Estudos TCC

November 7, 2022

1 Anéis

Definição 1.1 (Anel). *Um anel R é um conjunto com duas operações $+$ e $*$ tal que dados $x, y, z \in R$ temos:*

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

Observação 1.2. *A definição de anel varia de autor para autor, alguns consideram anéis comutativos com unidade, outro já não consideram a existência do neutro multiplicativo. Também existem anéis sem associatividade, então podemos ter um anel sem nenhuma propriedade sobre a multiplicação*

Quando a multiplicação também é comutativa, isto é $a * b = b * a$ chamamos de anel comutativo.

Exemplo 1.3. *Temos que $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ com as operações usuais de soma e produto são anéis.*

Proposição 1.4. *Seja R um anel não trivial, se $x \in R$ então $x * 0 = 0$*

Proof. Temos que

$$x * 0 = x * (0 + 0) = x * 0 + x * 0$$

mas como existe o oposto de $x * 0$ podemos somar

$$x * 0 - x * 0 = x * 0 + x * 0 - x * 0$$

logo

$$0 = x * 0$$

$\square$

Temos que caso $1 = 0$ o anel é trivial. Já que $x = x * 1 = x * 0 = 0$.

Definição 1.5 (Subaneis)**.** *Seja $S \subseteq R$, onde R é um anel, dizemos que S é um subanel de R se dados $x, y \in S$ temos:*

1. $x + y \in S$
2. *Se $x \in S$ então $-x \in S$*
3. $0 \in S$
4. $xy \in S$

Definição 1.6 (Homomorfismo)**.** *Uma função $f : A \to B$ é dita homomorfismo de anéis se:*

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

Definição 1.7 (Ideais(maximal e primo))**.** *Colocar a definição de ideal, ideal maximal, ideal primo*

Definição 1.8 (Divisores de zero)**.** *Colocar a definição de divisores de zero*

Definição 1.9 (Anéis quociente)**.** *Fazer a construção de quociente de anéis*

1.1 Corpo de fração

1.2 Localização em anéis comutativos

Vamos seguir a demonstração a partir de um anel A sem unidade, na referência [1] temos a demonstração feita em anel com unidade.

Definição 1.10. *Um subconjunto S de um anel A é dito um conjunto multiplicativo se $1 \in S$ e $x \cdot y \in S$ para todo $x, y \in S$.*

Mas como estamos partindo de um anel sem unidade, não faz sentido querer que $1 \in S$, então para o nosso caso vamos considerar que exista $a_s \neq 0$ tal que $a \in S$.

Agora que já temos todas as definições necessárias para iniciar a construção, vamos começar.

Definição 1.11. *Seja A um anel e S um conjunto multiplicativo de A. Vamos definir uma relação em $A \times S$ como*

$$(a, s) \equiv (b, t) \Leftrightarrow (at - sb)u = 0$$

para algum $u \in S$.

Esta relação, é uma relação de equivalência.

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

Reflexiva $(a,s) \equiv (a,s)$, de fato, pois $as = sa$, já que estamos trabalhando com um anel comutativo, portanto $as - sa = 0$ e assim $(as - sa)a_s = 0$.

Simétrica Temos que $(a,s) \equiv (b,t)$ nos leva a $(at - sb)u = 0$. Note que podemos somar o inverso aditivo do elemento $(at-sb)u$ em ambos lados da igualdade que nos leva a

$$(at - sb)u - ((at - sb)u) = -(at - sb)u$$

$$0 = -(at - sb)u$$

$$0 = (-at + sb)u$$

Como o anel A é comutativo

$$0 = (sb - at)u$$

Usando a comutatividade novamente para reorganizar os produtos

$$0 = (bs - ta)u$$

que é equivalente a

$$(b,t) \equiv (a,s)$$

Transitividade Seja $(a,s) \equiv (b,t)$ e $(b,t) \equiv (c,r)$, devemos chegar em $(a,s) \equiv (c,r)$.

De $(a,s) \equiv (b,t)$ temos $(at - sb)u_1 = 0$ para algum $u_1 \in S$.

De $(b,t) \equiv (c,r)$ temos $(br - tc)u_2 = 0$ para algum $u_2 \in S$.

Multiplicando a primeira equação por ru_2 e a segunda por su_1 chegamos a

$$ru_2(at - sb)u_1 = 0$$

$$su_1(br - tc)u_2 = 0$$

Utilizando a comutatividade para agrupar os termos em u.

$$r(at - sb)u_1u_2 = 0$$

$$s(br - tc)u_1u_2 = 0$$

Aplicando a propriedade distributiva

$$(rat - rsb)u_1u_2 = 0$$

$$(sbr - stc)u_1u_2 = 0$$

Novamente utilizando a comutatividade para ajustar os termos

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

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

Em (**) temos que ao aplicar a distributiva

$$sbru_1u_2 = sctu_1u_2$$

Mas note que temos em (*) ao aplicar a distributiva

$$artu_1u_2 = sbru_1u_2(*)$$

Então temos que

$$artu_1u_2 = sctu_1u_2$$
$$artu_1u_2 - sctu_1u_2 =$$
$$(art - sct)u_1u_2$$
$$(ar - sc)tu_1u_2$$

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

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

□

Notação 1.12. *Denotamos por $S^{-1}A$ o conjunto das classes de equivalência. Denotamos por $\frac{a}{s}$ a classe de equivalência de (a, s).*

Vamos agora definir as operações de soma e multiplicação em $S^{-1}A$.

Definição 1.13. *A soma em $S^{-1}A$ é definida por $(a, s) + (b, t) = (at + sb, st)$*

Definição 1.14. *A multiplicação em $S^{-1}A$ é definida por $(a, s) * (b, t) = (ab, st)$*

Vamos verificar se as operações estão bem definidas, ou seja, se as operações acima não dependem do representante da classe.

Proposição 1.15. *As operações de soma e multiplicação em $S^{-1}A$ não dependem dos representantes da classe.*

Proof. Seja $(a, s) = (a', s')$, vamos fazer as operações com esses dois representantes e ver que a operação não depende da escolha. Sabemos que $(as' - sa')u = 0$ para algum u.

Soma Vamos tomar as somas de (a, s) e (a', s') com (b, t).

$$(a, s) + (b, t) = (at + sb, st)$$
$$(a', s') + (b, t) = (a't + s'b, s't)$$

Quero mostrar que $(a, s) + (b, t) = (a', s') + (b, t)$, para isso vamos fazer

$$(at + sb, st) = (a't + s'b, s't)$$

$$(at + sb)s't - st(a't + s'b)$$

$$ats't + sbs't - sta't - sts'b$$

Usando a comutatividade

$$atts' + bsts' - stta' - bsts' = atts' - stta' = (as' - sa')tt$$

Multiplicando por u

$$(as' - sa')ttu$$

Mas como

$$(as' - sa')u = 0$$

Logo

$$(as' - sa')ttu = 0$$

Portanto

$$(a, s) + (b, t) = (a', s') + (b, t)$$

Produto Vamos tomar os produtos de (a, s) e (a', s') com (b, t).

$$(a, s) * (b, t) = (ab, st)$$
$$(a', s') * (b, t) = (a'b, s't)$$

Quero mostrar que

$$(ab, st) = (a'b, s't)$$

Então tome

$$abs't - sta'b$$

Utilizando a comutatividade para reorganizar

$$as'bt - sa'bt$$

Colocando em evidência

$$(as' - sa')bt$$

Multiplicando por u temos

$$(as' - sa')ubt$$

Mas sabemos que

$$(as' - sa')u = 0$$

Portanto

$$(as' - sa')ubt = 0$$

Logo

$$(ab, st) = (a'b, s't)$$

□

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

Agora vamos ver alguns exemplos de anéis que podemos fazer essa construção. Mas antes vamos o que é um domínio de integridade, que é um tipo especial de anel.

Definição 1.16. *Um domínio de integridade (ou simplesmente domínio) é um anel comutativo unitário A tal que se $a, b \in A$ e $a \cdot b = 0$ então $a = 0$ ou $b = 0$.*

Exemplo 1.17. *O caso quando A é um domínio de integridade é um caso particular do anel de frações, isso acontece pois $S = A - \{0\}$ é um conjunto multiplicativo.*

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

Proposição 1.18. *Seja A um domínio de integridade, então o conjunto $C = A - \{0\}$ é um conjunto multiplicativo.*

Proof. Como $1 \in A$, logo $1 \in C$. Temos também que para xy com $x, y \in C$ $xy \neq 0$, pois A é um domínio de integridade e x e y não podem ser nulos. Portanto C é fechado na multiplicação, logo é um conjunto multiplicativo. □

Exemplo 1.19. *Tomando como nosso anel os inteiros ($\mathbb{Z}$) e o nosso conjunto multiplicativo como $S = \mathbb{Z} - 0$, 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.*

Exemplo 1.20. *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 $n \geq 0$.*

Exemplo 1.21. *Temos que $S^{-1}A$ será o anel zero se tivemos que $0 \in S$. De fato, pois se $0 \in S$ podemos tomar u da relação de equivalência como 0, dessa forma $(ad - bc)0 = 0$ para todo $\frac{a}{b}$ e $\frac{c}{d}$, dessa forma todos os elementos são equivalentes entre si, em particular serão equivalente ao elemento $\frac{0}{0}$, ou seja, $S^{-1}A$ pode ser representado por um único elemento, o $\frac{0}{0}$*

Observação 1.22. *Um importante homomorfismo é* $f(a) = (a, 1)$ *para* $f : A \to s^{-1}A$. *Mas vamos definir esse homomorfismo para um anel* A *sem unidade, então queremos algo como* $f(a) = (as, s)$ *onde* $s \in S$ *com* $s \neq 0$. *Na referência [1] temos o resultado para um anel com unidade.*

Definição 1.23. *Seja* A *um anel associativo, comutativo mas não necessariamente com unidade e* S *um conjunto multiplicativo não vazio, então definimos o seguinte homomorfismo* $f : A \to S^{-1}A$ *como* $f(a) = (as, s)$ *onde* $s \in S$ *com* $s \neq 0$.

Proposição 1.24. $f : A \to S^{-1}A$ *como* $f(a) = (as, s)$ *onde* $s \in S$ *com* $s \neq 0$ *é um homomorfismo.*

Proof. Soma Queremos mostrar que $f(a + b) = f(a) + f(b)$

$$f(a + b) = ((a + b)s, s) = (as + bs, s)$$

$$f(a) + f(b) = (as, s) + (bs, s) = (ass + bss, ss)$$

Como estamos trabalhando com classes de equivalência, devo mostrar que as classes $(as + bs, s)$ e $(ass + bss, ss)$ são equivalentes. Note que

$$(as + bs, s) = (ass + bss, ss)$$

Se e somente se

$$[(as + bs)ss - (ass + bss)s]u \text{ para algum } u \in S$$

Mas note que

$$[(as + bs)ss - (ass + bss)s] = asss + bsss - asss - bsss = 0$$

Portanto, podemos escolher qualquer $u \in S$, em particular vamos tomar s

$$[(as + bs)ss - (ass + bss)s]s = 0$$

Portanto

$$(as + bs, s) = (ass + bss, ss)$$

Produto Queremos mostrar que $f(ab) = f(a)f(b)$

$$f(ab) = ((ab)s, s) = (abs, s)$$

$$f(a)f(b) = (as, s)(bs, s) = (asbs, ss)$$

Aplicando uma estratégia semelhante ao que fizemos para a soma, queremos mostrar que $(abs, s) = (asbs, ss)$. Para isto ocorrer, devemos ter

$$(absss - asbss)u \text{ para algum } u \in S$$

Mas note que pela comutatividade temos que

$$absss - asbss = absss - absss = 0$$

Logo podemos tomar $u = s$ e assim $(abs, s) = (asbs, ss)$.

Portanto f é um homomorfismo. □

Proposição 1.25. *Seja $f : A \to S^{-1}A$ como $f(a) = (as, s)$ onde $s \in S$ com $s \neq 0$ um homomorfismo de anéis. f é um homomorfismo injetor se e somente se S não possui divisores de zero e $0 \notin S$.*

Proof. $\Leftarrow$ Temos que f é injetora se $f(a) = f(b)$ então $a = b$.

$$f(a) = f(b) = (as, s) = (bs, s)$$

Logo temos que

$$(ass - sbs)u = 0 \text{ para algum } u \in S$$

Utilizando a comutatividade de A e colocando s em evidência temos que

$$(a - b)ssu = 0 \text{ para algum } u \in S$$

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.
$\Rightarrow$ Fazer a volta $\square$

Proposição 1.26. *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 $g = h \circ f$*

Proof. Vamos definir $h(a, s) = g(a)g(s)^{-1}$

Primeiro, vamos verificar que h está bem definida, ou seja, não depende do representante da classe escolhido.

$$(a, s) = (b, t)$$

Que significa

$$(at - sb)u = 0 \text{ para algum } u \in S$$

Mas como sabemos g é um homomorfismo de A para B e todos elementos estão em A, logo podemos aplicar g na igualdade.

$$g((at - sb)u) = g(0)$$
$$g(at - sb)g(u) = 0$$
$$g(at - sb)g(u)g(u)^{-1} = 0g(u)^{-1}$$
$$g(at - sb) = 0$$
$$g(a)g(t) - g(s)g(b) = 0$$
$$g(a)g(t) = g(s)g(b)$$
$$g(s)^{-1}g(a)g(t)g(t)^{-1} = g(s)^{-1}g(s)g(b)g(t)^{-1}$$
$$g(s)^{-1}g(a) = g(b)g(t)^{-1}$$

Como estamos trabalhando com anéis comutativos

$$h(a, s) = g(a)g(s)^{-1} = g(b)g(t)^{-1} = h(b, t)$$

Ou seja, h não depende dos representantes escolhidos.

Agora vamos mostrar que h é um homomorfismo.

soma Queremos mostrar que $h((a,s)+(b,t)) = h(a,s)+h(b,t)$ Sabemos que

$$h((a,s)+(b,t)) = h(at+sb, st) = g(at+sb)g(st)^{-1}$$

$$g(at+sb)g(st)^{-1} = [g(a)g(t)+g(s)g(b)][g(s)g(t)]^{-1}$$
$$[g(a)g(t)+g(s)g(b)]g(s)^{-1}g(t)^{-1}$$
$$g(a)g(t)g(s)^{-1}g(t)^{-1} + g(s)g(b)g(s)^{-1}g(t)^{-1}$$

Utilizando a comutatividade do anel B

$$g(a)g(t)g(t)^{-1}g(s)^{-1} + g(b)g(s)g(s)^{-1}g(t)^{-1}$$

$$g(a)g(s)^{-1} + g(b)g(t)^{-1} = h(a,s)+h(b,t)$$

produto Queremos mostrar que $h((a,s)(b,t)) = h(a,s)h(b,t)$ Sabemos que

$$h((a,s)(b,t)) = h(ab, st)$$

$$h(ab,st) = g(ab)g(st)^{-1}$$
$$g(ab)g(st)^{-1} = g(ab)[g(st)]^{-1}$$
$$g(a)g(b)g(s)^{-1}g(t)^{-1}$$

Como o anel B é comutativo, temos que

$$g(a)g(s)^{-1}g(b)g(t)^{-1} = h(a,s)h(b,t)$$

Portanto, temos que h é homomorfismo.
Agora, basta mostrar que $g = h \circ f$.
Temos que

$$h \circ f = h(f(a)) = h(as, s)$$
$$h(as,s) = g(as)g(s)^{-1} = g(a)g(s)g(s)^{-1} = g(a)$$

Portanto a composição se verifica.

□

2 Módulo

Definição 2.1. *Seja A um anel associativo, comutativo e não necessariamente com unidade. Chamamos um conjunto M não vazio de A-Modulo 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. $(\alpha_1+\alpha_2)m_1 = \alpha_1 m_1 + \alpha_2 m_1$

Observação 2.2. *Os módulos podem ser definidos para anéis com unidades, mas para isso precisamos adicionar a condição $1m_1 = m_1$ para $m_1 \in M$. Um módulo com essa propriedade é chamado de módulo unital.*

Exemplo 2.3. *Todo espaço vetorial sobre um corpo K é um K-Módulo.*

Exemplo 2.4. *Se tomarmos um ideal I de um anel A, I é um A-Modulo*

Exemplo 2.5. *Se tomarmos um grupo abeliano g, com a seguinte operação $nx = x + x + ... + x$ onde $n \in \mathbb{Z}$ e $x \in g$, temos que g é um $\mathbb{Z}$-Modulo.*

Definição 2.6. *Seja M um A-modulo. 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 $an \in N$*

Proposição 2.7. *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 $m \in M$*

Proof.
1. $0m = 0$, de fato, pois $0m_1 = (0 + 0)m_1 = 0m_1 + 0m_1$ adicionando $-0m_1$ em ambos lados ficamos com $0m_1 = 0$
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 $a(-m) = a(-m) + am - (am) = a(-m + m) - (am) = -(am)$

□

Proposição 2.8. *Um subconjunto n não vazio de m é um submódulo se e somente se*

1. *Para todo $n_1, n_2 \in n$ temos que $n_1 + n_2 \in n$*
2. *Para todo $a \in A$ e $n \in N$ temos que $an \in N$*

Proof. Para a ida, temos que se N é um submódulo, então n é um subgrupo aditivo de M, logo para $n_1, n_2 \in n$ temos que $n_1 + n_2$. A segunda condição da proposição é exatamente igual a segunda condição de submódulo. Para a volta, temos que $n_1, n_2 \in n$ temos que $n_1 + n_2 \in n$, isto é, n é fechado na soma. Sabemos pelo segundo item que a multiplicação de um elemento do subconjunto com um elemento do anel deve estar no subconjunto, em particular $0n_1 = 0 \in n$(pelo item i da proposição anterior), então o elemento neutro está em n. Finalmente, sabemos que para todo n_1 implica em $-n_1 \in n$, pois $(-1)(n_1) = -n_1$, então $-n_1 \in n$(pelo item ii da proposição anterior). Logo n é subgrupo aditivo. E a segunda condição é idêntica. □

Definição 2.9. *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. *$f(am_1) = af(m_1)$*

Definição 2.10. *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.

Proposição 2.11. *Seja $f : F \to G$ e $g : G \to H$ A-morfismos então $im(f) \subset ker(g)$ se e somente se $g \circ f = 0$*

Proof. $\Rightarrow$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 $im(f) \subset ker(g)$. □

2.1 Localização em módulos

Para fazer localização em módulos sobre anéis comutativos vamos seguir um caminho parecido.

Definição 2.12. *Seja A um anel associativo e comutativo, S um conjunto multiplicativo de A e M é um módulo sobre A. Vamos definir uma relação em $M \times S$ como*

$$(m_1, s_1) \equiv (m_2, s_2) \Leftrightarrow s(s_1 m_2 - s_2 m_1) = 0$$

para algum $s \in S$.

Proposição 2.13. *A relação definida anteriormente é uma relação de equivalência em $M \times S$.*

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

Reflexiva $(m_1, s_1) \equiv (m_1, s_1)$, temos que $s_1 m_1 - s_1 m_1 = 0$, logo s pode ser qualquer elemento de S.

Simétrica Temos que $(m_1, s_1) \equiv (m_2, s_2)$ nos leva a $t(s_1 m_2 - s_2 m_1) = 0$ onde $s_i m_j \in M$, como M é um grupo abeliano com a soma, temos que podemos os termos de lugar e pela propriedade que vimos na proposição anterior $-s(m) = s(-m)$, logo ao somar os opostos temos

$$-t(s_1 m_2 - s_2 m_1) + t(s_1 m_2 - s_2 m_1) = -t(s_1 m_2 - s_2 m_1)$$

$$t(-s_1 m_2 + s_2 m_1) = t(s_2 m_1 - s_1 m_2) = 0$$

logo temos que $(m_2, s_2) \equiv (m_1, s_1)$.

Transitividade Seja $(m_1, s_1) \equiv (m_2, s_2)$ e $(m_2, s_2) \equiv (m_3, s_3)$, devemos chegar em $(m_1, s_1) \equiv (m_3, s_3)$. De $(m_1, s_1) \equiv (m_2, s_2)$ temos $t_1(s_1 m_2 - s_2 m_1) = 0$ para algum $t_1 \in S$.

De $(m_2, s_2) \equiv (m_3, s_3)$ 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

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

$$t_1t_2s_1(s_2m_3 - s_3m_2) = 0 \; (**)$$

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

Somando as equações (*) e (**) e realizando as distributivas temos

$$t_2t_1s_3s_1m_2 - t_2t_1s_3s_2m_1 + t_1t_2s_1s_2m_3 - t_1t_2s_1s_3m_2 = 0$$

Reorganizando os termos com a comutatividade temos

$$t_1t_2s_1s_3m_2 - t_1t_2s_2s_3m_1 + t_1t_2s_1s_2m_3 - t_1t_2s_1s_3m_2 = 0$$

O primeiro e o último termo são idênticos a menos de um sinal, logo ficamos com

$$-t_1t_2s_2s_3m_1 + t_1t_2s_1s_2m_3 = 0$$

Como M é um grupo abeliano, podemos trocar os termos de lugar e usando a distributiva do módulo temos

$$t_1t_2s_2(s_3m_1 - s_1m_3)$$

Como S é multiplicativo e $t_1, t_2 \in S$, logo $t_1t_2s_2 \in S$ e portanto $(m_1, s_1) \equiv (m_3, s_3)$.

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

□

Notação 2.14. *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 2.15. *$S^{-1}M$ é um $S^{-1}A$-Módulo com as operações*

$$(m_1, s_1) + (m_2, s_2) = (s_1m_2 + s_2m_1, s_1s_2)$$

e

$$(a_1, s_3) * (m_1, s_1) = (a_1m_1, s_3s_1)$$

.

Proof. Devo 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 $(m_1, s_1) = (m_2, s_2)$ e tome (m, s), queremos mostrar que $(m_1, s_1) + (m_s) = (m_2, s_2) + (m, s)$. Temos que $(m_1, s_1) + (m, s) = (s_1m + sm_1, s_1s)$ e $(m_2, s_2) + (m, s) = (s_2m + sm_2, s_2s)$. Da hipótese da igualdade das classes temos que $u(s_1m_2 - s_2m_1) = 0$ para algum $u \in S$. Queremos mostrar que

$$(s_1m + sm_1, s_1s) = (s_2m + sm_2, s_2s)$$

Sabemos que

$$(s_2m + sm_2)s_1s - (s_1m + sm_1)s_2s$$

Mas como estamos trabalhando com comutatividade podemos reorganizar e aplicando a distributiva, temos

$$ss_1s_2m + sss_1m_2 - ss_1s_2m - sss_2m_1 = ss(s_1m2 - s_2m1)$$

Podemos multiplicar por u

$$ssu(s_1m2 - s_2m1) = ss0 = 0$$

Portanto $(s_1m + sm_1, s_1s) = (s_2m + sm_2, s_2s)$

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

Comutativa

$$(m_1, s_1) + (m_2, s_2) = (s_1m_2 + s_2m_1, s_1s_2)$$
$$(m_2, s_2) + (m_1, s_1) = (s_2m_1 + s_1m_2, s_2s_1)$$

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.

Associativa

$$((m_1, s_1) + (m_2, s_2)) + (m_3, s_3) = (s_1m_2 + s_2m_1, s_1s_2) + (m_3, s_3)$$

$$(s_3(s_1m_2+s_2m_1)+s_1s_2m_3, s_1s_2s_3) = (s_3s_1m_2+s_3s_2m_1+s_1s_2m_3, s_1s_2s_3)$$

Agora desenvolvendo por outra ordem

$$(m_1, s_1) + ((m_2, s_2) + (m_3, s_3)) = (m_1, s_1) + (s_3m_2 + s_2m_3, s_3s_2)$$

$$= (s_1(s_3m_2+s_2m_3)+s_3s_2m_1, s_1s_3s_2) = (s_1s_3m_2+s_1s_2m_3+s_3a_2m_1, s_1s_3s_2)$$

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

Elemento neutro $(0, s)$, temos que $(m_1, s_1) + (0, s) = (s_10 + m_1s, s_1s) = (m_1s, s_1s)$
Mas note que $(m_1s, s_1s) = (m_1, s_1)$, ou seja, são classes equivalentes.
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, $(m_1, s_1) + (0, s) = (m_1s, s_1s) = (m_1, s_1)$.

Elemento inverso Para (m_1, s_1) o elemento neutro seria $(-m_1, s_1)$
$(m_1, s_1) + (-m_1, s_1)$ tem que ser igual a alguém da classe de $(0, s)$.

$$(m_1, s_1) + (-m_1, s_1) = (s_1 m_1 - s_1 m_1, s_1 s_1) = (0, s_1 s_1)$$

Então temos que mostrar que $(0, s_1 s_1)$ é da mesma classe que $(0, s)$. $(0, s_1 s_1) = (0, s)$ se e somente se existe $u \in S$ tal que $u(0s - 0s_1 s_2) = 0$, mas como $(0s - 0s_1 s_2) = 0$, logo u pode ser qualquer elemento de S, portanto $(m_1, s_1) + (-m_1, s_1) = (0, s_1 s_1) = (0, s)$

Logo $S^{-1}M$ é um grupo abeliano.

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

   Como $a_1 m_1 \in M$, por M ser um A-modulo. Como $s_3 \in S \subseteq A$, logo $s_3 s_1 \in A$, portanto está bem definida a operação.

□

Proposição 2.16. *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 $S^{-1}M$.*

Proof. Sabemos que a sequência $M' \xrightarrow{f} M \xrightarrow{g} M''$ é exata, portanto temos que $kerg = imf$, ou seja, todo mundo na 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 $f : A \xrightarrow{B}$, então o homomorfismo $S^{-1}f : S^{-1}A \xrightarrow{S}^{-1} B$ é dado por $S^{-1}f(a/s) = f(a)/s$.

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 $kerS^{-1}g = imS^{-1}f$.

Primeiro vamos mostrar que $imS^{-1}f \subset kerS^{-1}g$.

Tome x/s na imagem de $S^{-1}f$ Temos que $S^-1g \circ S^-1f(x/s) = S^-1g(f(x)/s) = g(f(x))/s$, mas como a sequência é exata, logo $g(f(x)) = 0$ e portanto $g(f(x))/s = 0$.

Agora vamos mostrar que

□

References

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

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

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