1 Definizioni

- Un **gruppo** è una coppia $(A, *)$ tale che A è un insieme non vuoto, e $*$ un'operazione su A dotata della propietà associativa, di elemento neutro e di reciproco per ogni elemento.
- L' **ordine del gruppo** è la cardinalità dell'insieme A. Un gruppo è detto commutativo se $*$ soddisfa la propietà commutativa.
- In un gruppo, l'elemento neutro è unico; il reciproco di ogni elemento è unico; vale la legge di cancellazione; il reciproco di un prodotto è il prodotto dei reciproci in ordine inverso.
- Un **sottogruppo** è un insieme non vuoto $B \subseteq A$ tale che $(B, *)$ è un gruppo rispetto alla stessa operazione $*$ di A. I sottogruppi banali di A sono A e $\{e\}$.
- Un **anello** è una terna $(A, +, \cdot)$ tale che A è non vuoto, $(A, +)$ è un gruppo commutativo, l'operazione $\cdot$ è associativa, e vale la legge distributiva tra $+$e$\cdot$.
- Un anello è detto unitario se il prodotto $\cdot$ ha elemento neutro (unico). E' detto commutativo se il prodotto $\cdot$ è commutativo. - Un **campo** è un anello tale che $(A, \cdot)$ è un gruppo commutativo; cioè è un anello commutativo unitario tale che $\forall a \in A \ \exists \ a^{-1} \in A$ (cioè l'inverso di a).
- Un **sottoanello** è un insieme non vuoto $B \subseteq A$ tale che $(B, +, \cdot)$ è un anello rispetto alle stesse operazioni $+$ e $\cdot$ di A. Se A e B sono campi, B è un sottocampo di A.
- Un **K-spazio vettoriale** è un insieme non vuoto V se dotato di $+$ tale che $(V, +)$ è gruppo commutativo e definita operazione $K \times V \to V$ tale che (varie operazioni).
- Un **K-sottospazio vettoriale** di V è un insieme non vuoto $W \subseteq V$ se W è un K-spazio vettoriale su cui sono definite le stesse operazioni di V.
- V e $\{\underline{0}\}$ sono sottospazi vettoriali banali di V.
- Una **matrice** a valori in K a m righe e n colonne è un insieme ordinato A di mn elementi di K disposti su m righe e n colonne.
- La matrice **trasposta** di A è la matrice $B \in M_{n,m}(K)$ definita come $b_{ij} = a_{ij}, \quad \forall i = 1 \ldots n, \quad \forall j = 1 \ldots m$.
- Una matrice è detta diagonale se è triangolare superiore e inferiore. E' simmetrica se $A = {}^tA$, antisimmetrica se $A = -{}^tA$.
- Il prodotto righe per colonne tra due matrici è definito solo se le colonne di A sono quante le righe di B. Definito come $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$.
- Le matrici quadrate sono dotate di struttura ad anello (non integro) grazie al prodotto righe per colonne. Il prodotto righe per colonne è associativo.
- Gli elementi invertibili di un anello unitario formano un gruppo. Le matrici quadrate invertibili di ordine n formano il gruppo generale lineare di ordine n, cioè $\mathbf{GL}_n(K)$.
- Il $\mathbf{MCD}(a, b)$ è un intero d tale che $d|a$, $d|b$, $\forall c$ tale che $c|a$ e $c|b$, risulta che $c|d$.
- La relazione $\equiv_n$ è compatibile con le operazioni di somma e prodotto in Z. $(Z_n, \cdot, +)$ è un anello commutativo unitario. Se è un campo, allora n è primo.
- La **funzione di Eulero** $\varphi : N \to N$ è definita come $\varphi(n) = |\{k \in Z : 1 \leq k \leq n$ e k, n sono coprimi $\}|$.
- Un' **omomoforfismo di gruppi** è un'applicazione $f : G \to H$ tale che $f(a_1) \cdot f(a_2) = f(a_1 * a_2)$, dove $(G, *)$ e $(H, \cdot)$ sono due gruppi.
- W è un K-sottospazio vettoriale di $V \Leftrightarrow a_1\underline{w}_1 + a_2\underline{w}_2 \in W, \forall \underline{w}_1, \underline{w}_2 \in W, \forall a_1, a_2 \in K$.
- Il **nucleo** di un omomorfismo $f : G \to G'$ la controimmagine in G dell'elemento neutro G'. $Ker(f)$ è un sottogruppo di G, e $Im(f)$ è un sottogruppo di G'.
- f è iniettivo $\Leftrightarrow Ker(f) = \{1_G\}$. $\quad f$ è suriettivo $\Leftrightarrow Im(f) = G'$.
- I vettori $\underline{v}_1 \ldots \underline{v}_n$ sono **linearmente indipendenti** se non esistono $c_1 \ldots c_n$ non tutti nulli tali che $c_1\underline{v}_1 + \ldots + c_n\underline{v}_n = \underline{0}$
- $\underline{v}_1 \ldots \underline{v}_n$ sono linearmente dipendenti $\Leftrightarrow$ almeno uno di essi è combinazione lineare degli altri.
- Il **sottospazio generato** dai vettori $\underline{u}_1 \ldots \underline{u}_t$ è l'insieme di tutte le loro combinazioni lineari, cioè $\langle \underline{u}_1 \ldots \underline{u}_t \rangle = \{\sum_{i=1}^{t} a_i\underline{u}_i, \forall a_i \in K\}$.
- I vettori $\underline{u}_1 \ldots \underline{u}_t \in V$ con V un K-spazio vettoriale sono detti **sistema di generatori** di V se il sottospazio da essi generato coincide con V.
- I vettori $\underline{u}_1 \ldots \underline{u}_n \in V$ con V un K-spazio vettoriale sono detti **base** di V se sono linearmente indipendenti e formano un sistema di generatori per V.
- $\{\underline{u}_1 \ldots \underline{u}_n\}$ è una base di $V \Leftrightarrow$ ogni vettore $\underline{v} \in V$ si scrive in modo unico come combinazione lineare dei vettori $\underline{u}_1 \ldots \underline{u}_n$.
- La **dimensione** di un K-spazio vettoriale V è il numero di vettori di una base di V. Lo spazio vettoriale nullo $\{\underline{0}\}$ non ha basi, e ha dimensione 0.
- Dato $dim_K(V) = n$, n vettori linearmente indipendenti formano una base; un sistema di generatori di V formato da n vettori è una base.
- Un elemento $a \in A$ si dice **divisore dello zero** se $a \cdot b = 0$ per qualche $b \neq 0$.
- Un anello commutativo unitario si dice **dominio d'integrità** se non ha divisori dello zero.
- L'insieme Σ delle soluizoni di un sistema lineare è un sottospazio vettoriale di K^n se il sistema è omogeneo.
- Le soluzioni di un sistema lineare sono in corrispondenza biunivoca con quelle dell'omogeneo associato. $\Sigma = \underline{z}_0 + \Sigma_0$.
- Ogni sistema lineare a scala è compatibile e ha ∞^{n-m} soluzioni.
- Se A è diagonale, $det(A) = \prod a_{ii}$. In particolare, $det(I_n) = 1$. Se A ha una riga o una colonna nulla, $det(A) = 0$. $det(A) = det({}^tA)$. Se $A \in GL_n(K)$, allora $det(A^{-1}) = 1/det(A)$. Scambiando fra loro due righe o due colonne, il determinante cambia segno. $det(AB) = det(A)det(B)$ (teorema di Binet). Se due righe o colonne sono uguali o proporzionali, allora $det(A) = 0$.
- Se $A \in M_n(K)$, con $n \geq 2$, vale che $A \in GL_n(K) \Leftrightarrow det(A) \neq 0$.
- Il rango per colonne di una matrice $A \in M_{m,n}(K)$ è la dimensione del K-sottospazio vettoriale di $M_{1,n}(K)$ generato dalle righe di A, cioè $r_A = dim(\langle A^1, \ldots A^m \rangle)$.
- Per ogni matrice $A \in M_{m,n}$, risulta che il rango per colonne è uguale al rango per righe.
- $rg(A) = rg({}^tA)$. Inoltre, se $A \in GL_n(K) \Leftrightarrow det(A) \neq 0 \Leftrightarrow rg(A) = n$.
- Ogni sistema lineare omogeneo è sempre compatibile (la soluzione banale $\underline{0}$). Ma vale che: il sistema è privo di autosoluzioni $\Leftrightarrow n = rg(A)$ (teorema rouchè-capelli).
- Per ottenere la matrice del cambiamento da una base F a una E, basta esprimere i vettori di F come combinazioni lineari di quelli di E, e poi scrivere i coefficienti per colonna.
- Il nucleo di una matrice A è un autospazio se e solo se ci sta un autovalore 0.
- L'autospazio di un autovalore sono tutti gli X tali che $AX = \lambda X$.
- Gli autovettori sono i vettori non nulli che compongono l'autospazio.
- Gli autovettori relativi a autovettori diversi sono perforza indipendenti.
- Una matrice di rotazione non ha autovettori. Gli autovalori sono quei fattori con cui la matrice A può moltiplicare un certo vettore. Se ce ne sono più di uno, si moltiplica il vettore in base alla combinazione degli autovettori.
- Se una matrice che ha determinante 0, vuol dire che un autovalore è uguale a 0, e non è invertibile: infatti vuol dire che una delle sue colonne è dipendente dalle altre; cioè in altre parole rappresenta un'applicazione non suriettiva, $R^n \to R^{n-rg(A)}$. Se una matrice ha determinante diverso da 0, allora il suo rango è n.
- Due matrici si dicono **simili** se esiste una matrice $C \in GL_n(K)$ tale che $B = C^{-1}AC$, o che $CB = AC$.
- Per ogni applicazione lineare, sia il nucleo che l'immagine sono sottospazi vettoriali. Vale quindi che l'immaine e controimmagine di sottospazi vettoriali di un'applicazione lineare, sono sottospazi vettoriali.
- Due matrici diagonalizzabili che hanno gli stessi autovalori sono simili fra loro, in quanto sono simili alla stessa matrice diagonale.
- Se due matrici hanno determinante diverso, non sono simili. Se due matrici hanno traccia diversa, non sono simili.
- Un vettore $\underline{v}$ si dice **autovettore** se data un'applicazione lineare T esiste un autovalore λ tale che $T(\underline{v}) = \lambda\underline{v}$.
- Un sottospazio vettoriale definito come $E_\lambda = Ker(T - \lambda I)$ dove λ è un autovalore si chiama **autospazio** relativo a λ. La molteplicità geometrica di λ è la dimensione di E_λ.
- Un operatore lineare T è detto **diagonalizzabile** se ammette una base di autovettori di T.
- Un autovalore ha **molteplicità algebrica** h se nel polinomio caratteristico appare un fattore $(\lambda - \lambda_0)^h$.
- Il determinante di una matrice $A \in M_2(K)$ rappresenta l'area del parallelogramma formato dai due vettori formati dalle colonne della matrice.
- Il nucleo di una matrice A ha come dimensione $n - rg(A)$.
- L'immagine di una matrie A è lo spazio vettoriale generato dai vettori le cui coordinate sono le colonne di A. La dimensione dell'immagine di A è quindi il rango di A.
- Un **sottogruppo ciclico** è un sottogruppo del gruppo $(G, \cdot)$ e definito come l'insieme $\{x^h, \forall h \in Z\}$, dove x è un elemento di G. L'ordine del sottogruppo è il periodo di x.
- Il **periodo** di un elemento x di un gruppo $(G, \cdot)$ è il minimo intero positivo t tale che $x^t = 1$.
- Se in un sistema lineare la matrice dei coefficienti ha determinante 0, vuol dire che ammette una sola soluzione. Se è 0, potrebbe avere infinite soluzioni o nessuna soluzione.
- Per trovare l'autospazio relativo a λ: $AX = \lambda X \to AX - \lambda X = 0 \to (A - \lambda I)X = 0 \to Ker(A - \lambda I)$.
- Un sistema lineare non omogeneo non ha mai uno spazio vettoriale come soluzioni, poichè $\underline{0} \notin \Sigma$.

2 Teoremi

Teorema 1
Siano $a, b \in Z$ con $b \neq 0$. Esiste un' unica $(q, r) \in Z \times Z$ tale che $a = bq + r, \quad 0 \leq r < |b|$.

Identità di Bezout
Siano $a, b \in Z$ non nulli. Se $d = MCD(a, b)$, esistono $x, y \in Z$ tali che $d = ax + by$.

Lemma 1
Siano $a, b \in Z$ con $b \neq 0$. Sia $a = bq + r$ con $0 \leq r < |b|$. Risulta che $MCD(a, b) = MCD(b, r)$.

Teorema fondamentale dell'aritmetica
Ogni naturale $n \geq 2$ è prodotto di un numero finito di primi. Tale scrittura è unica a meno dell'ordine dei fattori.

Teorema di Eulero-Fermat
Sia $n \geq 2$ e sia a coprimo con n. Risulta che $a^{\varphi(n)} \equiv 1(mod\ n)$.

Piccolo teorema di Fermat
Siano a, p interi coprimi. Se p è primo, risulta che $a^{p-1} \equiv 1(mod\ n)$.

Teorema della dimensione

Se un K-spazio vettoriale V ha una base formata da n vettori, ogni altra base di V è formata da n vettori.

Teorema del completamento

Sia $dim_K(V) = n$ e siano $\underline{u}_1 \dots \underline{u}_t \in V$ vettori linearmente indipendenti, con $t < n$. Esistono $n - t$ vettori $\underline{u}_{t+1} \dots \underline{u}_n \in V$ tali che $\{\underline{u}_1 \dots \underline{u}_t, \underline{u}_{t+1} \dots \underline{u}_n\}$ è una base di V.

Teorema dell'estrazione di una base

Sia $dim_K(V) = n$ e sia $\{\underline{u}_1 \dots \underline{u}_m\}$ un sistema di generatori di V. Esistono n vettori distinti $\underline{u}_{i_1} \dots \underline{u}_{i_n} \in \{\underline{u}_1 \dots \underline{u}_m\}$ formanti una base di V.

Formula di Grassmann

Siano W_1, W_2 due sottospazi vettoriali di V, con $dim_K(V)$ finita. Risulta che $dim_K(W_1) + dim_K(W_2) = dim_K(W_1 + W_2) + dim_K(W_1 \cap W_2)$.

Dim. Sia $n_1 = dim_K(W_1), n_2 = dim_K(W_2)$ e $i = dim(W_1 \cap W_2)$. Sia $\{\underline{z}_1 \dots \underline{z}_i\}$ una base di $W_1 \cap W_2$. Dato che $W_1 \cap W_2$ è un sottospazio di W_1, possiamo completare fino a ottenere $\{\underline{z}_1 \dots \underline{z}_i, \underline{u}_1 \dots \underline{u}_{n_1 - i}\}$, una base di W_1, e $\{\underline{z}_1 \dots \underline{z}_i, \underline{v}_1 \dots \underline{v}_{n_1 - i}\}$, una base di W_2. Tutti i vettori insieme sono gli $\underline{z}, \underline{u}, \underline{v}$, e sono $i + (n_1 - i) + (n_2 - i) = n_1 + n_2 - i$. Se dimostriamo che formano una base di $W_1 + W_2$, abbiamo dimostrato la formula. Banalmente, formano un sistema di generatori di V (per ogni vettore $w_1 + w_2$, w_1 è combinazione lineare degli $\underline{z}, \underline{u}$, mentre w_2 è combinazione lineare degli $\underline{z}, \underline{v}$).

Teorema 5

Sia $\{e_1 \dots e_n\}$ una base di V. L'applicazione $f : V \to K^n$, tale che $\forall \underline{v} \in V : f(\underline{v}) = (c_1 \dots c_n)$, se $\underline{v} = \sum_{i=1}^{n} c_i \underline{e}_i$, è un isomorfismo di spazi vettoriali. Quindi due spazi vettoriali n-dimensionali sono isomorfi.

Teorema di Laplace

Sia $A \in M_n(K)$, con $n \geq 2$. Risulta, $\forall i, j \in \{1 \dots n\}$, che $det(A) = \sum_{t=1}^{n} a_{it}\alpha_{it}$ e $det(A) = \sum_{t=1}^{n} a_{tj}\alpha_{tj}$, dove α è il complemento algebrico.

Teorema di Cramer

Dato un sistema lineare $AX = b$ con $A \in GL_n(K)$, il sistema ammette una sola soluzione: $(1/det(A))(det(B_1), \dots, det(B_n))$, dove B_i è ottenuta sostituendo i termini noti b all'i-esima colonna di A.

Teorema di Rouchè-Capelli

Dato un sistema lineare $AX = b$, risulta: E' compatibile $\Leftrightarrow rg(A) = rg((A\ b))$, dove $((A\ b))$ è la matrice completa. Se è compatibile, ammette $\infty^{n - rg(A)}$ soluzioni.

Teorema 6

Data un'applicazione lineare $T : V \to W$. Risulta che $dim(Ker(T)) + dim(Im(T)) = dim(V)$.

Teorema 7

Data un'applicazione lineare $T : V \to W$. Se $dim(V) = dim(W)$, allora risulta che T è iniettiva $\Leftrightarrow T$ è suriettiva.