Estudos TCC

October 2, 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

$$0 = x * 0$$

□

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*

2 Corpo de fração

3 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 3.1. *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 3.2. *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 3.3. *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 3.4. *A soma em $S^{-1}A$ é definida por $(a, s) + (b, t) = (at + sb, st)$*

Definição 3.5. *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 3.6. *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 3.7. *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 3.8. *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 3.9. *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 3.10. *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 3.11. *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 3.12. *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 $\frac{0}{0}$*

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 $s \neq 0$.

Definição 3.13. *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 3.14. *$f : A \to S^{-1}A$ como $f(a) = (as, s)$ onde $s \in S$ com $s \neq 0$ é um homomorfismo.*

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

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

Produto

□

quando f é injetora? <=> sem divisor de zero

Proposição 3.15. *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.

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

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.

□

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.