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*

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

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

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

$$\overline{v} = \{v' \in V : v' \equiv v \pmod{U}\}$$

$$= v + U \overset{DEF}{=} \{v + u : u \in U\}.$$

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

$$\overline{\mathbf{v}} \oplus \overline{\mathbf{w}} \overset{DEF}{=} \overline{\mathbf{v} + \mathbf{w}}, \qquad \alpha \odot \overline{\mathbf{v}} \overset{DEF}{=} \overline{\alpha \cdot \mathbf{v}}.$$

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

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

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

Teorema (**Isomorfismo**). *Se $T : V \to W$ é K-linear e sobrejetor, então $\mathbf{V}/\mathrm{Ker}(\mathbf{T}) \simeq \mathbf{W}$. Em geral, $\mathbf{V}/\mathrm{Ker}(\mathbf{T}) \simeq \Im(\mathbf{T})$.*

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

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

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

$$\dim_{\mathbf{K}}(\mathbf{V}) - \dim_{\mathbf{K}}(\mathrm{Ker}(\mathbf{T})) = \dim_{\mathbf{K}}(\Im(\mathbf{T})).$$

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

def (**Unidade $R^\times$**). *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**).

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

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

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

$$\phi_{\mathbf{d}}(\mathbf{T}) \overset{DEF}{=} \prod_{\lambda \in \mathbf{U}_\infty, \ \mathrm{o}(\lambda) = \mathbf{d}} (\mathbf{T} - \lambda).$$

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 $n \geq 1$, $\mathbf{T^n - 1} = \prod_{\mathbf{d}|\mathbf{n}} \phi_{\mathbf{d}}(\mathbf{T})$.*

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 $f : R \to S$ 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 $f : R \to R$ então f é **endomorfismo**.*

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**).

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

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

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

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

4 Ideais

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

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

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 $\mathbf{I} \triangleleft \mathbf{R}$; 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 $S \subseteq R$,*

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

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

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

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

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

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

prop (**Ideais de $\mathbb{Z}$**). *Se $I \triangleleft \mathbb{Z}$, então $\mathbf{I = (n)}$ 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.*

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),*

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

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* $\pi : \mathbf{R} \to \mathbf{R/I}$ *dado por* $\pi(x) = \overline{x}$ *é o* ***mapa quociente****.*

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

cor (**Teorema do Isomorfismo**). *Para* $f : R \to S$*, vale* $\mathbf{R}/\operatorname{Ker}(\mathbf{f}) \simeq \Im(\mathbf{f})$*.*

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*

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

onde $J/I = \pi(J)$ *é ideal de* R/I*.*

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

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

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

6 Domínios de Ideais Principais

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

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

def (**Reticulado(Lattice)**). . *Um* reticulado *é um conjunto parcialmente ordenado* $(L, \leq)$ *no qual 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). O* corpo de frações *de* A *é um corpo* $Frac(A)$ *juntamente com um monomorfismo* $i : A \to K$ *tal que cada elemento de* K *pode ser escrito como uma fração*

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

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 Fracões**). *Se* K *é um corpo, então* $Frac(K) \cong K$

def (**Associado**). a, b *são* associados *se existe* $u \in D^{\times}$*, tal que:* $a = bu$*.*

def (**Irredutível**). π *é Irredutível se* $\pi = ab \implies a$ *é* associado *ou* b *é* associado a π*.*

def (**Primo**). $\pi | ab \implies \pi | a$ *ou* $\pi | b$

Lema (**Primo implica irredutivel**). *Sejam* D *um domínio e* $\pi \in D$*. Se* π *é primo então* π *é irredutivel.*