

Algebra II

Paolo Bettelini

Contents

1	Teoremi di isomorfismo su quozienti di spazi vettoriali	1
2	Anelli	4
3	Esempi di quozienti	5
3.1	Quozienti di polinomi	5

1 Teoremi di isomorfismo su quozienti di spazi vettoriali

Let V be a vector space over \mathbb{K} and W be a linear subspace of V .

We have a map

$$\pi: V \rightarrow V/W$$

defined as

$$\pi(v) \triangleq v + W \in V/W$$

which is a linear map.

Indeed,

1.

$$\pi(0_V) = 0_V + W = w + W$$

2.

$$\begin{aligned}\pi(v_1 + v_2) &= \pi(v_1) + \pi(v_2) \\ (v_1 + v_2) + W &= (v_1 + W) + (v_2 + W)\end{aligned}$$

3.

$$\pi(\lambda v) = (\lambda v) + W = \lambda(v + W)$$

We now consider a morphism $\varphi: V_1 \rightarrow V_2$ between vector spaces. We know that its kernel is a subspace of V_1 . We now construct a new morphism

$$\bar{\varphi}: V_1/\ker_{\varphi} \rightarrow V_2$$

such that

$$\bar{\varphi}(v + \ker_{\varphi}) \triangleq \varphi(v)$$

We need to ensure that such mapping is well-defined. Let $v' \in v + \ker_{\varphi}$, meaning that $v' = v + w$ with $w \in \ker_{\varphi}$.

$$\begin{aligned}\bar{\varphi}(v' + \ker_{\varphi}) &= \varphi(v') = \varphi(v + w) = \varphi(v) + \varphi(w) \\ &= \varphi(v) = \bar{\varphi}(v + \ker_{\varphi})\end{aligned}$$

We now show that it is also linear:

1.

$$\overline{\varphi}(0_{V_1} + \ker \varphi) = \varphi(0_{V_1}) = 0_{V_2}$$

2.

$$\begin{aligned}\overline{\varphi}((v_1 + \ker \varphi) + (v_2 + \ker \varphi)) &= \overline{\varphi}((v_1 + v_2) + \ker \varphi) \\ &= \varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2) \\ &= \overline{\varphi}(v_1 + \ker \varphi) + \overline{\varphi}(v_2 + \ker \varphi)\end{aligned}$$

3.

$$\overline{\varphi}(\lambda(v + \ker \varphi)) = \lambda(\overline{\varphi}(v + \ker \varphi))$$

Il seguente diagramma commuta e π è suriettiva in quanto $v + \ker \varphi = \pi(v)$.

$$\begin{array}{ccc} V_1 & \xrightarrow{\varphi} & V_2 \\ \pi \downarrow & & \nearrow \overline{\varphi} \\ V_1/\ker \varphi & & \end{array}$$

Quindi $\varphi = \overline{\varphi} \circ \pi$.

Teorema First isomorphism theorem

Let $\varphi: V_1 \rightarrow V_2$ be a morphism between vector spaces.

$$\overline{\varphi}: V_1/\ker \varphi \rightarrow \text{im}_\varphi$$

is an isomorphism of vector spaces, meaning

$$V_1/\ker \varphi \cong \text{im}_\varphi$$

Proof First isomorphism theorem

We need to show that the morphism is both surjective and injective:

1. let $v_2 \in \text{im}_\varphi$. We want to find a $v_1 \in V_1$ such that $v_2 = \varphi(v_1)$. This is precisely

$$\overline{\varphi}(v_1 + \ker \varphi)$$

2. we want to show that the kernel is trivial.

$$\begin{aligned}\ker \overline{\varphi} &= \{v + \ker \varphi \mid \overline{\varphi}(v + \ker \varphi) = 0_{V_2}\} \\ &= \{v + \ker \varphi \mid v \in \ker \varphi\} \\ &= 0_{V_1} + \ker \varphi\end{aligned}$$

since $v + \ker \varphi = \ker \varphi$ and we can just choose 0_{V_1} .

Esempio

Consider a vector space $V = W_1 \oplus W_2$ with $W_1, W_2 \leq V$ and consider the mappings

$$p_1: V \rightarrow W_1, \quad p_2: V \rightarrow W_2$$

Using the diagrams with $\overline{p_1}, \pi_1$ and $\overline{p_2}, \pi_2$, we have

$$W_1 \cong V/W_2, \quad W_2 \cong V/W_1$$

since $W_2 = \ker_{p_1}$ and $W_1 = \ker_{p_2}$.

Teorema Second isomorphism theorem

Let V be a vector space over \mathbb{K} and $U, W \leq V$. Then,

$$\frac{W}{W \cap U} \cong \frac{W + U}{U}$$

Proof Second isomorphism theorem

We apply the first isomorphism theorem. Construct a surjective mapping

$$\varphi: \frac{W}{W \cap U} \rightarrow W + U$$

such that $\ker \varphi = U$. We first note that

$$\frac{W}{W \cap U} \leq V/U$$

and so we define

$$\varphi(w) \triangleq w + U \in V/U$$

We need to show that it is linear (todo). It is surjective as

$$\text{Im} \varphi = \frac{W + U}{U}$$

since $w + u + U = w + U = \varphi(w)$. We now need to study that it is injective

$$\begin{aligned} \ker \varphi &= \{w \in W \mid w + U = 0_{V/U} = 0_V + U\} \\ &= \{w \in W \mid w \in U\} = W \cap U \end{aligned}$$

since $w + U = 0_V + U$ means that $w \in U$.

Notiamo che U potrebbe non essere sottospazio di W quindi non possiamo rimpiazzare $W + U$ con W/U .

Teorema Third isomorphism theorem

Sia V uno spazio vettoriale e $W \leq V$ e $U \leq W$ dei sottospazi. Consideriamo V/U e $W/U \leq V/U$. e possiamo fare

$$\frac{V/U}{W/U} \cong V/W$$

Proof Third isomorphism theorem

Costruiamo un morfismo (suriettivo) $\bar{\varphi} = V/U \rightarrow V/W$ tale che $\ker \bar{\varphi} = W/U$. Applicando il primo teorema di isomorfismo otteniamo

$$\frac{V/U}{\ker \bar{\varphi}} \cong \text{Im} \bar{\varphi} = V/W$$

Definiamo $\bar{\varphi}(v + U) = v + W$. Mostriamo che è ben definito: dato $v' \in v + U$ diverso da v , e quindi $v' = v + u$ con $u \in U$ vale

$$\bar{\varphi}(v' + U) = v' + W = (v + u) + W = v + W = \bar{\varphi}(v + U)$$

siccome $u \in W$. Mostriamo ora che è lineare

1.

$$\bar{\varphi}((v_1 + U) + (v_2 + U)) = \bar{\varphi}((v_1 + v_2) + U) = (v_1 + v_2) + W$$

Per la suriettività basta prendere un qualsiasi elemento del quoziente $v + W \in V/W$ arbitrario, $v + W = \overline{\varphi}(v + U)$ e quindi $v + W \in \text{Im } \overline{\varphi}$. Per l'iniettività

$$\begin{aligned}\ker \overline{\varphi} &= \{v + U \in U/V \mid v + W = \overline{\varphi}(v + U) = 0_{V/W} = 0_V + W\} \\ &= \{v + U \in V/U \mid v \in W\} = W/U\end{aligned}$$

2 Anelli

$(Z, +, \cdot)$ è un anello commutativo dove gli elementi invertibili sono solo ± 1 .

$(\mathbb{K}[x], +, \cdot)$ è un anello commutativo dove gli elementi invertibili sono solo i polinomi di grado zero.

Algebra grupale: Sia G un gruppo e sia \mathbb{K} un campo.

$$G[\mathbb{K}] = \left\{ \sum_{g \in G} \lambda g \mid \lambda \in \mathbb{K} \right\}$$

(Giusto?) La addizione è data da.

$$\left(\sum_{g \in G} \lambda_g \cdot g \right) + \left(\sum_{h \in G} \lambda_h \cdot h \right) = \sum_{g, h \in G} (\lambda_g + \lambda_h)(gh)$$

La moltiplicazione è data da

$$\begin{aligned}\left(\sum_{g \in G} \lambda_g \cdot g \right) \cdot \left(\sum_{h \in G} \lambda_h \cdot h \right) &= \sum_{g, h \in G} (\lambda_g \cdot \lambda_h)(gh) \\ &= \sum_{k \in G} \left(\sum_{g \cdot h = k} (\lambda_g \lambda_h) \right) \cdot k\end{aligned}$$

L'elemento neutro è dato da

$$0 = \sum_{g \in G} 0 \cdot g$$

e l'identità

$$1 = 1 \cdot 1_G + \sum_{g \in G} 0 \cdot g$$

Esempio I quaternioni sono una algebra reale

$$\mathbb{H} = \text{span}\{e, i, j, k\}$$

Abbiamo che

$$Z(\mathbb{H}) = \text{span}\{e\} \cong \mathbb{R}$$

Vale $A_1, A_2, A_3 \leq \mathbb{H}$ con

$$A_1 = \text{span}\{e, i\},$$

$$A_2 = \text{span}\{e, j\},$$

$$A_3 = \text{span}\{e, k\},$$

Sono autocentralizzanti e sono isomorfi ai complessi come algebra reale.

3 Esempi di quozienti

Le classi di resto sono un anelli. Sia $A = \mathbb{Z}$ e $I = (n) = \{n \cdot k \mid k \in \mathbb{Z}\}$. Abbiamo quindi il quoziente $\mathbb{Z}/(n)$ che è dato da

$$a + I = a + (n) = [a]_n$$

Chiaramente $1_{\mathbb{Z}/(n)} = [1]_n$. Questo quoziente non è un dominio di integrità se n non è un numero primo. Se non è primo allora esistono interi a, b tali che $a, b \neq \pm 1$ tale che $n = ab$. Allora

$$[a]_n \cdot [b]_n = [ab]_n = [n]_n = [0]_n$$

Se n è primo allora \mathbb{Z}/p è addirittura un campo. Infatti se $[a]_p \neq [0]_p$ prendiamo $0 < a < p$ con a, p coprimi fra loro. Allora esistono $k_1, k_2 \in \mathbb{Z}$ tale che $ak_1 + pk_2 = 1$ quindi $a_1 = 1 + (-k_2)p$. Da ciò otteniamo che

$$\begin{aligned} [ak_1]_p &= ak_1 + (p) = (1 + (-k_2)p) + (p) = 1 + (p) = [1]_p \\ \implies [k_1]_p &= [a]_p^{-1} \end{aligned}$$

3.1 Quozienti di polinomi

Sia $f = x^2 - 3x + 2 = (x - 2)(x - 1)$. Consideriamo $\mathbb{Q}[x]/(f)$. Due laterali sono per esempio $(x - 2) + (f)$ e $(x - 1) + (f)$ che non sono lo zero. Invece il loro prodotto

$$((x - 2) + (f)) \cdot ((x - 1) + (f)) = f + (f) = 0 + (f)$$

che è lo zero, quindi i due termini sono divisori di zero. Consideriamo $x^3 - 1 = (x - 1)(x^2 + x + 1)$. Anche in questo caso

$$((x - 2) + (f)) \cdot ((x^3 - 1) + (f)) = f \cdot (x^2 + x + 1) + (f) = 0 + (f)$$

Dalla definizione di f abbiamo $x^2 = f + (3x - 2)$

$$\begin{aligned} x^3 &= x \cdot (f + (3x - 2)) \\ &= x \cdot f + 3f + 9x - 6 - 2x \\ &= f(x + 3) + 7x - 6 \end{aligned}$$

Da questo otteniamo che

$$\begin{aligned} (x^3 - 1) + (f) &= 7x - 6 - 1 + (f) \\ &= 7x - 7 + (f) \\ &= 7(x + 1) + (f) \end{aligned}$$

che è un suo rappresentante di un grado minore.