Strutture algebriche - qualche definizione

Dato un insieme non vuoto X, un'operazione su X è una applicazione $* : X \times X \to X$.

$(X, *)$ è un **gruppo** se l'operazione è:

associativa

Per ogni $a, b, c \in X$, $a * (b * c) = (a * b) * c$

ammette un (necessariamente unico) *elemento neutro* u, cioè tale che, per ogni $x \in X$,

$u * x = x * u = x$;

per ogni $x \in X$ esiste un (necessariamente unico) *inverso* y, cioè tale che

$x * y = y * x = u$.

Ad esempio $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}/m\mathbb{Z}, +)$, $(S(X), \circ)$ sono gruppi.

Se l'operazione è anche commutativa,

$a * b = b * a$, per ogni $a, b \in X$

allora si dice che si tratta di un *gruppo commutativo* o, equivalentemente, *abeliano*.

Se X ha almeno tre elementi distinti, allora $(S(X), \circ)$ **non** è abeliano. $(\mathbb{N}, +)$ e $(\mathbb{Z}^*, \cdot)$ non sono gruppi.

Genericamente per una operazione si usa la *notazione moltiplicativa*, $x * y = xy$, $u = 1$, x^{-1} per indicare l'inverso di x. Facendo questo si sottintende che può non essere commutativa. Se è commutativa e vogliamo sottolineare questo fatto, si usa la *notazione additiva*, $x * y = x + y$, $u = 0$, $-x$ per l'inverso.

Consideriamo un insieme munito di due operazioni $(A, +, \cdot)$. È un **anello** se valgono le seguenti proprietà:

$(A, +)$ è un gruppo abeliano;

$(A, \cdot)$ è associativa ed ammette l'elemento neutro $1 \neq 0$;

Per ogni $x, y, z \in A$,

$x(y + z) = xy + xz$, $(y + z)x = yx + zx$.

Se il prodotto è anche commutativo, allora si tratta di un *anello commutativo*.

Ad esempio

$(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$

sono anelli commutativi. Vedremo poi importanti esempi di anelli non commutativi.

Per ogni anello A, poniamo

$$A' := \{a \in A; \exists b \in A, ba = ab = 1\}$$

A' munito della restrizione del prodotto è il *gruppo degli elementi invertibili di* A.

Oss: 0 non può essere invertibile: per ogni $x \in A$, $0x = (0+0)x = 0x + 0x$, $0x = 0 \neq 1$.

"Non si può dividere per 0."

$\mathbb{Z}' = \{\pm 1\}$, $\mathbb{Q}' = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.

Un anello commutativo A è un **campo** se

$$A' = A^*$$

$\mathbb{Z}$ non è un campo; $\mathbb{Z}/m\mathbb{Z}$ è un campo (finito) se e solo se m è primo; $\mathbb{Q}$, $\mathbb{R}$ sono campi.

Per ogni campo $\mathbf{K}$, abbiamo associato l'**anello commutativo dei polinomi in una indeterminata a coefficienti in** $\mathbf{K}$, indicato con $\mathbf{K}[t]$.

Ogni polinomio è della forma

$$p(t) = a_0 + a_1 t + \cdots + a_k t^k$$

per qualche $k \in \mathbb{N}$, $a_j \in \mathbf{K}$, $a_k \neq 0$;

$k :=$ grado$(p(t))$.

$\mathbf{K}$ si include in $\mathbf{K}[t]$ come il sottoanello dei polinomi di grado 0.

Su $\mathbf{K}[t]$ vale una versione della divisione con il resto:

Per ogni $p(t), a(t) \in \mathbf{K}[t]$, $a(t) \neq 0$, esistono unici $q(t)$ e $r(t)$ tali che

$$p(t) = a(t)q(t) + r(t)$$

$$0 \leq \text{grado}(r(t)) < \text{grado}(a(t))$$

La costruzione di $\mathbb{Q}$ a partire da $\mathbb{Z}$ può essere ripetuta parola per parola partendo dall'anello $\mathbf{K}[t]$ e produce il **campo delle funzioni razionali in una indeterminata a coefficienti in** $\mathbf{K}$, indicato con $\mathbf{K}(t)$.

La costruzione di $\mathbb{Z}/m\mathbb{Z}$ come anello quoziente di $\mathbb{Z}$, può essere ripetuta parola per parola sostituendo $\mathbb{Z}$ con $\mathbf{K}[t]$, m con $m(t) \neq 0 \in \mathbf{K}[t]$, $m\mathbb{Z}$ con $m(t)\mathbf{K}[t]$. La costruzione produce l' anello quoziente $\mathbf{K}[t]/(m(t))$.

Come per $\mathbb{Z}$, abbiamo la funzione "resto per la divisione per $m(t)$"

$r : \mathbf{K}[t] \to \{p(t) \in \mathbf{K}[t]; \text{grado}(p(t)) < \text{grado}(m(t))\}$

$a(t) \sim b(t)$ se e solo se $r(a(t)) = r(b(t))$.

$\mathbf{K}$ si identifica con il sottoanello formato dalle classi dei polinomi di grado uguale a zero. Per ogni $x \in \mathbf{K}$, scriveremo $x = [x]_{m(t)}$.

$\mathbf{K}[t]/(m(t))$ è un campo se e solo se $m(t)$ è irriducibile. In tal caso $\mathbf{K}[t]/(m(t))$ è un campo che **estende** $\mathbf{K}$.

Esempio importante.

$t^2 + 1 \in \mathbb{R}[t]$ non ha radici reali e quindi è irriducibile.

$\mathbb{C} := \mathbb{R}[t]/(t^2 + 1)$ è un campo.

Ogni $[p(t)] = [a+bt] = a+b[t]$, $a, b \in \mathbb{R}$ in modo unico.

$$0 = [t^2 + 1] = [t]^2 + 1, [t]^2 = -1$$

per cui $[t] \in \mathbb{C}$ è una radice del polinomio

$$t^2 + 1 \in \mathbb{C}[t]$$

che quindi è riducibile in $\mathbb{C}[t]$.

$$(a + b[t]) + (c + d[t]) = (a + c) + (b + d)[t]$$

$$(a + b[t])(c + d[t]) = (ac - bd) + (bc + ad)[t]$$

Se $a + b[t] \neq 0 + 0[t] = 0$, $a^2 + b^2 \neq 0$,

$$(a + b[t])^{-1} = \frac{1}{a^2 + b^2}(a + (-b)[t])$$

Se $z = a + b[t]$,

$$\bar{z} := a + (-b)[t] := a - b[t]$$

$$z\bar{z} = a^2 + b^2$$

$$z^{-1} = \frac{\bar{z}}{z\bar{z}}$$

$$\mathbb{R} = \{z \in \mathbb{C}; z = \bar{z}\}$$

In questo modo abbiamo ottenuto un modello per il **campo dei numeri complessi**. Di solito si pone $i := [t]$, per cui $i^2 = -1$, e si scrive $z = a + ib$.

Sia X un insieme non vuoto, $\mathbf{K}$ un campo. Sia

$$\mathbf{K}^X := \{f : X \to \mathbf{K}\}$$

Possiamo munire in modo naturale $\mathbf{K}^X$ di una operazione di somma: per ogni $x \in X$,

$$(f + g)(x) := f(x) + g(x)$$

$(\mathbf{K}^X, +)$ è un gruppo abeliano: lo 0 coincide con l'applicazione nulla $0(x) = 0 \in \mathbf{K}$ per ogni $x \in X$. $(-f)(x) = -f(x)$.

Consideriamo anche l'applicazione

$$\cdot : \mathbf{K} \times \mathbf{K}^X \to \mathbf{K}^X, (\lambda, f) \to \lambda f$$

dove per ogni $x \in X$, $(\lambda f)(x) = \lambda f(x)$.

Elenchiamo altre proprietà di $(\mathbf{K}^X, +, \cdot)$, oltre il fatto già osservato che $(\mathbf{K}^X, +)$ è un gruppo abeliano.

$(\lambda + \mu)f = \lambda f + \mu f$

$\lambda(f + g) = \lambda f + \lambda g$

$(\lambda\mu)f = \lambda(\mu f)$

$1f = f, 0f = 0$

Astraiamo queste proprietà e diamo la **definizione assiomatica** si $\mathbf{K}$-spazio vettoriale.

Dato un campo $\mathbf{K}$, un insieme non vuoto V ha una struttura di $\mathbf{K}$-**spazio vettoriale** se è munito di una operazione $(V, +)$ che lo rende un gruppo abeliano, e di una "operazione"

$$\cdot : \mathbf{K} \times V \to V$$

tali $(V, +, \cdot)$ soddisfi formalmente tutte le proprietà prima elencate per $(\mathbf{K}^X, +, \cdot)$.

$\mathbf{K}$ è anche detto il **campo degli scalari** dello spazio vettoriale.

Esempio di conseguenza degli assiomi:

$-1v = -v$

$0 = 0v = (1 - 1)v = v + (-1v)$

Esempi.

• Se $X = \mathbb{N}$, $\mathbf{K}^{\mathbb{N}}$ è lo spazio vettoriale delle *successioni* a valori in $\mathbf{K}$:

$$a = \{a_n \in \mathbf{K}\}_{n \in \mathbb{N}}$$

le operazioni si effettuano indice per indice:

$a + b = \{a_n + b_n\}$, $\lambda a = \{\lambda a_n\}$.

• $X = X_{m,n} = \{(i,j) \in \mathbb{N} \times \mathbb{N}; i = 1, \ldots, m, j = 1, \ldots n\}$. Ogni $f \in \mathbf{K}^X$ può essere codificata da una tabella (*matrice*)

$$A = A_f = (a_{i,j})_{i=1,\ldots m, j=1,\ldots n}$$

con m righe e n colonne, assegnando alla posizione (i,j) intersezione della i-esima riga e della j-esima colonna, il valore

$f(i,j) := a_{i,j} \in \mathbf{K}$.

Le operazioni vengono eseguite “posto-per-posto” .

Con queste convenzioni abbiamo definito lo spazio vettoriale

$M(m, n, \mathbf{K})$

delle matrici di taglia (formato) $m \times n$ a coefficienti in $\mathbf{K}$. In particolare poniamo

$\mathbf{K}^n = M(n, 1, \mathbf{K})$.

Se $m = n$ le matrici sono *quadrate* e scriviamo

$M(n, \mathbf{K}) := M(n, n, \mathbf{K})$.

Se $\mathbf{K}[t]$ è l'anello dei polinomi, restringendo il prodotto definito su $\mathbf{K}[t] \times \mathbf{K}[t]$ sul sottoinsieme $\mathbf{K} \times \mathbf{K}[t]$ otteniamo una struttura di $\mathbf{K}$-spazio vettoriale.

Applicazioni lineari.

Se V e W sono $\mathbf{K}$-spazi vettoriali, $f : V \to W$ è *lineare* (equivalentemente, *un omomorfismo di* $\mathbf{K}$*-spazi vettoriali*) se per ogni $v, v' \in V$, $\lambda \in \mathbf{K}$

$$f(v + v') = f(v) + f(v')$$

$$f(\lambda v) = \lambda f(v).$$

$$\mathrm{Hom}(V, W) := \{f : V \to W; f \text{ lineare}\}$$

Esempi.

$$f : \mathbf{K}[t] \to \mathbf{K}^{\mathbb{N}}$$

$f(a_0 + a_1 t + \ldots a_k t^k) = (a_0, a_1, \ldots, a_k, 0, 0, 0, \ldots,)$
è lineare e iniettiva.

L' applicazione *trasposta*

$M(m, n, \mathbf{K}) \to M(n, m, \mathbf{K})$

$A \to A^t, a^t_{i,j} := a_{j,i}$

è lineare e bigettiva; coincide con la sua inversa: $(A^t)^t = A$.

Quando $\mathbf{K} = \mathbb{R}$, lo spazio $\mathbb{R}^n$ ($\mathbb{R}^2$, $\mathbb{R}^3$, ...) è il *supporto analitico della geometria ordinaria*. Per esempio la somma su $\mathbb{R}^2$,

$$(a, b)^t + (c, d)^t = (a + c, b + d)^t$$

esprime la regola del parallelogramma per la somma delle forze applicate in un punto.

$X = (a, b)^t \in \mathbb{R}^2$, $a^2 + b^2 = d(0, X)^2$ (teorema di Pitagora).

Per ogni $\theta \in \mathbb{R}$,

$$r_\theta : \mathbb{R}^2 \to \mathbb{R}^2, r_\theta((a, b)^t) :=$$

$$(\cos(\theta)a + \sin(\theta)b, -\sin(\theta)a + \cos(\theta)b)^t$$

è lineare e rappresenta analiticamente la rotazione di angolo θ.

Torniamo al campo $\mathbb{C}$ dei numeri complessi che estende $\mathbb{R}$. Come insieme $\mathbb{C}$ può essere identificato con $\mathbb{R}^2$:

$a + ib \leftrightarrow (a, b)^t$.

Le operazioni di campo $(\mathbb{C}, +, \cdot)$ estendono le operazioni della struttura di $\mathbb{R}$-spazio vettoriale $(\mathbb{R}^2, +, \cdot)$. Precisamente il prodotto

$\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$,

estende

$\cdot : \mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2$

dove consideriamo $\mathbb{R} \times \mathbb{R}^2 \subset \mathbb{C} \times \mathbb{C}$.

Grazie a queste identificazioni, la rotazione

$r_\theta : \mathbb{R}^2 \to \mathbb{R}^2$

può essere espressa nella forma

$r_\theta : \mathbb{C} \to \mathbb{C}, r_\theta(z) = e^{i\theta} z, e^{i\theta} := \cos(\theta) + i \sin(\theta)$

Hom(V, W) è munito a sua volta di una struttura naturale di $\mathbf{K}$-spazio vettoriale. Si definiscono le operazioni analogamente a quanto fatto per $\mathbf{K}^X$

$$(f + g)(v) = f(v) + g(v)$$

$$(\lambda f)(v) = \lambda f(v)$$

Si verifica prima che tali operazioni sono ben definite, cioè che $(f+g)$, (λf) sono lineari. Poi che tutte le proprietà che definiscono un $\mathbf{K}$-spazio sono soddisfatte da (Hom$(V, W), +, \cdot)$.

Se $f : V \to W$, $g : W \to Z$ sono lineari, allora la composizione

$g \circ f : V \to Z$ è lineare:

$g(f(v + v')) = g(f(v) + f(v')) =$

$g(f(v)) + g(f(v'))$

...

$f : V \to W$ è un *isomorfismo* di $\mathbf{K}$-spazi se è lineare, è bigettiva e anche l'applicazione inversa insiemistica f^{-1} è lineare.

L'ultima richiesta è una conseguenza delle prime due.

$w = f(v), w' = f(v'),\ w + w' = f(v) + f(v') = f(v + v')$

$f^{-1}(w + w') = v + v' = f^{-1}(w) + f^{-1}(w')$

La composizione di isomorfismi è un isomorfismo.

...

Sottospazi vettoriali.

Dato un $\mathbf{K}$-spazio $V = (V, +, \cdot)$, un sottoinsieme $W \subset V$ è un **sottospazio** se:

$0 \in W$

W è *chiuso per le operazioni di* V:

per ogni $w, w' \in W$, $\lambda \in \mathbf{K}$, $w+w' \in W$, $\lambda w \in W$.

Quindi W munito della restrizione delle operazioni di V è a sua volta un $\mathbf{K}$-spazio vettoriale.

Esempi.

$S(n, \mathbf{K}) = \{A \in M(n, \mathbf{K}); A = A^t\}$ è il sottospazio delle matrici *simmetrice*. Analogamente $A(n, \mathbf{K}) = \{A = -A^t\}$ è il sottospazio delle matrici *anti-simmetriche*.

Il sottoinsieme W di $\mathbf{K}^{\mathbb{N}}$ formato dalle successioni *definitivamente nulle* è un sottospazio, isomorfo a $\mathbf{K}[t]$.

$c : M(m, n, \mathbf{K}) \to \mathbf{K}^{mn}$ che riordina in una sola colonna $c(A)$ i coefficienti di ogni matrice A secondo l' ordinamento **lessicografico** degli indici, è un isomorfismo.

Poiché la composizione di isomorfismi è un isomorfismo, se $mn = m'n'$, allora gli spazi $M(m, n, \mathbf{K})$ e $M(m', n', \mathbf{K})$ sono isomorfi.

Tralasciando la questione sottile se la classe di tutti i $\mathbf{K}$-spazi sia o no un insieme, la relazione di "isomorfismo" è formalmente una relazione di equivalenza ed è interessante studiarne il quoziente.

Nucleo e immagine di un'applicazione lineare.

Sia $f : V \to W$ lineare.

L' *immagine* di f è

$\mathrm{Im}(f) := \{w \in W; \exists v \in V, f(v) = w\}$.

Il *nucleo* di f è

$\ker(f) := \{v \in V; f(v) = 0\}$

Il nucleo è un sottospazio di V, l'immagine è un sottospazio di W.

Verifiche.

Nucleo: $f(0) = f(0+0) = f(0) + f(0)$, quindi $f(0) = 0$, cioè $0 \in \ker(f)$;

Se $f(v) = 0, f(v') = 0$, allora $f(v+v') = f(v) + f(v') = 0 + 0 = 0$

...

Immagine: $f(0) = 0 \in \mathrm{Im}(f)$;

$w = f(v), w' = f(v')$, allora $w + w' = f(v) + f(v') = f(v + v')$

...

$f : V \to W$ lineare, è iniettiva se e solo se $\ker(f) = \{0\}$.

Dim. Se f è iniettiva, se $f(v) = 0$ allora $v = 0$ perché $f(0) = 0$.

Se $\ker(f) = \{0\}$ e $f(v) = f(v')$, allora

$f(v) - f(v') = f(v - v') = 0$

quindi $v - v' \in \ker(f)$, $v - v' = 0$, $v = v'$. Dunque f è iniettiva.

$f : V \to W$ lineare, $Z \subset V$ sottospazio, allora $f(Z)$ è un sottospazio di W.

Infatti la restrizione $f|Z : Z \to W$ è lineare, surgettiva e

$f(Z) = \mathrm{Im}(f|Z)$;

$\ker(f|Z) = \ker(f) \cap Z$.

Se f è iniettiva, allora $f|Z : Z \to f(Z)$ è un isomorfismo.

Se T è un sottospazio di W, allora l' *immagine inversa* $f^{-1}(T) = \{v \in V; f(v) \in T\}$ è un sottospazio di V.

Data una composizione $g \circ f$ di applicazioni lineari

$$\mathrm{Im}(g \circ f) = \mathrm{Im}(g|\mathrm{Im}(f))$$

$$\ker(g \circ f) = f^{-1}(\ker(g) \cap \mathrm{Im}(f))$$

Endomorfismi.

$\mathrm{End}(V) := \mathrm{Hom}(V, V)$

è lo spazio degli **endomorfismi** di V. Oltre che alle solite operazioni $+$, $\cdot$, esso è munito dell' operazione di composizione. In particolare

$$(\mathrm{End}(V), +, \circ)$$

è un anello che in generale **non** è commutativo. Il suo gruppo degli elementi invertibili viene indicato con $GL(V)$ e detto il *gruppo lineare di* V. È un sottogruppo di $S(V)$, cioè è un gruppo di trasformazioni di V.

Costruzioni di (sotto) spazi vettoriali.

Dati due $\mathbf{K}$-spazi V e W, l'insieme prodotto $V \times W$ eredita una struttura di $\mathbf{K}$-spazio:

$(v, w) + (v', w') := (v + v', w + w')$

$\lambda(v, w) = (\lambda v, \lambda w)$.

Questo si estende al prodotto di una famiglia arbitraria di $\mathbf{K}$-spazi.

Se $f : V \to W$ è lineare, allora il *grafico di* f $G(f) = \{(v, f(v)) \in V \times W\}$ è un sottospazio di $V \times W$.

$V \to G(f), v \to (v, f(v))$ è un isomorfismo.

Dato un $\mathbf{K}$-spazio V e un sottospazio W,

“ $v \sim_W v'$ se $v - v' \in W$ ”

è una relazione di equivalenza; le operazioni passano al quoziente definendo lo *spazio quoziente* V/W.

La proiezione $\pi : V \to V/W$ è una applicazione lineare surgettiva.

Data una famiglia non-vuota arbitraria $\mathcal{F}$ di sottospazi di V, l' *intersezione*

$F = \cap_{W \in \mathcal{F}} W$

è un sottospazio di V.

Dato un sottoinsieme non-vuoto X di V, sia

$$\mathcal{F}(X)$$

la famiglia dei sottospazi W di V tali che

$X \subset W$.

Tale famiglia non è vuota perché $V \in \mathcal{F}(X)$. La corrispondente intersezione viene indicata con

$$\text{span}(X)$$

Questo sottospazio appartiene a $\mathcal{F}(X)$ ed è contenuto in ogni $W \in \mathcal{F}(X)$. Quindi $\text{span}(X)$ è il più piccolo sottospazio (rispetto all'ordinamento $\subset$) che contenga X. Per questo è detto il **sottospazio generato dall'insieme X.**

Sia $X \subset V$ come sopra. Il *supporto* di una applicazione

$$a : X \to \mathbf{K}, x \to a_x$$

è l'insieme $\text{supp}(a) = \{x \in X; a_x \neq 0\}$. Se $\text{supp}(a)$ è **finito**, ha senso considerare

$$v = \sum_{x \in X} a_x x := \sum_{x \in \text{supp}(a)} a_x x \in V$$

dove conveniamo che $v = 0$ se $\text{supp}(a) = \emptyset$. Si dice che in questo modo il vettore v è espresso come una **combinazione lineare di elementi di** X. Ogni a a supporto finito porta una combinazione lineare di elementi di X; al variare di a, i supporti, benché finiti, possono avere un numero arbitrariamente grande di elementi.

Poniamo $\text{Comb}(X)$ il sottoinsieme di V formato dai vettori che si possono esprimere come combinazione lineare di elementi di X. Abbiamo

$$\text{Comb}(X) = \text{span}(X)$$

Dimostriamo intanto che Comb$(X) \in \mathcal{F}(X)$.

$x \in X$, $x = 1x$, quindi $X \subset$ Comb(X)

Comb(X) è un sottospazio di V:

sia $x \in X \neq \emptyset$, allora $0 = 0x \in$ Comb(X);

$v = \sum_x a_x x, v' = \sum_x a'_x x$,

allora $v + v' = \sum_x (a_x + a'_x)x$

supp$(a + a') =$ supp$(a) \cup$ supp(a') che è finita.

...

Vediamo ora che per ogni $W \in \mathcal{F}(X)$,

Comb$(X) \subset W$.

Infatti poiché $X \subset W$ e W è chiuso per le operazioni di V, ogni combinazione lineare di elementi di X appartiene a W.

Se W_1, W_2 sono sottospazi di V, in generale l'unione $W_1 \cup W_2$ **non** è un sottospazio (non è chiuso per la somma). Poniamo allora

$$W_1 + W_2 = \text{span}(W_1 \cup W_2)$$

Equivalentemente, è il sottospazio formato dai vettori v di V che si possono esprimere nella forma

$$v = w_1 + w_2, w_j \in W_j$$

$W_1 \cap W_2 = \{0\}$ *se e solo se per ogni* $v \in W_1 + W_2$ *l' espressione della forma* $v = w_1 + w_2$ è **unica**.

Dim. Se l'intersezione è nulla e

$$w_1 + w_2 = w_1' + w_2',$$

allora $w_1 - w_1' = w_2' - w_2 \in W_1 \cap W_2 = \{0\}$, da cui $w_j = w_j'$.

Viceversa, sia $z \in W_1 \cap W_2$, $0 = z - z = 0 + 0$, da cui per l'unicità della scrittura, $z = 0$.

Se $W_1 \cap W_2 = \{0\}$, diciamo che la somma è *diretta* e scriviamo $W_1 \oplus W_2$. In tal caso esistono due *proiezioni sugli addendi*

$$p_j : V \to W_j, p_j(w_1 + w_2) = w_j$$

che sono lineari e surgettive.

Dato un sottospazio W, Z è un sottospazio *complementare* di W in V, se $V = W \oplus Z$. Attenzione: la proiezione $p_W : V \to W$ dipende dalla scelta di Z.

Uno spazio vettoriale V si dice **finitamente generato** se esiste $X \subset V$ **finito** tale che

$$V = \text{span}(X)$$

Esempi. $M(m, n, \mathbf{K})$ è finitamente generato. Possiamo prendere come insieme finito di generatori l'insieme formato dalle mn matrici

$$E(i, j) \in M(m, n, \mathbf{K})$$

che hanno coefficiente 1 nel posto (i, j), coefficiente 0 in tutti gli altri posti. Per ogni matrice $m \times n$ A,

$A = (a_{i,j}) = \sum_{i,j} a_{i,j} E(i, j)$

Nel caso particolare di $\mathbf{K}^n = M(n, 1, \mathbf{K})$, poniamo $E(i, 1) := E^i$.

$\mathbf{K}[t]$ **non** è finitamente generato. Infatti, supponiamo per assurdo che sia generato da un insieme finito di polinomi $\{p_1, \ldots, p_k\}$. Sia d il massimo dei gradi dei p_j. Ogni polinomio che sia combinazione lineare di essi ha grado $\leq d$. Quindi per esempio t^{d+1} non può essere ottenuto.

L'insieme dei monomi $\{t^0, t^1, \ldots, t^m, \ldots\}$ è un insieme **numerabile** che genera $\mathbf{K}[t]$.

Vogliamo esplicitare Hom($\mathbf{K}^n, \mathbf{K}^m$).

Sia $f : \mathbf{K}^n \to \mathbf{K}^m$ lineare. Per ogni $X \in \mathbf{K}^n$

$X = (x_1, \ldots, x_n)^t = x_1 E^1 + \cdots + x_n E^n$

$f(X) = x_1 A^1 + \cdots + x_n A^n, A^j = f(E^j) \in \mathbf{K}^m$

Organizziamo gli A^j nella matrice

$A = A_f = (A^1, \ldots, A^n) \in M(m, n, \mathbf{K})$

Allora l'applicazione f è codificata dalla matrice $A = A_f$

$f(X) = AX := x_1 A^1 + \cdots + x_n A^n$

Viceversa, data $A = (A^1, \ldots, A^n) \in M(m, n, \mathbf{K})$, poniamo

$f = f_A(X) := AX$

si verifica che f_A è lineare, $A_{f_A} = A$, $f_{A_f} = f$.

In questo modo, almeno come insieme, possiamo dire senza ambiguità che

$$\mathrm{Hom}(\mathbf{K}^n, \mathbf{K}^m) = M(m, n, \mathbf{K})$$

Questa identificazione è anche compatibile con le operazioni della struttura di apazio vettoriale.

$$A_{f+g}X = (f+g)(X) =$$

$$x_1(f+g)(E^1) + \cdots + x_n(f+g)(E^n) =$$

$$x_1(f(E^1) + g(E^1)) + \cdots + x_n(f(E^n) + g(E^n)) = A_f X + A_g X$$

...

Quindi lo spazio vettoriale

$(\mathrm{Hom}(\mathbf{K}^n, \mathbf{K}^m), +, \cdot) = (M(m, n, \mathbf{K}), +, \cdot)$

Trattiamo ora la composizione:

$f = f_A : \mathbf{K}^n \to \mathbf{K}^m,\ g = g_B : \mathbf{K}^m \to \mathbf{K}^s$

$h = g \circ f = h_C.$

Come è fatta la matrice $C \in M(s, n, \mathbf{K})$?

$C^i = h(E^i) = g(f(E^i)) = B(AE^i) = BA^i$

quindi

$C = BA := (BA^1, \ldots, BA^n)$

$$(\text{End}(\mathbf{K}^n), +, \cdot, \circ) = (M(n, \mathbf{K}), +, \cdot, *)$$

dove $A * B = AB$ definito prima.

$$GL(\mathbf{K}^n) := GL(n, \mathbf{K})$$

è il gruppo lineare (matriciale) classico formato dalle matrici A $n \times n$ **invertibili** cioè tali che esiste (unica) A^{-1} tale che

$$AA^{-1} = A^{-1}A = I_n$$

Se $n > 1$, $GL(n, \mathbf{K})$ non è commutativo.

Vari modi di esprimere $C = BA$.

$c_{k,j} = B_k A^j$

dove B_k è la k-esima **riga** di B, mentre, al solito, A^j è la j-esima **colonna** di A. A volte il prodotto di matrici è detto "*prodotto righe per colonne*" .

Se $A = (a_{i,j})_{i=1,\ldots,m;j=1,\ldots n}$

$B = (b_{k,i})_{k=1,\ldots,s;i=1,\ldots,m}$

allora

$c_{k,j} = \sum_i b_{k,i} a_{i,j}$

Data $f = f_A : \mathbf{K}^n \to \mathbf{K}^m, X \to AX$, allora $\ker f_A = \ker A$ è dato dai vettori $X \in \mathbf{K}^n$ tali che

$$AX = 0 \in \mathbf{K}^m$$

quindi $\ker A$ è lo spazio delle soluzioni di un *sistema lineare omogeneo di m equazioni in n incognite*.

Decidere se $D \in \mathbf{K}^m$, $D \neq 0$, appartenga o no all'immagine $\mathrm{Im}(f_A) = \mathrm{Im}(A)$, corrisponde a studiare l'esistenza di soluzioni per il *sistema lineare* **non** *omogeneo di m equazioni in n incognite*

$$AX = D.$$

$$\mathrm{Im}(A) = \mathrm{span}\{A^1, \ldots, A^n\}$$

il sottospazio di $\mathbf{K}^m$ generato dalle colonne di A.