[a,b]^{aba^{-1}} = [a,b]^{-a^{-1}}[a,b]^{b}[a,b]^{a^{-1}};$$
$$[a,b]^{abb} = [a,b]^{-b}[a,b]^{2ab}[a,b]^{-1}[a,b]^{-a}[a,b]^{1+b}.$$

Do Lema 2, temos que $[a,b]$ comuta com $[a,b]^a$ e $[a,b]^b$.

Trocando a por ab, no Lema 1, temos que $[a,b]$ comuta com $[a,b]^{ab}$.

Logo $[a,b] \in Z(\langle a,b\rangle')$, que é característico em $\langle a,b\rangle'$ e, daí, $Z(\langle a,b\rangle') \trianglelefteq \langle a,b\rangle$, o que acarreta $\langle a,b\rangle'$ abeliano e, portanto, $\langle a,b\rangle$ metabeliano.

Claramente,

$$[b,a,a,b] \in Z(\langle a,b\rangle) \tag{1}$$

e

$$[b,b,a,b] = [b,b,b,a]^{-1} = 1 \tag{2}$$

Para mostrarmos que $\langle a,b\rangle$ é nilpotente de classe no máximo 4, demonstraremos que

$$[x_1,x_2,x_3,x_4,x_5] = 1$$

para $x_1,x_2,x_3,x_4,x_5 \in \{a,b\}$.

O que ocorre, realmente por (1) e (2), logo $\langle a,b\rangle$ é nilpotente de classe no máximo 4.

■

Essa demonstração foi concebida na elaboração da dissertação de mestrado do autor deste texto, em 1997, na Universidade de Brasília-UnB, sob a orientação do Professor Pavel Shumyatsky.

REFERÊNCIAS BIBLIOGRÁFICAS

BACHMUTH, S. and MOCHIZUKI, H. Y.. **Third Engel Groups and the Macdonald-Neumann Conjecture**, Bull. Austral. Math. Soc. 5 (1971), 379-386.

BAER, R..**Engelsche Elemente Noetherscher Gruppen**, Math. Ann. 133 (1957), 256-270.

BRAZIL, SÉRGIO JUNIOR. **Condição de Engel em Teoria dos Grupos,** Dissertação de Mestrado, UnB, (1997).

GOLOD, E. S.. **Some Problems de Burnside Type**, in “Proc. Int. Congr. Math., Moscow, 1966”, pp. 284-289, 1968; Englisch Translation, in Amer. Math. Soc. Transl. Ser. 2, Vol.84, pp. 83-88, Amer. Math. Soc., Providence, RI, 1969.

GRUENBERG, K. W.. **Two Theorems on Engel Groups**, Math. Proc. Cambridge Philos. Soc. 49 (1953), 377-380.

HEINEKEN, H. **Engelsche Elemente der Länge Drei**, Illinois J. Math. 5 (1961), 681-707.

KAPPE, L. C. and KAPPE, W. P.. **On Three-Engel Groups**, Bull. Austral. Math. Soc. 7 (1972).

LEVI, F. W.. **Groups in Which the Commutator Operation Satisfies Certain Algebraic Conditions**, J. Indian Math. Soc. 6 (1942), 87-97.

TRAUSTASON, G.. **On 4-Engel Groups**, J. Algebra 178 (1995), 414-429.

VAUGHAN-LEE, M. R.. Engel-4 Groups of exponent 5, Proc. London. Math. Soc. (3) 74 (1997), 306-334.

WILSON, J. S.. **Two Generator Conditions for Residually Finite Groups**, Bull. London Math. Soc. 23 (1991), 239-248.

ZORN, M.. **Nilpotency of Finite Groups**, Bull. Amer. Math. Soc. 42 (1936), 485-486.

Sérgio Brazil Júnior
Centro de Ciências Exatas e Tecnológicas
Universidade Federal do Acre
Rio Branco Acre
sbrazil@ufac.br
(68)9984-1922

SEMIGRUPOS ASSOCIADOS A GERMES DE CURVAS PLANAS IRREDUTÍVEIS[1]

LEANDRO NERY DE OLIVEIRA

Professor Assistente do Centro de Ciências Exatas e

Tecnológicas da Universidade Federal do Acre.

RESUMO

Os semigrupos numéricos são estruturas simples e que não necessitam de uma teoria muito forte para a sua compreensão. No entanto, sua aplicação dentro da própria matemática como fora dela é surpreendente, passando pelas curvas algébricas até a teoria dos códigos corretores de erros. Neste artigo de revisão, veremos uma associação entre germes de uma curva plana irredutível e semigrupos numéricos, chamado semigrupo de valores.

ABSTRACT

The numerical semigroups are simple structures that do not require a strong theory for their understanding. However, its application within and outside mathematics itself is amazing, through algebraic curves to the theory of error correcting codes. In this review, we see an association between a plane curve germs of irreducible numerical semigroups, called semigroup of values.

Palavras chaves: Semigrupos, Curvas Planas, Germes de Curvas.

---

[1] Como esse artigo foi fruto de pesquisa para a dissertação de mestrado [5], quero dar um agradecimento especial ao Prof. Dr. Leonardo Meireles Câmara - UFES, que me orientou nesses estudos.

1. Introdução

Iniciamos este artigo enunciando os resultados e definições iniciais na teoria de semigrupos numéricos. Veremos como a Apéry-sequência nos ajuda a calcular um conjunto de geradores de um semigrupo e como expressar um semigrupo por meio de sistema mínimos de geradores. A partir daí, faremos uma explanação geral sobre a teoria de curvas planas com o objetivo de relacionar curvas do tipo $f(X,Y)=0$, com um elemento irredutível f em $\mathbb{C}[[X,Y]]$, com um semigrupo. Esse semigrupo é definido como semigrupo de valores.

Consideremos G um subconjunto dos naturais contendo 0 (zero). Temos as seguintes definições:

1.1 Definição

a) Dizemos que G é um semigrupo numérico de $\mathbb{N}$ se G é fechado em relação à operação usual de adição.

b) Sendo G um semigrupo, definimos o conjunto das lacunas de G como o conjunto $L_G = \mathbb{N}\backslash G$. No caso em que $L_G = \{l_1 < l_2 < \cdots < l_g\}$ for finito chamaremos a maior lacuna l_G de número de Frobenius de G.

   Além disso, existe um único elemento $c \in G$ tal que

   i) $c - 1 = l_g \notin G$;

   ii) para todo $z \in \mathbb{N}$ temos $c + z \in G$.

   Esse elemento será chamado de *condutor* do semigrupo G.

c) O número $m = mín(G \setminus \{0\})$ é chamado de *multiplicidade* do semigrupo G.

1.2 Exemplos

1. Seja $G_1 = \{0, 5, 6, 7, 8, 9, \dots\}$. Obviamente, G_1 é semigrupo. O conjunto das lacunas de G_1 é $L_{G_1} = \mathbb{N} \setminus G^1 = \{1,2,3,4\}$ e, além disso, o condutor de G_1 é o número $c = 5$ e o número de Frobenius é $l_g = 4$. Observe que a multiplicidade de G_1 é 5.
2. Seja $G_2 = \{0, 2, 4, 6, 8, 10, \dots\}$. Temos que $L_{G_1} = \{1, 3, 5, 7, 9, 11, \dots\}$ é o conjunto das lacunas e não existe condutor em G_2. Além disso, G_2 tem multiplicidade 2.

Observe que se representamos um semigrupo da forma

$$G = \{0, g_1, g_2, \ldots, g_n, \ldots\},$$

poderia restar dúvidas se os sucessores de g_n, no semigrupo, são todos os naturais maiores que g_n. Para evitar esses equívocos, expressaremos um semigrupo G por meio de seus geradores. Para isso precisamos determinar os geradores desse semigrupo.

Existe uma sequência, chamada sequência de Apéry, que nos ajudar a construir um conceito na direção de um conjunto de geradores de um semigrupo.

Sejam G um semigrupo com condutor c e p qualquer elemento não nulo de G. Tomemos $a_0 := 0$, e indutivamente

$$a_j = mín\left(G \setminus \bigcup_{i=0}^{j-1} (a_i + p\mathbb{N}) \right)$$

para cada j, $1 \leq j \leq p - 1$; onde $a_i + p\mathbb{N} = \{a_i + \lambda p : \lambda \in \mathbb{N}\}$. A sequência $a_0 < a_1 < \cdots < a_{p-1}$ é chamada de *Apéry-sequência* em relação a p e o conjunto $A_p = \{a_0,\ a_1,\ \ldots, a_{p-1}\}$ é o *Apéry-conjunto* de G em relação a p.

Seja $G = \{0, 4, 5, 6, 7, \ldots\}$ um semigrupo com condutor 4 e seja $p = 6 \in G$. Temos pela definição que $a_0 = 0$ e que

$$0 + 6\mathbb{N} = \{0, 6, 12, 18, \ldots\} \Rightarrow a_1 = mín(G \backslash 6\mathbb{N}) = 4;$$

$$4 + 6\mathbb{N} = \{4, 10, 16, 22, \ldots\} \Rightarrow a_2 = mín[G \backslash (6\mathbb{N} \cup (4 + 6\mathbb{N}))] = 5;$$

$$5 + 6\mathbb{N} = \{5, 11, 17, 23, \ldots\} \Rightarrow a_3 = 7;$$

$$7 + 6\mathbb{N} = \{7, 13, 19, 25, \ldots\} \Rightarrow a_4 = 8;$$

$$8 + 6\mathbb{N} = \{8, 14, 20, 26, \ldots\} \Rightarrow a_5 = 9.$$

Logo $0 < 4 < 5 < 7 < 8 < 9$ é a Apéry-sequência e o Apéry-conjunto é $A_6 = \{0, 4, 5, 7, 8, 9\}$.

Observe que cada elemento da Apéry-sequência de G em relação à p é o menor elemento de G em sua classe módulo p. Diremos simplesmente Apéry-sequência de G quando $p = mín(G \backslash \{0\})$.

Desse modo, sendo G um semigrupo com $p \in G$ e $a_0 < a_1 < \cdots < a_{p-1}$ a *Apéry-sequência* de G em relação a p, podemos definir o conjunto $\{p, a_1, a_2, \ldots, a_{p-1}\}$ como um conjunto de geradores G.

1.3 Proposição Sejam G um semigrupo com condutor c, $p \in G \setminus \{0\}$ fixo e $a_0 < a_1 < \cdots < a_{p-1}$ a Apéry-sequência de G em relação à p. Então valem as seguintes propriedades:

$a)$ $a_i \not\equiv a_j (\text{mod}\, p)$ para $0 \leq i \neq j \leq p-1$;

$b)$ $G = \bigcup_{i=0}^{j-1} (a_i + p\mathbb{N})$;

$c)$ $c = a_{p-1} - p + 1$.

Prova:

a) Sejam a_i e a_j termos da Apéry-sequência de G em relação a p tais que $i \neq j$, isso implica que $a_i + p\mathbb{N} \neq a_j + p\mathbb{N}$, pois $a_i \notin a_j + p\mathbb{N}$ e $a_j \notin a_i + p\mathbb{N}$. Suponha, por absurdo, que $a_i \equiv a_j \ (mod\, p)$, isto é, $a_i - a_j = kp$, para algum $k \in \mathbb{Z}$. Temos duas possibilidades:

Caso I: se $k \geq 0$ então $k \in \mathbb{N}$ e daí $a_i \notin a_j + p\mathbb{N}$.

Caso II: se $k < 0$, basta tomar $a_j = a_i - kp$, daí $-k \in \mathbb{N}$ o que implica que $a_j \notin a_i + p\mathbb{N}$. Em qualquer caso temos uma contradição.

b) Basta observar que para qualquer $z \in G$ existe i tal que $z \equiv a_i \ (mod\, p)$. Então $z \in (a_i + p\mathbb{N})$.

c) Seja $n \in \mathbb{N}$ tal que $n \geq a_{p-1} - p + 1$. Observe que n se escreve de maneira única sob a forma $n = a_i + mp$ com $i = 0, 1, \ldots, p-1$ e $m \in \mathbb{Z}$. Suponha $m < 0$, então $n \leq a_i - p \leq a_{p-1} - p < n$, contradição. Portanto $m \geq 0$ o que implica que $n \in G$. Como $a_{p-1} - p \notin G$ segue que $c = a_{p-1} - p + 1$. ■

Um sistema de geradores de G pode ser dado por $S = \{x_0, x_1, \ldots, x_r\}$ onde $x_0 := m$ e recursivamente $x_j = min(G \setminus < x_0, x_1, \ldots, x_{j-1} >)$, para cada $1 \leq j \leq r$. S é chamado de sistema mínimo de geradores de G. Por exemplo, sendo $G = \{0, 3, 6, 8, 9, 11, 12, 14, 15, \ldots\}$, temos $x_0 = 3$ e, portanto, $x_1 = min(G \setminus < 3 >) = 8$ e $x_2 = min(G \setminus < 3,8 >) = \nexists$. Logo, $G =< 3,8 >$.

1.4 Proposição Seja $a_0 < a_1 < \cdots < a_{p-1}$ a Apéry-sequência de um semigrupo G. São equivalentes as afirmações:

$a)$ G é gerado por dois elementos;

$b)$ $a_k = ka_1$ para cada $k, 0 \leq k \leq m-1$;

$$(c)\ G = \bigcup_{k=0}^{m-1} (ka_1 + m\mathbb{N}).$$

Prova:

$(a) \Longrightarrow (b)$ Imediata.

$(b) \Longrightarrow (c)$ Sabemos que $G = \bigcup_{k=0}^{m-1} (a_k + m\mathbb{N})$, pela propriedade da Apéry-sequências. Como por (b) vale a igualdade $a_k = ka_1$ para cada k, $0 \leq k \leq m-1$ então

$$G = \bigcup_{k=0}^{m-1} (a_k + m\mathbb{N}) = \bigcup_{k=0}^{m-1} (ka_1 + m\mathbb{N}).$$

$(c) \Longrightarrow (a)$ Seja $x \in G$ qualquer, como $G = \bigcup_{i=0}^{m-1} (ka_1 + m\mathbb{N})$ então existem $0 \leq k \leq m-1$ e $\lambda \in \mathbb{N}$ tais que $x = ka_1 + \lambda m$, para todo $x \in G$. Logo G é gerado por a_1 e m. ■

A seguir definimos um tipo especial de semigrupo.

1.5 Definição Seja G um semigrupo com condutor c. Diz-se que G é simétrico se $\#L_G = \#(G \cap [0, c-1])$, isto é, se o número de elementos de L_G é igual ao número de elementos de $(G \cap [0, c-1])$.

Neste caso $\#L_G = c/2$. De fato, observe que $[0, c-1] = L_G \cup (G \cap [0, c-1])$ e ainda que $L_G \cap (G \cap [0, c-1]) = \emptyset$. Portanto, $\#[0, c-1] = \#[L_G \uplus (G \cap [0, c-1])] = \#L_G + \#(G \cap [0, c-1]) = \#L_G + \#L_G$. Logo $\#L_G = (c/2)$.

A seguir mostramos alguns resultados que nos ajudam a determinar se um semigrupo é simétrico ou não.

1.6 Proposição Um semigrupo com condutor é simétrico se, e só se, $l_g = 2g - 1$.

Prova: Suponha G um semigrupo com condutor c. Seja $L_G = \{l_1, \dots, l_g\}$ o conjunto das lacunas de G. Se G é simétrico então $2\#L_G = c$ o que implica que $2g = c$ portanto $2g = l_g + 1$. Logo $l_g = 2g - 1$.■

1.7 Proposição Se G é um semigrupo simétrico então para todo $z \in \mathbb{Z}$ tem-se que $z \in G$ se, e somente se, $l_g - z \notin G$.

Prova: Uma prova para essa proposição pode ser encontrada em [5] (Oliveira, pág. 7).

1.8 Proposição Sejam G um semigrupo, $0 = p \in G$ e $a_0 < a_1 < \cdots < a_{p-1}$ a Apéry-sequência de G em relação a p. Então, as afirmações que seguem são equivalentes:

a) G é um semigrupo simétrico.

b) Existe um único $A \in \mathbb{Z}$ tal que para cada par $x, y \in \mathbb{Z}$ tem-se que $x + y = A$ se, e somente se, $(x \in G\ e\ y \notin G)$ ou $(x \notin G\ e\ y \in G)$.

c) Dado $z \in \mathbb{Z}$ tem-se que $z \in G$, se e somente se, $a_{p-1} - p - z \notin G$.

d) $a_{p-1} - a_i \in A_p$ para cada $i \in \{0, 1, \ldots, p-1\}$.

e) $a_i + a_j = a_{p-1}$ para $0 \leq i, j \leq p-1$ e $i + j = p - 1$.

Prova: Uma prova para essa proposição pode ser encontrada em [5] (Oliveira, pág. 7).

1.9 Proposição Seja G um semigrupo gerado por dois elementos. Então G é simétrico.

Prova: Sejam G um semigrupo gerado por dois elementos e $a_0 < a_1 < \cdots < a_{m-1}$ a Apéry-sequência de G, segue que $a_k = ka_1$ para cada k, $0 \leq k \leq m-1$, pela Proposição 1.4. Afirmamos que $a_{m-1} - a_i \in A_m$, para cada $i = 0, 1, \ldots, m-1$. De fato, como G é gerado por dois elementos temos que $a_{m-1} - a_i = (m-1)a_1 - ia_1 = (m-1-i)a_1 = a_{m-1-i} \in A_m$, para todo $i \in \{0,1, \ldots, m-1\}$. Portanto, pela Proposição 1.8, G é simétrico. ∎

2. Germes de Curvas Planas

Sejam X e Y indeterminadas sobre $\mathbb{C}$. Denotemos por $\mathbb{C}[[X, Y]]$ o conjunto de todas as somas formais do tipo $f = \sum_{i=0}^{\infty} P_i$ onde P_i é um polinômio de grau i nas indeterminadas X, Y com coeficientes em $\mathbb{C}$. Os elementos de $\mathbb{C}[[X, Y]]$ são chamados de séries de potências formais na indeterminadas X, Y com coeficientes em $\mathbb{C}$.

Sejam

$$f = \sum_{i=0}^{\infty} P_i \text{ e } g = \sum_{i=0}^{\infty} Q_i$$

elementos de $\mathbb{C}[[X, Y]]$. Definimos as seguintes operações:

$$f + g = \sum_{i=0}^{\infty}(P_i + Q_i) \ e \ f \cdot g = \sum_{i=0}^{\infty}\sum_{j=0}^{i} P_j Q_{i-j}.$$

Com essas operações é fácil verificar que $\mathbb{C}[[X,Y]]$ é um anel comutativo com unidade, chamado *anel das séries formais em duas variáveis com coeficientes em* $\mathbb{C}$.

Considere o anel das séries formais em duas variáveis com coeficientes complexos, $\mathbb{C}[[X,Y]]$. Seja f um elemento de $\mathbb{C}[[X,Y]]$ que satisfaz as seguintes propriedades:

a) f define uma série de potências convergente em uma vizinhança da origem em $\mathbb{C}^2$;

b) f é irredutível em $\mathbb{C}[[X,Y]]$.

A equação $f(X,Y) = 0$ define um *germe de uma curva analítica irredutível.*

Um elemento $u \in \mathbb{C}[[X,Y]]$ é chamada de uma unidade se $u(0) \neq 0$.

Dois elementos f e g em $\mathbb{C}[[X,Y]]$ são chamados associados se existe uma unidade u em $\mathbb{C}[[X,Y]]$ tal que $f = u \cdot g$.

2.1 Definição Uma curva algebroide plana ou germe de uma curva (f) é a classe de equivalência de um elemento não invertível f de $\mathbb{C}[[X,Y]]\backslash\{0\}$ módulo a relação de associados. Isto é,

$$(f) = \{u \cdot f;\ u \text{ é uma unidade em } \mathbb{C}[[X,Y]]\}.$$

Portanto, por definição, temos $(f) = (g)$ se, e somente se, existe uma unidade $u \in \mathbb{C}[[X,Y]]$ tal que $g = u \cdot f$.

Um germe de uma curva plana (f) é irredutível se a série de potências formal f é irredutível em $\mathbb{C}[[X,Y]]$.

Representamos por $\langle f \rangle$ o ideal gerado por $f \in \mathbb{C}[[X,Y]]$.

2.2 Definição Seja f um elemento irredutível em $\mathbb{C}[[X,Y]]$. O anel $\mathcal{O} = \mathbb{C}\big[[X,Y]\big]/\langle f \rangle = \mathbb{C}[[x,y]]$ onde x, y são as classes de X, Y em $\mathcal{O}$ é chamado anel local do germe (f).

Seja $\mathcal{O}$ $(= \mathbb{C}[[x,y]])$ o anel local do germe (f). Dizemos que um elemento $q \in \mathbb{C}((x,y))$ é inteiro sobre $\mathcal{O}$ se existe um elemento $g \in \mathcal{O}[Z]$ tal que $g(q) = 0$. O conjunto de todos os elementos do corpo de frações $\mathbb{C}((x,y))$ que são inteiros sobre $\mathcal{O}$ será denotado por $\bar{\mathcal{O}}$, i.e.,

$$\bar{\mathcal{O}} = \{q \in \mathbb{C}((x,y)) : g(q) = 0, \text{para algum } g \in O[Z]\}.$$

Seja $p(Z) \in \mathcal{O}[Z]$ dado como $p(Z) = Z^{\mathrm{n}} + a_1 Z^{\mathrm{n}-1} + \cdots + a_k Z^{n-k} + \cdots + a_{n-1} Z + a_n$ e considere $\frac{g}{h} \in \mathbb{C}((x,y))$. Por definição, temos que $\frac{g}{h} \in \mathcal{O}$ se, e somente se, $p(\frac{g}{h}) = 0$ em $\mathcal{O}$. Ou seja

$$\left(\frac{g}{h}\right)^n + a_1 \left(\frac{g}{h}\right)^{n-1} + \cdots + a_{n-1}\left(\frac{g}{h}\right) + a_n = 0 \Rightarrow$$
$$g^{\mathrm{n}} + a_1 g^{\mathrm{n}-1} h + \cdots + a_{n-1} g h^{\mathrm{n}-1} + a_n h^{\mathrm{n}} = 0.$$

Nesse caso, $\bar{\mathcal{O}}$ é chamado de *fecho inteiro* de $\mathcal{O}$.

Dizemos que dois germes (f) e (g) são equisingulares, denotando por $(f) \equiv (g)$, se e somente se, (f) e (g) são topologicamente equivalentes como germes complexos imersos em $(\mathbb{C}^2, 0)$, isto é, quando existe um homeomorfismo $\varphi: U_f \to U_g$, onde U_f e U_g são vizinhanças da origem em $\mathbb{C}^2$ tal que (f) e (g) são convergentes em U_f e U_g, respectivamente e $\varphi((f) \cap C_f) = (g) \cap U_g$.

O conjunto de todos os germes que são equisingulares um ao outro é chamado de classe equisingular.

Se a transformação φ é um isomorfismo analítico, dizemos que (f) e (g) são analiticamente equivalentes, ou simplesmente equivalentes, denotando por $(f) \sim (g)$. Assim dois germes (f) e (g) são equivalentes se, e somente se, existe um automorfismo φ^* e uma unidade u de $\mathbb{C}[[x,y]]$ tais que $\varphi^*(f) = ug$.

3. Parametrização de Puiseux

Considere uma série formal $f(x,y) = \sum_{i,j=1}^{\infty} \alpha_{ij} x^i y^j \in \mathbb{C}[[x,y]]$ e seja $f(x,y) = 0$ uma equação local para o germe de uma curva plana C.

3.1 Definição Seja C uma curva plana irredutível. Por parametrização de C denotamos um mapa holomorfo

$$\varphi: (\mathbb{C}, 0) \longrightarrow (\mathbb{C}^2, 0)$$

definido por $t \to (x(t), y(t))$ com $\varphi(\mathbb{C}, 0) \subset (\mathbb{C}^2, 0)$ e satisfazendo a seguinte propriedade universal de fatorização: cada mapa holomorfo $\psi: (\mathbb{C}, 0) \to (\mathbb{C}^2, 0)$, $\psi(\mathbb{C}, 0) \subset (C, 0)$, é fatorado de maneira única através de φ, isto é, existe um mapa holomorfo $\psi': (\mathbb{C}, 0) \to (\mathbb{C}, 0)$ tal que $\psi = \varphi \circ \psi'$. Se $(C, 0) = (f)$ então chamamos uma parametrização de $(C, 0)$ também de uma parametrização de f.

3.2 Exemplo Seja $f(x,y) = y^2 - x^3$ com $f(x,y) = 0$. Uma parametrização para f pode ser dada por $\phi: (\mathbb{C}, 0) \to (\mathbb{C}^2, 0)$ definido como $\phi(t) = (t^2, t^3)$. Note que $f(\phi(t)) = f(t^2, t^3) = (t^3)^2 - (t^2)^3 = 0$.

Podemos definir a expansão de Puiseux da seguinte forma:

3.3 Definição Seja $f(x,y) = \sum_{i,j=1}^{\infty} \alpha_{ij} x^i y^j \in \mathbb{C}[[x,y]]$ uma série formal y-geral de ordem n (isto é, $a_{0n} \neq 0$ e $a_{0j} = 0$ para $j < n$). A série $y(x^{\frac{1}{n}}) = \sum a_i x^{\frac{i}{n}}$ é uma expansão de Puiseux para a curva com equação $f(x,y) = 0$.

3.4 Exemplo Seja $f(x,y) = y^3 - x^5 - 3x^4 y - x^7 \in \mathbb{C}[[x,y]]$ uma série formal y-geral de ordem 3. A expansão de Puiseux para a curva com equação $f(x,y) = 0$ é $y(x^{1/3}) = x^{5/3} + x^{7/3}$.

O resultado a seguir é um importante e bem conhecido teorema.

3.5 Teorema (*Teorema da Expansão de Puiseux*) Seja $f(x,y) = \sum_{i,j=1}^{\infty} \alpha_{ij} x^i y^j \in \mathbb{C}[[x,y]]$ uma série formal y-geral de ordem n. Então existe $y(t) \in \mathbb{C}[[t]]$ tal que $f\big(t^n y(t)\big) = 0$. Mais ainda, $t \to (t^n, y(t))$ é uma parametrização de f.

Uma demonstração deste teorema, que segue o método construtivo de Newton, é apresentada em [4] (Greuel, pg. 165).

3.6 Definição A forma paramétrica de $f(x,y) = \sum_{i,j=1}^{\infty} \alpha_{ij} x^i y^j \in \mathbb{C}[[x,y]]$ dada por $x = t^n$ e $y = \sum_{i \geq m} a_i t^i$ é chamada parametrização de Puiseux da curva com equação $f(x,y) = 0$.

A parametrização dada no exemplo 3.2 é de Puiseux, pois f é y-geral de ordem 2. A parametrização de Puiseux da curva dada no exemplo 3.4 é dada por $x = t^3$ e $y = t^5 + t^7$. De fato, observe que

$$\begin{aligned} f(t^3, t^5 + t^7) &= (t^5 + t^7)^3 - (t^3)^5 - 3(t^3)^4 (t^5 + t^7) - (t^3)^7 \\ &= (t^5 + t^7)(t^{10} + 2t^{12} + t^{14}) - t^{15} - 3t^{12}(t^5 + t^7) - t^{21} \\ &= t^{15} + 3t^{17} + 3t^{19} + t^{21} - t^{15} - 3t^{17} - 3t^{19} - t^{21} = 0. \end{aligned}$$

4. Semigrupos de Valores

Iniciamos essa seção definindo uma aplicação especial.

4.1 Definição Seja K um corpo. Uma valorização discreta em K, ou simplesmente uma valorização, é uma função $\nu : K \backslash \{0\} \to \mathbb{Z}$ que satisfaz as seguintes propriedades:

(1) $\nu(x \cdot y) = \nu(x) + \nu(y)$;

(2) $\nu(x + y) \geq min\{\nu(x), \nu(y)\}$;

(3) Existe $z \in K$ tal que $\nu(z) = 1$.

Pelas condições (1) e (3), segue imediatamente que $\nu : K\backslash\{0\} \to \mathbb{Z}$ é sobrejetiva. Decorre de (1) que $\nu(1) = 0$.

Pode-se definir a valorização também como $\nu : K \to \mathbb{Z} \cup \{\infty\}$. Nesse caso, por definição teremos que $\nu(0) = \infty$.

O conjunto de elementos $x \in K$ tal que $\nu(x) \geq 0$ é um anel chamado anel de valorização ν (cf. , pg. 33). Para cada $x \in K$ temos $\nu(x) \geq 0$ ou $\nu(x) \leq 0$, i.e., $\nu(x^{-1}) \geq 0$, portanto x ou x^{-1} pertence a um anel de valorização.

Sabe-se que $\bar{\mathcal{O}}$ é um anel de valorização sob seu corpo de frações $\mathbb{C}((x, y))$.

Sabe-se que qualquer germe é equivalente a um germe com uma parametrização de Puiseux. Por isso, a partir de agora, assumimos φ como uma parametrização de Puiseux de um germe (f), isto é,

$$\varphi(t) = \left(t^{\mathrm{n}}, \sum_{i \geq m} a_i t^i \right)$$

onde $f \circ \varphi(t) = 0$.

A parametrização de Puiseux induz um homomorfismo $\varphi^* : \mathcal{O} \to \mathbb{C}[[t]]$ onde $\varphi^*(h) = h \circ \varphi^*(t)$ e $\mathcal{O}$ é o anel local do germe (f).

4.2 Definição Seja φ uma parametrização de Puiseux de um germe (f). Uma valorização natural sobre o fecho inteiro $\bar{\mathcal{O}}$ (lembrando que $\bar{\mathcal{O}}$ é um anel de valorização) é definida como $\nu : \bar{\mathcal{O}}\backslash\{0\} \to \mathbb{N}$ onde $\nu(h) = ord_t h(\varphi(t))$.

Segue da definição que $\nu(u) = 0$ onde u é uma unidade em $\bar{\mathcal{O}}$.

4.3 Proposição Sejam $g, h \in \bar{\mathcal{O}}$. Se $\frac{g}{h} \in \bar{\mathcal{O}}$ então $\nu(g) \geq \nu(h)$.

Prova. Reduzindo ao absurdo, suponha que $\nu(g) < \nu(h)$. Assim $\nu(g^{\text{n}}) = n \cdot \nu(g)$ e $\nu(a_k g^{n-k} h^k) = \nu(a_k) + (n-k) \cdot \nu(g) + k \cdot \nu(h)$, com $k = 1, \dots, n$. Como $\nu(g) < \nu(h)$ então para todo $k = 1, \dots, n$, temos

$$\nu(a_k) + (n-k) \cdot \nu(g) + k \cdot \nu(h) =$$
$$= \nu(a_k) + n \cdot \nu(g) - k \cdot \nu(g) + k \cdot \nu(h) >$$
$$> \nu(a_k) + n \cdot \nu(g) - k \cdot \nu(h) + k \cdot \nu(h) =$$
$$= \nu(a_k) + n \cdot \nu(g) \geq n \cdot \nu(g) = \nu(g^{\text{n}})$$

Isso implica que $\nu(g^n + a_1 g^{n-1} h + \cdots + a_{n-1} g h^{n-1} + a_n h^n) = \nu(g^{\text{n}}) = n \cdot \nu(g)$, contradição, pois $\nu(g^n + a_1 g^{n-1} h + \cdots + a_{n-1} g h^{n-1} + a_n h^n) = \nu(0) = \infty$.■

Portanto, podemos definir uma aplicação de valorização sobre $\mathcal{O}$, a saber,

$$\nu_\varphi : \mathcal{O} \backslash \{0\} \to \mathbb{N}$$

definida como $\nu_\varphi(h) = ord_t(\varphi^*(h))$.

O subconjunto dos naturais dado por $\Gamma = \nu_\varphi(\mathcal{O} \backslash \{0\})$ é um semigrupo dos naturais.

De fato, observe que $0 \in \Gamma$, pois $\mathcal{O}$ é um anel comutativo com unidade e $\nu_\varphi(1) = 0$. Sejam $\nu_\varphi(g), \nu_\varphi(h) \in \Gamma$, $g, h \in \mathcal{O} \backslash \{0\}$, por definição temos $\nu_\varphi(g \cdot h) = \nu_\varphi(g) + \nu_\varphi(h)$. Como $g \cdot h \in \mathcal{O} \backslash \{0\}$ segue que $\nu_\varphi(g) + \nu_\varphi(h) = \nu_\varphi(g \cdot h) \in \Gamma$. Portanto Γ é um semigrupo dos naturais.

4.4 Definição O semigrupo dos naturais $\Gamma = \nu_\varphi(\mathcal{O} \backslash \{0\})$ é chamado de *semigrupo de valores* associado à curva $f = 0$.

4.5 Exemplo Se $f = Y^2 - X^3$ então uma parametrização de Puiseux para o germe (f) é $\varphi : \mathbb{C} \longrightarrow \mathbb{C}^2$ definido como $\varphi(t) = (t^2, t^3)$. Veja que $\nu_\varphi(X) = ord_t(\varphi^*(X)) = ord_t(t^2) = 2$ e que $\nu_\varphi(Y) = ord_t(\varphi^*(Y)) = ord_t(t^3) = 3$. Uma vez que qualquer número natural l pode ser escrito como $l = 2a + 3b$, com $a, b \in \mathbb{N}$, podemos concluir que $\Gamma = \{0,2,3,4,5, \dots\}$ é o semigrupo de valores associado ao germe $f = 0$. Como a multiplicidade de Γ é 2 segue que seu conjunto mínimo de geradores é dado por $\{2,3\}$ (lembre-se que podemos encontrar esse conjunto via sequência de Apéry), portanto $\Gamma = \langle 2,3 \rangle$.

4.6 Exemplo Seja $f(X,Y) = Y^3 - X^3Y^3 - X^5 + X^8$. Já que $X = t^3$ e $Y = t^5$ é a parametrização de Puiseux do germe (f), então temos $\nu_\varphi(X) = ord_t(\varphi^*(X)) = ord_t(t^3) = 3$ e que $\nu_\varphi(Y) = ord_t(\varphi^*(Y)) = ord_t(t^5) = 5$. Agora, é fácil escrever qualquer número natural $l > 7$ como $l = 3a + 5b$, com $a, b \in \mathbb{N}$. Portanto, $\Gamma = \{0,2,3,4,5, \dots\} = \langle 3,5 \rangle$.

Considerações Finais

Vemos assim que se um germe de uma curva plana irredutível pode ser representado por uma parametrização de Puiseux então é possível encontrar seu semigrupo associado. Isso muitas vezes é trabalhoso e cansativo, mas podemos lançar mão do uso de algoritmos para o cálculo de semigrupos associados a germes de curvas. Em [3] (pg. 25), Hernandes mostra que é possível, por meio de algoritmos, determinar o semigrupo de valores associado a um germe de uma curva.

O estudo local de uma singularidade isolada se mostra ainda hoje um campo vasto para pesquisa e com muitas questões sem respostas. Por exemplo, como decidir se dois germes de curvas analíticas irredutíveis planas equisingulares são analiticamente equivalentes; ou seja, como decidir se algum dos homeomorfismos θ que realizam a equivalência topológica é um isomorfismo analítico? Tal questão central da teoria de curvas irredutíveis planas ainda permanece aberta.

Na direção de uma resposta e esta e outras questões K. Brauner, W. Burau e O. Zariski, em 1930, mostraram que duas curvas planas irredutíveis são topologicamente equivalentes (equisingulares) se, e somente se, elas têm o mesmo semigrupo de valores. Isso demonstra a importância da aplicação da teoria dos semigrupos.

Referências Bibliográficas

[1] Fulton, W. *Algebraic Curves: An Introduction to Algebraic Geometry*. Versão digital, 2008.

[2] Hefez, A. *Irreducible Plane Curve Singularities. In Real and Complex Singularities*. D. Mond and M. J. Saia, Editors, Lecture Notes in Pure and Applied Math. Vol. 232, Marcel Dekker, 1-120, 2003.

[3] Hernandes, M. *Métodos Computacionais na Teoria de Curvas Algebróides Irredutíveis.* Tese de Doutorado, ICMC-USP, 2001.

[4] Greuel, G.-M. & Lossen, C. & Shustin, E. *Introduction to singularities and deformations*. Springer, 2007.

[5] Oliveira, L. N. *Caracterização dos Germes de Curvas Planas Irredutíveis com Torção Maximal*. Dissertação de Mestrado: UFES, 2011.

[6] Zariski, O. & Samuel, P. *Commutative Algebra*. Vol I, by D. Van Nostrand Company, Inc., 1958.

Universidade Federal do Acre, Rio Branco - AC, Brasil
E-mail address: leandroner@gmail.com
URL: www.ufac.br

Conjuntos Abelianos Maximais

(Dedicado para meu filho Demetrius)

por

José Ivan da Silva Ramos

(Doutor em Álgebra e membro efetivo do Centro de Ciências Exatas e Tecnológicas da Universidade Federal do Acre)

Resumo

Dado que em qualquer grupo G a família $\mathfrak{A}G = \{H \leq G/H \text{ é } abeliano\}$ é indutivamente ordenada, concluímos, através do *lema de Zorn*, que sempre existe um subgrupo abeliano maximal em *G*. Neste trabalho mostramos que a família desses subgrupos maximais tem uma forte ligação com $\Pi_{\mathfrak{A}}(G)$, o subgrupo preservador da comutatividade em *G* (ver definição 2.1.1 em [4]).

Abstract

As in any group G the family $\mathfrak{A}G = \{H \leq G/H \text{ is ab}\square\text{lian}\}$ is inductively ordered, we conclude, by *Zorn's lemma*, there is always a maximal abelian subgroup in *G*. We show that the family of maximal subgroups has a strong connection to $\Pi_{\mathfrak{A}}(G)$, the preserver subgroup of commutativity in *G* (see definition 2.1.1 in [4]).

Palavras Chave: Família, cadeia, lema de Zorn, grupo, subgrupo, abeliano, preservador de propriedade, centralizador e maximal.

1. Introdução

Iniciamos nossas considerações dando destaque para alguns conceitos elementares e gerais da teoria dos conjuntos. Consideramos claros os significados de união, interseção, relações de pertinência entre elementos e conjuntos e relações de inclusão entre conjuntos, produtos e produtos cartesianos.

Se S é um conjunto, $P(S) = 2^S = \{X/X \subset S\}$ é o conjunto das partes de S. Todo subconjunto F de $P(S)$ é denominado uma *família* de subconjuntos de S.

Definição 1: Sejam S um conjunto não vazio e $F \subset P(S)$ uma família (de subconjuntos) de S. Dizemos que F é uma *cadeia* se, e somente se, valem as condições:
i) $F \neq \Phi$;
ii) $\forall\, X, Y \in F$, vale que $X \subset Y$ ou $Y \subset X$.

A família $\mathcal{C}(\mathbb{N}) = \{\{0\},\{0,1\},\{0,1,2\},...,\{0,1,2,...,n\},...\} \subset \mathfrak{F}\mathbb{N}$ é uma cadeia (infinita) tal que a união de seus elementos, que é exatamente o conjunto $\mathbb{N}$, não é um membro da família $\mathfrak{F}\mathbb{N}$, dos subconjuntos finitos de $\mathbb{N}$.

Definição 2: Dizemos que uma família F de subconjuntos de um conjunto não vazio S é *indutivamente ordenada* se, e somente se, F sempre contém $\bigcup\limits_{W \in \mathcal{C}(S)} W$, a união dos termos de qualquer cadeia $\mathcal{C}(S)$ dentro da família F.

Exemplo 1: Seja E um conjunto não vazio no qual uma operação $*$ está definida; i. e., $\forall\, x, y \in E$, vale que $x * y \in E$.

A família

$$\mathfrak{A}E = \{X \subset E / \forall\, x, y \in X, \text{ vale que } x * y = y * x\},$$

dos subconjuntos comutativos de E, é indutivamente ordenada: Para qualquer cadeia $\mathcal{C}(E)$ contida na família $\mathfrak{A}E$, consideremos a união $L = \bigcup\limits_{A \in \mathcal{C}(E)} A$. Dados quaisquer elementos h, $k \in L$, vale que $h \in H$ e $k \in K$; onde H e K são elementos não necessariamente distintos da cadeia $\mathcal{C}(E)$. Como $H \subset K$ ou $K \subset H$, vale que $h, k \in H$ ou h, $k \in K$. Como $H, K \in \mathfrak{A}E$, vale que $h * k = k * h$. Isso nos mostra que L é comutativo. Conseqüentemente $L \in \mathfrak{A}E$ e $\mathfrak{A}E$ é indutivamente ordenada.

Especializando os conjuntos onde esses conceitos podem ser testados podemos pensar nas famílias de subgrupos de um dado grupo G.

Definição 3: Dizemos que $\mathfrak{X}$ é uma classe ou propriedade de grupos se para todo grupo G podemos decidir se G possui ou não a propriedade $\mathfrak{X}$; ou seja, se podemos decidir se $G \in \mathfrak{X}$ ou $G \notin \mathfrak{X}$.

São exemplos de classes de grupos: $\mathfrak{A}$, $\mathfrak{C}$, $\mathfrak{F}$ e $\mathfrak{N}$ as classes dos grupos (comutativos ou) abelianos, cíclicos, finitos e nilpotentes, respectivamente.

Comumente dizemos que G é um $\mathfrak{X}$-grupo se G possui a propriedade $\mathfrak{X}$. Por $\mathfrak{X}G = \{H \leq G / H \in \mathfrak{X}\}$ denotamos a família dos $\mathfrak{X}$-subgrupos de G; isto é, a família dos subgrupos de G que possuem a propriedade $\mathfrak{X}$.

2. Apresentação de resultados

Em um grupo G não finito, a investigação de resultados não pode contar com a estratégia de se usar indução sobre $|G|$, a ordem do grupo G. Para investigar grupos mais gerais podemos, em muitos casos, usar um importante resultado que é o

Lema de Zorn: Toda família de subconjuntos indutivamente ordenada possui um elemento maximal.

Considerando o que foi discutido em nosso exemplo 1, se G é qualquer grupo, a família $\mathfrak{A}G = \{H \leq G / H \in \mathfrak{A}\}$, dos subgrupos abelianos de G, é indutivamente ordenada.

Pelo lema de Zorn, $m(\mathfrak{A}G) = \{M / M \text{ é um elemento maximal em } \mathfrak{A}G\}$, o conjunto formado pelos subgrupos abelianos maximais de G é não vazio.

Exemplo 2: Se G é um grupo vale a igualdade $Z(G) = \bigcap_{M \in m(\mathfrak{A}G)} M$: Podemos supor que G não é um grupo abeliano e considerar primeiramente $x \in Z(G)$. Então, $\forall\, M \in m(\mathfrak{A}G)$, vale que $\langle x \rangle\, M \in \mathfrak{A}$. Pela maximalidade de M, temos $\langle x \rangle\, M = M$. Segue então que $x \in M$ e isso mostra que $x \in \bigcap_{M \in m(\mathfrak{A}G)} M$. Agora, se $x \in \bigcap_{M \in m(\mathfrak{A}G)} M$, para todo elemento y em G, vale que $\langle y \rangle \leq M$, para algum $M \in m(\mathfrak{A}G)$. Assim, $x, y \in M$ e vale que $xy = yx$; $\forall\, y \in G$. Portanto, $x \in Z(G)$ e vale a igualdade $Z(G) = \bigcap_{M \in m(\mathfrak{A}G)} M$.

O subgrupo $\bigcap_{M \in m(\mathfrak{A}G)} M$, intersecção dos elementos de $m(\mathfrak{A}G)$, tem conexão com o conjunto dos elementos de G cujos fechos normais, juntamente com qualquer subgrupo abeliano de G, formam, via produto, subgrupos abelianos.

As técnicas empregadas no entendimento das pequenas afirmações que apresentamos a seguir fazem parte de uma abordagem feita em classes de grupos mais gerais (ver [4]).

Proposição 1: Seja G um qualquer grupo G. Então:

a) O conjunto $\Pi_{\mathfrak{A}}(G) = \{x \in G \;/\; \langle x^G \rangle A \in \mathfrak{A};\ \forall\, A \in \mathfrak{A}G\}$ é um subgrupo característico de G.

b) Se $H \leq G$, vale que $\Pi_{\mathfrak{A}}(G) \cap H \leq \Pi_{\mathfrak{A}}(H)$.

Demonstração: a) Claro que $1 \in \Pi_{\mathfrak{A}}(G)$. Além disso, $\forall\, y \in \Pi_{\mathfrak{A}}(G)$, para todo $A \in \mathfrak{A}G$, temos que $\langle y^G \rangle A \in \mathfrak{A}$. Assim, qualquer que seja $x \in \Pi_{\mathfrak{A}}(G)$, temos que $\langle x^G \rangle (\langle y^G \rangle A) = \langle x^G \rangle \langle y^G \rangle A \in \mathfrak{A}$. Como xy^{-1}é um elemento de $\langle x^G \rangle \langle y^G \rangle A$, vemos que $\langle (xy^{-1})^G \rangle A \leq \langle x^G \rangle \langle y^G \rangle A$. Sendo $\mathfrak{A}$ fechada para subgrupos, $\langle (xy^{-1})^G \rangle A \in \mathfrak{A}$, o que mostra que $xy^{-1} \in \Pi_{\mathfrak{A}}(G)$. Segue então que $\Pi_{\mathfrak{A}}(G)$ é um subgrupo de G.

Agora, se σ é um automorfismo de G, $\sigma(x) \in \Pi_{\mathfrak{A}}(G)$; para todo elemento $x \in \Pi_{\mathfrak{A}}(G)$; ou seja, $\Pi_{\mathfrak{A}}(G)$ é um subconjunto característico de G.

b) Seja x qualquer elemento em $\Pi_{\mathfrak{A}}(G) \cap H$ e A qualquer elemento em $\mathfrak{A}H$. Como $\mathfrak{A}H \subset \mathfrak{A}G$ e $x \in \Pi_{\mathfrak{A}}(G)$, vemos que $\langle x^H \rangle A \leq \langle x^G \rangle A \in \mathfrak{A}$. Isso mostra que $x \in \Pi_{\mathfrak{A}}(H)$.$\blacksquare$

O próximo resultado dá uma forte indicação para a comparação que fazemos entre $\Pi_{\mathfrak{A}}(G)$ e $Z(G)$, no final desta seção.

Proposição 2: Seja $G = G_1 \times G_2$ um produto direto dos grupos G_1 e G_2. Então, vale a seguinte relação: $\Pi_{\mathfrak{A}}(G) = \Pi_{\mathfrak{A}}(G_1) \times \Pi_{\mathfrak{A}}(G_2)$.

Demonstração: Provaremos a igualdade mostrando que esses conjuntos estão contidos um no outro.

Inicialmente, consideremos qualquer subgrupo $A \in \mathfrak{A}G$. Valem as seguintes relações: $G_1 \cap AG_2 = (G_1 \cap AG_2)/1 = G_1 \cap AG_2 / (G_1 \cap AG_2) \cap G_2$. Por isomorfismo temos que $G_1 \cap AG_2 / (G_1 \cap AG_2) \cap G_2 \cong (G_1 \cap AG_2)\, G_2/G_2 = AG_2/G_2 \cong A/A \cap G_2$.

Como a classe $\mathfrak{A}$ é fechada para quocientes, concluímos que $G_1 \cap AG_2 \in \mathfrak{A}$. De maneira análoga concluímos que $G_2 \cap AG_1 \in \mathfrak{A}$.

Seja x um elemento em $\Pi_{\mathfrak{A}}(G_1)$. Vale que $\langle x^{G_1} \rangle = \langle x^G \rangle$. Portanto, temos que $\langle x^G \rangle (G_1 \cap AG_2) = \langle x^{G_1} \rangle (G_1 \cap AG_2) \in \mathfrak{A}$.

Do fato que $A \leq AG_1 \cap AG_2 = (G_1 \cap AG_2) \times (G_2 \cap AG_1)$, podemos observar que $\langle x^G \rangle A \leq \langle x^G \rangle (AG_1 \cap AG_2) = \langle x^G \rangle ((G_1 \cap AG_2) \times (G_2 \cap AG_1))$. Segue que $\langle x^G \rangle A \leq \langle x^{G_1} \rangle ((G_1 \cap AG_2) \times (G_2 \cap AG_1)) = (\langle x^{G_1} \rangle (G_1 \cap AG_2)) \times (G_2 \cap AG_1) \in \mathfrak{A}$, o que mostra que $x \in \Pi_{\mathfrak{A}}(G)$ e que $\Pi_{\mathfrak{A}}(G_1) \leq \Pi_{\mathfrak{A}}(G)$. Argumentos análogos mostram que $\Pi_{\mathfrak{A}}(G_2) \leq \Pi_{\mathfrak{A}}(G)$. Concluímos então que $\Pi_{\mathfrak{A}}(G_1) \times \Pi_{\mathfrak{A}}(G_2) \subset \Pi_{\mathfrak{A}}(G)$.

Agora, $\forall\, x \in \Pi_{\mathfrak{A}}(G)$, pelo fato de $G = G_1 \times G_2$ ser um produto direto, vale que $x = ab$; com $a \in G_1$ e $b \in G_2$. Pela escolha de x, sendo $\langle b \rangle$ um subgrupo (cíclico) abeliano de G, temos $\langle a^{G_1} \rangle = \langle (xb^{-1})^{G_1} \rangle \leq \langle x^A \rangle \langle b \rangle \leq \langle x^G \rangle \langle b \rangle \in \mathfrak{A}$. Segue que $\langle a^{G_1} \rangle A_1 \leq \langle x^G \rangle \langle b \rangle A_1 \leq \langle x^G \rangle (\langle b \rangle \times A_1) \in \mathfrak{A}$; $\forall A_1 \in \mathfrak{A}G_1$. Isso mostra que $a \in \Pi_{\mathfrak{A}}(G_1)$. Argumentando da mesma forma, obtemos que $\langle b^{G_2} \rangle A_2 \in \mathfrak{A}$; $\forall A_2 \in \mathfrak{A}G_2$ e assim $b \in \Pi_{\mathfrak{A}}(G_2)$. Portanto, temos $x = ab \in \Pi_{\mathfrak{A}}(G_1) \times \Pi_{\mathfrak{A}}(G_2)$. De onde segue que $\Pi_{\mathfrak{A}}(G) \subset \Pi_{\mathfrak{A}}(G_1) \times \Pi_{\mathfrak{A}}(G_2)$. Com isso temos que $\Pi_{\mathfrak{A}}(G) = \Pi_{\mathfrak{A}}(G_1) \times \Pi_{\mathfrak{A}}(G_2)$. ∎

Conforme definição 2.1.1 em [5; pág. 30], $\Pi_{\mathfrak{A}}(G)$ pode ser entendido como um subgrupo *preservador da propriedade* $\mathfrak{A}$ em G. A coincidência da interseção dos elementos da família $m(\mathfrak{A}G)$, dos subgrupos abelianos maximais de G, com $\Pi_{\mathfrak{A}}(G)$ é um particular resultado da proposição 3.1 em [6], pág. 251, dado que a classe $L\mathfrak{A}$, dos grupos localmente abelianos, coincide com a classe $\mathfrak{A}$ dos grupos abelianos. Vale a seguinte

Proposição 3: Se G é um grupo; então vale a igualdade $\Pi_{\mathfrak{A}}(G) = \bigcap_{M \in m(\mathfrak{A}G)} M$.

Demonstração: Seja $x \in \Pi_{\mathfrak{A}}(G)$. Então, $\forall\, M \in m(\mathfrak{A}G)$, vale que $\langle x^G \rangle M \in \mathfrak{A}$. Sendo M abeliano maximal, temos $\langle x^G \rangle M = M$, conseqüentemente, $x \in \langle x^G \rangle \leq M$, o que mostra que $x \in \bigcap_{M \in m(\mathfrak{A}G)} M$.

Reciprocamente, considere $x \in \bigcap_{M \in m(\mathfrak{A}G)} M$. Para qualquer $A \in \mathfrak{A}G$, existe em G um subgrupo abeliano maximal L tal que $A \leq L$ e por isso, temos que $\langle x^G \rangle A \leq L$. Segue que $\langle x^G \rangle A \in \mathfrak{A}$. Portanto, vale que $x \in \Pi_{\mathfrak{A}}(G)$. ∎

É possível obtermos $\Pi_{\mathfrak{A}}(G)$ interceptando os centralizadores dos subgrupos abelianos maximais de *G*. Isso é uma conseqüência da seguinte

Observação 1: Se G é um grupo e $A \in \mathfrak{A}G$, para todo *x* em $\mathcal{C}_G(A)$, vale que $\langle x, A\rangle \in \mathfrak{A}G$. Em particular, se *G* não é abeliano e $A \in m(\mathfrak{A}G)$, vale que $A = \mathcal{C}_G(A)$ é auto centralizante.

Demonstração: Primeiramente observemos que se $h \in \langle x, A\rangle$, vale que $h = u_1u_2u_3 \cdots u_k$; onde $1 \leq k \in \mathbb{N}$ e $u_i \in A$, $u_i = x$ ou $u_i = x^{-1}$, para cada *i*. Como *A* é abeliano e é centralizado por *x*, podemos juntar os fatores de *h*, que estão em *A*, colocando todos à esquerda desse produto. Assim temos $h = lx^m$, onde $m \in \mathbb{Z}$ e l é o produto dos fatores em *A*.

Agora, $\forall\, l_1x^{m_1}, l_2x^{m_2} \in \langle x, A\rangle$, temos $(l_1x^{m_1})\,(l_2x^{m_2}) = ((l_1x^{m_1})\,l_2)x^{m_2}$. Como *x* centraliza *A* e *A* é abeliano temos $((l_1x^{m_1})\,l_2)x^{m_2} = (l_2\,(l_1x^{m_1})\,)x^{m_2} = l_2(l_1(x^{m_1}\,x^{m_2})) = l_2(l_1(x^{m_2}\,x^{m_1})) = l_2((l_1x^{m_2})\,x^{m_1}) = l_2((x^{m_2}l_1)\,x^{m_1}) = (l_2x^{m_2})(l_1\,x^{m_1})$. Isso mostra que $\langle x, A\rangle$ é abeliano.

Se *A* é maximal, vale que $\langle x, A\rangle = A$ e assim, $x \in A, \forall x \in \mathcal{C}_G(A)$. Isso mostra que $\mathcal{C}_G(A) \leq A$. Que $A \leq \mathcal{C}_G(A)$ é claro.■

Corolário: Em qualquer grupo *G* vale que $\Pi_{\mathfrak{A}}(G) = \bigcap_{M \in m(\mathfrak{A}G)} \mathcal{C}_G(M)$.

Demonstração: Pela proposição 3 vale que $\Pi_{\mathfrak{A}}(G) = \bigcap_{M \in m(\mathfrak{A}G)} M$. Pela observação anterior vale que $M = \mathcal{C}_G(M), \forall\, M \in m(\mathfrak{A}G)$.■

Uma natural pergunta que surge é: Sempre temos a coincidência de $\Pi_{\mathfrak{A}}(G)$ com a interseção $\bigcap_{M \in m(\mathfrak{A}G)} \mathcal{N}_G(M)$, dos subgrupos normalizadores em *G* dos elementos de $m(\mathfrak{A}G)$?

Claro que sempre temos $\Pi_{\mathfrak{A}}(G)\left(= \bigcap_{M \in m(\mathfrak{A}G)} \mathcal{C}_G(M)\right) \leq \bigcap_{M \in m(\mathfrak{A}G)} \mathcal{N}_G(M)$, em qualquer grupo *G*. Porém, se *G* não é um grupo abeliano, essa inclusão pode ser própria como mostra o

Exemplo 3: Consideremos "$\cdot$", a multiplicação usual de matrizes no conjunto $Q_3 = \left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}_{2x2}, \pm \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}_{2x2}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}_{2x2}, \pm \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}_{2x2} \right\}$. Temos que $(Q_3, \cdot)$ é um grupo não abeliano e todos os seus subgrupos são normais. Nesse grupo denominado *grupo dos quatérnios*, temos que

$$\Pi_{\mathfrak{A}}(Q_3) \left(= \bigcap_{M \in m(\mathfrak{A}Q_3)} \mathcal{C}_{Q_3}(M) \right) \neq \bigcap_{M \in m(\mathfrak{A}Q_3)} \mathcal{N}_{Q_3}(M) = Q_3$$

De forma direta ou usando o fato de que $\Pi_{\mathfrak{A}}(G) = \bigcap_{M \in m(\mathfrak{A}G)} M$, podemos ver facilmente que $Z(G) = \Pi_{\mathfrak{A}}(G) = \bigcap_{M \in m(\mathfrak{A}G)} M = \bigcap_{M \in m(\mathfrak{A}G)} \mathcal{C}_G(M)$. Essa comparação entre o preservador da propriedade $\mathfrak{A}$ e o centro de um grupo evidencia a comparação que fizemos no exemplo 2.

3. Elementos $\mathfrak{A}$-preservadores e o $\mathfrak{A}$C- centro de um grupo *G*

Nesta seção introduzimos o conceito de $Z_{\mathfrak{A}}(G)$, o $\mathfrak{A}C$- *centro* do grupo *G*. Mostramos que sempre $\Pi_{\mathfrak{A}}(G)$ é parte de $Z_{\mathfrak{A}}(G)$ e que, mesmo que esses conjuntos não coincidam, cada elemento do $\mathfrak{A}C$- *centro* de *G* ainda é centralizado por algum membro da família $m(\mathfrak{A}G)$.

Definição 4: (Ver [1]) Seja *G* um grupo e *x* um elemento em *G*. Dizemos que *x* é um $\mathfrak{A}C$-elemento de *G* se, e somente se, ${G}/{\mathcal{C}_G(\langle x^G \rangle)} \in \mathfrak{A}$, ou seja, *G* induz sobre $\langle x^G \rangle$ um $\mathfrak{A}$-grupo de automorfismos.

O conjunto dos $\mathfrak{A}C$-elementos de *G*, denotado por

$$Z_{\mathfrak{A}}(G) = \left\{ x \in G \ / \ {G}/{\mathcal{C}_G(\langle x^G \rangle)} \in \mathfrak{A} \right\},$$

é denominado o $\mathfrak{A}C$- *centro* de *G*. Se $Z_{\mathfrak{A}}(G) = G$, dizemos que *G* é um o $\mathfrak{A}C$- *grupo*.

O fechamento da classe $\mathfrak{A}$ para subgrupos, quocientes e para produto direto de dois fatores, permite concluir que sempre $Z_{\mathfrak{A}}(G)$ é um subgrupo de *G* que goza de algumas propriedades. Temos a seguinte

Observação 2: Seja G um grupo. Então valem as seguintes proposições:

a) Se ${}^{G}\!/_{\Pi_{\mathfrak{A}}(G)}$ é abeliano, então $\mathrm{Z}_{\mathfrak{A}}(G) = G$ é um $\mathfrak{A}C$-grupo.

b) $\mathrm{Z}_{\mathfrak{A}}(G)$ é um $\mathfrak{A}C$-subgrupo de G.

c) Para todo subgrupo H de G, temos que $\mathrm{Z}_{\mathfrak{A}}(G) \cap H \leq \mathrm{Z}_{\mathfrak{A}}(H)$.

Demonstração: a) Segue imediatamente usando isomorfismo e o fato de que $\mathfrak{A}$ é fechada a quocientes: Temos $G/\mathcal{C}_G(\langle x^G \rangle) \cong \left(G/\Pi_{\mathfrak{A}}(G) \right) \Big/ \left(\mathcal{C}_G(\langle x^G \rangle)/\Pi_{\mathfrak{A}}(G) \right)$; $\forall x \in G$.

Que todo elemento em $\Pi_{\mathfrak{A}}(G) \leq \mathcal{C}_G(\langle x^G \rangle)$ é claro (ver o exemplo 2, na seção 2).

b) Provaremos primeiro que $\mathrm{Z}_{\mathfrak{A}}(G)$ é um subgrupo de G: Sejam x, y quaisquer elementos em $\mathrm{Z}_{\mathfrak{A}}(G)$. Pondo $z = xy^{-1}$, temos $\langle z^G \rangle \leq \langle x^G \rangle \langle y^G \rangle$ e assim, vale que $E = \mathcal{C}_G(\langle x^G \rangle) \cap \mathcal{C}_G(\langle y^G \rangle) \leq \mathcal{C}_G(\langle z^G \rangle)$. Sendo a classe $\mathfrak{A}$ fechada para subgrupos e produto direto de dois fatores, vemos que G/E é um grupo abeliano. Pelo fechamento da classe $\mathfrak{A}$ a quocientes, temos que $G/\mathcal{C}_G(\langle z^G \rangle) \cong (G/E) \Big/ \left(\mathcal{C}_G(\langle z^G \rangle)/E \right) \in \mathfrak{A}$. Isso mostra que $\mathrm{Z}_{\mathfrak{A}}(G)$ é um subgrupo de G.

Consideremos agora qualquer elemento x em $\mathrm{Z}_{\mathfrak{A}}(G)$. Vale que $\mathrm{Z}_{\mathfrak{A}}(G)\mathcal{C}_G(\langle x^G \rangle)/\mathcal{C}_G(\langle x^G \rangle) \cong \mathrm{Z}_{\mathfrak{A}}(G)/\mathrm{Z}_{\mathfrak{A}}(G) \cap \mathcal{C}_G(\langle x^G \rangle) \leq G/\mathcal{C}_G(\langle x^G \rangle)$ é um grupo abeliano. Como $\mathrm{Z}_{\mathfrak{A}}(G) \cap \mathcal{C}_G(\langle x^G \rangle) \leq \mathcal{C}_{\mathrm{Z}_{\mathfrak{A}}(G)}\left(\langle x^{\mathrm{Z}_{\mathfrak{A}}(G)} \rangle\right)$ e a classe $\mathfrak{A}$ também é fechada para quocientes, vemos que $\mathrm{Z}_{\mathfrak{A}}(G)/\mathcal{C}_{\mathrm{Z}_{\mathfrak{A}}(G)}(\langle x^{\mathrm{Z}_{\mathfrak{A}}(G)} \rangle) \in \mathfrak{A}$ e assim, $\mathrm{Z}_{\mathfrak{A}}(G)$ é um $\mathfrak{A}C$-subgrupo de G.

c) Seja x um elemento em $\mathrm{Z}_{\mathfrak{A}}(G) \cap H$. Pelo teorema do isomorfismo, temos que $H/H \cap \mathcal{C}_G(\langle x^G \rangle) \cong H\mathcal{C}_G(\langle x^G \rangle)/\mathcal{C}_G(\langle x^G \rangle) \leq G/\mathcal{C}_G(\langle x^G \rangle)$ é um grupo abeliano. Como, $H \cap \mathcal{C}_G(\langle x^G \rangle) \leq \mathcal{C}_H(\langle x^H \rangle)$, novamente por isomorfismo temos que o grupo

$$\left. {}^{H}\!/_{H \cap \mathcal{C}_G(\langle x^G \rangle)} \middle/ {}^{\mathcal{C}_H(\langle x^H \rangle)}\!/_{H \cap \mathcal{C}_G(\langle x^G \rangle)} \right. \cong {}^{H}\!/_{\mathcal{C}_H(\langle x^H \rangle)}$$ é abeliano. Isso mostra que x é um elemento em $Z_{\mathfrak{A}}(H)$.■

Observação 3: Se G é um grupo e $x \in Z_{\mathfrak{A}}(G)$, vale que $\langle x^G \rangle \leq M$, para algum M na família $m(\mathfrak{A}G)$.

Demonstração: É suficiente provarmos que o fecho normal de x é abeliano. De fato: Seja x um $\mathfrak{A}C$-elemento de G. Então, vale que ${}^{G}\!/_{\mathcal{C}_G(\langle x^G \rangle)} \in \mathfrak{A}$. Desde que $\mathcal{C}_G(\langle x^G \rangle) \leq \mathcal{C}_G(x)$, por isomorfismo e pelo fechamento da classe $\mathfrak{A}$ para quocientes,

$$\left. {}^{G}\!/_{\mathcal{C}_G(\langle x^G \rangle)} \middle/ {}^{\mathcal{C}_G(x)}\!/_{\mathcal{C}_G(\langle x^G \rangle)} \right. \cong {}^{G}\!/_{\mathcal{C}_G(x)}$$ é abeliano e $\mathcal{C}_G(x) \trianglelefteq G$. Isso significa que $\forall\, g_1, g_2 \in G$, vale que $x^{g_1} \in \mathcal{C}_G(x^{g_2})$, ou seja, $\langle x^G \rangle$ é abeliano.

Observação 4: Em qualquer grupo G vale que:

a) $\Pi_{\mathfrak{A}}(G) \leq Z_{\mathfrak{A}}(G)$;

b) Se $x \in Z_{\mathfrak{A}}(G)$, $\langle x^G \rangle$ é centralizado por algum elemento M de $m(\mathfrak{A}G)$.

Demonstração: a) Para todo x em $\Pi_{\mathfrak{A}}(G)$, usando a caracterização de $\Pi_{\mathfrak{A}}(G)$ na proposição 3 e o fato de que para todo g em G, temos $\langle g \rangle \leq M$, onde $M \in m(\mathfrak{A}G)$, vemos que $x,\ g \in M$ e assim, $xg = gx$. Isso mostra que $\mathcal{C}_G(\langle x^G \rangle) = \mathcal{C}_G(x) = G$ e assim temos que ${}^{G}\!/_{\mathcal{C}_G(\langle x^G \rangle)} = 1$ é um grupo abeliano. Portanto vale que $x \in Z_{\mathfrak{A}}(G)$.

b) Pela observação 3, vale que $\langle x^G \rangle$ é um subgrupo (normal) abeliano de G. Assim, temos que $\langle x^G \rangle \leq M$. Segue que $\mathcal{C}_G(M) \leq \mathcal{C}_G(\langle x^G \rangle)$. Pela observação 1, vale que $M = \mathcal{C}_G(M)$ o que mostra que M centraliza $\langle x^G \rangle$.■

Exemplo 4: Em muitos casos temos $\Pi_{\mathfrak{A}}(G) \neq Z_{\mathfrak{A}}(G)$. Por exemplo, em S_3, temos $\Pi_{\mathfrak{A}}(S_3) = 1$, enquanto que $1 \neq A_3 \leq Z_{\mathfrak{A}}(S_3)$.

4. Considerações finais

A existência de subgrupos abelianos maximais em um grupo G, garantida pelo lema de Zorn, permite que o conjunto $\Pi_{\mathfrak{A}}(G)$, preservador da propriedade $\mathfrak{A}$ em *G*, seja obtido como a interseção desses subgrupos. O exemplo 2 e as proposições 1 e 2, ***motivam uma "nova" definição do centro de um grupo***.

O fato de que o produto de dois subgrupos normais abelianos de um grupo *G*, em geral não é um subgrupo (normal) abeliano de *G*, de certa forma, "diminui" as possibilidades de obtermos mais resultados utilizando esses subgrupos maximais dentro do grupo *G*.

Conforme o exemplo 3, o $\mathfrak{A}C$-centro de um grupo *G* pode conter propriamente $\Pi_{\mathfrak{A}}(G)$. Nesse caso, podemos comparar os elementos desses subgrupos: Para um elemento $1 \neq x \in \Pi_{\mathfrak{A}}(G)$ vale que ***todo subgrupo abeliano maximal de G centraliza*** $\langle \boldsymbol{x^G} \rangle$, o fecho normal de *x* em *G*. Enquanto que se $1 \neq x \in Z_{\mathfrak{A}}(G)$, com $x \notin \Pi_{\mathfrak{A}}(G)$, o item b) da observação 3 garante que $\langle x^G \rangle$ é abeliano e por isso está contido em ***um subgrupo abeliano maximal de G***. Esse subgrupo certamente ***centraliza*** $\langle \boldsymbol{x^G} \rangle$.

O conceito mais geral de preservador de uma propriedade $\mathfrak{X}$ de grupos, formulada por Maier e Ramos (ver [5]), foi investigado a partir da classe $L\mathfrak{N}$ dos grupos *localmente nilpotentes*, grupos nos quais todo subgrupo finitamente gerado é nilpotente.

A existência de subgrupos localmente nilpotentes maximais e do maior subgrupo normal localmente nilpotente de um grupo *G* são garantidas, respectivamente, pelo lema de Zorn e por um teorema Hirsch e Plotkin (ver [2], § 12.1) que mostra que o produto de dois subgrupos normais localmente nilpotentes de um grupo *G* é um subgrupo (normal) localmente nilpotente de *G*. Utilizando esses fatos foi possível definir o conjunto $\Pi_{L\mathfrak{N}}(G) = \{x \in G \ / \ \langle x^G \rangle H \in L\mathfrak{N};\ \forall\, H \in L\mathfrak{N}\}$, preservador da propriedade de um grupo ser localmente nilpotente, mostrar que $\Pi_{L\mathfrak{N}}(G) = \bigcap_{M \in m(L\mathfrak{N}G)} M$ e estudar as propriedades desse conjunto.

Investigações mais cuidadosas mostraram que, sempre que uma classe $\mathfrak{X}$ de grupos é fechada para subgrupos, quocientes e produto direto de dois fatores, o conjunto $\Pi_{\mathfrak{X}}(G) = \{x \in G / \langle x^G \rangle U \in \mathfrak{X}; \forall U \in \mathfrak{X}G\}$ merece uma atenção especial.

5. Bibliografia

[1] Maier, R. and Rogério, J. R.; *$\mathfrak{X}$C-elements in groups and Dietzmann classes*; Contribuitions to algebra and geometry **40**; 243-260 (1999);

[2] Robinson, D. J. S.; *A course in the theory of groups*; Springer Verlag; New York-Berlim-Heidelberg (1996);

[3] Robinson, D. J. S.; *Finiteness conditions and generalized soluble groups*; Part 1; Springer Verlag; New York-Berlim-Heidelberg (1972);

[4] Robinson, D. J. S.; *Finiteness conditions and generalized soluble groups*; Part 2; Springer Verlag; New York-Berlim-Heidelberg (1972);

[5] Ramos, J. I. S.; *Subgrupos preservadores de propriedades em grupos*; Tese de doutorado; Brasília (1993);

[6] Ramos, J. I. S. and Maier, R.; *Propert preserving subgroups of a group*; JP Journal of Algebra, Number Theory and Applications **6**; Issue **2**; PP. 237-264 (2006).

José Ivan da Silva Ramos

Rua Maranhão, nº 133 – Bairro Bosque – Rio Branco – Acre

CEP: 69908-240

ivanr@ufac.br

Tels.: 0xx68-3224-5054 e 0xx68-84132219.

Évariste Galois

Évarist Galois (*galuá*): (Bourg-la-Reine, 25 de outubro de 1811 — Paris, 31 de maio de 1832) foi um matemático francês.

Ao determinar a condição necessária e suficiente para que um polinómio pudesse ser resolvido por raízes, não só resolveu um antigo problema em aberto, como criou um domínio inteiramente novo da álgebra abstrata: a Teoria dos Grupos. Morreu num duelo com a idade de 20 anos. Tendo crescido durante um período de grande agitação social e política, colocou-se, repetidamente, no centro de controvérsias, o que não apenas o afastou de sua brilhante carreira, como também acabou por levá-lo a uma morte prematura.

Infância: O interesse de Galois pela política foi inspirado por seu pai, Nicolas Gabriel Galois que, quando Évariste tinha apenas quatro anos de idade, foi eleito prefeito de Bourg-la-Reine. Isto aconteceu durante o retorno triunfante de Napoleão ao poder, um período em que os fortes valores liberais de seu pai estavam de acordo com o clima do país. Nicolas-Gabriel era um homem culto e cortês e durante seu mandato como prefeito conquistou o respeito da comunidade. Mesmo depois que Luís XVIII da França retornou ao poder, ele manteve seu posto. Fora da política, seu maior interesse parece ter sido a composição de versos satíricos que ele lia nas reuniões da cidade, para a alegria de seus eleitores. Muitos anos depois, este seu talento para a sátira levaria à sua queda.

Com a idade de doze anos, Évariste Galois foi para a escola no Liceu de Louis-le-Grand. Era uma instituição de prestígio e muito autoritária. Lá não encontrou nenhum curso de matemática, que representava seu maior interesse. No primeiro período da escola, devido às lutas entre republicanos e monárquicos, a maioria dos estudantes planejou uma rebelião. Uma dúzia de líderes foi expulsa. No dia seguinte foi exigida uma demonstração de fidelidade a Luís XVIII. Muitos se recusaram. Mais de cem foram expulsos. Galois, muito jovem para se envolver na fracassada rebelião, ao ver seus colegas serem humilhados, aumentou suas tendências republicanas.

Estudos: Diziam seus professores: "este aluno só se preocupa com os altos campos da matemática; a loucura matemática domina este garoto; seria melhor para ele se seus pais o deixassem estudar apenas isto, de outro modo ele está perdendo tempo aqui e não faz nada senão atormentar seus professores e sofrer castigos." Assim, somente aos dezesseis anos pôde fazer seu primeiro curso exclusivo de matemática. Passou a negligenciar todas as outras matérias concentrando-se apenas em sua nova paixão.

O conhecimento de Galois pela matemática logo superou o conhecimento do seu professor. Passou a estudar diretamente dos livros escritos pelos gênios de sua época. Rapidamente absorveu os conceitos mais modernos e com a idade de dezessete anos publicou seu primeiro trabalho nos Annales de Gergonne. Havia um caminho claro para o jovem prodígio, todavia seu brilho seria o maior obstáculo ao seu progresso. Embora soubesse mais matemática do que seria necessário para passar nas provas do Liceu, as soluções de Galois eram freqüentemente tão sofisticadas e inovadoras que seus professores não conseguiam julgá-las corretamente. Além disto, Galois fazia muitos cálculos de cabeça, sem transcrevê-los, deixando os professores frustrados e perplexos.

Com seu temperamento explosivo e sua precipitação conquistava a inimizade de seus tutores e de todos os que cruzavam seu caminho. Quando prestou exame para a École Polytechnique, o mais prestigiado colégio de seu país, os seus modos rudes e a falta de explicações na prova oral fizeram com que sua admissão fosse recusada. Desejando desesperadamente freqüentar a Polytechnique, não só por sua excelência como centro acadêmico, mas por sua reputação de ser um centro do ativismo republicano, tentou no ano seguinte nela ingressar e, mais uma vez seus saltos lógicos na prova oral só confundiram o examinador, Monsieur Dinet. Sentindo que estava a ponto de ser reprovado pela segunda vez, e frustrado por sua inteligência não estar sendo reconhecida, Galois perdeu a calma e jogou um apagador em Dinet, acertando em cheio. Nunca mais ele voltaria a entrar nas famosas salas da Polytechnique.

Sem se deixar abalar pelas reprovações Galois continuou confiante em seu talento matemático. Prosseguiu com suas pesquisas, seu principal interesse sendo a busca de soluções para certas equações, como a equação quadrática. Era também obcecado pela idéia de encontrar uma receita para resolver as equações de quinto grau, um dos grandes desafios de sua época. Com a idade de dezessete anos, ele fizera progressos suficientes para submeter dois trabalhos de pesquisa à Academia de Ciências. Cauchy ficou muito impressionado com o trabalho do jovem e o julgou capaz de participar na competição pelo Grande Prêmio de Matemática da Academia. De modo a se qualificarem para a competição os dois trabalhos teriam que ser reapresentados na forma de uma única tese e assim Cauchy os mandou de volta para Galois e aguardou que ele se inscrevesse.

Infelizmente, nesta mesma ocasião, em julho de 1829 um novo sacerdote jesuíta chegou ao vilarejo de Bourg-la-Reine, onde o pai de Galois ainda era prefeito. Não gostando das simpatias republicanas do prefeito, o jesuíta começou uma campanha para depô-lo. Escreveu uma série de versos vulgares ridicularizando membros da comunidade e os assinou com o nome do prefeito. O velho Galois não pode suportar a vergonha e o embaraço resultantes e se suicidou. Évariste Galois voltou para assistir ao enterro do pai e viu pessoalmente as divisões que o sacerdote tinha criado. Quando o caixão estava sendo baixado à sepultura, tendo os partidários do prefeito percebido ter sido tudo uma trama para depô-lo, iniciou-se uma briga que se transformou em tumulto, o caixão atirado para dentro da cova… Ver o sistema francês humilhar e destruir seu pai consolidou o apoio fervoroso de Galois para a causa republicana.

Voltando a Paris, Galois juntou seus dois trabalhos num só e os enviou para o secretário da Academia, Joseph Fourier, bem antes do limite do prazo. Fourier por sua vez devia entregá-lo para o comitê de avaliação. O trabalho de Galois não apresentava uma solução para os problemas do quinto grau, mas oferecia uma visão tão brilhante que muitos matemáticos, incluindo Cauchy, o consideravam como o provável vencedor.

Para espanto de Cauchy e seus amigos, o trabalho não ganhou o prêmio e nem foi oficialmente inscrito. Fourier morrera algumas semanas antes da data da decisão dos juizes, e embora um maço de trabalhos tivesse sido entregue ao comitê, o de Galois não estava entre eles. O trabalho nunca foi encontrado e a injustiça foi registrada por um jornalista francês.

Galois achou que seu trabalho fora propositalmente perdido devido às orientações políticas da Academia. Uma crença que foi reforçada no ano seguinte, quando a Academia rejeitou seu manuscrito seguinte, alegando que os argumentos não eram suficientemente claros nem desenvolvidos para que pudessem ser julgados com exatidão. Galois decidiu que havia uma conspiração para excluí-lo da comunidade matemática. Em conseqüência disso passou a negligenciar suas pesquisas em favor da luta pela causa republicana. A essa altura ele era aluno da École Normale Supérieure, onde sua fama como criador de casos estava se tornando mais forte do que sua reputação como matemático, atingindo o auge durante a revolução de julho de 1830, quando Carlos X fugiu da França e as facções políticas lutaram pelo controle nas ruas de Paris. Os alunos foram confinados ao dormitório. Galois foi impedido de lutar com seus companheiros e seu ódio e frustração dobraram quando os republicanos foram derrotados. Na primeira oportunidade, ele publicou um ataque sarcástico contra o diretor do colégio, acusando-o de covardia, do que resultou sua expulsão e extinção da carreira de matemático.

Anos rebeldes: Em 4 de dezembro de 1830, o gênio contrariado tentou se tornar um rebelde profissional alistando-se na Artilharia da Guarda Nacional. Tratava-se de um ramo de milícia conhecido também como "inimigos do povo". Antes do fim do mês o novo rei, Louis-Phillipe, ansioso em evitar novas rebeliões, extinguiu a Artilharia da Guarda e Galois se viu desamparado e sem lar. Alguns de seus colegas matemáticos começaram a se preocupar com o seu destino. Sophie Germain, na ocasião uma tímida e idosa representante da Matemática Francesa, expressou suas preocupações aos seus amigos da família do conde Libri-Carrucci. "Decididamente havia uma maldição atingindo tudo o que se relaciona com a matemática. A morte de Monsieur Fourier foi o golpe final sobre o estudante Galois, que, apesar de sua impertinência, mostrava sinais de um grande talento. Ele foi expulso da École Normale, estava sem dinheiro, sua mãe também estava pobre e ele continuava com seus insultos. Dizem que ele vai acabar maluco e eu temo que isto seja verdade".

Um fato documentado por Alexandre Dumas. Dumas estava no restaurante Vendanges des Bourgogne quando houve um banquete em homenagem a dezenove republicanos acusados de conspiração. "Subitamente, no meio de uma conversa particular que eu estava tendo com a pessoa à minha esquerda, ouvi o nome Louis-Phillipe seguido de assobios. Virei-me para olhar e presenciei uma cena muito agitada. Um jovem que erguera seu cálice em saudação segurava um punhal e estava tentando se fazer ouvir – era Évariste Galois, um dos mais ardentes republicanos. Tudo que consegui entender foi uma ameaça e o nome de Louis-Phillipe sendo mencionado: o punhal na mão do rapaz tornava tudo muito claro. Isso estava muito além das minhas opiniões republicanas. Eu e meu amigo pulamos a janela e saímos para o jardim". Estava claro que o episódio teria sérias conseqüências. Dois ou três dias depois Évariste Galois foi preso. Ficou na prisão de Sainte-Pélagie durante um mês, acusado de ameaçar a vida do rei e levado a julgamento. Embora houvesse pouca dúvida de que Galois fosse culpado, a natureza agitada do banquete significava que ninguém poderia confirmar tê-lo ouvido fazer qualquer ameaça direta Um júri simpático e a idade do rapaz—ainda com apenas vinte anos – levaram à sua absolvição. Mas no mês seguinte ele foi preso de novo, sentenciado a seis meses de prisão. Embora abstêmio, influenciado pelos malandros que o cercavam, passou a beber. Uma semana depois um franco-atirador, num sótão do lado oposto da prisão, disparou um tiro contra a cela, ferindo um homem que estava ao lado de Galois, que ficou convencido ser a bala a ele destinada, havendo um complô do governo para assassiná-lo. O medo da perseguição política o aterrorizava. O isolamento dos amigos e da família e a rejeição de suas idéias matemáticas o mergulharam num estado de depressão. Bêbado e delirante, ele tentou se matar com uma faca, mas seus colegas republicanos conseguiram dominá-lo e desarmá-lo.

Uma paixão perigosa: Em março de 1832, um mês antes do final da sentença, irrompeu uma epidemia de cólera em Paris e os prisioneiros de Sainte-Pélagie foram libertados. O que aconteceu com Galois nas semanas seguintes tem motivado muita especulação, mas o que se sabe com certeza é que a tragédia foi o resultado de um romance com uma mulher misteriosa, chamada Stéphanie-Félice Poterine du Motel, filha de um respeitado médico parisiense. Embora ninguém saiba como o caso começou, os detalhes de seu trágico fim estão bem documentados.

Stephanie já estava comprometida com um cidadão chamado Pescheux d'Herbinville, que descobriu a infidelidade de sua noiva. Furioso e sendo um dos melhores atiradores da França não hesitou em desafiar Galois para um duelo ao raiar do dia. Évarist conhecia a perícia de seu desafiante com a pistola. Na noite anterior ao confronto, que ele acreditava ser a última oportunidade que teria para registrar suas idéias no papel, ele escreveu cartas para os amigos explicando as circunstâncias. "Eu peço aos patriotas, meus amigos, que não me censurem por morrer por outro motivo que não pelo meu país. Eu morri vítima de uma infame namoradeira e dos dois idiotas que ela envolveu. Minha vida termina em conseqüência de uma miserável calúnia. Ah! Por que tenho que morrer por uma coisa tão insignificante e desprezível? Eu peço aos céus que testemunhem que foi apenas pela força e a coação que eu cedi à provocação que tentei evitar por todos os meios". Apesar de sua devoção à causa republicana e seu envolvimento romântico, Galois mantivera sua paixão pela matemática. Um de seus maiores temores era de que sua pesquisa, rejeitada pela Academia, se perdesse para sempre. Em uma tentativa desesperada de conseguir reconhecimento, ele trabalhou a noite toda, escrevendo o teorema que, acreditava, explicaria o enigma da equação do quinto grau. As páginas eram, na maior parte, uma transcrição das idéias que ele já enviara a Cauchy e Fourier, mas ocultas em meio à complexa álgebra havia referências ocasionais a "Stéphanie", ou "une femme", e exclamações de desespero – "Eu não tenho tempo, eu não tenho tempo!" No final da noite, quando seus cálculos estavam completos, ele escreveu uma carta explicativa ao seu amigo Auguste Chevalier, pedindo que, caso morresse, aquelas páginas fossem enviadas aos grandes matemáticos da Europa.

"Meu Querido Amigo: Eu fiz algumas novas descobertas em análise. A primeira se refere à teoria das equações do quinto grau e as outras, a funções integrais. Na teoria das equações eu pesquisei as condições para a solução de equações por radicais. Isto me deu a oportunidade de aprofundar esta teoria e descrever todas as transformações possíveis em uma equação, mesmo que ela não seja resolvida pelos radicais. Está tudo aqui nesses três artigos… Em minha vida eu freqüentemente me atrevi a apresentar idéias sobre as quais não tinha certeza. Mas tudo que escrevi aqui estava claro em minha mente durante um ano e não seria do meu interesse deixar suspeitas de que anunciei um teorema dos quais não tenho a demonstração completa. Faça um pedido público a Carl Gustav Jakob Jacobi ou Gauss para que dêem suas opiniões, não pela verdade mas devido à importância desses teoremas. Afinal, eu espero que alguns homens achem valioso analisar esta confusão. Um abraço caloroso. E. Galois"

O duelo: Na manhã seguinte, Quarta-feira, 30 de maio de 1832, num campo isolado, Galois e d'Herbinville se enfrentaram a uma distância de vinte e cinco passos, armados com pistolas. D'Herbinville viera acompanhado de dois assistentes, Évarist Galois estava sozinho. Ele não contara a ninguém sobre seu drama. Um mensageiro que enviara ao seu irmão Alfred, só entregaria a notícia depois do duelo terminado. E as cartas que escrevera na noite anterior só chegariam aos seus amigos vários dias depois. As pistolas erguidas e disparadas. D'Herbinville continuou de pé. Galois foi atingido no estômago. Ficou agonizando no chão. Não havia nenhum cirurgião por perto e o vencedor foi embora calmamente, deixando seu oponente ferido para morrer. Algumas horas depois Alfred chegou ao local e levou seu irmão para o hospital Cochin. Era muito tarde, já ocorrera uma peritonite e no dia seguinte Galois faleceu. Antes de morrer disse para seu irmão: "- Não chore, preciso de toda a minha coragem para morrer aos vinte anos".

Seu funeral foi quase uma réplica do que acontecera com seu pai. A polícia acreditava que a cerimônia seria o foco de uma manifestação política e prendeu trinta amigos de Galois na noite anterior. Ainda assim, dois mil republicanos se reuniram para o enterro e houve brigas inevitáveis entre os colegas de Galois e os representantes do governo que chegaram para vigiar os acontecimentos. Os colegas de Galois estavam furiosos devido à crença cada vez mais forte de que o noivo traído era um agente do governo e Stéphanie não fora apenas uma mulher volúvel, mas uma sedutora usada para levar Galois a uma armadilha. De qualquer modo, um dos maiores matemáticos do mundo morrera com a idade de vinte anos, tendo estudado matemática por apenas cinco anos.

Reconhecimento: Passou-se uma década antes que os trabalhos de Galois fossem reconhecidos. Uma cópia chegou às mãos de Joseph Liouville em 1846. Liouville reconheceu a centelha do gênio naqueles cálculos e passou meses tentando interpretar seu significado. Finalmente ele editou os artigos e os publicou no prestigioso Journal de

Mathématiques Pures et Appliquées. A resposta dos outros matemáticos foi imediata e impressionante. Galois tinha de fato formulado uma completa explicação de como se poderia obter soluções para equações do quinto grau. Primeiro ele classificara todas as equações em dois tipos: que podiam ser solucionadas e as que não podiam. Então, para aquelas que eram solucionáveis, ele deduziu uma fórmula para encontrar as soluções das equações. Além disso, Galois examinou as equações de grau mais alto do que cinco, aquelas que continham x^6, x^7 e assim por diante, podendo identificar as que tinham soluções. Era uma das obras-primas da matemática do século XIX, criada por um de seus mais trágicos heróis.

Referência:

- LIVIO, Mario (1945); "A Equação que ninguém Conseguia Resolver"/ Mario Livio [tradução Jesus de Paula Assis]. Rio de Janeiro: Record, 2008 (http://pt.wikipedia.org/wiki/Evariste_Galois)

“Assidente” versus “limpesa”

Sérgio Brazil
Professor Adjunto da Universidade Federal do Acre

Quando fui cursar mestrado em Brasília, morei em um alojamento estudantil com alguns colegas dos mais diversos Estados. Tinha goiano, paraibano, mineiro, paulista, etc. Era uma turma muito boa. Gostávamos de jogar futebol e depois tomar umas cervejas. Foi uma época muito divertida.

O caso a seguir ocorreu quando um de nossos colegas, chamado aqui ficticiamente por Erasmo, foi tirar sua carteira de motorista, a tão sonhada CNH. Erasmo era do interior de São Paulo, um cara muito bacana e engraçado, gostava de tirar sarro de todo mundo.

Era boca da noite e estávamos na sala de estudo de Erasmo, quando vi uma apostila do DETRAN/DF em sua mesa e comecei a folheá-la. Quando, para minha surpresa, vi, na resposta de uma pergunta, a palavra “assidente”. Não me contive e comecei a rir e mostrei para os demais colegas que estavam presentes na sala de Erasmo. Foi aquela gozação. O pobre do Erasmo ficou sem jeito e constrangido.

Arrependi-me do que fiz, pois Erasmo era um bom amigo e eu, de certa forma, fui sacana com Erasmo, revelando sua deficiência na língua mater.

Na turma tinha um goiano, aqui chamado de Celso, que era muito gozador também e era o que mais sacaneava com o Erasmo por conta do citado episódio. Celso chamava Erasmo de burro, e dizia: “como um cara faz mestrado e não sabe escrever?”

Passaram-se algumas semanas, quando o nosso amigo Celso escreveu uma lista de materiais necessários para a faxina do apartamento que morávamos. Quando ele me passou a bendita lista para eu ver se estava faltando algo, vi que tinha escrito “limpesa”.

No mesmo instante, pensei: Agora me “limpo” com o meu amigo Erasmo.

Era noite quando Erasmo chegou e eu, bem sorridente e sarcástico, mostrei-lhe a lista.

- Veja Erasmo! Observe como nosso amigo Celso escreveu a palavra Limpeza na lista de compras?

Erasmo, não se conteve e depois de muita gargalhada, e num estado de êxtase, detonou:

- Goiano burro, analfabeto, depois fica falando de mim. Todo mundo saber que limpeza se escreve com “ene” e não com “eme”.

Após esse desabafo desrespeitoso para com nossa tão bela língua portuguesa, ficamos todos em silêncio e em seguida demos uma gargalhada. Nosso amigo Erasmo não tem jeito!

MESTRADO PROFISSIONAL EM MATEMÁTICA-PROFMAT

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

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

CURSO DE MESTRADO EM MATEMÁTICA
MINTER CAPES/FUNTAC/UFAC/UFAM

UNIVERSIDADE FEDERAL DO AMAZONAS
UNIVERSIDADE FEDERAL DO ACRE
PRÓ-REITORIAS DE PESQUISA E PÓS-GRADUAÇÃO

No primeiro semestre de 2012, terá início o Curso de Mestrado em Matemática tipo MINTER. O projeto de mestrado é fruto da parceria entre as instituições: UFAM/UFAC/CAPES/FUNTAC e será realizado na UNIVERSIDADE FEDERAL DO ACRE (UFAC). Serão oferecidas 12 vagas onde os alunos podem optar pelas áreas de Geometria, Otimização ou Álgebra.

toujours le même nombre de permutations.

Mais il est curieux de savoir si le degré peut s'abaisser.

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

Voyons donc si l'équation de degré $p+1$ dont les racines x_k s'indiquent en donnant à k toutes les valeurs y compris l'infini et dont le groupe a pour substitutions

$$x_k \qquad x_{\frac{ak+b}{ck+d}}$$

$ad-bc$ étant un carré peut s'abaisser au degré p.

Or il faut pour cela que le groupe se décompose (improprement, s'entend) en p groupes de $(p+1)\frac{p-1}{2}$ permutations chacun.

Soient 0 et ∞ deux lettres conjointes dans l'un de ces groupes. Les substitutions qui ne font pas changer 0 et ∞ de place seront de la forme

$$x_k \qquad x_{m^2k}$$

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

Pour $p=7$ on trouve un groupe de $(p+1)\frac{p-1}{2}$ permutations où $\infty\ 1\ 2\ 4$ ont respectivement pour lettres conjointes $0\ 3\ 6\ 5$.

Ce groupe a ses substitutions de la forme

$$x_k \qquad x_{a\frac{k-b}{k-c}}$$

b étant la lettre conjointe de c et a une lettre qui est à la fois résidu ou non résidu en même temps que c.

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

$\infty\ 1\ 3\ 4\ 5\ 9$ ayant respectivement

pour conjointes $0\ 2\ 6\ 8\ 10\ 7$

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

En toute rigueur cette réduction n'est pas possible dans les cas