Trabalho de Conclusão de Curso - Bacharelado em Matemática

Processos de localização em estruturas algébricas

Juacy Silva Nascimento Santos

Universidade Federal do ABC

Título: Processos de localização em estruturas algébricas

Autor: Juacy Silva Nascimento Santos
Orientador: Prof. Dr. Luis Enrique Ramirez

Trabalho de conclusão de curso apresentado como requisito parcial para obtenção do título de Bacharel em Matemática pela Universidade Federal do ABC.

Banca Examinadora:

Prof. Dr. João Schwarz
Universidade Federal do ABC

Prof. Dr. Nazar Arakelian
Universidade Federal do ABC

Santo André, 31 de agosto de 2023.

Sumário

Resumo

Este trabalho se propõe a elucidar o processo de localização em duas distintas estruturas algébricas: anéis e módulos. No contexto dos anéis, investigaremos esse processo tanto em âmbitos comutativos quanto não comutativos. Em relação aos módulos, a analise será exclusivamente no cenário comutativo. O objetivo da localização reside na capacidade de conferir aos elementos da estrutura a habilidade de se tornarem invertíveis em relação à operação de multiplicação. Um exemplo específico de localização aplicado a anéis comutativos é o conceito de corpo de frações, que por meio de relações de equivalência, alcançamos o menor corpo que contém o anel. Em outras palavras, esse processo torna todos os elementos não nulos do anel original invertíveis. No caso mais geral de localização, a meta não é tornar todos os elementos da estrutura invertíveis, mas sim determinados subconjuntos com propriedades específicas. No contexto dos anéis não comutativos, o processo torna-se mais complexo, uma vez que as operações devem ser executadas sem a comutatividade, uma propriedade fundamental frequentemente utilizada sem o devido reconhecimento. Para compensar a ausência da comutatividade, neste caso, as condições de Ore vêm à tona como requisitos essenciais para viabilizar a localização. Sobre módulos, o trabalho se propõe a apresentar suas propriedades básicas e mostrar a localização para módulos comutativos.

Palavras Chaves: Localização, Anéis, Módulos, Condições de Ore

Abstract

This work aims to elucidate the process of localization in two distinct algebraic structures: rings and modules. In the context of rings, we will investigate this process in both commutative and non-commutative realms. As for modules, the analysis will be exclusively within the commutative scenario. The objective of localization lies in the ability to confer to the elements of the structure the capability of becoming invertible with respect to the multiplication operation. A specific example of localization applied to commutative rings is the concept of the field of fractions, wherein through equivalence relations, we attain the smallest field containing the ring. In other words, this process renders all non-zero elements of the original ring invertible. In the broader context of localization, the goal is not to render all elements of the structure invertible, but rather specific subsets with particular properties. In the context of non-commutative rings, the process becomes more intricate, as operations must be carried out without commutativity, a fundamental property often utilized without due recognition. To compensate for the absence of commutativity, in this case, the Ore conditions emerge as essential requirements to facilitate localization. Regarding modules, the work aims to present their fundamental properties and demonstrate localization for commutative modules.

Keywords: Localization, Rings, Modules, Ore Conditions

1 Introdução

O conceito de fração de números inteiros é fundamental na matemática, sendo apresentado na infância e tendo aplicações em diversas áreas como geometria, computação e entre outras. Porém a noção de fração pode ser estendida, de forma que anéis e módulos tenham suas frações através do processo de localização. O objetivo dessa ferramenta é criar elementos invertíveis para a estrutura e podemos enxergar isso como a construção das frações neste ambiente. Esse análogo é tão interessante que entenderemos porque a divisão por zero não é vantajosa de ser definida.

Inicialmente abordaremos o problema sob o ponto de vista de anéis comutativos, portanto o objetivo será a partir de um anel comutativo que não necessariamente tem unidade, realizar o processo de localização, resultando em um novo anel que possui inversos multiplicativos para alguns elementos.

O próximo passo é entender como podemos fazer localização em módulos, porém essa é uma estrutura que não é estudada durante a graduação na UFABC, por isso, veremos algumas propriedades básicas para termos ferramentas necessárias para a localização em módulos. Além disso, seguir essa ordem é importante, pois o conceito de módulo depende da estrutura de anel e veremos que a localização de um módulo, depende da localização de um anel também.

Por último, a ideia é entender o processo de localização em anéis não comutativos. A comutatividade é uma propriedade que tão intrínseca aos números do nosso cotidiano, que muitas vezes não percebemos que estamos utilizando e perder isso torna muito mais complexo operar em um anel. Por conta disso, para fazer localização é necessário que o anel atenda a algumas condições, essas condições são chamadas condições de Ore e através delas, veremos que é possível construir a localização em um anel não comutativo.

2 Anéis

2.1 Conceitos iniciais

Na álgebra abstrata, a estrutura que chamamos de anel é um conjunto com duas operações binárias, isto é, são operações que atuam em dois elementos deste conjunto e nos resulta em um terceiro, costumamos chamar essas operações de soma e multiplicação. Na verdade, já conhecemos alguns anéis desde a infância mas podemos não enxergar sua estrutura, um exemplo disso são os números inteiros, que com sua soma e multiplicação usual é um anel. Porém, nem todo conjunto com duas operações binárias é um anel, para isso aconteça, as suas operações devem ter algumas propriedades e vamos definir isso a seguir.

Definição 2.1 (Anel) *Seja A um conjunto com duas operações binárias denotadas por $+$ e $*$, se para todo $x, y, z \in A$, temos:*

1. $x + (y + z) = (x + y) + z$
2. $\exists 0 \in A$ *tal que* $\forall x, x + 0 = x$
3. $x + y = y + x$
4. $\exists -x$ *tal que* $x, x + (-x) = 0$
5. $(a * b) * c = a * (b * c)$
6. $a * (b + c) = a * b + a * c$
7. $b * a + c * a = (b + c) * a$

Dizemos que $(A, +, *)$ é um anel, ou só que A é um anel.

Essa definição quer dizer que esperamos que um anel tenha algumas boas propriedades para a sua soma, como comutatividade, existência de oposto, associatividade e para a sua multiplicação esperamos que tenha a associatividade apenas. Também temos uma propriedade que liga essas duas operações.

Existem anéis que tem mais algumas propriedades com relação a multiplicação, por exemplo, quando a multiplicação é comutativa, isto é $a * b = b * a$ chamamos de anel comutativo. Outro exemplo, são anéis que possuem elemento neutro para a multiplicação, isto é, $a * 1 = 1 * a$, chamamos esses anéis de anéis com unidade.

De maneira geral, a definição de anel varia de autor para autor ou com o propósito do trabalho em questão, alguns consideram anéis comutativos com unidade, outros já não necessitam da existência do neutro multiplicativo. Também existem anéis não associativos, então podemos ter um anel sem nenhuma propriedade sobre a multiplicação de maneira mais geral. Para este texto, iremos assumir associatividade, e ao longo do texto estudaremos os casos comutativo e não comutativo sem assumir a existência de identidade.

Agora vamos ver alguns exemplos de anéis:

Exemplo 2.2 Temos que $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ com as suas respectivas operações usuais de soma e produto são anéis comutativos e com unidade.

Exemplo 2.3 Os números inteiros pares, denotados por $2\mathbb{Z}$ também formam um anel com a soma e multiplicação usual. Mas neste caso, note que temos um anel sem a unidade, já que $1 \notin 2\mathbb{Z}$.

Exemplo 2.4 As matrizes quadradas de ordem n, denotadas por A_n, com as operações de soma e produto de matrizes formam um anel não comutativo, já que não é verdade $a, b \in A_n$ $ab = ba$. Por exemplo, em A_2 tomando $a = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ e $b = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ temos que $ab = \begin{pmatrix} 1 & 4 \\ 2 & 5 \end{pmatrix}$ e $ba = \begin{pmatrix} 5 & 5 \\ 2 & 1 \end{pmatrix}$.

Com esses exemplos, já temos uma boa intuição sobre os anéis, mas vemos que algumas coisas não são garantidas por definição. Por exemplo, sabemos que se multiplicarmos um número inteiro por zero, que é o neutro da adição, o resultado do produto é zero, mas isto é válido para todo anel? Veremos que sim.

Proposição 2.5 *Seja A um anel, para todo $x \in A$ temos $x * 0 = 0 * x = 0$.*

Demonstração: Tome $x \in A$, temos que $x * 0 = x * (0 + 0)$ já que 0 é o neutro da soma. Agora aplicando a propriedades distributiva, temos que $x * (0 + 0) = x * 0 + x * 0$, mas isto nos indica que $x * 0 = x * 0 + x * 0$. Somando o inverso aditivo em ambos lados da equação temos que $x * 0 + (-x * 0) = x * 0 + x * 0 + (-x * 0)$ que é igual a $0 = x * 0$.

Analogamente, podemos fazer o caso para $0 * x$, que resultará em $0 * x = 0 = x * 0$. □

A partir desses exemplos e da proposição anterior, podemos imaginar que muitas propriedades desses anéis conhecidos são estendidas para qualquer anel, porém devemos tomar cuidado porque nem tudo é válido e pode ser um caso particular de apenas um anel.

Outra noção importante que temos relacionada aos anéis, são os subanéis, que nada mais são do que anéis dentro de anéis. Ou seja, dentro de uma estrutura de um anel, pode existir uma segunda estrutura, ou seja, restringindo as operações a uma parte do anel, tudo continua sendo respeitado dentro deste subconjunto. Voltando para os nossos exemplos já conhecidos, temos que $\mathbb{Z}$ e $\mathbb{Q}$ são anéis, mas $\mathbb{Z} \subset \mathbb{Q}$, portanto podemos enxergar os números inteiros como um subanel dos números racionais.

Veja agora a definição formal disso:

Definição 2.6 (Subanéis) *Seja $S \subseteq A$, onde A é um anel, dizemos que S é um subanel de A se dados $s, t \in S$ temos:*

1. $s + t \in S$
2. *Se $s \in S$ então $-s \in S$*
3. $0 \in S$
4. $s * t \in S$

Exemplo 2.7 O conjunto dos números pares, que vamos denotar por $2\mathbb{Z}$ é um subanel dentro do anel $\mathbb{Z}$.

Outra definição que é importante para o estudo de anéis é a de ideal. Este conceito tem a característica de "absorver" elementos de fora com a multiplicação, isto é, ao multiplicar um elemento do ideal por outro que não está, o resultado da multiplicação também está no ideal. Isto parece bem estranho, mas pensando no subconjunto dos pares com relação aos números inteiros, sabemos que a soma de dois número pares é par e a multiplicação de um ímpar por um par, é par, então os pares "absorvem" os impares nesse sentido.

Outro ponto que é importante ressaltar sobre os ideias é que quando o anel é não comutativo, temos distinção entre os lados em que ocorre a "absorção" , dessa forma teremos ideias à esquerda ou à direita. Neste texto, irei fazer as definições à esquerda. De maneira mais formal, temos

Definição 2.8 *Seja A um anel com $I \subseteq A$ e $I \neq \emptyset$ dizemos que I é um ideal a esquerda de A se:*

1. $0_A \in I$
2. $x, y \in I$ *então* $x + y \in I$
3. $a \in A$ *e* $x \in I$ *então* $ax \in I$

Observação 2.9 *Analogamente, podemos definir o ideal à direta de um anel. Vale ressaltar que para anéis comutativos, um ideal à esquerda também é um ideal à direita, já que $ax = xa$. Quando I é um ideal à esquerda e à direita, dizemos que I é um ideal bilateral.*

Os ideais são importantes nos estudos de anéis, pois através deles conseguimos por exemplo fazer quociente de anéis.

Dois tipos de ideais que são bem importantes e vamos utilizar durante o texto são os ideias primos e os ideais maximais que vamos definir agora.

Definição 2.10 (Ideal maximal) *Seja A um anel e $I \subseteq A$ tal que I é ideal a esquerda de A. Dizemos que I é um ideal maximal a esquerda de A se não existe outro ideal a esquerda $J \neq A$ tal que $I \subset J$.*

De maneira mais simples, um ideal maximal é um ideal que não está contido propriamente dentro de outro ideal além do próprio anel.

Definição 2.11 (Ideal primo) *Seja A um anel e I ideal à esquerda de A. Dizemos que I é um ideal primo, se dados J, L ideais à esquerda de A, tal que $JL \subseteq I$ tem-se $J \subseteq I$ ou $L \subseteq I$ para todos ideais à esquerda J, L de A.*

Para simplificar, como só iremos trabalhar com ideias primos em anéis comutativos, definiremos ideal primo neste caso mais restrito.

Definição 2.12 (Ideal primo) *Seja A um anel comutativo e $I \subseteq A$ tal que I é ideal de A. Dizemos que I é um ideal primo, se dado $xy \in I$ tem-se $x \in I$ ou $y \in I$.*

Em outras palavras, se um produto pertence ao ideal I, então pelo menos um dos fatores do produto pertence ao ideal. Note, que está definição é especifica para anéis comutativos.

Além desses ideais, podemos ter outros ideais a partir de subconjuntos de um anel, falamos que esses ideais são gerados por um conjunto.

Definição 2.13 *Seja A um anel e $S \subseteq A$ com $S \neq \emptyset$, o ideal à esquerda gerado pelo conjunto S é o menor ideal que contêm S. Denotamos esse ideal por $\langle S \rangle$. Dessa forma $\langle S \rangle = \bigcap_{S \subseteq I} I$, onde I é um ideal à esquerda de A.*

Especificamente, para um anel comutativo com unidade A, conseguimos caracterizar o ideal gerado por I com ainda mais clareza. Pois, o ideal gerado será formado pelas somas finitas de elementos da forma ai, onde $a \in A$ e $i \in I$.

Proposição 2.14 *Seja A um anel comutativo com unidade, onde $1 \neq 0$ e $S \subseteq A$ então $\langle S \rangle = \{\sum_{i=1}^{n} a_i s_i$ onde $a_i \in A, s_i \in S\}$.*

Demonstração:

Primeiro, vamos mostrar que $J = \{\sum_{i=1}^{n} a_i s_i$ onde $a_i \in A, s_i \in S\}$ é um ideal.

1. $0_A \in < S >$.

   Temos que $S \neq \emptyset$, tome $x \in S$ temos que $0_A x = 0_A \in J$.

2. $x, y \in J$ então $x + y \in J$.

   Temos então que $x = \sum_{i=1}^{k} a_i x_i$ e $y = \sum_{j=1}^{m} b_j y_j$ onde $a_i, b_j \in A$ e $x_i, y_j \in S$.

   Temos então $x + y = \sum_{i=1}^{k} a_i x_i + \sum_{j=1}^{m} b_j y_j = \sum_{l=1}^{k+m} c_l z_l$ onde $c_l = a_i$, $z_l = x_i$ quando $1 \leq l \leq k$ e $c_l = b_i$, $z_l = y_i$ quando $k + 1 \leq l \leq k + m$ portanto $x + y \in J$

3. $a \in A$ e $x \in J$ então $x + y \in J$.

   Temos então que $x = \sum_{i=1}^{k} a_i x_i$, logo $ax = a \sum_{i=1}^{k} a_i x_i = \sum_{i=1}^{k} a a_i x_i \in J$.

Portanto, J é um ideal de A.

Agora devemos mostrar que $\langle S \rangle = J$. Claramente que $S \subseteq J$, dessa forma $\langle S \rangle \subseteq J$, já que J está na intersecção de todos os ideias que contém S.

Para mostrar que $J \subseteq \langle S \rangle$, suponha $x \in J$, sabemos que $x = \sum_{i=1}^{n} a_i s_i$ para $a_i \in A$ e $s_i \in S$, onde $s_i \in \langle S \rangle$ e como $\langle S \rangle$ é um ideal, então $a_i s_i \in \langle S \rangle$ e a suas somas finitas também, dessa forma $x = \sum_{i=1}^{n} a_i s_i \in \langle S \rangle$. □

Além de ideias e subanéis, outro conceito importante que precisamos estudar é o conceito de homomorfismo. Dados dois anéis, seria interessante também estabelecer uma relação entre essas duas estruturas, de forma que isso respeitasse a estrutura dos anéis. Geralmente, quando vamos relacionar dois conjuntos, utilizamos funções, mas no caso de anéis essas funções precisam de uma propriedade a mais e são chamadas de homomorfismo.

Definição 2.15 (Homomorfismo) *Sejam A, B anéis e f uma função $f : A \rightarrow B$, f é dita homomorfismo de anéis se:*

1. $f(x+y) = f(x) + f(y)$

2. $f(xy) = f(x)f(y)$

Observação 2.16 *Caso A, B sejam anéis com unidade, temos que a seguinte condição também é necessária $f(1_A) = 1_B$.*

Agora vamos começar a misturar um pouco as coisas, falando de ideais e homomorfismos.

Proposição 2.17 *Seja $f : A \to B$ um homomorfismo de anéis e J um ideal à esquerda de B então $f^{-1}(J)$ é um ideal à esquerda de A. Ou seja, a pré-imagem de um ideal à esquerda é um ideal à esquerda.*

Observação 2.18 *Seja $f : A \to B$ um homomorfismo de anéis e I um ideal a esquerda de A, não podemos garantir que $f(I)$ é um ideal a esquerda de B.*

Por exemplo, tome $i : \mathbb{Z} \to \mathbb{Q}$ sendo $i(x) = x$. Temos que $\mathbb{Q}$ é um corpo, portanto seus únicos ideias são $\{0\}$ e $\mathbb{Q}$. Tome $2\mathbb{Z}$ ideal bilateral de $\mathbb{Z}$ temos que $i(2\mathbb{Z}) \neq \{0\}$ e $i(2\mathbb{Z}) \neq \mathbb{Q}$ portanto não é um ideal de $\mathbb{Q}$.

Para finalizar essa seção de conceitos básicos de anéis que iremos utilizar, definiremos a noção de divisor de zero. Intuitivamente, sabemos que dividir por zero não é uma característica que esperemos dos números, na verdade, no contexto dos números reais, não existe a divisão por zero, porém no caso mais geral de anéis, podemos ter a multiplicação de dois elementos não nulo sendo igual a zero e chamamos os elementos que possuem essa propriedade de divisores do zero. Porém, muitas vezes queremos evitar esses casos, então também definiremos o conceito de domínio de integridade, que são anéis comutativos que não possuem elementos que são divisores do zero.

Definição 2.19 (Divisores de zero) *Se A um anel se $xy = 0$ com $x \neq 0$ e $y \neq 0$, x é chamado de divisor de zero a esquerda.*

Observação 2.20 *No caso comutativo em particular, como $xy = yx$, ser divisor de zero à esquerda implica em ser divisor de zero à direita e vice-versa. Neste caso, dizemos apenas que o elemento é um divisor de zero.*

Definição 2.21 (Domínio de integridade) *Seja A um anel comutativo, sem divisores de zero, dizemos que A é um domínio de integridade.*

2.2 Corpo de frações

Nesta seção, vamos tratar de uma construção que é vista durante o curso de Anéis e Corpos. Essa construção é importante neste trabalho, porque vemos que a localização é uma generalização desse conceito. Ou seja, vamos ver que esta construção, é um caso particular de localização. Por se tratar de um caso particular, não vamos acompanhar as demonstrações com todos os detalhes, já que iremos fazer o caso mais geral quando estivermos tratando de localização. Os passos com mais detalhes são encontrados na referência [Her75].

O objetivo aqui, é mostrar que a partir de um domínio de integridade, podemos encontrar um corpo no qual esse anel "está contido". Ou seja, queremos expandir esse anel para um corpo e para que isso seja necessário, todo elemento original do anel deverá ter um inverso multiplicativo. Um exemplo disso são os números inteiros, que é um anel mas podemos encontrar-lós dentro dos racionais que formam um corpo.

Um ponto que precisa de mais formalidade no que foi dito acima é o conceito de estar contido.

Definição 2.22 *Se temos f um homomorfismo injetivo de A para B então podemos identificar A com um subanel de B. Diremos que A está embutido em B.*

Proposição 2.23 *Todo domínio de integridade está embutido em um corpo.*

Demonstração: Seja A um anel que é um domínio de integridade, ou seja, não possui divisores de zero. Vamos definir uma relação no conjunto $A \times S$, onde $S = A \setminus \{0\}$. Dessa forma, podemos identificar os elementos de $A \times S$ como $\overline{(a,s)}$ onde $s \neq 0$, são as frações de elementos do anel. Primeiro queremos definir algumas propriedades básicas:

1. Duas frações são iguais se $\overline{(a,s)} = \overline{(b,t)}$, isto é, significa que $at = sb$ onde $s,t \neq 0$.
2. Para somar as frações temos que $\overline{(a,s)} + \overline{(b,t)} = \overline{(at+sb,st)}$.
3. Para multiplicar as frações temos que $\overline{(a,s)} * \overline{(b,t)} = \overline{(ab,st)}$.

Com isto, temos que a relação dada por $\overline{(a,s)} = \overline{(b,t)}$ se e somente se $at = sb$, é uma classe de equivalência. Novamente, não vamos fazer esses detalhes agora, mas veremos algo bem parecido a frente.

Seja C o conjunto de todas as classes de equivalência com as operações de soma e multiplicação que definimos acima, isto forma um corpo.

Aqui também não vamos fazer todos os passos, apenas o passo que para cada elemento existe um inverso multiplicativo, já que no caso de localização vamos ter um anel e não um corpo.

Seja $\overline{(a,s)}$ uma classe de equivalência, temos então que achar um elemento $\overline{(b,t)}$ de tal forma que $\overline{(a,s)} * \overline{(b,t)} = \overline{(d,d)}$, onde $d \neq 0$.

O primeiro ponto dessa igualdade acima, é que o elemento $\overline{(d,d)}$ onde $d \neq 0$, se comporta como a unidade no conjunto C. De fato, seja $\overline{(a,b)} \in C$, temos que $\overline{(a,b)} * \overline{(d,d)} = \overline{(ad,bd)}$. Mas note que essas classes são equivalentes. Perceba que $\overline{(a,b)} = \overline{(ad,bd)}$ se e somente se $abd = bad$ e como A é um anel comutativo, essa última igualdade é válida. Então, multiplicar o denominador e o numerador por um elemento não nulo, não modifica a classe.

Agora vamos tentar encontrar o inverso multiplicativo do elemento $\overline{(a,s)}$. Tomando $\overline{(b,t)} = \overline{(s,a)}$, temos então que $\overline{(a,s)} * \overline{(s,a)} = \overline{(as,sa)}$. Como $as = sa$ pois é um anel comutativo e $as \neq 0$ pois é um domínio de integridade, logo $\overline{(a,s)}$ é invertível. Ou seja, todo elemento diferente do zero possui inverso.

Para finalizar, veremos que existe um homomorfismo injetor entre A e C.

Seja o isomorfismo dado por $f : A \to C$ tal que $f(a) = \overline{(as,s)}$ para um $s \neq 0$. Geralmente, nos livros pegamos o elemento 1, porém pode ser qualquer outro diferente de zero, caso não tenha unidade no anel original.

Para f ser homomorfismo injetivo, temos que verificar as condições de soma, multiplicação e injetividade.

1. (Soma) Seja $a,b,s \in A$, logo $f(a+b) = \overline{((a+b)s,s)} = \overline{(as+bs,s)} = \overline{(ass+bss,ss)} = \overline{(as,s)} + \overline{(bs,s)} = f(a) + f(b)$.

2. (Multiplicação) Seja $a,b,s \in A$, logo $f(ab) = \overline{(abs,s)} = \overline{(abss,ss)} = \overline{(as,s)}\overline{(bs,s)} = f(a)f(b)$.

3. (Injetividade) Tome $a \neq b$, onde $a,b \in A$. Aplicando a definição de f, $f(a) = \overline{(as,s)}$ e $f(b) = \overline{(bs,s)}$. Vamos supor que $\overline{(as,s)} = \overline{(bs,s)}$, logo $ass = sbs = bss$ que nos leva a $ass - bss = (a-b)ss = 0$, dessa forma como A é um domínio de integridade $a - b = 0$ ou $ss = 0$ no entanto $s \neq 0$, assim $ss \neq 0$ e $a \neq b$, logo $a - b \neq 0$, portanto $\overline{(as,s)} \neq \overline{(bs,s)}$.

□

Então, o que fizemos aqui foi a partir de um domínio de integridade qualquer, chegamos em um corpo. De maneira informal, seria como se a gente estivéssemos, adicionando os inversos para que tenhamos um corpo. Agora o que vamos ver é uma generalização disso, invés da gente fazer para todos os elementos não nulos do anel, vamos escolher quem vai ganhar o inverso na localização e por causa disso não necessariamente vamos ter um corpo mas sim um anel, já que nem todos os elementos não nulos vão ser invertíveis.

2.3 Localização em anéis comutativos

Como dito na seção anterior, vamos tentar generalizar o que foi feito para o corpo de frações, mas de forma que vamos escolher quem se tornará inversível.

Vamos seguir a demonstração a partir de um anel A que não necessariamente tem unidade, na referência [AM69] temos a demonstração feita para anel com unidade, porém preferimos não assumir em prol da generalidade.

Para iniciar, vamos precisar do conceito de conjunto multiplicativo. Que nada mais é, do que um conjunto não vazio e fechado para a multiplicação.

Definição 2.24 *Um subconjunto S de um anel A é dito um conjunto multiplicativo se $S \neq \emptyset$ e $x \cdot y \in S$ para todo $x, y \in S$.*

Observação 2.25 *Na referência [AM69], é utilizado um anel com unidade, por isso a definição de subconjunto multiplicativo pede $1 \in S$. No nosso caso, não faz sentido pedir $1 \in S$, para adaptar vamos trocar aquela condição pela existência de um elemento no conjunto que não seja o zero do anel. No exemplo 2.36 vamos entender porque não desejamos que $0 \in S$.*

Agora que já temos todas as definições necessárias para iniciar a construção. Primeiro, vamos definir uma relação de equivalência no conjunto $A \times S$ que será dada por $\overline{(a,s)} \equiv \overline{(b,t)} \Leftrightarrow (ta - sb)u = 0$ para algum $u \in S$.

Proposição 2.26 *A relação em $A \times S$ definida por $\overline{(a,s)} \equiv \overline{(b,t)} \Leftrightarrow (ta - sb)u = 0$ para algum $u \in S$, é de equivalência.*

Demonstração: Vamos mostrar que é uma relação reflexiva, simétrica e transitiva.

1. (Reflexiva)

   Vejamos que $\overline{(a,s)} \equiv \overline{(a,s)}$. De fato, pois $sa - sa = 0$, tomando qualquer $t \in S$ temos que $(sa - sa)t = 0$.

2. (Simétrica)

Suponha que $\overline{(a,s)} \equiv \overline{(b,t)}$ logo existe $u \in S$ tal que $(ta - sb)u = 0$. Note que podemos somar o inverso aditivo do elemento $(ta - sb)u$ em ambos lados da igualdade que nos leva a $(ta - sb)u - ((ta - sb)u) = -(ta - sb)u$. Logo temos que, $0 = -(ta - sb)u = (-ta + sb)u = 0$ reorganizando os termos, $-ta + sb = sb - ta$ portanto $(sb - ta)u = 0$ que é equivalente a $\overline{(b,t)} \equiv \overline{(a,s)}$.

3. (Transitiva)

   Assumindo que $\overline{(a,s)} \equiv \overline{(b,t)}$ e $\overline{(b,t)} \equiv \overline{(c,r)}$, devemos chegar em $\overline{(a,s)} \equiv \overline{(c,r)}$. De $\overline{(a,s)} \equiv \overline{(b,t)}$ temos $(ta - sb)u_1 = 0$ para algum $u_1 \in S$. De $\overline{(b,t)} \equiv \overline{(c,r)}$ temos $(rb - tc)u_2 = 0$ para algum $u_2 \in S$.

   Multiplicando a primeira equação por ru_2 e a segunda por su_1 chegamos a $ru_2(ta - sb)u_1 = 0$ e $su_1(rb - tc)u_2 = 0$. Utilizando a comutatividade para agrupar os termos em u chegamos a $r(ta - sb)u_1u_2 = 0$ e $s(rb - tc)u_1u_2 = 0$. Aplicando a propriedade distributiva $(rta - rsb)u_1u_2 = 0$ e $(srb - stc)u_1u_2 = 0$. Novamente utilizando a comutatividade para ajustar os termos, chegamos as duas equações

   (*) $(art - sbr)u_1u_2 = 0$

   (**) $(sbr - sct)u_1u_2 = 0$

   Em (**) temos que ao aplicar a distributiva e chegamos a $sbru_1u_2 = sctu_1u_2$, porém note que temos em (*) ao aplicar a distributiva $artu_1u_2 = sbru_1u_2$. Portanto temos, $artu_1u_2 = sctu_1u_2$. Logo, $0 = (art - sct)u_1u_2 = (ar - sc)tu_1u_2$.

   Mas como $t, u_1, u_2 \in S$ e S é um conjunto multiplicativo, logo $tu_1u_2 \in S$ e portanto $(a,s) \equiv (c,r)$.

Portanto, a relação definida em $A \times S$ é de equivalência.

$\square$

Denotamos por $S^{-1}A$ o conjunto das classes de equivalência e por $\overline{(a,s)}$ ou $\frac{a}{s}$ a classe de equivalência de (a,s). Neste texto, vamos preferir a notação $\overline{(a,s)}$.

Já temos o conjunto com as relações de equivalência, agora queremos definir operações em $S^{-1}A$ e mostrar que com essas operações o conjunto é um anel.

Definição 2.27 *A soma em $S^{-1}A$ é definida por $\overline{(a,s)} + \overline{(b,t)} = \overline{(at + sb, st)}$.*

Definição 2.28 *A multiplicação em $S^{-1}A$ é definida por $\overline{(a,s)} * \overline{(b,t)} = \overline{(ab, st)}$.*

Como estamos trabalhando com classes de equivalência precisamos garantir que essas operações estão bem definidas, ou seja, que as operações acima não dependem do representante da classe.

Proposição 2.29 *As operações de soma e multiplicação em $S^{-1}A$ não dependem dos representantes da classe.*

Demonstração: Seja $\overline{(a_1, s_1)} = \overline{(a_2, s_2)}$ e $\overline{(b_1, t_1)} = \overline{(b_2, s_2)}$, devemos mostrar que $\overline{(a_1, s_1)} + \overline{(b_1, t_1)} = \overline{(a_2, s_2)} + \overline{(b_2, t_2)}$ e que $\overline{(a_1, s_1)} * \overline{(b_1, t_1)} = \overline{(a_2, s_2)} * \overline{(b_2, t_2)}$.

1. (Soma)

   Realizando as somas temos $\overline{(a_1, s_1)} + \overline{(b_1, t_1)} = \overline{(t_1 a_1 + s_1 b_1, s_1 t_1)}$ e $\overline{(a_2, s_2)} + \overline{(b_2, t_2)} = \overline{(t_2 a_2 + s_2 b_2, s_2 t_2)}$.

   Devemos mostrar que $\overline{(t_1 a_1 + s_1 b_1, s_1 t_1)} = \overline{(t_2 a_2 + s_2 b_2, s_2 t_2)}$, para isso devemos ter $\alpha[s_2 t_2(t_1 a_1 + s_1 b_1) - s_1 t_1(t_2 a_2 + s_2 b_2)]$ para $\alpha \in S$.

   Sabemos pela igualdade das classes que

   a) Existe $u_1 \in S$ tal que $(s_2 a_1 - s_1 a_2)u_1 = 0$ que é equivalente a $s_2 a_1 u_1 = s_1 a_2 u_1$

   b) Existe $u_2 \in S$ tal que $(t_2 b_1 - t_1 b_2)u_2 = 0$ que é equivalente a $t_2 b_1 u_2 = t_1 b_2 u_2$

   Ao multiplicar a) por $t_1 t_2 u_2$ e b) por $s_1 s_2 u_1$ ficamos com $t_1 t_2 u_2 s_2 a_1 u_1 = t_1 t_2 u_2 s_1 a_2 u_1$ e $s_1 s_2 u_1 t_2 b_1 u_2 = s_1 s_2 u_1 t_1 b_2 u_2$. Somando as duas equações agora ficamos com $t_1 t_2 u_2 s_2 a_1 u_1 + s_1 s_2 u_1 t_2 b_1 u_2 = t_1 t_2 u_2 s_1 a_2 u_1 + s_1 s_2 u_1 t_1 b_2 u_2$. Colocando em evidência os termos em com $s_1 s_2 u_1 u_2$ e $t_1 t_2 u_1 u_2$ ficamos com $t_1 t_2 u_1 u_2(s_2 a_1 - s_1 a_2) - s_1 s_2 u_1 u_2(t_2 b_1 - t_1 b_2) = 0$. Note que, colocando $u_1 u_2$ em evidência ficamos com $u_1 u_2[t_1 t_2(s_2 a_1 - s_1 a_2) - s_1 s_2(t_2 b_1 - t_1 b_2)] = 0$ portanto, tomando $\alpha = u_1 u_2$ chegamos a igualdade das classes. Lembre que $u_1, u_2 \in S$, logo $u_1 u_2 \in S$.

2. (Produto)

   Realizando os produtos $\overline{(a_1, s_1)} * \overline{(b_1, t_1)} = \overline{(a_1 b_1, s_1 t_1)}$ e $\overline{(a_2, s_2)} * \overline{(b_2, t_2)} = \overline{(a_2 b_2, s_2 t_2)}$.

   Queremos mostrar que $\overline{(a_1 b_1, s_1 t_1)} = \overline{(a_2 b_2, s_2 t_2)}$, que é equivalente a mostrar que existe $\alpha \in S$ tal que $(s_2 t_2 a_1 b_1 - s_1 t_1 a_2 b_2)\alpha = 0$.

   Sabemos pela igualdade das classes que

   a) Existe $u_1 \in S$ tal que $(s_2 a_1 - s_1 a_2)u_1 = 0$ que é equivalente a $s_2 a_1 u_1 = s_1 a_2 u_1$

   b) Existe $u_2 \in S$ tal que $(t_2 b_1 - t_1 b_2)u_2 = 0$ que é equivalente a $t_2 b_1 u_2 = t_1 b_2 u_2$

Ao multiplicar a) por $t_2b_1u_2$ e b) por $s_1a_2u_1$ ficamos com $t_2b_1u_2s_2a_1u_1 = t_2b_1u_2s_1a_2u_1$ e $s_1a_2u_1t_2b_1u_2 = s_1a_2u_1t_1b_2u_2$. Reordenando os termos do produto da segunda parcela da igualdade da primeira equação e a primeira parcela da igualdade da segunda equação temos que $t_2b_1u_2s_2a_1u_1 = a_2b_1s_1t_2u_1u_2$ e $a_2b_1s_1t_2u_1u_2 = s_1a_2u_1t_1b_2u_2$, logo $t_2b_1u_2s_2a_1u_1 = s_1a_2u_1t_1b_2u_2$. Portanto $t_2b_1u_2s_2a_1u_1 - s_1a_2u_1t_1b_2u_2 = 0$, colocando u_1u_2 em evidência temos $u_1u_2(t_2b_1s_2a_1 - s_1a_2t_1b_2) = 0$ reordenando os termos ficamos com $u_1u_2(s_2t_2a_1b_1 - s_1t_1a_2b_2) = 0$ tomando $\alpha = u_1u_2$ chegamos a igualdade das classes.

□

Agora sabemos que as operações de soma e multiplicação não dependem dos elementos escolhidos para representar a classe, porém antes de verificarmos que com essas operações temos um anel em $S^{-1}A$, vamos estudar umas propriedades que vamos utilizar mais a frente.

A primeira delas, é que quando temos uma fração e multiplicamos pelo mesmo elemento o numerador e o denominador é esperado que a fração resultante equivalente a fração inicial. Por exemplo, nos racionais $\frac{1}{2} = \frac{2}{4}$, ou seja, multiplicar por 2 nos levou a uma fração equivalente. Para a localização, isto também acontece mas temos uma pequena restrição nos elementos que podemos multiplicar.

Proposição 2.30 *Seja $\overline{(a,s)} \in S^{-1}A$, temos que se $t \in S$, então $\overline{(a,s)} = \overline{(ta,ts)}$.*

Demonstração: Para termos que $\overline{(a,s)} = \overline{(ta,ts)}$, devemos ter que existe $u \in S$ tal que $(tsa - sta)u = 0$. Mas como estamos em um anel comutativo, $tsa = sta$ logo $tsa - sta = 0$, portanto podemos tomar como sendo qualquer elemento de S que é não vazio. □

Outro ponto interessante dessa proposição, é que podemos ver essa multiplicação por um mesmo elemento no numerador e no denominador como uma multiplicação pela unidade. $\overline{(a,s)} = \overline{(ta,ts)}$ onde $t \in S$, mas também $\overline{(ta,ts)} = \overline{(t,t)} * \overline{(a,s)}$. Portanto, basicamente toda fração composta pelo mesmo elemento no numerador e no denominador é a identidade, com a restrição que esse elemento deve pertencer a S.

Agora, sabendo isto, vamos mostrar que $S^{-1}A$ é um anel com as operações que definimos.

Proposição 2.31 *$S^{-1}A$ com a soma e a multiplicação definidas acima é um anel com unidade.*

Demonstração:

1. (Associatividade da soma) $[\overline{(a,s)} + \overline{(b,t)}] + \overline{(c,v)} = \overline{(a,s)} + [\overline{(b,t)} + \overline{(c,v)}]$

Temos que $[\overline{(a,s)}+\overline{(b,t)}] = \overline{(at+sb,st)}$, logo $\overline{(at+sb,st)}+\overline{(c,v)} = \overline{([at+sb]v+stc,stv)} = \overline{(atv+sbv+stc,stv)}$.

Agora partindo para o outro lado da igualdade $[\overline{(b,t)}+\overline{(c,v)}] = \overline{(bv+tc,tv)}$, logo $\overline{(a,s)}+\overline{(bv+tc,tv)} = \overline{(atv+s[bv+tc],stv)} = \overline{(atv+sbv+stc,stv)}$.

Portanto a igualdade é verdadeira, logo é associativa.

2. (Elemento neutro da soma) Se existe elemento tal que $\overline{(a,s)}+x = \overline{(a,s)}$.

   Tome $x = \overline{(0,u)}$ para $u \in S$, logo temos que $\overline{(a,s)}+\overline{(0,u)} = \overline{(au+s0,su)} = \overline{(au,su)} = \overline{(a,s)}$.

   Portanto $\overline{(0,u)}$ é o elemento neutro. Ou seja, o elemento neutro da soma é formado pelo 0 no numerador e qualquer elemento de S no denominador.

3. (Oposto da soma) Se existe elemento tal que $\overline{(a,s)}+x = \overline{(0,u)}$.

   Tome $x = \overline{(-a,s)}$, assim $\overline{(a,s)}+\overline{(-a,s)} = \overline{(as-sa,ss)} = \overline{(0,ss)} = \overline{(0,u)}$.

4. (Comutatividade da soma) $\overline{(a,s)}+\overline{(b,t)} = \overline{(b,t)}+\overline{(a,s)}$

   $\overline{(a,s)}+\overline{(b,t)} = \overline{(at+sb,st)}$ e $\overline{(b,t)}+\overline{(a,s)} = \overline{(bs+ta,tb)}$. Como A é comutativo, logo $at+sb = bs+ta$ e $st = tb$, portanto a igualdade é válida.

5. (Associatividade da multiplicação) $[\overline{(a,s)}*\overline{(b,t)}]*\overline{(c,v)} = \overline{(a,s)}*[\overline{(b,t)}*\overline{(c,v)}]$.

   Primeiro, o lado direito da equação $[\overline{(a,s)}*\overline{(b,t)}] = \overline{(ab,st)}$, logo $= \overline{(ab,st)}*\overline{(c,v)} = \overline{(abc,stv)}$.

   Agora o lado esquerdo $[\overline{(b,t)}*\overline{(c,v)}] = \overline{(bc,tv)}$, logo $= \overline{(a,t)}*\overline{(bc,tv)} = \overline{(abc,stv)}$.

   Logo a igualdade é válida.

6. (Elemento neutro da multiplicação) Se existe elemento tal que $\overline{(a,s)}*x = \overline{(a,s)}$.

   Tome $x = \overline{(u,u)}$, logo temos que $\overline{(a,s)}*\overline{(u,u)} = \overline{(au,su)} = \overline{(a,s)}$. Ou seja, quando o denominador e o numerador são formados pelo mesmo elemento de S, teremos o elemento neutro da multiplicação.

7. (Distributividade) $\overline{(a,s)}*[\overline{(b,t)}+\overline{(c,v)}] = \overline{(a,s)}*\overline{(b,t)}+\overline{(a,s)}*\overline{(c,v)}$.

   Vamos desenvolver o lado esquerdo da equação, temos então que $\overline{(a,s)}*[\overline{(b,t)}+\overline{(c,v)}] = \overline{(a,s)}*\overline{(bv+tc,tv)} = \overline{(a[bv+tc],stv)} = \overline{(abv+atc,stv)}$.

   Agora desenvolvendo o lado direito, temos $\overline{(a,s)}*\overline{(b,t)}+\overline{(a,s)}*\overline{(c,v)} = \overline{(ab,st)}+\overline{(ac,sv)} = \overline{(absv+stac,stsv)}$. Como tudo é comutativo, temos que $\overline{(absv+stac,stsv)} = \overline{(sabv+satc,sstv)} = \overline{(abv+atc,stv)}$.

Logo a igualdade se verifica.

$\square$

Para solidificar um pouco o nosso entendimento, vamos ver alguns exemplos. O primeiro deles mostra que realmente o caso do corpo de frações é um caso particular do que fizemos para a localização para um anel comutativo.

Exemplo 2.32 Quando A é um domínio de integridade temos um caso particular do anel de frações, isso acontece pois tomando $S = A \setminus \{0\}$ é um conjunto multiplicativo.

Para provar o exemplo acima, basta provar a seguinte proposição.

Proposição 2.33 *Seja A um domínio de integridade, então o conjunto $S = A \setminus \{0\}$ é um conjunto multiplicativo.*

Demonstração: Temos também que para xy com $x, y \in s$ já que $xy \neq 0$, pois A é um domínio de integridade e x e y não podem ser nulos. Portanto S é fechado na multiplicação, logo é um conjunto multiplicativo. $\square$

Exemplo 2.34 Tomando como nosso anel os inteiros $\mathbb{Z}$ e o nosso conjunto multiplicativo como $S = \mathbb{Z} \setminus 0$, teremos $\frac{a}{b}$, onde $a \in \mathbb{Z}$ e $b \in S$, ou seja, b deve ser inteiro não nulo e isso é exatamente a definição dos números racionais, que sabemos que é um corpo. Vimos a construção do corpo dos racionais a partir dos inteiros, como localização.

Um outro exemplo, agora realmente mostrando que teremos um anel e não um corpo sempre.

Exemplo 2.35 Podemos tomar como $A = \mathbb{Z}$ e S sendo as potências de 2, ou seja, $S = \{2^n\}$ com $n \geq 0$, dessa forma $S^{-1}A = \{\frac{a}{b}$ tal que $a \in A$ e $b = 2^n\}$ com $n \geq 0$.

A localização resultante neste exemplo não é um corpo, pois vários elementos não possuem inverso multiplicativo, como por exemplo o número 3.

Outro comentário que havia feito no inicio dessa seção é com relação ao conjunto S. Havia dito que não gostaríamos que ocorresse , $0 \in S$. Caso isso ocorresse, estaríamos permitindo frações com zero no denominador, mas dividir por zero, tem um preço e veremos isso nesse próximo exemplo.

Exemplo 2.36 Temos que $S^{-1}A$ será o anel trivial se $0 \in S$. De fato, se $0 \in S$ podemos tomar u da relação de equivalência como 0, dessa forma $(at - sb)0 = 0$ para todo $\overline{(a, s)}$ e $\overline{(b, t)}$, dessa forma todos os elementos são equivalentes entre si, em particular serão equivalente ao elemento $\overline{(0,0)}$, ou seja, $S^{-1}A$ pode ser representado por um único elemento, o $\overline{(0,0)}$. Portanto o preço de localizar por zero é que todo mundo vira o mesmo elemento.

Observação 2.37 *Um importante homomorfismo é o que pode garantir que $f(A) \subseteq S^{-1}A$. Seja $f : A \to S^{-1}A$ definida como $f(a) = \overline{(as,s)}$ onde $s \in S$ com $s \neq 0$.*

Proposição 2.38 *Seja A um anel e S um conjunto multiplicativo, então a função f : $A \to S^{-1}A$ definida como $f(a) = \overline{(as,s)}$ onde $s \in S$ com $s \neq 0$ é um homomorfismo.*

Demonstração:

1. (Soma) Queremos mostrar que$f(a+b) = f(a)+f(b)$. Note que $f(a+b) = \overline{((a+b)s,s)} = \overline{(as+bs,s)} = \overline{(ass+bss,ss)} = \overline{(as,s)} + \overline{(bs,s)} = f(a)+f(b)$.

2. (Produto) Queremos mostrar que $f(ab) = f(a)f(b)$. Perceba que $f(ab) = \overline{((ab)s,s)} = \overline{(abs,s)} = \overline{(abss,ss)} = \overline{(asbs,ss)} = \overline{(as,s)}\overline{(bs,s)} = f(a)f(b)$.

Portanto f é um homomorfismo. □

Proposição 2.39 *Seja $f : A \to S^{-1}A$ a $f(a) = \overline{(as,s)}$ onde $s \in S$ com $s \neq 0$. Então f é um homomorfismo injetor se e somente se S não possui divisores de zero e $0 \notin S$.*

Demonstração: ($\Leftarrow$) Temos que f é injetora se $f(a) = f(b)$ implica $a = b$. $f(a) = f(b)$ implica que $\overline{(as,s)} = \overline{(bs,s)}$. Logo temos que $(ass - sbs)u = 0$ para algum $u \in S$. Utilizando a comutatividade de A e colocando s em evidência temos que $(a-b)ssu = 0$ para algum $u \in S$. Note que como S não possui divisores de zero e nem o elemento nulo, logo $ssu \neq 0$ e assim $(a-b) = 0$ logo $(a = b)$, portanto f é injetora.
($\Rightarrow$) f é injetor, queremos mostrar que S não possui divisores do zero.
Tome $st = 0 \in S$, então $f(st) = f(s)f(t) = 0$ □

Proposição 2.40 *Seja $g : A \to B$ um homomorfismo de anéis tal que $g(s)$ é invertível em B para todo $s \in S$. Então existe um único homomorfismo de anel $h : S^{-1}A \to B$ tal que $g = h \circ f$.*

Demonstração: Vamos definir $h\overline{(a,s)} = g(a)g(s)^{-1}$
Primeiro, vamos verificar que h está bem definida, ou seja, não depende do representante de classe escolhido. Tome $\overline{(a,s)} = \overline{(b,t)}$ que é equivalente a $(at - sb)u = 0$ para algum $u \in S$.
Como sabemos g é um homomorfismo de A para B e $(at-sb)u \in A$, então $g((at-sb)u) = g(at-sb)g(u) = 0$. Mas $g(u)$ possui inverso, logo $g(at-sb)g(u)g(u)^{-1} = 0$ que

é igual a $g(at - sb) = g(a)g(t) - g(s)g(b) = 0$. Portanto $g(a)g(t) = g(s)g(b)$, aplicando os inversos de $g(s)$ e $g(t)$ temos que $g(s)^{-1}g(a)g(t)g(t)^{-1} = g(s)^{-1}g(s)g(b)g(t)^{-1}$ que é igual a $g(s)^{-1}g(a) = g(b)g(t)^{-1}$.

Como estamos trabalhando com anéis comutativos, podemos trocar a ordem de alguns termos, ficando com $g(a)g(s)^{-1} = g(b)g(t)^{-1}$.

Agora olhando para a definição de h, aplicada em $\overline{(a,s)}$, temos que $h\overline{(a,s)} = g(a)g(s)^{-1} = g(b)g(t)^{-1} = h\overline{(b,t)}$, ou seja, h não depende dos representantes escolhidos.

Agora vamos mostrar que h é um homomorfismo.

1. (Soma)

   Queremos mostrar que $h(\overline{(a,s)} + \overline{(b,t)}) = h\overline{(a,s)} + h\overline{(b,t)}$. Sabemos que $h(\overline{(a,s)} + \overline{(b,t)}) = h\overline{(at+sb,st)} = g(at+sb)g(st)^{-1}$. Aplicando o inverso de $g(st)$, temos que $g(at+sb)g(st)^{-1} = [g(a)g(t)+g(s)g(b)][g(s)g(t)]^{-1} = [g(a)g(t)+g(s)g(b)]g(s)^{-1}g(t)^{-1}$. Agora fazendo a distributiva, temos que $g(a)g(t)g(s)^{-1}g(t)^{-1}+g(s)g(b)g(s)^{-1}g(t)^{-1}$. Utilizando a comutatividade do anel B, segue que $g(a)g(t)g(t)^{-1}g(s)^{-1}+g(b)g(s)g(s)^{-1}g(t)^{-1} = g(a)g(s)^{-1} + g(b)g(t)^{-1} = h\overline{(a,s)} + \overline{h(b,t)}$.

2. (Produto)

   Queremos mostrar que $h(\overline{(a,s)}\,\overline{(b,t)}) = h\overline{(a,s)}h\overline{(b,t)}$. Partindo de $h(\overline{(a,s)}\,\overline{(b,t)}) = h\overline{(ab,st)} = g(ab)g(st)^{-1}$.

   Aplicando o inverso, $g(ab)g(st)^{-1} = g(ab)[g(st)]^{-1} = g(a)g(b)g(s)^{-1}g(t)^{-1}$. Novamente, utilizando a comutatividade de B, temos que $g(a)g(s)^{-1}g(b)g(t)^{-1} = h\overline{(a,s)}h\overline{(b,t)}$.

Portanto, h é homomorfismo.

Para finalizar, basta mostrar que $g = h \circ f$.

Temos que $(h \circ f)(a) = h(f(a)) = h(as,s) = g(as)g(s)^{-1} = g(a)g(s)g(s)^{-1} = g(a)\ \forall a \in A$.

□

Exemplo 2.41 Esse último exemplo, mostra porque chamamos de localização esse processo. Seja A um anel comutativo e P um ideal primo. Temos que $A \setminus P$ é um subconjunto multiplicativo. Temos que se $x, y \in A \setminus P$, temos que $xy \in A \setminus P$. Pois se $xy \in P$, teríamos que $x \in P$ ou $y \in P$, o que nos leva a absurdo.

A localização de A por $A \setminus P$ é denotada por A_P e intuitivamente, nesta localização todos elementos possuem inverso, menos os elementos que pertencem ao ideal primo. Dizemos que um anel é local, quando existe um único ideal maximal dentro deste anel e é isto que ocorre na localização por um ideal primo. Ou seja, A_P tem um único ideal maximal. Este ideal é dado por $M = \{(a,s)$ tal que $a \in P$ e $s \in A \setminus P\}$.

Primeiro temos que mostrar que M é um ideal de A_P. Tome $(a,s),(b,t) \in M$, então $\overline{(a,s)} + \overline{(b,t)} = \overline{(at + sb, st)}$. Temos que $at \in P$ já que $a \in P$ e também $sb \in P$ pois $b \in P$. Como P é ideal, logo $at + sb \in P$ e $st \in A \setminus P$, logo M é fechado para a soma.

Agora, seja $\overline{(a,s)} \in M$ e $\overline{(c,v)} \in A_P$ então temos que $\overline{(a,s)} * \overline{(c,v)} = \overline{(ac,sv)}$, temos que $ac \in P$, já que $a,c \in P$ e $sv \in A \setminus P$ já que $s,v \in A \setminus P$ e é fechado para a multiplicação, assim $\overline{(a,s)} * \overline{(c,v)} \in M$.

Agora, temos que mostrar que M é um ideal maximal e é o único. Seja I um ideal, tal que $M \subset I$. Então existe um elemento $\overline{(a,t)} \in I$ tal que $\overline{(a,t)} \notin M$, dessa forma temos que $\overline{(a,t)}$ é da forma que $a \in A \setminus P$ mas assim $\overline{(a,t)}$ passa a ser um elemento inversível e sabemos que se um ideal possui um elemento inversível, logo ele possui todo o anel, dessa forma $A = I$, portanto M é maximal.

Seja J um outro ideal maximal, temos que J não pode possuir elementos invertíveis, se não $J = A$. Então com isso temos que $J \subset M$, logo J não é maximal.

3 Módulos

3.1 Conceitos iniciais

Uma outra estrutura na qual também podemos fazer localização, é na estrutura de módulo. Diferente da estrutura de Anel, a estrutura de módulo não é vista nas matérias obrigatórias da graduação em matemática na UFABC. Por isso, vou definir alguns conceitos básicos relacionados a módulos e depois vamos utilizar isto para construir o processo de localização.

Definição 3.1 *Seja A um anel associativo, comutativo e não necessariamente com unidade. Chamamos um conjunto M não vazio de A-módulo á esquerda se M é um grupo abeliano com uma operação que vamos denotar por $+$ e se está definida uma lei de composição externa que a cada par $(\alpha, m) \in A \times M$ associa a um elemento $\alpha m \in M$ e tal que para todos $\alpha_1, \alpha_2 \in A$ e $m_1, m_2 \in M$, verifica que:*

1. $\alpha_1(\alpha_2 m_1) = (\alpha_1 \alpha_2) m_1$
2. $\alpha_1(m_1 + m_2) = \alpha_1 m_1 + \alpha_1 m_2$
3. $(\alpha_1 + \alpha_2) m_1 = \alpha_1 m_1 + \alpha_2 m_1$

Os módulos podem ser definidos para anéis com unidade, mas para isso precisamos adicionar a condição $1 m_1 = m_1$ para $m_1 \in M$. Um módulo com essa propriedade é chamado de módulo unital.

De maneira mais informal, podemos ver os módulos como uma espécie de espaço vetorial, mas invés de termos seus escalares em cima de um corpo, eles são baseados em um anel. Por causa disso, já temos alguns exemplos simples de módulos em um corpo.

Exemplo 3.2 Todo espaço vetorial sobre um corpo K é um K-módulo.

Exemplo 3.3 Se tomarmos um ideal I de um anel A comutativo, I é um A-módulo.

Exemplo 3.4 Seja G um grupo abeliano, com a seguinte operação

$$f(x) = \begin{cases} nx = x + x + ... + x & \text{se } n > 0 \\ 0 & \text{se } n = 0 \\ -nx = -x - x - ... - x & \text{se } n < 0 \end{cases} \tag{3.1}$$

onde $n \in \mathbb{Z}$ e $x \in G$, temos que G é um $\mathbb{Z}$-módulo.

Assim como para outras estruturas algébricas, podemos definir subestruturas, então dentro de um módulo, podemos ter um submódulo.

Definição 3.5 *Seja M um A-módulo. Um subconjunto $N \subseteq M$ é dito um A-submódulo de M se:*

1. *N é um subgrupo aditivo de M.*
2. *Para todo $\alpha \in A$ e $n \in N$, temos que $\alpha n \in N$.*

Como vamos fazer algumas operações com módulos, é importante saber como lidar com a multiplicação por escalar no caso do zero e com negativos. Para isso, temos a seguinte proposição.

Proposição 3.6 *Seja M, um A-módulo, então vale as seguintes propriedades:*

1. *$0m = 0$ para todo $m \in M$*
2. *$(-a)m = a(-m) = -(am)$ para todo $a \in A$ e $m \in M$*

Demonstração:

1. $0m = 0$, de fato, pois $0m = (0+0)m = 0m + 0m$ adicionando $-0m$ em ambos lados ficamos com $0m = 0$
2. $(-a)m = a(-m) = -(am)$ para $m \in M$ e $a \in A$, de fato, pois $(-a)m = (-a)m + am - (am) = (-a+a)m - (am) = -(am)$ e de forma análoga $a(-m) = a(-m) + am - (am) = a(-m+m) - (am) = -(am)$

□

Assim como podemos relacionar anéis, também queremos relacionar diferentes módulos com funções que conservem as operações dos módulos, essas relações que preservam essas operações são chamadas de homomorfismos.

Definição 3.7 *Sejam M e N dois A-módulos. Uma função $f : M \to N$ diz-se um homomorfismo de A-módulos se para todo $m_1, m_2 \in M$ e todo $a \in A$*

1. $f(m_1 + m_2) = f(m_1) + f(m_2)$
2. $f(am_1) = af(m_1)$

Em posse dos conceitos de módulos e homomorfismo de módulos, podemos entender o conceito de sequências exatas.

Definição 3.8 *Sejam F, G, H três A-módulos e $f : F \to G$, $g : G \to H$ A-morfismos. Diz-se que o diagrama:*

$$F \xrightarrow{f} G \xrightarrow{g} H$$

é uma sequência de ordem 2 em G se $im(f) \subset ker(g)$. Em particular, se $im(f) = ker(g)$ o diagrama diz-se uma sequência exata em G.

Uma consequência direta que nos ajuda a ver uma relação entre a imagem e o núcleo de uma sequência é se a composta dos homomorfismos for nulo.

Proposição 3.9 *Seja $f : F \to G$ e $g : G \to H$ A-morfismos então $im(f) \subset ker(g)$ se e somente se $g \circ f = 0$*

Demonstração: ($\Rightarrow$) Temos que se $im(f) \subset ker(g)$, então $g(f(a)) = 0$ para todo $a \in F$, mas $g(f(a)) = g \circ f(a) = 0$
($\Leftarrow$) $g \circ f = 0$, então $f(a) \in ker(g)$ para todo $a \in F$, logo $im(f) \subset ker(g)$. □

3.2 Localização em módulos

Para fazer localização em módulos sobre anéis comutativos vamos seguir um caminho parecido. Primeiro definir um conjunto, depois uma relação neste conjunto, mostrar que é de equivalência e após isso com determinadas operações concluir que o conjunto das relações de equivalência é um módulo.

Definição 3.10 *Seja A um anel associativo, comutativo e não necessariamente com unidade, S um conjunto multiplicativo de A e M é um módulo sobre A. Vamos definir uma relação em $M \times S$ como $\overline{(m_1, s_1)} \equiv \overline{(m_2, s_2)} \Leftrightarrow s(s_1 m_2 - s_2 m_1) = 0$ para algum $s \in S$.*

Proposição 3.11 *A relação definida anteriormente é uma relação de equivalência em $M \times S$.*

Demonstração: Vamos mostrar que é um relação reflexiva, simétrica e transitiva.

1. (Reflexiva) $\overline{(m_1, s_1)} \equiv \overline{(m_1, s_1)}$

   Temos que $s_1 m_1 - s_1 m_1 = 0$, logo s pode ser qualquer elemento de S.

2. (Simétrica) Supondo que $\overline{(m_1, s_1)} \equiv \overline{(m_2, s_2)}$ devemos concluir que $\overline{(m_2, s_2)} \equiv \overline{(m_1, s_1)}$.

   De $\overline{(m_1, s_1)} \equiv \overline{(m_2, s_2)}$ sabemos que existe $t \in S$ tal que $t(s_1 m_2 - s_2 m_1) = 0$ onde $s_i m_j \in M$, como M é um grupo abeliano com a soma, podemos comutar os termos e pela propriedade que vimos na proposição anterior $-s(m) = s(-m)$, logo ao somar os opostos temos $-t(s_1 m_2 - s_2 m_1) + t(s_1 m_2 - s_2 m_1) = -t(s_1 m_2 - s_2 m_1)$ que é igual a $t(-s_1 m_2 + s_2 m_1) = t(s_2 m_1 - s_1 m_2) = 0$ logo temos que $\overline{(m_2, s_2)} \equiv \overline{(m_1, s_1)}$.

3. (Transitividade) A partir de $\overline{(m_1, s_1)} \equiv \overline{(m_2, s_2)}$ e $\overline{(m_2, s_2)} \equiv \overline{(m_3, s_3)}$, devemos chegar em $\overline{(m_1, s_1)} \equiv \overline{(m_3, s_3)}$.

   De $\overline{(m_1, s_1)} \equiv \overline{(m_2, s_2)}$ temos $t_1(s_1 m_2 - s_2 m_1) = 0$ para algum $t_1 \in S$.

   De $\overline{(m_2, s_2)} \equiv \overline{(m_3, s_3)}$ temos $t_2(s_2 m_3 - s_3 m_2) = 0$ para algum $t_2 \in S$.

   Multiplicando a primeira equação por $t_2 s_3$ e a segunda por $t_1 s_1$ chegamos a

   (*) $t_2 t_1 s_3 (s_1 m_2 - s_2 m_1) = 0$

   (**) $t_1 t_2 s_1 (s_2 m_3 - s_3 m_2) = 0$

   Lembrando que os únicos elementos de M são os m_i, o resto pertence a $S \subseteq A$, que é comutativo, podemos trocar a ordem dos elementos.

   Somando as equações (*) e (**) e realizando as distributivas temos $t_2 t_1 s_3 s_1 m_2 - t_2 t_1 s_3 s_2 m_1 + t_1 t_2 s_1 s_2 m_3 - t_1 t_2 s_1 s_3 m_2 = 0$. Reorganizando os termos com a comutatividade temos $t_1 t_2 s_1 s_3 m_2 - t_1 t_2 s_2 s_3 m_1 + t_1 t_2 s_1 s_2 m_3 - t_1 t_2 s_1 s_3 m_2 = 0$.

   O primeiro e o último termo são idênticos a menos de um sinal, logo ficamos com $-t_1 t_2 s_2 s_3 m_1 + t_1 t_2 s_1 s_2 m_3 = 0$

   Como M é um grupo abeliano, podemos trocar os termos de lugar e usando a distributiva do módulo $t_1 t_2 s_2 (s_3 m_1 - s_1 m_3) = 0$. Dessa forma, como S é multiplicativo e $t_1, t_2 \in S$, logo $t_1 t_2 s_2 \in S$ e assim concluímos que $\overline{(m_1, s_1)} \equiv \overline{(m_3, s_3)}$.

Portanto, a relação definida em $M \times S$ é de equivalência.

$\square$

Denotamos por $S^{-1}M$ o conjunto das classes de equivalência da relação acima. Agora vamos mostrar que $S^{-1}M$ é um $S^{-1}A$-Módulo.

Proposição 3.12 *$S^{-1}M$ é um $S^{-1}A$-Módulo com as seguintes operações:*

1. $\overline{(m_1,s_1)}+\overline{(m_2,s_2)}=\overline{(s_1m_2+s_2m_1,s_1s_2)}$

2. $\overline{(a_1,s_3)}*\overline{(m_1,s_1)}=\overline{(a_1m_1,s_3s_1)}$

Demonstração: Devemos mostrar que $S^{-1}M$ é um grupo abeliano com a soma e temos a operação de compatibilidade entre $S^{-1}A$ e $S^{-1}M$ bem definida. Mas antes disso precisamos mostrar que a soma está bem definida, ou seja, não depende dos representantes de classe.

1. A operação de soma está bem definida. Seja $\overline{(m_1,s_1)}=\overline{(m_2,s_2)}$ e tome $\overline{(m,s)}$, queremos mostrar que $\overline{(m_1,s_1)}+\overline{(m,s)}=\overline{(m_2,s_2)}+\overline{(m,s)}$. Temos que $\overline{(m_1,s_1)}+\overline{(m,s)}=\overline{(s_1m+sm_1,s_1s)}$ e $\overline{(m_2,s_2)}+\overline{(m,s)}=\overline{(s_2m+sm_2,s_2s)}$. Da hipótese da igualdade das classes temos que $u(s_1m_2-s_2m_1)=0$ para algum $u\in S$. Queremos mostrar que $\overline{(s_1m+sm_1,s_1s)}=\overline{(s_2m+sm_2,s_2s)}$. Para que isso seja válido, devemos mostrar que $t[(s_2m+sm_2)s_1s-(s_1m+sm_1)s_2s]=0$ para algum $t\in S$. Concentrando no termo dentro das chaves, temos $s_2ms_1s+sm_2s_1s-s_1ms_2s-sm_1s_2s$. Agora multiplicando todos os termos por u ficamos com $us_2ms_1s+usm_2s_1s-us_1ms_2s-usm_1s_2s$, note que ao fazer isso podemos utilizar a igualdade da hipótese que as classes são equivalentes, dessa forma o segundo e o quarto termo da ultima expressão se anulam e o primeiro e o terceiro também, portanto tudo é igual a zero. Logo tomando $t=u$, mostramos que as classes são equivalentes. Portanto $(s_1m+sm_1,s_1s)=(s_2m+sm_2,s_2s)$.

2. $S^{-1}M$ é um grupo abeliano com a operação $\overline{(m_1,s_1)}+\overline{(m_2,s_2)}=\overline{(s_1m_2+s_2m_1,s_1s_2)}$, onde no primeiro termo temos a soma no módulo e no segundo temos o produto do anel.

   a) (Comutativa) $\overline{(m_1,s_1)}+\overline{(m_2,s_2)}=\overline{(m_2,s_2)}+\overline{(m_1,s_1)}$.

      Realizando a soma no lado direito da igualdade $\overline{(m_1,s_1)}+\overline{(m_2,s_2)}=\overline{(s_1m_2+s_2m_1,s_1s_2)}$ e para o lado esquerdo $\overline{(m_2,s_2)}+\overline{(m_1,s_1)}=\overline{(s_2m_1+s_1m_2,s_2s_1)}$.

      Como a primeira coordenada é um elemento de M, onde M é um grupo abeliano, logo temos a comutatividade na primeira coordenada e na segunda coordenada temos elementos de um anel comutativo, logo a segunda coordenada também comuta e portanto as duas equações são iguais.

   b) (Associativa) $(\overline{(m_1,s_1)}+\overline{(m_2,s_2)})+\overline{(m_3,s_3)}=\overline{(m_1,s_1)}+(\overline{(m_2,s_2)}+\overline{(m_3,s_3)})$.

      Começando pelo lado esquerdo, $(\overline{(m_1,s_1)}+\overline{(m_2,s_2)})+\overline{(m_3,s_3)}=\overline{(s_1m_2+s_2m_1,s_1s_2)}+\overline{(m_3,s_3)}=\overline{(s_3(s_1m_2+s_2m_1)+s_1s_2m_3,s_1s_2s_3)}=\overline{(s_3s_1m_2+s_3s_2m_1+s_1s_2m_3,s_1s_2s_3)}$

Agora desenvolvendo o lado direito $\overline{(m_1,s_1)}+(\overline{(m_2,s_2)}+\overline{(m_3,s_3)}) = \overline{(m_1,s_1)}+ \overline{(s_3m_2+s_2m_3,s_3s_2)} = \overline{(s_1(s_3m_2+s_2m_3)+s_3s_2m_1,s_1s_3s_2)} = \overline{(s_1s_3m_2+s_1s_2m_3+s_3a_2m_1,s_1s_3s_2)}$

Pela comutatividade de cada coordenada temos que as duas equações são iguais.

c) (Elemento neutro) Existe $\overline{(m,s)}$ um elemento tal que $\overline{(n,t)}+\overline{(m,s)} = \overline{(n,t)}$.

Temos que $\overline{(0,s)}$ é o elemento neutro, já que $\overline{(m_1,s_1)}+\overline{(0,s)} = \overline{(s_1 0+m_1s,s_1s)} = \overline{(m_1s,s_1s)}$.

Perceba que multiplicar por um elemento de S no numerador e no denominador resulta em uma classe equivalente, assim como na localização para anéis. De fato, pois $m_1ss_1-m_1s_1s=0$, pela comutatividade, logo podemos tomar qualquer $u\in S$ de tal forma que $u(m_1ss_1-m_1s_1s)=0$.

Portanto, $\overline{(m_1,s_1)}+\overline{(0,s)} = \overline{(m_1s,s_1s)} = \overline{(m_1,s_1)}$.

d) (Elemento inverso) Existe $\overline{(m,s)}$ um elemento tal que $\overline{(n,t)}+\overline{(m,s)} = \overline{(0,s)}$.

Para $\overline{(m_1,s_1)}$ o elemento neutro seria $\overline{(-m_1,s_1)}$. Ou seja, devemos mostrar que $\overline{(m_1,s_1)}+\overline{(-m_1,s_1)}$ tem que ser da mesma classe que $\overline{(0,s)}$.

$\overline{(m_1,s_1)}+\overline{(-m_1,s_1)} = \overline{(s_1m_1-s_1m_1,s_1s_1)} = \overline{(0,s_1s_1)}$

Portanto, $\overline{(m_1,s_1)}+\overline{(-m_1,s_1)} = \overline{(0,s_1s_1)} = \overline{(0,s)}$

Logo $S^{-1}M$ é um grupo abeliano.

3. Operação compatibilidade entre $S^{-1}A$ e $S^{-1}M$ $\overline{(a_1,s_3)}*\overline{(m_1,s_1)} = \overline{(a_1m_1,s_3s_1)}$, onde $a_1\in A, m_1\in M$ e $s_1,s_3\in S$.

Como $a_1m_1\in M$, por M ser um A-modulo. Como $s_3\in S\subseteq A$, logo $s_3s_1\in A$, portanto está bem definida a operação.

□

Como foi dito anteriormente, um homomorfismo é uma função que preserva a estrutura de A-módulo, como a localização de um módulo também é um módulo, naturalmente isto deve acontecer também para um homomorfismo na localização. Porém, além disso vamos mostrar que um homomorfismo entre módulos induz um homomorfismo na localização desses módulos.

Proposição 3.13 *Seja $u: M\to N$ um A–homomorfismo. Então nós temos que $S^{-1}A$-modulo homomorfismo $S^{-1}u: S^{-1}M\to S^{-1}N$ que manda $\overline{(m,s)}$ para $\overline{(u(m),s)}$.*

Demonstração: Para mostrar que $S^{-1}u$ é um homomorfismo, devemos mostrar que

1. $S^{-1}u\overline{(m,s)} + S^{-1}u\overline{(n,t)} = S^{-1}u(\overline{(m,s)} + \overline{(n,t)})$

   $S^{-1}u\overline{(m,s)}+S^{-1}u\overline{(n,t)} = \overline{(u(m),s)}+\overline{(u(n),t)} = \overline{(tu(m)+su(n),st)} = \overline{(u(tm)+u(sn),st)} = \overline{(u(tm+sn),st)} = S^{-1}u\overline{(tm+sn,st)} = S^{-1}u(\overline{(m,s)} + \overline{(n,t)})$

2. $S^{-1}u(\overline{(a,r)} * \overline{(m,s)}) = \overline{(a,r)} * S^{-1}u\overline{(m,s)}$, onde $\overline{(a,r)} \in S^{-1}A$

   $S^{-1}u(\overline{(a,r)} * \overline{(m,s)}) = S^{-1}u\overline{(am,rs)} = \overline{(u(am),rs)} = \overline{(au(m),rs)} = \overline{(a,r)} * \overline{(u(m),s)} = \overline{(a,r)} * S^{-1}u(\overline{(m,s)})$

□

Esse homomorfismo induzido é importante pois a partir dele, conseguimos mostrar que a localização é uma operação exata. Isso quer dizer que se aplicar a localização numa sequência exata, a sequência resultante também é exata.

Proposição 3.14 *A operação S^{-1} é exata, isto é, se $M' \xrightarrow{f} M \xrightarrow{g} M''$ é exata em M, então $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ é exata em $S^{-1}M$.*

Demonstração: Sabemos que a sequência $M' \xrightarrow{f} M \xrightarrow{g} M''$ é exata, portanto temos que $ker(g) = im(f)$, ou seja, todo elemento da imagem de f pertence ao núcleo de g, assim temos que $g(f(x)) = 0$ para todo x, portanto $g \circ f = 0$.

Lembrando que se tivermos o homomorfismo $f : A \to B$, então o homomorfismo $S^{-1}f : S^{-1}A \to S^{-1}B$ é dado por $S^{-1}f(a,s) = \overline{(f(a),s)}$.

Para mostrar que a sequência $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ é exata, devemos mostrar que $ker(S^{-1}g) = im(S^{-1}f)$.

Primeiro vamos mostrar que $im(S^{-1}f) \subset ker(S^{-1}g)$.

Tome $(a,s) \in im(S^{-1}f)$, então sabemos que $S^{-1}f\overline{(a_f,s)} = (f(a_f),s) = \overline{(a,s)}$ para $a_f \in M'$. Mas como $g \circ f = 0$, logo $S^{-1}g\overline{(a,s)} = S^{-1}g\overline{(f(a_s),s)} = \overline{(g(f(a_s),s))} = \overline{(0,s)}$, portanto $\overline{(a,s)} \in ker(S^{-1}g)$.

Agora vamos mostrar que $ker(S^{-1}g) \subset im(S^{-1}f)$. Tome $(a,s) \in ker(S^{-1}g)$, logo $S^{-1}g\overline{(a,s)} = \overline{(g(a),s)} = \overline{(0,s)}$. Mas, como $ker(g) = im(f)$, logo existe $b \in M'$ tal que $f(b) = g(a)$ e dessa forma $\overline{(g(a),s)} = \overline{(f(b),s)} \in im(S^{-1}f)$

□

4 Localização em anéis não comutativos

O nosso objetivo nesta seção é fazer a mesma construção que fizemos da localização em anéis comutativos, mas agora para anéis que não são necessariamente comutativos, isto é, anéis cujo a multiplicação não é obrigatoriamente comutativa. Embora isso seja possível, não é exatamente análogo, já que a comutatividade é uma propriedade muito forte.

Como perdemos a comutatividade da multiplicação, vamos precisar de outras condições para poder manipular os elementos do anel para construir a localização. Essas condições são chamadas de condições de Ore e vamos definir a seguir.

Definição 4.1 (Condições de Ore) *Seja A um anel e $S \subset A$ um subconjunto multiplicativo de A. Se as seguintes condições:*

1. *(Condição de Ore a esquerda) Para todo $a \in A$ e $s \in S$, temos que $Sa \cap As \neq \emptyset$.*
2. *(Reversibilidade a esquerda) Para todos $a, b \in A$ e $s \in S$ tal que $as = bs$ então existe $t \in S$ tal que $ta = tb$.*

São satisfeitas, então dizemos que S é chamado de um conjunto de Ore à esquerda de A. De maneira análoga, podemos definir o conjunto de Ore à direita. Neste texto vamos fazer quase tudo a esquerda.

Observação 4.2 *Como este caso não é comutativo, faz diferença multiplicar pela direita ou pela esquerda e por conta disso, um conjunto pode ser de Ore a esquerda e não ser a direita, veremos isso no exemplo 4.13.*

Com essas condições, seguiremos como no caso comutativo, definindo uma relação de equivalência entre os elementos do anel e do subconjunto multiplicativo. Em sequência descreveremos as operações de soma e multiplicação para termos um anel.

Precisamos entender quando duas frações serão equivalentes neste caso não comutativo. De alguma forma, igualaremos os denominadores e a ferramenta que teremos a disposição para isso, vem das condições de Ore.

Proposição 4.3 *Seja A um anel e S um conjunto de Ore à esquerda, então a relação em $S \times A$, definida de forma que $\overline{(s,a)} \equiv \overline{(t,b)}$ se e somente se $cs = ut$ e $ca = ub$ para algum $c \in A$ e $u \in S$ é de equivalência. Uma outra forma de ver a relação é $\overline{(s,a)} \equiv \overline{(t,b)}$ se e somente se existe $c \in A$ e $u \in S$ tal que $u(t,b) = c(s,a)$ coordenada a coordenada.*

Demonstração: Devemos mostrar que é uma relação reflexiva, simétrica e transitiva.

1. (Reflexiva)

   Um elemento deve estar relacionado consigo mesmo, ou seja, $\overline{(s,a)} \equiv \overline{(s,a)}$. Para isso, basta tomar $t \in S$.

   É claro que $ts = ts$ e $ta = ta$.

2. (Simétrica)

   Temos que mostrar que se $\overline{(s,a)} \equiv \overline{(t,b)}$ então $\overline{(t,b)} \equiv \overline{(s,a)}$.

   Como $\overline{(s,a)} \equiv \overline{(t,b)}$ sabemos que existe $c \in A$ e $r \in S$ tal que $r(t,b) = c(s,a)$.

   Utilizando a propriedade de Ore, temos que dados $x \in S$ e $y \in A$ existe s_1 e a_1 tal que $s_1 y = a_1 x$. Tomando $x = t$ e $y = s$ temos que $s_1 s = a_1 t$.

   Utilizando novamente a propriedade de Ore, mas agora em $x = rt$ e $y = a_1 t$, temos $s_2 a_1 t = a_2 rt$ para $s_2 \in S$ e $a_2 \in A$.

   Resumindo, temos as seguintes igualdades:

   a) $rt = cs$

   b) $rb = ca$

   c) $s_1 s = a_1 t$

   d) $s_2 a_1 t = a_2 rt$

   Multiplicando (a) por a_2 temos $a_2 cs = a_2 rt$, mas note que por (d) temos que $a_2 rt = s_2 a_1 t$. E que ao multiplicar (c) por s_2 temos $s_2 a_1 t = s_2 s_1 s$. Portanto temos que $a_2 cs = s_2 s_1 s$. Pela reversibilidade à esquerda, temos que existe $u \in S$ tal que $u a_2 c = u s_2 s_1$.

   Definindo $d = u a_2 r \in A$ e $z = u s_2 s_1$ sabemos que

$zs = us_2s_1s$, utilizando a igualdade (c) obtemos $us_2s_1s = us_2a_1t$ e agora notando que por (d) temos $us_2a_1t = ua_2rt = dt$.

$za = us_2s_1a = ua_2ca = ua_2rb = db$.

Ou seja, mostramos que $z(s,a) = d(t,b)$ que é $\overline{(t,b)} \equiv \overline{(s,a)}$.

3. (Transitiva)

   Temos que mostrar que se $\overline{(s,a)} \equiv \overline{(t,b)}$ e $\overline{(t,b)} \equiv \overline{(u,c)}$, então $\overline{(s,a)} \equiv \overline{(u,c)}$.

   Por conta disso, já temos que existem $d,e \in A$ e $v,w \in S$ tal que $v(t,b) = d(s,a)$ e $w(u,c) = e(t,b)$.

   Utilizando a condição de Ore em $x = v \in S$ e $y = e \in A$, temos que existem $a_1 \in A$ e $s_1 \in S$ tal que $s_1e = a_1v$.

   Chamando $f = a_1d \in A$ e $z = s_1w \in S$, temos que

   $zu = s_1wu = s_1et = a_1vt = a_1ds = fs$

   $zc = s_1wc = s_1eb = a_1vb = a_1da = fa$

   Assim $z(u,c) = f(s,a)$ logo $\overline{(s,a)} \equiv \overline{(u,c)}$.

□

Com isso, sabemos que temos uma relação de equivalência com essas frações onde os denominadores estão em S, mas ainda não temos ideia de como vamos operar esses elementos. As usuais soma e multiplicação de frações que utilizamos no caso comutativo não funciona neste cenário, porém vamos entender a definição do caso não comutativo e perceber que devido a falta de comutatividade e as condições de Ore, ela é natural, apesar de que em um primeiro momento os elementos da definição pareçam arbitrários, veremos que existem um paralelo com a soma e multiplicação de frações comum.

Definição 4.4 *Seja A um conjunto e S um subconjunto de Ore a esquerda de A, definimos a soma em $S \times A$ da seguinte forma: $\overline{(s_1,a_1)} + \overline{(s_2,a_2)} = \overline{(ts_1, ta_1 + ba_2)}$ onde $bs_2 = ts_1$ $b \in A$ e $t \in S$.*

Como dito antes, a definição parece meio arbitrária por depender dos elementos que surgem da condição de Ore, mas vamos ver que a soma não depende desses elementos. Outra forma de enxergar essa soma é a seguinte. Temos as frações $\overline{(s_1,a_1)}$ e $\overline{(s_2,a_2)}$, podemos deixar o denominador igual usando as condições de Ore, sabemos que $bs_2 = ts_1$ então vamos multiplicar a segunda fração por b e a primeira por

t, ficamos com $\overline{(ss_1, sa_1)}$ e $\overline{(bs_2, ba_2)}$. Agora as duas frações estão sob o mesmo denominador, então vamos somar ficando com $\overline{(ss_1, sa_1 + ba_2)}$. Note que escolhemos o denominador como ss_1 pois $ss_1 \in S$ e dessa forma o nosso elemento está bem definido.

Definição 4.5 *Seja A um conjunto e S um subconjunto de Ore a esquerda de de A, definimos a multiplicação na relação de equivalência em $S \times A$ da seguinte forma: $\overline{(s_1, a_1)} * \overline{(s_2, a_2)} = \overline{(us_1, ca_2)}$ onde $cs_2 = ua_1$ $c \in A$ e $u \in S$.*

Agora aqui a lógica é um pouco diferente, não vamos igualar os denominadores mas vamos igualar o denominador de uma fração com o numerador de outra de forma que podemos simplificar a fração resultante da multiplicação das duas. Tomando frações $\overline{(s_1, a_1)}$ e $\overline{(s_2, a_2)}$ ao multiplicar a primeira por u e a segunda por c ficando com $\overline{(us_1, ua_1)}$ e $\overline{(cs_2, ca_2)}$, mas ao multiplicar podemos simplificar as frações ficando só com $\overline{(us_1, ca_2)}$.

Perceba que ao tentar dar uma explicação mais natural, acabei utilizando uma propriedade que ainda não provamos, mas faz sentido que é a seguinte, ao multiplicar o denominador e o numerador por um mesmo elemento do anel, resulta numa classe equivalente. A demonstração dessa propriedade é vista na proposição 4.7.

Agora vamos mostrar que a soma e a multiplicação, não depende dos elementos que são originados da condição de Ore.

Proposição 4.6 *Sejam $\overline{(s_1, a_1)}$ e $\overline{(s_2, a_2)}$ tal que $bs_2 = ts_1$ e $cs_2 = us_1$ para $b, c \in A$ e $t, u \in S$. Então $\overline{(ts_1, ta_1 + ba_2)} \equiv \overline{(us_1, ua_1 + ca_2)}$.*

Demonstração: Utilizando a condição de Ore em t e u, temos que existem $w \in S$ e $f \in A$, tal que $wu = ft$.

Sabemos que $cs_2 = us_1$, multiplicando por w a esquerda temos que $wcs_2 = wus_1 = fts_1 = fbs_2$. Pela reversibilidade a esquerda, temos que existe $z \in S$ tal que $zwc = zfb$.

Tomando $y = zw \in S$ e $x = zf \in A$, temos que

$yus_1 = zwus_1 = zfts_1 = xfs_1$

$y(ua_1 + ca_2) = yua_1 + yca_2 = zwua_1 + zwca_2 = zfta_1 + zfba_2 = xta_1 + xba_2 = x(ta_1 + ba_2)$.

Logo $\overline{(ts_1, ta_1 + ba_2)} \equiv \overline{(us_1, ua_1 + ca_2)}$. □

Uma propriedade que é bastante intuitiva pensando em frações usuais é a de multiplicar por um mesmo elemento, o denominador e o numerador e a fração resultante é equivalente a fração original. Isto, também é válido aqui com a restrição de que o denominador tem que ser um elemento de S ao final da multiplicação, o que é natural, já que o denominador só é definido para elementos que pertencem a S.

Proposição 4.7 *Seja $s \in S$ e $b \in A$ tal que $bs \in S$, então temos que $(s,a) \equiv (bs,ba)$.*

Demonstração: Queremos mostrar que $\overline{(s,a)} \equiv \overline{(bs,ba)}$, mas isto implica dizer que existe $u \in S$ e $c \in A$ tal que $u(bs,ba) = c(s,a)$ coordenada a coordenada.

Tomando $u = bs \in S$ e $c = bsb \in A$ temos o seguinte

$ubs = bsbs = cs$

$uba = bsba = ca$

Portanto a equivalência é válida. □

Sempre que trabalhamos com relações de equivalências e definimos operações, precisamos mostrar que essas operações estão bem definidas, ou seja, não dependem do representa escolhido da classe. Essa demonstração é relativamente simples no caso comutativo, porém no cenário atual veremos como a situação complica.

Proposição 4.8 *A soma não depende dos representantes de classe.*

Demonstração: Queremos mostrar que independente do elemento escolhido, a soma está bem definida. Porém, isso é complexo de fazer como fizemos no caso comutativo, para este caso, vamos dividir em duas etapas.

A primeira etapa é mostrar que a soma não depende da classe do primeiro elemento, isto é, dados $\overline{(s_1,a_1)} \equiv \overline{(s_2,a_2)}$ então $\overline{(s_1,a_1)} + \overline{(t,b)} \equiv \overline{(s_2,a_2)} + \overline{(t,b)}$.

Como $\overline{(s_1,a_1)} \equiv \overline{(s_2,a_2)}$, logo existem $c \in A$ e $v \in S$ tal que $c(s_2,a_2) = v(s_1,a_1)$, que nos leva as seguintes equações:

(I) $cs_2 = vs_1$

(II) $ca_2 = va_1$

Utilizando a condição de Ore em s_2 e t, temos que existem $w \in S$ e $d \in A$ tal que $ws_2 = dt$. Ou seja, estamos deixando as frações $\overline{(s_2,a_2)}$ e $\overline{(t,b)}$ sob o mesmo denominador.

Agora aplicando a condição de Ore em $c \in A$ e $w \in S$ temos que existe $f \in A$ e $y \in S$ tal que $yc = fw$.

Portanto temos mais duas igualdades.

(III) $ws_2 = dt$

(IV) $yc = fw$

Partindo da igualdade (III) multiplicada por f a esquerda, temos o seguinte:

(V) $fdt = fws_2 = ycs_2 = yvs_1$

Agora partindo de (IV) multiplicada por a_2 a direita, temos o seguinte:

(VI) $fwa_2 = yca_2 = yva_1$

Pela igualdade (V) , temos que podemos fazer a soma $\overline{(s_1, a_1)} + \overline{(t, b)}$ com os elementos $fd \in A$ e $yv \in S$. Então, pela definição da soma temos:
$\overline{(s_1, a_1)} + \overline{(t, b)} = \overline{(yvs_1, yva_1 + fdb)}$ por (VI) temos que isto é igual $\overline{(yvs_1, fwa_2 + fdb)} = \overline{(ycs_2, fwa_2 + fdb)}$ por (V) temos que $\overline{(ycs_2, fwa_2 + fdb)} = \overline{(fws_2, fwa_2 + fdb)}$. Como $fws_2 = yvs_1$, onde todos os elementos do lado direito da igualdade estão em S, logo $fws_2 \in S$, portanto podemos utilizar a propriedade de multiplicar a fração no numerador e no denominador, de tal forma que $\overline{(fws_2, fwa_2 + fdb)} = \overline{(ws_2, wa_2 + db)} = \overline{(s_2, a_2)} + \overline{(t, b)}$,desde $ws_2 = dt$ mas isto é garantido pela equação (III).

Para a segunda etapa temos que mostrar que a soma não depende da classe do segundo elemento, isto é, dados $\overline{(s_1, a_1)} \equiv \overline{(s_2, a_2)}$ então $\overline{(t, b)} + \overline{(s_1, a_1)} \equiv \overline{(t, b)} + \overline{(s_2, a_2)}$. A demonstração é bem parecida com o que fizemos acima, tomando apenas cuidado com a ordem dos elementos, por isso iremos omitir essa parte.

Logo, a soma não depende dos representantes de classe.

□

Proposição 4.9 *A multiplicação não depende dos representantes de classe.*

Demonstração: Aqui vamos seguir a mesma tática aplicada a soma, primeiro vamos mostrar que a multiplicação não depende do representante do primeiro fator e depois vamos mostrar que não depende do representante do segundo fator.

Para o primeiro fator

Sejam $\overline{(s_1, a_1)} \equiv \overline{(s_2, a_2)}$, queremos mostrar que $\overline{(s_1, a_1)} * \overline{(t, b)} \equiv \overline{(s_2, a_2)} * \overline{(t, b)}$.

Como $\overline{(s_1, a_1)} \equiv \overline{(s_2, a_2)}$, logo existe $v \in S$ e $c \in A$ tal que $v(s_1, a_1) = c(s_2, a_2)$.

Utilizando a condição de Ore em a_2 e t, existem $f \in A$ e $w \in S$ tal que $ft = wa_2$.

Agora aplicando a condição de Ore em $c \in A$ e $w \in S$, temos que existe $g \in A$ e $z \in S$ tal que $zc = gw$.

Dessa forma, partindo de $ft = wa_2$ temos que $gft = gwa_2 = zca_2 = zva_1$ com $gf \in A$ e $zv \in S$, logo podemos fazer a multiplicação com esse elementos.

$\overline{(s_1, a_1)} * \overline{(t, b)} = \overline{(zvs_1, gft)} = \overline{(zcs_2, gft)} = \overline{(gws_2, gft)}$. Note que $gws_2 = zvs_1 \in S$, logo podemos aplicar a propriedade tirando g da fração $\overline{(gws_2, gft)} = \overline{(ws_2, ft)}$ que é igual a $\overline{(s_2, a_2)} * \overline{(t, b)}$ caso $ft = wa_2$, mas isso é garantido pela primeira vez que utilizamos a condição de Ore.

O segundo fator é feito de maneira análoga.

Portanto a multiplicação também está bem definida.

□

Agora que temos o conjunto com as suas operações bem definidas, podemos mostrar que temos um anel. No entanto, antes de prosseguir, demonstraremos uma proposição que diz que podemos colocar um número finito de frações sob o mesmo denominador. Comparando com o caso comutativo dos inteiros é uma propriedade intuitiva e isto também é válido para este cenário.

Proposição 4.10 *Seja A um anel e S um conjunto de Ore de A, então dadas n classes de equivalência da relação estabelecida em $S \times A$, temos que é possível deixar todas as classes com o mesmo elemento em S. Ou seja, dados $\overline{(s_1, a_1)}, ..., \overline{(s_n, a_n)}$ existe $u \in S$ tal que $\overline{(u, b_{a_1})}, ..., \overline{(u, b_{a_n})}$, onde $\overline{(u, b_{a_i})} = \overline{(s_i, a_i)}$ para $i \in \{1, .., n\}$ e $n >= 2$*

Demonstração: Para provar esta proposição vamos seguir por indução, onde o caso base é feito quando temos duas frações.

Dados $\overline{(s_1, a_1)}$ e $\overline{(s_2, a_2)}$ queremos deixar as duas classes com o mesmo denominador. Nós temos que pela condição de Ore, existem $t \in S$ e $c \in A$ tal que $ts_1 = cs_2$. Assim, temos que $\overline{(s_1, a_1)} = \overline{(ts_1, ta_1)}$ e $\overline{(s_2, a_2)} = \overline{(cs_2, ca_2)} = \overline{(ts_1, ca_2)}$. Portanto, o caso base é válido.

Agora supondo que é possível deixar n elementos sob o mesmo denominador. Nós temos que $\overline{(s_1, a_1)}, ..., \overline{(s_n, a_n)}$ tal que existe $u \in S$ tal que $\overline{(u, b_{a_1})}, ..., \overline{(u, b_{a_n})}$ onde $\overline{(u, b_{a_i})} = \overline{(s_i, a_i)}$ para $i \in \{1, .., n\}$ e $n >= 2$.

Seja $\overline{(s_{n+1}, a_{n+1})}$ o enésimo primeiro elemento, podemos aplicar a condição de Ore entre u e s_{n+1}, assim existe $v \in S$ e $d \in A$ tal que $vu = ds_{n+1}$. Dessa forma temos que $\overline{(s_{n+1}, a_{n+1})} = \overline{(ds_{n+1}, da_{n+1})} = \overline{vu, a_{n+1})}$ e $\overline{(vu, vb_{ai})} = \overline{(vs_i, va_i)} = \overline{(s_i, a_i)}$,assim concluímos que todos os n+1 elementos podem ser expressos sob o mesmo denominador. □

Essa proposição nos ajudará a provar que as classes de equivalência de SxA pela relação que visto a pouco é um anel.

Proposição 4.11 *Seja A um anel e S um conjunto de Ore, então temos que o conjunto das classes de equivalência de $S \times A$ definidos pela relação, junto com a soma e a multiplicação como definimos é um anel não comutativo com unidade.*

Demonstração:

1. (Associatividade da soma) $(\overline{(s_1,a_1)}+\overline{(s_2,a_2)})+\overline{(s_3,a_3)} = \overline{(s_1,a_1)}+(\overline{(s_2,a_2)}+\overline{(s_3,a_3)})$. Podemos supor sem perda de generalidade que existe $u \in S$ e $b_{a_i} \in A$ tal que $\overline{(u,b_{a_i})} = \overline{(s_i,b_{a_i})}$ para $i = 1,2,3$. Ou seja, existem elementos equivalentes que deixam as 3 classes originais sob o mesmo denominador.

   Assim, nós temos que $(\overline{(s_1,a_1)} + \overline{(s_2,a_2)}) + \overline{(s_3,a_3)} = (\overline{(u,b_{a_1})} + \overline{(u,b_{a_2})}) + \overline{(u,b_{a_3})} = \overline{(u,b_{a_1} + b_{a_2})} + \overline{(u,b_{a_3})} = \overline{(u,b_{a_1} + b_{a_2} + b_{a_3})} = \overline{(u,b_{a_1})} + (\overline{(u,b_{a_2})} + \overline{(u,b_{a_3})}) = \overline{(s_1,a_1)} + (\overline{(s_2,a_2)} + \overline{(s_3,a_3)})$

2. (Elemento neutro da soma) Existe um elemento $\overline{(t,b)}$ tal que $\overline{(s,a)}+\overline{(t,b)} = \overline{(s,a)}$.

   Seja $\overline{(t,b)} = \overline{(t,0)}$ para $t \in S$, temos que $\overline{(s,a)} + \overline{(t,0)} = \overline{(us,ua + c0)} = \overline{(us,ua)} = \overline{(s,a)}$, onde $ct = us$ que é a condição de Ore aplicada em s e t.

3. (Elemento inverso da soma) Existe um elemento $\overline{(t,b)}$ tal que $\overline{(s,a)}+\overline{(t,b)} = \overline{(s,0)}$.

   Para isso, basta tomar $\overline{(t,b)} = \overline{(s,-a)}$. Assim $\overline{(s,a)}+\overline{(t,b)} = \overline{(s,a)}+\overline{(s,-a)} = \overline{(s,a-a)} = \overline{(s,0)}$.

4. (Comutatividade da soma) $\overline{(s_1,a_1)} + \overline{(s_2,a_2)} = \overline{(s_2,a_2)} + \overline{(s_1,a_1)}$

   Novamente usando a proposição 4.10 temos sem perda de generalidade que existe $u \in S$ e $b_{ai} \in A$ tal que $\overline{(u,b_{a_i})} = \overline{(s_i,b_{a_i})}$ para $i = 1,2$. Assim, $\overline{(s_1,a_1)} + \overline{(s_2,a_2)} = \overline{(u,b_{a_1})}+\overline{(u,b_{a_2})} = \overline{(u,b_{a_1} + b_{a_2})} = \overline{(u,b_{a_2} + b_{a_1})} = \overline{(u,b_{a_2})}+\overline{(u,b_{a_1})} = \overline{(s_2,a_2)}+\overline{(s_1,a_1)}$.

5. (Associatividade da multiplicação) $[\overline{(s_1,a_1)} * \overline{(s_2,a_2)}] * \overline{(s_3,a_3)} = \overline{(s_1,a_1)} * [\overline{(s_2,a_2)} * \overline{(s_3,a_3)}]$

   Começando pelo lado esquerdo, temos que $\overline{(s_1,a_1)} * \overline{(s_2,a_2)} = \overline{(s_4s_1,a_4a_2)}$ onde $s_4a_1 = a_4s_2$ que é a condição de Ore aplicada ao elementos a_1 e s_2. Desta forma, temos então que $[\overline{(s_1,a_1)} * \overline{(s_2,a_2)}] * \overline{(s_3,a_3)} = \overline{(s_4s_1,a_4a_2)} * \overline{(s_3,a_3)} = \overline{(s_5s_4s_1,a_5a_3)}$, onde $s_5a_4a_2 = a_5s_3$.

   Pelo lado direito temos $\overline{(s_2,a_2)} * \overline{(s_3,a_3)} = \overline{(s_6s_2,a_6a_3)}$ para $s_6a_a = a_6a_3$. Portanto $\overline{(s_1,a_1)} * [\overline{(s_2,a_2)} * \overline{(s_3,a_3)}] = \overline{(s_1,a_1)} * \overline{(s_6s_2,a_6a_3)} = \overline{(s_7s_1,a_7s_6s_2)}$ onde $s_7a_1 = a_7s_6s_2$.

   Até aqui temos quatro equações:

   (I) $s_4a_1 = a_4s_2$

   (II) $s_5a_4a_2 = a_5s_3$

   (III) $s_6a_2 = a_6a_3$

   (IV) $s_7a_1 = a_7s_6s_2$

Aplicando a condição de Ore em s_7 e s_5s_4 temos que existe $s \in S$ e $a \in A$ tal que $ss_7 = rs_5s_4$, que é a nossa quinta equação.

(V) $ss_7 = rs_5s_4$

Começando a partir da equação (IV) multiplicada por s à esquerda, temos que $sa_7s_6s_2 = ss_7a_1$ mas sabendo por (V) que $ss_7 = as_5s_4$ assim $ss_7a_1 = rs_5s_4a_1$ e agora utilizando a equação (I) $rs_5s_4a_1 = as_5a_4s_2$. De maneira completa, temos $sa_7s_6s_2 = ss_7a_1 = as_5s_4a_1 = as_5a_4s_2$. Mas sabemos que pela reversibilidade á esquerda que existe $t_1 \in S$ tal que $t_1sa_7s_6 = t_1as_5a_4$ que é a nossa sexta equação.

(VI) $t_1sa_7s_6 = t_1as_5a_4$

A partir da equação (III) multiplicada por t_1sr_7 a esquerda, temos que $t_1sr_7a_6a_3 = t_1sa_7s_6a_2$, utilizando a equação (VI) $t_1sa_7s_6a_2 = t_1as_5a_4a_2$ e por (II) $t_1as_5a_4a_2 = t_1aa_5s_3$, de maneira completa temos $t_1sr_7a_6a_3 = t_1sa_7s_6a_2 = t_1as_5a_4a_2 = t_1aa_5s_3$. Novamente, usando a reversibilidade a esquerda, temos que $t_2t_1sr_7a_6 = t_2t_1aa_5$ para $t_2 \in S$.

(VII) $t_2t_1sr_7a_6 = t_2t_1aa_5$

Lembrando que queremos mostrar que $\overline{(s_5s_4s_1, a_5a_3)} = \overline{(s_7s_1, a_7s_6s_2)}$.Isso é válido, para comprovar tome $d = t_2t_1a \in A$ e $v = t_2t_1s \in S$.

Assim $d(s_5s_4s_1, a_5a_3) = v(s_7s_1, a_7s_6s_2)$. De fato, para a primeira coordenada $ds_5s_4s_1 = t_2t_1as_5s_4s_1$ que por (V) é $t_2t_1as_5s_4s_1 = t_2t_1ss_7s_1 = vs_7s_1$. Na segunda, $da_5a_3 = t_2t_1aa_5a_3$ que por (VI) é $t_2t_1sa_7a_6a_3 = va_7a_6a_3$.

6. (Elemento neutro da multiplicação) $\overline{(s,a)} * \overline{(t,b)} = \overline{(s,a)}$.

   Tomando $\overline{(t,b)} = \overline{(t,t)}$, onde $t \in S$. Pela condição de Ore em t e a temos que existe $u \in S$ e $c \in A$ tal que $ua = ct$, assim $\overline{(s,a)} * \overline{(t,t)} = \overline{(us,ct)} = \overline{(us,ca)} = \overline{(s,a)}$.

7. (Distributividade à esquerda) $\overline{(s_1,a_1)} * [\overline{(s_2,a_2)} + \overline{(s_3,a_3)}] = \overline{(s_1,a_1)} * \overline{(s_2,a_2)} + \overline{(s_1,a_1)} * \overline{(s_3,a_3)}$

   Para facilitar, vamos deixar os elementos da soma sob a mesmo denominador. Sem perda de generalidade sabemos que existe $u \in S$ e $b_{ai} \in A$ tal que $\overline{(u,b_{ai})} = \overline{(s_i,b_{ai})}$ para $i = 2,3$. Assim, $\overline{(s_1,a_1)} * [\overline{(s_2,a_2)} + \overline{(s_3,a_3)}] = \overline{(s_1,a_1)} * [\overline{(u,b_{a2})} + \overline{(u,b_{a3})}] = \overline{(s_1,a_1)} * \overline{(u,b_{a2}+b_{a3})}$. Realizando a multiplicação temos que $\overline{(s_1,a_1)} * \overline{(u,b_{a2}+b_{a3})} = \overline{(vs_1,c[b_{a2}+b_{a3}])}$ para $vu = ca_1$. Assim, $\overline{(vs_1,c[b_{a2}+b_{a3}])} = \overline{(vs_1,cb_{a2})} + \overline{(vs_1,cb_{a3})}$. Porém, note que $\overline{(vs_1,cb_{a2})} = \overline{(s_1,a_1)} * \overline{(u,b_{a2})}$ e $\overline{(vs_1,cb_{a3})} = \overline{(s_1,a_1)} * \overline{(u,b_{a3})}$. Portanto, $\overline{(s_1,a_1)} * [\overline{(s_2,a_2)} + \overline{(s_3,a_3)}] = \overline{(s_1,a_1)} * \overline{(u,b_{a2})} + \overline{(s_1,a_1)} * \overline{(u,b_{a3})} = \overline{(s_1,a_1)} * \overline{(s_2,a_2)} + \overline{(s_1,a_1)} * \overline{(s_3,a_3)}$.

8. (Distributividade à direita) $[\overline{(s_1,a_1)}+\overline{(s_2,a_2)}]*\overline{(s_3,a_3)} = \overline{(s_1,a_1)}*\overline{(s_3,a_3)}+\overline{(s_2,a_2)}*\overline{(s_3,a_3)}$

   Primeiro, vamos deixar os elementos $\overline{(s_1,a_1)}$ e $\overline{(s_2,a_2)}$ sob o mesmo denominador.

   Começando pelo lado direito temos $\overline{(s_1,a_1)}*\overline{(s_3,a_3)}+\overline{(s_2,a_2)}*\overline{(s_3,a_3)} = \overline{(u,b_{a1})}*\overline{(s_3,a_3)}+\overline{(u,b_{a2})}*\overline{(s_3,a_3)}$. Realizando as somas temos que $\overline{(u,b_{a1})}*\overline{(s_3,a_3)}+\overline{(u,b_{a2})}*\overline{(s_3,a_3)} = \overline{(tu,ca_3)}+\overline{(vu,da_3)}$, onde $cr_3 = tb_{a1}$ e $dr_3 = vb_{a2}$, para $c,d \in A$ e $t,v \in S$.

   Aplicando a condição de Ore, para t e v temos que existe $a \in A$ e $x \in S$ tal que $at = xv$.

   Portanto $\overline{(tu,ca_3)}+\overline{(vu,da_3)} = \overline{(atu,aca_3)}+\overline{(xvu,xda_3)}$ que estão no mesmo denominador já que $at = xv$, assim $\overline{(atu,aca_3+xda_3)}$, colocando a_3 em evidência, temos $\overline{(atu,[ac+xd]a_3)}$.

   Analisando só o termo $[ac+xd]a_3 = aca_3+xda_3 = atb_{a1}+xvb_{a2} = xv(b_{a1}+b_{a2})$

   Voltando para o lado esquerdo, temos que $[\overline{(s_1,a_1)}+\overline{(s_2,a_2)}]*\overline{(s_3,a_3)} = [\overline{(u,b_{a1})}+\overline{(u,b_{a2})}]*\overline{(s_3,a_3)} = \overline{(u,b_{a1}+b_{a2})}*\overline{(s_3,a_3)}$.

   Tomando $f = ac+xd$ e $y = xv$, assim $\overline{(u,b_{a1}+b_{a2})}*\overline{(s_3,a_3)} = \overline{(tu,[ac+xd]a_3)}$ que o mesmo elemento do lado direito.

$\square$

Após nossos cálculos, mostramos que $S \times A$ é um anel não necessariamente comutativo, onde S é um conjunto de Ore a esquerda de A.

Apesar de não abordarmos o caso comutativo explicitamente com o noção de conjuntos de Ore, podemos ver que ele é generalizado pelo caso não comutativo. De maneira mais concreta, podemos ver que em um anel comutativo, todo conjunto multiplicativo é um conjunto de Ore a direita e a esquerda. Temos se A é um anel comutativo e S um conjunto multiplicativo de A, então para $a \in A$ e $s \in S$, temos que $as = sa$, portanto é válida a condição de Ore. Seja $b,c \in A$ e $t \in S$ tal que $bs = cs$ temos que é válido $sb = sc$ concluímos então que a reversibilidade a esquerda ou a direita é respeitada.

Seguiremos com alguns exemplos de conjuntos de Ore em anéis não comutativos. Os dois primeiros exemplos são adaptações do que podemos ver no capitulo 10 da refenrencia [HL19].

Exemplo 4.12 O conjunto dos Quartênios, denotado por $\mathbb{H}$, cujo seus elementos são da forma $u+xi+yj+zk$ com $u,x,y,z \in \mathbb{R}$ e $i^2 = j^2 = k^2 = 1$ é um anel não comutativo. Veremos que $S = \mathbb{Z} \setminus \{0\}$ satisfaz a condição de Ore a esquerda dos Quartênios.

Devemos mostrar que dados a, s nos quarternios existem t, b tal que $at = sb$.

Sabemos que $a = u_1 + x_1 i y_1 j + z_1 k$, $b = u_2 + x_2 i y_2 j + z_2 k$, $t = u_3 + x_3 i y_3 j + z_3 k$ e $s = u_4 + x_4 i y_4 j + z_4 k$.

Como $t, s \in S$ sabemos que $x_3 = x_4 = y_3 = y_4 = z_3 = z_4 = 0$.

Devemos ter $at = sb$, assim $at = (u_1 + x_1 i y_1 j + z_1 k)(u_3)$ e $sb = (u_4)(u_2 + x_2 i y_2 j + z_2 k)$.

Como as coordenadas devem ser iguais, temos 4 equações, onde os termos em negritos são oriundos de a e s, ou seja, são valores fixados.

1. $\boldsymbol{u_1} u_3 = \boldsymbol{u_4} u_2$
2. $\boldsymbol{x_1} u_3 = \boldsymbol{u_4} x_2$
3. $\boldsymbol{y_1} u_3 = \boldsymbol{u_4} y_2$
4. $\boldsymbol{z_1} u_3 = \boldsymbol{u_4} z_2$

O nosso objetivo é determinar os valores dos termos que não estão em negrito de forma que o sistema de equações acima tenha solução. Nós temos liberdade, para manipular os termos que não estão em negrito, já queremos garantir a existência desses elementos.

Podemos tomar $u_3 = 1$, assim $u_2 = \frac{u_1}{u_4}$, $y_2 = \frac{y_1}{u_4}$, $x_2 = \frac{x_1}{u_4}$ e $z_2 = \frac{z_1}{u_4}$.

Onde $u_3 \neq 0$ e $u_4 \neq 0$, pois $s = u_4$ e $t = u_3$, onde $s, t \in S$.

Note que com isso temos que $t = 1$ e $b = \frac{u_1}{u_4} + \frac{x_1}{u_4} i + \frac{y_1}{u_4} j + \frac{z_1}{u_4} k$, ou seja, podemos tomar $t = 1$, enquanto o b é determinado pelo coeficientes que vem de a, s, portanto S é um conjuto de Ore dos Quartênios.

Agora iremos abordar um exemplo em outro anel não comutativo relevante, que é formado pelas matrizes.

Exemplo 4.13 Seja $A = \{\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}\}$, onde $a_{11} \in K$, e $a_{12}, a_{22} \in K[x]$, onde K é um corpo e S um subconjunto de A, tal que $S = \{\begin{pmatrix} c & f \\ 0 & g \end{pmatrix}$ com $c \in K$ e $f, g \in K[x]$ tal que $c(x)g(x) \neq 0\}$. Queremos mostrar que S é um conjunto de Ore a direita de A.

Temos que mostrar que dados $a \in A$ e $s \in S$ existem $b \in A$ e $t \in S$ tal que $ta = bs$.

Dessa forma, temos $a = \begin{pmatrix} \alpha & p(x) \\ 0 & q(x) \end{pmatrix}$, $b = \begin{pmatrix} \theta & r(x) \\ 0 & s(x) \end{pmatrix}$, $s = \begin{pmatrix} \beta & f(x) \\ 0 & g(x) \end{pmatrix}$ e $t = \begin{pmatrix} \gamma & h(x) \\ 0 & j(x) \end{pmatrix}$, onde $\beta g(x) \neq 0$ e $\gamma j(x) \neq 0$.

Realizando as multiplicações das matrizes,

$at = \begin{pmatrix} \alpha\gamma & \alpha h(x) + p(x)j(x) \\ 0 & q(x)j(x) \end{pmatrix}$ e $sb = \begin{pmatrix} \beta\theta & \beta r(x) + f(x)s(x) \\ 0 & g(x)s(x) \end{pmatrix}$

Resultando em 3 equações, onde os termos oriundos das matrizes a e s são dados e os elementos que vem de t e b devem ser descobertos. Para separar e facilitar a leitura, os valores fixados estão em negrito.

1. $\boldsymbol{\alpha}\gamma = \boldsymbol{\beta}\theta$

2. $\boldsymbol{\alpha} h(x) + \boldsymbol{p(x)} j(x) = \boldsymbol{\beta} r(x) + \boldsymbol{f(x)} s(x)$

3. $\boldsymbol{q(x)} j(x) = \boldsymbol{g(x)} s(x)$

Para os coeficientes que devem ser descobertos, podemos atribuir valores, desde que respeite as regras estabelecidas pelos elementos, pois queremos encontrar os elementos que façam valer a igualdade da condição de Ore.

Para resolver a primeira igualdade, podemos tomar $\gamma = 1$, temos então que $\theta = \frac{\alpha}{\beta}$.

Para a segunda igualdade temos, podemos definir $h(x) = 0$, dessa forma ficamos com $\boldsymbol{p(x)} j(x) = \boldsymbol{\beta} r(x) + \boldsymbol{f(x)} s(x)$, isolando o $r(x)$ ficamos com $r(x) = \frac{\boldsymbol{p(x)} j(x) - \boldsymbol{f(x)} s(x)}{\boldsymbol{\beta}}$.

Para terminamos, falta definir $j(x)$ e $s(x)$. Utilizando a terceira equação temos que podemos definir $s(x) = q(x)$ e $j(x) = g(x)$. Dessa forma, podemos concluir que tal conjunto é um conjunto de Ore a direita.

Porém, esse mesmo conjunto não pode ser um conjunto de Ore a esquerda. Tome $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ e $s = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, para que a propriedade de Ore valha para esses elementos, deveríamos ter $t = \begin{pmatrix} c & f(x) \\ 0 & g(x) \end{pmatrix}$, com $cg(x) \neq 0$ e $b = \begin{pmatrix} d & p(x) \\ 0 & q(x) \end{pmatrix}$ tal que $ta = bs$.

Mas, note que $ta = \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}$ e $bs = \begin{pmatrix} d & p(x)x \\ 0 & q(x)x \end{pmatrix}$. Para isto ter solução, precisamos que

1. $0 = d$

2. $c = p(x)x$

3. $0 = q(x)x$

Então teríamos, $q(x) = 0$ e $p(x) = \frac{c}{x}$. Porém, $p(x) \notin K[x]$, logo não é possível termos tais coeficientes.

Exemplo 4.14 Trabalharemos com a primeira álgebra de Weyl que é o anel de operadores diferenciais com coeficientes em K, um corpo de característica zero, onde os elementos são da forma $f_m(x)\delta_x^m + f_{m-1}(x)\delta_x^{m-1} + ... + f_1(x)\delta_x + f_0(x)$. Esse exemplo é uma adaptação do que podemos ver no exemplo 2.7 de [LT42].

A primeira álgebra de Weyl, também pode ser definida da seguinte forma, o quociente da álgebra livre gerada por x, δ e o ideal gerado por $\delta x - x\delta = 1$. Ou seja, $D = K < x, \delta/\delta x = x\delta + 1 >$.

Um elemento importante desde anel é $\theta = x\delta$, que também é conhecido como elemento de Euler, vamos utiliza-lo durante todo o exemplo. Uma definição que também iremos utilizar é a definição de grau induzida naturalmente por $\mathbb{Z}$, fixando $deg(x) = -1$ e $deg(\delta) = 1$.

Nosso objetivo é mostrar que o conjunto $\Theta_z = [\theta + z]$ é um conjunto de Ore a esquerda de D. Onde $[M] = \{\prod_{i=1}^{n} m_i$ onde $n \in \mathbb{N}, m_i \in M\}$, ou seja, Θ_z é formado pelas potências finitas de $(\theta + Z)$ e $z \in Z(D)$, tal que $Z(D)$ é o centro de D, ou seja, z comuta com todos os elementos de D.

Para mostrar isso, vamos precisar da seguinte propriedade. Para $n, m \in \mathbb{N}$, $(\theta + z)^m x^n = x^n(\theta + z + n)^m$ e $\delta^n(\theta + z)^m = (\theta + z + n)^m \delta^n$. Ou seja, queremos mostrar como se comporta x e δ ao serem permutados com elementos de Θ_z.

Vamos trabalhar com a primeira identidade $(\theta + z)^m x^n = x^n(\theta + z + n)^m$, fazendo a sua prova por indução.

Trata-se de uma indução dupla, para $n, m \in \ltimes$ tal que $n, m >= 0$. Para provar, vamos seguir os seguintes passos:

1. (Base) Devemos mostrar que a proposição é válida para $m = 1$ e $n = 1$. Após isso, devemos mostrar que é válida para qualquer $n >= 1$ desde que $m = 1$. Para simplificar, irei chamar a identidade de $P(m, n)$ e ir atribuindo os valores conforme necessidade.

   a) $P(1, 1)$ é válido.

      Devemos mostrar que $(\theta + z)x = x(\theta + z + 1)$.

      Partindo de $(\theta + z)x$ e lembrando que $\delta x - x\delta = 1$ e $\theta = x\delta$, temos que $(\theta + z)x = \theta x + zx = x\delta x + zx = x(1 + x\delta) + xz = x(x\delta + z + 1) = x(\theta + z + 1)$.

   b) $P(1, n) \rightarrow P(1, n + 1)$.

      Este caso, nada mais é do que uma indução em n, com $m = 1$. Note que o caso base dessa indução seria $P(1, 1)$ que já foi provado. Então, supondo que $P(1, n)$ é válido, devemos mostrar que $P(1, n + 1)$ também é.

      Partindo de $(\theta + z)x^n$, podemos multiplicar por x a direita $(\theta + z)x^n + 1 = (\theta + z)x^n x$, onde podemos aplicar a nossa hipótese para n, ficando com

$(\theta + z)x^n x = x^n(\theta + z + n)x = x^n(x\delta x + zx + nx) = x^n(x(1 + x\delta) + xz + xn) = x^n(x(1 + \theta + z + n)) = x^{n+1}(\theta + z + (n + 1))$

2. (Passo indutivo) Agora, utilizando que $P(m,n)$ é válido para todo $n >= 1$ devemos mostrar que $P(m+1,n+1)$.

   a) $P(m+1,1)$ é válido.

      Ou seja, devemos mostrar que $(\theta + z)^{m+1}x = x(\theta + z + 1)^{m+1}$.

      Sabemos por hipótese, que é válido para m qualquer e $n = 1$. Logo $(\theta + z)^m x = x(\theta + z + 1)^m$ é válido por hipótese de indução. Partindo do termo a esquerda e multiplicando por $(\theta + z)$ temos que $(\theta + z)^{m+1}x = (\theta + z)(\theta + z)^m x = (\theta + z)x(\theta + z + 1)^m$, mas note que $(\theta + z)x = x(\theta + z + 1)$, vimos isso em $P(1,1)$. Assim, $(\theta + z)^{m+1}x = x(\theta + z + 1)^{m+1}$.

   b) $P(m+1,n) \rightarrow P(m+1,n+1)$.

      Supondo que $(\theta + z)^{m+1}x^n = x^n(\theta + z + n)^{m+1}$ é válido, devemos chegar que a implicação é válida para n+1.

      $(\theta + z)^{m+1}x^{n+1} = (\theta + z)^{m+1}x^n x$, usando a hipótese anterior, temos que $(\theta + z)^{m+1}x^n x = x^n(\theta + z + n)^{m+1}x$. Porém, perceba que $(\theta + z + n)^{m+1}x = x(\theta + z + n + 1)^{m+1}$, como vimos em $P(m+1,1)$, assim $(\theta + z)^{m+1}x^n = x^n(\theta + z + n)^{m+1}$.

A segunda propriedade, $\delta^n(\theta + z)^m = (\theta + z + n)^m\delta^n$, tem uma demonstração bem parecida, por isso iremos omitir seus detalhes.

Para prosseguirmos, queremos mostrar que para qualquer elemento homogêneo de grau k, teremos um comportamento parecido com as identidades que acabamos de analisar. Seja $d \in D$ homogêneo de grau k, então $(\theta + z + k)r = r(\theta + z)$, onde $k \in \mathbb{N}$ e $z \in Z(D)$.

Como d é homogêneo, então pode ser escrito como $d = \sum_{(a,b)} c_{a,b}x^a\delta^b$, onde $c_{a,b} \in K$ e sabemos que $a - b = k$.

Portanto, $(\theta+z+k)r = \sum_{(a,b)} c_{a,b}(\theta+z+k)x^a\delta^b = \sum_{(a,b)} c_{a,b}x^a(\theta+z+k+a)\delta^b = \sum_{(a,b)} c_{a,b}x^a\delta^b(\theta + z + k + a - b) = \sum_{(a,b)} c_{a,b}x^a\delta^b(\theta + z)$.

Por fim, seja $d \in D$, este elemento pode ser decomposto em uma soma, onde cada um dos termos é homogeneo, então $d = \sum r_{ki}$ a decomposição de um elemento qualquer em partes homogeneas de grau ki.

Se tormarmos $t = \prod_{i=1}^{n}(\theta + z + k_i) \in \Theta_z$ e $a = \sum_{i=1}^{n}(\prod_{j=i}^{n}(\theta + z + j_j)r_{ki})$, chegamos em $a(\theta + z) = tr$ que é a condição de Ore a esquerda.

Portanto, Θ_z é um conjunto de Ore a esquerda de Θ_z.

Referências Bibliográficas

[AM69] Atiyah M. F.; MacDonald M. G., Introduction to Commutative Algebra . Addison-wesley publishing company, 1969.

[FJ03] Fraleigh, J. B., A first course in abstract algebra. Person , 2003.

[Her75] Herstein I. N., Topics in algebra. University of Chicago, 1975.

[HL19] Hoffmann, J.; Levandovskyy, V.2019. Left saturation closure for Ore localizations. Disponível em https://doi.org/10.48550/arXiv.1903.03172

[SZ05] Skoda Z. 2005. Noncommutative localization in noncommutative geometry. Disponível em https://doi.org/10.48550/arXiv.math/0403276

[BT20] Bowles, T. B. 2020. Universal Localizations of Certain Noncommutative Rings. Disponível em https://digitalcommons.usu.edu/etd/7881

[LT42] Lam, T. Y.Lectures on modules and rings. Springer, 1942.