UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

CENTRO DE EDUCAÇÃO E SAÚDE

UNIDADE ACADÊMICA DE EDUCAÇÃO

Curso de Graduação em Licenciatura em Matemática

Francilene Almeida Sousa

ESPECTRO PRIMO:

Uma Aplicaçao de Ideais Primos e Maximais

Cuité-PB

2015

Francilene Almeida Sousa

ESPECTRO PRIMO

Uma Aplicação de Ideais Primos e Maximais

TCC apresentado ao curso Graduação em Licenciatura em Matemática do Centro de Educação e Saúde da Universidade Federal de Campina Grande em cumprimento às exigências do Componente Curricular Trabalho Acadêmico Orientado, para obtenção do grau de Graduado em Licenciatura em Matemática.

Orientador: Prof. Dr. Aluizio Freire da Silva Junior

Cuité-PB

2015

FICHA CATALOGRÁFICA ELABORADA NA FONTE
Responsabilidade Jesiel Ferreira Gomes – CRB 15 – 256

S725e Sousa, Francilene Almeida.

Espectro primo: uma aplicação de ideais primos e maximais. / Francilene Almeida Sousa. – Cuité: CES, 2015.

50 fl.

Monografia (Curso de Licenciatura em Matemática) – Centro de Educação e Saúde / UFCG, 2015.

Orientador: Aluizio Freire da Silva Junior.

1. Ideais primos. 2. Ideais maximais. 3. Topologia. I. Título.

CDU 51

Francilene Almeida Sousa

ESPECTRO PRIMO

Uma Aplicação de Ideais Primos e Maximais

Monografia de Trabalho de Conclusão de Curso submetida à banca examinadora como parte dos requisitos necessários a obtenção do grau de Graduação em Licenciatura em Matemática.

A citação de qualquer trecho deste trabalho é permitida, desde que seja feita de conformidade com as normas de ética científica.

Trabalho de Conclusão de Curso (TCC) aprovado em 25 de novembro de 2015.

BANCA EXAMINADORA

Prof. Dr. Aluizio Freire da Silva Junior - UFCG
(Orientador)

Msc. Edna Cordeiro de Souza - UFCG

Msc. Marciel Medeiros de Oliveira - UFCG

Aos meus familiares, especialmente a minha mãe Maria de Fátima e meu noivo Ramon de Farias que me ajudaram a realizar este sonho.

Agradecimentos

Agradeço primeiramente a Deus por ter me concedido o término deste curso. Aos meus pais: Genaldo Balbino e Maria de Fátima por serem minha força, meu refúgio e foram peças fundamentais na concretização deste sonho.

Aos meus queridos irmãos: Francisco de Assis, Francinaldo, Francineide e Francinalva, os quais estavam sempre presentes nos momentos mais difíceis e sempre me deram total apoio.

As minhas sobrinhas, Maria Clara, Mikaely e Heloisa, as quais são pessoas muito especiais e que amo muito.

Ao meu noivo Ramon de Farias, que foi tão paciente e dedicado para comigo, sempre me dando apoio e ajudando a superar as dificuldades.

Ao meu professor orientador Aluízio, por seu compromisso e dedicação e por ter acreditado em mim em todos os momentos.

Aos professores que tive o privelégio de estudar e contribuiram para minha formação, em especial: Aluízio Freire, Gisélia Vasconcelos, Márcia Cristina, Célia Franco, Maria de Jesus, Glageane Sousa, Renato Ignácio, Maciel Medeiros, Anselmo Lopes, Jorge Alves, entre outros.

Ao professor e coordenador Alecxandro Alves do PIBID/matemática, por ter me dado a oportunidade de ser integrante deste projeto, o qual foi de suma importância para a minha formação e só veio a fortalecer ainda mais o meu desejo de exercer a profissão.

A minha querida amiga/irmã Jucileide Almeida, por todo apoio e carinho que me proporcionou, mesmo depois que concluiu o curso, sempre esteve ao meu lado e por ser minha melhor amiga. Obrigada por tudo.

Aos meus amigos e colegas do PIBID e de curso, Josevandro Barros, Maria Ioneris, José filho, Leonardo, Gerivaldo Bezerra, Silvana Santos, Fabíola Martins, José Joelson, João Crispim, José Francisco, Robéria, Ysmênia Karla, Aparecida Lima, Edvenilson, Paula Francinete, entre outros. A professora Cida e Professora Suênia, e todos que participaram da minha vida acadêmica.

Enfim agradeço a todos da UFCG, que de alguma maneira contribuiram para a minha formação acadêmica.

"Por isso não tema, pois estou com você; não tenha medo, pois sou o seu Deus. Eu o fortalecerei e o ajudarei; eu o segurarei com a minha mão direita vitoriosa"

Isaías 41:10

Resumo

Este trabalho tem como objetivo construir uma topologia sobre um anel comutativo com unidade. Para isto, inicialmente foi feita uma revisão sobre os conceitos de anéis, ideais primos e maximais assim como também de anéis quociente. Em seguida, apresentamos definições de anel nilpotente e inversível, fizemos o uso do lema de Zorn, do princípio da boa ordenação e do algoritmo da divisão. Para o estudo de topologia apresentamos os conceitos básicos e importantes, indo desde as noções elementares de abertos e fechados e conexidade. Finalmente construímos uma topologia sobre um conjunto de ideais primos de um anel comutativo com unidade. Através deste trabalho percebemos que é possível fazer aplicações da álgebra na topologia, contribuindo assim para o ensino da matemática superior.

Palavras-chave: Ideais primos. Ideais maximais. Topologia.

Abstract

This work aims to construct a topology over a commutative ring with unit. For this, it was firstly done a review on the concepts rings, prime ideals and maximal as well as quotient rings. Then we present definitions nilpotent and invertible ring, we use the precept of Zorn, the well-ordering principle and the division algorithm. For the topology of study we introduced the basic and important idea, ranging from the elementary notions of open and closed and connectivity. Ultimately we built a topology on a set of prime ideals of a commutative ring with unity. Through this work we understand it is possible to make applications of algebra in topology, thus contributing to the higher education of mathematics.

Keywords: Prime ideals. Maximal ideals. Topology.

Sumário

Introdução **9**

1 Aspectos Históricos **11**

2 Anéis **15**

2.1 Tipos de Anéis 16

2.2 Exemplos 17

2.3 Subanéis 21

2.4 Ideais 23

2.5 Ideais Maximais e Primos 28

2.6 Anéis Quociente 29

3 Aplicações de Ideais Maximais e Primos **33**

3.1 Nilradical e Radical Jacobson 39

3.2 Espectro Primo 45

Conclusão **49**

Referências Bibliográficas **50**

Introdução

A Álgebra é um ramo da matemática, que trata dentre outros conteúdos o estudo das estruturas algébricas. Inicialmente a álgebra se preocupava muito com o estudo das equações e suas incógnitas. Porém por volta de 1830 na Inglaterra, os matemáticos Georg Peacock (1791-1858), Duncan Farquharson Gregory (1813-1844), Augustus de Morgan (1806-1871) e William Rowan Hamilton (1805-1865) expandiu os estudos da álgebra para diversas áreas bem mais complexas e um tanto abstratas como o estudo dos grupos, anéis e corpos

Na metade do século XIX os matemáticos Abel (1802 - 1829) e Galois (1811 - 1832) desenvolveram novos conceitos algébricos. Um dos conceitos presentes na obra de Abel e Galois, era a definição implícita de corpo. Durante esse período de surgimento de novas álgebras, aconteceu amplas generalizações quanto a número e aritmética.

O matemático Ernst Eduard Kummer (1810-1893) também deu sua contribuição para a álgebra moderna, este matemático introduziu o conceito de "ideal", tendo como base a noção de Anel. Dizemos que um conjunto de elementos forma um anel se 1) é um grupo abeliano com relação a adição; 2) o conjunto é fechado com relação à multiplicação e 3) a multiplicação é associativa e é distributiva com relação à adição.

Notemos que o desenvolvimento de novos conceitos da álgebra, foram de suma importância para a construção de uma base mais sólida, no entanto não iremos aqui dar um maior aprofundamento nesta área, iremos estudar conceitos básicos de anéis e ideais, mais precisamente faremos aplicações da topologia em ideais primos e maximais. Diante disso, este trabalho está pautado da seguinte forma:

O capítulo 1 está inteiramente dedicado aos aspectos históricos da teoria de anéis, enfatizamos sobre sua origem, os principais colaboradores para o desenvolvimento dessa teoria e nos dedicamos a expor a respeito da matemática Emmy Noether a qual deu sua maior contribuição na caracterização da definição de Anel.

No capítulo 2 temos a teoria básica de anéis e apresentaremos definições de anéis subanéis, anéis quociente e ideais primos e maximais, falaremos das propriedades de anéis e suas características, assim como também, faremos uma exposição de exemplos de anéis comutativos e não comutativos.

No capítulo 3 abordaremos sobre aplicações de ideais maximais e primos, neste capítulo consideraremos que todos os anéis são comutativos e com unidade, apresentaremos definições de anel nilpotente e inversível, faremos o uso do lema de Zorn, assim como também do princípio da boa ordenação e do algoritmo da divisão. Abordaremos um estudo rápido da topologia geral. Para tal falaremos dos principais conceitos e exemplos de um curso introdutório de topologia, indo desde as noções elementares de abertos e fechados e conexidade. E finalizaremos com a aplicação da topologia em ideais primos e maximais.

Capítulo 1

Aspectos Históricos

Neste capítulo buscaremos expor brevemente um estudo do surgimento da teoria de anéis, faremos uma apresentação geral de alguns acontecimentos históricos, destacando os fatos importantes que estão relacionados com a construção desta teoria. Daremos destaque aos matemáticos: Adolf Fraenkel (1891- 1965), Richard Dedekind (1831-1916), David Hilbert (1862-1945) e Edmund Lasker (1868-1941), que tiveram papel fundamental neste desenvolvimento. E logo depois veremos que a matemática Emmy Noether (1882-1935) deu sua maior contribuição no avanço desta teoria, dando-se origem a teoria dos Anéis.

Em 1893 surgiu a teoria abstrata de corpos introduzida pelos matemáticos Heinrich Weber (1842-1913), Leonard Eugene Dickson (1874-1954) e Edward V. Huntington (1874-1952). Eles deram suas contribuições nas definições de corpo através de conjuntos de postulados. Em meados de 1908, Kurt Hensel (1861-1941) introduziu um novo tipo de corpo: o corpo dos números p- ádicos que tem, também, aplicações na teoria algébrica de números.

No século XX surgiram as primeiras definições da teoria abstrata de anéis, e toda a teoria de anéis que estudamos hoje em dia é resultado de trabalhos de matemáticos dos últimos 80 anos. A teoria dos anéis cresceu a partir do estudo de duas classes particulares de anéis, anéis de polinômios em n variáveis sobre os números reais ou complexos e os inteiros de um número algébrico. (FRALEIGH, 2003)

Neste sentido podemos citar o matemático Adolf Fraenkel (1891- 1965) que em 1914 deu inicio a definição abstrata de Anel, tendo em vista que o nome Anel já tinha sido usado por volta do século XIX, através do trabalho de generalizar o teorema fundamental Aritmética a contextos mais abstratos do matemático Richard Dedekind (1831-1916) e também em alguns trabalhos dos matemáticos David Hilbert (1862-1945), Edmund Lasker (1868-1941) e F. S. Macaulay (1862-1927), o qual tratava de anéis de polinômios.

Adolf Fraenkel que nasceu em 17 de fevereiro de 1891, em Munique, Alemanha, filho de Sigmund e Charlotte (Neuberger) Fraenkel, avançou rapidamente em seus estudos globais e estudou em várias universidades, a primeira universidade que ele iniciou seus estudos superiores foi na Universidade de Munique e posteriormente, estudou nas universidades alemãs de Marburg, Berlim e Breslau. Com 23 anos Fraenkel recebeu o seu diploma de doutorado em matemática.

Adolf Fraenkel (1891-1965) foi o matemático que explorou a teoria de anéis em seu artigo intitulado de "On the divisors of zero and the decomposition of rings", ele fez o uso da primeira caracterização axiomática da ideia de anel. Ilustrando a abrangência do conceito, ele deu vários exemplos de anéis: inteiros módulo n, sistemas de números hipercomplexos, matrizes e inteiros p-ádicos. Ele tinha por objetivo sair do estudo particular dos corpos, de maneira a obter uma teoria satisfatória para poder ser aplicadas aos inteiros módulo n, aos números p-ádicos e aos sistemas de "números hipercomplexos."

De acordo com Milies, a definição de anel de Adolf Fraenkel é muito próxima da atual. Ele considera um sistema com duas operações, que chama de soma e produto e estabelece que, em relação à soma, o sistema deve formar um grupo. Sobre o produto, ele especifica que deve ser associativo e distributivo em relação à soma e inclui a existência de um elemento unidade. A comutatividade da soma, que não foi postulada, é demonstrada a partir destes axiomas, bem como uma série de resultados elementares.

Outro matemático que contribuiu para o avanço da teoria de anéis foi a Alemã Amalie Emmy Noether (1882-1935) uma das mais importantes matemáticas no campo da álgebra.

No artigo "Ideal Theory in Rings"(1921) Noether prova que cada ideal em um anel é finitamente gerado se, e só se a condição de inclusão em cadeia ascendente (a.c.c.) é satisfeita, já no artigo "Abstract Study of Ideal Theory in Algebraic Number and Function fields (1927)", a matemática caracteriza os anéis comutativos nos quais todo ideal é um produto único de ideais primos ("principais"). Atualmente, tais anéis são chamados Domínios de Dedekind. Em ambos os trabalhos Noether fez uma caracterização para um anel abstrato generalizando o que Richard Dedekind (1831-1916) realizara para o anel de números algébricos em 1871.

Emmy Noether nasceu em Erlangen, na Alemanha, em 23 de Março de 1882, uma matemática e física alemã, considerada como a criadora da álgebra moderna, ficou conhecida por seu trabalho no estudo da álgebra, tendo desenvolvido vários conceitos matemáticos inovadores ao longo de sua carreira.

Figura 1.1: Amalie Emmy Noether (1882 - 1935)
Fonte: AZNAR(2007)

Filha de Max Noether um ilustre matemático da universidade de Erlarge que trabalhou na teoria das funções algébricas e de Ida Amalia Kaufmann Noether. Dois de seus irmãos tornaram-se cientistas, Fritz foi um matemático e Alfred obteve um doutoramento em química e desde de pequena ela aprendeu a estudar matemática com o pai.

Emmy Noether, estudou alemão, inglês, francês, aritmética e deu aulas de piano. Em 1900 ela começa a lecionar nas escolas de meninas da Baviera. Aos 18 anos, Emmy decidiu estudar matemática na Universidade de Erlangen, onde seu irmão estudava e seu pai lecionava, porém pelo fato de ser mulher, a universidade recusou sua matrícula, lhe concedendo apenas a permissão para ser aluna ouvinte. Em 1903, passou no exame em Nurnberg e foi para a Universidade de Göttingen. Estudou com Blumenthal, Hilbert, Klein e Minkowski, e em 1904 conseguiu permissão para se matricular em Erlangen, onde dedicou-se exclusivamente ao estudo da matemática, atitude esta difícil para uma mulher naquela época enfrentando os preconceitos da época e a rejeição.

Em 1908, ela conclui sua dissertação intitulada: "On Complete Systems of Invariants for Ternary Biquadratic Forms", donde obteve seu doutorado. Emmy Noether tornou-se a mulher mais importante da história da matemática, sendo considerada uma grande algebrista que além de ter trabalhado com álgebra abstracta, dando atenção especial aos anéis, grupos e corpos, trabalhou também na teoria dos ideais e das álgebras não-comutativa. Porém em 1935 ela teve complicações de uma cirurgia para remover um tumor uterino devido esse fato ela veio falecer no dia 14 de Abril de 1935, com 53 anos.

Capítulo 2

Anéis

Este capítulo será dedicado a apresentação de algumas definições básicas de Anéis, ideais e anéis quociente, além de ideais maximais e primos, que são necessárias para o entendimento do nosso trabalho.

Definição 2.1. *Seja A um conjunto não vazio onde estejam definidas duas operações, as quais chamaremos de produto* $(\cdot)$ *e soma* $(+)$ *em* A*, da forma:*

$$\begin{array}{rccc} + : & A \times A & \longrightarrow & A \\ & (a,b) & \longmapsto & a+b \end{array} \quad \text{e} \quad \begin{array}{rccc} \cdot : & A \times A & \longrightarrow & A \\ & (a,b) & \longmapsto & a \cdot b \end{array}$$

Dizemos que A é um anel, e denotamos por $(A, +, \cdot)$, se as seguintes propriedades são satisfeitas para quaisquer que sejam a, b, $c \in$ A:

$(A1)$ $(a+b)+c = a+(b+c)$; (associatividade da soma)

$(A2)$ Existe $0 \in A$ tal que $a+0 = 0+a = a$; (existência do elemento neutro)

$(A3)$ Para qualquer $a \in A$ existe um único $b \in A$, denotado por $b = -a$, tal que $a+b = b+a = 0$; (existência do inverso aditivo)

$(A4)$ $a+b = b+a$; (comutatividade da soma)

$(A5)$ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$; (associatividade do produto)

$(A6)$ $a \cdot (b+c) = a \cdot b + a \cdot c$ e $(a+b) \cdot c = a \cdot c + b \cdot c$. (distributividade do produto em relação a soma)

Observação 2.1. *Note que o elemento neutro da proposição A_2 é único.*

Demonstração. *De fato, por A_2*

$$a + 0 = 0 + a = a \ \ \forall a \ \ \in A$$

Suponhamos que existe outro elemento neutro da adição $0' \in A$ tal que $\forall a \in A$ temos que

$$a + 0' = 0' + a = a.$$

Daí, como $0'$ é neutro, temos $0 = 0' + 0$ e como 0 é neutro, temos

$$0' = 0 + 0'$$

por A_4, segue que $0 = 0'$. Assim temos a unicidade do elemento neutro. ■

2.1 Tipos de Anéis

O objetivo desta seção é explorar os anéis comutativos, não comutativos, com unidade e sem unidade.
Por simplicidade em alguns caso usarei A para denotar anel em invés de $(A, +, .)$, ficando subentendido as operações.

Definição 2.2. *Um anel $(A, \cdot, +)$ é chamado* ***anel com unidade****, se:*

$$\exists 1 \in A, 0 \neq 1, \ \textit{tal que } x \cdot 1 = 1 \cdot x = x, \forall x \in A.$$

Definição 2.3. *Dizemos que um anel $(A, +, \cdot)$ é* ***comutativo****, se:*

$$\forall x, y \in A, \ x \cdot y = y \cdot x.$$

Definição 2.4. *Dizemos que um anel $(A, +, \cdot)$ é um* ***anel sem divisores de zero****, se:*

$$x, y \in A, x \cdot y = 0 \Rightarrow x = \textit{0 ou } y = \textit{0}.$$

Se $x \in A, x \neq 0$, dizemos que x é um divisor de zero se existe $y \in A, y \neq 0$, tal que

$$x \cdot y = 0.$$

Definição 2.5. *Se $(A, +, \cdot)$ é um anel comutativo, com unidade e sem divisores de zero, dizemos que $(A, +, \cdot)$ é um* ***domínio de integridade****.*

Definição 2.6. *Dizemos que um anel comutativo com unidade $(A, +, \cdot)$ é um* ***corpo*** *, se:*

$$\forall x \in A, x \neq 0, \exists y \in A, \ \textit{denotado por}\, y = x^{-1}, \ \ \textit{tal que} \ \ xy = yx = 1.$$

Proposição 2.1. *Todo corpo é um domínio de integridade.*

Demonstração. Consideremos $(A, +, \cdot)$ um corpo. Por definição temos que um corpo é um anel comutativo com unidade, deste modo falta-nos provar que $(A, +, \cdot)$ não possui divisores de zero, suponhamos por absurdo que $(A, +, \cdot)$ tenha divisores de zero, deste modo, existem $x, y \in A$ tais que,

$$x \neq 0, \ \ y \neq 0 \ \ e \ \ x \cdot y = 0.$$

Daí, como todo elemento possui inverso multiplicativo, temos

$$\begin{aligned} x^{-1} \cdot (x \cdot y) &= x^{-1} \cdot 0 \\ (x^{-1} \cdot x) \cdot y &= 0 \\ 1 \cdot y &= 0 \\ y &= 0 \end{aligned}$$

o que é um absurdo, pois por hipótese $y \neq 0$. Daí concluimos que A não possui divisores de zero e portanto todo corpo é um domínio de integridade. ■

2.2 Exemplos

Nesta seção, mostraremos alguns exemplos de anéis para melhor compreensão.

Exemplo 2.1. *Notemos que os conjuntos $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$ e $\mathbb{C}$, munidos das operações usuais de soma e produto, são anéis comutativos.*

Exemplo 2.2. *Notemos que o conjunto $n\cdot$ $\mathbb{Z}$, munido das operações de soma e produto usuais é um anel comutativo e sem divisores de zero.*

Exemplo 2.3. *O conjunto*

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Z}\}$$

munido das operações,

$$\begin{aligned} (a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a + c) + (b + d)\sqrt{2} \\ (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) &= (ac + 2bd) + (ad + bc)\sqrt{2} \end{aligned}$$

É um anel.

Mostraremos que $\mathbb{Z}[\sqrt{2}]$ *é comutativo. De fato, sejam* $(x + y\sqrt{2}), (w + z\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$*, temos*

$$(x + y\sqrt{2}) \cdot (w + z\sqrt{2}) = (xw + 2yz) + (xz + yw)\sqrt{2}$$

Como w, x, y e z são elemento de $\mathbb{Z}$*, então são comutativos. Logo,*

$$(xw + 2yz) + (xz + yw)\sqrt{2} = (zx + 2wy) + (yx + zy)\sqrt{2} = (w + z\sqrt{2}) \cdot (x + y\sqrt{2})$$

Agora mostraremos que $\mathbb{Z}[\sqrt{2}]$ *possui unidade*
consideremos,

$$a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \text{ e } 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

Daí,

$$(a + b\sqrt{2})(1 + 0\sqrt{2}) = (a + 0) + (0 + b)\sqrt{2} = a + b\sqrt{2}$$

Pela proposição da comutatividade que já foi demonstrada temos,

$$(1 + 0\sqrt{2})(a + b\sqrt{2}) = (a + b\sqrt{2}).$$

Logo $(1 + 0\sqrt{2})$ *é a unidade de* $\mathbb{Z}[\sqrt{2}]$*, e portanto* $\mathbb{Z}[\sqrt{2}]$ *é um anel comutativo e com unidade.*

Exemplo 2.4. $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, ..., \overline{n-1}\}$ *possui divisores de zero se n é composto. Por exemplo em* $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$*, temos* $\bar{2} \cdot \bar{3} = \bar{0}$*, mas* $\bar{2} \neq \bar{0}$ *e* $\bar{3} \neq \bar{0}$*. Neste caso,* $\bar{2}$ *e* $\bar{3}$ *são divisores de zero em* $\mathbb{Z}_6$*.*

Exemplo 2.5. $\mathbb{Z}$ *e* $\mathbb{Z}_n$ *com n compostos não são corpos. Por exemplo em* $\mathbb{Z}$ *o inverso de 2 é* $\frac{1}{2} \notin \mathbb{Z}$*.*

Exemplo 2.6. $\mathbb{Z}[\sqrt{2}]$ *não é corpo.*

De fato, seja $(a+b\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$, *com* $a \neq 0$ *ou* $b \neq 0$ *e suponha que existe* $(c+d\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$, *tal que*

$$(ac+2bd)+(ad+bc)\sqrt{2} = 1+0\sqrt{2}$$

Daí temos,

$$\begin{cases} ac+2bd = 1 \quad (I) \\ ad+bc = 0 \quad (II) \end{cases}$$

De (I), temos

$$ac = 1-2bd \Rightarrow c = \frac{1-2bd}{a} \quad (III)$$

substituindo (III) em (II), obtemos

$$ad + b\cdot\frac{1-2bd}{a} = 0 \Rightarrow d(a^2-2b^2) = -b \Rightarrow d = \frac{-b}{a^2-2b^2} \quad (IV)$$

substituindo (IV) em (III), temos

$$c = \frac{a}{a^2-2b^2}.$$

Portanto, $c \notin \mathbb{Z}$ *e* $d \notin \mathbb{Z}$. *Assim* $(c+d\sqrt{2}) \notin \mathbb{Z}[\sqrt{2}]$, *o que é uma contradição. Daí, não existe* $(c+d\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$ *tal que,* $(a+b\sqrt{2})(c+d\sqrt{2}) = 1+0\sqrt{2}$. *Logo,* $\mathbb{Z}[\sqrt{2}]$ *não é um corpo.*

Exemplo 2.7. $\mathbb{Q}[\sqrt{2}]$ *é um corpo.*

De fato, seja $(a+b\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$, *com* $a \neq 0$ *ou* $b \neq 0$ *e suponha que existe* $(c+d\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$, *tal que*

$$(ac+2bd)+(ad+bc)\sqrt{2} = 1+0\sqrt{2}$$

Pelo o exemplo anterior, temos que $d = \frac{-b}{a^2-2b^2}$ *e* $c = \frac{a}{a^2-b^2}$. *Portanto* $c \in \mathbb{Q}$ *e* $d \in \mathbb{Q}$ *e* $(c+d\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$. *Logo* $\mathbb{Q}[\sqrt{2}]$ *é um corpo.*

Exemplo 2.8. *Anel* ***não-comutativo***

Seja A *o conjunto de todas as matrizes reais* 2×2, *isto é,*

$$A = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}; a,b,c,d \in \mathbb{R} \right\}.$$

Dizemos que $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \Leftrightarrow \begin{cases} a = a', \quad b = b' \\ c = c', \quad d = d' \end{cases}$

Definiremos as operações $+$ *e* $\cdot$ *no conjunto* A *acima o qual denotamos por* $Mat_2(\mathbb{R})$. *Dados* $a, b, c, d, a', b', c', d' \in \mathbb{R}$, *temos*

$$Soma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a+a' & b+b' \\ c+c' & d+d' \end{bmatrix}$$

$$Produto = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{bmatrix}.$$

Notemos que $Mat_2(\mathbb{R})$ *munida das operações soma e produto definidas é um anel, além disso,*

$0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, *é o elemento neutro de* $Mat_2(\mathbb{R})$.

Mostraremos que $Mat_2(\mathbb{R})$ *é um anel com unidade, não comutativo e com divisores de zero. Temos que,*

$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ *é a unidade de* $Mat_2(\mathbb{R})$

De fato, considere

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Mat_2(\mathbb{R})$, *temos*

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Daí temos que $Mat_2(\mathbb{R})$ *é um anel com unidade.*

Notemos que se $a \in \mathbb{R}$ *e* $X_a = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \in Mat_2(\mathbb{R})$ *e* $X_b = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \in Mat_2(\mathbb{R})$, *então*

$$X_a \cdot X_b = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \forall a, b, \in \mathbb{R}.$$

Assim o anel $(Mat_2(\mathbb{R})\ +, \cdot)$ *possui uma infinidade de divisores de zero. Vejamos também*

$$\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Ou seja, a equação $x^2 = 0$ *possui infinitas soluções no anel* $Mat_2(\mathbb{R})$
Agora consideremos os seguintes elementos:

$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ *e* $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ *de* $Mat_2(\mathbb{R})$ *e calculemos:*

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

Daí temos que:

$$\begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

Portanto, conclui-se que $Mat_2(\mathbb{R})$ *é um anel não comutativo.*

2.3 Subanéis

O conceito de subanéis é indispensável para nosso estudo de anéis, tendo em vista que é de suma importância no desenvolvimento do nosso trabalho. Nesta seção detalharemos mais sobre o tema.

Definição 2.7. *Seja $(A, +, \cdot)$ um anel e B um subconjunto não vazio de A. Suponha que:*

i) $x, y \in B \Rightarrow x + y \in B$;

ii) $x, y \in B \Rightarrow x \cdot y \in B$.

*Dizemos que $(B, +, \cdot)$ é um **subanel** de A, se B é um anel com as operações de A. Denotaremos por $B \leqslant A$.*

Proposição 2.2. *Sejam $(A, +, \cdot)$ um anel e B um subconjunto de A. Então B é um subanel de A se, e somente se, as seguintes condições forem satisfeitas:*

i) $0 \in B$; (o elemento neutro de A pertence a B)

ii) $x, y \in B \Rightarrow x - y \in B$; (B é fechado para a diferença)

iii) $x, y \in B \Rightarrow x \cdot y \in B$. (B é fechado para o produto)

Demonstração. ($\Rightarrow$) Suponhamos que B é um subanel de A. Temos que verificar as seguintes condições i), ii) e iii);

Como B é subanel, se $b \in B$, então $-b \in B$, assim $0 = b + (-b) \in B$.

ii) Sejam $x, y \in B$. Como B é subanel, então $-y \in B$, assim

$$x - y = x + (-y) \in B.$$

iii) Como B é subanel, por definição,

$$x, y \in B \Rightarrow x \cdot y \in B$$

($\Leftarrow$) Por i), segue que $B \neq \varnothing$ e por (i) e (ii) temos que

$$\text{se } x \in B, \text{então} - x = 0 - x \in B. \tag{2.1}$$

Agora, por (ii) e por (2.1) teremos que, se $x, y \in B$ então, $x + y = x - (-y) \in B$, isto é, B é fechado para a soma. Por (iii) B é fechado para o produto. Como todo elemento de B é elemento de A, segue que as propriedades, A_1, A_4, A_5 e A_6 são satisfeitas.

■

Exemplo 2.9. *Mostre que $\mathbb{Z}[\sqrt{p}] \leqslant \mathbb{R}$, como p número primo.*

De fato, seja $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p}; a, b \in \mathbb{Z}\}$, temos que verificar as condições i), ii) e iii).

i) Note que $0 = (0 + 0\sqrt{p}) \in \mathbb{Z}[\sqrt{p}]$;

ii) Provaremos que $x - y \in \mathbb{Z}[\sqrt{p}]$;

Consideremos $x = a + b\sqrt{p}$ *e* $y = c + d\sqrt{p}$; $a, b, c, d \in \mathbb{Z}$, *temos que*

$$(a + b\sqrt{p}) - (c + d\sqrt{p}) = (a - c) + (b - d)\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$$

iii) Agora mostraremos que $x \cdot y \in \mathbb{Z}[\sqrt{p}]$.

$$(a + b\sqrt{p})(c + d\sqrt{p}) = (ac + pbd) + (ad + bc)\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$$

Como as condições foram satisfeitas, segue que $\mathbb{Z}[\sqrt{p}]$ *é subanel de* $\mathbb{R}$.

Proposição 2.3. *As únicas soluções da equação* $x^2 = x$ *em um domínio de integridade são* 0 *e* 1.

Demonstração. *Seja* D *um domínio de integridade e* $x \in D$ *tal que*

$$x^2 - x = (x - 1) \cdot x = 0$$

e daí segue que $x - 1 = 0$ *ou* $x = 0$. *Como queríamos demonstrar.* ■

Corolário 2.1. *Seja* D *um domínio de integridade com unidade* 1 *e seja* B *um subanel de* D *com unidade* $1'$. *Então* $1 = 1'$.

Demonstração. *Temos que,*

$$(1')^2 = 1' \cdot 1' = 1'$$

pela proposição anterior, temos

$$1' = 0 \quad ou \quad 1' = 1.$$

Como $1'$ *é unidade, segue que* $1' \neq 0$. *Logo* $1' = 1$. ■

2.4 Ideais

O conceito de ideal, generalizado para anéis quaisquer é uma das ferramentas mais importante para o desenvolvimento da teoria dos anéis. Nesta seção faremos um estudo sobre ideais à esquerda e à direita, assim como também os ideias triviais. No decorrer dos estudos veremos exemplos para melhor entendimento do tema.

Definição 2.8. *Sejam A um anel e I um subanel de A. Dizemos que I é um ideal à esquerda de A, se:*

$$a \cdot x \in I, \forall a \in A \;\; e \;\; \forall x \in I$$

Simbolicamente, $A \cdot I \subset I$.

Definição 2.9. *Sejam A um anel e J um subanel de A. Dizemos que J é um ideal à direita de A, se:*

$$x \cdot a \in J, \forall a \in A \;\; e \;\; \forall x \in J$$

Simbolicamente, $J \cdot A \subset J$.

Se I é simultaneamente um ideal à esquerda e à direita de um anel A, dizemos que I é um ideal de A.

Claramente, $\{0\}$ e A são ideais de A chamados ideais triviais de A. Os ideais não triviais de A são chamados de ideais próprios de A.

Observação 2.2. *Note que se A é comutativo, então todo ideal à esquerda ou a direita é um ideal.*

Exemplo 2.10. *Verifique se o subanel $\{\bar{0}, \bar{2}\}$ é um ideal do anel $(\mathbb{Z}_4, +, \cdot)$. Seja $I = \{\bar{0}, \bar{2}\} \subset (\mathbb{Z}_4, +, \cdot)$, verificaremos que:*

$$a \cdot x \in I \;\; \forall x \quad \in I, \forall a \in \mathbb{Z}_4$$

De fato:

Para $x = \bar{0}$

$$\bar{0} \cdot \bar{0} = \bar{0} \in I$$

$$\bar{0} \cdot \bar{1} = \bar{0} \in I$$

$$\bar{0} \cdot \bar{2} = \bar{0} \in I$$

$$\bar{0} \cdot \bar{3} = \bar{0} \in I$$

Para $x = \bar{2}$

$$\bar{2} \cdot \bar{0} = \bar{0} \in I$$
$$\bar{2} \cdot \bar{1} = \bar{0} \in I$$
$$\bar{2} \cdot \bar{2} = \bar{0} \in I$$
$$\bar{2} \cdot \bar{3} = \bar{0} \in I$$

Como $\mathbb{Z}_4$ *é comutativo, então* I *é um ideal.*

Exemplo 2.11. *Vamos agora ver um exemplo de ideais no anel* $A = C[0,1]$*, das funções contínuas* $f : [0,1] \to \mathbb{R}$ *com as operações usuais de* $+$ *e* $\cdot$ *de funções. Sabemos que* A *é um anel comutativo com unidade* 1 *(função constante igual a 1). Seja* $b \in [0,1]$ *e seja* $I = \{f \in A; f(b) = 0\}$*. Provemos primeiramente que* I *é um subanel de* A*.*
De fato,
(i) $0 \in I$*, pois* 0 *é a função constante zero.*
(ii) - (iii) Se $f, g \in I$ *então* $(f - g) \in I$*, pois* $(f - g)(b) = f(b) - g(b) = 0$*.*
Alem disso,

$$(f \cdot g)(b) = f(b) \cdot g(b) = 0 \cdot 0 = 0$$

Portanto, $f \cdot g \in I$*. Logo,* I *é subanel de* A*.*
Agora iremos mostrar, que I *é ideal. Sejam* $h \in A$ *e* $g \in I$*, então*

$$(h \cdot g)(b) = h(b) \cdot g(b) = h(b) \cdot 0$$

Portanto, $h \cdot g \in I$*. Analogamente,* $g \cdot h \in I$*. Logo* I *é ideal de* A*.*

Observação 2.3. *Se* I *é um ideal de um anel* A *e* $1 \in I$*, então* $I = A$*.*
De fato, seja $a \in A$*. Então,*

$$a = a \cdot 1 \in I$$

Portanto, $A \subseteq I$*, como* I *é ideal de* A*, segue que* $I \subseteq A$*. Logo,* $I = A$*.*

Exemplo 2.12. *Seja* A *o anel* $Mat_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}; a, b, c, d \in \mathbb{R} \right\}$ *e sejam* I *e* J *definidos como segue:*

$$I = \left\{ \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix}; a, c \in \mathbb{R} \right\} e \ \ J = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}; a, b \in \mathbb{R} \right\}$$

Notemos que I é ideal à esquerda de A e J é um ideal à direita de A.

De fato, sejam $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in A$ *e* $\begin{bmatrix} e & 0 \\ f & 0 \end{bmatrix} \in I$

Daí temos que:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & 0 \\ f & 0 \end{bmatrix} = \begin{bmatrix} ae + bf & 0 \\ ce + df & 0 \end{bmatrix} \in I$$

Deste modo, temos que $A \cdot I \subset I$

Agora, sejam $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in A$ *e* $\begin{bmatrix} g & h \\ 0 & 0 \end{bmatrix} \in J$*, temos que:*

$$\begin{bmatrix} g & h \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ga + hc & gb + ha \\ 0 & 0 \end{bmatrix} \in J$$

.

Porém nenhum dos dois é ideal de A. Agora vamos provar que os únicos ideais de $A = Mat_2(\mathbb{R})$ são os triviais. De fato,

Seja I um ideal de $A = Mat_2(\mathbb{R})$ e vamos assumir que $I \neq \{0\}$. Assim existe,

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in I$$

onde algum dos $a_{ij}'s$ é diferente de zero, $1 \leqslant i, j \leqslant 2$. Sejam $e_{rs} \in Mat_2(\mathbb{R}), 1 \leq r, s \leq 2$, as seguintes matrizes.

$$e_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, e_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, e_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \text{ e } e_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Através de cálculos é fácil verificar que:

$$e_{rs} \cdot \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot e_{mn}$$

É uma matriz 2×2 *contendo o elemento* a_{sm} *na posição (r,n) da matriz, sendo que os demais elementos são nulos. Então temos que* $A \cdot I \subset I$ *e* $I \cdot A \subset I$.

Por exemplo, Consideremos

$$e_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, e_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad e_{rs} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

multiplicando as três matrizes, temos:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & a_{11} \\ 0 & 0 \end{bmatrix}$$

Notemos que é uma matriz 2×2 *contendo o elemento* a_{11} *na posição* a_{12}.

Como $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in I$ *e* I *é o ideal, temos* $e_{1s} \cdot \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot e_{m1} = \begin{bmatrix} a_{sm} & 0 \\ 0 & 0 \end{bmatrix} \in I$

e, $e_{2s} \cdot \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot e_{m2} = \begin{bmatrix} 0 & 0 \\ 0 & a_{sm} \end{bmatrix} \in I$, *onde 1* $\leq s$ *e* $m \leq 2$.

Podemos concluir que $\forall s, m, 1 \leq s, m \leq 2$, *donde:*

$$\begin{bmatrix} a_{sm} & 0 \\ 0 & a_{sm} \end{bmatrix} = \begin{bmatrix} a_{sm} & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & a_{sm} \end{bmatrix} \in I.$$

Escolhamos s *e* m, $1 \leq s, m \leq 2$ *de modo que* $a_{sm} \neq 0$. *Assim,*

$$\begin{bmatrix} a_{sm}^{-1} & 0 \\ 0 & a_{sm}^{-1} \end{bmatrix} \cdot \begin{bmatrix} a_{sm} & 0 \\ 0 & a_{sm} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in I.$$

Como $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ *é a unidade do anel* A, *segue então que* $I = A$.

2.5 Ideais Maximais e Primos

Definição 2.10. *Seja A um anel comutativo e M um ideal de A tal que $M \neq A$. Dizemos que M é ideal maximal, se os únicos ideais em A que contém M são o próprio M e A.*

Definição 2.11. *O ideal I num anel A diz-se um **ideal principal** se existe $a \in A$ tal que $I =< a >$.*

Definição 2.12. *Um anel de ideais principais A que também é um domínio de integridade é chamado de Domínio de Ideais Principais (DIP).*

Teorema 2.1. *Seja $(K, +, \cdot)$ um anel comutativo com unidade $1 \in K$. Então as seguintes condições são equivalentes.*
i) K é um corpo;
ii) $\{0\}$ é um ideal maximal em K;
iii) Os únicos ideais de K são os triviais.

Demonstração. *(i) $\Rightarrow$ (ii) Seja K um corpo e J um ideal de K tal que $\{0\} \subseteq J \subseteq K$. Suponhamos que $J \neq \{0\}$, assim existe $0 \neq a \in J$. Como K é um corpo, então existe $b \in K$ tal que $b \cdot a = 1$, então $1 \in J$ e daí segue que $J = K$.*
(ii) $\Rightarrow$ (iii) Suponha que $\{0\}$ é ideal maximal em K. Seja I um ideal de K tal que $I \neq \{0\}$. Como $\{0\} \subseteq I \subset K$ e $\{0\}$ é maximal, segue que $I = K$. Logo, K possui apenas ideais triviais.
(iii) $\Rightarrow$ (i) Para K ser um corpo falta apenas verificar a definição 2.6, a qual, $\forall a \in K, a \neq 0$, existe $b \in K$ tal que $a \cdot b = b \cdot a = 1$. Seja $0 \neq a \in K$ e $I = K \cdot a$ o ideal principal de K gerado por a. Mas $a = 1 \cdot a \in I$, então $I \neq \{0\}$. Como K possui apenas ideais triviais, temos que $I = K$. Assim $1 \in I = K \cdot a$ e, deste modo, existe $b \in K$ tal que $1 = b \cdot a$. Logo, K é um corpo. ■

Definição 2.13. *Seja P um ideal num anel comutativo A. Diz-se que P é um ideal primo se $P \neq A$ e se qualquer relação do tipo $ab \in P$, em que $a, b \in A$, tiver como consequência que $a \in P$ ou $b \in P$.*

Exemplo 2.13. *Consideremos o anel $\mathbb{Z} \times \mathbb{Z}$ e seja $I = \{0\} \times \mathbb{Z}$ ideal de $\mathbb{Z} \times \mathbb{Z}$. Definiremos as operações $+$ e $\cdot$ no conjunto $\mathbb{Z} \times \mathbb{Z}$.*

$$Soma = (a, b) + (c, d) = (a + c, b + d)$$

$$Produto = (a,b)\cdot(c,d) = (ac,bd).$$

Para $(a,b),(c,d) \in \mathbb{Z}\times\mathbb{Z}$

Note que I é ideal primo. D fato, sejam $(a,b),(c,d) \in \{0\}\times\mathbb{Z} = \{(0,x),\ x\in\mathbb{Z}\}$, *temos* $(a,b)\cdot(c,d) \in \{0\}\times\mathbb{Z} \Rightarrow (ac,bd) \in \{0\}\times\mathbb{Z}$, *então* $ac = 0$, *como* $a,c\in\mathbb{Z}$, *segue que* $a = 0$ *ou* $c = 0$. *Donde* $(a,b)\in\{0\}\times\mathbb{Z}$ *ou* $(c,d)\in\{0\}\times\mathbb{Z}$.

2.6 Anéis Quociente

Esta seção será dedicada ao estudo da definição de equivalência, assim como também a introdução de conjuntos quocientes.

Definição 2.14. *Sejam A um anel qualquer e J um ideal de A. Definiremos a seguinte relação de equivalência em A.*
Denotaremos por $\bar{x}$, *a classe de equivalência de* $x\in A$ *a partir da relação* $\equiv (mod\ J)$.
Assim,

$$\bar{x} = \{y\in A; y\equiv x(mod\ J)\}$$

Notemos que $y\in\bar{x} \Leftrightarrow (y-x)\in J$, *e por isso também denotaremos a classe* $\bar{x}$ *por* $\bar{x} = x + J = \{x+z; z\in J\}$. *Chamaremos de conjunto quociente de A pelo ideal J ao conjunto* $A/J = \{\bar{x} = x+J; x\in A\}$.

Enunciaremos a seguinte duas proposições que nos ajudará nas demonstrações de alguns exemplos, porém ocultaremos suas demonstrações. Mas o leitor que tiver interesse pode consultar em [9].

Proposição 2.4. *Sejam A um anel e J um ideal em A. Se* $\equiv x'(mod\ J)$ *e* $y\equiv y'(mod\ J)$, *então:*
(i) $x+y\equiv(x'+y')(mod\ J)$;
(ii) $x\cdot y\equiv x'\cdot y'(mod\ J)$.

Proposição 2.5. *Sejam A um anel, J um ideal de A. Se* $\overline{x} = \overline{x'}$ *e* $\overline{y} = \overline{y'}$ *então:*
(i) $\overline{x+y} = \overline{x'+y'}$;
(ii) $\overline{x\cdot y} = \overline{x'\cdot y'}$.

Enunciaremos o seguinte resultado, porém não apresentaremos a demonstração. O leitor que tiver interesse pode consultar em [9].

Teorema 2.2. *Seja A um anel e J um ideal de A. Se $\bar{x} = x + J$ e $A/J = \{\bar{x}; x \in A\}$, então:*

(i) As operações em A/J são definidas por:

$$\begin{array}{rcl} + \ : \ A/J \times A/J & \longrightarrow & A/J \\ (\bar{x}, \bar{y}) & \longmapsto & \overline{x+y} = \bar{x} + \bar{y} \end{array} \quad e \quad \begin{array}{rcl} \cdot \ : \ A/J \times A/J & \longrightarrow & A/J \\ (\bar{x}, \bar{y}) & \longmapsto & \overline{x \cdot y} = \bar{x} \cdot \bar{y} \end{array}$$

munidas de duas operações (denominadas soma e produto) em A/J;

(ii) $(A/J, +, \cdot)$ é um anel (chamado anel quociente de A por J);

(iii) Se 1 é a unidade de A então $\bar{1}$ é a unidade de A/J;

(iv) Se A é comutativo então A/J é comutativo.

Exemplo 2.14. $a \in J \Leftrightarrow \bar{a} = \bar{0}$

$(\Rightarrow)$ *De fato,*

$$a = a - 0 \in J$$

Assim, $a \equiv 0 (mod\ J)$. Portanto $\bar{a} = \bar{0}$.

$(\Leftarrow)$ *A recíproca é análoga.*

Exemplo 2.15. $J + L = \{p + q;\ p \in J \ \text{ e } \ q \in L\}$ *é um ideal de A.*

De fato,

(i) Como $0 \in J$ e $0 \in L$, então $0 = 0 + 0 \in J + L$.

(ii) Sejam $r, s \in J + L$, então $r = p_1 + q_1$ e $s = p_2 + q_2$, para elementos convenientes, $p_1, p_2 \in J$ e $q_1, q_2 \in L$. Então $r - s = (p_1 - p_2) + (q_1 - q_2) \in J + L$, uma vez que $(p_1 - p_2) \in J$ e $(q_1 - q_2) \in L$.

(iii) Sejam $t \in J + L$ e $a \in A$. Então $t = p + q$ $(p \in J \ \text{ e } \ q \in L)$ e $at = ap + aq$. Como $ap \in J$ e $aq \in L$, então $at \in J + L$. Logo $J + L$ é ideal de A.

Teorema 2.3. *Seja A um anel comutativo com unidade $1 \in A$ e seja J um ideal de A. então*

J é ideal maximal de A se, e somente se, A/J é um corpo.

Demonstração. $(\Rightarrow)$ Suponhamos J maximal em A. Mostraremos que A/J é um corpo. Consideremos $\bar{a} \neq \bar{0} \in A/J$ e mostraremos que $\bar{a} \neq \bar{0}$ possui inverso. Para isso, considere um ideal principal

$$L = A \cdot a = \{xa; x \in A\}$$

gerado por a. Além disso, temos que

$$J + L = \{p + q; p \in J \ \ e \ \ q \in L\}$$

é ideal e contém J. Por outro lado, temos que $a \notin J$ pois $\bar{a} \neq \bar{0}$. Por isso, $J \neq L + J$. Como J é maximal, segue que $L+J = A$. Como A tem unidade 1, então $1 \in L+J$ e daí

$$1 = u + v$$

com $u \in L$ e $v \in J$. Assim $u = xa$, para algum $x \in A$. Daí $1 = xa + v$, passando a barra, obtemos $\bar{1} = \bar{x}\bar{a} + \bar{v}$, mas $v \in J$, então pelo exemplo 2.14 $\bar{v} = \bar{0}$ e daí $\bar{1} = \bar{x}\bar{a} + \bar{0} \Rightarrow \bar{1} = \bar{x}\bar{a}$. Portanto, o inverso de $\bar{a}$ é $\bar{x}$, logo A/J é um corpo.
$(\Leftarrow)$ Suponhamos que A/J seja um corpo e consideremos $\bar{0}, \bar{1} \in A/J$, temos que $A \neq J$. Mostremos que J é maximal. Seja então um ideal M de A com $M \neq J$ e tal que $J \subset M \subset A$, deste modo, existe $a \in M$, tal que, $a \notin J$, ou seja, $\bar{a} \neq \bar{0}$. Como por hipótese A/J é um corpo, segue que existe $\bar{b} \in A/J$, tal que $\bar{a} \cdot \bar{b} = \bar{1}$. Assim $ab \equiv 1(mod\ J) \Leftrightarrow ab - 1 \in J \Leftrightarrow ab - 1 = x$, com $x \in J$, ou seja, $ab - x = 1$. Mas $a \in M$ (M é ideal), então $ab \in M$ e mais $x \in J \subset M$, então $x \in M$. Deste modo, $1 = ab - x \in M$ o que significa $1 \in M$. Logo, $M = A$, portanto $J \subset M = A$ e daí J é maximal. ■

Teorema 2.4. *Seja A um anel comutativo com unidade $1 \in A$, e seja P um ideal de A. Então:*
(i) P é um ideal primo de A se, e so se A/P é um domínio de integridade;
(ii) Se P é um ideal maximal de A, então P é um ideal primo de A.

Demonstração. (i) $(\Rightarrow)$ Pelo teorema 2.2, como A é comutativo e tem unidade, segue que A/P é um anel comutativo com unidade. Basta provar que A/P não possui divisores de zero. Agora, sejam $\bar{x}, \bar{y} \in A/P$ tais que $\bar{x} \cdot \bar{y} = 0$, ou seja, $xy \in P$. Como P é primo, temos que $\bar{x} \in P$ ou $\bar{y} \in P$. Portanto, $\bar{x} = \bar{0}$ ou $\bar{y} = \bar{0}$. Logo A/P não possui divisores de zero.
$(\Leftarrow)$ Suponhamos que A/P é um domínio de integridade. Iremos mostrar que P é primo. Sejam $x, y \in A$, tais que $xy \in P$. Então $\bar{x}\bar{y} = \bar{0}$. Como A/P é um domínio de integridade, segue que $\bar{x} = \bar{0}$ ou $\bar{y} = \bar{0}$. Portanto $x \in P$ ou $y \in P$. Logo, P é um ideal primo.

(ii) Se P é maximal, então $P \neq A$. Daí, basta provar que, se a e b são elementos de A, tais que $ab \in P$, então $a \in P$ e $b \in P$. Suponhamos que $a \notin P$ e consideremos o ideal $I =< a > +P$. Notemos que $I \supset P$. Como $a = 1 \cdot a + 0$ e $0 \in P$, temos que $a \in I$. Estamos supondo que $a \notin P$, então I contém propriamente P, logo $I = A$. Isto implica que a unidade de A pode ser escrita assim:

$$1 = ra + m$$

Em que r e m são elementos de A e P, respectivamente. Multiplicando -se ambos membros dessa igualdade por b:

$$b = r(ab) + mb$$

Da igualdade temos que $b \in P$, já que tanto ab como m são elementos de P. Logo P é um ideal primo de A. ■

Exemplo 2.16. *O ideal* $\{0\} \times \mathbb{Z}$ *é primo em* $\mathbb{Z} \times \mathbb{Z}$*, como já foi mostrado no exemplo* 2.4*, mas não é maximal.*
De fato, notemos que $2\mathbb{Z} \times \mathbb{Z}$ *é também um ideal em* $\mathbb{Z} \times \mathbb{Z}$*, temos também que* $2\mathbb{Z} \times \mathbb{Z}$ *contém propriamente* $\{0\} \times \mathbb{Z}$ *e que, obviamente* $2\mathbb{Z} \times \mathbb{Z} \neq \mathbb{Z} \times \mathbb{Z}$ *.*

Capítulo 3

Aplicações de Ideais Maximais e Primos

Neste capítulo, veremos uma aplicação de ideais maximais e primos. Nosso objetivo é construir uma topologia no conjunto dos ideais primo de um anel.

Observação 3.1. *A partir de agora todos os anéis serão considerados anéis comutativos e com unidade.*

Definição 3.1. *Sejam A um anel e $a \in A$. Dizemos que a é:*
(i) Nilpotente: se existe $n \in \mathbb{Z}$, com $n > 0$, tal que $a^n = 0$.
(ii) Inversível: se existe $a^{-1} \in A$ tal que $a \cdot a^{-1} = 1$.

Denotaremos por U(A) o conjunto dos elementos inversíveis de A. Note que $U(A) \neq \{0\}$, pois $1 \in U(A)$, qualquer que seja o anel A. Observe que U(A) é fechado para multiplicação. De fato, sejam $a, b \in U(A)$. Então existem $a^{-1}, b^{-1} \in A$ tais que:

$$a \cdot a^{-1} = 1 \ \ e \ \ b \cdot b^{-1} = 1$$

Agora, note que $(ab)^{-1} = b^{-1} \cdot a^{-1}$. Assim,

$$\begin{aligned} (ab)(ab)^{-1} &= ab(b^{-1} \cdot a^{-1}) \\ &= a \cdot a^{-1} \cdot \\ &= 1 \end{aligned}$$

Logo, $a \cdot b \in U(A)$.

Para cada $a \in U(A)$ existe um único $a^{-1} \in A$ tal que $a \cdot a^{-1} = 1$. De fato, suponha que existe $b \in A$, com $b \neq a^{-1}$ tal que,

$$ab = 1$$

Assim,

$$\begin{aligned} a \cdot a^{-1} &= ab \\ a^{-1} &= (a^{-1}a)b \\ a^{-1} &= b \end{aligned}$$

O que é uma contradição, logo a^{-1} é único. Finalmente, temos que $a^{-1} \in U(A)$ e $(a^{-1})^{-1} = a$.

Se $a \in U(A)$ e $n \in \mathbb{Z}$, $n < 0$, defina $a^n := (a^{-1})^{|n|}$.

Exemplo 3.1. *Se $a \in A$, então $(a) = \{ax; x \in A\}$ é um ideal principal gerado por a. Observe que*

$$(a) = A \text{ se, e só se } a \in U(A)$$

Suponhamos que $(a) = A$. Então $1 = ax$, para algum $x \in A$. Portanto $a \in U(A)$. Reciprocamente, suponhamos que $a \in U(A)$. Claramente, $(a) \subset A$. Consideremos, $y \in A$. Como $a \in U(A)$, então $y = a(a^{-1}y) \in (a)$. Portanto $(a) = A$.

Denotaremos por N(A) o conjunto dos elementos nilpotentes de A. Note que, $0 \in N(A)$. O conjunto N(A) é chamado de **nilradical** de A.

Exemplo 3.2. *Note que:*

(1) *Se $x \in N(A)$ então x é divisor de zero.*

(2) *A recíproca de* (1) *não vale*

(3) *Se $x \in U(A)$ então x não pode ser divisor de zero.*

Solução 3.1. (1) *Seja $x \in N(A)$, tal que $x \neq 0$. Então existe $n_1 \in \mathbb{Z}, n_1 > 0$, que satisfaça a condição*

$$x^{n_1} = 0$$

Consideremos n_1 o menor inteiro tal que

$$x^{n_1} = 0$$

Deste modo,

$$x^{n_1-1} \neq 0$$

Daí, $x \cdot x^{n_1-1} = x^{n_1} = 0$. *Logo,* x *é divisor de zero.*

(2) *Consideremos o anel*

$$A = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} ; a, b, c, d \in \mathbb{R} \right\}$$

munido das operações usuais de soma e produto de matrizes.

Note que a matriz

$$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

é um divisor de zero, pois

$$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Por outro lado, temos

$$\left(\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right)^n = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \forall n \in \mathbb{Z}$$

Assim, $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ *não é nilpotente*

Agora consideremos o anel $f(\mathbb{R})$ *das funções* $f : \mathbb{R} \longrightarrow \mathbb{R}$, *munida das operações de soma e produto usuais de funções.*

Note que a função $f : \mathbb{R} \longrightarrow \mathbb{R}$ *definida por:*

$$f(x) = \begin{cases} x^2, & se \quad x < 0, \\ 0, & se \quad x \geqslant 0. \end{cases}$$

É um divisor de zero, pois dada a função $g : \mathbb{R} \longrightarrow \mathbb{R}$ *definida por:*

$$g(x) = \begin{cases} 0, & se \quad x < 0, \\ x, & se \quad x \geqslant 0. \end{cases}$$

temos que

$$f(x) \cdot g(x) = 0, \forall x \in \mathbb{R}$$

Por outro lado, se $x > 0$*, temos* $[f(x)]^n \neq 0$*, para todo* $n \in \mathbb{Z}$*, com* $n > 0$*, ou seja,* $(f)^n$ *é diferente da função nula.*

(3) *Suponha, por absurdo, que* x *é um divisor de zero. Então existe* $y \in A$*, com* $y \neq 0$*, tal que*

$$x \cdot y = 0$$

Como $x \in U(A)$*, então existe* $x^{-1} \in A$ *tal que*

$$x^{-1} \cdot x = 1$$

Assim,

$$\begin{aligned} x^{-1}(xy) &= x^{-1}0 \\ (x^{-1}x)y &= 0 \\ 1y &= 0 \\ y &= 0 \end{aligned}$$

O que é uma contradição. Logo x *não possui divisor de zero.*

Exemplo 3.3. *O anel* $\mathbb{Z}$ *dos inteiros é um DIP(domínio de ideais principais).*
De fato, seja J *um ideal de* $\mathbb{Z}$*. Se* $J = 0$ *então* J *é um ideal de* $\mathbb{Z}$ *gerado por 0. Suponhamos que existe* $x \in J$ *tal que* $x \neq 0$*. Então* $-x \in J$*. Deste modo,* $|x| \in J$*. Pelo princípio da boa ordenação, consideremos d o menor inteiro positivo de J. Mostraremos que* $J = d\mathbb{Z}$*. Com efeito, seja* $x \in d\mathbb{Z}$*. Então* $x = dn$*, para algum* $n \in \mathbb{Z}$*. Como* J *é um ideal,* $x = dn \in J$*, portanto,* $d\mathbb{Z} \subset J$*. Agora seja* $x \in J$*. Então* $|x| \in J$*. Daí, pelo algoritmo da divisão, existem* $q, d, r \in \mathbb{Z}$*, tais que* $|x| = qd + r, 0 \leqslant r < d$ *o que implica*

$$|x| - qd = r.$$

Como $|x|, qd \in J$ *e* $0 \leqslant r < d$*. Pela minimilidade de* d*, temos que* $r = 0$*. Daí* $|x| = qd \in J$*, assim* $x \in d\mathbb{Z}$*. Portanto,* $J = d\mathbb{Z}$*. Logo,* $\mathbb{Z}$ *é um DIP.*

Proposição 3.1. *Se* P *é primo e* $x^n \in P$ $(n \in \mathbb{N})$*, então* $x \in P$*. Além disso,* $N(A) \subseteq P$*.*

Demonstração. Seja P um ideal primo de um anel A, e seja $x \in A$ tal que $x^n \in P$. Suponha que n é o menor natural tal que $x^n \in P$. Assim, como P é primo e $x^n = x \cdot x^{n-1} \in P$, segue que $x \in P$. Além disso, se $x \in N(A)$, existe $n \in \mathbb{N}$,tal que

$$x^n = 0 \in P.$$

Pelo que acabamos de mostrar $x \in P$. Logo $N(A) \subseteq P$. ■

Enunciaremos o lema de Zorn, porém ocultaremos sua demonstração. Mas o leitor que tiver interesse pode consultar em [11].

Lema 3.1. Lema de Zorn

Seja X um conjunto parcialmente ordenado não vazio tal que cada cadeia em X é limitada superiormente. Então X possui pelo menos um elemento maximal.

Teorema 3.1. *Sejam A um anel e I um ideal próprio de A. Então I está contido em algum ideal maximal de A.*

Demonstração. Sejam J o conjunto de todos os ideais próprios de A contendo I, ordenado pela inclusão ($\subset$). Sendo

$$C = \{J_\lambda; \lambda \in \Lambda\}$$

uma cadeia em J, ou seja, $J_{\lambda_1} \subset J_{\lambda_2} \subset ...$, tomemos $J = \bigcup_{\lambda \in \Lambda} J_\lambda$. Observe que $I \subset J$ e J é cota superior para C. Pelo lema de Zorn, C possui elemento maximal, e assim temos o resultado. ■

Corolário 3.1. *Se A é um anel, então*

$a \in U(A)$ se, e somente se não existe maximal de A contendo a

Demonstração. ($\Rightarrow$) Suponha que $a \in U(A)$ e que existe um ideal maximal $M \neq A$ tal que $a \in M$. Como $a \in U(A)$, então existe $a^{-1} \in A$ tal que

$$a \cdot a^{-1} = 1$$

Como M é ideal, segue que

$$1 = a \cdot a^{-1} \in M$$

Portanto, $M = A$, o que é uma contradição. Logo não existe o ideal maximal M contendo (a).

($\Leftarrow$) Suponha que não existe um ideal maximal contendo a. Considere o ideal principal gerado por a, isto é,

$$(a) = \{ax; x \in A\}$$

Note que não existe ideal maximal contendo (a), pois, caso contrário a pertenceria a este ideal. Pelo teorema 3.1, (a) não é próprio, ou seja, $(a) = \{0\}$ ou $(a) = A$. Como (a) não está contido em um ideal maximal, segue que $(a) = A$. Assim $1 \in (a)$, portanto, existe $b \in A$ tal que

$$ab = 1$$

Logo, $a \in U(A)$. ■

Pelo corolário 3.1, temos que

$$A - U(A) = \bigcup_{\substack{\text{M é ideal} \\ \text{maximal}}} M. \tag{3.1}$$

Definição 3.2. *Um anel é dito local se possui um único ideal maximal.*

Exemplo 3.4. *Considere o anel*

$$R = \left\{\frac{m}{n} \in \mathbb{Q};\ n \text{ é impar}\right\}.$$

Note que

$$U(R) = \left\{\frac{n}{m};\ n \text{ e } m \text{ ímpares}\right\}$$

Além disso, note que $R - U(R) = \left\{\frac{m}{n} \in \mathbb{Q};\ n \text{ é ímpar}\right\}$ *é o único maximal de* R*, e portanto,* R *é local.*

Exemplo 3.5. *Seja* $f(\mathbb{R})$ *o anel das funções de* $\mathbb{R}$ *em* $\mathbb{R}$*. Considere* $a \in \mathbb{R}$*,*

$$Y_a = \{f \in f(\mathbb{R}); f(a) = 0\}.$$

Então temos que Y_a *é ideal principal e maximal. Note que* Y_a *é um subanel de* $f(\mathbb{R})$*. Agora suponhamos que existe um ideal* J *em* $f(\mathbb{R})$*, tal que* $Y_a \subset J$*, mas* $Y_a \neq J$*. Então existe* $f \in J$ *tal que* $f \notin Y_a$*. Assim* $f(a) = b \neq 0$*. Denotando por* b *a função constante igual a* b*, temos*

$$h = f - b \in Y_a,$$

pois $h(a) = f(a) - b(a) = 0$. Agora, notemos que $b = f - h \in J$, pois $f \in J$ e $h \in Y_a \subseteq J$. Assim a função constante 1 pertence a J, pois $1 = (b^{-1} \cdot b) \in J$ ($b \in J$ e J é ideal). Portanto $J = A$. Logo, Y_a é maximal.

Proposição 3.2. *Sejam A um anel e M um ideal próprio de A, então valem:*
(i) Se $A - M \subseteq U(A)$, então A é local e M é o único ideal maximal de A.
(ii) Se M é maximal e $1 + M = \{1 + M/x \in M\} \subseteq U(A)$ então A é local.

Demonstração. (i) Se I é ideal próprio de A, então $I \cap U(A) = \varnothing$. Daí,

$$U(A) \subseteq A - I$$

Logo $A - M \subseteq A - I$, e assim $I \subseteq M$.
(ii) Se $a \in A - M$, então $M + (a) = A$ e daí $1 = m + ax$, com $x \in A$ e $m \in M$. Logo, $ax = 1 - m \in 1 + M \subset U(A)$. Daí $a \in U(A)$, portanto $A - M \subseteq U(A)$. Pelo item (i) M é único ideal maximal de A, e assim A é local. ■

Proposição 3.3. *Seja A um anel. Se $I_1, ..., I_n$ e P são ideais de A, com P primo, tais que:*

$$I_1 \cap ... \cap I_n \subseteq P$$

Então $I_j \subseteq P$, para algum j. Ademais, se $I_1 \cap ... \cap I_n = P$ então $P = I_j$ para algum j.
Demonstração. *Suponha por absurdo, que existe $x_j \in I_j - P$, para cada $j = 1, ..., n$. Como I_j é ideal, para cada j, temos*

$$x_1 x_2 ... x_n \in (I_1 \cap ... \cap I_n) \subseteq P \text{ e } x_i \notin P, \forall i = 1, ..., n$$

O que é um absurdo, pois P é primo. Se $I_1 \cap ... \cap I_n = P$, então $I_j \subseteq P$, para algum j. Por outro lado, dado $x \in P$, temos $x \in I_1 \cap ... \cap I_n \subseteq I_j$. Assim $I_j = P$ para algum j.
■

3.1 Nilradical e Radical Jacobson

Nesta seção introduziremos alguns conceitos necessários para os resultados posteriores.

Seja A um anel. Então, temos que $N(A) = \{x \in A;\ \ x \text{ é } \text{nilpotente}\}$ é um ideal de A e que $N(A/N(A)) = \{\bar{0}\}$.

$$\begin{aligned} x \in N(A/N(A)) &\Leftrightarrow \exists\, n \in \mathbb{N}/(\bar{x})^n = \bar{0} \\ &\Leftrightarrow \overline{x^n} = \bar{0} \\ &\Leftrightarrow x^n \in N(A) \\ &\Leftrightarrow x \in N(A) \Leftrightarrow x \equiv 0 (mod\ N(A)) \\ &\Leftrightarrow \bar{x} = \bar{0}. \end{aligned}$$

Enunciaremos a seguinte proposição, a qual nos ajudará a entender a interseção de todos ideais primos, porém não apresentaremos a demonstração, devido a mesma fugir de nossos objetivos. O leitor que tiver interesse pode consultar em [2].

Proposição 3.4. *Seja A um anel. Então N(A) é interseção de todos ideais primos de A.*

Definição 3.3. *Seja A um anel. Definimos o radical de Jacobson de A, denotado por J(A), como sendo a interseção de todos ideais maximais de A.*
Note que

$$J(A) \supseteq N(A)$$

Seja $x \in N(A)$*. Então* $x \in P$ *qualquer que seja o ideal primo P, como todo ideal maximal M é primo segue que* $x \in M$*. Portanto,* $x \in \bigcap\limits_{\substack{M \text{ é ideal} \\ \text{maximal}}} M$.

Proposição 3.5. *Se* $x \in A$*, são equivalentes:*
(i) $x \in J(A)$;
(ii) $1 + xy \in U(A)$*, para todo* $y \in A$.

Demonstração. $(i) \Rightarrow (ii)$ $x \in J(A) \Rightarrow xy \in J(A) \Rightarrow xy \in M$, para todo ideal maximal M de $A \Rightarrow 1 + xy \notin M \Rightarrow 1 + xy \in U(A)$.
$(ii) \Rightarrow (i)$ Suponha $x \in A - M$ para algum ideal maximal M de A. Daí, $M + (x) = A$ (pois $M \subset M + (x)$) e daí $1 = m + xy$ para algum $m \in M$ e algum $y \in A$. Logo,

$$\begin{aligned} m &= 1 - xy \\ &= 1 + x(-y) \notin U(A). \end{aligned}$$

O que é um contradição. Logo $x \in M$ qualquer que seja o maximal M, e assim $x \in J(A)$. ■

Definição 3.4. *Sejam A um anel e I um ideal de A. Definimos o radical de I, denotado por r(I,) como sendo*

$$r(I) = \{x \in A; x^n \in I \ \ para \ \ algum \ \ n \in \mathbb{N}\}.$$

Definição 3.5. *Uma função $f : A \to B$ diz-se um* **homomorfismo** *de A em B se satisfaz as seguintes condições:*
(i) $f(x + y) = f(x) + f(y), \ \forall x, \ y \in A$;
(ii) $f(x \cdot y) = f(x) \cdot f(y), \ \forall x, \ y \in A$.

Apresentaremos agora um resultado de Homomorfismo, o qual será usado para a demonstração de uma das observações dadas a seguir.
Seja o homomorfismo sobrejetor $\phi : A \longrightarrow A/I$, definido por $\phi(a) = \bar{a}$, onde I é um ideal de A. Se Q é um ideal primo de A/I, então $\phi^{-1}(Q) = P$ é um ideal primo de A. O fato de P ser ideal é trivial. Sejam $x, y \in A$ tais que

$$x \cdot y \in P = \phi^{-1}(Q)$$

Então

$$\phi(x) \cdot \phi(y) = \phi(xy) \in Q$$

Como Q é ideal primo de A/I, segue que

$$\phi(x) \in Q \ \text{ ou } \ \phi(y) \in Q,$$

ou seja,

$$x \in \phi^{-1}(Q) = P \text{ ou } y \in \phi^{-1}(Q) = P$$

Portanto, $P = \phi^{-1}(Q)$ é ideal primo de A.

Observação 3.2.

(1) *Num anel de idempotentes todo ideal coincide com o seu radical;*

(2) $I \subseteq r(I)$;

(3) *Se P é ideal primo de A, então r(P) = P;*

(4) $N(A) = r(\{\bar{0}\})$;

(5) *Prove que* $r(I) = \phi^{-1}(N(A/I))$;

$$\phi : A \longrightarrow A/I \qquad N(r(I)) \text{ é ideal}$$

$$a \longrightarrow \phi(a) = \bar{a};$$

(6) $r(I) = \cap P$, *P ideal primo de A, $I \subseteq P$.*

Demonstração. (2) Dado $x \in I$, temos $x = x^1$, daí $x \in r$. Portanto $I \subset r(I)$.

(3) Por (2), temos $P \subseteq r(P)$. Seja $x \in r(P)$. Então existe $n \in \mathbb{N}$ tal que $x^n \in P$. Considere n o menor inteiro, daí $x \cdot x^{n-1} = x^n \in P \Rightarrow x \in P$. Portanto $r(p) \subseteq P$. Logo $r(P) = P$.

(4) $x \in N(A)$. Então existe $n \in \mathbb{N}$ tal que $x^n = 0 \in \{\bar{0}\}$. Então, existe $n \in \mathbb{N}$ tal que $x^n \in \{\bar{0}\}$, ou seja, $x^n = 0$.

(5) Se $x \in r(I)$, então existe $n \in \mathbb{N}$ tal que $x^n \in I$. Assim $\bar{x}^n = \overline{x^n} = \bar{0}$. Daí, $\bar{x} \in N(A/I)$, donde $x = \phi^{-1} \in \phi^{-1}(N(A/I))$. Reciprocamente, considere $x \in \phi^{-1}(N(A/I))$. Então $\bar{x} = \phi(x) \in N(A/I)$. Assim, existe $n \in \mathbb{N}$ tal que:

$$\bar{x}^n = \overline{x^n} = \bar{0},$$

donde, $x^n \in I$. Portanto, $x \in r(I)$.

(6) Se $x \in r(I)$, então $x \in \phi^{-1}(N(A/I))$, donde $\phi(x) \in N(A/I)$. Assim, $\phi(x) \in Q$, para todo ideal primo Q de A/I, donde $x \in \phi^{-1}(Q)$, para todo ideal primo $\phi^{-1}(Q) = P$ de A tal que $I \subseteq P$. Reciprocamente, seja $x \in \cap P$ $x \in P$, para todo ideal primo de A contendo I. Então $x \in P = \phi^{-1}(Q)$, para todo ideal primo Q de A/I, ou seja, $\phi(x) \in N(A/I)$, donde $x \in \phi^{-1}(N(A/I)) = r(I)$. ∎

Definição 3.6. *Dizemos que I e J são coprimos se $I + J = A$.*

Propriedades

(1) $I \subseteq J \Rightarrow r(I) \subseteq r(J)$;

(2) $I \subseteq r(J) \Rightarrow r(I) \subseteq r(J)$;

(3) $r(r(I)) = r(I)$;

(4) $r(IJ) = r(I \cap J) = r(I) \cap r(J)$;

(5) $r(I) = A \Leftrightarrow I = A$;

(6) $r(I + J) = r(r(I) + r(J))$;

(7) P é ideal primo $\Rightarrow r(P^n) = P$;

(8) I e J são coprimos $\Leftrightarrow r(I)$ e $r(J)$ são coprimos.

Demonstração. (1) Se $x \in I$, existe $n \in \mathbb{N}$ tal que $x^n \in I \subseteq J$. Portanto, $x \in r(J)$, e assim $r(I) \subseteq r(J)$.
(2) Seja $x \in r(I)$. Então existe $n \in \mathbb{N}$ tal que $x^n \in I \subseteq r(J)$. Assim, existe $n \in \mathbb{N}$ tal que

$$(x^n)^m = x^{n \cdot m} \in J.$$

Portanto, $x \in r(J)$, e assim $r(I) \subseteq r(J)$.
(3) Seja $x \in r(r(I))$. Então, existe $n \in \mathbb{N}$ tal que $x^n \in r(I)$. Daí, existe $m \in \mathbb{N}$ tal que

$$(x^n)^m = x^{(mn)} \in I.$$

Portanto $x \in r(I)$. Reciprocamente, seja $x \in r(I)$ temos que:

$$x^1 = x \in r(I).$$

Assim, $r(I)$ possui uma potência de x. Portanto $x \in r(r(I))$.
(4) Como $IJ \subset I \cap J$, segue por (1), que $r(IJ) \subset r(I \cap J)$. Além disso,

$$I \cap J \subseteq I \ \text{ e } \ I \cap J \subseteq J.$$

Donde temos, $r(I \cap J) \subseteq r(I)$ e $r(I \cap J) \subseteq r(J)$. Assim

$$r(IJ) \subseteq r(I \cap J) \subseteq r(I) \cap r(J)$$

Finalmente, seja $x \in r(I) \cap r(J)$. Então $x \in r(I)$ e $x \in r(J)$. Daí existem $m, n \in \mathbb{N}$ tais que

$$x^m \in I \ \text{ e } \ x^n \in J.$$

Assim,

$$x^{m+n} = x^m x^n \in IJ.$$

(5) ($\Rightarrow$) Suponha que $r(I) = A$. Como A é um anel com unidade 1, segue que $1 \in r(I)$. Assim existe $n \in \mathbb{N}$ tal que

$$1 = 1^n \in I$$

Como I é um ideal e $1 \in I$, segue que $I = A$.

($\Leftarrow$) Note que $r(A) = A$. Assim, se $I = A$, segue que

$$r(I) = r(A) = A$$

(6) Uma vez que $I \subseteq r(I)$ e $J \subseteq r(J)$, temos

$$I + J \subseteq r(I) + r(J)$$

Daí, por (1)

$$r(I + J) \subseteq r(r(I) + r(J))$$

Finalmente, note que

$$r(I) + r(J) \subseteq r(I + J)$$

De fato, $r(I) \subseteq r(I+J)$ e $r(J) \subseteq r(I+J)$. Assim, se $x+y \in r(I)+r(J)$, onde $x \in r(I)$ e $y \in r(J)$, temos $x + y \in r(I + J)$, pois $x, y \in r(I + J)$ e radical é ideal. Portanto

$$r(r(I) + r(J)) \subseteq r(I + J).$$

(7) Façamos uma indução sobre n. Se $n = 1$, por a observação 3, temos que a afirmação é válida. Suponha que vale para $n = k$. Então

$$r(P^k) = P$$

Assim,

$$\begin{aligned} r(P^{k+1}) &= r(P^k P) \\ &= r(P^k) \cap r(P) \\ &= P \cap P \\ &= P. \end{aligned}$$

(8) Suponha que $r(I)$ e $r(J)$ são coprimos. Então

$$r(I + J) = r(r(I) + r(J)) = r(A) = A$$

O que implica $A = I + J$. Portanto, I e J são coprimos. Reciprocamente, suponha que I e J são coprimos. Então

$$A = r(A) = r(I + J) = r(r(I) + r(J))$$

Daí $A = r(I) + r(J)$. Logo, $r(I)$ e $r(J)$ são coprimos. ■

3.2 Espectro Primo

Topologia

Topologia é o campo da Matemática que objetiva basicamente descrever como estão "colocadas"determinadas classes de subconjuntos de um conjunto maior, chamado de espaço topológico, e no qual alguma noção de proximidade está definida. A linguagem introduzida pela Topologia é fundamental para a generalização do conceito de continuidade de funções. Trata-se portanto, de um importante campo de estudo. Contudo, uma vez que não faz parte dos objetivos deste texto o aprofundamento desse tema, nos limitaremos a apresentar as noções topológicas necessárias para trabalhar a aplicação de topologia nos anéis e ideais.

Uma topologia em um conjunto X é um conjunto $T \subset P(X)$ que satisfaz as seguintes propriedades:
(i) $\varnothing$ e X pertence a T;
(ii) Se $(A_\lambda)\lambda \in r$ é um família de elementos de T, então $\bigcup_{\lambda \in r} A_\lambda \in T$;
(iii) Se $A_j \in T$, $\forall j = 1, ..., n$, então $\bigcap_{j=1}^{n} A_\lambda \in T$.
Os elementos de T são chamados de abertos. Dizemos que $E \subset X$ é fechado se $X - E$ é aberto.

Teorema 3.2. *Se f é a coleção de fechados de um espaço topológico X, então:*
(i) Qualquer interseção de elementos de f é ainda um elemento de f;
(ii) União finita de elementos de f, ainda pertence a f;
(iii) X e $\varnothing$ pertence a f.

Agora, seja A um anel e X o conjunto de todos ideais primos de A. Para cada

$E \subseteq A$, considere

$$V(E) = \{P \in X; E \subseteq P\}.$$

Então:

(i) Se I é o ideal de A gerado por E, então $V(E) = V(I) = V(r(I))$;

(ii) $V(0) = X, V(1) = \varnothing$;

(iii) Se $\{E_i; i \in \lambda\}$ é uma família de subconjuntos de A, então

$$V(\bigcup_{j\in\lambda} E_j) = \bigcap_{j\in\lambda} V(E_j);$$

(iv) Se I e J são ideais de A, então:

$$V(I \cap J) = V(IJ) = V(I) \cup V(J).$$

Demonstração. (i) De fato, seja $P \in V(r(I))$. Então P é um ideal primo tal que $r(I) \subseteq P$. Por outro lado, $I \subseteq r(I) \subseteq P$. Assim $P \in V(I)$, e portanto $V(r(I)) \subseteq V(I)$. Além disso, como I é gerado por E, segue que $E \subseteq I$. Deste modo, dado o ideal primo $Q \in V(I)$, temos que

$$E \subseteq I \subseteq Q \Rightarrow Q \in V(E).$$

Portanto,

$$V(r(I)) \subseteq V(I) \subseteq V(E).$$

Agora, seja $P \in V(E)$. Então $E \subseteq P$, por outro lado, $I = AE \subseteq AP \subseteq P$. Daí $r(I) \subseteq r(P) = P$. Assim, $P \in V(r(I))$. Logo, $V(r(I)) = V(I) = V(E)$.

(ii) Claramente, $0 \in P \subseteq X$, para todo ideal primo P. Assim $V(0) = X$. Agora, note que não existe um ideal primo P tal que $1 \in P$. Assim $V(1) = \varnothing$.

(iii) Seja $P \in V(\bigcup_{j\in\lambda} E_j)$. Então

$$\bigcup_{j\in\lambda} E_j \subseteq P.$$

Deste modo, $E_j \subseteq P$, para todo $j \in \lambda$. Assim $P \in V(E_j)$, para todo $j \in \lambda$. Daí

$$P \in \bigcap_{j\in\lambda} V(E_j).$$

Reciprocamente, seja $P \in \bigcap_{j\in\lambda} V(E_j)$. Então,

$$P \in V(E_j),$$

para cada $j \in \lambda$. Assim,

$$E_j \subseteq P,$$

para cada $j \in \lambda$, donde

$$\bigcup_{j \in \lambda} E_j \subseteq P.$$

Portanto,

$$P \in V(\bigcup_{j \in \lambda} E_j).$$

Logo,

$$V(\bigcup_{j \in \lambda} E_j) = \bigcap_{j \in \lambda} V(E_j).$$

iv) De fato, pela propriedade (iv), temos

$$V(I \cap J) = V(r(I \cap J)) = V(r(IJ)) = V(IJ).$$

Agora, seja $P \in V(I \cap J)$. Então

$$I \cap J \subset P$$

Daí, pela proposição 3.3, $I \subseteq P$ ou $J \subseteq P$. Assim,

$$P \in V(I) \cup V(J).$$

Portanto,

$$P \in V(I \cap J) \subset V(I) \cup V(J).$$

Reciprocamente, seja $P \in V(I) \cup V(J)$. Então $I \subset P$ ou $J \subset P$. Mas $I \cap J \subseteq I, J$. Daí $I \cap J \subseteq P$, e assim $P \in V(I \cap J)$. Portanto

$$V(I \cap J) = V(I) \cup V(J).$$

■

Notemos que o resultado acima nos mostra que os conjuntos V(E) satisfazem às condições de axioma para conjuntos abertos em um espaço topólogico.

Denotamos o espaço topológico construído sobre o anel A de $Spec(A)$.

Definição 3.7. *Um conjunto $T \subset P(X)$ chama-se* ***conexo*** *quando não admite outra cisão além da trivial. Assim, quando T é conexo, $T = V(I_1) \cup V(I_2)$, com $V(I_1)$ e $V(I_2)$ são disjuntos e abertos em T. Implica $V(I_1) = \varnothing$ ou $V(I_2) = \varnothing$.*

Definição 3.8. *Quando existir um cisão não - trivial* $T = V(I_1) \cup V(I_2)$, *dizemos que* T *é* ***desconexo***.

Exemplo 3.6. *Seja* D *um domínio de integridade. Então Spec(D) é conexo.*

Considere I_1 *e* I_2 *ideais de* D *tais que* $V(I_1) \cup V(I_2) = Spec(D)$. *Como* D *é domínio, segue que.*

$$\{0\} \in Spec(D) = V(I_1) \cup V(I_2) = V(I_1 I_2)$$

Assim, $I_1 I_2 \subseteq \{0\}$, *donde* $I_1 I_2 = \{0\}$. *Daí* $I_1 = \{0\}$ *ou* $I_2 = \{0\}$. *Portanto, ou*

$$V(I_1) = Spec(D) \ \ ou \ \ V(I_2) = Spec(D).$$

Exemplo 3.7. *Spec*$(\mathbb{Z} \times \mathbb{Z})$ *é desconexo.*

$$Spec(\mathbb{Z} \times \mathbb{Z}) = V(1,0) \cup V(0,1)$$

Como $(1,0) + (0,1) \notin P$ *para todo ideal primo, segue que* $V(1,0) \cap V(0,1) = \varnothing$. *Finalmente, note que* $\mathbb{Z} \times \{0\}$ *e* $\{0\} \times \mathbb{Z}$ *são ideais primos de* $\mathbb{Z} \times \mathbb{Z}$. *Assim*

$$V(1,0) \neq \varnothing \ \ e \ \ V(1,0) \neq Spec(\mathbb{Z} \times \mathbb{Z}).$$

Conclusão

Neste trabalho vemos o quão à álgebra é importante na área da matemática, constatou-se que a mesma tem várias aplicações nas sub áreas da matemática e é possível aplicarmos uma estrutura de espaço topólogico sobre um anel comutativo com unidade.

Este trabalho permitiu-me um estudo mais detalhado sobre anéis e seus aspectos históricos que foram de suma importância para o entendimento dos resultados posteriores, além de ver a importância da aplicação da álgebra em espaço topológico e que através deste trabalho os leitores poderão trabalhar estas teorias de uma maneira mais significativa e atraente, contribuindo assim para o ensino da matemática superior.

Referências Bibliográficas

[1] ALDO, B.Maciel. OSMUNDO, A. Lima. *Introdução à Ánalise Real.* 1ª edição.

[2] ATIYAH, M. F.; MACDONALD, I. G. *Introducción al álgebra conmutativa.* España: Reverté, 2010.

[3] AZNAR, Enrique R. *Emmy Amalie Noether.* Dpto Álgebra, facultad de ciências. 2007 Disponível em: http:// www.ugr.es/ eaznar/$emmy_noether$.htm. (Acessado em 12/11/2015).

[4] BOYER, Cal B. *História da matemática.* Tradução de Elza F. Gomide. 2ª ed. São Paulo: Edgard Blucher, 1996.

[5] DOMINGUES, H. IEZZI, G. *Álgebra moderna.* São Paulo: Atual, 2003.

[6] EVES, Howard. *Introdução à história da matemática.* H.Domingues. - Campinas, SP: Editora da UNICAMP, 2014.

[7] EXEL,Ruy. *Von Neumann e a Teoria de Álgebras de operadores.* Disponível em: http://http://mtm.ufsc.br/ exel/papers/vn.pdf. (Acessado em 02/06/2015).

[8] FRANLEIG, John B. *A First Course In Abstract Algebra.* Pearson Education, 2003.

[9] GONÇALVES, Adilson. *Introdução à Álgebra.* 5ª ed.Rio de Janeiro :IMPA, 2007.

[10] HYGINO, D.; GELSON, I. *Algebra Moderna.* 4ª ed. São Paulo: editora atual, 2003.

[11] LIMA, Elon L. *Ánalise real volume 1.* 8ª ed. Rio de Janeiro :IMPA, 2006.

[12] LIMA, Elon L. *Ánalise real volume 2.* 8ª ed. Rio de Janeiro :IMPA, 2006.

[13] MILIES, César P. *Breve História da Álgebra Abstrata.* Universidade de São Paulo. Disponível em: http://www.bienasbm.ufba.br/M18.pdf. (Acessado em 02/06/2015).

[14] MILIES, César P. *Unidades em Anéis de Grupos.* Insituto de matemática pura e aplicada. Rio de Janeiro, 1998. Disponível em: http://www.impa.br/opencms/pt/biblioteca/mono/$Mon_5$8.pdf. (Acessado em 28/05/2015).