Algebra II

Paolo Bettelini

Contents

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

$$\pi\colon V \to V/W$$

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

$$\overline{\varphi}\colon V_1/\ker_\varphi \to V_2$$

such that

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

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

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

We now show that it is also linear:

1. $$\overline{\varphi}(0_{V_1} + \ker_\varphi) = \varphi(0_{V_1}) = 0_{V_2}$$

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

3. $$\overline{\varphi}(\lambda(v + \ker_\varphi)) = \lambda\left(\overline{\varphi}(v + \ker_\varphi)\right)$$

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

$$\begin{tikzcd} V_1 \arrow[r, "\varphi"] \arrow[d, two heads, "\pi"'] & V_2 \\ V_1/\ker_\varphi \arrow[ur, bend right, "\overline{\varphi}"'] & \end{tikzcd}$$

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

Teorema First isomorphism theorem

Let $\varphi \colon V_1 \to V_2$ be a morphism between vector spaces.

$$\overline{\varphi} \colon V_1/\ker_\varphi \to \mathrm{im}_\varphi$$

is an isomorphism of vector spaces, meaning

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

Proof First isomorphism theorem

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

1. let $v_2 \in \mathrm{im}_\varphi$. 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.

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

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

$$p_1 \colon V \to W_1, \quad p_2 \colon V \to W_2$$

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 isomoprhism theorem. Construct a surjective mapping

$$\varphi \colon \frac{W}{W \cap U} \to W + U$$

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

$$\mathrm{Im}_\varphi = \frac{W+U}{U}$$

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 isomoprhism 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 isomoprhism theorem

Costruiamo un morphismo (suriettivo) $\overline{\varphi} = V/U \to V/W$ tale che $\ker_{\overline{\varphi}} = W/U$. Applicando il primo teorema di isomormorfismo otteniamo

$$\frac{V/U}{\ker_{\overline{\varphi}}} \cong \mathrm{Im}_{\overline{\varphi}} = V/W$$

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

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

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

1. $$\overline{\varphi}((v_1 + U) + (v_2 + U)) = \overline{\varphi}((v_1 + v_2) + U) = (v_1 + v_2) + W$$

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

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

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 gruppale: 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

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

Abbiamo che

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

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

$$\begin{aligned}A_1 &= \mathrm{span}\{e, i\}, \\ A_2 &= \mathrm{span}\{e, j\}, \\ A_3 &= \mathrm{span}\{e, k\},\end{aligned}$$

Sono autocentralizzanti e sono isomorfi ai complessi come algebra reale.

3 Esempi di quozienti

Le class 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 numro 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

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

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.

4 21/10/2025

Recuperare lezione dell'anno scorso.

Teorema Teorema cinese del resto

Let A be a commutative ring, $I_1, \cdots, I_r$ coprime ideals. The homomorphism

$$\varphi \colon A \to \bigoplus_{i=1}^{r} A/I_i$$

dato da $\varphi = (\pi_1, \cdots, \pi_r)$ le proiezioni $\pi_i \colon A \to A/I_r$. The kernel

$$\ker(\varphi) = \bigcap_{i=1}^{r} I_i = \prod_{i=1}^{r} I_r$$

is surjective. Thus, by the first isomorphism theorem

$$A/\bigcap_{i=1}^{r} I_i \cong \bigoplus_{i=1}^{r} A/I_i$$

Proof

We show that the kernel is

$$\begin{aligned}
\ker(\varphi) &= \{a \in A \,|\, \varphi(a) = 0_{\oplus A/I_i} = (0_{A/I_1}, \cdots, 0_{A/I_r})\} \\
&= \{a \in A \,|\, \varphi(a) = (0_A + I_1, \cdots, 0_A + I_r)\} \\
&= \{a \in A \,|\, a \in I_1, I_2, \cdots, I_2\} \\
&= \bigcap_{i=1}^{r} I_i = \prod_{i=1}^{r} I_i
\end{aligned}$$

We now show that it is surjective. We need to show that $\forall i$, there exists $a_i \in A$ such that

$$\varphi(a_i) = (0_A + I_1, \cdots, 1_A + I_i, \cdots, 0_A + I_r)$$

Furthermore, $\pi_i \colon A \to A/I_i$ is surjective which means that $\forall b + I_i \in A/I_i$.

$$\begin{aligned}
\pi_i(b) = b + I_i \implies & (0_A + I_1, \cdots, b + I_i, \cdots, 0_A + I_r) \\
&= \varphi(b) \cdot \varphi(a_i) = (x_1, \cdots, b + I_i, \cdots, *) \cdot (0_{A/I_i}, \cdots, 1 + I_i, \cdots, 0_{A/I_r}) \\
&= \varphi(b \cdot a_i)
\end{aligned}$$

We can thuse create every element by composing 0's.
Note that I_i and $\bigcap_{i \neq j} I_j$ are coprimi, meaning $\exists x_i \in I_i$ and $y_i \in \bigcap_{i \neq j} I_j$ such that $x_i + y_i = 1_A$. Thus

$$\begin{aligned}
\varphi(y_i) &= (\pi_1(y_i), \cdots, \pi_i(y_i), \cdots, \pi_r(y_i)) \\
&= (y_i + I_1, \cdots, y_i + I_i, \cdots, y_i + I_r) \\
&= (0_A + I_1, \cdots, (1_A - x_i) + I_i, \cdots, 0_A + I_r) \\
&= (0_{A/I_1}, \cdots, 1_{A/I}, \cdots, 0_{A/I_r})
\end{aligned}$$

e quindi $a_i = y_i$. Quindi un generico elemento della somma diretta pu?o essere scritto come immagine di questo.