Aneis de Dedekind

(Trabalho da disciplina Introdução à Álgebra Comutativa)

Maria Clara Cardoso

Instituto de Matemática e Estatística
Univerdidade de São Paulo
São Paulo, julho de 2020

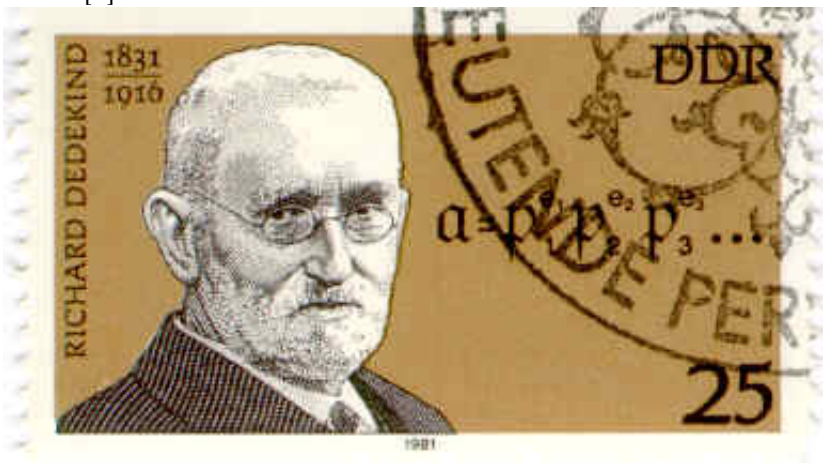
Sumário

1 Introdução

Julius Wilhelm Richard Dedekind (1831 - 1916) foi um matemático alemão. Ele fez contribuições importantes na álgebra abstrata (especialmente na teoria dos anéis), na fundamentação axiomática dos números naturais, na teoria algébrica dos números e na definição de número real.

A noção de ideais foi primeiramente proposta por Dedekind em 1876 na terceira edição do livro Vorlesungen über Zahlentheorie (Notas de Teorias dos Números). Era uma generalização do conceito de números ideais desenvolvida por Ernst Kummer. Depois o conceito foi mais desenvolvido por David Hilbert e, especialmente, por Emmy Noether.

O nome anéis de Dedekind (ou domínios de Dedekind) foi dado em homenagem a Dedekind, que foi um dos primeiros a estudar esses aneis por volta de 1870. [1]



(selo com Richard Dedekind e com um ideal com sua decomposição em ideais primos - http://users.wfu.edu/kuz/Stamps/Dedekind/Dedekind.html)

Vimos que:

Teorema 1.1. Seja R um anel Noetheriano. Então todo ideal I de R contém um produto finito de ideais primos.

Demonstração. Exercício 13.1 da lista 5. □

Dessa forma, poderiamos nos perguntar sobre aneis cujos ideais são produtos finitos de ideais primos. Esses são os aneis de Dedekind:

Definição 1.1. Um *anel de Dedekind* (ou *domínio de Dedekind*) é um domínio de integridade em que todos ideais são produtos de ideais primos.

O interesse pelos aneis de Dedekind surgiu na metade do século 19 porque notou-se que oa anéis de inteiros algébricos não eram domínios de fatoração única mas seus ideais poderiam ser escritos como produtos de ideais primos. [2]

2 Exemplos e definições equivalentes

Essa seção é baseada em [2].

Exemplo 2.1. Todo domínio de ideais principais é um anel de Dedekind:

Seja R um domínio de ideais principais (DIP) e I um ideal de R. Para $I = 0$, I é primo. Se $I \neq 0$, então existe $a \in R$, $a \neq 0$, tal que $I = \langle a \rangle$. Como todo DIP é um domínio de fatoração única (DFU), existem $u \in R$ unidade, $p_1, \ldots, p_k \in R$ irredutíveis (=primos em DFU) distintos e $e_1, \ldots, e_k$ inteiros positivos tais que $a = up_1^{e_1} \cdots p_k^{e_k}$. Assim $I = \langle p_1 \rangle^{e_1} \cdots \langle p_k \rangle^{e_k}$ onde $\langle p_1 \rangle, \ldots, \langle p_k \rangle$ são ideais primos.

Exemplo 2.2. Sejam R um anel de Dedekind e $S \subset R$ um conjunto multiplicativo. Então $S^{-1}R$ é um anel de Dedekind:

Se J é um ideal de $S^{-1}R$, vimos em aula que existe I ideal de R tal que $J = S^{-1}I$. Como R é anel de Dedekind, existem $P_1, \ldots, P_n$ ideais primos tais que $I = \prod_{i=1}^{n} P_i$. Se $P_i \cap S = \emptyset$, $S^{-1}P_i$ é ideal primo de $S^{-1}R$. Caso contrário, $S^{-1}P_i = S^{-1}R$. Assim, $J = \prod_{\substack{i=1 \\ P_i \cap S = \emptyset}}^{n} S^{-1}P_i$ é fatoração de J por ideais primos.

Exemplo 2.3. Seja $\mathbb{K}$ um corpo de números algébricos e $\mathcal{O}(\mathbb{K})$ seu anel de inteiros. Então $\mathcal{O}(\mathbb{K})$ é um anel de Dedekind. Isso será provado na seção 4.

Agora temos como objetivo provar que a fatoração de um ideal em ideais primos em um anel de Dedekind é única.

Definição 2.1. Seja R um domínio de integridade com corpo de frações k. Um R-submódulo I de k é chamado de *ideal fracionado* se existir um elemento $d \in R$, $d \neq 0$, tal que $J = dI$ é um ideal de R.

Exemplo 2.4. Seja R um domínio de integridade. Se I um ideal de R, então I é um ideal fracionado pois $1I = I$ é um ideal de R.

Exemplo 2.5. Sejam R um domínio de integridade e k seu corpo de frações. Se $\frac{a}{b} \in k$, então $\frac{a}{b}R$ é um ideal fracionado pois $b\frac{a}{b}R = aR = \langle a \rangle$ é o ideal de R gerado por $a \in R$.

Proposição 2.1. Seja R um domínio de integridade com corpo de frações k. Se I_1 e I_2 ideais fracionados, então I_1+I_2, I_1I_2 e $I_1 \cap I_2$ são ideais fracionados.

Demonstração. Por definição, existem $d_1, d_2 \in R$, d_1 e d_2 não nulos, tais que $J_1 = d_1I_1$ e $J_2 = d_2I_2$ são ideais de R.

Note que:

- $d_1d_2(I_1 + I_2) = d_2J_1 + d_1J_2$ é ideal de R
- $d_1d_2(I_1I_2) = J_1J_2$ é ideal de R
- $d_1d_2(I_1 \cap I_2) = (d_1d_2I_1) \cap (d_1d_2I_2) = (d_2J_1) \cap (d_1J_2)$ é ideal de R.

Assim segue que $I_1 + I_2$, I_1I_2 e $I_1 \cap I_2$ são ideais fracionados. □

Definição 2.2. Seja R um domínio de integridade com corpo de frações k. Dizemos que um ideal fracionado não nulo I é *invertível* se existir um ideal fracionado I' tal que $II' = R$. I' é chamado de *inverso* de I.

Observação 2.1. Seja R um domínio de integridade com corpo de frações k. Todo ideal principal não nulo é invertível: Seja $I = \langle a \rangle = aR$, $a \neq 0$. Defina $J = \frac{1}{a}R$. Temos: $IJ = R$ e J é ideal fracionado (pois $I = a^2J$ é ideal de R). Portanto I é invertível.

Definição 2.3. Seja R um domínio de integridade com corpo de frações k. Seja I um ideal fracionado não nulo. Defina:

$$I^{-1} = \{x \in k \mid xI \subset R\}$$

Observação 2.2. Seja I um ideal fracionado não nulo. Então I^{-1} é um ideal fracionado. De fato, seja $d \in R$, $d \neq 0$, tall que $J = dI$ é um ideal de R. Seja $a \in I$, $a \neq 0$. Então $daI^{-1} \subset R$ e $da \in J \subset R$. Claramente daI^{-1} é R-módulo, assim segue que daI^{-1} é ideal de R e I^{-1} é ideal fracionado.

Lema 2.1. Seja R um domínio de integridade com corpo de frações k. Seja I um ideal fracionado não nulo invertível. Então I^{-1} é o único inverso de I. Consequentemente, I é invertível se e somente se $II^{-1} = R$.

Demonstração. Seja I ideal fracionado não nulo e invertível. Então existe $d \in R$ não nulo tal que $J = dI$ é ideal de R e existe ideal fracionado I' tal que $II' = R$.

Pela definição de I^{-1}, claramente $I' \subset I^{-1}$. Por outro lado, temos:

$$I^{-1} = RI^{-1} = I'II^{-1} \subset I'R = I'$$

Portanto, $I' = I^{-1}$. □

Lema 2.2. Seja R um domínio de integridade com corpo de frações k. Se todos ideais fracionados não nulos forem invertíveis, então o conjunto dos ideais fracionados não nulos é um grupo com a multiplicação e identidade R.

Demonstração. Direto da proposição 2.1 e do lema 2.1. □

Lema 2.3. Seja R um domínio de integridade com corpo de frações k. Se I é um ideal fracionado invertível, então I é finitamente gerado como R-módulo.

Demonstração. Como I é invertível, temos $II^{-1} = R$. Então existem $x_1, \ldots .x_n \in I$ e $y_1, \ldots, y_n \in I^{-1}$ tais que $\sum_{i=1}^{n} x_i y_i = 1$. Assim, se $a \in I$ temos $a = \sum_{i=1}^{n} (ay_i)x_i$. Pela definição de I^{-1}, $ay_i \in R$ para todo $i \in \{1, \ldots, n\}$. Portanto $\{x_1, \ldots, x_n\}$ gera I como R-módulo. □

Lema 2.4. Seja R um domínio de integridade. Se $I_1, \ldots, I_n$ ideais de R tais que $J = \prod_{i=1}^{n} I_i$ é invertível, então $I_1, \ldots, I_n$ são invertíveis. Em particular, Se $J = \prod_{i=1}^{n} I_i$ é ideal principal, então $I_1, \ldots, I_n$ são invertíveis.

Demonstração. Como J é invertível, temos $JJ^{-1} = R$. Ou seja:

$$R = \left(\prod_{i=1}^{n} I_i \right) J^{-1} = I_j \left(\prod_{\substack{i=1 \\ i \neq j}}^{n} I_i \right) J^{-1}$$

Portanto, I_j é invertível com inversa $\left(\prod_{\substack{i=1\\ i\neq j}}^{n} I_i\right) J^{-1}$ para todo $j \in \{1, \ldots, n\}$.

□

Lema 2.5. Seja R um domínio de integridade. Seja $J = \prod_{i=1}^{n} I_i$ onde $I_1, \ldots, I_n$ são ideais de R primos e invertíveis. Então essa é a única fatoração de J em ideais primos.

Demonstração. Seja $J = \prod_{i=1}^{m} J_i$ outra fatoração de J onde $J_1, \ldots, J_m$ são primos. Vamos provar o lema por indução em n.

Considere $n = 1$. Então J é primo e invertível. Como $\prod_{i=1}^{m} J_i \subset J$ e J é primo, existe $r \in \{1, \ldots, m\}$ tal que $J_r \subset J$. Mas também temos $J \subset \prod_{i=1}^{m} J_i \subset J_r$. Então $J = J_r$. Se $m \neq 1$, teriamos $R = \prod_{\substack{i=1\\ i\neq r}}^{m} J_i \subset J_i$ para todo $i \in \{1, \ldots, m\}$, $i \neq r$, i.e, $J_i = R$, o que não pode acontecer já que J_i é primo. Portanto $m = 1$.

Suponha agora que o lema vale para $n \geq 1$. Vamos provar para $n + 1$. Seja I_r ideal minimal de $\{I_1, \ldots, I_n\}$. Novamente, como $\prod_{i=1}^{m} J_i \subset \prod_{i=1}^{n} I_i \subset I_r$, existe J_s tal que $J_s \subset \prod_{i=1}^{n} I_i \subset I_r$. Mas $\prod_{i=1}^{n} I_i \subset \prod_{i=1}^{m} J_i \subset J_s$. Então existe I_t tal qe $I_t \subset \prod_{i=1}^{m} J_i \subset J_s$. Assim temos $I_t \subset J_s \subset I_r$. Como escolhemos I_r minimal, temos $I_t = J_s = I_r$. Como I_r é invertível, multiplicanto J por I_r^{-1} obtemos:

$$\prod_{\substack{i=1\\ i\neq r}}^{n} I_i = \prod_{\substack{i=1\\ i\neq s}}^{m} J_i$$

Pela hipótese de indução, temos $n - 1 = m - 1$ e $\prod_{\substack{i=1\\ i\neq r}}^{n} I_i$ é uma fatoração igual a $\prod_{\substack{i=1\\ i\neq s}}^{m} J_i$. Portanto, o lema está provado. □

Teorema 2.1. Seja R um anel de Dedekind. Então todo ideal primo não nulo é invertível e maximal.

Demonstração. Vamos primeiro provar que todo ideal primo invertível de R é maximal. Dessa forma, seja P ideal primo invertível e $x \in R \setminus P$. Considere os ideais $P + Rx$ e $P + Rx^2$. Como R é um anel de Dedekind, existem $I_1, \ldots, I_k, J_1, \ldots, J_l$ ideais primos tais que $P + Rx = \prod_{i=1}^{k} I_i$ e $P + Rx^2 = \prod_{i=1}^{l} J_i$. Temos:

- $\frac{P+Rx}{P} = \prod_{i=1}^{k} \frac{I_i}{P} = \langle \frac{x}{P} \rangle$
- $\frac{P+Rx^2}{P} = \prod_{i=1}^{l} \frac{J_i}{P} = \langle \frac{x^2}{P} \rangle$

Pelo lema 2.4, concluimos que $\frac{I_1}{P}, \ldots, \frac{I_k}{P}, \frac{J_1}{P}, \ldots, \frac{J_l}{P}$ são invertíveis. Note que $\frac{P+Rx^2}{P} = \left(\frac{P+Rx}{P}\right)^2$. Então: $\prod_{i=1}^{k} \left(\frac{I_i}{P}\right)^2 = \prod_{i=1}^{l} \frac{J_i}{P}$. Pelo lema 2.5, temos $2k = l$ e podemos renumerar os J_i de forma que $I_i = J_{2i} = J_{2i-1}$ para todo $i \in \{1, \ldots, k\}$. Podemos concluir assim que $P + Rx^2 = (P + Rx)^2$. Então temos:

$$P \subset P + Rx^2 = (P + Rx)^2 = P^2 + Rx^2 \subset P^2 + Rx$$

Então, para todo $a \in R$, existem $b \in P^2$ e $c \in R$ tais que $a = b + cx$. Note que $cx = a - b \in P$. Como P é primo e $x \notin P$, temos $c \in P$. Assim temos $P \subset P^2 + Px$. Claramente $P^2 + Px \subset P$. Portanto, $P = P^2 + Px$. Como P é invertível, multiplicanto os dois lado da última igualdade por P^{-1} temos: $R = P + Rx$. Como x é arbitrário em $R \setminus P$, concluimos que P é maximal.

Agora vamos provar que todo ideal primo de R é invertível. Seja P um ideal primo de R. Seja $y \in P$, $y \neq 0$. Como R é um anel de Dedekind, existem ideais primos $P_1, \ldots, P_n$ tais que $\langle y \rangle = \prod_{i=1}^{n} P_i$. Assim P contém $\prod_{i=1}^{n} P_i$ e, consequentemente, existe P_j tal que $P_j \subset P$. Pelo lema 2.4, como $\langle y \rangle$ é principal, P_j é invertível. Pelo que acabamos de provar acima, sabemos que P_j é maximal. Então, $P_j = P$ e, portanto, P é invertível. □

Corolário 2.1. Seja R um anel de Dedekind. Então para todo ideal de R, sua fatoração em ideais primos é única.

Demonstração. Consequência do lema 2.5 e do teorema 2.1. □

Dessa forma, temos a seguinte definição para os aneis de Dedekind que é equivalente a primeira definição 1.1:

Definição 2.4. Um *anel de Dedekind* (ou *domínio de Dedekind*) é um domínio de integridade R em que todo ideal I de R pode ser fatorado de forma essencialmente única como produto de ideais primos, i.e.:

- (existência) existem $P_1, \ldots, P_k$ ideais primos distintos e $e_1, \ldots, e_k$ inteiros positivos tais que $I = P_1^{e_1} \cdots P_k^{e_k}$
- (unicidade) se existirem $Q_1, \ldots, Q_l$ ideais primos distintos e $f_1, \ldots, f_l$ inteiros positivos tais que $I = Q_1^{f_1} \cdots Q_l^{f_l}$, então $k = l$ e existe uma permutação σ de $\{1, \ldots, k\}$ tal que $P_i = Q_{\sigma(i)}$ e $e_i = f_{\sigma(i)}$ para todo $i \in \{1, \ldots, k\}$.

Segundo o teorema 1.1, em um anel Noetheriano todo ideal contém um produto finito de ideais primos. Assim poderiamos nos perguntar se todo anel Noetheriano é um anel de Dedekind.

Exemplo 2.6. $\mathbb{Z}[x]$ é Noetheriano mas não é anel de Dedekind. $\mathbb{Z}[x]$ é Noetheriano pois $\mathbb{Z}$ é Noetheriano. $\mathbb{Z}[x]$ não é Dedekind pois $\langle x \rangle$ é um ideal primo que não é maximal (ele está contido no ideal $\langle 2, x \rangle$).

Observação 2.3. Então nem todo anel Noetheriano é anel de Dedekind. Mas pode existir condições que podemos acrescentar a aneis Noetherianos para que eles sejam aneis de Dedekind. Com isso em mente, vamos agora em direção de provar que R é um anel de Dedekind se e somente se:

R é um domínio de integridade que satifaz as seguintes condições:

1. Todo ideal primo de R é maximal.
2. R é Noetheriano.
3. R é integralmente fechado no seu corpo de frações.

Lema 2.6. Seja R um anel de Dedekind. Se I e J são ideais de R tais que $I \subset J$, então existe Q ideal de R tal que $I = JQ$.

Demonstração. Sabemos que todos ideais de um anel de Dedekind são invertíveis, então podemos definir $Q = J^{-1}I$. Q é um ideal de R, pois $Q = J^{-1}I \subset J^{-1}J = R$, e $JQ = JJ^{-1}I = I$. □

Lema 2.7. Seja R um anel de Dedekind. Sejam I e J são ideais de R tais que $I \subset J$ e suas fatorações em ideais primos são $I = P_1^{e_1} \cdots P_k^{e_k}$ e $J = Q_1^{f_1} \cdots Q_l^{f_l}$. Então $l \leq k$ e renumerando os Q_i e f_i temos $Q_i = P_i$ e $f_i \leq e_i$ para todo $i \in \{1, \ldots, l\}$.

Demonstração. Pelo lema anterior existe ideal Q tal que $I = JQ$. Como a fatoração em ideais primos é única, concluimos que a fatoração de I é igual a fatoração de J multiplicada pela de Q. Assim segue o lema. □

Proposição 2.2. Seja R um anel de Dedekind. Todo ideal fracionado pode ser fatorado de forma única como produto de ideais primos e de inversos de ideais primos.

Demonstração. Seja I um ideal fracionado. Então existe $d \in R$, $d \neq 0$ tal que $J = dI$ é um ideal.

Vamos primeiro provar a existência da fatoração. Como R é um domínio de Dedekind, existem $P_1, \ldots, P_k, Q_1, \ldots, Q_l$ ideais primos tais que $J = \prod_{i=1}^{k} P_i$ e $Rd = \prod_{j=1}^{l} Q_j$. Como $J = RJ = (Rd)I$ temos $I = \left(\prod_{i=1}^{k} P_i\right)\left(\prod_{j=1}^{l} Q_j^{-1}\right)$. Se dado P_i, existir $Q_j = P_i$, temos $P_i Q_j^{-1} = R$. Então esses casos podem ser eliminados da fatoração e a fatoração obtida disso é única.
Agora vamos provar a unicidade da fatoração. Seja

$$I = \left(\prod_{i=1}^{k} P_i\right)\left(\prod_{j=1}^{l} Q_j^{-1}\right) = \left(\prod_{i=1}^{r} P_i'\right)\left(\prod_{j=1}^{s} (Q_j')^{-1}\right)$$

onde $P_1, \ldots, P_k, Q_1, \ldots, Q_l, P_1', \ldots, P_r', Q_1', \ldots, Q_s'$ são primos,
$\{P_1, \ldots, P_k\} \cap \{Q_1, \ldots, Q_l\} = \emptyset$ e $\{P_1', \ldots, P_r'\} \cap \{Q_1', \ldots, Q_s'\} = \emptyset$. Então

$$\left(\prod_{i=1}^{k} P_i\right)\left(\prod_{j=1}^{s} Q_j'\right) = \left(\prod_{i=1}^{r} P_i'\right)\left(\prod_{j=1}^{l} Q_j\right)$$

Pelo corolário 2.1 e por $\{P_1, \ldots, P_k\} \cap \{Q_1, \ldots, Q_l\} = \emptyset$, temos $k = r$, $l = s$, $\prod_{i=1}^{k} P_i = \prod_{i=1}^{k} P_i'$ e $\prod_{j=1}^{l} Q_j = \prod_{j=1}^{l} Q_j'$. Assim segue que a fatoração de I é única. □

Observação 2.4. Como consequência da proposição anterior, temos que num anel de Dedekind, para todo ideal fracionado I existem $P_1, \ldots, P_n$ ideais primos e $e_1, \ldots, e_n$ números inteiros não nulos tais que $I = P_1^{e_1} \cdots P_n^{e_n}$ (se $e_i < 0$, $P_i^{e_i} := (P_i^{-1})^{-e_i}$).

Definição 2.5. Dado I um ideal fracionado e P um ideal primo definiremos $\sigma_P(I)$ da seguinte forma:

$$\sigma_P(I) = \begin{cases} 0, & \text{se } P \text{ não aparece na fatoração de } I \\ e, & \text{se } P \text{ aparece na fatoração de } I \text{ como } P^e \end{cases}$$

A próxima parte será baseada em [3].

Lema 2.8. Seja R um anel que satisfaz as condições de 2.3. Se I é um ideal primo não nulo, então $R \subsetneq I^{-1}$.

Demonstração. Claramente $R \subset I^{-1}$. Então basta provar que $R \neq I^{-1}$. Seja $a \in I$, $a \neq 0$. Como R é Noetheriano, pelo teorema 1.1, existem $P_1, \ldots, P_n$ ideais primos tais que $\prod_{i=1}^{n} P_i \subset Ra$. Escolha esse produto de forma que n seja o menor possível. Se $n = 1$, como por hipótese todo ideal primo é maximal, temos $P_1 = Ra = I$. Como $a \neq 0$, temos $\frac{1}{a} \notin R$ mas $\frac{1}{a} \in I^{-1}$. Se $n > 1$, como P é primo, existe $P_j \subset P$. Como todo primo é maximal, temos $I = P_j$. Considere $J = \prod_{\substack{i=1 \\ i \neq j}} P_i$. Como n é minimal, temos $J \not\subset Ra$. Seja $b \in J \setminus Ra$. Como $IJ \subset Ra$, temos $Ib \subset Ra$. Então $\frac{b}{a} I \in R$. Ou seja, $\frac{b}{a} \in I^{-1}$. Mas $\frac{b}{a} \notin R$, pois $b \notin Ra$. Assim concluimos que $R \neq I^{-1}$. □

Lema 2.9. Seja R um anel que satisfaz as condições de 2.3. Se I é um ideal primo não nulo, então I é invertível.

Demonstração. Pelo lema 2.1 basta provar que $II^{-1} = R$. Claramente $II^{-1} \subset R$. Como I e I^{-1} são ideais fracionados, concluimos que II^{-1} é ideal de R. Por hipótese, como I é primo não nulo, I é maximal. Temos: $I \subset IR \subset II^{-1} \subset R$, então $II^{-1} = I$ ou $II^{-1} = R$.

Suponha que $II^{-1} = I$. Seja $x \in I^{-1}$. Então $xI \subset II^{-1} = I$. Por indução temos $x^n I \subset I$ para todo $n \in \mathbb{N}$. Seja $r \in R$. Então $rx^n I \subset rI \subset R$. Ou seja $R[x] = \langle 1, x, x^2, \ldots \rangle \subset I^{-1}$. Como I^{-1} é fracionado, existe $d \neq 0$ tal que dI^{-1} é ideal de R. Como $R[x]$ é R-módulo, $dR[x]$ é ideal de R. Pelo lema 2.3, $R[x]$ é finitamente gerado como R-módulo. Então x é integral sobre R. Mas por hipótese R é integralmente fechado. Portanto $x \in R$ e $I^{-1} \subset R$. Mas isso não acontece segundo o lema 2.8. Portanto $II^{-1} = R$ e I é invertível. □

Teorema 2.2. R é um anel de Dedekind se e somente se satisfaz as condições de 2.3.

Demonstração. Vamos provar primeiro que todo anel de Dedekind R satisfaz 1., 2. e 3. de 2.3. R satisfaz 1. pelo teorema 2.1. R satisfaz 2. pois, pelo lema 2.7, um ideal não nulo está dentro de apenas um número finito de ideais. Então toda cadeia ascendente de ideais se estabiliza. Falta agora provar que R satisfaz 3., ou seja, que R é integralmente fechado no seu corpo de frações. Seja $x = \frac{a}{b} \in k$ (k corpo de frações) que é integral sobre R. Assim existe polinômico mônico de $\mathbb{Z}[x]$ tal que x é raiz. Seja k o grau desse polinômio. Então $R[x]$ é um R-módulo gerado por $1, x, \ldots, x^{n-1}$. Então $b^{n-1}R[x] \subset R$. Denote por d o elemento b^{n-1}. Então, para todo $n \in \mathbb{N}$, $dx^n \in R$. Seja P ideal primo. Como a fatoração de um ideal fracionado é única temos $\sigma_P(dx^nR) = \sigma_P(dR) + n\sigma_P(xR)$, para todo $n \in \mathbb{N}$. Como $dx^n \in R$, dx^nR é um ideal de R e $\sigma_P(dx^nR) \geq 0$. Se $\sigma_P(xR) < 0$ existiria $n \in \mathbb{N}$ tal que $\sigma_P(dx^nR) = \sigma_P(dR) + n\sigma_P(xR) < 0$, então temos que ter $\sigma_P(xR) \geq 0$. Como isso ocorre para todo P ideal primo, concluimos que xR é produto finito de ideais primos, ou seja, é um ideal de R. Como $x \in xR$ concluimos que $x \in R$. Portanto R é integralmente fechado.

Agora temos que provar a volta. Seja R um anel que satisfaz 2.3. Vamos provar que R é um anel de Dedekind. Consideramos R produto de uma coleção vázia de conjuntos primos. Suponha que existe I ideal de R que não é produto finito de ideais primos. Seja $\mathcal{C}$ o conjunto de todos ideais que não são produto de ideais primos. $\mathcal{C} \neq \emptyset$ pois $I \in \mathcal{C}$. Como R é Noetheriano, $\mathcal{C}$ possui um elemento maximal J. Como $J \neq R$, existe ideal maximal de R tal que $J \subset M$. Pelo lema 2.9 temos $J = JR \subset JM^{-1} \subset MM^{-1} = R$. Então JM^{-1} é ideal de R.

Suponha $JM^{-1} = J$. Seja $x \in M^{-1}$. Então $xJ \subset JM^{-1} = J$. Por indução temos $x^nJ \subset J$ para todo $n \in \mathbb{N}$. Seja $r \in R$. Então $rx^nJ \subset rJ \subset R$. Ou seja $R[x] = \langle 1, x, x^2, \ldots \rangle \subset J^{-1}$. Como J^{-1} é fracionado, existe $d \neq 0$ tal que dJ^{-1} é ideal de R. Como $R[x]$ é R-módulo, $dR[x]$ é ideal de R. Pelo lema 2.3, $R[x]$ é finitamente gerado como R-módulo. Então x é integral sobre R. Mas por hipótese R é integralmente fechado. Portanto $x \in R$ e $M^{-1} \subset R$. Mas isso não acontece segundo o lema 2.8. Portanto $JM^{-1} \neq J$.

Pela maximilidade de J, existem $P_1, \ldots, P_n$ ideais primos tais que $JM^{-1} = \prod_{i=1}^{n} P_i$. Portanto $J = M \prod_{i=1}^{n} P_i$, ou seja, J é produto finito de ideais primos. O que é uma contradição.
Portanto todo ideal de R é produto finito de ideais primos, i.e., R é um anel de Dedekind. □

Assim temos essa nova definição equivalente as anteriores:

Definição 2.6. Um *anel de Dedekind* (ou *domínio de Dedekind*) é um domínio de integridade que satifaz as seguintes condições:

1. Todo ideal primo de R é maximal.
2. R é Noetheriano.
3. R é integralmente fechado no seu corpo de frações.

3 DIP se e somente se DFU

Essa seção é baseada em [4].

Teorema 3.1. Seja R um domínio de Dedekind. Então R é DIP se e somente se R é DFU.

Demonstração. Todo DIP é DFU. Então precisamos provar apenas a volta. Seja R um domínio de Dedekind e DFU. Vamos provar que todos ideais de R são principais. Como todo ideal de R é produto de ideais primos, basta provar que todo ideal primo é principal.

Seja P um ideal primo e x em P não nulo. Como R é um DFU, existem $p_1, \ldots, p_n$ primos e $e_1, \ldots, e_n$ inteiros positivos tais que $x = p_1^{e_1} \cdots p_n^{e_n}$. Assim, temos $p_1^{e_1} \cdots p_n^{e_n} \in P$. Como P é primo, existe p_j tal que $p_j \in P$. Assim $\langle p_j \rangle \subset P$. Vamos provar que $\langle p_j \rangle$ é maximal.

Seja J um ideal tal que $\langle p_j \rangle \subsetneq J$. Então seja $y \in J \setminus \langle p_j \rangle$. Pelo lema acima, existe ideal Q tal que $JQ = \langle p_j \rangle$. Seja $z \in Q$. Então $yz \in \langle p_j \rangle$. Ou seja, p_j divide yz. Como p_j é primo e $y \notin \langle p_j \rangle$, temos $z \in \langle p_j \rangle$. Isso acontece para todo $z \in Q$, portanto $Q \subset \langle p_j \rangle$. Mas $\langle p_j \rangle = JQ \subset Q$. Assim concluimos que $\langle p_j \rangle = Q$. Então $J\langle p_j \rangle = \langle p_j \rangle$. Como estamos em um domínio de integridade, isso implica $1 \in J$. Portanto $J = R$ e $\langle p_j \rangle$ é maximal.

Como $\langle p_j \rangle \subset P$ e $\langle p_j \rangle$ é maximal, concluimos que $P = \langle p_j \rangle$. Ou seja, P é ideal principal. Assim segue o teorema. □

4 Anéis de inteiros

Essa seção é baseada em [4].

Seja $\mathbb{K}$ um subcorpo de $\mathbb{C}$ (conjunto dos números complexos). Então $\mathbb{K}$ é um espaço vetorial sobre $\mathbb{Q}$ (conjunto dos números racionais). A dimensão de $\mathbb{K}$ sobre $\mathbb{Q}$ é chamada de grau e é denotada por $\deg_{\mathbb{K}/\mathbb{Q}}$.

Definição 4.1. Seja $\mathbb{K}$ um subcorpo de $\mathbb{C}$. Chamamos $\mathbb{K}$ de *corpo de números algébricos* se $\deg_{\mathbb{K}/\mathbb{Q}} < \infty$.

Observação 4.1. Todo elemento de $\mathbb{K}$ é um número algébrico sobre $\mathbb{Q}$.

Definição 4.2. Seja $\mathbb{K}$ um corpo de números algébricos. Defina o seguinte conjunto:

$$\mathcal{O}(\mathbb{K}) := \{x \in \mathbb{K} \mid x \text{ é um inteiro algébrico}\}$$

Chamamos esse conjunto de *anel de inteiros* de $\mathbb{K}$.

Proposição 4.1. Seja $\mathbb{K}$ um corpo de números algébricos e $x \in \mathbb{K}$. Existe inteiro não nulo m tal que mx é inteiro algébrico.

Demonstração. x é algébrico sobre $\mathbb{Q}$. Então existem $\frac{a_0}{b_0}, \frac{a_1}{b_1}, \ldots, \frac{a_{n-1}}{b_{n-1}}$ tais que $x^n + \frac{a_{n-1}}{b-1}x^{n-1} + \cdots + \frac{a_1}{b_1}x + \frac{a_0}{b_0} = 0$. Seja m o menor múltiplo comum de $b_0, b_1, \ldots, b_{n-1}$. Então temos:

$$0 = x^n + \frac{a_{n-1}}{b_{n-1}} + \cdots + \frac{a_1}{b_1}x + \frac{a_0}{b_0} = m^n\left(x^n + \frac{a_{n-1}}{b-1} + \cdots + \frac{a_1}{b_1}x + \frac{a_0}{b_0}\right) =$$
$$= (mx)^n + m\frac{a_{n-1}}{b-1}(mx)^{n-1} + \cdots + m^{n-1}\frac{a_1}{b_1}mx + m^n\frac{a_0}{b_0}$$

com $m\frac{a_{n-1}}{b_{n-1}}, \ldots, m^{n-1}\frac{a_1}{b_1}, m^n\frac{a_0}{b_0} \in \mathbb{Z}$. Então mx é inteiro algébrico. □

Proposição 4.2. Seja $\mathbb{K}$ um corpo de números algébricos. Então $\mathcal{O}(\mathbb{K})$ é um $\mathbb{Z}$-módulo livre de posto $\deg_{\mathbb{K}/\mathbb{Q}}$.

Demonstração. Seja $n = \deg_{\mathbb{K}/\mathbb{Q}}$ e $\{x_1, \ldots, x_n\}$ base de $\mathbb{K}$ sobre $\mathbb{Q}$. Pela proposição anterior, existem $a_1, \ldots, a_n \in \mathbb{Z}$ tais que $\{a_1x_1, \ldots, a_nx_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ formada por elementos de $\mathcal{O}(\mathbb{K})$. Assim, $\mathcal{O}(\mathbb{K})$ possui o $\mathbb{Z}$-módulo de posto n gerado por $\{a_1x_1, \ldots, a_nx_n\}$.

Por outro lado, seja $\{y_1, \ldots, y_{n+1}\} \subset \mathcal{O}(\mathbb{K})$. Como $\mathcal{O}(\mathbb{K})$ é $\mathbb{Q}$-subespaço de $\mathbb{K}$, $\{y_1, \ldots, y_{n+1}\}$ é linearmente dependente. Então existem $\frac{b_1}{c_1}, \ldots, \frac{b_{n+1}}{c_{n+1}} \in \mathbb{Q}$ tais que $\frac{b_1}{c_1}y_1 + \cdots + \frac{b_{n+1}}{c_{n+1}}y_{n+1} = 0$. Seja d o mínimo múltiplo comum de $c_1, \ldots, c_{n+1}$. Então $d\frac{b_1}{c_1}y_1 + \cdots + d\frac{b_{n+1}}{c_{n+1}}y_{n+1} = 0$ e $d\frac{b_1}{c_1}, \ldots, d\frac{b_{n+1}}{c_{n+1}} \in \mathbb{Z}$. Ou seja, $\{y_1, \ldots, y_{n+1}\}$ são linearmente dependentes também sobre $\mathbb{Z}$. Então $\mathcal{O}(\mathbb{K})$ não pode conter $\mathbb{Z}$-submódulos de posto $n+1$.

Então $\mathcal{O}(\mathbb{K})$ tem que ser $\mathbb{Z}$-módulo livre de posto n. □

Seja S um conjunto. Denote por $|S|$ a cardinalidade S.

Lema 4.1. Seja $\mathbb{K}$ um corpo de números algébricos e $R = \mathcal{O}(\mathbb{K})$. Seja $n = \deg_{\mathbb{K}/\mathbb{Q}}$.

1. Se $I = \langle m \rangle$ para algum inteiro m não nulo, então $|R/I| = |m|^n$.
2. Se I é um ideal de R, então $|R/I|$ é finito.

Demonstração. 1. Pela proposição 4.2, R é um $\mathbb{Z}$-módulo de posto n. Dessa forma, seja $\{x_1, \ldots, x_n\}$ uma base de R. Então $\{mx_1, \ldots, mx_n\}$ é base de I. Assim temos que R/I é isomórfico como $\mathbb{Z}$-módulo à $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^n$. Como $\left|\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^n\right| = |m|^n$, segue $|R/I| = |m|^n$.

2. Vamos provar que I possui um inteiro positivo m não nulo. Seja $x \in I$. Como $x \in R$, existem $a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}$ com $a_0 \neq 0$ tais que $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$. Defina $m = a_0$. Então m é inteiro não nulo e $m = -x^n - a_{n-1}x^{n-1} - \cdots - a_1 x \in I$.

   Seja $J = \langle m \rangle$. Temos $J \subset I$ e $\frac{R/J}{I/J} \cong R/I$. Como $|R/J|$ é finito por 1. desse lema, concluimos que $|R/I|$ é finito.

□

Teorema 4.1. Seja $\mathbb{K}$ um corpo de números algébricos e $R = \mathcal{O}(\mathbb{K})$ seu anel de inteiros. Então $R = \mathcal{O}(\mathbb{K})$ é um anel de Dedekind.

Demonstração. Vamos verificar que R satisfaz 1., 2. e 3. da definição 2.6.

- Seja P um ideal primo não nulo. Vamos provar que P é maximal. Como P é primo, R/P é domínio de integridade. Pelo lema anterior, R/P é finito. Mas todo domínio de integridade finito é um corpo. Portanto, R/P é um corpo. Isso implica que P é maximal.

- Sejam I e J ideais de R tais que $I \subset J$. Temos $\frac{R/I}{J/I} \cong R/J$. Pelo lema anterior $|R/I| < \infty$. Assim $|R/J| \leq |R/I| < \infty$. Então se $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ é uma cadeia ascendente de R, temos $0 \leq \cdots \leq |R/I_n| \leq \cdots \leq |R/I_2| \leq |R/I_1| < \infty$. Então $\{|R/I_1|, \ldots, |R/I_n|, \ldots\}$ é finito. Portanto, a cadeia ascendente de ideais tem que se estabilizar e R é Noetheriano.

- Primeiro vamos provar que $R \cap \mathbb{Q} = \mathbb{Z}$. Claramente $\mathbb{Z} \subset R \cap \mathbb{Q}$. Vamos provar que $R \cap \mathbb{Q} \subset \mathbb{Z}$. Seja $\frac{a}{b} \in R \cap \mathbb{Q}$ com a e b coprimos. Então existem $c_0, c_1, \ldots, c_{n-1} \in \mathbb{Z}$ tais que $\left(\frac{a}{b}\right)^n + \cdots + c_1 \frac{a}{b} + c_0 = 0$. Então: $a^n + \cdots + b^{n-1} c_1 a + b^n c_0 = 0$ e $a^n = -ba^{n-1} - \cdots - b^{n-1} c_1 a - b^n c_0 \in \mathbb{Z}$. Então b divide a^n. Impossível, pois a e b são coprimos. Portanto $b = 1$ ou $b = -1$ e $\frac{a}{b} \in \mathbb{Z}$.

  Agora seja x no corpo de frações de R tal que x é integral sobre R. Então $x \in \mathbb{K}$, pois $\mathbb{K}$ e um corpo que contém R. Assim x é integral sobre $\mathbb{Q}$. Portanto x é integral sobre $R \cap \mathbb{Q} = \mathbb{Z}$, ou seja, $x \in R$. Portanto R é integralmente fechado.

□

Exemplo 4.1. $\mathcal{O}(\mathbb{Q}[\sqrt{-5}]) = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Q}\}$:
Temos

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$$

- 6 é raiz de $x - 6 \Rightarrow 6 \in \mathcal{O}(\mathbb{Q}[\sqrt{-5}])$
- 2 é raiz de $x - 2 \Rightarrow 2 \in \mathcal{O}(\mathbb{Q}[\sqrt{-5}])$
- 3 é raiz de $x - 3 \Rightarrow 3 \in \mathcal{O}(\mathbb{Q}[\sqrt{-5}])$
- $1 + \sqrt{-5}$ é raiz de $x^2 - 2x + 6 \Rightarrow 1 + \sqrt{-5} \in \mathcal{O}(\mathbb{Q}[\sqrt{-5}])$
- $1 - \sqrt{-5}$ é raiz de $x^2 - 2x + 6 \Rightarrow 1 - \sqrt{-5} \in \mathcal{O}(\mathbb{Q}[\sqrt{-5}])$

Portanto $\mathcal{O}(\mathbb{Q}[\sqrt{-5}])$ não é DFU. Mas, pelo teorema anterior, é um anel de Dedekind.

Referências

[1] Wikipedia. Richard Dedekind. `https://en.wikipedia.org/wiki/Richard_Dedekind`. Acessado em: 2020-07-14.

[2] I.S. Cohen Oscar Zariski, Pierre Samuel. *Commutative Algebra - Volume I*. University Series in Higher Mathematics. D. Van Nostrand Co Inc, 5 pr. edition, 1958.

[3] Robert B. Ash. Dedekind Domains. `https://faculty.math.illinois.edu/~r-ash/Ant/AntChapter3.pdf`. Acessado em: 2020-07-14.

[4] Steven H. Weintraub. *Factorization: Unique and Otherwise*. CMS Treatises in Mathematics. A. K. Peters, 2008.