Aula 11

IDEAIS E ANÉIS QUOCIENTES

META

Apresentar o conceito de ideal e definir anel quociente.

OBJETIVOS

Aplicar as propriedades de ideais na resolução de problemas.

Reconhecer a estrutura algébrica de anel quociente.

PRÉ-REQUISITO

O curso de Fundamentos de Matemática e a aula 10.

INTRODUÇÃO

Avançando na teoria dos anéis, vamos a mais uma aula. Nesta, iniciaremos o estudo dos ideais que são subanéis especiais, estudados inicialmente pelos matemáticos alemães Kummer e Dedekind motivados pelo famoso, último teorema de Fermat, no final do século XIX. Atualmente, a noção de ideal é fundamental na teoria dos anéis que é um dos temas centrais da álgebra comutativa.

Veremos a seguir que os ideais, cumprem um papel na construção dos anéis quocientes, semelhante ao papel dos subgrupos normais na construção dos grupos quocientes.

A partir desta aula trataremos apenas dos anéis comutativos.

O CONCEITO DE IDEAL

Definição 1. Seja A *um anel. Dizemos que um subconjunto* I *de* A *é um ideal, se cumpre as seguintes condições:*

i) $(I,+)$ *é um subgrupo de* $(A,+)$.

ii) Para cada $a \in A$ *e cada* $b \in I$, $ab \in I$.

Notemos que em especial, $\forall a, b \in I$, $ab \in I$. *Logo, todo ideal é subanel. Ou melhor,* $I \subset A$ *é um ideal se:*

i) $I \neq \phi$

ii) Se $a, b \in I$ *então* $a - b \in I$,

iii) Se $a \in A$ *e* $b \in I$ *então* $ab \in I$.

Notemos que sendo $I \neq \phi$, *existe pelo menos um* $a \in I$ *e* $0 = a - a \in I$. *Se* $a, b \in I$ *então* $-b = 0 - b \in I$ *e* $a + b = a - (-b) \in I$.

Exemplo 1. Os subanéis $\{0\}$ *e* A *de* A *são, trivialmente, ideais de* A.

Exemplo 2. Sejam A *um anel e* $a \in A$. *Então o conjunto* $aA = \{ax; x \in A\}$ *dos múltiplos de* a *em* A *é um ideal de* A. *De fato, pois,* $0 = a.0 \in A \neq \phi$ *e se* $ax_1, ax_2 \in aA$ $(x_1, x_2 \in A)$ *então* $ax_1 - ax_2 = a(x_1 - x_2)$ *com* $x_1 - x_2 \in A$, *portanto* $ax_1 - ax_2 \in aA$. *Se* $b \in A$ *e* $ax \in A, (x \in A)$, *então* $b.ax = a.(bx) \in A$. *O ideal* aA *é chamado ideal principal de* A *gerado pelo elemento* a. *Denotamos também este ideal por* (a) *ou* $< a >$.

Exemplo 3. Sejam A *um anel e* $a_1, a_2, \ldots, a_n \in A$. *O conjunto* $I = a_1A + a_2A + \cdots + a_nA = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n; x_1x_2, \ldots, x_n \in A\}$ *é um ideal, chamado ideal de* A

gerado por $a_1, a_2, \dots, a_n$. *A verificação de que este conjunto é de fato, um ideal é simples e deixamos como atividade. Indicamos este ideal também por* $(a_1, a_2, \dots, a_n)$ *ou* $< a_1, a_2, \dots, a_n >$.

Observação. Quando A *tem identidade o ideal principal gerado por* 1 *é o próprio* A. *Notemos que* $I \subset A$ *e para cada* $a \in A$, $a = 1.a \in I$ *ou seja* $A \subset I$. *Se* A *é um corpo e* I *é um ideal de* A *então* $I = \{0\}$ *ou* $I = A$. *Notemos que neste caso, se* $I \neq \{0\}$ *e* $a \in I \backslash \{0\}$ *existe* $a^{-1} \in A$ *e como* $1 = a^{-1}.a \in I$, *temos* $I = A$.

Exemplo 4. Na aula 2, quando estudamos o máximo divisor comum entre inteiros, estabelecemos o conceito de ideal especialmente para os inteiros. Vimos que todo ideal de $\mathbb{Z}$ *é principal.*

Definição 2. Quando num domínio todo ideal é principal, dizemos que o mesmo é um domínio de ideais principais (DIP).

Definição 3. Sejam A *um anel e* $a, b \in A$. *Dizemos que* a *divide* b $(a|b)$ *se existe um* $c \in A$ *tal que* $b = ac$.

Notamos que esta definição é a mesma que estabelecemos quando estávamos estudando os inteiros e, analogamente, valem as seguintes propriedades:

i) $a|a, \ \forall a \in A$

ii) Se $a, b, c \in A, \ a|b$ *e* $b|c$ *então* $a|c$

iii) Se $a, b_1, \dots, b_n \in A$ *e* $a|b_1, \dots, b_n$ *então, para todos* $c_1, \dots, c_n \in A$, *temos que* $a|b_1c_1 + \cdots + b_nc_n$.

Definição 4. Sejam A *um domínio e* $a_1, \dots, a_n \in A$ *não todos nulas. Dizemos que* $d \in A$ *é um máximo divisor comum de* $a_1, \dots, a_n$ *se:*

i) $d|a_1, \dots, a_n$.

ii) Se existe $c \in A$ *tal que* $c|a_1, \dots, a_n$, *então* $c|d$.

Exemplo 5. Para $a \in \mathbb{Z}$, -6 *e* 6 *são máximos divisores comuns de* 12 *e* 18.

Proposição 1. Sejam A *um domínio e* $a, b \in A$. *Se* $a|b$ *então* $bA \subset aA$.

Demonstração. Existe $c \in A$ *tal que* $b = ac$, *logo* $ac \in aA$, *ou seja,* $b \in aA$. *Segue que para todo* $d \in A, \ bd \in aA$, *ou seja,* $bA \subset aA$.

Definição 5. Sejam A *um anel com identidade e* $a, b \in A$. *Dizemos que* a *e* b *são associados se existe um invertível* u $(u \in A^*)$ *tal que* $b = a.u$. *Indicamos:* $a \sim b$.

Proposição 2. Se A *é um anel com identidade e* $a, b \in A$ *são elementos associados então* $a\mathbb{Z} = b\mathbb{Z}$.

Demonstração. Seja $ad \in a\mathbb{Z}$. *Como existe* $v \in \cup(A)$ *tal que* $a = bv$, *temos* $ad = (bv)d = b(vd) \in bA \Longrightarrow aA \subset bA$. *Analogamente,* $bA \subset aA$, *donde temos a igualdade.*

Observação. A recíproca desta proposição só é verdadeira se A *é um domínio. Notemos que* $aA = bA \neq \{0\} \Longrightarrow b \in aA$ *e* $a \in bA \Longrightarrow a|b$ *e* $b|a$. *Então, existem* $u, v \in A$ *tais que* $b = au$ *e* $a = bv \Longrightarrow a = (au)v = a(uv) \Longrightarrow a(1 - uv) = 0$. *Sendo* $a \neq 0$ *e* A *domínio, segue que* $uv = 1$ *ou seja* $a \sim b$.

Definição 6. Sejam A *um anel e* $I, J \subset A$ *ideais. Definimos a soma de* I *e* J *como sendo o conjunto* $I + J = \{a + b;\ a \in I, b \in J\}$.

Notemos que $0 \in I \cap J \Longrightarrow 0 = 0 + 0 \in I + J \neq \phi$. *Se* $a_1 + b_1, a_2 + b_2 \in I + J$ $(a_1, a_2, \in I$ *e* $b_1, b_2 \in J)$ *então* $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I + J$. *Se* $c \in A$ *e* $a + b \in I + J$ *(com* $a \in I, b \in J$*), então* $c(a + b) = ca + cb$. *Com* $ca \in I$ *e* $cb \in J$, *pois* I *e* J *são ideais, segue que* $c(a + b) \in I + J$. *Portanto* $I + J$ *é um ideal de* A.

Definição 7. Sejam A *um anel e* $I, J \subset A$ *ideais. Definimos o produto de* I *por* J *como sendo o conjunto* $I.J = \{\sum_{i=1}^{n} a_i b_i;\ a_i \in I, b_1 \in J, k \in \mathbb{N}\}$.

Notamos que IJ *é o conjunto de todos os elementos de* A *que podem ser escritos como uma soma com um número finito de parcelas do tipo* ab *com* $a \in I$ *e* $b \in J$.

É fácil ver que o pode ser escrito desta forma, que se $\alpha, \beta \in A$ *são escritos desta forma,* $\alpha - \beta$ *também pode ser escrito desta forma e finalmente, se* $c \in A$ *e* α *é uma soma de parcelas do tipo* ab *com* $a \in I$ *e* $b \in J$, *então* $c\alpha$ *também o é. Portanto* IJ *é um ideal de* A.

Exemplo 6. Sejam $A = \mathbb{Z}, I = 2\mathbb{Z}$ *e* $J = 4\mathbb{Z}$. *Então:*

$I + J = \{2a + 4a; a, b \in \mathbb{Z}\} = \{2(a + 2b); a, b \in \mathbb{Z}\} = \{2c; c \in \mathbb{Z}\} = I$

$I.J = \{\sum_{i=1}^{n} a_i b_i;\ a_i \in I$ *e* $b_i \in J, n \in \mathbb{N}\} = \{\sum_{i=1}^{n} 8ab;\ a, b \in \mathbb{Z}\} = 8\mathbb{Z}$

Observação: $aA.bA = abA$

Definição 8. Sejam A *um anel e* I *um ideal de* A. *Dizemos que* I *é um ideal primo de* A *se,* $I \neq A$ *e toda vez que* $ab \in I$ *com* $a, b \in A$, *temos que* $a \in I$ *ou* $b \in I$.

Exemplo 7. O ideal nulo e os ideais gerados por elementos primos de $\mathbb{Z}$, *são todos ideais primos. Se* $p \in \mathbb{Z}$ *é primo então* $p\mathbb{Z} \neq \mathbb{Z}$ *e se* $ab \in p\mathbb{Z}$ *com* $a, b \in \mathbb{Z}$ *então* $p|ab$ *donde temos que* $p|a (\Longrightarrow a \in p\mathbb{Z})$ *ou* $p|b (\Longrightarrow b \in p\mathbb{Z})$.

Exemplo 8. Seja $A = \{f : [0,1] \longrightarrow \mathbb{R}$ *tal que* f *é continua*$\}$ *e seja* $I = \{f \in A; f(0) = 0\}$. *Então,* I *é um ideal primo do anel* A. *Com efeito, se* $f, g \in A$ *e* $(fg)(0) = f(0).g(0) = 0 \Longrightarrow f(0) = 0\ (\Longrightarrow f \in I)$ *ou g(0)=0* $\ (\Longrightarrow g \in I)$. *Notemos que* $I \neq A$.

Definição 9. Sejam A *um anel e* I *um ideal de* A. *Dizemos que* I*é maxámal se toda vez que* $J \subset A$ *é um ideal tal que* $I \subset J \subset A$ *temos* $J = I$ *ou* $J = A$ *(ou seja, não existe um ideal próprio de* A *contendo* I *e diferente de* I*).*

Exemplo 9. Todos os ideais primos e não nulos de $\mathbb{Z}$ *são maximais. Seja* $p \in \mathbb{Z}$ *um primo e suponhamos que existe um ideal* $J = q\mathbb{Z}$ *tal que* $p\mathbb{Z} \subset q\mathbb{Z} \subset \mathbb{Z}$. *Então* $q|p\ (\Longrightarrow q = \pm 1$ *ou* $q \pm p)$. *Se* $q = \pm 1$, *temos* $J = \mathbb{Z}$ *e, se* $q = \pm p$, *temos* $J = p\mathbb{Z}$.

ANÉIS QUOCIENTES

Sejam A *um anel e* I *um ideal de* A. *Vamos definir em* A *a seguinte relação binária:*

Definição 1. Dados $a, b \in A$, *dizemos que* a *é congruente a* b *módulo* I *e escrevemos* $a \equiv b(mod\ I)$ *se* $a - b \in I$.

Proposição 1. A relação acima definida em A *é de equivalência.*

Demonstração. i) $\forall a \in A,\ a - a = 0 \in I \Longrightarrow a \equiv a(mod\ I)$.

ii) Se $a \equiv b(mod\ I)$ *então* $a - b \in I \Longrightarrow b - a = -(a - b) \in I \Longrightarrow b \equiv a(mod\ I)$.

iii) Se $a \equiv b(mod\ I)$ *e* $b \equiv c(mod\ I)$ *então* $a - b, b - c \in I \Longrightarrow a - c \in I \Longrightarrow a \equiv c(mod\ I)$.

A classe de um elemento $a \in A$, *módulo esta relação é:*

$\bar{a} = \{b \in A; b \equiv a(mod\ I)\} = \{b \in A; b - a \in I\} = \{b \in A; b - a = c \in I\} = b = a + c; c \in I\} = a + I$

O conjunto quociente é ${}^{A}/_{I} = \{\bar{a}; a \in A\} = \{a + I; a \in A\}$. *Agora, vamos definir duas operações uma adição e uma multiplicação no conjunto quociente* ${}^{A}/_{I}$ *do seguinte modo: dados* $a + I, b + I \in {}^{A}/_{I}$, $(a + I) + (b + I)$ *e* $(a + I).(b + I) = a.b + I$.

Proposição 2. As operações acima estão bem definidas. Ou melhor, não dependem dos representantes das classes.

Demonstração. Sejam $a, a', b, b'b \in A$ *e suponhamos que* $a + I = a' + I$ *e* $b + I = b' + I$ *ou seja* $c = a - a', d = b - \in I$. *Temos então:* $c + d = a - a' + b - b' \in I \Longrightarrow (a + b) - (a' + b') \in I \Longrightarrow (a + b) + I = (a' + b') + I$. *Agora,* $a = a' + c, b = b' + d \Longrightarrow$

$ab = (a + c)(b' + d) = a'b' + a'd + cb' + cd \Longrightarrow ab + a'b' \quad a'd + cb' + cd \in I \Longrightarrow ab + I = a'b' + I.$

Proposição 3. O conjunto quociente $^{A}/_{I}$***, munido das operações acima definidas tem estrutura de anel.***

Demonstração. Dados $a + I, b + I, c + I \in {}^{A}/_{I}$***, temos,***

i) $\big((a + I), b + I\big) + c + I = \big((a + b) + I\big) + c + I = \big((a + b) + c\big) + I = (a + (b + c) + I) = a + I + \big((b + c) +\big).$

ii) $(a + I) + (b + I) = (a + b) + I = (b + a) + I = (b + I) + (a + I).$

iii) existe $I = 0 + I$ ***tal que*** $(a + I) + (0 + I) = (a + 0) = a + I, \ \forall a + I \in {}^{A}/_{I}.$

iv) para cada $a + I \in {}^{A}/_{I}$***, existe*** $-(a + I) = (-a) + I$ ***tal que*** $(a + I) + \big((-a) + I\big) = \big(a + (-a)\big) + T = 0 + I = I.$

v) $\big((a + I).(b + I)\big).(c + I) = \big((ab) + I\big).(c + I) = ((ab).c + I = (a(b.c) + I) = (a + I).\big((bc) + I\big) = (a + I)((b + I).(c + I)).$

vi) $(a + I)\big((b + I) + (c + I)\big) = \quad (a + I)((b + c) + I = \ (a(b + c) + I) = \ \big((ab + ac) + I\big) = (ab + I) + (ac + I) = (a + I)(b + I) + (a + I)(c + I)\ .$

Analogamente, $\big((a + I) + (b + I)\big).(c + I) = (a + I)(c + I) + (b + I).(c + I).$

Notemos que se A ***tem identidade, então*** $^{A}/_{I}$ ***tem identidade, pois,*** $\forall a + I \in {}^{A}/_{I}, (a + I).(1 + I) = (a.1) + I = a + I.$

Exemplo 1. Sejam $A = \mathbb{Z}$ ***e*** $n\mathbb{Z}$ ***um ideal de*** $\mathbb{Z}$***. Notamos que*** $a, b \in \mathbb{Z}, \ a \equiv b(n\mathbb{Z}) \Longrightarrow a - b \in n\mathbb{Z} \Leftrightarrow n|a - b \Leftrightarrow a \equiv b(mod\ n).$ ***Logo,*** $^{\mathbb{Z}}/_{n\mathbb{Z}} = \mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}.$

Ou seja, $^{\mathbb{Z}}/_{n\mathbb{Z}}$ ***é o anel*** $\mathbb{Z}_n$ ***que já estudamos na aula 3.***

Proposição 4. Sejam A ***um anel com identidade e*** I ***um ideal de*** A***.***

i) I ***primo se, e somente se,*** $^{A}/_{I}$ ***domínio.***

ii) I ***maximal se, e somente se,*** $^{A}/_{I}$ ***corpo.***

Demonstração. i) $(\Longrightarrow)$ ***se*** $^{A}/_{I}$ ***não fosse um domínio, existiriam*** $a + I, b + I \in {}^{A}/_{I} \setminus \{I\}$ ***tais que*** $(a + I).(b + I) = ab + I = I.$ ***Neste caso,*** $ab \in I$ ***e como*** I ***é um ideal primo, teríamos*** $a \in I\ (\Longrightarrow a + I = I)$ ***ou*** $b \in I (\Longrightarrow b + I = I)$***, contradição.***

($\Leftarrow$) *Suponhamos que* A/I *domínio. Se* I *não fosse um ideal primo então* $I = A$ *e neste caso* $A/I = \{0\}$, *uma contradição, ou existiriam* $a, b \in A$ *tais que* $ab \in I$ *com* $a \notin I$ *e* $b \notin I$. *Mas, teríamos então* $a + I + I$, $a + I \neq I$ *e* $(a + I)(b + I) = ab + I = I$, *contrariando a hipótese de que* A/I *é domínio.*

ii) ($\Longrightarrow$) *Seja* $a + I \in A/I \setminus \{I\}$, *logo* $a \notin I$. *Segue que o ideal* $I + aA$ *contém propriamente o ideal* I. *Como* I *é maximal segue que* $I + aA = A$ *e, existem* $u \in I$ *e* $v \in A$ *tais que* $u + av = 1$. *Assim,* $av - 1 \in I$ *ou seja,* $av + I = 1 + I \Longrightarrow (a + I).(v + I) = 1 + I$. *Portanto,* $a + I$ *é invertível e conseqüentemente* A/I *é corpo.*

($\Leftarrow$) *Seja* $J \in A/I$ *um ideal tal que* $I \subset J \subset A$ *e suponhamos que* $j \neq I$ *segue que existe* $a \in J - I$. *Como* A/I *é corpo e* $a \notin I$, *temos que* $a + I$ *é invertivel em* A/I *ou seja, existe* $b + I \in A/I$ *tal que* $(a + I)(b + I) = ab + I = 1 + I$. *Logo,* $c = ab - 1 \in I$ *ou melhor,* $ab - c = 1 \in J$ *pois* $a \in J$ *e* $c \in J$. *Portanto,* $J = A$ *e* I *é maximal.*

Exemplo 2. Os ideais do tipo $p\mathbb{Z}$, *de* $\mathbb{Z}$ *com* p *primo são todos maximais. Com efeito, se existe um ideal* $q\mathbb{Z}$ *de* $\mathbb{Z}$ *tal que* $p\mathbb{Z} \subset q\mathbb{Z} \subset \mathbb{Z}$ *então* $q|p$, *ou seja,* $q \in \{\pm 1, \pm p\}$. *Se* $q = \pm p$, *temos* $q\mathbb{Z} = p\mathbb{Z}$.

RESUMO

Nesta aula, estudamos inicialmente o conceito de ideal, no geral definimos os domínios principais, o máximo divisor comum nestes domínios, definimos a adição e o produto de ideais definimos ideais primos e maximais. No final estudamos conceito de anel quociente onde estabelecemos os dois resultados importantes de que quando um ideal é primo (maximal) o quociente é domínio (corpo).

ATIVIDADES

1. Seja $\{I_\lambda\}_{\lambda \in L}$ *uma família de ideais de um anel* A. *Prove que* $\cap_{\lambda \in L} I_\lambda$ *é também um ideal de* A.

2. Seja $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ *uma cadeia ascendente de ideais de* $\mathbb{Z}$. *Prove que existe um* $m \in \mathbb{N}$ *tal que* $I_n = I_m$, $\forall n \geq m$. *(Anéis que tem esta propriedade são chamados Noetheriamos).*

3. Se I *e* J *são ideais de um anel* A. *Prove que em geral* $I \cup J$ *não é um ideal.*

4. Sejam I, J, K *ideais de um anel* A. *Prove que:*

a) $(I + J) + K = I + (J + K)$.

b) $I + J = \{0\} \Leftrightarrow I = J = \{0\}$.

c) $I + A = A$.

d) $I.J \subset I \cap J$.

5. Sejam A *um anel comutativo e* N *o nilradical de* A*.prove que* N *é um ideal de* A*. Prove também que o único elemento nilpotente do anel quociente* $^{A}/_{N}$ *é* N*.*

6. Sejam A *um anel e* I *um ideal de* A*. Defina* $\sqrt{I} = \{a \in A$ *tal que* $a^n \in I$ *para algum* $n \in \{1,2,3,\dots\}\}$*. Prove que* $\sqrt{I}$ *é um ideal de* A*. (Este ideal é chamado o radical de* I*).*

7. Seja A *o anel das funções* $f : [0,1] \longrightarrow \mathbb{R}$ *contínuas e seja* I *um ideal maximal de* A*. Prove que para cada* $f \in I$ *existe um* $a \in [0,1]$ *tal que* $f(a) = 0$*.*

COMENTÁRIO DAS ATIVIDADES

Na primeira atividade você, caro aluno, deve ter aplicado apenas a definição de ideal.

Na segunda atividade, você deve ter usado o fato de que o domínio dos inteiros é principal, conseqüentemente, fatorial. Se a cadeia ascendente de ideais não estabilizasse, teríamos algum inteiro com infinitos divisores.

Na terceira atividade, você deve ter notado que a união de dois ideais só é um ideal, quando um é subconjunto do outro.

Na quarta atividade, se você a fez, deve ter apenas aplicado a definição de ideal e as respectivas definições.

Nas quinta e sexta atividades, você deve ter usado novamente a definição de ideal e como se trata de anéis comutativos, a fórmula do binômio de Newton pode ser aplicada.

Na sétima atividade você deve ter percebido que se a afirmação não fosse verdadeira a função 1 pertenceria ao ideal e o mesmo não seria maximal.

REFERÊNCIAS

GONÇALVES, Adilson. Introdução à álgebra. 5. ed. Rio de Janeiro: IMPA, 2007. 194 p. (Projeto Euclides) ISBN.

HUNGERFORD, Thomas W. Abstract algebra: an introduction. 2nd. ed. Austrália: Thomson Learning, ©1997.

GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de álgebra. 3. ed. Rio de Janeiro: IMPA, 2005. 326 p. (Série: Projeto Euclides).