UNIVERSIDADE DA BEIRA INTERIOR
Ciências

Anéis Filiais

Tânia Cristina Gonçalves Robalo Chouzal

Relatório de Estágio para obtenção do Grau de Mestre em
Ensino de Matemática no 3.° Ciclo do Ensino Básico e no Ensino Secundário
(2.° ciclo de estudos)

Orientador: Prof. Doutora Deolinda Isabel da Conceição Mendes

Covilhã, Outubro de 2011

Agradecimentos

Os meus agradecimentos à minha orientadora, Professora Doutora Deolinda Isabel da Conceição Mendes, pela sua inteira disponibilidade em acompanhar e orientar o presente trabalho.

Ao Professor Doutor Rui Manuel Pires Almeida pela ajuda disponibilizada.

Um agradecimento especial aos meus pais e ao meu marido, pela amizade e companheirismo, pelo apoio, incentivo e perseverança constante.

Resumo

O nosso principal objectivo é estudar o trabalho de G. Ehrlich e também de R. Andruszkiewicz e E.R. Puczylowski no que concerne aos anéis filiais, isto é, anéis em que a relação de ideal é transitiva. Começamos por resumir algum material de base que será usado ao longo do trabalho. Em particular, referimo-nos a anéis primos e semiprimos, ao Radical de Jacobson e algumas das suas propriedades; apresentamos a construção de um anel de fracções a partir de um anel comutativo e registamos algumas propriedades da estrutura dos seus ideais. Além disso, recordamos algumas definições básicas e conceitos acerca dos domínios de ideais principais e dos domínios de factorização única. Em seguida, definimos anel filial e apresentamos vários exemplos. São dadas várias caracterizações de anéis filiais e, em particular, de anéis filiais semiprimos, Artinianos e nilpotentes. Também é investigada a filialidade de domínios de integridade. Por último, é apresentada uma ligação entre os grupos abelianos e os anéis filiais.

Palavras-chave

Anel, anel filial, domínio de integridade, anel de fracções.

Abstract

Our main objective is to study the work of G. Ehrlich and also of R. Andruszkiewicz and E.R. Puczylowski concerning filial rings; that is, rings in which the ideal relation is transitive. We begin by summarizing some basic material which will be used in the sequel. In particular, we refer to prime and semiprime rings, to the Jacobson radical and to some of their properties; we present the construction of a ring of fractions of a commutative ring and note some properties of its ideal structure. In addition, we recall some basic definitions and concepts concerning principal ideal domains and unique factorization domains. Next, we define a filial ring and present various examples. Several characterizations of filial rings are given and, in particular, of semiprime, Artinian and nilpotent filial rings. Filiality of integral domains is also investigated. Finally, a link between abelian groups and filial rings is presented.

Keywords

Ring, filial ring, integral domain, ring of quotients.

Conteúdo

Introdução

Este trabalho tem como objectivo analisar resultados sobre os anéis filiais. Ehrlich introduziu os anéis filiais e as suas principais conclusões concernem aos anéis comutativos. Posteriormente, Andruszkiewicz e Puczylowski estenderam o seu estudo aos anéis filiais não comutativos. Os seus artigos serviram de base para a redacção deste trabalho.

No que respeita à estrutura, o trabalho encontra-se dividido em duas partes. Na primeira parte, relembramos algumas definições e propriedades dos anéis. Além disso, apresentamos determinados resultados relativos ao radical de Jacobson. Recordamos a construção de um anel de fracções a partir de um anel comutativo. Por fim, referimos alguns conceitos relativos aos domínios de ideais principais e aos domínios de factorização única. A segunda parte é dedicada ao estudo dos anéis filiais, anéis que satisfazem a condição de transitividade para ideais. São apresentados alguns exemplos, propriedades e caracterizações deste tipo de anéis. Em particular, são abordados os domínios de integridade filiais. Por fim, caracterizam-se os grupos abelianos em termos de anéis filiais.

Capítulo 1

Preliminares

Neste trabalho pressupomos adquiridos conhecimentos básicos da teoria de conjuntos, teoria de números, teoria de grupos e de anéis. Começamos, porém, por relembrar conceitos e resultados da teoria dos anéis necessários ao estudo do próximo capítulo e estes podem encontrarem-se em ([6], [7] e [5]).

1.1 Conceitos gerais de anéis

Um *anel* é um sistema algébrico $(R, +, \cdot)$ constituído por um conjunto R, não vazio, e duas operações binárias, adição $(+)$ e multiplicação $(\cdot)$, definidas em R, satisfazendo:

(i) R é um grupo abeliano relativamente à adição;

(ii) a operação multiplicação é associativa:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

para todos os elementos $a, b, c \in R$;

(iii) a multiplicação é distributiva relativamente à adição:

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (b + c) \cdot a &= (b \cdot a) + (c \cdot a) \end{aligned}$$

para todos os elementos $a, b, c \in R$.

O produto $a \cdot b$ dos elementos a e b de R será representado por ab. O anel $(R, +, \cdot)$, que também se diz um anel em relação às operações binárias $+$ e $\cdot$, será denotado simplesmente por R. A identidade de R, relativamente à adição, é designada por 0 e diz-se o zero do anel.

O *anel* R diz-se *comutativo* quando a multiplicação é comutativa:

$$ab = ba$$

para todos os elementos $a, b \in R$.

Dizemos que um anel R é um *anel com identidade* quando existe em R um elemento, designado por 1, que é identidade para a multiplicação:

$$1a = a = a1$$

para todo o $a \in R$.

Se R for um anel com identidade 1, então $a \in R$ diz-se uma *unidade* se existir $a' \in R$ tal que $aa' = a'a = 1$. O elemento a' designa-se por *inverso* de a e denota-se por a^{-1}.

Um elemento $a \neq 0$ de um anel R diz-se divisor de zero à esquerda (respectivamente à direita) se existir $0 \neq b \in R$ tal que $ab = 0$ (respectivamente $ba = 0$). Um *divisor de zero* é um elemento que é divisor de zero à esquerda ou à direita.

Um anel comutativo R, com identidade $1 \neq 0$ e sem divisores de zero, designa-se por *domínio de integridade*. Um anel R, com identidade $1 \neq 0$ e tal que todos os elementos diferentes de zero são unidades, denomina-se *anel de divisão*. Um *corpo* é um anel de divisão comutativo.

Exemplo 1.1.1

(i) Os conjuntos dos números inteiros ($\mathbb{Z}$)*, racionais* ($\mathbb{Q}$)*, reais* ($\mathbb{R}$) *e complexos* ($\mathbb{C}$)*, com as correspondentes operações usuais de adição e multiplicação, são anéis.*

(ii) O conjunto dos inteiros de Gauss, $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$*, com a multiplicação e adição usuais de números complexos é um domínio de integridade.*

(iii) Os conjuntos $\mathbb{Z}_n$ *(n inteiro positivo), das classes de congruência módulo n, com as operações de adição e multiplicação módulo n, são anéis. Verifica-se que* $\mathbb{Z}_n$ *é um corpo se e só se n é primo.*

(iv) O conjunto $R[x]$ *de todos os polinómios na indeterminada x com coeficientes pertencentes a um anel R, onde para* $f(x) = a_0 + a_1x + a_2x^2 + ...$ *e* $g(x) = b_0 + b_1x + b_2x^2 + ...$*, elementos arbitrários de* $R[x]$*, se definem as operações:*

$$\begin{aligned} f(x) + g(x) &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + ... \\ f(x)\, g(x) &= c_0 + c_1x + c_2x^2 + ... \end{aligned}$$

onde $c_i = a_0b_i + a_1b_{i-1} + ... + a_ib_0$*, para cada* $i = 0, 1, ...$ *é um anel.* $R[x]$ *é um anel comutativo e com identidade se o anel R for comutativo e com identidade. Além disso, se R é um domínio de integridade, então* $R[x]$ *também é um domínio de integridade.*

(v) *Dado um anel R, o conjunto $M_n(R)$ das matrizes $n \times n$ (n inteiro positivo) com elementos pertencentes a R, relativamente à adição e multiplicação usuais de matrizes, é um anel não comutativo. Se R é um anel com identidade então $M_n(R)$ tem identidade, nomeadamente a matriz identidade.*

Num anel R, se existir um inteiro positivo n tal que $na = 0$, para todo o $a \in R$, então o menor inteiro positivo, caso exista, com esta propriedade chama-se *característica de R*. Se não existir um tal inteiro positivo, diz-se que R tem característica zero. É bem conhecido que se R é um domínio de integridade de característica $n > 0$, então n é um número primo. Por exemplo, $\mathbb{Z}_p$ (p primo) tem característica p, enquanto que os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ têm característica 0.

Seja S um subconjunto não vazio, de um anel R. S diz-se um *subanel* de R se for um anel relativamente às operações de adição e multiplicação definidas em R. É imediato verificar que S é um subanel de R se e só se para quaisquer elementos $a,\ b \in S$, se tem $a - b \in S$ e $ab \in S$.

Seja F um corpo. Um seu subanel K diz-se um *subcorpo* (respectivamente, *subdomínio*) de F quando tem a estrutura de corpo (respectivamente domínio de integridade). Quando K é um subcorpo de F também se diz que F é uma *extensão do corpo K*.

Entre os subanéis de um anel, os ideais têm um papel importante.
Um subanel A de um anel R, denomina-se por *ideal esquerdo* se

$$rx \in A, \text{para quaisquer } r \in R \text{ e } x \in A$$

e denomina-se por *ideal direito* se

$$xr \in A, \text{para quaisquer } r \in R \text{ e } x \in A.$$

A diz-se um *ideal* (bilateral), e escreve-se abreviadamente $A \lhd R$, se é simultaneamente ideal esquerdo e direito de R.

Exemplo 1.1.2 *No caso do anel dos inteiros $\mathbb{Z}$, todos os seus subaneis $n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$, n inteiro, são ideais.*

Um anel R tem sempre pelo menos dois ideais, o ideal nulo e o próprio anel, designados por ideais triviais. Os ideais de R, diferentes de R, dizem-se ideais próprios. Um *anel* denomina-se *simples* se não tiver ideais próprios.

Exemplo 1.1.3 *Qualquer anel de divisão é um anel simples. De facto, seja R um anel de divisão e $I \neq 0$ um ideal de R. Tomemos em I um elemento $x \neq 0$. Como R é um anel de divisão, x é uma unidade e $x^{-1}x = 1 \in I$, pelo que, $I = R$.*

Entre os anéis simples encontram-se aqueles que não têm ideais direitos (esquerdos) não triviais. Prova-se que estes são anéis de divisão ou anéis com multiplicação nula (o produto de quaisquer dois elementos do anel é zero) com um número primo de elementos.

Seja $\{A_i : i \in \Lambda\}$, onde $\Lambda = \{1, 2, ..., n\}$, isto é, uma família finita de subconjuntos não vazios de um anel R. Definimos a soma e o produto destes subconjuntos como sendo, respectivamente:

$$\sum_{i\in\Lambda} A_i = A_1 + A_2 + ... + A_n = \{a_1 + a_2 + ... + a_n : a_i \in A_i,\, i \in \Lambda\}.$$

e

$$A_1A_2...A_n = \left\{ \sum_{finita} a_1a_2...a_n : a_i \in A_i,\, i \in \Lambda \right\}.$$

Se A consiste num único elemento a, escrevemos aB em vez de AB. Semelhantemente, se $B = \{b\}$, escrevemos Ab em vez de AB. No caso particular em que $A_1 = A_2 = ... = A_n = A$ escrevemos $A_1A_2...A_n$ abreviadamente por A^n. Em particular, se $A_1, A_2, ..., A_n$ são ideais de um anel R, então $A_1 + A_2 + ... + A_n$ e $A_1A_2...A_n$ são ideais de R.

No caso de termos uma família infinita de ideais de R, $\{A_i : i \in \Lambda\}$, a soma é definida por:

$$\sum_{i\in\Lambda} A_i = \left\{ a \in R : a \in \sum_{i\in\Lambda_0} A_i, \text{ para algum subconjunto finito } \Lambda_0 \text{ de } \Lambda \right\}.$$

Verifica-se que $\sum_{i\in\Lambda} A_i$ ainda é um ideal de R.

A intersecção de uma família arbitrária de ideais de um anel R ainda é um ideal de R. Seja K um subconjunto de um anel R. A intersecção I de todos os ideais que contêm K designa-se por *ideal gerado* por K. Este é o menor ideal de R que contém K, no seguinte sentido: para qualquer $J \lhd R$ tal que $K \subseteq J$ verifica-se que $I \subseteq J$.

Um ideal que pode ser gerado por um único elemento, designa-se por *ideal principal*. O ideal de R gerado por $a \in R$, denotado por $(a)_R$ (ou simplesmente por (a)), é dado por $(a)_R = \mathbb{Z}a + aR + Ra + RaR$. Em particular, se R é um anel comutativo e com identidade, então $(a)_R = Ra = aR$.

O resultado que a seguir apresentamos é de bastante utilidade no que respeita à ausência de transitividade para ideais.

Lema 1.1.4 (Lema de Andrunakievich) *Seja R um anel. Se I é um ideal de R, e J é um ideal de I, então*

$$(J_R)^3 \subseteq J$$

onde J_R denota o ideal de R gerado por J.

Demonstração: É claro que $J_R = J + RJ + JR + RJR$. Assim,

$$(J_R)^3 \subseteq IJ_RI = I\left(J + RJ + JR + RJR\right)I \subseteq IJI \subseteq J.$$

■

Seja R um anel e A um ideal de R, então o conjunto

$$R/A = \{x + A : x \in R\}$$

com as operações assim definidas:

$$(x + A) + (x' + A) = (x + x') + A$$

e

$$(x + A)(x' + A) = xx' + A,$$

para quaisquer $x,\ x' \in R$, é um anel, designado por *anel quociente* de R por A.

Para os anéis R e R', uma aplicação $\varphi : R \to R'$ diz-se um *homomorfismo* quando se verificam as seguintes condições

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = \varphi(a)\varphi(b)$$

para quaisquer $a, b \in R$.

Um homomorfismo injectivo (respectivamente: sobrejectivo, bijectivo) chama-se um *monomorfismo* (respectivamente: *epimorfismo*, *isomorfismo*). No caso de $R = R'$, dizemos que se trata de um *endomorfismo*. Quando existe um isomorfismo de R para R', dizemos que o anel R é isomorfo ao anel R' e escrevemos abreviadamente $R \cong R'$.

O *núcleo de um homomorfismo* $\varphi : R \to R'$, denotado por $Nuc(\varphi)$, é o ideal de R assim definido:

$$Nuc(\varphi) = \{a \in R : \varphi(a) = 0\}.$$

A *imagem de um homomorfismo* $\varphi : R \to R'$, denotada por Im φ, é o subanel de R' definido por:

$$\text{Im}\ \varphi = \{\varphi(a) : a \in R\}.$$

Sejam R um anel e A um ideal de R. A aplicação $\pi : R \to R/A$ definida por $\pi(a) = a + A$, para todo o $a \in R$ é um epimorfismo, que se diz o *homomorfismo natural* de R sobre R/A e $Nuc(\pi) = A$.

Sejam R um anel e I um ideal de R. Então I' é um ideal do anel quociente R/I se e só se I' é da forma J/I, onde J é um ideal de R que contém I.

De seguida recordamos dois teoremas importantes relativos a homomorfismos.

Teorema 1.1.5 (Teorema Fundamental dos Homomorfismos) *Seja $\varphi : R \to R'$ um homomorfismo de anéis. Então*

$$R/Nuc(\varphi) \cong \varphi(R).$$

Teorema 1.1.6 *Sejam I e J ideais de um anel R tais que $I \subseteq J$. Então*

$$(R/I) / (J/I) \cong R/J.$$

Um anel R' diz-se *imagem homomorfica* de um anel R, se existe um epimorfismo de R para R'. De acordo com o Teorema Fundamental dos Homomorfismos, toda a imagem homomorfica de um anel R é isomorfa a R/I, para algum ideal I de R. Se $I \neq 0$, o anel R/I diz-se imagem homomorfica própria de R.

Um anel R diz-se *imerso* no anel S, quando existe um monomorfismo de R para S. Assim, o anel R pode ser imerso no anel S se existir um subanel T de S tal que $R \cong T$. Diz-se também que S é uma *extensão do anel* R.

É importante observar que todo o anel R pode ser imerso num anel $R^{\#}$ com identidade. De facto, o anel $R^{\#} = R \times \mathbb{Z}$ com as operações assim definidas

$$(a, m) + (b, n) = (a + b, m + n)$$

e

$$(a, m)\,(b, n) = (ab + na + mb, mn)$$

para todo o a, $b \in R$ e todo o m, $n \in \mathbb{Z}$, é um anel com identidade $(0, 1)$ que contém R como ideal. O anel $R^{\#}$ diz-se a extensão natural de R a um anel com identidade.

Um ideal (ideal direito, ideal esquerdo) I de um anel R, diz-se um *ideal* (ideal direito, ideal esquerdo) *minimal* de R, se $I \neq 0$ e para qualquer ideal (ideal direito, ideal esquerdo) J de R, $J \subseteq I$ implica $J = 0$ ou $J = I$.

Um ideal I (ideal direito, ideal esquerdo) de um anel R, diz-se um *ideal* (ideal direito, ideal esquerdo) *maximal* de R, se $I \neq R$ e para qualquer ideal (ideal direito, ideal esquerdo) J de R, $I \subseteq J$ implica $J = I$ ou $J = R$.

Se num anel R toda a sequência decrescente de ideais direitos (esquerdos) de R,

$$A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots$$

for estacionária, isto é, se existir um número natural n tal que $A_i = A_n$, para qualquer $i \geq n$, dizemos que a *condição de cadeia descendente* para ideais direitos (esquerdos), é satisfeita em R.

Um anel R que satisfaz a para ideais direitos (esquerdos), diz-se um anel Artiniano direito (esquerdo). Um *anel* diz-se *Artiniano* se for anel Artiniano direito e esquerdo.

Exemplo 1.1.7 *Um anel de divisão D é Artiniano, uma vez que os seus únicos ideais direitos e esquerdos são os triviais.*

Notamos que toda a imagem homomorfica de um anel Artiniano ainda é um anel Artiniano.

Seja $\{R_i : i \in \Lambda\}$ uma família arbitrária de anéis. O conjunto

$$R = \prod_{i \in \Lambda} R_i = \{(\ldots, a_i, \ldots) : a_i \in R_i, i \in \Lambda\}$$

com as operações

$$(\ldots, a_i, \ldots) + (\ldots, b_i, \ldots) = (\ldots, a_i + b_i, \ldots)$$

e

$$(\ldots, a_i, \ldots)\,(\ldots, b_i, \ldots) = (\ldots, a_i b_i, \ldots)$$

é um anel que se diz *soma directa completa dos anéis* R_i, $i \in \Lambda$.

O subanel

$$S = \sum_{i \in \Lambda}{}^{\oplus} R_i = \{(\ldots, a_i, \ldots) : a_i \neq 0 \text{ para apenas um número finito de } i \in \Lambda\}$$

de R chama-se a *soma directa dos anéis* $R_i, i \in \Lambda$. Se Λ é um conjunto finito, $\Lambda = \{1, ..., k\}$, então $\sum_{i \in \Lambda}{}^{\oplus} R_i$ também se escreve na forma $R_1 \oplus R_2 \oplus ... \oplus R_k$.

Cada anel R_i pode ser imerso, como um ideal, em R e S respectivamente através da correspondência

$$a_i \to (\ldots, 0, a_i, 0, \ldots)\,.$$

Portanto, as parcelas R_i podem considerar-se como ideais de R e de S, respectivamente. Se o conjunto Λ de índices é finito, então é claro que $R = S$.

Seja $\{A_i : i \in \Lambda\}$ uma família de ideais de um anel R, onde Λ é um conjunto não vazio e finito. Então R diz-se *soma directa interna dos* A_i, se

$$R = \sum_{i \in \Lambda} A_i$$

e

$$A_i \cap \left(\sum_{j \in \Lambda \setminus \{i\}} A_j \right) = 0$$

para cada $i \in \Lambda$.

Note-se que, se R é soma directa interna dos ideais A_i, $i \in \Lambda$, e S é soma directa dos A_i, $i \in \Lambda$, então $R \cong S$.

Seja T um subanel da soma directa completa R dos anéis R_i, $i \in \Lambda$. Para cada $i \in \Lambda$, seja π_i o homomorfismo de R sobre R_i definido por $\pi_i(a) = a_i$, para cada $a = (..., a_i, ...) \in R$. Se $\pi_i(T) = R_i$, para cada $i \in \Lambda$, T designa-se por *soma subdirecta dos anéis* R_i, $i \in \Lambda$.

Como um caso especial, temos que a soma directa completa dos anéis R_i, $i \in \Lambda$ é uma soma subdirecta desses anéis.

Teorema 1.1.8 *Um anel R é isomorfo a uma soma subdirecta de anéis R_i, $i \in \Lambda$, se e só se, para cada $i \in \Lambda$, existe em R um ideal K_i tal que $R/K_i \cong R_i$ e $\bigcap_{i\in\Lambda} K_i = 0$.*

Seja A um *ideal* do anel R. O ideal A diz-se *nilpotente* se existe um inteiro positivo n tal que $A^n = 0$. Se n é o menor inteiro positivo tal que $A^n = 0$, diz-se que A é nilpotente de índice n.

Um elemento $a \in R$ diz-se nilpotente se existir um inteiro positivo n tal que $a^n = 0$. Se todos os elementos de A são nilpotentes, dizemos que A é um *ideal nil* de R. Em particular, se todos os elementos de R são nilpotentes, então R designa-se por *anel nil*.

Todo o ideal nilpotente é nil. Em geral, o recíproco não se verifica, como mostra o seguinte exemplo.

Exemplo 1.1.9 ([3], Exemplo 3) *Seja F um corpo. Consideremos o conjunto de todos os símbolos x_α onde $\alpha \in \mathbb{Q}$ e $0 < \alpha < 1$. Seja*

$$A = \left\{ \sum_{finita} a_\alpha x_\alpha : a_\alpha \in F,\ \alpha \in \mathbb{Q},\ 0 < \alpha < 1 \right\}.$$

A adição é definida de forma usual e $a_\alpha x_\alpha + a'_\alpha x_\alpha = (a_\alpha + a'_\alpha)\, x_\alpha$. A multiplicação destes elementos é definida por

$$x_\alpha x_\beta = x_{\alpha+\beta},\ \text{se } \alpha + \beta < 1,$$

e

$$x_\alpha x_\beta = 0,\ \text{se } \alpha + \beta \geq 1.$$

É claro que A é um anel comutativo e todo o elemento em A é nilpotente. De facto, para qualquer inteiro n maior que $1/\alpha$, $(x_\alpha)^n = 0$ e $\left(\sum_{finita} a_\alpha x_\alpha \right)^k = 0$, onde k é um inteiro maior que $1/\alpha$, sendo α o menor dos índices desta soma finita. Então A é um anel nil. Contudo, A não é nilpotente, pois $x_{1/2} \cdot x_{1/4} \cdot x_{1/8} ... x_{1/2^n} ... \neq 0$. De facto $A^2 = A$, pois para qualquer α dado, existe um β tal que $x_\beta x_\beta = x_\alpha$. Tomemos qualquer elemento x_α e consideremos o ideal (x_α). Este é um ideal nilpotente, pois $(x_\alpha)^n = 0$, para qualquer inteiro $n > 1/\alpha$. O anel A coincide com a soma de todos os ideais da forma (x_α) e não é nilpotente. A reunião de todos os ideais (x_α) preenche todos os A e assim, a reunião dos ideais nilpotentes de A não é um ideal nilpotente.

Um *ideal* próprio P de um anel de R diz-se *primo* se, para todos os ideais A e B de R, $AB \subseteq P$ implica $A \subseteq P$ ou $B \subseteq P$. No caso do anel R ser comutativo, um ideal próprio é primo se e só se para quaisquer a, $b \in R$, $ab \in P$ implica $a \in P$ ou $b \in P$.

Um *anel* R diz-se *primo* se o ideal nulo é um ideal primo de R.

O seguinte teorema apresenta condições equivalentes à definição de ideal primo.

Teorema 1.1.10 *Se $P \neq R$ é um ideal de um anel R, as seguintes condições são equivalentes:*

(i) *P é um ideal primo;*

(ii) *se $a,\ b \in R$ tal que $aRb \subseteq P$, então $a \in P$ ou $b \in P$;*

(iii) *se $(a)_R$ e $(b)_R$ são ideais principais de R tais que $(a)_R(b)_R \subseteq P$, então $a \in P$ ou $b \in P$;*

(iv) *se U e V são ideais direitos de R tais que $UV \subseteq P$, então $U \subseteq P$ ou $V \subseteq P$;*

(v) *se U e V são ideais esquerdos de R tais que $UV \subseteq P$, então $U \subseteq P$ ou $V \subseteq P$.*

Demonstração: (i) implica (ii). Seja $aRb \subseteq P$. Como P é um ideal de R, segue que $RaRbR \subseteq RPR \subseteq P$ e por conseguinte $(RaR)(RbR) \subseteq RaRbR \subseteq P$. Uma vez que RaR e RbR são ideais e $(RaR)(RbR) \subseteq P$, a condição (i) implica que $RaR \subseteq P$ ou $RbR \subseteq P$. Suponhamos que $RaR \subseteq P$. Se estabelecermos $A = (a)_R$, segue que $A^3 \subseteq RaR \subseteq P$ e, usando novamente (i), temos $A \subseteq P$ e $a \in P$. Semelhantemente, se $RbR \subseteq P$, vem que $b \in P$, e a condição (ii) está estabelecida.

(ii) implica (iii). Se $(a)_R(b)_R \subseteq P$, segue que $aRb \subseteq (a)_R(b)_R \subseteq P$ e (ii) implica que $a \in P$ ou $b \in P$.

(iii) implica (iv). Sejam U e V ideais direitos de R tal que $UV \subseteq P$. Vamos supor que $U \nsubseteq P$, de forma a provarmos que $V \subseteq P$. Suponhamos que $u \in U$ com $u \notin P$, e que v é um elemento arbitrário de V. Uma vez que $(u)_R(v)_R \subseteq UV + RUV \subseteq P$ e $u \notin P$, a condição (iii) implica que $v \in P$. Por isso, $V \subseteq P$, e a condição (iv) está estabelecida.

De forma semelhante mostra-se que a condição (iii) implica a condição (v).

É trivial que tanto (iv) como (v) implicam (i).

■

Um *ideal* A de um anel R diz-se *semiprimo* se, para todo o ideal Q de R, $Q^2 \subseteq A$ implica $Q \subseteq A$. É claro que todo o ideal primo é semiprimo. Além disso, se A é um ideal semiprimo e Q é um ideal de R tal que $Q^n \subseteq A$, para algum inteiro positivo n, então é fácil verificar que $Q \subseteq A$.

Um *anel* R denomina-se *semiprimo* se o ideal nulo é um ideal semiprimo de R, ou seja, se A é um ideal de R tal que $A^2 = 0$, então $A = 0$.

Teorema 1.1.11 *Um ideal Q de um anel R é um ideal semiprimo em R se e só se o anel quociente R/Q não contém ideais nilpotentes não nulos.*

É possível provar resultados sobre os ideais semiprimos análogos aos dos ideais primos. Apresentamos o seguinte teorema, cuja demonstração é omitida, uma vez que, pode ser realizada com pequenas modificações à demonstração do Teorema 1.1.10.

Teorema 1.1.12 *Se Q é um ideal de um anel R, as seguintes condições são equivalentes:*

(i) Q *é um ideal semiprimo;*

(ii) se $a \in R$ *tal que* $aRa \subseteq Q$, *então* $a \in Q$;

(iii) se $(a)_R$ *é um ideal principal de* R *tal que* $(a)_R^2 \subseteq Q$, *então* $a \in Q$;

(iv) se U *é um ideal direito de* R *tal que* $U^2 \subseteq Q$, *então* $U \subseteq Q$;

(v) se U *é um ideal esquerdo de* R *tal que* $U^2 \subseteq Q$, *então* $U \subseteq Q$.

Corolário 1.1.13 *Para um anel R, as seguintes condições são equivalentes:*

(i) R *é um anel semiprimo;*

(ii) R *não contém ideais direitos nilpotentes não nulos;*

(iii) R *não contém ideais esquerdos nilpotentes não nulos;*

(iv) R *não contém ideais nilpotentes não nulos;*

(v) para $x \in R$, $xRx = 0$ *implica* $x = 0$.

Por fim, apresentamos o conceito de radical de Jacobson, o qual é importante no estudo da estrutura de anéis.

Um elemento a de um anel R diz-se *quasi-regular à direita* se existe um elemento $b \in R$ tal que $a + b - ab = 0$. Por sua vez, a diz-se *quasi-regular à esquerda* se existe um elemento $c \in R$ tal que $c + a - ca = 0$. Um elemento a diz-se *quasi-regular* se é quasi-regular à direita e quasi-regular à esquerda.

Um ideal (ideal direito, ideal esquerdo) é quasi-regular à direita se cada um dos seus elementos for quasi-regular à direita. Analogamente definimos os conceitos de ideal (ideal direito, ideal esquerdo) quasi-regular à esquerda e quasi-regular.

O *radical de Jacobson* de um anel R é o ideal

$$\mathfrak{J}(R) = \{a \in R : aR \text{ é quasi regular à direita}\}.$$

Teorema 1.1.14 $\mathfrak{J}(R)$ *é um ideal quasi-regular de R que contém todo o ideal quasi-regular à direita e todo o ideal quasi-regular à esquerda de R.*

De acordo com este teorema, podemos observar que $\mathfrak{J}(R)$ é o maior ideal quasi-regular de R e este pode ser caracterizado como a soma de todos os ideais quasi-regulares à direita de R (ou como soma de todos os ideais quasi-regulares à esquerda de R).

Todo o elemento nilpotente de um anel é quasi-regular. De facto, se a é um elemento de um anel R tal que $a^n = 0$ e $b = -\sum_{k=1}^{n-1} a^k$, então

$$\begin{aligned} a+b-ab &= a+(-a-a^2-\ldots-a^{n-1})-a(-a-a^2-\ldots-a^{n-1}) \\ &= a-a-a^2-\ldots-a^{n-1}+a^2+a^3+\ldots+a^n = a^n = 0. \end{aligned}$$

Deste modo temos:

Corolário 1.1.15 *$\mathfrak{J}(R)$ contém todos os ideais nil direitos e esquerdos de R.*

O radical de Jacobson, mesmo quando não é nulo, pode não conter nenhum elemento nilpotente não nulo, como se pode observar no exemplo seguinte.

Exemplo 1.1.16 *Seja S o anel dos números racionais que podem ser expressos da forma i/m, onde i é um inteiro arbitrário e m um inteiro ímpar. A equação*

$$\frac{2i}{m}+\frac{(-2i)}{m-2i}-\left(\frac{2i}{m}\right)\left(\frac{-2i}{m-2i}\right)=0$$

mostra que $2x$ é quasi-regular, para qualquer $x = \frac{i}{m}$ em S; logo $2 \in \mathfrak{J}(S)$. Obviamente, S não tem elementos nilpotentes não nulos, uma vez que é um subanel do corpo dos números racionais. Na realidade, $\mathfrak{J}(S)$ é o ideal de S gerado por 2.

Observamos que se I é um ideal de R então nem todo o ideal de I é ideal de R; no entanto, $\mathfrak{J}(I)$ é ideal de R.

Teorema 1.1.17 *Se I é um ideal de um anel R, então $\mathfrak{J}(I) = I \cap \mathfrak{J}(R)$.*

Se $\mathfrak{J}(R) = 0$, R diz-se *semisimples*. Seguidamente apresentamos uma caracterização dos anéis comutativos semisimples.

Teorema 1.1.18 *Um anel comutativo R com mais de um elemento, é isomorfo a uma soma subdirecta de corpos se e só se R é semisimples.*

1.2 Anéis de fracções

A construção do corpo dos números racionais a partir do anel dos inteiros é bem conhecida. Neste ponto, podemos observar como construir um anel de fracções a partir de um anel comutativo. Para tal, necessitamos de definir o conceito de conjunto multiplicativo.

Um *subconjunto* não vazio S de um anel R diz-se *multiplicativo* se

$$a, b \in S \text{ implica } ab \in S.$$

Exemplo 1.2.1

(i) O conjunto S de todos os elementos não nulos, de um anel R com identidade, que não são divisores de zero, é multiplicativo.

(ii) O conjunto de todas as unidades de um anel com identidade é multiplicativo.

(iii) Seja R um anel comutativo. Se P é um ideal primo de R, então P e $R - P$ são conjuntos multiplicativos.

Seja S um subconjunto multiplicativo de um anel comutativo R. A relação definida no conjunto $R \times S = \{(r, s) : r \in R \text{ e } s \in S\}$ por

$$(r, s) \sim (r', s') \text{ se e só se } s_1(rs' - r's) = 0, \text{ para algum } s_1 \in S$$

é uma relação de equivalência. Notamos que se R não tiver divisores de zero e $0 \notin S$ então $(r, s) \sim (r', s') \Leftrightarrow rs' - r's = 0$.

Denotaremos a classe de equivalência de $(r, s) \in R \times S$ por $\frac{r}{s}$ e o conjunto das classes de equivalência nesta relação por $S^{-1}R$.

É fácil a verificação de que $S^{-1}R$ com as operações abaixo definidas:

$$\frac{r}{s} + \frac{r'}{s'} = \frac{(rs' + r's)}{ss'}$$

e

$$\left(\frac{r}{s}\right)\left(\frac{r'}{s'}\right) = \frac{rr'}{ss'}$$

é um anel que se diz o *anel de fracções* de R por S.

Sejam R um anel comutativo e S o conjunto de todos os elementos de R que não são divisores de zero. Se S é não vazio (o que se verifica se R tem identidade), então $S^{-1}R$ diz-se o *anel de fracções (completo)* do anel R. Em particular, se S é o conjunto de todos os elementos não nulos de um domínio de integridade R, então o anel de fracções $S^{-1}R$ é um corpo, nomeadamente o corpo dos quocientes do domínio de integridade R, (ver [5]).

Para um anel R comutativo e com identidade e P ideal primo de R, $S = R - P$ é um conjunto multiplicativo de R, conforme referido no exemplo anterior. O anel de fracções $S^{-1}R$ também se diz localização de R com respeito a P e denota-se por R_P. Se I é um ideal de R então $S^{-1}I = \left\{\frac{a}{s} : a \in I,\ s \in S\right\}$ é um ideal de R_P, denotado por I_P.

Exemplo 1.2.2 *Sendo (p) o ideal de $\mathbb{Z}$ gerado por p, onde p é primo, temos que*

$$\mathbb{Z}_{(p)} = \left\{\frac{r}{s} \in \mathbb{Q} : (s, p) = 1\right\}$$

onde $(s, p) = 1$ significa que 1 é máximo divisor comum de s e p.

Se R é um anel comutativo e com identidade e P um ideal primo de R, então:

(i) existe uma correspondência biunívoca entre os ideais primos de R contidos em P e o conjunto dos ideais primos de R_P, dada por:

$$Q \longmapsto Q_P;$$

(ii) o ideal P_P de R_P é o único ideal maximal de R_P.

Um *anel local* é, por definição, um anel comutativo e com identidade que tem um único ideal maximal. Deste modo R_P é um anel local.

1.3 Domínios de ideais principais e domínios de factorização única

Neste ponto, R denota um anel comutativo e com identidade. Relembramos alguns conceitos relativos a estes anéis, que serão úteis nas demonstrações de teoremas do próximo capítulo.

Se todo o ideal de R é um ideal principal, então R diz-se um *anel de ideais principais*. Um domínio de integridade, que é anel de ideais principais, diz-se um *domínio de ideais principais*.

Dizemos que um *elemento* $a \in R - \{0\}$ *divide* um elemento $b \in R$ se existe $c \in R$ tal que $b = ac$ e nesse caso escreve-se a/b.

Sejam $a_1, a_2, ..., a_n$ elementos, não todos nulos, de R. Um elemento $0 \neq d \in R$ diz-se um *máximo divisor comum* de $a_1, a_2, ..., a_n$ se satisfizer as seguintes condi

(i) d/a_i para cada $i = 1, 2, ..., n$;

(ii) para todo o $0 \neq c \in R$ tal que c/a_i para cada $i = 1, 2, ..., n$, tem-se c/d.

Em particular, se R é um domínio de ideais principais, então existe um máximo divisor comum d de qualquer conjunto finito de elementos não nulos e não unidades $a_1, a_2, ..., a_n \in R$ e este pode escrever-se na forma

$$d = r_1a_1 + r_2a_2 + ... + r_na_n$$

com $r_1, r_2, ..., r_n \in R$.

Seja R um anel comutativo e com identidade. Um *elemento* $0 \neq p \in R$ diz-se *primo* se p não é uma unidade e, para a, $b \in R$, p/ab implica que p/a ou p/b. Dois *elementos* a, $b \in R$ dizem-se *associados* se $a = bu$, para alguma unidade $u \in R$.

Exemplo 1.3.1 *Consideramos o anel dos inteiros de Gauss* $\mathbb{Z}[i]$. *Para* $\alpha = a + bi \in \mathbb{Z}[i]$, *define-se a norma de* α, *como sendo* $n(\alpha) = a^2 + b^2$. *Recordemos que as unidades de* $\mathbb{Z}[i]$ *são* -1, $-i$, 1, i. *Todo o primo em* $\mathbb{Z}[i]$ *é associado de um dos seguintes primos (ver [2]):*

i) $1 + i$;

ii) π *ou* $\overline{\pi}$, *onde a norma é um número primo* p *positivo que é congruente a* 1 *mod* 4;

iii) p, *onde* p *é um número primo positivo e* $p \equiv 3$ *mod* 4.

Um domínio de integridade R chama-se um *domínio de factorização única*, se verificar as seguintes condições:

(i) todo o elemento $0 \neq a \in R$ que não é uma unidade, pode escrever-se na forma

$$a = p_1 p_2 ... p_k$$

onde $p_1, p_2, ..., p_k$ são elementos primos de R;

(ii) se

$$a = q_1 q_2 ... q_l$$

é outra factorização de a do tipo descrito em (i), então $k = l$ e é possível reordenar os $q_1, q_2, ..., q_l$ por forma que o primeiro seja associado de p_1, o segundo de p_2 e assim sucessivamente.

É bem conhecido que todo o domínio de ideais principais R é um domínio de factorização única.

Exemplo 1.3.2 *Os anéis* $\mathbb{Z}$, $\mathbb{Z}[i]$ *e* $F[x]$ *(onde* F *é um corpo) são domínios de ideais principais e consequentemente domínios de factorização única.*

Capítulo 2

Anéis filiais

O conceito de anel filial foi introduzido por Ehrlich [4]. Contudo, Szász [9], já tinha considerado um tipo especial destes anéis. Os resultados apresentados por Ehrlich, referem-se principalmente a anéis comutativos. Posteriormente, Andruszkiewicz e Puczylowski em [1], estenderam a caracterização a anéis não comutativos. Os resultados deste capítulo encontram-se em [4] e [1].

2.1 Conceitos gerais de anéis filiais

Em geral, se I é um ideal de um anel R e J um ideal de I, J não é necessariamente um ideal de R. Ehrlich [4] define anéis filiais como sendo anéis que satisfazem a condição de transitividade para ideais.

Definição 2.1.1 *Um anel R é filial se para quaisquer subanéis H, K de R*

$$H \lhd K \lhd R \text{ implica } H \lhd R.$$

Exemplo 2.1.2

(i) É evidente que os anéis simples são anéis filiais.

(ii) Os anéis Hamiltonianos (anéis cujos subanéis são ideais) são filiais. Em particular, o anel dos inteiros é filial.

(iii) Um anel R designa-se por von Neumann regular se para cada $a \in R$ existe $x \in R$ tal que $axa = a$. Estes anéis também são filiais, pois se $H \lhd K \lhd R$, então, para $h \in H$, existe $x \in R$ tal que $hxh = h$. Assim, se $y \in R$ temos $yh = yhxh \in KH \subset H$. De modo análogo, mostra-se que $hy \in H$, pelo que $H \lhd R$ e R é um anel filial.

No seguinte lema, podemos observar que a classe dos anéis filiais é homomorficamente fechada e hereditária, isto é, imagens homomorficas e ideais de anéis filiais são anéis filiais.

Lema 2.1.3 *Se R é um anel filial e I um ideal de R, então I e R/I são filiais.*

Demonstração: Suponhamos que R é um anel filial e $I \lhd R$. Primeiro vamos mostrar que I é filial. Se $H \lhd K \lhd I$ então $K \lhd R$, donde $H \lhd R$. Consequentemente $H \lhd I$. Assim I é filial. Seguidamente vamos mostrar que R/I é filial. Sejam J/I e K/I subanéis de R/I tais que $J/I \lhd K/I \lhd R/I$. Então $J \lhd K \lhd R$ e, como R é filial, temos $J \lhd R$ e logo $J/I \lhd R/I$.

■

Teorema 2.1.4 *Se R é filial, então todo o ideal minimal M de R, ou é idempotente (isto é, $M^2 = M$) ou nilpotente de índice 2 e com um número primo de elementos.*

Demonstração: Seja M um ideal minimal de R. Sendo $M^2 \lhd R$ e $M^2 \subseteq M$ então ou $M^2 = M$ ou $M^2 = 0$. No último caso, se S é subgrupo do grupo aditivo de M e $S \neq M$, então temos $MS \subseteq M^2 = 0$ e do mesmo modo, $SM = 0$, pelo que S é ideal de M. Uma vez que $S \lhd M \lhd R$ e R é filial, segue que S é um ideal de R. Visto que $S \neq M$, por definição de ideal minimal vem que $S = 0$. Assim, o grupo aditivo de M não tem subgrupos próprios, pelo que não tem ideais esquerdos ou direitos próprios. Assim, M tem um número primo de elementos.

■

Condições necessárias e suficientes para que um anel seja filial, são apresentadas no seguinte teorema.

Teorema 2.1.5 *Um anel R é filial se e só se*

(i) Toda a imagem homomorfica própria de R é filial

e

(ii) $S \lhd T \lhd J$ implica $S \lhd R$, onde $J = \mathfrak{J}(R)$.

Demonstração: Se R é filial, (ii) é óbvio, pois $S \lhd T \lhd J \lhd R$ implica $S \lhd R$. E a condição (i) segue do Lema 2.1.3, pois sendo R filial e $0 \neq I \lhd R$, R/I é filial.

Reciprocamente, suponhamos que (i) e (ii) se verificam. Para $H \neq 0$ e $H \lhd K \lhd R$ temos $KHK \lhd R$. No primeiro caso, se $KHK = 0$ então $H^3 = 0$. Sendo H um ideal nilpotente de K, pelo Corolário 1.1.15 e pelo Teorema 1.1.17, este está contido no radical $\mathfrak{J}(K) = K \cap J$ de K. De $H \subseteq K \cap J$ e $H \lhd K$ vem que $H \lhd K \cap J$. Sendo $H \lhd K \cap J \lhd J$, por (ii), podemos concluir que $H \lhd R$. No segundo caso, se $KHK \neq 0$, então por (i), $\overline{R} = R/KHK$ é filial. De $KHK \lhd H \lhd K \lhd R$, temos $\overline{H} \lhd \overline{K} \lhd \overline{R}$, onde $\overline{H} = H/KHK$ e $\overline{K} = K/KHK$. Mas, por (i), $\overline{R}$ é filial e então $\overline{H} \lhd \overline{R}$. Logo $H \lhd R$.

■

Corolário 2.1.6 *Um anel semiprimo R é filial se e só se toda a imagem homomorfica própria de R é filial.*

Demonstração: Sendo R um anel semiprimo, pelo Teorema 1.1.13 (iv), este não contém ideais nilpotentes não nulos e o primeiro caso na demonstração do Teorema 2.1.5 não pode ocorrer. Por isso, a condição (i) é suficiente para assegurar que o anel R é filial.

■

Corolário 2.1.7

(i) Se R é um anel Artiniano, então R é filial se e só se

a) R/I é filial para cada ideal minimal I de R

e

b) $S \lhd T \lhd \mathfrak{J}(R) \Rightarrow S \lhd R$.

(ii) Cada imagem homomorfica de um anel Artiniano filial é Artiniano filial.

Demonstração:

(i) Suponhamos que as condições a) e b) se verificam. Seja $K \lhd R$, $K \neq 0$. Dado que R é um anel Artiniano, então existe um ideal minimal $I \neq 0$ de R tal que $I \subset K$. Pelo Teorema 1.1.6, $(R/I)\,/\,(K/I) \cong R/K$. Sendo R/K imagem homomorfica própria de R/I e R/I filial então, pelo Lema 2.1.3, R/K é filial. Pelo Teorema 2.1.5, segue que R é filial. O recíproco é um caso particular do Teorema 2.1.5.

(ii) Sejam R um anel Artiniano filial e $K \lhd R$. Então, pelo Lema 2.1.3, R/K é filial. Além disso, R/K é um anel Artiniano.

■

Somas directas de anéis filiais não são em geral anéis filiais, como podemos observar no seguinte exemplo.

Exemplo 2.1.8 *$\mathbb{Z}\oplus\mathbb{Z}$ não é um anel filial. De facto, se $A = \{(a,a) : a \in 2\mathbb{Z}\} + 4\mathbb{Z}\oplus 4\mathbb{Z}$, então $A \lhd 2\mathbb{Z}\oplus 2\mathbb{Z} \lhd \mathbb{Z}\oplus\mathbb{Z}$, mas A não é um ideal de $\mathbb{Z}\oplus\mathbb{Z}$, pois $(6,6) \in A$, $(1,2) \in \mathbb{Z}\oplus\mathbb{Z}$ mas $(6,6)\cdot(1,2) \notin A$.*

Recordemos que a *ordem* de um elemento a de um grupo é o menor inteiro positivo n (caso exista) tal que $na = 0$. Um grupo diz-se um *p-grupo*, onde p é um número primo, se a ordem de cada um dos seus elementos é uma potência de p.

Proposição 2.1.9 *Se, para um conjunto de primos p distintos, o grupo aditivo do anel R_p é um p-grupo, então $R = \oplus R_p$ é um anel filial se e só se cada R_p é um anel filial.*

Demonstração: Se R é um anel filial então cada R_p (imagem homomorfica própria de R) é filial.

Reciprocamente, é bem conhecido se N é um subgrupo do grupo aditivo de R então $N = \oplus (N \cap R_p)$. Agora se $J \lhd I \lhd R$ então $J = \oplus (J \cap R_p)$, $I = \oplus (I \cap R_p)$, e para cada p, $J \cap R_p \lhd I \cap R_p \lhd R_p$, pelo que $J \cap R_p \lhd R_p$. Isto implica que $J \lhd R$ e assim R é um anel filial.

■

No Exemplo 2.1.8 observámos que a classe dos anéis filiais não é fechada para a soma directa. O seguinte exemplo, mostra que a classe dos anéis filiais também não é fechada sob extensões obtidas pela adjunção da identidade.

Exemplo 2.1.10 *Seja $\mathbb{Z}^0$ o anel com multiplicação nula no grupo aditivo dos inteiros e seja $\left(\mathbb{Z}^0\right)^{\#}$ a sua extensão natural a um anel com identidade. Podemos observar que o anel $\left(\mathbb{Z}^0\right)^{\#}$ é isomorfo ao anel de matrizes*

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}.$$

De facto, a aplicação

$$\begin{array}{rccc} \varphi : & R & \longrightarrow & \left(\mathbb{Z}^0\right)^{\#} \\ & \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} & \longmapsto & (a, b) \end{array}$$

é um isomorfismo. Verifica-se que

$$J = \left\{ \begin{pmatrix} 2x & 4y \\ 0 & 2x \end{pmatrix} : x, y \in \mathbb{Z} \right\} \lhd \left\{ \begin{pmatrix} 2a & 2b \\ 0 & 2a \end{pmatrix} : a, b \in \mathbb{Z} \right\} \lhd R$$

mas J não é ideal de R.

Um *anel* R diz-se *subidempotente* se para todo I ideal de R, $I^2 = I$.

Proposição 2.1.11 *Se I é um ideal de um anel R, onde I é um anel subidempotente e R/I é filial então R é um anel filial.*

Demonstração: Se $J \lhd K \lhd R$ então $J + I/I \lhd K + I/I \lhd R/I$. Uma vez que R/I é um anel filial, $J + I \lhd R$. Assim, $RJ \subseteq J + I$ e $JR \subseteq J + I$, donde $J_R + I = J + RJ + JR + RJR + I \subseteq J + I \subseteq J_R + I$. Agora, uma vez que I é um anel subidempotente, $(J_R \cap I)^2 = J_R \cap I$. Pelo Lema de Andrunakievich, segue que $(J_R \cap I)^3 \subseteq (J_R)^3 \subseteq J$ e então $(J_R \cap I)^3 \subseteq J \cap I$. Desta forma, como $(J_R \cap I)^3 = J_R \cap I$ temos $J_R \cap I = J \cap I$. Assim $J + I = J_R + I$ e $J_R \cap I = J \cap I$. Temos $J_R \subseteq J_R \cap (J_R + I) = J_R \cap (J + I) = (J_R \cap J) + (J_R \cap I) = J + (J \cap I) \subseteq J$, o que implica que $J = J_R$ e portanto $J \lhd R$. ■

O resultado seguinte dá-nos uma condição necessária e suficiente para que um anel subidempotente seja filial.

Proposição 2.1.12 *Um anel R é subidempotente se e só se $\mathbb{Z} \oplus R$ é um anel filial.*

Demonstração: Seja R um anel subidempotente. Como $\mathbb{Z} \oplus R/R \cong \mathbb{Z}$ e $\mathbb{Z}$ é um anel filial, então pela Proposição 2.1.11, $\mathbb{Z} \oplus R$ é um anel filial.

Reciprocamente, suponhamos que $I \lhd R$ e $i \in I$. Então para cada $n \in \mathbb{Z}$, $\left(n^2\mathbb{Z} \oplus I^2\right) + \mathbb{Z}(n,i) \lhd n\mathbb{Z} \oplus I \lhd \mathbb{Z} \oplus R$. Como $\mathbb{Z} \oplus R$ é um anel filial, então $\left(n^2\mathbb{Z} \oplus I^2\right) + \mathbb{Z}(n,i) \lhd \mathbb{Z} \oplus R$, para $n \in \mathbb{Z}$. Isto implica que $(n,0) = (1,0) \cdot (n,i) \in \left(n^2\mathbb{Z} \oplus I^2\right) + \mathbb{Z}(n,i)$. Assim, para certos $k, t \in \mathbb{Z}$ temos $n = n^2k + nt$ e $ti \in I^2$. Tomando $n = 2$ obtemos que $(1+2z)\, i \in I^2$, para algum $z \in \mathbb{Z}$ e, tomando $n = 1 + 2z$, vem que $(1 + (1+2z)\, z')\, i \in I^2$, para algum $z' \in \mathbb{Z}$. Assim, $i = (1 + (1+2z)\, z')\, i - z'\,(1+2z)\, i \in I^2$. Isto prova que $I = I^2$ e o resultado segue.

■

No teorema seguinte apresentamos várias condições necessárias e suficientes para que um anel seja filial.

Teorema 2.1.13 *As seguintes condições num anel R são equivalentes:*

(i) *R é filial;*

(ii) *para cada elemento $a \in R$, $(a)_R = (a)_R^2 + \mathbb{Z}a$;*

(iii) *se $I \lhd R$ e S é um subanel de I, então $I^2 + S \lhd R$;*

(iv) *se $I \lhd R$ e S é um subanel de I, então para cada $n \geq 2$, $I^n + S \lhd R$;*

(v) *existe um inteiro $n \geq 2$ tal que para cada $I \lhd R$ e cada subanel S de I, $I^n + S \lhd R$;*

(vi) *se $I \lhd R$ e S é um subanel de I, então para algum inteiro $n \geq 2$, $I^n + S \lhd R$.*

Demonstração: (i) implica (ii). É claro que para cada $a \in R$, $(a)_R^2 + \mathbb{Z}a \lhd (a)_R \lhd R$. Assim, sendo R filial vem que $(a)_R^2 + \mathbb{Z}a \lhd R$. Disto, do facto de $(a)_R^2 + \mathbb{Z}a \subseteq (a)_R$ e de $(a)_R$ ser o menor ideal de R que contém a, segue que $(a)_R^2 + \mathbb{Z}a = (a)_R$.

(ii) implica (iii). Seja $a \in S$. Sendo S um subanel de I, $\mathbb{Z}a \subset S$. De $a \in S \subset I$ vem que $(a)_R \subset I$ e logo $(a)_R^2 \subset I^2$. Então $\sum\limits_{a \in S} \left((a)_R^2 + \mathbb{Z}a\right) \subset I^2 + S$. No entanto $S \subset \sum\limits_{a \in S} \left((a)_R^2 + \mathbb{Z}a\right)$. Assim, $I^2 + S = I^2 + \sum\limits_{a \in S} \left((a)_R^2 + \mathbb{Z}a\right)$. Uma vez que por hipótese, para cada $a \in S$, $(a)_R^2 + \mathbb{Z}a = (a)_R$ é um ideal de R, também $I^2 + S$ é um ideal de R.

(iii) implica (iv). A prova é feita recorrendo ao método de indução. Para $n = 2$, as condições coincidem. Seja $n > 2$ e suponhamos que para $n > k \geqslant 2$, $I^k + S \lhd R$. Em particular, $J = I^{n-1} + S \lhd R$. Aplicando (iii) ao ideal J obtemos que $J^2 + S \lhd R$, donde $\left(I^{n-1} + S\right)^2 + S \lhd R$. Agora $\left(I^{n-1} + S\right)^2 + S \subseteq I^n + S$ e I^n é um ideal de R. Assim $I^n + S \lhd R$.

(v) é um caso especial de (iv) e (vi) é um caso especial de (v).

(vi) implica (i). Sejam $J \lhd K \lhd R$ e $I = J_R$. A hipótese garante que para algum $n \geq 2$, $I^n + J \lhd R$. Se $n \geq 3$ então, pelo Lema de Andrunakievich, $(J_R)^n \subseteq J$ e como $I = J_R$ vem que $I^n \subseteq J$. Assim $I^n + J = J$ e portanto neste caso $J \lhd R$. Assim R é filial. Se $n = 2$ então $I^2 + J \lhd R$. Aplicando (vi) a $I^2 + J$ e $S = J$ obtemos que $(I^2 + J)^n + J \lhd R$, para algum $n \geq 2$. Do Lema de Andrunakievich resulta que $\left(I^2 + J\right)^n \subseteq J$. Assim, $J = \left(I^2 + J\right)^n + J \lhd R$ e então R é filial.

■

No caso de R ser um anel comutativo e com identidade, é fácil ver que R é filial se e só se, para cada $a \in R$, $aR = a^2R + \mathbb{Z}a$.

Como consequência do Teorema 2.1.13 (v) obtemos o seguinte corolário.

Corolário 2.1.14 *Um anel nilpotente é filial se e só se todo o seu subanel é um ideal.*

Demonstração: Seja R um anel filial e nilpotente ($R^n = 0$, n inteiro positivo) e S um subanel de R. Pelo Teorema 2.1.13 (v), $R^n + S \lhd R$ e portanto $S \lhd R$. A outra implicação é imediata.

■

Se R é um anel tal que $R^2 = 0$ então R é filial; contudo, existem anéis R tais que $R^3 = 0$ e que não são filiais.

Exemplo 2.1.15 *Consideremos o anel $R = xF[x]/x^3F[x]$, onde F é um corpo, e o subanel P de R gerado por 1. Se $P = F$ então o corpo F é finito e primo e então o anel R é filial. Se $P \neq F$, então, para $a = x + x^3F[x]$, $Pa^2 \lhd Fa^2$ e Pa^2 não é ideal de R. Assim neste caso, o anel R não é filial.*

É claro que $[a]_R = aR + Ra + RaR$ é um ideal de R. Como consequência imediata do Teorema 2.1.13 (ii), obtemos que se para cada $a \in R$, $[a]_R = [a]_R^2$ então R é um anel filial. Contudo existem anéis filiais, que não satisfazem esta condição, como por exemplo o anel dos inteiros.

Proposição 2.1.16 *Dado um anel R, o anel $R \oplus R$ é filial se e só se $[a]_R = [a]_R^2$, para cada elemento $a \in R$.*

Demonstração: Suponhamos que o anel $R \oplus R$ é filial e seja $a \in R$. Claramente $((a,a))_{R\oplus R} = ([a]_R \oplus [a]_R) + \mathbb{Z}(a,a)$, isto é, $([a]_R \oplus [a]_R) + \mathbb{Z}(a,a)$ é o menor ideal de $R \oplus R$ que contém (a,a), e $((a,a))^2_{R\oplus R} = \left([a]_R^2 \oplus [a]_R^2\right) + ([a]_R\, a \oplus [a]_R\, a) + (a\,[a]_R \oplus a\,[a]_R) + \mathbb{Z}\left(a^2, a^2\right)$. Pelo Teorema 2.1.13 (ii), como $R \oplus R$ é filial, então $((a,a))^2_{R\oplus R} + \mathbb{Z}(a,a) =$

$((a,a))_{R\oplus R}$, logo $((a,a))^2_{R\oplus R} + \mathbb{Z}(a,a) \lhd R \oplus R$. Isto implica que para cada $r \in R$, $(ar,0) = (a,a)(r,0) \in ((a,a))^2_{R\oplus R} + \mathbb{Z}(a,a)$. Assim,

$$ar = x + na^2 + ma$$

e

$$0 = y + na^2 + ma$$

para quaisquer $x, y \in [a]^2_R + [a]_R a + a[a]_R = I$ e $n, m \in \mathbb{Z}$. Assim, para todo o $r \in R$, $ar = x - y \in I$. Consequentemente, $aR \subseteq I$ e semelhantemente $Ra \subseteq I$. Como I é um ideal de R e $a \in R$ então $aI \subseteq I$, isto é, $a\left([a]^2_R + [a]_R a + a[a]_R\right) \subseteq [a]_R \subseteq I = [a]^2_R + [a]_R a + a[a]_R$. Substituindo duas vezes na última inclusão $[a]^2_R + [a]_R a + a[a]_R$ em vez de $[a]_R$, obtemos $[a]_R \subseteq [a]^2_R$. Como $[a]^2_R \lhd [a]_R$, segue que $[a]_R = [a]^2_R$.

Reciprocamente, se $[a]_R = [a]^2_R$ então, pela nota anterior à proposição, R é um anel filial. Sendo R um anel subidempotente e $R \oplus R\ /R \cong R$ e R um anel filial, segue pela Proposição 2.1.11 que $R \oplus R$ é filial.

■

2.2 Domínios de integridade filiais

Neste ponto, vamos estudar a filialidade dos domínios de integridade.

Teorema 2.2.1 *As seguintes condições num domínio de integridade R são equivalentes:*

(i) *R é filial;*

(ii) *para cada $a \in R$, $a \neq 0$, $R = aR + \mathbb{Z}1$;*

(iii) *cada imagem homomorfica de R também é imagem homomorfica de $\mathbb{Z}$.*

Demonstração: (i) implica (ii). Sendo R um domínio de integridade, então $(a)_R = aR$. Como R é um anel filial, pelo Teorema 2.1.13 (ii), segue que $aR = a^2R + \mathbb{Z}a$, para qualquer $a \in R$. Assim, para qualquer $x \in R$, existem $y \in R$ e $n \in \mathbb{Z}$ tais que $ax = a^2y + na$, ou seja, $a(x - ay + n1) = 0$. Como R não tem divisores de zero, podemos concluir que para $a \neq 0$, $x = ay + n1$. Deste modo, $R = aR + \mathbb{Z}1$.

(ii) implica (iii). Suponhamos $K \neq 0$ e $K \lhd R$. Pelo Teorema 1.1.6, se $a \neq 0$, $a \in K$ então $(R/aR)/(K/aR) \cong R/K$, isto é, R/K é imagem homomorfica de R/aR. Assim, é suficiente provar que R/aR é imagem homomorfica de $\mathbb{Z}$. Definimos $\alpha : \mathbb{Z} \to R/aR$ por $\alpha(n) = aR + n1$, para qualquer $n \in \mathbb{Z}$. Então α é claramente um homomorfismo. Uma vez que pela condição (ii), $R = aR + \mathbb{Z}1$, α é uma aplicação sobrejectiva. Assim, α é um epimorfismo e portanto, R/aR é imagem homomorfica de $\mathbb{Z}$.

(iii) implica (i). Aplicando o Lema 2.1.3 ao anel $\mathbb{Z}$ (filial), obtemos que cada imagem homomorfica de $\mathbb{Z}$ é filial. Pela condição (iii), segue que cada imagem homomorfica de R

é filial. Suponhamos que R não é um anel semiprimo. Então existe $I \neq 0$, $I \lhd R$ tal que $I^2 = 0$. Deste modo, para $a \neq 0$, $a \in I$ teríamos $a^2 = 0$. Contradição com o facto de R ser um domínio de integridade. Deste modo, pelo Corolário 2.1.6, podemos concluir que R é filial.

■

Nos seguintes corolários são apresentados domínios de integridade que não são filiais.

Corolário 2.2.2 *Se A é um domínio de integridade, então o domínio de integridade $A[x]$ não é filial.*

Demonstração: A equação $x = x^2 r + n1$ é impossível, com $r \in R$, $n \in \mathbb{Z}$. Assim, R não satisfaz a condição (ii) do Teorema 2.2.1 e então R não é filial.

■

Seguidamente pretendemos mostrar que somas subdirectas de anéis filiais não são necessariamente filiais. Do Corolário 2.2.2 temos que o domínio de integridade $\mathbb{Q}[x]$ não é filial. Para $a \in \mathfrak{J}(A)$ então a é quasi-regular à direita e quasi-regular à esquerda. Consequentemente $1 - a$ é uma unidade em A. Visto que as únicas unidades em A são os elementos não nulos de $\mathbb{Q}$, segue que $a \in \mathbb{Q}$. Assim, $\mathfrak{J}(A) \lhd \mathbb{Q}$. Como $\mathbb{Q}$ é um anel simples, então $\mathfrak{J}(A) = 0$ ou $\mathfrak{J}(A) = \mathbb{Q}$. Uma vez que 1 não é quasi-regular à esquerda, $1 \notin \mathfrak{J}(A)$. Assim $\mathfrak{J}(A) = 0$ e portanto $A = \mathbb{Q}[x]$ é semisimples. Pelo Teorema 1.1.18, $\mathbb{Q}[x]$ é isomorfo a uma soma subdirecta de corpos, que são obviamente filiais.

Corolário 2.2.3 *Se R é um domínio de integridade que não é um corpo e se R contém um corpo como subanel, então R não é filial.*

Demonstração: Seja R um domínio de integridade que não é um corpo. Suponhamos que R contém um corpo F como subanel. Se 1_F é a identidade de F, então $1_F^2 = 1_F = 1_F 1$. Assim, $1_F(1_F - 1) = 0$ e sendo R um domínio de integridade, então $1_F = 1$. Mas então $1 \in F$ e logo $\mathbb{Z}1 \subset F$. Assim, como F é um corpo, temos que $n1$ é uma unidade em R, para qualquer $n \in \mathbb{Z}$ não nulo. Suponhamos que R é filial. Então, para $a \neq 0$, onde a não é uma unidade em R, temos $a^2 \neq 0$, assim pelo Teorema 2.2.1 (ii), $R = a^2 R + \mathbb{Z}1$. Em particular, $a = a^2 x + n1$, para certos $x \in R$ e $n \in \mathbb{Z}$. Se $n = 0$, então $a(1 - ax) = 0$. Uma vez que $a \neq 0$, $ax = 1$, e a é uma unidade. Contradição, assim R não é filial. Se $n \neq 0$, então sendo $n1$ uma unidade, temos que $a(1 - ax)(n1)^{-1} = 1$, e a é uma unidade. Contradição. Segue que R não é filial.

■

Corolário 2.2.4 *Todo o domínio de integridade filial, que não é um corpo, tem característica zero.*

Demonstração: Suponhamos que R tem característica $p \neq 0$. A aplicação

$$\begin{array}{rccc} \varphi: & \mathbb{Z}1 & \longrightarrow & \mathbb{Z}_p \\ & n1 & \longmapsto & \bar{n} \end{array}$$

é um isomorfismo. Assim $\mathbb{Z}1$ é um corpo com p elementos, contido em R. Consequentemente, pelo Corolário 2.2.3, R não é filial.

■

O lema que se segue serve de partida para os dois seguintes teoremas, que descrevem subanéis de domínios de integridade que são filiais.

Lema 2.2.5 *Seja A um domínio de ideais principais, F o seu corpo dos quocientes, e R um subdomínio de F contendo A. Então:*

(i) $R = S^{-1}A$, *onde S é a intersecção dos complementares de certos ideais primos de R;*

(ii) para qualquer $a \in R$, $R = aR + A$.

Demonstração:

(*i*) Seja D o conjunto de todos os denominadores que ocorrem em fracções irredutíveis que representam elementos de R, e seja $S \supset D$ o conjunto de todos os produtos finitos de elementos de D. Então $1 \in S$ e S é um subconjunto multiplicativo de A. Para cada $\delta \in D$, existe um $\alpha \in A$ tal que $(\alpha, \delta) = 1$ e $\frac{\alpha}{\delta} \in R$. Portanto, sendo A um domínio de ideais principais, existem ξ, $\eta \in A$ tal que $1 = \alpha\xi + \delta\eta$ e então, para $k \in A$, $\frac{k}{\delta} = k\xi\frac{\alpha}{\delta} + k\eta\frac{\delta}{\delta} \in R$. Agora, se $\sigma \in S$, então $\sigma = \delta_1 ... \delta_n$ ($\delta_i \in D$, $n \geq 1$). Consequentemente se $k \in A$, então $\frac{k}{\delta_1}, \frac{1}{\delta_2}, ..., \frac{1}{\delta_n}$ pertencem a R, e logo $\frac{k}{\delta} \in R$. Assim, $R = S^{-1}A$.

Seja $\overline{S} = A - S$. Uma vez que S é fechado para a multiplicação, $\overline{S}$ é um "conjunto primo", isto é, para $a, b \in A$, $ab \in \overline{S}$ implica $a \in \overline{S}$ ou $b \in \overline{S}$. Seja $\alpha \in \overline{S}$. Sendo $\alpha \in A$ e A um domínio de ideais principais, que por sua vez é um domínio de factorização única, então $\alpha = \pi_1 ... \pi_n \in \overline{S}$, onde $\pi_1, \pi_2, ..., \pi_n$ são elementos primos de A. Assim, uma vez que $\overline{S}$ é um "conjunto primo", então pelo menos um dos divisores primos π_α de α pertence a $\overline{S}$. Seja $X = \{\pi_\alpha : \alpha \in \overline{S}\}$. Então $\overline{S} \subset \bigcup_{\alpha \in \overline{S}} (\pi_\alpha)$. Vamos mostrar que para cada $\pi_\alpha \in X$, o ideal (π_α) está contido em $\overline{S}$. De facto, suponhamos que para algum $\pi \in X$, $\mu\pi \in S$, para algum $\mu \in A$. Então π/δ, para algum $\delta \in D$. Seja $\delta = \pi\gamma$ com $\gamma \in A$. Pela definição de D, existe $\beta \in A$ tal que $(\beta, \delta) = 1$ e $\frac{\beta}{\delta} \in R$. Mas então, $\gamma\frac{\beta}{\delta} = \gamma\frac{\beta}{\gamma\pi} \in S^{-1}A = R$. Uma vez que $(\beta, \pi) = 1$, concluímos que $\pi \in S$. Contradição. Segue que $(\pi_\alpha) \subset \overline{S}$ para todo o $\alpha \in \overline{S}$. Então $\overline{S} = \bigcup_{\alpha \in \overline{S}} (\pi_\alpha)$, assim $S = \bigcap_{\alpha \in \overline{S}} \overline{(\pi_\alpha)}$.

(*ii*) Por (*i*), existe um conjunto X de elementos primos em A tal que $R = S^{-1}A$, onde S é a intersecção dos complementares dos ideais (π), para $\pi \in X$. Vamos mostrar que para cada $\alpha \in A$, $\alpha \neq 0$, $\sigma \in S$, $R = \frac{\alpha}{\sigma}R + A$. Sejam $\delta \in A$ e $\rho \in S$. Queremos encontrar $\beta \in A$, $\tau \in S$, $\upsilon \in A$ tais que $\frac{\delta}{\rho} = \frac{\alpha}{\sigma}\frac{\beta}{\tau} + \frac{\upsilon}{1}$ ou equivalentemente, $\tau\sigma(\delta - \upsilon\rho) = \rho\alpha\beta$. Sem perder generalidade, podemos assumir que $(\alpha, \sigma) = 1$. Para cada um dos primos $\pi_i \in X$ $(i = 1, ..., h,\ h \geq 0)$ que dividem α, existe um inteiro positivo k_i e um elemento γ_i de A tal que $\alpha = \pi_i^{k_i}\gamma_i$ e $(\pi_i, \gamma_i) = 1$. Uma vez que $(\rho, \pi_i) = 1$, para todo o $i = 1, ..., h$, a congruência $\delta - \upsilon\rho \equiv 0 \bmod \pi_i^{k_i}$ tem soluções simultâneas $\upsilon \in A$. Com υ assim escolhido, a potência máxima de π_i que divide $\sigma(\delta - \upsilon\rho)$ é da forma $\pi_i^{l_i}$, onde $l_i \geq k_i$ $(i = 1, ..., h)$. Mas então cada um dos primos em X ocorre como um factor em $\sigma(\delta - \upsilon\rho)$, pelo menos tantas vezes quantas em $\rho\alpha$. Assim, se μ é o mínimo múltiplo comum de $\sigma(\delta - \upsilon\rho)$ e $\rho\alpha$, então $\mu = \tau\sigma(\delta - \upsilon\rho) = \rho\alpha\beta$, para τ, $\beta \in A$ com $(\tau, \pi) = 1$, para cada $\pi \in X$. Segue que $\frac{\beta}{\tau} \in S^{-1}A = R$ e $\upsilon \in A$ têm as propriedades desejadas.

■

Teorema 2.2.6 *Todo o subdomínio do corpo racional é filial.*

Demonstração: Seja R um subdomínio do corpo racional $\mathbb{Q}$. Uma vez que R é um domínio de integridade, então $1 \in R$ e por conseguinte temos $\mathbb{Z} \subset R$. Portanto, pelo Lema 2.2.5 (*ii*), segue que, para cada $a \in R$, $R = aR + \mathbb{Z}$ e, pelo Teorema 2.2.1, R é filial.

■

Recordemos que se E é uma extensão de um corpo F e $\alpha \in E$, o *elemento* α diz-se *algébrico* sobre F, quando α é raiz de algum polinómio não nulo de $F[x]$. Se $p(x)$ é o polinómio mínimo de α sobre F e se o grau de $p(x) = n$, então $\left\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\right\}$ é uma base de $F(\alpha)$ sobre F.

O seguinte teorema apresenta uma classe de domínios de integridade não filais.

Teorema 2.2.7 *Seja A um subdomínio próprio de $\mathbb{Q}$ e seja α um elemento de alguma extensão do corpo $\mathbb{Q}$ tal que α é algébrico de grau $s \geqslant 2$ sobre $\mathbb{Q}$ e α é integral sobre A, isto é, α é raiz de um polinómio mónico sobre A. Então $R = A[\alpha]$ não é filial.*

Demonstração: Sendo $\mathbb{Z}$ um domínio de ideais principais e $\mathbb{Q}$ o seu corpo dos quocientes, pelo Lema 2.2.5 (*i*), $A = S^{-1}\mathbb{Z}$, onde S é a intersecção dos complementares de certos ideais primos de $\mathbb{Z}$. Seja p um primo em $\mathbb{Z} - S$. Se R é filial, então pelo Lema 2.2.5 (*ii*), $R = p\alpha R + \mathbb{Z}$. Mas então $\alpha = p\alpha x + n$, para certos $x \in R$, $n \in \mathbb{Z}$, e assim $\alpha x = \frac{1}{p}\alpha - \frac{n}{p} \in R$. Uma vez que α é integral sobre A, a representação de αx como combinação linear, sobre $\mathbb{Q}$, de $1, \alpha, ..., \alpha^{s-1}$ deve ter todos os coeficientes em A. Mas $\frac{1}{p} \notin A$, pois se $\frac{1}{p} \in A$ então $p \in S$, o que é uma contradição com o facto de $p \in \mathbb{Z} - S$. Assim R não é filial.

■

Pelo Teorema 2.2.7, $\mathbb{Z}[i]$ não é filial. No entanto, o seguinte teorema mostra que localizações de $\mathbb{Z}[i]$, relativamente a certos ideais primos são filiais. Na demonstração do seguinte lema, serão utilizados resultados da Teoria dos Números (ver [8]).

Teorema 2.2.8 *Seja P um ideal primo não nulo de $\mathbb{Z}[i]$, e seja $S = \mathbb{Z}[i] - P$. Então $R = S^{-1}\mathbb{Z}[i]$ é filial se e só se $P = (\pi)$ onde π é um inteiro de Gauss, cuja norma é um primo racional $p \equiv 1$ mod 4.*

Demonstração: Temos $P = (\pi)$ para algum inteiro de Gauss π, e os ideais do anel local $R = S^{-1}\mathbb{Z}[i]$ da forma $\pi^k R$, $k \geq 1$. Pelo Teorema 2.2.1, R é filial se e só se $R = \pi^k R + \mathbb{Z}$, para cada $k \geq 1$. Pelo Lema 2.2.5 (ii), $R = \pi^k R + \mathbb{Z}[i]$, para cada $k \geq 1$. Assim, R será filial se e só se para cada $k \geq 1$, $i \in \pi^k R + \mathbb{Z}$.

Suponhamos que $\pi\overline{\pi} = p$, onde p é um primo racional congruente a 1 mod 4. Então a congruência $n^2 + 1 \equiv 0 \bmod p^k$ tem uma solução em $\mathbb{Z}$ para cada $k \geq 1$. Para um dado k, com n assim escolhido, π divide $i+n$ ou π divide $i-n$, mas não ambos, em $\mathbb{Z}[i]$. De facto, se $\pi/i+n$ e $\pi/i-n$ em $\mathbb{Z}[i]$, então $\frac{2n}{\pi} = \frac{2n\overline{\pi}}{p} \in \mathbb{Z}[i]$, mas p é um primo ímpar que não divide n em $\mathbb{Z}$, pois $n^2+1 \equiv 0 \bmod p$ implica $p/\left(n^2+1\right)$. Portanto temos que $\pi^k/i-n$ ou $\pi^k/i+n$, em $\mathbb{Z}[i]$. No primeiro caso, $i = \pi^k \frac{i-n}{\pi^k} + n \in \pi^k R + \mathbb{Z}$, e no segundo caso $i = \pi^k \frac{i+n}{\pi^k} - n \in \pi^k R + \mathbb{Z}$. Segue que R é filial.

Reciprocamente, seja R filial. Então pelo Teorema 2.2.1, para cada $k \geq 1$, $i = \pi^k x + n$, para certos $x \in R$, $n \in \mathbb{Z}$, pelo que $x = \frac{i-n}{\pi^k} \in R$. Então $(\pi\overline{\pi})^k / \left(n^2+1\right)$ em $\mathbb{Z}$, para cada $k \geq 1$. Se $\pi = i+1$, então $\pi\overline{\pi} = 2$, e a congruência $n^2+1 \equiv 0 \bmod 2^k$ não é solúvel para $k \geq 3$. Se $\pi = p$ é um primo racional congruente a -1 mod 4, então $\pi\overline{\pi} = p^2$, mas a congruência $n^2+1 \equiv 0 \bmod p^h$ nunca é solúvel. De acordo com o Exemplo 1.3.1, uma vez que todo o primo de Gauss é associado de $1+i$ ou a um primo racional congruente a -1 mod 4 ou a um primo π de Gauss com norma $\pi\overline{\pi} = p$, um primo racional congruente a 1 mod 4, segue que o ideal primo P é gerado por um primo π da forma requerida.

■

Exemplo 2.2.9 *Sejam*

$$R_1 = \mathbb{Z}[i]_{(1+2i)} = \left\{ \frac{a+bi}{c+di} : a,b,c,d \in \mathbb{Z} \text{ e } (1+2i, c+di) = 1 \right\}$$

e

$$R_2 = \mathbb{Z}_{(5)}[1+2i] = \{x + y(1+2i) : x, y \in \mathbb{Z}_5\},$$

onde $\mathbb{Z}_{(5)} = \left\{ \frac{r}{s} : r, s \in \mathbb{Z}, (s,5) = 1 \right\}$ é a localização de $\mathbb{Z}$ relativamente ao ideal gerado por 5. Verifica-se que $R_2 \subseteq R_1$. De facto se $z \in R_2$ então existem $r, s, r', s' \in \mathbb{Z}$ com $(s,5) = 1$ e $(s',5) = 1$ tais que

$$z = \frac{r}{s} + \frac{r'}{s'}(1+2i) = \frac{(rs' + sr') + (2sr')\,i}{ss'}.$$

Agora vamos mostrar que $(1+2i, ss') = 1$. Suponhamos que $(1+2i, ss') = d$. Então d/ss' e $d/(1+2i)$ e logo $n(d)/n(ss')$ e $n(d)/n(1+2i)$. No último caso, se $n(d)/5$ então

$n(d) = 1$ *ou* $n(d) = 5$. *Suponhamos que* $n(d) = 5$ *e* $d = a + bi$, *então* $a = \pm 1$ *e* $b = \pm 2$ *ou* $a = \pm 2$ *e* $b = \pm 1$. *Consideremos o caso* $d = 1 + 2i$. *Uma vez que* $(1+2i)/ss'$ *e do facto de* $1 + 2i$ *ser um elemento primo de* $\mathbb{Z}[i]$, *vem que* $(1+2i)/s$ *ou* $(1+2i)/s'$. *Então* s *ou* s' *é divisível por* 5, *o que é uma contradição. De modo idêntico obtemos uma contradição para os restantes casos. Assim* $n(d) = 1$ *pelo que* $d = 1$. *Segue pelo Teorema 2.2.8 que* R_1 *é filial, enquanto o seu subanel* R_2, *não é filial, pelo Teorema 2.2.7.*

2.3 Grupos abelianos e anéis filiais

Seja M um grupo abeliano aditivo. O conjunto $\begin{pmatrix} \mathbb{Z} & M \\ 0 & 0 \end{pmatrix}$ das matrizes 2×2 da forma $\begin{pmatrix} a & m \\ 0 & 0 \end{pmatrix}$, onde $a \in \mathbb{Z}$ e $m \in M$, munido das operações usuais, é um anel.

Um *grupo abeliano* M diz-se *divisível* se $nM = M$, para cada número n natural, ou seja, a equação $nx = g$ é solúvel em M, para todo o $g \in M$ e para todo o $n \in \mathbb{N}$.

O seguinte resultado caracteriza os grupos abelianos divisíveis por meio da filialidade.

Proposição 2.3.1 *Um grupo abeliano* M *é divisível se e só se o anel* $\begin{pmatrix} \mathbb{Z} & M \\ 0 & 0 \end{pmatrix}$ *é filial.*

Demonstração: Suponhamos que o anel $\begin{pmatrix} \mathbb{Z} & M \\ 0 & 0 \end{pmatrix}$ é filial. Para todo o número natural a, $I = \begin{pmatrix} a\mathbb{Z} & M \\ 0 & 0 \end{pmatrix}$ é um ideal de $\begin{pmatrix} \mathbb{Z} & M \\ 0 & 0 \end{pmatrix}$. Assim, pelo Teorema 2.1.13 (iii), para todo o $m \in M$,

$$K = \begin{pmatrix} a^2\mathbb{Z} & aM \\ 0 & 0 \end{pmatrix} + \mathbb{Z}\begin{pmatrix} a & m \\ 0 & 0 \end{pmatrix} \lhd \begin{pmatrix} \mathbb{Z} & M \\ 0 & 0 \end{pmatrix}.$$

Em particular,

$$\begin{pmatrix} 0 & m \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & m \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} a & m \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in K.$$

Assim, existem $z, k \in \mathbb{Z}$ e $m_1 \in M$ tais que $a^2z + ka = 0$ e $m = am_1 + km$. Agora $k = -az$ e $m = a(m_1 - zm)$. Esta relação pode ser obtida para todo o m e a, assim para todo o número natural a, $M = aM$ e o grupo M é divisível.

Reciprocamente, seja I um ideal de $\begin{pmatrix} \mathbb{Z} & M \\ 0 & 0 \end{pmatrix}$. É fácil ver que $I = \begin{pmatrix} a\mathbb{Z} & N \\ 0 & 0 \end{pmatrix}$ para algum $a \in \mathbb{Z}$ e para um subgrupo N de M. De $I \lhd \begin{pmatrix} \mathbb{Z} & M \\ 0 & 0 \end{pmatrix}$, vem que $I\begin{pmatrix} \mathbb{Z} & M \\ 0 & 0 \end{pmatrix} \subseteq I$.

Uma vez que $I\begin{pmatrix} \mathbb{Z} & M \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a\mathbb{Z} & aM \\ 0 & 0 \end{pmatrix}$, segue que $\begin{pmatrix} a\mathbb{Z} & aM \\ 0 & 0 \end{pmatrix} \subseteq \begin{pmatrix} a\mathbb{Z} & N \\ 0 & 0 \end{pmatrix}$ e temos $aM \subseteq N$. Isto e o facto do grupo M ser divisível implica que $I = \begin{pmatrix} 0 & M \\ 0 & 0 \end{pmatrix}$ ou $I = \begin{pmatrix} a\mathbb{Z} & M \\ 0 & 0 \end{pmatrix}$, para algum $0 \neq a \in \mathbb{Z}$. No primeiro caso, para todo o subanel S de I, $I^2 + S = S \lhd \begin{pmatrix} \mathbb{Z} & M \\ 0 & 0 \end{pmatrix}$. No outro caso, $I^2 = \begin{pmatrix} a^2\mathbb{Z} & aM \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a^2\mathbb{Z} & M \\ 0 & 0 \end{pmatrix}$, assim se S é um subanel de I então $I^2 + S = \begin{pmatrix} P & M \\ 0 & 0 \end{pmatrix}$, para algum subanel P de $\mathbb{Z}$. Desta forma, $I^2 + S$ é um ideal de $\begin{pmatrix} \mathbb{Z} & M \\ 0 & 0 \end{pmatrix}$ e pelo Teorema 2.1.13 (iii), $\begin{pmatrix} \mathbb{Z} & M \\ 0 & 0 \end{pmatrix}$ é filial.

■

Seja M um grupo abeliano aditivo. O conjunto $\begin{pmatrix} \mathbb{Z} & M \end{pmatrix}$ das matrizes 2×2 da forma $\begin{pmatrix} a & m \\ 0 & a \end{pmatrix}$, onde $a \in \mathbb{Z}$ e $m \in M$ com as operações usuais é um anel. O anel $\begin{pmatrix} \mathbb{Z} & M \end{pmatrix}$ é isomorfo ao anel $(M^0)^{\#}$, obtido pela adjunção da identidade ao anel trivial no grupo aditivo M.

Proposição 2.3.2 *O anel* $\begin{pmatrix} \mathbb{Z} & M \end{pmatrix}$ *é filial se e só se* $zM = z^2M$, *para todo o* $z \in \mathbb{Z}$.

Demonstração: Uma vez que o anel $\begin{pmatrix} \mathbb{Z} & M \end{pmatrix}$ é comutativo, então o ideal gerado por $\begin{pmatrix} z & m \\ 0 & z \end{pmatrix} \in \begin{pmatrix} \mathbb{Z} & M \end{pmatrix}$ é da forma $\begin{pmatrix} z & m \\ 0 & z \end{pmatrix} \cdot \begin{pmatrix} \mathbb{Z} & M \end{pmatrix}$. Assim, pelo Teorema 2.1.13 (ii), $\begin{pmatrix} \mathbb{Z} & M \end{pmatrix}$ é filial se e só se

$$\begin{pmatrix} z & m \\ 0 & z \end{pmatrix} \cdot \begin{pmatrix} \mathbb{Z} & M \end{pmatrix} = \begin{pmatrix} z & m \\ 0 & z \end{pmatrix}^2 \cdot \begin{pmatrix} \mathbb{Z} & M \end{pmatrix} + \mathbb{Z}\begin{pmatrix} z & m \\ 0 & z \end{pmatrix}.$$

Agora

$$\begin{pmatrix} z & m \\ 0 & z \end{pmatrix} \cdot \begin{pmatrix} \mathbb{Z} & M \end{pmatrix} = \left\{ \begin{pmatrix} za & zx + am \\ 0 & za \end{pmatrix} \ : \ a \in \mathbb{Z},\ x \in M \right\}$$

e

$$\begin{pmatrix} z & m \\ 0 & z \end{pmatrix}^2 \cdot \begin{pmatrix} \mathbb{Z} & M \end{pmatrix} = \left\{ \begin{pmatrix} z^2b & z^2y + 2bzm \\ 0 & z^2b \end{pmatrix} \ : \ b \in \mathbb{Z},\ m \in M,\ y \in M \right\}.$$

Portanto $\begin{pmatrix} \mathbb{Z} & M \end{pmatrix}$ é um anel filial se e só se para cada a, $z \in \mathbb{Z}$ e x, $m \in M$ existem b, $k \in \mathbb{Z}$ e $y \in M$ tais que

$$za = z^2b + kz$$
$$zx + am = z^2y + 2bzm + km.$$

Estas condições são trivialmente satisfeitas para $z = 0$. Se $z \neq 0$ então a primeira igualdade é equivalente a $a = zb + k$. Usando esta relação na segunda igualdade obtemos $zx = z^2y + bzm$. Fazendo $m = 0$, temos que para cada $z \in \mathbb{Z}$ e cada $x \in M$ existe $y \in M$ com $zx = z^2y$. Assim $zM = z^2M$.

Reciprocamente, suponhamos que para todo o $z \in \mathbb{Z}$, $zM = z^2M$. Então para todo o $x \in M$ existe $y \in M$ com $zx = z^2y$. Para um dado $a \in \mathbb{Z}$, $m \in M$, fazendo $k = a$ e $b = 0$ obtemos

$$za = z^2b + kz$$

e

$$zx + am = z^2y + 2bzm + km.$$

■

O grupo cíclico aditivo $\mathbb{Z}_p$, onde p é primo, não é divisível, mas satisfaz $n\mathbb{Z}_p = n^2\mathbb{Z}_p$, para todo o $n \in \mathbb{Z}$.

Conclusão

Os anéis, em geral, não satisfazem a condição de transitividade para ideais. Ehrlich designou os anéis que satisfazem esta condição por anéis filiais e apresentou alguns exemplos: os anéis simples, os von Neumann regulares e os Hamiltonianos. Além disso, introduziu condições necessárias e suficientes para que um anel seja filial. O mesmo autor enunciou um lema onde considera que somas directas de anéis são filiais; contudo, Andruszkiewicz e Puczylowski apresentaram um contra-exemplo. Assim a classe dos anéis filiais não é fechada para a soma directa, como também não é fechada sob extensões obtidas pela adjunção da identidade. Mostrámos que os ideais e imagens homomorficas de anéis filiais são filiais; e todo o ideal minimal não idempotente de um anel filial tem um número primo de elementos. Caracterizámos os anéis R tais que $R \oplus R$ é filial. No que respeita aos domínios de integridade, o anel dos inteiros de Gauss, $\mathbb{Z}[i]$, não é filial; no entanto localizações de $\mathbb{Z}[i]$ relativamente a certos ideais primos são filiais. Podemos observar que os domínios de integridade filiais incluem todos os subdomínios do corpo racional. Por último, estabelecemos uma ligação entre os grupos abelianos divisíveis e os anéis filiais.

Bibliografia

[1] Andruszkiewicz, R. e Puczylowski; On filial rings, *Portugaliae Mathematica*, 45:139-149, 1988.

[2] Conrad, K.; *The gaussian integers*, em http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/Zinotes.pdf (acedido: 2 de Julho de 2011).

[3] Divinski, N.; *Rings and radicals*, University of Toronto Press, London, 1965.

[4] Ehrlich, G; Filial rings, *Portugaliae Mathematica*, 42:185-194, 1983/84.

[5] Hungerford, T.; *Algebra*, Springer, New York, 1974.

[6] Kertész, A.; *Lectures on artinian rings*, Akadémiai Kiadó, Budapest, 1987.

[7] McCoy, N.; *The theory of rings*, The Macmillan Company, New York, 1964.

[8] Rosen, K.; *Elementary number theory and its applications*, Addison - Wesley Publishing Company, Massachusetts, 1993.

[9] Szász, F.; *Radicals of rings*, Akadémiai Kiadó, Budapest, 1981.