Algebra

Leonardo Ganzaroli

Indice

Introduzione

Questi appunti del corso *Algebra* sono stati creati durante la laurea Triennale di informatica all'università "La Sapienza".

Prima di procedere rivedere la parte di insiemistica, relazioni e funzioni negli appunti di *Metodi Matematici per l'informatica* e gli insiemi numerici in *Calcolo differenziale*.

1 Numeri

1.1 Interi

Partendo da $\mathbb{N} \times \mathbb{N}$ costruisco la relazione di equivalenza:

$$(n, m) \sim (n', m') \iff n + m' = m + n'$$

Scegliendo come rappresentanti per ogni classe di equivalenza gli elementi contenenti uno 0 definisco i sottoinsiemi:

$\mathbb{Z}^+ = \{[(n, 0)] \mid n \in \mathbb{N} \setminus \{0\}\}$ (positivi)
$\mathbb{Z}^- = \{[(0, n)] \mid n \in \mathbb{N} \setminus \{0\}\}$ (negativi, rappresentati con $-n$)

Si può quindi definire $\mathbb{Z} = \mathbb{Z}^+ \cup [(0, 0)] \cup \mathbb{Z}^- = \mathbb{N} \times \mathbb{N}_{/\sim}$

Definizione Due numeri $a, b \in \mathbb{Z}$ si dicono coprimi sse il loro unico divisore comune è ± 1.

Teorema 1 (Fondamentale dell'aritmetica) *Ogni numero naturale maggiore di 1 o è un numero primo o si può esprimere come prodotto di numeri primi.*

1.1.1 Operazioni

- **Somma**

$$[(n, m)] + [(n', m')] = [(n + n', m + m')]$$

- **Prodotto**

$$[(n, m)] * [(n', m')] = [(n * n' + m * m', n' * m + n * m')]$$

1.2 Razionali

Partendo da $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ costruisco la relazione di equivalenza:

$$(a, b) \sim (c, d) \iff a * d = b * c$$

Come per gli interi definisco $\mathbb{Q} = \{\mathbb{Z} \times \mathbb{Z} \setminus \{0\}_{/\sim}\}$, un elemento $[(a, b)]$ sarà rappresentato come $\frac{a}{b}$.

1.2.1 Operazioni

- **Somma**

$$[(a,b)] + [(c,d)] = [(a*d + b*c, b*d)]$$

- **Prodotto**

$$[(a,b)] * [(c,d)] = [(a*c, b*d)]$$

1.3 Teorema fondamentale dell'algebra

Teorema 2 *Ogni equazione algebrica con coefficienti complessi di grado n ammette n soluzioni in* $\mathbb{C}$*, inoltre* $\mathbb{C}$ *si dice algebricamente chiuso.*

2 Divisibilità in $\mathbb{Z}$

Definizione Dati $m, n \in \mathbb{Z}$. La relazione "m divide n" $(m|n)$ è definita come:

$$m|n \iff \exists q \in \mathbb{Z} \mid n = mq$$

Definizione Dati $a, b \in \mathbb{Z}, n \in \mathbb{N}$ con $n \geq 2$. La relazione "a è congruente a b in modulo n" $(a \equiv b \mod n)$ è definita come:

$$a \equiv b \mod n \iff n|(b-a)$$

Teorema 3 (Divisione euclidea con resto)
Dati $m, n \in \mathbb{Z}$ *con* $n > 0$*. Si ha:*

$$\exists! q, r \in \mathbb{Z} \;\; 0 \leq r < n \mid m = nq + r$$

2.1 MCD

Definizione Dati $a, b \in \mathbb{Z}$. $d \geq 1$ è detto massimo comun divisore di a, b se:

- $d|a \wedge d|b$
- $d'|a \wedge d'|b \Rightarrow d'|d$

Per trovare l'MCD si può usare l'algoritmo euclideo:

1. $a|b \rightarrow a = bq_1 + r_1$, se $r_1 \neq 0$ continuo
2. $b|r_1 \rightarrow b = r_1q_2 + r_2$, se $r_2 \neq 0$ continuo
3. $r_1|r_2 \rightarrow r_1 = r_2q_3 + r_3$, se $r_3 \neq 0$ continuo
4. ...
5. $r_{n-2}|r_{n-1} \rightarrow r_{n-2} = r_{n-1}q_n + r_n$ con $r_n = 0$

A questo punto si ha che $MCD(a, b) = r_{n-1}$, ossia l'ultimo resto non nullo.

Definizione Un'equazione diofantea è un'equazione in una o più incognite con coefficienti interi di cui si ricercano le soluzioni intere, le equazioni con forma $ax + by = c$ hanno soluzione intera sse $MCD(a, b)|c$.

Definizione Il MCD di 2 numeri si può riscrivere come l'equazione diofantea $d = ax_0 + by_0$, questa forma viene detta identità di Bézout.

Per risolvere $ax + by = c$ si seguono questi passi:

1. Se $MCD(a, b) = d|c$ allora ammette soluzione
2. Trovare un'identità di Bézout per d
3. Moltiplicare (x_0, y_0) per $\frac{c}{d}$
4. $\forall\ k \in \mathbb{Z}$ le soluzioni sono $(x_0 + k * \frac{b}{d}, y_0 - k * \frac{a}{d})$

2.2 mcm

Definizione Dati $a, b \in \mathbb{Z}$. $d \in \mathbb{Z}$ è detto minimo comune multiplo di a, b se:

- $a|d \wedge b|d$
- $a|d' \wedge b|d' \Rightarrow d|d'$

In particolare risulta che $MCD(a, b) * mcm(a, b) = ab$

3 Strutture algebriche principali

Definizione Una funzione è detta operazione binaria se ha la forma:

$$f : S \times S \to S$$

Un'operazione binaria gode di:

- **Prop. associativa** se l'ordine di applicazione non influenza il risultato
- **Prop. commutativa** se l'ordine degli elementi non influenza il risultato
- **Esistenza del neutro** se $\exists! e \in S \mid \forall\ x \in S \quad f(x,e) = f(e,x) = x$
- **Esistenza dell'inverso** se $\forall\ x \in S\ \ \exists! x^{-1} \in S \mid f(x,x^{-1}) = f(x^{-1},x) = e$

N.B. Da qui in poi $f(x,y)$ sarà scritta come xy.

Definizione Una struttura algebrica è un insieme S con una o più operazioni binarie applicate su di esso, alcune sono (+ e * sono 2 operazioni generiche):

- **Semigruppo** $(S,+)$
  L'operazione deve essere associativa.
- **Monoide** $(S,+)$
  Un semigruppo + l'elemento neutro (indicato con 0).
- **Gruppo** $(S,+)$
  Un monoide + l'elemento inverso.
- **Gruppo abeliano** $(S,+)$
  Un gruppo + commutatività.
- **Anello** $(A,+,*)$
  - $(A,+)$ è un gruppo abeliano
  - $(A,*)$ è un semigruppo
  - $\forall\ a,b,c \in A \quad a(b+c) = ab + ac,\ \ (b+c)a = ba + ca$
- **Anello commutativo**
  Un anello ma $*$ è commutativa.
- **Anello unitario**
  Un anello + il neutro per $*$ (indicato con 1).

- **Dominio d'integrità**

  Un anello commutativo e unitario senza divisori dello 0, ossia $a * b = 0 \Rightarrow (a = 0 \vee b = 0)$

- **Campo** $(K, +, *)$
  - $(K, +, *)$ è dominio d'integrità
  - $\forall\ x \in K \setminus \{0\}\ \ \exists! x^{-1} \in K \setminus \{0\} \mid xx^{-1} = x^{-1}x = 1$

Esempi:

- $(\mathbb{N} \setminus \{0\}, +)$ è un semigruppo
- $(\mathbb{N}, +)$ è un monoide commutativo
- $(\mathbb{R}, *)$ è un gruppo abeliano
- $(\mathbb{Z}, +, *)$ è un anello
- $(\mathbb{Q}, +, *)$ è un campo

---

4 Teoria dei gruppi

4.1 Sottogruppi

Definizione Dato $(G, *)$. $(H, *)$ è un sottogruppo di G ($H \leqslant G$) se:

- $H \subseteq G$
- H contiene il neutro di G
- $x, y \in H \Rightarrow xy \in H$
- $x \in H \Rightarrow x^{-1} \in H$

In particolare i sottogruppi:

- Di $(\mathbb{Z}, +)$ hanno la forma $n\mathbb{Z}$

  $(2\mathbb{Z}, +)$ è un sottogruppo formato dai numeri pari

- Di $(\mathbb{Z}_n, +)$ hanno la forma H_d con d divisore di n

  $$\mathbb{Z}_{12} \to \{[0]\}, \mathbb{Z}_{12}, H_2, H_3, H_4, H_6$$

  .

4.2 Gruppi ciclici

Definizione Dato un gruppo $(G, *)$. Prendendo $g \in G, t \in \mathbb{Z}$ definisco:

$$g^t = \begin{cases} 1_G \text{ se } t = 0 \\ g * \ldots * g \text{ per t volte se } t > 0 \\ g^{-1} * \ldots * g^{-1} \text{ per t volte se } t < 0 \end{cases}$$

L'insieme $\{g^t, t \in \mathbb{Z}\}$ risulta essere un sottogruppo di G, viene definito generato da g e si indica con $\langle g \rangle$.

Definizione Un gruppo ciclico è un gruppo generato da un solo elemento.

Definizione L'ordine di un gruppo ciclico $(o(g))$ è un numero $n \in \mathbb{N}$ tale che $g^n = 1$, esso combacia con la cardinalità dell'insieme.

Per esempio $(\mathbb{Z}, +) = \langle 1 \rangle$, infatti si può ottenere qualsiasi numero intero k sommando k volte 1.

Definizione Il gruppo di Klein è il più piccolo gruppo non ciclico:

$$\kappa_4 = \{1, a, b, c\}$$

Teorema 4 (Struttura dei gruppi ciclici)

- $H \leqslant G = \langle g \rangle \Rightarrow H$ *è ciclico*
- $H \leqslant G = \langle g \rangle \wedge |G| = n \Rightarrow o(H) | n$
- $\forall\ k \ \ n = k * c \ \ \exists! H \leqslant G \mid (|H| = k \Rightarrow H = \langle g^{\frac{n}{k}} \rangle)$

Teorema 5 (Cauchy)
Dati G gruppo finito e $p \in \mathbb{P}$:

$$p || G| \Rightarrow \exists g \in G \mid o(g) = p$$

4.3 Classi laterali

Definizione Dati $H \leqslant G$ e le relazioni:

$$x \sim_{sx} y \iff x^{-1}y \in H,\ x \sim_{dx} y \iff xy^{-1} \in H$$

Si definiscono le classi laterali sx/dx di $x \in G$ come:

$$xH = [x]_{sx} = \{y \in G \mid x \sim_{sx} y\},\ Hx = [x]_{dx} = \{y \in G \mid x \sim_{dx} y\}$$

Teorema 6 (Lagrange)
Dati $H \leqslant G$. Risulta che $|G| = |H| *$ numero di classi laterali sx (o dx) distinte

Definizione Un sottogruppo è detto normale ($H \trianglelefteq G$) se $\forall\ x \in G\ \ xH = Hx$.

4.4 Gruppi simmetrici

Definizione Un gruppo simmetrico è formato dalle permutazioni degli elementi di un certo insieme X, nel caso X sia finito il gruppo ha grado $|X|$.

In questo caso si denota S_n come il gruppo formato dalle mappature biunivoche $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, esso ha ordine $n!$.

Una permutazione viene denotata come $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$.

Definizione Il supporto ($supp()$) di una permutazione è $\{j \in \sigma \mid \sigma(j) \neq j\}$.

Definizione Una trasposizione è una permutazione $(i, j) = \begin{pmatrix} 1 & 2 & \ldots & i & j & \ldots & n \\ 1 & 2 & \ldots & j & i & \ldots & n \end{pmatrix}$.

Definizione Un k-ciclo è una permutazione tale che:

$$\sigma(j_1) = j_2,\ \sigma(j_2) = j_3,\ \ldots,\ \sigma(j_k) = j_1$$

L'ordine di una permutazione è il mcm tra le lunghezze dei suoi cicli.

In presenza di cicli è possibile scomporre una permutazione in un unico prodotto:

$$\sigma = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_k \mid \forall i, j \leq k\ \ supp(\sigma_i) \cap supp(\sigma_j) = \emptyset$$

Per esempio $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 4 & 1 & 2 \end{pmatrix} \longrightarrow (1\ 3\ 5)(2\ 6)$

Un prodotto può a sua volta essere scomposto in una serie di trasposizioni:

$$(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2)$$

Se il numero di elementi è pari allora la permutazione è pari, altrimenti dispari.

5 Teoria degli anelli

5.1 Invertibili

In caso di anello unitario si definisce l'insieme degli invertibili come:

$$A^* = \{a \in A \mid \exists a' \ \ a' * a = a * a' = 1\}$$

Esso forma un gruppo con $*$.

Vale inoltre $a, b \in A^* \Rightarrow a * b \in A^*$.

5.2 Sottoanelli

Definizione Dato $(A, +, *)$. $(B, +, *)$ è un sottoanello di A ($A \leqslant B$) se:

- $(B, +) \leqslant (A, +)$
- $x, y \in B \Rightarrow xy \in B$

5.3 Ideali

Definizione Dato $(A, +, *)$. $(I, +, *)$ è un ideale di A ($I \lhd A$) se:

- $I \subseteq A$
- $(I, +) \leqslant (A, +)$
- $\{ax \mid x \in I, a \in A\} \subseteq I$
- $\{yb \mid y \in I, b \in A\} \subseteq I$

Definizione Dato l'anello A e $a_1, \ldots, a_n \in A$. Un ideale I è detto generato da $a_1, \ldots, a_n$ se:

$$I(a_1, \ldots, a_n) = \{a_1 b_1 + \ldots + a_n b_n \mid b_1, \ldots, b_n \in A\}$$

Nel caso $I(a) \lhd A$ si dice ideale principale.

6 $\mathbb{Z}_n$

$\mathbb{Z}_n$ è l'insieme quoziente della relazione:

$$a \sim_n b \iff n|a-b$$

Insieme a $+, *$ forma un anello commutativo unitario infatti:

- $[k] + [h] = [k + h]$, con neutro $[0]$
- $[k] * [h] = [k * h]$, con neutro $[1]$
- $+, *$ sono commutatice e associative
- Vale la proprietà distributiva
- Esistono divisori dello zero

Definizione La funzione di Eulero (φ) restituisce il numero di numeri coprimi inferiori a n.

Gli invertibili di $\mathbb{Z}_n$ sono gli elementi coprimi ad n, il loro numero è dato dalla funzione di Eulero.

Per esempio gli invertibili di $\mathbb{Z}_8$ sono le classi $1, 3, 5, 7$.

6.1 Congruenze lineari

Definizione Una congruenza lineare $ax \equiv b \mod n$ equivale all'equazione diofantea:

$$ax + ny = b$$

Se x_0 è soluzione, tutte le soluzioni della congruenza sono della forma:

$$x_0 + h * \frac{n}{MCD(a,n)} \quad \text{con } h \in \mathbb{Z}$$

Il numero di soluzioni diverse è dato da $MCD(a, n)$.

Teorema 7 (Eulero)
Dati a, n interi positivi coprimi:

$$a^{\varphi(n)} \equiv 1 \mod n$$

Teorema 8 (Fermat)
Dato p numero primo:

$$\forall a \in \mathbb{Z} \quad a^p \equiv a \mod p$$

6.2 Sistemi e Tcs

Teorema 9 (Cinese del resto)
Dato il sistema (detto cinese):

$$\begin{cases} x \equiv b_1 \mod a_1 \\ x \equiv b_2 \mod a_2 \\ \dots \\ x \equiv b_n \mod a_n \end{cases}$$

In cui:

- $\forall \ \ i, j \in [1, n] \ \ i \neq j \Rightarrow MCD(a_i, a_j) = 1$
- $\forall \ i \in [1, n] \ \ 0 \leq b_i < a_i$

Se il sistema è compatibile allora esiste un'unica soluzione in $\mod a_1 * \ldots * a_n$.

Si può trasformare un sistema di congruenze lineari in *cinese* a patto che:

- Ogni equazione ammetta soluzione
- Gli argomenti dei moduli siano tutti coprimi

Procedimento:

1. Dividere ogni elemento dell'equazione per il corrispettivo MCD tra a_i e n_i
2. Moltiplicare ogni riga per l'inverso di $\frac{a_i}{d_i}$

7 Omomorfismi

Definizione Una funzione tra 2 strutture algebriche dello stesso tipo $f : G \to H$ viene detta omomorfismo se:

$$\forall\ g, h \in G \quad f(g *_G h) = f(g) *_H f(h)$$

Nel caso le strutture abbiano più operazioni deve valere per ognuna.

Definizione Un isomorfismo è un omomorfismo biunivoco.

Definizione Un endomorfismo è un omomorfismo sulla stessa struttura.

Definizione Un automorfismo è l'unione dei 2 precedenti.

Si può definire la relazione "G è isomorfo ad H" ($G \cong H$) come:

$$G \cong H \iff \exists f : G \to H \quad \text{isomorfismo}$$

Il nucleo di un omomorfismo ($ker()$) è $\{g \in G \mid f(g) = 0_H\}$

L'immagine di un omomorfismo ($im()$) è $\{y \in H \mid \exists x \in G \quad f(x) = y\}$

Se tra gruppi risulta $ker(f) \leqslant G$ e $im(f) \leqslant H$.

Teorema 10 (Isomorfismo tra gruppi ciclici)
Se esiste un isomorfismo tra due gruppi ciclici G, H e $o(g \in G)$ è finito allora $\langle g \rangle \cong \langle f(g) \rangle$.

Teorema 11 (Primo teor. d'isomorfismo)

$$f : A \to B \quad \textit{è omomorfismo tra anelli} \Rightarrow A \setminus ker(f) \cong im(f)$$

8 Spazi vettoriali

Definizione Uno spazio vettoriale su un campo K è una struttura algebrica $(V, +, *)$ dove:

- $+ : V \times V \to V : (u, v) \to w$
- $* : K \times V \to V : (\lambda, v) \to w$
- Un elemento v di V è detto vettore
- Un elemento λ di K è detto scalare
- $(V, +)$ è un gruppo abeliano
- $\exists x \in K \mid \forall v \in V \quad x * v = v$
- $\forall\ s, t \in K, v \in V \quad (s * t)v = s(t * v)$
- $\forall\ s, t \in K, v \in V \quad (s + t)v = sv + tv$
- $\forall\ s \in K, v, w \in V \quad s(v + w) = sv + sw$

Dato V su K. W su K è un sottospazio di V se:

- $(W, +) \leqslant (V, +)$
- $w \in W, \lambda \in K \Rightarrow \lambda w \in W$

Definizione Una combinazione lineare dei vettori $v_1, \ldots, v_n$ è:

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_k v_k \quad \text{con } \alpha_1, \ldots, \alpha_k \in K$$

Definizione Lo span dei vettori $v_1, \ldots, v_n$ è l'insieme di tutte le combinazioni lineari di quei vettori:

$$span(v_1, \ldots, v_n) = \{\lambda_1 v_1 + \ldots + \lambda_n v_n \mid \lambda_1, \ldots, \lambda_n \in K\}$$

Definizione I vettori $v_1, \ldots, v_n \neq 0_v$ sono un insieme di generatori per V sse:

$$\forall\ v \in V \quad \exists \lambda_1, \ldots, \lambda_n \mid v = \lambda_1 v_1 + \ldots \lambda_n v_n$$

Definizione I vettori $v_1, \ldots, v_n \neq 0_v$ sono linearmente indipendenti sse:

$$\lambda_1 v_1 + \ldots \lambda_n v_n = 0_v \iff \lambda_1 = \ldots = \lambda_n = 0$$

Definizione Un insieme di generatori linearmente indipendenti sono detti base.

Definizione Una base è detta canonica se contiene solo 0 e 1.

Teorema 12 (Cardinalità delle basi) *Tutte le basi di uno spazio vettoriale hanno la stessa cardinalità.*

Definizione La dimensione di uno spazio vettoriale è pari alla cardinalità di una sua base.

Teorema 13 (Grassmann)
Dati U, V sottospazi dello stesso spazio:

$$U + V = \{u + v \mid u \in U, v \in V\}$$

$$U \cap V = \{u \mid u \in U \wedge u \in V\}$$

Entrambi gli insiemi sono sottospazi, la loro dimensione è legata dalla formula:

$$dim(U + V) = dim(U) + dim(V) - dim(U \cap V)$$

Definizione Dati V, W su K. Una funzione $f : V \to W$ è detta trasformazione lineare se:

- $\forall\ v, v' \in V \quad f(v + v') = f(v) + f(v')$
- $\forall \lambda \in K, v \in V \quad f(\lambda v) = \lambda f(v)$

Teorema 14 (Dimensione)
Data $T : V \to W$:

$$dim(V) = dim(im(T)) + dim(ker(T))$$

Teorema 15 (Rango)
Data $f : V \to W$. Il rango di f è:

$$dim(V) - dim(ker(f))$$

9 Matrici

9.1 Definizioni

Definizione Dati $m, n \in \mathbb{N}$. Una matrice $m \times n$ a coefficienti in campo K è una griglia di m righe e n colonne i cui elementi appartengono al campo:

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix}$$

Definizione Un vettore riga è una matrice $1 \times n$, uno colonna invece $n \times 1$.

Definizione Data una matrice A. La matrice trasposta di A (A^T) ha l'i-esima riga pari all'i-esima colonna di A.

Definizione Una matrice è detta a scala se il pivot della riga i (primo elemento non nullo da sx) è più a sinistra di quello della riga $i+1$.

Definizione Una matrice è detta triangolare (superiore) se tutti gli elementi sotto la diagonale principale sono pari a 0.

Definizione Una matrice quadrata è detta simmetrica se $\forall\ i, j \in [1, n]\ \ a_{i,j} = a_{j,i}$.

Le operazioni elementari eseguibili sono:

- Scambio di 2 righe/colonne
- Somma di una riga/colonna ad un'altra riga/colonna
- Moltiplicazione di una riga/colonna per uno scalare

Definizione Due matrici si dicono equivalenti se usando solo operazioni elementari si può ottenere una partendo dall'altra.

Definizione La moltiplicazione tra matrici A, B è il prodotto riga per colonna, un elemento $c_{i,j}$ della nuova matrice sarà dato da:

$$\sum_{r=1}^{n} a_{i,r} b_{r,j}$$

Risulta necessario num. righe B = num. colonne A.

Definizione Il rango di una matrice è il massimo numero di righe/colonne linearmente indipendenti.

9.2 Sistemi lineari

Definizione Una sottomatrice di una matrice A è ottenuta cancellando un certo numero di righe/colonne da A.

Un sistema di equazioni lineari può essere riscritto in forma di matrice:

$$\begin{cases} a_{1_1}x_1 + a_{2_1}x_2 + \cdots + a_{1_n}x_n = b_1 \\ \cdots \\ a_{m_1}x_1 + a_{m_2}x_2 + \cdots + a_{m_n}x_n = b_m \end{cases}$$

Si riscrive come:

$$\begin{pmatrix} a_{1_1} & \cdots & a_{1_n} \\ \vdots & \ddots & \vdots \\ a_{m_1} & \cdots & a_{m_n} \end{pmatrix} * \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \rightarrow A\bar{x} = \bar{b}$$

Si può anche rappresentare tramite la matrice completa dei coefficienti A_b:

$$\left(\begin{array}{ccc|c} a_{1_1} & \cdots & a_{1_n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m_1} & \cdots & a_{m_n} & b_n \end{array}\right)$$

Teorema 16 (Rouché-Capelli)
Il sistema $Ax = b$ ammette soluzioni sse $rg(A) = rg(A_b)$.

Teorema 17 (Fondamentale per i sistemi lineari)
Dati $Ax = b$ e la sua riduzione a scala $Sx = c$:

- *Hanno le stesse soluzioni*
- *Hanno lo stesso rango*
- *Le colonne di S con i pivot sono quelle di A linearmente indipendenti*

Riducendo la matrice completa a scala è possibile semplificare il sistema associato, per farlo si può usare l'algoritmo di Gauss:

1. Se la prima riga ha il primo elemento nullo, scambiala con una riga che ha il primo elemento non nullo
2. Per ogni riga A_i con primo elemento non nullo (eccetto la prima) moltiplica la prima riga per un coefficiente scelto in maniera tale che la somma tra la prima riga e A_i abbia il primo elemento nullo, sostituisci A_i con la somma appena ricavata
3. Riapplica i punti precedenti sulla sottomatrice ottenuta cancellando la prima riga e colonna

Teorema 18 (Sistemi triangolari) *Un sistema triangolare $Tx = c$ ammette un'unica soluzione sse la diagonale principale di T non ha valori nulli.*

9.3 Determinante

Definizione Il determinante di una radice quadrata è un numero che ne descrive alcune proprietà.

Ci sono diversi modi per calcolarlo:

- 1×1, equivale all'unico elemento
- 2×2, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow (a * d) - (b * c)$
- 3×3, $\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \rightarrow aei + bfg + cdh - gec - hfa - idb$
- Sviluppo di Laplace:

  $\sum_{k=1}^{n} (-1)^{i+k} * a_{i,k} * det(A_{i,k})$ con $i \in [1, n]$ e $M_{i,k}$ sottomatrice senza riga i e colonna k
- Se la matrice è triangolare allora è il prodotto della diagonale

Definizione Il polinomio caratteristico di una matrice è:

$$det(xI_n - A) \quad \text{con } xI_n \text{ la matrice identità con x invece di 1}$$

Teorema 19 (Binet)

$$det(AB) = det(A) * det(B)$$

9.4 Applicazioni lineari

Definizione L'insieme delle coordinate di un vettore rispetto alla base è l'insieme degli scalari per cui va moltiplicata la base per ottenere il vettore.

Data la trasformazione lineare $f : V \to W$ con $dim(V) = n, dim(W) = m$. Si può associare una matrice $m \times n$ alla funzione usando come colonne i coefficienti ottenuti applicando la funzione sui vettori della base canonica di V.
N.B. La matrice è unica per ogni coppia di basi scelte.

Se la funzione dà:

- $f \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$
- $f \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
- $f \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

La matrice sarà $\begin{pmatrix} 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, quindi $f : \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2x + y \\ z \end{pmatrix}$.

9.4.1 Diagonalizzazione

Definizione Dato un endomorfismo sullo spazio V. Un vettore $v \neq 0_V$ è detto autovettore associato all'autovalore $\lambda \in K$ se $f(v) = \lambda * v$, risulta che anche ogni vettore $\neq 0_V$ multiplo di v è un autovettore associato a λ.

Definizione L'autospazio relativo di un autovalore è l'insieme di autovettori con esso come autovalore, forma uno sottospazio.

Definizione La molteplicità algebrica di un autovalore è il numero di volte che esso è radice del polinomio caratteristico.

Definizione La molteplicità geometrica di un autovalore è la dimensione del suo autospazio relativo.

Definizione Dato un endomorfismo sullo spazio V. f è diagonalizzabile se esiste una base di V formata da autovettori.