Introdução aos anéis de divisão

Carla Mörschbächer*

Teoria de Anéis não comutativos

Professor Eliezer Batista

Pós-Graduação em Matemática Pura e Aplicada

Universidade Federal de Santa Catarina

17 de julho de 2014

Resumo

Neste trabalho vamos apresentar a demonstração de três resultados principais a respeito de anéis de divisão: o Teorema de Wedderburb, o Teorema de Jacobson e o Teorema de Frobenius.

1 Introdução

Um anel R é denominado um *anel de divisão* se $R\backslash\{0\}$ é um grupo multiplicativo, ou seja, se para todo $x \in R \setminus \{0\}$, existe $y \in R$, tal que

$$xy = yx = 1_R.$$

É uma estrutura rica, pois nela podemos somar, subtrair, multiplicar e dividir. Notemos que, acrescentando o axioma da comutatividade da multiplicação a um anel de divisão, obtemos um corpo. Deste modo, todo corpo é um exemplo de anel de divisão. No entanto, os exemplos mais interessantes são os não comutativos.

Um exemplo tradicional de anel de divisão não comutativo é o anel dos quatérnios $\mathbb{H}$, apresentado em 1843 por Hamilton:

$$\mathbb{H} = \{a + bi + cj + dk | a; b; c; d \in \mathbb{R}\}.$$

A adição e a multiplicação em $\mathbb{H}$ são definidos da seguinte maneira:

$$(\mathbf{a_1} + \mathbf{b_1 i} + \mathbf{c_1 j} + \mathbf{d_1 k}) + (\mathbf{a_2} + \mathbf{b_2 i} + \mathbf{c_2 j} + \mathbf{d_2 k}) = (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k$$

$$(\mathbf{a_1} + \mathbf{b_1 i} + \mathbf{c_1 j} + \mathbf{d_1 k}).(\mathbf{a_2} + \mathbf{b_2 i} + \mathbf{c_2 j} + \mathbf{d_2 k}) =$$
$$= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 b_1 a_2 + c_1 d_2 - d_1 c_2)i +$$

*carlamtm@gmail.com

$$+(a_1c_2+c_1a_2+d_1b_2-b_1.d_2)j+(a_1d_2+d_1a_2+b_1c_2-c_1b_2)k.$$

Além disso, dado $a+bi+cj+dk \in \mathbb{H}$, não nulo, seu inverso multiplicativo é dado por

$$\frac{a}{m}-\frac{b}{m}i-\frac{c}{m}j-\frac{d}{m}k,$$

em que, $m=a^2+b^2+c^2+d^2$. Assim $\mathbb{H}$ é um anel de divisão não comutativo.

Outros exemplos podem ser encontrados na seção 14 da referência [5], onde o autor apresenta a construção clássica de vários anéis de divisão não comutativos.

Com relação aos ideais de um anel de divisão, temos o seguinte resultado:

"Em um anel de divisão os únicos ideais à esquerda (resp. direita) são os triviais."

De fato, sejam R um anel de divisão e S um ideal de R. Supomos que $S \neq \emptyset$. Se $s \in S, s \neq 0$, então $rs \in S$, para todo $r \in R$. Em particular, considerando $r = s^{-1}$ obtemos que $s^{-1}s = 1_R \in S$. E assim concluímos que $S = R$. Segue, deste fato, que todo anel de divisão é um anel simples.

Neste trabalho vamos focar nossa atenção em três resultados principais a respeito de anéis de divisão. O primeiro relaciona, de forma surpreendente, a comutatividade da operação de multiplicação com a quantidade de elementos do conjunto. Mais precisamente o resultado afirma que:

Todo anel de divisão finito é um corpo.

Esse resultado é conhecido como *Teorema de Wedderburn* ou *Pequeno Teorema de Wedderburn* pois é devido ao Matemático MacLagan Wedderburn, que em 1905 apresentou três provas diferentes para o teorema. Outros matemáticos, como por exemplo, Leonard E. Dickson, Emil Artin, Hans Zassenhaus, Nicolas Bourbaki, Ernest Witt, etc, também apresentaram demontrações. Escolhemos, neste trabalho, apresentar a prova feita em 1931 por Ernest Witt, que se destaca por ser bastante simples. Essa versão de Ernest Witt pode ser encontrada na referência [1].

O segundo resultado, conhecido como Teorema de Jacobson, é uma generalização do Teorema de Wedderburn feita em 1945 por Nathan Jacobson, um brilhante aluno de doutorado do próprio MacLagan Wedderburn. Mostraremos que:

Se para todo elemento de um anel de divisão existir um número natural $n > 1$ ***tal que*** $a^n = a$***, então o anel de divisão é um corpo.***

Notemos que o Teorema de Jacobson é de fato uma genaralização do Teorema de Wedderburn:
Se D um anel de divisão finito, com q elementos, então $D \setminus \{0\}$ é um grupo multiplicativo com $q-1$ elementos e portanto $d^{q-1}=1$, donde segue $d^q = d$. Assim, um anel de divisão finito sempre satisfaz as hipóteses do Teorema de Jacobson.

O terceiro resultado, Teorema de Frobenius, trata-se de uma classificação de anéis de divisão:

"Todo anel de divisão algébrico sobre o corpo dos reais é isomorfo: ao corpo dos reais, ou ao corpo dos complexos, ou ao anel de divisão dos quatérnios."

Esse resultado foi demonstrado em 1877, anteriormente aos dois resultados já citados, pelo Matemático alemão Ferdinand Georg Frobenius. Ele caracteriza, a menos de isomorfismo, os anéis de divisão sobre o corpo dos números reais.
A demonstração do segundo e terceiro resultado, bem como uma outra prova para o Teorema de Wedderburn, podem ser encontrados na referência [3].

2 O Teorema de Wedderburn

Iniciamos discutindo alguns ingredientes necessários para a demonstração do Teorema de Wedderburn.

2.1 Raízes da unidade

Qualquer número complexo $z = x + iy$ pode ser escrito na forma polar

$$z = re^{i\theta} = r(cos\theta + i\sin\theta),$$

em que $r = |z| = \sqrt{x^2 + y^2}$ é a distância de z até a origem e θ é o ângulo medido a partir do eixo x positivo.
A partir da forma polar de um número complexo podemos obter os resultados a seguir, que dizem respeito a exponenciação e raízes n-ésimas no conjunto dos números Complexos.

Teorema 2.11: Dado o número complexo $z = \rho(\cos\theta + i.\sin\theta)$, não nulo, e o número inteiro n, então

$$z^n = \rho^n(\cos n\theta + i\sin n\theta) \quad (1^{\text{a}} \text{ Fórmula de Moivre}).$$

Teorema 2.12: Dado número complexo $z = \rho(\cos\theta + i.\sin\theta)$ e o número natural $n(n \geq 2)$, então existem n raízes n-ésimas de z que são da forma:

$$z_k = \sqrt[n]{\rho}.\left[\cos\left(\frac{\theta}{n} + k.\frac{2\pi}{n}\right) + i\sin\left(\frac{\theta}{n} + k.\frac{2\pi}{n}\right)\right] \quad (2^{\text{a}} \text{ Fórmula de Moivre}),$$

em que, $\sqrt[n]{\rho} \in \mathbb{R}^+$ e $0 < k < n - 1$.

Consideremos o polinômio $x^n - 1$. Como $1 = 1(cos0 + i\sin 0)$, as n raízes de $x^n - 1$, chamadas *raízes n-ésimas da unidade*, em $\mathbb{C}$, são

$$\lambda_k = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right) = e^{\frac{2k\pi i}{n}}, \qquad 0 \leq k \leq n - 1.$$

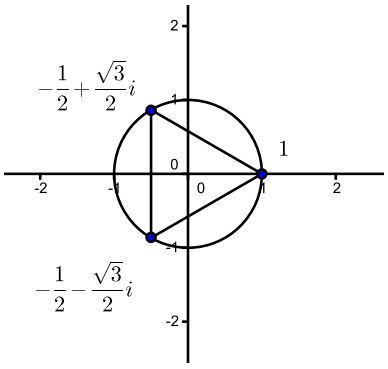
Definindo $\xi := e^{\frac{2\pi i}{n}}$, vemos que $\lambda_k = \xi^k$ e portanto o conjunto de todas as raízes da unidade

$$\beta = \{\xi, \xi^2, ..., \xi^n = 1\}$$

forma um grupo cíclico de ordem n gerado por ξ.
Observemos que a ordem (menor expoente positivo tal que $\xi^d = 1$) de uma raiz da unidade pode ser menor do que n, por exemplo, $(-1)^2 = 1$ e portanto -1 é uma raiz de ordem 2, já 1 é raiz de ordem 1, pois $1^1 = 1$. Por outro lado, existem raízes de ordem n. De fato, considere $\lambda_1 = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$, teremos $(\lambda_1)^n = 1$ e $(\lambda_1)^k \neq 1$ para $0 < k < n$.

Observemos também que a ordem de uma raiz n-ésima da unidade é numericamente igual a quantidade de elementos do subgrupo gerado por ela. Logo, pelo Teorema de Lagrange, a ordem de uma raiz divide n, em que n é a quantidade de elementos do grupo β.
Além disso, como β é cíclico, para cada inteiro m que divide n, existem raízes da unidade de ordem m ([2], página 65).

Geometricamente as raízes da unidades localizam-se no plano complexo, sob o círculo unitário. Formam um polígono regular de n lados. Segue abaixo representação gráfica de raízes n-ésimas para $n = 3$:



2.2 Resultados auxiliares

Notação: No decorrer do trabalho $|A|$ representará a quantidades de elementos do conjunto A.

Definição 2.21: Seja R um anel, o centro de R, denotado por $Z(R)$ é o conjunto de todos os elementos que comutam em R, ou seja,

$$Z(R) = \{x \in R | xr = rx, \forall r \in R\}.$$

Definição 2.22: Sejam R um anel e $s \in R$, o centralizados de s em R, denotado por C_s é o conjunto de todos os elementos de R que comutam com s, ou seja,

$$C_s = \{x \in R | xs = sx\}.$$

Lema 2.23: Sejam R um anel de divisão, $Z(R)$ o centro de R, C_s ($s \in R$) o centralizador de s em R, então $Z(R)$ e C_s são subanéis de divisão de R.

Demonstração: Sejam $z_1, z_2 \in Z(R)$, então

$$r.(z_1 + z_2) = r.z_1 + r.z_2 = z_1.r + z_2.r = (z_1 + z_2).r$$

e

$$r.(z_1.z_2) = (r.z_1).z_2 = (z_1.r)z_2 = z_1.(r.z_2) = z_1.(z_2.r) = (z_1.z_2).r.$$

Logo $z_1 + z_2, z_1.z_2 \in Z(R)$, donde $Z(R)$ é subanel de R.
Seja $z \in Z(R), z \neq 0$, então $z^{-1} \in Z(R)$. De fato, notemos que,

$$r = r.1 = rzz^{-1} = zrz^{-1}, \forall r \in R.$$

Multiplicando em ambos os lados (pela esquerda) da equação acima por z^{-1} obtemos,

$$z^{-1}r = rz^{-1} \forall r \in R.$$

Assim $z^{-1} \in Z(R)$ e portanto, $Z(R)$ é um subanel de divisão de R.
Agora, seja $s \in R$, $r_1, r_2 \in C_s$

$$s.(r_1 + r_2) = s.r_1 + s.r_2 = r_1.s + r_2.s = (r_1 + r_2).s$$

e

$$s.(r_1.r_2) = (s.r_1).r_2 = (r_1.s)r_2 = r_1.(s.r_2) = r_1.(r_2.s) = (r_1.r_2).s.$$

Deste modo, $r_1 + r_2, r_1.r_2 \in C_s$, donde C_s é subanel de R.
Seja $r \in C_s, r \neq 0$, então $r^{-1} \in C_s$. De fato, notemos que,

$$s = s.1 = srr^{-1} = rsr^{-1}.$$

Multiplicando em ambos os lados (pela esquerda) por r^{-1} obtemos,

$$r^{-1}s = sz^{-1}.$$

Logo $r^{-1} \in C_s$ e C_s é um subanel de divisão de R.

■

Corolário 2.24: $Z(R)$ é um corpo.

Demonstração: Pelo resultado anterior $Z(R)$ é um anel de divisão. Como $Z(R)$ é comutativo, segue que é corpo.

■

2.3 Demonstração do Teorema de Wedderburn

Teorema (WEDDERBURN): Todo anel de divisão finito é um corpo.

Demonstração: Parte 1: Sejam R um anel de divisão finito, $Z(R)$ o centro de R,

$$Z(R) = \{x \in R | xr = rx, \forall r \in R\},$$

e para todo elemento $s \in R$ o conjunto C_s dos elementos de R que comutam com s,

$$C_s = \{x \in R | xs = sx\}.$$

Pelos lemas anteriores, segue que C_s é um subanel de divisão finito de R e $Z(R)$ um corpo finito contido em R com, digamos, q elementos. Como $0, 1 \in Z(R)$ segue que $q \geq 2$.
Considerando R como um espaço vetorial sobre $Z(R)$ temos $|R| = q^n$, em que, $n = dim_{Z(R)}R$. Analogamente, considerando, para cada $s \in R$, C_s como um espaço vetorial sobre $Z(R)$, temos $|C_s| = q^{n_s}$, onde $n_s := dim_{Z(R)}C_s$.

Suponhamos, por contradição, que R não é um corpo, ou seja, que R não é comutativo, então $n > 1$. De fato, se R não é comutativo e $n = 1$, então existe uma base de R com apenas um elemento. Seja $\beta = \{b\}$ esta base. Assim, dado $r \in R \setminus Z(R)$, existe $z \in Z(R)$, de modo que $r = zb$. Por outro lado, dado $r' \in Z(R)$, existe $z' \in Z(R)$ tal que $r' = z'b$, ou seja, $b = \dfrac{r'}{z'} \in Z(R)$, donde concluímos que $r \in Z(R)$. Contradição. Logo, se R não é comutativo, segue que $n > 1$.

Seja $R^* := R \setminus \{0\}$, o grupo multiplicativo associado a R. Consideremos em R^* a seguinte relação:

$$r' \sim r :\Leftrightarrow r' = x^{-1}rx \text{ para algum } x \in R^*.$$

$\sim$ é uma relação de equivalência e particiona R^* em classes de equivalências denominadas Classes de Conjugação.
Seja $A_s := \{x^{-1}sx : x \in R^*\}$ a classe que contém s. Notemos que $|A_s| = 1$ se, e somente se, $s \in Z(R)$. Como assumimos que R não é comutativo exite pelo menos um elemento $s \in R^*$ tal que $|A_s| \geq 2$.
Sejam $A_1, ..., A_t, A_{t+1}, ...A_{t+q-1}$ as classes de conjugação de R^*, em que $A_{t+1}, ...A_{t+q-1}$ são classes associadas a elementos do centro de R^* (cada elemento de $Z(R)^*$ define uma classe com um elemento). Concluímos que:

$$\begin{aligned} |R^*| &= \sum_{i=1}^{t+q-1} |A_i| \\ &= \sum_{i=1}^{t} |A_i| + \sum_{i=1}^{q-1} |A_{t+i}| \\ &= \sum_{i=1}^{t} |A_i| + |Z(R)^*|. \end{aligned} \tag{1}$$

Nosso objetivo agora é encontrar uma relação para a quantidade de elementos de A_s, para todo $s \in R$. Para tanto, consideremos, para todo $s \in R^*$, a aplicação sobrejetiva $f_s : R^* \to A_s$, definida por $f_s(x) = x^{-1}sx$. Notemos que

$$\begin{aligned} f_s(x) = f_s(y) &\Leftrightarrow x^{-1}sx = y^{-1}sy \\ &\Leftrightarrow (yx^{-1})s = s(yx^{-1}) \\ &\Leftrightarrow yx^{-1} \in C_s^* \\ &\Leftrightarrow y \in C_s^*x, \end{aligned}$$

em que, $C_s^*x := \{zx | z \in C_s^*\}$ e $|C_s^*| = |C_s^*x|$, ou seja, $|C_s^*x| = q^{n_s} - 1$.
Logo, cada elemento $x^{-1}sx \in A_s$ está associado, pela f_s, precisamente à todos os $q^{n_s} - 1$ elementos de C_s^*x. Deste modo,

$$|R^*| = |A_s||C_s^*x| = |A_s||C_s^*|.$$

Em particular, obtemos que a quantidade de elementos de C_s^* divide a quantidade de elementos de R^*, ou seja:

$$\frac{|R^*|}{|C_s^*|} = \frac{q^n - 1}{q^{n_s} - 1} = |A_s| \text{ é um inteiro para todo s.} \tag{2}$$

Substituindo a equação (2) em (1) e lembrando que $|R^*| = q^n - 1$ e $Z^* = q - 1$, obtemos a chamada Fórmula de Classe:

$$q^n - 1 = q - 1 + \sum_{i=1}^{t} \frac{q^n - 1}{q^{n_i} - 1},$$

em que, $\dfrac{q^n - 1}{q^{n_i} - 1} > 1$ para $i \in \{1, ...t\}$, pois representa a quantidade de elementos da classe de um elemento que não está em $Z(R)$.
Mostremos agora que $n_i | n$ para todo i.
Suponhamos que $n = k.n_i + r$, com $0 \leq r < n_i$ e notemos que

$$q^n - 1 = (q^{n_i} - 1)(q^{n-n_i} + q^{n-2n_i} + ... + q^{n-kn_i}) + \underbrace{(q^{n-kn_i} - 1)}_{= q^r - 1}. \tag{3}$$

Como C_s^* é um subrugrupo multiplicativo de R^* temos, pelo Torema de Lagrange, que $|C_s^*|$ divide $|R^*|$, ou seja, $q^{n_i} - 1 | q^n - 1$. Assim, pela equação (3), obtemos que $q^{n_i} - 1 | q^r - 1$ e isto implica em r ser igual a zero, caso contrário teríamos uma contradição, pois $r < n_i$. Concluímos portanto que $r = 0$ e $n_i | n$.

Parte 2: Considere o polinômio $p(x) = x^n - 1$ e o grupo cíclico das raízes da unidade $\beta = \{\xi, \xi^2, ..., \xi^n\}$. Agrupamos as raízes de ordem d e definimos:

$$\phi_d(x) := \prod_{\lambda \text{ de ordem } d} (x - \lambda).$$

Deste modo,

$$x^n - 1 = \prod_{d|n} \phi_d(x). \tag{4}$$

Afirmação: Os coeficientes dos polinômios $\phi_n(x)$ são inteiros, ou seja, $\phi_n(x) \in \mathbb{Z}[x]$, e o coeficiente constante é 1 ou -1.
De fato, para $n = 1$, temos $\phi_1(x) = x - 1$ e a única raiz é 1. Agora vamos assumir, por indução, que $\phi_d(x) \in \mathbb{Z}[x]$ para todo $d < n$ e que o coeficiente contante de $\phi_d(x)$ é 1 ou -1. De (4) obtemos que

$$x^n - 1 = p(x)\phi_n(x), \tag{5}$$

em que,

$$p(x) = \sum_{i=0}^{l} p_i x^i \qquad \text{e} \qquad \phi_n(x) = \sum_{j=0}^{n-l} a_j x^j,$$

com $p_i \in \mathbb{Z}$ e $p_0 = 0$ ou $p_0 = -1$, pois

$$p(x) = \prod_{\lambda|n(\lambda\neq n)} \phi_d(x).$$

Observando os dois lados da equação (5) percebemos que $a_0 \in \{1, -1\}$, pois $-1 = p_0 a_0$. Agora, supondo que $a_0, a_1, ...a_{k-1} \in \mathbb{Z}$, mostremos que o coeficiente de x^k é um inteiro. O lado esquerdo de (5) afirma que o coeficiente de x^k é um inteiro e partir do lado direito de (5) temos que o coeficiente de x^k é dado por:

$$\sum_{i=0}^{k} p_i a_{k-i} = p_0 a_k + \sum_{i=1}^{k} p_i a_{k-i}.$$

Como $\left(p_0 a_k + \sum_{i=1}^{k} p_i a_{k-i}\right) \in \mathbb{Z}$, $a_0, ..., a_{k-1}, p_0, ..., p_k \in \mathbb{Z}$, concluímos que $p_0 a_k \in \mathbb{Z}$ e então, como $p_0 \in \{-1, 1\}$, segue que $a_k \in \mathbb{Z}$.
Logo, $\phi_n(x) \in \mathbb{Z}[x]$, para todo n.

Parte 3: Seja n_i um dos números que aparecem na Fórmula de Classes. Sabemos que n_i divide n, então existem raízes da unidade de ordem n_i. Deste modo, como as raízes de ordem até n_i são precisamente as raízes de $(x^{n_i} - 1)$, obtemos:

$$x^n - 1 = \prod_{d|n} \phi_d(x) = (x^{n_i} - 1)\phi_n(x) \prod_{d|n, d\nmid n_i, d\neq n} \phi_d(x).$$

Portanto, como $\phi_n(x) \in \mathbb{Z}[x]$ para todo n, temos em $\mathbb{Z}$ as seguintes relações de divisibilidade

$$\phi_n(q) | q^n - 1 \qquad \text{e} \qquad \phi_n(q) | \frac{q^n - 1}{q^{n_i} - 1}. \tag{6}$$

Como (6) vale para todo i, segue que

$$\phi_n(q)|q-1.$$

No entanto, isto não pode ocorrer. De fato, notemos que

$$\phi_n(x) = \prod_{\lambda \ de \ ordem \ n} (x-\lambda).$$

Seja $\widetilde{\lambda} = a+ib$ uma das raízes de ordem n. Como estamos supondo $n>1$, segue que $\widetilde{\lambda} \neq 1$ (1 é uma raiz de ordem 1). Deste modo, $a<1$, pois as raízes estão sobre o círculo unitário. Logo,

$$\begin{aligned} |q-\widetilde{\lambda}|^2 &= |q-a-ib|^2 = (q-a)^2+b^2 \\ &= q^2-2aq+a^2+b^2 \\ &= q^2-2aq+1 \\ &> q^2-2q+1, \qquad \text{pois } a<1 \\ &= (q-1)^2. \end{aligned}$$

Assim, para toda raiz $\widetilde{\lambda}$ de ordem n, temos válida a seguinte desigualdade

$$|q-\widetilde{\lambda}| > q-1,$$

e como $q \geq 2$, segue que,

$$|\phi_n(q)| = \prod_{\lambda \ de \ ordem \ n} |q-\lambda| > q-1.$$

Logo, $\phi_n(q)$ não pode ser um divisor inteiro de $q-1$. Contradição.
Portanto, a suposição de que D não é comutativo está incorreta, donde concluímos que D é um corpo.

■

Corolário: Seja D um anel de divisão e R um subanel finito de D, então R é um corpo.

Demonstração: Seja $R = \{r_1, ..., r_n\}$ um subanel finito de D. Para cada $r_i \neq 0$, $i \in \{1, ..., n\}$, considere os seguintes produtos:

$$r_ir_1, r_ir_2, ...r_ir_i, ..., r_ir_n.$$

Notemos que se $k \neq j$, então $r_ir_k \neq r_ir_j$. De fato, se $r_ir_k = r_ir_j$, então $r_i(r_k-r_j)=0$ e como D é anel de divisão, segue que $r_k-r_j=0$, ou seja, $r_k=r_j$.
Assim, todos os n produtos acima assumem valores distintos em R e portanto, existe $k \in \{1, ..., n\}$ de modo que $r_ir_k = r_i$. Isto implica que $r_k = 1$, ou seja, $1 \in R$. Mas se

$1 \in R$, então existe algum produto $r_i r_j$, tal que, $r_i r_j = 1$. Logo r_i é inversível e R é um anel de divisão.
Portanto, pelo Teorema de Wedderburn, R é um corpo.

■

3 O Teorema de Jacobson

Enunciamos abaixo algumas definições e lemas com o objetivo de provar o Teorema de Jacobson, que pode ser interpretado como uma generalização do Teorema de Wedderburn.

3.1 Resultados básicos

Lema 3.10: Se G é um grupo finito e $a \in G$, então $a^{|G|} = 1_G$.

Demonstração: Ver [3], página 51.

Definição3.11: Seja R um anel com unidade. A a característica de R é o menor inteiro positivo n, tal que, $n.1_R = 0$. Se R tem característica n, denotamos $char(R) = n$.

Proposição 3.12: Seja D um anel de integridade, então ou $char(D) = 0$ ou $char(D) = p$, em que p é um primo.

Demonstração: Ver [2], página 178.

Lema 3.13: Seja F um corpo finito, então F possui p^m elementos, em que, p é um número primo que representa a característica de F.

Demonstração: Ver [3], página 361.

Lema 3.14: Para todo número p primo e todo inteiro positivo m existe um único corpo que contém p^m elementos.

Demonstração: Ver [3], página 361.

Corolário 3.15: Se um corpo F possui p^m elementos, então $a^{p^m} = a$ para todo $a \in F$.

Demonstração: Ver [3], página 361.

Lema 3.16: Sejam K um corpo finito com q elementos e $F \subset K$, em que K também é corpo finito. Então K possui q^n elementos, em que $n = dim_F K$.

Demonstração: Ver [3], página 361.

Definição 3.17: Dado um corpo F, dizemos que L (corpo) é uma extensão de F se F é subcorpo de L. Denotamos essa extensão de corpos por $F \subset L$ ou $L = F$.

Definição 3.18: Seja $F \subset L$ extensão de corpos e seja $a \in L$. Então a é dito ser um elemento algébrico sobre F se existe um polinômio não nulo $p(x) \in F[x]$ tal que $p(a) = 0$. Se $F \subset L$ extensão de corpos e $a \in L$ tal que $a \notin F$. Então denotamos por $F(a)$ o menor corpo tal que $F \subset F(a)$ e $a \in F(a)$.

Lema 3.19: Suponha que $K \supset F$ e que $a \in K$ é algébrico sobre F de grau n. Então $F(a)$, o corpo obtido agregando a a F é uma extensão finita de F e $dim_F F(a) = h$.

Demonstração: Ver [3], página 201.

Lema 3.20: Se F é um corpo finito e $|F| = p^m$, então o polinômio $x^{p^m} - x \in F[x]$ se decompõe em $F[x]$ da seguinte forma:

$$x^{p^m} - x = \prod_{\lambda \in F} (x - \lambda).$$

Demonstração: Ver [3], página 362.

3.2 O Teorema

Lema 3.21: Sejam R um anel, $a \in R$ e a aplicação $T_a : R \to R$ definida por $xTa := xa - ax$. Então,

$$xT_a^m = xa^m - maxa^{m-1} + \frac{m(m-1)}{2}a^2xa^{m-2} - \frac{m(m-1)(m-2)}{3!}a^3xa^{m-3} + ...$$

Demonstração: Ver demonstração por indução em [3], página 369.

Lema 3.22: Sejam R um anel e p um número primo positivo. Se $px = 0$ para todo $x \in R$, então $xT_a^{p^m} = xa^{p^m} - a^{p^m}x$.

Demonstração: Ver demonstração por indução em [3], página 369.

Lema 3.23: Sejam D um anel de divisão com característica $p > 0$ (p primo), $Z(D)$ o centro de D e $P = \{0, 1, 2, ..., (p-1)\}$ o subcorpo de $Z(D)$ isomorfo a $\mathbb{Z}_p$. Suponha que $a \in D \setminus Z(D)$ é tal que $a^{p^n} = a$, para algum inteiro postitivo n. Então existe $x \in D$ tal que:

(i) $xax^{-1} \neq a$.

(ii) $xax^{-1} \in P(a)$, o corpo obtido pela adjunção de a a P.

Demonstração: Consideremos a aplicação $T_a : R \to R$, definida por, $xTa := xa - ax$. Como $a^{p^n} = a$, temos que a é raiz do polinômio $p(x) = x^{p^m} - x \in P[x]$. Assim, a é

algébrico sobre P e portanto, pelo Lema 3.19, $P(a)$, o corpo obtido pela adjunção de a a P, é finito.
Considerando $P(a)$ como um espaço vetorial sobre P obtemos que $|P(a)| = p^m$, em que, $m = dim_P P(a)$. Assim, pelo Lema 3.15 segue que $u^{p^m} = u$, para todo $u \in P(a)$. Logo, pelo lema anterior, temos:

$$\begin{aligned} yT_a^{p^m} &= ya^{p^m} - a^{p^m}y \\ &= ya - ay \\ &= yT_a, \end{aligned}$$

donde inferimos que a igualdade $T_a^{p^m} = T_a$ é verdadeira.
Seja $\lambda \in P(a)$, então,

$$\begin{aligned} (\lambda x)T_a &= (\lambda x)a - a(\lambda x) \\ &= \lambda xa - \lambda ax, \text{ pois } \lambda \in P(a) \subseteq Z(D) \\ &= \lambda(xa - ax) \\ &= \lambda(xT_a). \end{aligned}$$

Deste modo, a aplicação $\lambda I : D \to D$, definida por $\lambda I(y) := \lambda y$ comuta com T_a, para todo $\lambda \in P(a)$.
Consideremos o polinômio $x^{p^m} - x$. Pelo Lema 3.20, e como u é raiz, podemos reescrevê-lo da seguinte maneira:

$$u^{p^m} - u = \prod_{\lambda \in P(a)} (u - \lambda).$$

Como T_a comuta com λI para todo $\lambda \in P(a)$ e como $T_a^{p^m} = T_a$, obtemos que

$$0 = T_a^{p^m} - T_a = \prod_{\lambda \in P(a)} (T_a - \lambda I).$$

Suponha, por absurdo, que $y(T_a - \lambda I) \neq 0$ para todo $\lambda \in P(a)$, $\lambda \neq 0$ e para todo $y \in D$. Notemos que

$$\prod_{\lambda \in P(a)} (T_a - \lambda I)$$

pode ser reescrito da seguinte forma:

$$T_a(T_a - \lambda_1)...(T_a - \lambda_k),$$

em que $\lambda_1, ..., \lambda_k$ são os elementos não nulos de $P(a)$. Assim, se $y(T_a - \lambda I) \neq 0$ para todo $\lambda \in P(a)$, $\lambda \neq 0$ e para todo $y \in D$, obtemos que $T_a = 0$, donde segue que $0 = yT_a = ya - ay$, para todo $y \in D$. Neste caso, $ya = ay$, ou seja, $a \in Z(D)$. Contradição.
Concluímos que existe $0 \neq \lambda \in P(a)$ e $0 \neq x \in D$ tais que $x(T_a - \lambda I) = 0$. Deste modo, $xa - ax - \lambda x = 0$ e portanto

$$xax^{-1} = a + \lambda.$$

Como $a, \lambda \in P(a)$, segue $xax^{-1} \in P(a)$ e como $\lambda \neq 0$, obtemos que

$$xax^{-1} \neq a,$$

como queríamos mostrar.

■

Corolário 3.24: No lema anterior, temos $xax^{-1} = a^m$ para algum inteiro m.

Demonstração: Seja a de ordem r. As raízes de $p(x) = x^r - 1$ são $1, a, a^2, ..., a^{r-1}$. Notemos que $(x^{-1}ax)^r = x^{-1}a^r x = 1$. Logo $x^{-1}ax$ é uma raiz de $p(x) = x^r - 1$ e portanto é igual a a^m para algum m.

■

Teorema (JACOBSON): Seja D un anel com divisão tal que para todo $a \in D$ existe um inteiro positivo $n(a) > 1$, dependente de a, tal que $a^{n(a)} = a$. Então D é um corpo.

Demonstração: Seja $a \in D$, então, por hipótese, existem inteiros m e n tais que $a^n = a$ e $(2a)^m = 2a$. Considerando $s := (n-1)(m-1) + 1$, temos $s > 1$,

$$\begin{aligned} a^s &= a^{(n-1)(m-1)+1} \\ &= (a^{(n-1)})^{(m-1)}.a \\ &= (a^n.a^{-1})^{(m-1)}.a \\ &= (a.a^{-1})^{(m-1)}.a \\ &= 1^{m-1}.a = a \end{aligned}$$

e analogamente, $$(2a)^s = (2a). \tag{7}$$

Por outro lado, $(2a)^s = 2^s a^s$. De fato, para $s = 2$ temos $(2a)^2 = (a+a)^2 = 4a^2$. Por hipótese de indução assuma que $(2a)^k = 2^k a^k$, para $2 < k < s$.
Assim,

$$\begin{aligned} (2a)^s &= (2a)^{s-1+1} \\ &= (2a)^{s-1}(2a) \\ &= 2^{s-1}a^{s-1}.(2a) \\ &= 2^{s-1}a^{s-1}.(a+a) \\ &= 2^{s-1}a^{s-1}.a + 2^{s-1}a^{s-1}.a \\ &= 2^{s-1}a^s + 2^{s-1}a^s \\ &= 2^{s-1}(a^s + a^s) \\ &= 2^{s-1}(2.a^s) \\ &= 2^s.a^s. \end{aligned}$$

Notemos ainda que como $a^s = a$, obtemos que $2^s.a^s = 2^s.a$ (8)
De (7) e (8) temos que $2^s a = 2a$, ou seja,

$$(2^s - 2)a = 0 \quad \text{e } s > 1.$$

Logo D possui característica maior do que zero. Como D é anel de divisão sua característica é um número primo p.
É evidente que:

- $Z(D)$ é um corpo contido em D,

- $1_D \in Z(D)$,

- $m_i.1_D \in Z(D)$, para todo $m_i \in \mathbb{Z}, 1 \leq m_i \leq p-1$.

Além disso, se $i \neq j$ temos $m_i.1_D \neq m_j.1_D$: de fato, se $m_i.1_D = m_j.1_D$ com $(m_j > m_i)$, então $(m_j - m_i)1_D = 0$. Notemos que $(m_j - m_i) < p$, contradizendo o fato de D ter característica p.
Logo $Z(D)$ contém pelo menos p elementos distintos.
Denotemos por P, o corpo que possui p elementos e que está contido em $Z(D)$ (P é isomorfo a $\mathbb{Z}_p$). Como $a^n = a$, ou seja, a é raiz do polinômio $q(x) = x^n - x \in P[x]$ (pois $1 \in P$), obtemos que a é algébrico sobre P. Assim concluímos que $P(a)$, o corpo obtido pela adjunção de a com P, é finito; e a quantidade de elementos de $P(a)$ é p^h, em que $h = dim_P P(a)$.
Além do mais, como $a \in P(a)$, temos que $a^{p^h} = a$.
Suponhamos, por absurdo, que $a \notin Z(D)$, então, pelo lema anterior, existe $b \in D$, tal que,

$$bab^{-1} \neq a. \tag{9}$$

Analogamente ao raciocínio feito para a, obtemos que $b^{p^k} = b$, para algum inteiro k.
Definimos o seguinte subconjunto de D:

$$W := \{x \in D | x = \sum_{i=0}^{p^h-1} \sum_{j=0}^{p^k-1} p_{ij} a^i b^j, p_{ij} \in P\}.$$

Notemos que $W \neq \varnothing$ pois $a, b \in W$. Além disso, W é um subconjunto finito de D e é fechado em relação a soma. Mostremos que é fechado em relação a multiplicação:
Devido ao lema 3.24, temos $ba = a^m b$. Deste modo,

$$
\begin{aligned}
b^r a^s &= \underbrace{bb...bbb}_{r\ vezes}\underbrace{aa...aa}_{s\ vezes} \\
&= bb...bb\underbrace{\mathbf{b}a}_{=a^m b}a..aa \\
&= bb...bba^m\mathbf{b}a..aa \\
&= bb...bba^m\underbrace{\mathbf{b}a}_{=a^m b}..aa \\
&= bb...bba^m a^m\mathbf{b}a..a \\
&\ \ \vdots \\
&= bb...bb\underbrace{a^m a^m..a^m}_{s\ \ vezes}\mathbf{b} \\
&= bb..b\underbrace{\mathbf{b}a^{sm}}_{=a^{msm}b}\mathbf{b} \\
&= bb..ba^{m^2 s}\mathbf{bb} \\
&= a^{m^r s}b^r \forall r, s \in \mathbb{N}.
\end{aligned}
$$

Sejam $x, y \in W$, $x = \sum_{i=0}^{p^h-1}\sum_{j=0}^{p^k-1} p_{ij}a^i b^j$, $y = \sum_{k=0}^{p^h-1}\sum_{l=0}^{p^k-1} p_{kl}a^k b^l$. Logo,

$$
\begin{aligned}
xy &= \left(\sum_{i=1}^{p^h}\sum_{j=1}^{p^k} p_{ij}a^i b^j\right)\left(\sum_{k=1}^{p^h}\sum_{l=1}^{p^k} p_{kl}a^k b^l\right) \\
&= \sum_{i=0}^{p^h-1}\sum_{j=0}^{p^k-1}\sum_{k=0}^{p^h-1}\sum_{l=0}^{p^k-1} p_{ij}a^i b^j p_{kl}a^k b^l \\
&= \sum_{i=0}^{p^h-1}\sum_{j=0}^{p^k-1}\sum_{k=0}^{p^h-1}\sum_{l=0}^{p^k-1} p_{ij}p_{kl}a^i b^j a^k b^l \\
&= \sum_{i=0}^{p^h-1}\sum_{j=0}^{p^k-1}\sum_{k=0}^{p^h-1}\sum_{l=0}^{p^k-1} p_{ij}p_{kl}a^i a^{km^j} b^j b^l \\
&= \sum_{i=0}^{p^h-1}\sum_{j=0}^{p^k-1}\sum_{k=0}^{p^h-1}\sum_{l=0}^{p^k-1} p_{ij}p_{kl}a^{km^j+i} b^{j+l}
\end{aligned}
$$

Notemos que $a^{p^h-1} = 1$, então como $km^j + i = (p^h - 1)q + i'$ em que $0 \leq i' < p^h - 1$, temos $a^{km^j+i} = a^{i'}$. Analogamente, $b^{j+l} = b^{j'}$, em que $0 \leq j' < p^k - 1$. Denotando $p_{ij}p_{kl}$ por $p'_{i'j'}$, temos:

$$xy = \sum_{i'=0}^{p^h-1} \sum_{j'=0}^{p^k-1} p'_{ij} a^{i'} b^{j'} \in W.$$

Logo W é um subanel finito de D e portanto um subanel de divisão finito de D. Assim, pelo Teorema de Wedderburn, obtemos que W é comutativo.
Como $a, b \in W$ temos que $ab = ba$, mas essa igualdade contradiz (9) que afirma que $ba \neq ab$. Deste modo, não podemos supor que $a \notin Z(D)$. Concluímos que $a \in Z(D)$ e $D \subseteq Z$. Segue que D é comutativo e portanto um corpo.

■

4 O Teorema de Frobenius

Para demonstrar o Teorema de Frobenius usaremos os seguintes resultados:

Teorema 4.1: Todo polinômio de grau n sobre o corpo dos números complexos possui todas as suas raízes no corpo dos números complexos.

A demonstração pode ser encontrada na referência [6].

Teorema 4.2: Os únicos polinômios irredutíveis sobre o corpo dos números reais são os de grau 1 ou 2.

Demonstração: Os polinômios de grau 1 são irredutíveis. Os polinômios de grau dois, $p(x) = ax^2 + bx + c$, com $b^2 - 4ac < 0$ também são irredutíveis em $\mathbb{R}[x]$. Seja $q(x)$ um polinômio de grau 3 ou mais. Pelo teorema anterior, $q(x)$ possui uma raiz $\alpha \in \mathbb{C}$. Assim, $\overline{\alpha} \in \mathbb{C}$ também é raiz e portanto $(x - \alpha)(x - \overline{\alpha})$ divide $q(x)$. Notemos que

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - 2Re(\alpha)x + |\alpha|^2 \in \mathbb{R}[x].$$

Logo $q(x)$ é redutível em $\mathbb{R}[x]$.

■

Definição 4.3: Uma álgebra de divisão D é dita algébrica sobre um campo F se:

(i) F está contido no centro de D;

(ii) Todo $a \in D$ é raiz de um polinômio não trivial com coeficientes em F.

Lema 4.4: Sejam $\mathbb{C}$ o corpo dos números complexos e D um anel de divisão que é algébrico sobre $\mathbb{C}$. Então $D = \mathbb{C}$.

Demonstração: Seja $a \in D$, então como D é algébrico sobre $\mathbb{C}$, existem números complexos $\alpha_0, \alpha_1, .., \alpha_n$, tais que,

$$\alpha_0 + \alpha_1 a + ... + \alpha_n a^n = 0,$$

ou seja, a é uma raiz do polinômio $p(x) = \alpha_0 + \alpha_1 x + ... + \alpha_n x^n \in \mathbb{C}[x]$. Pelo Teorema 4.1, $p(x)$ possui todas as suas n raízes em $\mathbb{C}$. Logo $a \in \mathbb{C}$. Segue que $D \subseteq \mathbb{C}$ e portanto $D = \mathbb{C}$.

■

Teorema de Frobenius: Seja D um anel de divisão algébrico sobre o corpo dos números reais $\mathbb{R}$, então D é isomorfo a um dos seguintes conjuntos: o corpo dos números reais, ou o corpo dos números complexos ou o anel de divisão dos quatérnios.

Demonstração: Se $D = \mathbb{R}$, não há nada a fazer. Suponhamos então que $D \neq \mathbb{R}$.
Seja $a \in D \setminus \mathbb{R}$, então, como D é algébrico sobre $\mathbb{R}$, a é raiz de um polinômio com coeficientes em $\mathbb{R}$. Como $a \notin \mathbb{R}$, obtemos que este polinômio é irredutível sobre $\mathbb{R}$, sendo portanto de grau 1 ou 2.
No entanto, se a é raiz de um polinômio de grau 1 com coeficientes em $\mathbb{R}$, digamos $p(x) = p_0 + p_1 x$, então $0 = p_0 + p_1 a$, donde concluímos que $a = -\dfrac{p_0}{p_1} \in \mathbb{R}$, e isto não pode acontecer. Assim, a é raiz de um polinômio de grau 2 com coeficientes em $\mathbb{R}$ e irredutível em $\mathbb{R}$:

$$a^2 - 2\alpha a + \beta = 0 \quad (\alpha, \beta \in \mathbb{R}).$$

De $a^2 - 2\alpha a + \beta = 0$, segue que $(a - \alpha)^2 = \alpha^2 - \beta$, em que $\alpha^2 - \beta < 0$. De fato, se $\alpha^2 - \beta \geq 0$, então $\delta := \sqrt{\alpha^2 - \beta}$ e teríamos,

$$a = \alpha \pm \delta \in \mathbb{R}.$$

Como $a \notin \mathbb{R}$, segue $\alpha^2 - \beta < 0$ e portanto podemos escrever $\alpha^2 - \beta = -\gamma^2$, em que, $\gamma \in \mathbb{R} \setminus \{0\}$.
Consequentemente $(a - \alpha)^2 = -\gamma^2$, ou seja,

$$\left(\frac{a - \alpha}{\gamma}\right)^2 = -1.$$

Portanto, a partir das hipóteses, se $a \in D \setminus \mathbb{R}$, então existem números reais α e γ, tais que,

$$\left(\frac{a - \alpha}{\gamma}\right)^2 = -1.$$

Definindo $i := \dfrac{a - \alpha}{\gamma}$, obtemos que $\mathbb{R}(i) \subset D$, ou seja, D contém um corpo isomorfo ao conjunto dos números complexos.
Agora vamos dividir a demonstração em dois casos: no primeiro caso vamos supor que D é comutativo e no segundo que D não é comutativo.

Caso 1: Supondo que D é comutativo, obtemos que $\mathbb{R}(i)$ está contido no centro de D (pois o centro é todo conjunto D). Além disso, se D é algébrico sobre $\mathbb{R}$, então todo elemento de D é raiz de um polinômio com coeficientes em $\mathbb{R} \subset \mathbb{R}(i)$, logo D também é algébrico sobre $\mathbb{R}(i)$. Assim, segue do lema anterior que, $D = \mathbb{R}(i)$, e portanto D é isomorfo ao conjunto dos números complexos.

Caso 2: Vamos supor agora que D não é comutativo. Nesse caso afirmamos que o centro de D, $Z(D)$, é exatamente o corpo dos números reais. De fato, suponha que exista $a \in Z(D) \subset D$, tal que, $a \notin \mathbb{R}$. Então existem números reais α, γ, tais que,

$$\left(\frac{a-\alpha}{\gamma}\right)^2 = -1.$$

Notemos que $\dfrac{a-\alpha}{\gamma} \in Z(D)$, e como $\left(\dfrac{a-\alpha}{\gamma}\right)^2 = -1$, obtemos que $Z(D)$ contém um corpo $\mathbb{F}$ isomorfo ao corpo dos números complexos.
Agora, se D é algébrico sobre $\mathbb{R}$, então $Z(D)$ também é. Deste modo, como $\mathbb{R} \subset \mathbb{F}$, obtemos que $Z(D)$ é algébrico sobre $\mathbb{F}$(todo elemento de $Z(D)$ é raiz de um polinômio em $\mathbb{R}[x] \subset \mathbb{F}[x]$). Portanto, pelo lema anterior, $Z(D) = \mathbb{F}$.
Por outro lado, como D é algébrico sobre $\mathbb{R}$, em particular, também é algébrico sobre $Z(D)$, pois $\mathbb{R} \subset Z(D)$. Como $Z(D) = \mathbb{F}$ ($\mathbb{F}$ isomorfo aos números complexos), concluímos, novamente pelo lema anterior, que $D = \mathbb{F} = Z(D)$, donde segue D é comutativo. Contradição. Portanto, se assumirmos que D não é comutativo, devemos ter $Z(D) = \mathbb{R}$.
Seja $a \in D$, tal que, $a \notin \mathbb{R}$. Já sabemos que existem números reais α, γ, tais que, $\dfrac{a-\alpha}{\gamma} = i$ e $i^2 = -1$. Além disso, como $i \notin \mathbb{R}$, sabemos que $i \notin Z(D)$. Logo, existe $b \in D$, de modo que, $c = bi - ib \neq 0$.
Notemos que,

$$\begin{aligned} ic + ci &= i(bi - ib) + (bi - ib)i \\ &= ibi - i^2 b + bi^2 - ibi \\ &= ibi + 2b - b - ibi = 0, \text{ pois } i^2 = -1. \end{aligned}$$

Segue que $ic = -ci$. Usando este fato temos que c^2 comuta com i. De fato,

$$\begin{aligned} ic^2 &= (ic)c \\ &= (-ci)c \\ &= -c(ic) \\ &= -c(-ci) \\ &= c^2 i. \end{aligned}$$

Como $c \in D$ e D é algébrico sobre $\mathbb{R}$, segue que c é raiz de alguma equação quadrática com coeficientes reais, digamos

$$c^2 + \lambda c + \mu = 0.$$

Como c^2 e μ comutam com i ($\mu \in \mathbb{R} = Z(D)$), afirmamos que λc também comuta com i. De fato,

$$\begin{aligned}(\lambda c)i &= (-c^2-\mu)i \\ &= -c^2 i - \mu i \\ &= -ic^2 - i\mu \\ &= i(-c^2-\mu) \\ &= i(\lambda c).\end{aligned}$$

Usando respectivamente que, $(\lambda c)i = i(\lambda c), \lambda \in R = Z(D)$ e $ic = -ci$, obtemos,

$$\lambda ci = i\lambda c = \lambda ic = -\lambda ci.$$

Concluímos que $\lambda ci = -\lambda ci$, ou seja, $\lambda ci = 0$ e assim, como $c \neq 0, i \neq 0$ e D é anel de divisão, segue que $\lambda = 0$.
Logo $c^2 = -\mu$. Como $c \notin Z(D) = \mathbb{R}$, não podemos ter $\mu < 0$, pois isto implicaria em $c \in \mathbb{R}$. Segue que $\mu = \nu^2, \nu \in \mathbb{R}$ e $c^2 = -\nu^2$.
Definimos $j := \dfrac{c}{\nu}$. Notemos que j satisfaz as seguintes relações em D:

$$j^2 = \frac{c^2}{\nu^2} = -1.$$

$$ji + ij = \frac{c}{\nu}i + i\frac{c}{\nu} = \frac{ci+ic}{\nu} = 0.$$

Definindo $k := ij$, e notando que

$$ji + ij = \frac{c}{\nu}i + i\frac{c}{\nu} = \frac{ci+ic}{\nu} = 0,$$

obtemos elementos $i, j, k \in D$ com as seguintes propriedades:

$$i^2 = j^2 = k^2 = ijk = -1$$

$$ij = -ji = k$$

$$jk = -kj = i$$

$$ki = -ik = j$$

Definimos em D o seguinte subconjunto

$$T = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k | \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}\}.$$

Notemos que

$$(a_1+b_1i+c_1j+d_1k)+(a_2+b_2i+c_2j+d_2k) = ((a_1+a_2)+(b_1+b_2)i+(c_1+c_2)j+(d_1+d_2)k) \in T$$

e a multiplicação

$$(a_1 + b_1 i + c_1 j + d_1 k).(a_2 + b_2 i + c_2 j + d_2 k) =$$

$$= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2b_1a_2 + c_1d_2 - d_1c_2)i$$
$$+(a_1c_2 + c_1a_2 + d_1b_2 - b_1.d_2)j + (a_1d_2 + d_1a_2 + b_1c_2 - c_1b_2)k \in T.$$

Além disso, dado $a + bi + cj + dk \in T$, não nulo, seu inverso multiplicativo é dado por

$$\frac{a}{m} - \frac{b}{m}i - \frac{c}{m}j - \frac{d}{m}k,$$

em que, $m = a^2 + b^2 + c^2 + d^2$.
Logo T é um subanel de divisão não comutativo contido em D. T é isomorfo aos Quatérnios.

Para finalizar mostremos que $D = T$.
Seja $r \in D$, tal que, $r^2 = -1$ e considere $C_r = \{x \in D | xr = rx\}$, o conjunto dos comutadores de r em D. Já vimos que C_r é um subanel de divisão de D. Afirmamos que os elementos da forma $\alpha_0 + \alpha_1 r$, em que, α_0, α_1 são reais, estão contidos no centro de C_r. De fato, seja $x \in C_r$ e $\alpha_0 + \alpha_1 r$, em que, α_0, α_1 são reais, então

$$\begin{aligned}(\alpha_0 + \alpha_1 r)x &= \alpha_0 x + \alpha_1 rx \\ &= \alpha_0 x + \alpha_1 xr, \quad \text{pois } x \in C_r \\ &= x\alpha_0 + x\alpha_1 r, \quad \text{pois } \mathbb{R} = Z(D) \\ &= x(\alpha_0 + \alpha_1 r).\end{aligned}$$

Além disso, se C_r é algébrico sobre $\mathbb{R}$, então também é algébrico sobre os elementos da forma $\alpha_0 + \alpha_1 r$. Assim, pelo lema anterior, $C_r = \{\alpha_0 + \alpha_1 r | \alpha_0, \alpha_1 \in \mathbb{R}\}$.
Seja $u \in D, u \notin \mathbb{R}$. Sabemos que existem $\alpha, \beta \in \mathbb{R}$ tais que $\left(\frac{u-\alpha}{\beta}\right)^2 = -1$.
Definimos $w := \frac{u-\alpha}{\beta}$, então $w^2 = -1$. Notemos que $wi + iw$ comuta com i e com w. De fato,

$$\begin{aligned}(wi + iw)i &= wi^2 + iwi \\ &= w(-1) + iwi \\ &= (-1)w + iwi \\ &= i^2 w + iwi \\ &= i(iw + wi).\end{aligned}$$

De forma análoga, mostramos que $w(wi + iw) = (wi + iw)w$, pois $w^2 = -1$. Logo, $wi + iw \in C_w$ e $wi + iw \in C_i$ e assim, pelo raciocínio feito para C_r, obtemos,

$$wi + iw = \alpha_0' + \alpha_1' i = \alpha_0 + \alpha_1 w.$$

Suponha, por contradição, que $w \notin T$. Então devemos ter $\alpha_1 = 0$ na equação acima, caso contrário teríamos

$$w = \frac{(\alpha_0' - \alpha_0)}{\alpha_1} + \frac{\alpha_1'}{\alpha_1} i \in T.$$

Portanto $wi + iw = \alpha_0$, em que, $\alpha_0 \in \mathbb{R}$. Analogamente,

$$wj + jw = \beta_0, \beta_0 \in \mathbb{R} \quad \text{e} \quad wk + kw = \gamma_0, \gamma_0 \in \mathbb{R}.$$

Definimos

$$z := w + \frac{\alpha_0}{2}i + \frac{\beta_0}{2}j + \frac{\gamma_0}{2}k, \qquad (*)$$

e notemos que:

$$\begin{aligned}
zi + iz &= (w + \frac{\alpha_0}{2}i + \frac{\beta_0}{2}j + \frac{\gamma_0}{2}k)i + i(w + \frac{\alpha_0}{2}i + \frac{\beta_0}{2}j + \frac{\gamma_0}{2}k) \\
&= wi + \frac{\alpha_0}{2}i^2 + \frac{\beta_0}{2}ji + \frac{\gamma_0}{2}ki + iw + i\frac{\alpha_0}{2}i + i\frac{\beta_0}{2}j + i\frac{\gamma_0}{2}k \\
&= wi + \frac{\alpha_0}{2}i^2 + \frac{\beta_0}{2}ji + \frac{\gamma_0}{2}ki + iw + \frac{\alpha_0}{2}i^2 + \frac{\beta_0}{2}ij + \frac{\gamma_0}{2}ik, \text{ pois } i \text{ comuta com } \alpha_0, \beta_0, \gamma_0 \\
&= \underbrace{wi + iw}_{=\alpha_0} + \underbrace{\frac{\alpha_0}{2}(i^2 + i^2)}_{=-\alpha_0} + \frac{\beta_0}{2}\underbrace{(ji + ij)}_{=0} + \frac{\gamma_0}{2}\underbrace{(ki + ik)}_{=0} \\
&= 0.
\end{aligned}$$

Analogamente $zj + jz = 0$ e $zk + kz = 0$.
Afirmação: $z = 0$.
De fato,

$$\begin{aligned}
0 &= zk + kz \\
&= zij + ijz \\
&= zij + \underbrace{(izj - izj)}_{=0} + ijz \\
&= \underbrace{(zi + iz)}_{=0}j + i(jz - zj) \\
&= i(jz - zj)
\end{aligned}$$

Vemos que $i(jz - zj) = 0$, mas $i \neq 0$ e D é anel de divisão, então $jz - zj = 0$. No entanto, $zj + jz = 0$. Logo, somando $jz - zj = 0$, membro a membro, com $zj + jz = 0$, obtemos que $2jz = 0$. Como $2j \neq 0$, concluímos que $z = 0$.
Substituindo esta informação em (*) temos:

$$w + \frac{\alpha_0}{2}i + \frac{\beta_0}{2}j + \frac{\gamma_0}{2}k = 0$$

mas isto implica que $w \in T$. Contradição com a suposição de que $w \notin T$.
Portanto $w \in T$ e como $w = \dfrac{u - \alpha}{\beta}$, temos $u = \beta w + \alpha \in T$ como queríamos mostrar.
Provamos que $D \subset T$ e como $T \subset D$ temos $D = T$. Portanto D igual a T que por sua vez é isomorfo aos quatérnios.

■

Referências

[1] AIGNER, M, ZIEGLER, G. M. **As provas estão n'o Livro**. São Paulo:Edgard Blücher, 2002. 216p.

[2] HERSTEIN, I. N. **Álgebra abstracta**. México: Grupo editorial Iberoamericana, 1988. 249p.

[3] HERSTEIN, I. N. **Álgebra moderna**: Grupos, anillos, campos, teoría Galois. 5nd ed. México: Trillas: Centro Regional de Ayuda Tecnica, 1980. 393p.

[4] HUNGERFORD, T. W. **Algebra**. Springer-Verlag New York Inc., Cleveland, 1996. 502p.

[5] LAM, T. Y. **A first course in noncommutative rings**. 2nd ed. New York: Springer, 2001. 385p.

[6] MONTEIRO, L. H. J. **Elementos de álgebra**. Rio de Janeiro (RJ): Ao Livro Técnico, 1969. xvi, 552p.