

1 Quocientes de Espaços Vetoriais

Sejam V um K -espaço vetorial e $U \leq V$ um subespaço.

def (Relação de Congruência Módulo U). A relação \sim em V é definida por

$$\mathbf{v} \sim \mathbf{v}' \stackrel{DEF}{\iff} \mathbf{v} - \mathbf{v}' \in U.$$

É chamada de congruência módulo U . Também denotamos $v \sim v'$ por $\mathbf{v} \equiv \mathbf{v}' \pmod{U}$.

def (Classe Residual(ou de Equivalência)). Denotamos por \mathbf{V}/U o conjunto das classes módulo U . A classe de $v \in V$ em V/U é denotada por $\bar{\mathbf{v}}$, $\mathbf{v} \pmod{U}$ ou $\mathbf{v} + U$. Além disso,

$$\begin{aligned} \bar{\mathbf{v}} &= \{v' \in V : v' \equiv v \pmod{U}\} \\ &= v + U \stackrel{DEF}{=} \{v + u : u \in U\}. \end{aligned}$$

2 Teoria de Anéis

def (Anel). Um conjunto não vazio R com $+$ e \cdot é um **anel** $(R, +, \cdot)$ se:

- (i) $(R, +)$ é grupo abeliano (neutro 0);
- (ii) a multiplicação é associativa;
- (iii) a multiplicação é distributiva em relação à adição (e vice-versa).

def (Anel Comutativo). Se o produto é comutativo, $(R, +, \cdot)$ é **anel comutativo**.

def (Anel com 1). Se existe $1 \in R$ com $1 \neq 0$ tal que $a \cdot 1 = 1 \cdot a = a$ para todo $a \in R$, então R é **anel com 1**.

def (Divisor de Zero). Um $a \in R$ é **divisor de zero à esquerda** se $\mathbf{a} \cdot \mathbf{b} = \mathbf{0}$ para algum $b \neq 0$ (analogamente, à direita se $b \cdot a = 0$).

def (Operações no Espaço Quociente). Em V/U definimos

$$\bar{\mathbf{v}} \oplus \bar{\mathbf{w}} \stackrel{DEF}{=} \overline{\mathbf{v} + \mathbf{w}}, \quad \alpha \odot \bar{\mathbf{v}} \stackrel{DEF}{=} \overline{\alpha \cdot \mathbf{v}}.$$

def (Espaço Quociente). O K -espaço vetorial $(\mathbf{V}/U, \oplus, \odot)$ é chamado de **Espaço Quociente de V por U** .

def (Mapa Quociente (Projeção Canônica)). O mapa $\pi : \mathbf{V} \rightarrow \mathbf{V}/U$ dado por $\pi(v) = \bar{v}$ é o **mapa quociente** (projeção canônica).

Teorema (Propri. Universal do Quociente). Se $T : V \rightarrow W$ é K -linear e $U \leq \text{Ker}(T)$, então **existe um único** K -linear $\bar{T} : V/U \rightarrow W$ tal que $T = \bar{T} \circ \pi$, onde $\pi : V \rightarrow V/U$ é a projeção canônica.

def (Domínio). Um anel comutativo com 1 é **domínio** se não possui divisores de zero.

def (Unidade). Em anel com 1, $a \in R \setminus \{0\}$ é **unidade** se existe (único) $a^{-1} \in R \setminus \{0\}$ com $aa^{-1} = 1 = a^{-1}a$. O conjunto das unidades é \mathbf{R}^\times .

def (Corpo). Um domínio $(R, +, \cdot)$ é **corpo** se todo $a \in R^\times = R \setminus \{0\}$ é unidade.

def (Anel de Divisão). Um anel com 1 é **anel de divisão** se todo $a \in R \setminus \{0\}$ é unidade.

def (Centro do Anel).

$$\mathbf{Z}(\mathbf{R}) \stackrel{DEF}{=} \{\mathbf{y} \in \mathbf{R} : \mathbf{y}\mathbf{x} = \mathbf{x}\mathbf{y}, \forall \mathbf{x} \in \mathbf{R}\}$$

é um anel comutativo chamado **centro de R** .

Teorema (Isomorfismo). Se $T : V \rightarrow W$ é K -linear e sobrejetor, então $\mathbf{V}/\text{Ker}(\mathbf{T}) \simeq \mathbf{W}$. Em geral, $\mathbf{V}/\text{Ker}(\mathbf{T}) \simeq \mathfrak{I}(\mathbf{T})$.

Teorema (Dimensão para Quocientes). Se V tem dimensão finita e $U \leq V$, então

$$\dim_{\mathbf{K}}(\mathbf{V}/U) = \dim_{\mathbf{K}}(\mathbf{V}) - \dim_{\mathbf{K}}(U).$$

cor (Teorema do Núcleo e da Imagem). Se $T : V \rightarrow W$ é K -linear e $\dim_K(V) < \infty$, então

$$\dim_{\mathbf{K}}(\mathbf{V}) - \dim_{\mathbf{K}}(\text{Ker}(\mathbf{T})) = \dim_{\mathbf{K}}(\mathfrak{I}(\mathbf{T})).$$

def (Polinômio Ciclotômico). Se $U_\infty = \{z \in \mathbb{C} : z^n = 1 \text{ para algum } n \geq 1\}$, o d -ésimo **polinômio ciclotômico** é

$$\phi_d(\mathbf{T}) \stackrel{DEF}{=} \prod_{\lambda \in U_\infty, \text{o}(\lambda)=d} (\mathbf{T} - \lambda).$$

prop (Domínio Finito é Corpo). Se $(R, +, \cdot)$ é **domínio finito**, então R é **corpo**.

Teorema (Wedderburn). Se $(R, +, \cdot)$ é **anel de divisão finito**, então R é **corpo**.

prop (Critério da Deri. para Separabilidade). Se um polinômio não possui raízes em comum com sua derivada, então ele não possui raízes repetidas.

prop (Fatoração de $T^n - 1$). Para qualquer $n \geq 1$, $\mathbf{T}^n - 1 = \prod_{d|n} \phi_d(\mathbf{T})$.

3 Subanéis e Morfismos

def (Subanel). Um subconjunto $\emptyset \neq S \subseteq R$ é **subanel** de R se (i) S é anel com as operações induzidas; (ii) se R possui 1_R , então $1_R \in S$.

def (Morfismo (Homomorfismo) de Anéis). Um mapa $f : R \rightarrow S$ é **morfismo** de anéis se $f(a + b) = f(a) + f(b)$, $f(a \cdot b) = f(a) \cdot f(b)$ e, se há unidades, $f(1_R) = 1_S$.

def (Endomorfismo). Se f for morfismo e $f : R \rightarrow R$ então f é **endomorfismo**.

4 Ideais

def (Ideal à Esquerda / à Direita). Um $\emptyset \neq I \subseteq R$ é **ideal à esquerda** (resp. à direita) se

$$\alpha x + \beta y \in I \quad (\text{resp. } x\alpha + y\beta \in I)$$

para quaisquer $x, y \in I$ e $\alpha, \beta \in R$.

def (Ideal). Se I é ideal à esquerda e à direita, dizemos **ideal de R** . Em anel comutativo com 1, escrevemos $I \triangleleft R$; se $I \subsetneq R$, é **ideal próprio**.

def (Ideal Principal). Em anel comutativo com 1, $I \triangleleft R$ é **principal** se $\exists x \in R$ tal que $I = (x)$.

def (Ideal Gerado por S). Para $S \subseteq R$,

$$\langle S \rangle \stackrel{DEF}{=} \bigcap_{S \subseteq I \triangleleft R} I.$$

Se $S = \{s_1, \dots, s_N\}$, escrevemos (s_1, \dots, s_N) .

def (Isomorfismo). Se f for morfismo e a inversa é morfismo então f é isomorfismo.

def (Automorfismo). Se f for isomorfismo e endomorfismo então f é Automorfismo.

def (Monomorfismo). Se f for morfismo injetor então é monomorfismo.

def (Núcleo de um Morfismo).

$$\text{Ker}(f) \stackrel{DEF}{=} \{r \in R : f(r) = 0_S\} = f^{-1}(0_S).$$

def (Soma e Produto de Ideais). Se $I, J \triangleleft R$, definimos $I + J = \langle I \cup J \rangle$ e

$$I \cdot J \stackrel{DEF}{=} \langle \{a \cdot b : a \in I, b \in J\} \rangle.$$

def (Ideais Coprimos). Se $I, J \triangleleft R$ e $I + J = R = (1)$, dizemos que I e J são **coprimos**.

def (Ideal Primo e Maximal). Em anel comutativo com 1, ideal próprio I é **primo** se $ab \in I \Rightarrow a \in I$ ou $b \in I$ (notações: $I \triangleleft_p R$, $I \in \text{Spec}(R)$); é **maximal** se é maximal por inclusão entre ideais próprios (notações: $I \triangleleft_m R$, $I \in \text{Specm}(R)$).

prop (Ideais de \mathbb{Z}). Se $I \triangleleft \mathbb{Z}$, então $I = (n)$ para algum $n \geq 0$.

Lema (Lema de Zorn). Se (X, \leq) é um POSET não vazio e toda cadeia tem cota superior, então X possui elemento maximal.

prop (Caracterização de Subanel). Um $\emptyset \neq S \subseteq R$ é subanel de $R \iff$ para quaisquer $a, b \in S$, $a - b \in S$ e $a \cdot b \in S$; e, se R tem 1, então $1 \in S$.

prop (Morfismo Bijetor é Isomorfismo). Se $f : R \rightarrow S$ é morfismo, então f é bijetor $\iff f$ é isomorfismo.

prop (Imagem de anel é subanel). Se $f : R \rightarrow S$ é morfismo, então $f(R)$ é subanel de S .

Teorema (Existência de Ideal Maximal). Se R é comutativo com 1 ($\neq 0$), então R possui um ideal maximal.

Teorema (Ideal Próprio \subseteq Ideal Maximo). Se $I \triangleleft R$ é próprio (com R comutativo com 1, $\neq 0$), então existe ideal maximal m com $I \subseteq m$.

prop (Forma Explícita do Ideal Gerado). Para $S \subseteq R$ (anel comutativo com 1),

$$\langle S \rangle = \left\{ \sum_{i=1}^k r_i s_i : r_i \in R, s_i \in S, k \in \mathbb{Z}_{\geq 1} \right\}.$$

prop. Se $I \triangleleft R$ é maximal, então I é primo.

5 Quocientes de Anéis por Ideais

Seja R um anel comutativo com $1 (\neq 0)$ e $I \triangleleft R$.

def (Anel Quociente). O anel $\mathbf{R/I}$ é o **quociente de R por I** (anel das classes residuais de R módulo I).

def (Mapa Quociente (Anéis)). O morfismo $\pi : \mathbf{R} \rightarrow \mathbf{R/I}$ dado por $\pi(x) = \bar{x}$ é o **mapa quociente**.

Teorema (Propri. Universal do Quociente). Se $f : R \rightarrow S$ é morfismo de anéis e $I \subseteq \text{Ker}(f)$, então **existe único** $\bar{f} : R/I \rightarrow S$ tal que $\bar{f} \circ \pi = f$.

cor (Teorema do Isomorfismo). Para $f : R \rightarrow S$, vale $\mathbf{R/ Ker(f)} \simeq \mathfrak{S}(f)$.

6 Corpos de Ideais Principais

def (Domínio Euclidiano). Um domínio Euclidiano é um domínio integral R munido de uma função $\delta : R \setminus \{0\} \rightarrow \mathbb{N}$ (chamada de função euclidiana) tal que, para quaisquer $a, b \in R$ com $b \neq 0$, existem $q, r \in R$ satisfazendo

$$a = bq + r \quad \text{com} \quad r = 0 \text{ ou } \delta(r) < \delta(b).$$

def (Reticulado(Lattice)). Um reticulado é um conjunto parcialmente ordenado (L, \leq) no qual

prop (Caracterização de Id Primos e Max).

Se $I \triangleleft R$ é próprio, então

(a) I é primo $\iff R/I$ é domínio;

(b) I é maximal $\iff R/I$ é corpo.

cor. Todo ideal maximal é primo.

Teorema (Correspondência). Existe bijeção entre ideais de R/I e ideais de R que contêm I , preservando inclusões, dada por $J \mapsto \pi(J)$.

Teorema (Relação de Quocientes). Se $J \triangleleft R$ com $J \supset I$, então

$$\mathbf{R/J} \simeq (\mathbf{R/I})/(\mathbf{J/I}),$$

quaisquer dois elementos $x, y \in L$ possuem um mínimo superior (ou supremo) denotado por $x \vee y$, e um máximo inferior (ou ínfimo) denotado por $x \wedge y$.

def (Corpo de frações). Seja A um domínio integral(sem divisor por 0). O corpo de frações de A é um corpo $\text{Frac}(A)$ juntamente com um monomorfismo $i : A \rightarrow K$ tal que cada elemento de K pode ser escrito como uma fração

$$\frac{a}{b}, \quad \text{com } a, b \in A \text{ e } b \neq 0,$$

onde $J/I = \pi(J)$ é ideal de R/I .

Teorema (Chinês dos Restos). Se I_1, \dots, I_n são ideais próprios de R dois a dois coprimos ($I_i + I_j = R$, $i \neq j$), então

$$\mathbf{I_1} \cdot \dots \cdot \mathbf{I_n} = \bigcap_{k=1}^n \mathbf{I_k},$$

$$\mathbf{R/(\bigcap_{k=1}^n I_k)} \simeq \mathbf{R/I_1} \times \dots \times \mathbf{R/I_n}.$$

e todo elemento de K é da forma $i(a)i(b)^{-1}$. Equivalentemente, K é o menor corpo que contém A .

prop (Euclidiano implica D.I.P). Todo domínio Euclidiano é domínio de ideais principais, i.e. todos ideais são gerados por um elemento.

prop (Isomorfismo com Corpo de Frações). Se K é um corpo, então $\text{Frac}(K) \cong K$