Universidade Estadual de Campinas
Departamento de Matemática

Exemplo de um Anel de Ideais Principais que não é um Anel Euclidiano

Adriana Wagner
Gustavo Terra Bastos

Campinas - SP
2013

Resumo

Nesta monografia apresentaremos um exemplo de um anel de ideais principais que não é um anel euclidiano.

1 Introdução

O estudo de anéis originou-se da teoria de anéis de polinômios e da teoria de inteiros algébricos. Richard Dedekind foi quem introduziu o conceito de anel. O termo anel (Zahlring) foi criado por David Hilbert no artigo Die Theorie der algebraischen Zahlkörper, Jahresbericht der Deutschen Mathematiker Vereiningung, Vol. 4, 1897. A primeira definição axiomática de anéis foi dada por Adolf Fraenkel em um ensaio no Journal für die reine und angewandte Mathematik (A. L. Crelle), vol. 145, 1914. Em 1921, Emmy Noether criou a primeira fundação axiomática da teoria de anéis comutativos em seu monumental trabalho Ideal Theory in Rings.
Nesta monografia, primeiramente, apresentaremos algumas definições como conceito de anéis, anéis de ideais principais e anéis euclidianos. A partir destes conceitos provaremos que todo anel euclidiano é um anel de ideais principais. E teremos como objetivo principal mostrar que a recíproca deste resultado não é válida. Para isso apresentaremos um anel que é um subconjunto do anel dos números complexos ($\mathbb{C}$), mostraremos que esse anel é um anel de ideais principais mas não é um anel euclidiano.

2 Preliminares

Apresentaremos a definição de anel, de homomorfismo de aneís e alguns resultados relacionados (que omitiremos as demonstrações). Usaremos com livro texto o livro: Tópicos de Algebra de I. N. Hernstein.

Definição 2.1 *Um conjunto não vazio R é dito um anel associativo se em R estão definidas duas operações, indicadas por $+$ e $\cdot$ respectivamente, tais que para todos a, b e c em R:*
(1)$a+b$ está em R.
(2)$a+b=b+a$.
(3)$(a+b)+c=a+(b+c)$
(4)Existe um elemento 0 em R tal que $a+0=a$ (para cada a em R.
(5)Existe um elemento $-a$ em R tal que $a+(-a)=0$.
(6)$a\cdot b$ está em R.
(7)$a\cdot(b\cdot c)=(a\cdot b)\cdot c$.
(8)$a\cdot(b+c)=a\cdot b+a\cdot c$ e $(b+c)\cdot a=b\cdot a+c\cdot a$ (as duas leis distributivas).

Observação 2.1 *Pode muito bem acontecer ou não, que exista um elemento 1 em R tal que $a\cdot 1=a$ para todo $a\in R$; se existir tal elemento, R é denominado anel com elemento unidade.*

Observação 2.2 *Se a multiplicação de R é tal que $a\cdot b=b\cdot a$ para todos $a,b\in R$, então chamamos R um anel comutativo.*

Exemplo 2.1 *O conjunto dos números inteiros, $\mathbb{Z}$ sendo $+$ e $\cdot$ as operações usuais dos inteiros é um anel comutativo com elemento unidade.*

Exemplo 2.2 *O conjunto do números inteiros pares, $2\mathbb{Z}$ com as operações e multiplicações usuais é um anel comutativo mas não possui elemento unidade.*

Exemplo 2.3 *O conjuntos dos números racionais com as operações usuais de adição e multiplicação de números racionais é um anel comutativo com elemento unidade. Além disso, os números racionais diferentes de 0 formam um grupo abeliano com relação a multiplicação, com está última propriedade é denominada um corpo.*

Exemplo 2.4 *O conjunto dos inteiros módulo 7,* $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ *com as operações de adição e multiplicação mod 7 é um anel comutativo com elemente unidade. Como* $\bar{1} \cdot \bar{1} = \bar{1} = \bar{6} \cdot \bar{6}$, $\bar{2} \cdot \bar{4} = \bar{1} = \bar{4} \cdot \bar{2}$, $\bar{3} \cdot \bar{5} = \bar{1} = \bar{5} \cdot \bar{3}$ *os elementos não nulos de* R *formam um grupo abeliano com relação à operação de multiplicação. Portanto* $\mathbb{Z}_7$ *é um corpo.*

Exemplo 2.5 *O conjunto dos inteiros módulo 6,* $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ *com as operações de adição e multiplicação mod6 é um anel comutativo com unidade. Pode-se ver que* $\bar{2} \cdot \bar{3} = \bar{0}$, *com* $\bar{2}, \bar{3} \neq \bar{0}$. *Assim é possível num anel* R *que* $a \cdot b = 0$ *sem que se tenha* $a = 0$ *nem* $b = 0$. *Isso não pode acontecer num corpo, logo* $\mathbb{Z}_6$ *não é um corpo.*

O exemplo anterior nos leva a seguinte definição.

Definição 2.2 *Se* R *é um anel comutativo, então* $a \neq 0 \in R$ *é dito um divisor de zero se existe um* $b \in R$, $b \neq 0$, *tal que* $ab = 0$.

Definição 2.3 *Um anel comutativo é um anel de integridade se não possui divisores de zero.*

Um exemplo de anel de integridade é o conjunto dos números inteiros, $\mathbb{Z}$.

Definição 2.4 *Um anel é dito anel com divisão se seus elementos não nulos formam um grupo com relação a multiplicação. O elemento unidade com relação a multiplicação será indicado por* 1 *e o inverso multiplicativo do elemento* a *será indicado por* a^{-1}.

Definição 2.5 *Um corpo é um anel com divisão comutativo.*

Lema 2.1 *Se* R *é um anel, então para todos* $a, b \in R$,
(1)$a0 = 0a = 0$
(2)$a(-b) = (-a)b = -(ab)$
(3)$(-a)(-b) = ab$
Se além disso, R *possui um elemento unidade 1, então*
(4)$(-1)a = -a$
(5)$(-1)(-1) = 1$

Lema 2.2 *Um anel de integridade finito é um corpo.*

Corolário 2.1 *Se p é um número primo, então $\mathbb{Z}_p$, o anel dos inteiros mod p é um corpo.*

No estudo de grupos vimos que o conceito de homomorfismo foi de muita importância. Assim a analogia apropriada para anéis levará a ideais importantes.

Definição 2.6 *Uma apliçação ϕ do anel R no anel R' é dita um homomorfismo se*
(1)$\phi(a+b) = \phi(a) + \phi(b)$
(2)$\phi(ab) = \phi(a)\phi(b)$
para todos $a, b \in R$

Lema 2.3 *Se ϕ é um homomorfismo de R em R', então*
(1)$\phi(0) = 0$
(2)$\phi(-a) = -\phi(a)$ para todo $a \in R$.

Definição 2.7 *Se ϕ é um homomorfismo de R em R', então o núcleo de ϕ, $Nuc(\phi)$ é o conjunto de todos os elementos $a \in R$ tais que $\phi(a) = 0$, o elemento zero de R'.*

Lema 2.4 *Se ϕ é um homomorfismo de R em R', com núcleo $Nuc(\phi)$, então:*
(1)$Nuc(\phi)$ é um subgrupo de R com relação à adição.
(2)Se $a \in Nuc(\phi)$ e $r \in R$ então ar e ra estão em $Nuc(\phi)$.

Exemplo 2.6 *Sejam R e R' dois anéis arbitrários e definamos $\phi(a) = 0$ para todo $a \in R$. Trivialmente ϕ é um homomorfismo e $Nuc(\phi) = R$. ϕ é chamado o homomorfismo nulo.*

Exemplo 2.7 *Seja R um anel $R' = R$ e definamos $\phi(x) = x$ para todo $x \in R$. Evidentemente, ϕ é um homomorfismo e $Nuc(\phi)$ consiste apenas de 0.*

Exemplo 2.8 *Seja $\mathbb{Z}$ o anel dos inteiro, $\mathbb{Z}_n$ o anel dos inteiros módulo n. Definamos $\phi : \mathbb{Z} \to \mathbb{Z}_n$ por $\phi(a) =$ resto da divisão de a por n. Então ϕ é um homomorfismo sobrejetor e $Nuc(\phi) = n\mathbb{Z}$.*

Definição 2.8 *Um homomorfismo de R em R' é dito um monomorfismo se ele é uma aplicação injetora.*

Definição 2.9 *Dois anéis são ditos isomorfosmos se existe entre eles um homomorfismo injetor e sobrejetor.*

3 Aneís de Ideais Principais

Nesta seção apresentaremos a definição de ideais, de anéis de ideais principais e alguns resultados. Como na teoria de grupos a ideia de homomorfismo e e seu núcleo foram introduzidas para anéis, assim faremos a analogia para anéis do conceito de subgrupo normal.

Definição 3.1 *Um subonjunto não vazio U de R é dito um ideal (bilatetal) de R se:*
(1) U é um subgrupo de R com relação à adição.
(2) Para todo $u \in U$ e $r \in R$, ur e ru estão em U.

Dado um ideal U de um anel R, seja R/U o conjunto de todas as classas laterais distintas de U em R que obtemos quando consideramos U como um subgrupo de R com relação à adição. Assim, em símbolos, $R/U = \{a + U | a \in R\}$. Definimos em R/U as operaçãoes de adição e multiplicação, respectivamente, $(a + U) + (b + U) = (a + b) + U$ e $(a + U)(b + U) = ab + U$. Assim tem os o seguintes Lema.

Lema 3.1 *Se U é um ideal do anel R, então $(R/U, +, \cdot)$ é uma anel e é uma imagem homomorfa de R.*

Teorema 3.1 *Sejam R e R' anéis e ϕ um homomorfismo sobrejetor de R em R' com núcleo U. Então R' é isomorfo a R/U. Além do mais, existe uma correspondência bijetora entre o conjunto dos ideais de R' e o conjunto dos ideais de R que contém U. Esta correspondência pode ser conseguida associando com um ideal W' de R' o ideal W de R definido por $W = \{x \in R | \phi(x) \in W'\}$. Com W assim definido R/W é isomorfo a R'/W'.*

Lema 3.2 *Seja R um anel comutativo com elemento unidade cujos únicos ideais são (0) e o próprio R. Então R é um corpo.*

Definição 3.2 *Um ideal $M \neq R$ num anel R é dito um ideal maximal de R se sempre que U for um ideal de R tal que $M \subset U \subset R$, então $R = U$ ou $M = U$.*

Exemplo 3.1 *Seja $R = \mathbb{Z}$ o anel dos inteiros e seja U um ideal de R. Como U é um subgrupo de R com relação à adição, pelos resultados da teoria de grupos, sabemos que U consite de todos os múltiplos de um inteiro fixo n_0; indicamos isto por $U = (n_0)$. Temos que U será um ideal maximal se, e somente se, n_0 é um número primo.*

Teorema 3.2 *Se R é um anel comutativo com elemento unidade e M é um ideal de R, então M é um ideal maximal de R se, e somente se, R/M é um corpo.*

Agora introduzimos a notação $(a) = \{xa | x \in R\}$ para representar o ideal de todos os múltiplos de a. Assim introduzimos a seguinte definição.

Definição 3.3 *Um anel de integridade R com elemento unidade é um anel principal se todo ideal A em R é da forma $A = (a)$. para algum $a \in R$.*

4 Anel Euclidiano

Nesta seção apresentaremos a definição de Anel Euclidiano e o resultado que todo anel euclidiano é um anel de ideais principais.

Definição 4.1 *Um anel de integridade R é dito um anel euclidiano se para todo $a \neq 0$ em R está definido um inteiro não negativo $d(a)$ tal que*
(1) Para todos $a, b \in R$, ambos não nulos, $d(a) \leq d(ab)$.
(2) Para todos $a, b \in R$, ambos não nulos, existem $t, r \in R$ tais que $a = tb + r$, onde $r = 0$ ou $d(r) < d(b)$.

Um exemplo de anel euclidiano é o anel dos inteiros, $\mathbb{Z}$.

Teorema 4.1 *Seja R um anel euclidiano e seja A um ideal de R. Então existe um elemento $a_0 \in A$ tal que A consista exatamente de todos os $a_0 x$ quando x percorre R.*

Demonstração: Se A consiste apenas do elemento 0, basta fazer $a_0 = 0$ e a conclusão do teorema vale. Assim podemos admitir que $A \neq (0)$, logo existe um $a \neq 0$ em A. Tomemos um $a_0 \in A$ tal que $d(a_0)$ seja mínimo. (Como d assume valores inteiros não negativos isto é possível.)
Suponhamos que $a \in A$. Pelas propriedades dos anéis euclidianos existem $t, r \in R$ tais que $a = ta_0 + r$ onde $r = 0$ ou $d(r) < d(a_0)$. Como $a_0 \in A$ e A ideal de R, ta_0 está em A. Combinado com $a \in A$ isto resulta em $a - ta_0 \in A$, mas $r = a - ta_0$, donde $r \in A$. Se $r \neq 0$, então $d(r) < d(a_0)$, dando-nos um elemento r de A para o qual d assume um valor

menor que para a_0, em contradição com a nossa escolha de a_0 como elemento de A para o qual d assume valor mínimo. Consequentemente, $r = 0$ e $a = ta_0$, o que demonstra o teorema.

Assim com esse demonstramos que todo anel euclidiano é um anel de ideais principais.

Corolário 4.1 *Um anel euclidiano possui um elemento unidade.*

Demonstração Seja R um anel euclidiano, então R é certamente um ideal de R, de modo que pelo Teorema 4.1 podemos concluir que $R = (u_0$ para algum $u_0 \in R$. Assim todo elemento R é um múltiplo de u_0. Portanto, em particular, $u_0 = u_0 c$ para algum $c \in R$. Se $a \in R$ então $a = xu_0$ para algum $x \in R$, donde $ac = (xu_0)c = x(u_0 c) = xu_0 = a$. Vemos assim que c é o elemento unidade requerido.

Definição 4.2 *Se $a \neq 0$ e b estão num anel comutativo R, então diz-se que a divide b se existe um $c \in R$ tal que $b = ac$. Usaremos o símbolo $a|b$ para representar o fato de que a divide b e $a \nmid b$ para significar que a não divide b.*

Definição 4.3 *Se $a, b \in R$ então $d \in R$ é dito um máximo divisor comum de a e b se:*
(1)$d|a$ e $d|b$.
(2)Sempre que $c|a$ e $c|b$ então $c|d$.

Usaremos a notação $d = (a, b)$ para indicar que d é um máximo divisor comum de a e b.

Lema 4.1 *Seja R um anel euclidiano. Então dois elementos quaisquer a e b em R possuem um máximo divisor comum d. Além disso, $d = \lambda a + \mu b$ para certos $\lambda, \mu \in R$.*

Definição 4.4 *Seja R um anel comutativo com elemento unidade. Um elemento $a \in R$ é uma unidade em R se existe um elemento $b \in R$ tal que $ab = 1$.*

Lema 4.2 *Seja R um anel de integridade com elemento unidade e suponhamos que para $a, b \in R$, $a|b$ e $b|a$ sejam verdadeiras. Então $a = ub$ onde u é uma unidade em R.*

Demonstração: Como $a|b$, $b = xa$ para algum $x \in R$, como $b|a$, $a = yb$ para algum $y \in R$. Assim $b = x(yb) = (xy)b$, mas estes são elementos de um anel de integridade, de modo que podemos cancelar o b e obter $xy = 1$, y é assim uma unidade em R e $a = yb$, demostrado o lema.

Definição 4.5 *Seja R um anel comutativo com elemento unidade. Dois elementos a e b em R são ditos it associados se $b = ua$ para alguma unidade u em R.*

Lema 4.3 *Seja R um anel euclidiano e $a, b \in R$. Se b não for uma unidade em R então $d(a) < d(ab)$.*

Demostração: Consideremos o ideal $A = \{xa|x \in R\}$ de R. Pela condição (1) para um anel euclidiano. $d(a) \leq d(xa)$ para $x \neq 0$ em R. Assim o valor que d assume em a é o mínimo de d para quaisquer valores de A. Ora, $ab \in A$, se $d(ab) = d(a)$, pela demostra cão do Teorema 4.1 como o valor de d em ab é mínimo com relação a A, todo elemento de A é múltiplo de ab. Em particular, como $a \in A$, a é um múltiplo de ab, donde $a = abx$ para algum $x \in R$. Como tudo isto está ocorrendo num anel de integridade, obtemos $bx = 1$. Desta m aneira b é uma unidade. O resultado é que $d(a) < d(ab)$.

5 Exemplo de anel de ideais principais que não é um anel euclidiano

Nas seções anterioes definimos anel de ideais principais e anel euclidiano. Vimos pelo Teorema 4.1 vimos que todo anel euclidiano é um anel de ideais principais. Podemos nos perguntar se a recíproca deste Teorema é válido. Veremos abaixo que essa recíprova é falsa, ou seja, exibiremos um anel que é um anel de ideais principais, mas não é um anel euclidiano.

O anel que vamos tomar como contra exemplo da recíproca do Teorema 4.1 é o anel R um subconjunto do anel dos números complexos, $\mathbb{C}$, com as operações de adição e multiplicações usuais em $\mathbb{C}$. Então o nosso contraexemplo é:

$$R = \{a + b(1 + \sqrt{-19})/2 | a, b \in \mathbb{Z}\}$$

Temos que $(R, +, \cdot)$ é um anel de integridade com elemento unidade. Assim mostraremos que R é um anel de ideais principais mas não é um anel euclidiano. Para mostrar que R é um anel de ideais principais usaremos o seguinte resultado.

Teorema 5.1 *Se para todo par de elementos x e y em um anel R com $d(x) \geq d(y)$, ou $y|x$ ou existe z e w em R com $0 < d(xz - yw) < d(y)$, então R é um anel de ideais principais.*

Afirmação: O anel R é um anel de ideais principais
Em $\mathbb{R}$ existe a norma usual, $d(a + bi) = a^2 + b^2$, (a norma herdada de $\mathbb{C}$), que tem a proprieade que $d(xy) = d(x)d(y)$ para todo x e y. Em R essa norma é sempre um inteiro não negativo. Seja $A \neq (0)$ um ideal em R. Seja y um elemento de A com $y = min\{d(a), a \in A\}$ e x outro elemento de A. Para todo $z, w \in R$, $xz - yw \in A$ (pois A ideal de R), logo $xz - yw = 0$ ou $d(xz - yw) \geq d(y)$. Assim pelas condições em R requer que $y|x$, isto é, $x = ay$, ou seja, $A = (y)$.
Vamos mostrar que R satisfaz as condições do Teorema 5.1. Notemos que

$$0 < d(xz - yw) < d(y) \Leftrightarrow 0 < d(xz - yw) \cdot d(y^{-1}) < d(y) \cdot d(y^{-1}) \Leftrightarrow 0 < d(\frac{x}{y}z - w) < 1$$

Dado $x, y \in R$, ambos não zeros e $y \nmid x$, escreva

$$\frac{x}{y} = \frac{a + b\sqrt{-19}}{c}$$

onde $a, b, c \in \mathbb{Z}$, $(a, b, c) = 1$ e $c > 1$. Em primeiro lugar, assuma que $c \geq 5$. Escolha inteiros d, e, f, q, r tal que

$$ae + bd + cf = 1, \quad ad - 19be = cq + r \quad e \quad |r| \leq \frac{c}{2}$$

Seja

$$z = d + e\sqrt{-19} \quad e \quad w = q - f\sqrt{-19}.$$

Assim,

$$\begin{aligned}
\frac{x}{y} \cdot z - w &= \frac{(a + b\sqrt{-19})}{c} \cdot (d + e\sqrt{-19}) - (q - f\sqrt{-19}) \\
&= \frac{ad + ae\sqrt{-19} + bd\sqrt{-19} - 19be}{c} - (q - f\sqrt{-19}) \\
&= \frac{ad + (ae + bd)\sqrt{-19} - 19be - qc + cf\sqrt{-19}}{c}
\end{aligned}$$

$$= \frac{ad - 19be - qc + (ae + bd + cf)\sqrt{-19}}{c}$$

$$= \frac{cq + r - qc + \sqrt{-19}}{c}$$

$$= \frac{r + \sqrt{-19}}{c} = \frac{r}{c} + \frac{\sqrt{-19}}{c}$$

Esse número complexo é diferente de 0 e tem norma

$$d(\frac{x}{y} \cdot z - w) = (\frac{r}{c})^2 + (\frac{\sqrt{19}}{c})^2 = \frac{(r^2 + 19)}{c^2}$$

que é menor que 1 desde que $|r| \leq \frac{c}{2}$ e $c \geq 5$. O único caso que não é obvio é $c = 5$, mas então $|r| \leq 2$ de modo que $r^2 + 19 \leq 23 < c^2$.
As possibilidades restantes são $c = 2,\ 3$ ou 4.:
(i) Se $c = 2$, $y \nmid x$ e $(a, b, c) = 1$ implica que a e b são de paridades opostas (pois caso contrário $y|x$). Seja $z = 1$ e $w = \frac{[(a-1)+b\sqrt{-19}]}{2} \in R$. Assim

$$\frac{x}{y} \cdot z - w = \frac{a + b\sqrt{-19}}{2} \cdot 1 - \frac{[(a-1) + b\sqrt{-19}]}{2}$$

$$= \frac{a + b\sqrt{-19} - a + 1 - b\sqrt{-19}}{2} = \frac{1}{2} \neq 0$$

e tem norma menor que 1.
(ii) Se $c = 3$, $(a, b, c) = 1$ implica que $a^2 + 19b^2 \equiv a^2 + b^2 \not\equiv 0 (mod\ 3)$. Seja $z = a - b\sqrt{-19}$ e $w = q$ onde $a^2 + 19b^2 = 3q + r$ com $r = 1$ ou $r = 2$. Assim

$$\frac{x}{y} \cdot z - w = \frac{a + b\sqrt{-19}}{3} \cdot (a - b\sqrt{-19}) - q$$

$$= \frac{a^2 + 19b^2}{3} - q = \frac{a^2 + 19b^2 - 3q}{q}$$

$$= \frac{3q + r - 3q}{3} = \frac{r}{3} \neq 0$$

e tem norma menor que 1.
(iii) Se $c = 4$, a e b não são ambos pares, Se eles são de paridade oposta $a^2 + 19b^2 \equiv a^2 - b^2 \not\equiv 0 (mod\ 4)$. Seja $z = a - b\sqrt{-19}$ e $w = q$ onde $a^2 + 19b^2 = 4q + r$ com $0 < r < 4$. Assim

$$\frac{x}{y} \cdot z - w = \frac{a + b\sqrt{-19}}{4} \cdot (a - b\sqrt{-19}) - q = \frac{a^2 + 19b^2 - 4q}{4}$$

$$= \frac{r}{4} \neq 0$$

e tem norma menor que 1.
Se a e b ambos ímpares, $a^2 + 19b^2 \equiv a^2 + 3b^2 \not\equiv 0$ (mod 8. Sejam $z = fraca - b\sqrt{-19}2$ e $w = q$, onde $a^2 19b^2 = 8q + r$, $0 < r < 8$. Assim

$$\frac{x}{y} \cdot z - w = \frac{a + b\sqrt{-19}}{4} \cdot fraca - b\sqrt{-19}2 - q$$

$$\frac{a^2 + 19b^2}{8} - q = \frac{a^2 + 19b^2 - 8q}{8} = \frac{r}{8} \neq 0$$

e tem norma menor que 1.
Logo o anel R em questão satisfaz as condições do Teorema 5.1 e portanto R é um anel de ideais principais.

Afirmação: R não é um anel euclidiano
Para mostrarmos que o anel R em questão, que é um anel de ideais principais, não é um anel euclidiano precisamos de algumas definições e alguns resultados. A partir destes concluíremos que R não é um anel euclidiano.

Vamos considerar o conjunto R_0 como o conjunto de todos os elementos não zeros de um anel R, em símbolos, $R_0 = \{x \in R | x \neq 0\}$.

Definição 5.1 *Um subconjunto P de R_0 com a propriedade $PR_0 \subset P$, ou seja, xy é um elemento de P , $\forall x \in P$, $y \in R_0$, é chamado um ideal produto do anel R.*

Definição 5.2 *Se S é um subconjunto de um anel R, o conjunto derivado de S, denotado por S', é definido por*

$$S' = \{x \in S | y + xR \subset S, \text{ para algum } y \in R\}$$

Lema 5.1 *Se S é um ideal produto então S' também é um ideal produto.*

Demonstração: Se $x \in S'$ então $x \in S$ e existe $y \in R$ tal que $y + xR \subset S$. Seja $z \in R_0$. Como S é um ideal produto temos que $SR_o \subset S$ e $x \in S$, logo $xz \in S$. Além disso, $(y + (xz)R) \subset (y + xR) \subset S$. Logo mostramos que se $xz \in S'R_0$, obtemos que $xz \in S$ e que $y + (xz)R \subset S$, ou seja, $xz \in S'$. Portanto $S'R_0 \subset S'$, ou seja, S' é um ideal produto.

Lema 5.2 *Se $S \subset T$ então $S' \subset T'$.*

Demonstração Seja $x \in S'$, logo existe $y \in R$ tsl que $(y + xR) \subset S$, mas por hipótese $S \subset T$ o que implica que $(y + xR) \subset T$. Assim $x \in T'$ e portanto $S' \subset T'$.

Teorema 5.2 *Se R é um anel euclidiano, então existe uma sequência , $\{P_n\}$ de ideais produtos com a seguinte propriedades:*
(1)$R_0 = P_0 \supset P_1 \supset P_2 \supset \cdots \supset P_n \supset \cdots$
(2)$\cap P_n = \emptyset$
(3)$P_n^{'} \subset P_{n+1}$
(4) Para cada n, $R_0^{(n)}$, o n-ésimo conjunto derivada de R_0, é um subconjunto de P_n.

Demostração: Considere a norma euclidiana $d(x)$ em R, para $x \in R_0$. Para cada inteiro n não negativo, defina $P_n = \{x \in R_0 | d(x) \geq n\}$. Suponha que $x \in P_n$ e $y \in R_0$, então $d(xy) \geq d(x) \geq n$ o que implica que $xy \in P_n$, ou seja, $P_n R_0 \subset P_n$, isto é, P_n é um ideal produto. Temos que P_n define uma sequência $\{P_n\}$ que claramente satisfaz as condições (1) e (2). Vamos mostrar as condições (3) e (4).
(3): Seja $x \in P_n^{'}$, logo existe $y \in R$ tal que $y + xR \subset P_n'$. Aplicando o algoritmo de Euclides (pois R é um anel euclidiano) existem $q, r \in R$ tais que

$$y = xq + r, \quad r = 0 \ \ ou \ \ d(r) < d(x).$$

Assim

$$r = y + x(-q) \Rightarrow r \in y + xR$$

isso implica que $d(r) \geq n$ e assim $d(x) > d(r) \geq n$, de modo que $d(x) \geq n + 1$, ou seja, $x \in P_{n+1}$. Portanto $P_n' \subset P_{n+1}$.
(4): Temos que $R_0 = \{x \in R | x \neq 0\}$, logo $\forall x \in R_0$ temos que $d(x) \geq 0$ e $P_0 = \{x \in R | d(x) \geq 0\}$. Assim, $R_0 = P_0$. Então de (3) temos que $R_0' = P_0' \subset P_1$. Assumindo que $R_0^{(n)} \subset P_n$, pelo Lema5.2 e condição (3) temos que $R_0^{(n+1)} \subset P_n' \subset P_{n+1}$. Assim por indução obtemnos a condição (4).

Corolário 5.1 *Se $R_0' = R_0'' \neq \emptyset$ então R não é um anel euclidiano.*

Demonstração: A hipótese do corolário implica que para todo n, $R_0^{(n)} = R_0'$. Suponha por absurdo que R é um anel euclidiano, então do Teorema5.2 temos que $R_0' = \cap R_0^{(n)} \subset \cap P_n = \emptyset$. O que é uma contradição pois por hipótese $R_0' \neq \emptyset$. Portanto R não é um anel

euclidiano.

Usaremos o Corolário5.1 para provar que $R = \{a + b(1 + \sqrt{-19})/2 | a, b \in \mathbb{Z}\}$ não é uma anel euclidiano, mesmo sendo um anel de ideias principais. Mostraremos que $R_0' = R_0'' \neq \emptyset$ e assim R não será um anel euclidiano.

Primeiramente, vamos determinar R_0'. Se x é uma unidade em R, digamos $xy = 1$ e z um elemento de R, $z + x(-yz) = 0 \notin R_0$. Isso mostra que unidades de R não estão em R_0', lembrando que $R_0' = \{x \in R_0 | y + xR \subset R_0, y \in R\}$. Se x não é uma unidade em R, então usando $z = -1$, $z + xy \neq 0$, $\forall y \in R$ (pois caso contrário, existiria $y \in R$ tal que $xy = 1$, contráriando o fato de x não ser unidade), o que demonstra que se $x \neq 0$ e x uma não unidade de R então $x \in R_0'$. Assim, completamente, R_0' é precisamente o conjunto de todos os elementos de R que não são zero e nem unidades. Notemos que as únicas unidades de $R = \{a + b(1 + \sqrt{-19})/2 | a, b \in \mathbb{Z}\}$ são 1 e -1.
Para encontrarmos os elementos de R_0'' com $R = \{a + b(1 + \sqrt{-19})/2 | a, b \in \mathbb{Z}\}$, vamos usar a seguinte terminologia:

Definição 5.3 *Um elemento $x \in R_0'$ é dito ser um divisor lateral de $y \in R$ se existe $z \in R$, $z \notin R_0'$ tal que $x|(y + z)$. Um elemento $x \in R_0$ é um divisor lateral universal se ele é um divisor lateral de todo elemento de R.*

Agora, seja $x \in R_0''$ então $x \in R_0'$ e existe $y \in R$ tal que $y + xR \subset R_0'$, ou seja, x nunca divide $y + z$ se z é 0 ou uma unidade de R. Assim x não é um divisor lateral de y e portanto não será um divisor lateral universal. Reciprocamente, se $x \notin R_0''$ e $x \in R_0'$ então para cada $y \in R$ existe um $w \in R$ com $y + xw \notin R_0'$, ou sejja, $y + xw$ é zero ou uma unidade e portanto x é um divisor lateral de y. Como isso vale para cada $y \in R$, então x será um divisor lateral universal. Juntos os dois argumentos mostram que R_0'' é o conjunto R_0' exclusivo dos divisores laterais universais. Vamos mostrar que R não tem divisores laterais universais. Um divisor lateral de 2 em $R = \{a+b(1+\sqrt{-19})/2 | a, b \in \mathbb{Z}\}$ deve ser um divisor não unidade de 2 ou 3. Em R, 2 e 3 são irredutíveis e portanto os únicos divisores laterais de 2 sao 2, -2, 3 e -3. Por outro lado, um divisor de $\frac{(1+\sqrt{-19})}{2}$ deve ser um divisor não unidade de $\frac{(1+\sqrt{-19})}{2}$, $\frac{(3+\sqrt{-19})}{2}$ ou $\frac{(-1+\sqrt{-19})}{2}$. Esses elementos de R tem norma 5, 7 e 5, respectivamente, enquanto as normas de 2 e 3 e seus associados são 4 e 9, respectivamente. Assim com esse resultado, nenhum divisor lateral de 2 é um divisor lateral universal de $\frac{1+\sqrt{-19}}{2}$. Logo não existem divisores laterais universais em R.

Portanto, concluímos que para o anel de ideais principais $R = \{a+b(1+\sqrt{-19})/2 | a, b \in$

$\mathbb{Z}\}$, temos que $R_0' = R_0'' \neq \emptyset$ e assim pelo Corolário5.1, $R = \{a+b(1+\sqrt{-19})/2 | a, b \in \mathbb{Z}\}$ não é um anel euclidiano. Assim atingimos o objetivo dessa monografia.

Referências

[1] Wilson, J. C.: A Principal Ideal Ring That is Not a Euclidean Ring; Mathematics Magazine, Vol. 46, No. 1 (Jan., 1973), pp. 34-38.

[2] Hernstein, I. N.: Tópicas de Álgebra;Editora USP e Poligono, 1970- São Paulo.