- Una **relazione** (binaria) R tra due insiemi A e B è un **sottoinsieme del prodotto cartesiano A × B**
- R è una **relazione di equivalenza** se è una relazione **riflessiva, simmetrica e transitiva**
- R è una **relazione d'ordine** se R è **riflessiva, antisimmetrica, transitiva**
- Una relazione R tra due insiemi (non vuoti) A e B è detta **applicazione**, o **funzione**, se **∀a ∈ A esiste uno e un solo b ∈ B tale che aRb:**
    - **Iniettiva:** se F(a)=F(b) ⇨ a=b (ogni elemento di B ammette al più una contro-immagine)
    - **Suriettiva:** se ∀b ∈ B, ∃a ∈ A tale che F(a) = B (se ogni elemento di b ammette esattamente 1 contro-immagine)
    - **biettiva:** se è sia iniettiva che suriettiva
- **operazione è un'applicazione tale che** ★ : A × A → A (a, b) → a ★ b
- Un insieme su cui sia definito una o più operazioni si chiama "**struttura algebrica**" es (A,★)
- Un **monoide** (M, ★) è un insieme M dotato di una operazione ★ tale che **(1) ★ è associativa (2) ★ è dotata di elemento neutro e.**
- Un **gruppo** (G, ★) è un insieme G dotato di una operazione ★ tale che **(1) ★ associativa (2) ★ ammette neutro (3) ★ ammette inverso per ogni x del gruppo**
- un gruppo si dice **Gruppo abeliano** se ★è anche commutativa
- H è un **sottogruppo** di (G, ★) se **(1) H è chiuso rispetto a ★(2) elemento neutro di G appartiene ad H (3) ogni elemento di H ha inverso**
- Siano (G, ★) e (T, •) due gruppi: una applicazione si dice **omomorfismo di gruppi** se **∀a, b ∈ G, si ha f(a ★ b) = f(a) • f(b)**
    - Se (G, ★) = (T, •) allora omomorfismo si dice anche **endomorfismo**
- un omomorfismo biunivoco è detto **isomorfismo**
    - Se (G, ★) = (T, •) allora isomorfismo si dice anche **automorfismo**
- un **anello** (A,+,*) è un insieme A tale che **(1) (A,+) è gruppo abeliano (2) (A,*) è monoide (3) Proprietà distributive del prodotto rispetto alla somma**
    - **è commutativo se la seconda operazione (prodotto) è commutativa**
- un **campo** è un anello commutativo in cui **tutti gli elementi diversi da zero sono invertibili**
- Se ∼ è una relazione di equivalenza in A, ∀ a ∈ A si dice **classe di equivalenza** individuata da a, l'insieme di tutti e soli gli elementi che sono in relazione con a. si indica con **[a]. Essa PARTIZIONA L'INSIEME**
    - **a ∼ b ⇔ [a]∼ = [b]∼**
    - **a (not)∼ b ⇔ [a]∼ ∩ [b]∼ = ∅**
- L'insieme delle classi di equivalenza viene detto **insieme quoziente di A modulo ∼**
- **a ∼ b (mod n)** se esiste un h tale che **a-b=hn (a-b multiplo di n)**
- L'insieme quoziente di Z modulo la relazione di congruenza modulo n viene detto **insieme delle classi di resto modulo n** e denotato con Zn. In generale Zn ha n elementi
    - **le operazioni di prodotto e somma sono ben definite**
    - **(Zn, +n) è un gruppo abeliano**
    - **(Zn, ·n) è un monoide**
    - **quindi (Zn, +n, ·n) è un anello commutativo**
    - **(Zn, +n, ·n) è un campo se e solo se n è un numero primo**
- **algoritmo euclideo:** Vediamo un altro esempio: $MCD(539, 455)$

dividendo	=	divisore	·	quoziente	+	resto
539	=	455	·	1	+	84
455	=	84	·	5	+	35
84	=	35	·	2	+	14
35	=	14	·	2	+	7
14	=	7	·	2	+	0

- **Teorema di Ruffini:** Siano **$a(x) \in R[x]$ e $b(x) = x - \xi$**. Il resto della divisione di a(x) per $x - \xi$ è $a(\xi)$. In particolare, a**(x) è divisibile per $x - \xi$ se e solo se $a(\xi) = 0$.**
- Un numero $p \in Z$, con $p \neq 0, +1, -1$, si dice **primo** se ogni volta che p divide il prodotto $a \cdot b$ di due interi a e b **esso divide almeno uno dei due fattori**.
- Un numero $z \in Z$, con $z \neq 0, +1, -1$, si dice **irriducibile** se è divisibile solo per ± 1 e $\pm z$
- **p è primo ⇔ p è irriducibile.**
- **Teorema fondamentale Aritmetica:** Ogni $n \in Z - \{0, +1, -1\}$ può essere scritto come prodotto di $s \geq 1$ numeri primi

==========

- R^n è l'insieme i cui elementi sono n-uple di numeri reali.
- $(R^n, +)$ è un gruppo abeliano
- matrice **trasposta** è la matrice A^t che ha come colonne le righe della matrice A e come righe e le colonne di A
- **Matrice simmetrica :**
- **Matrice asimmetrica:**

$$\begin{pmatrix} 3 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 1 \end{pmatrix}$$
MATRICE SIMMETRICA

$$\begin{pmatrix} 0 & -1 & -3 \\ 1 & 0 & -2 \\ 3 & 2 & 0 \end{pmatrix}$$
MATRICE ANTISIMMETRICA

- $(Mat_{n\times m}, +)$ è un gruppo
- $(Mat_{n\times m}, *)$ è un monoide non commutativo
- A è una **matrice invertibile** se esiste $B \in Mat_{n\times n}$ Tale che $AB=BA=I$ → l'insieme delle mat invertibili è **GL**
- il **determinante** è un numero associato alla matrice quadrata
  - il **determinante dell'inversa** è uguale a **1/det(A)**
- Siano A e B due matrici allora **det(AB) = det(A) det(B) = det(BA)**
- Due **sistemi** si dicono **equivalenti** se i loro insiemi delle soluzioni coincidono
- **Rouche' Capelli:** si consideri un sistema con matrice dei coefficienti A e matrice orlata:
  - se pivot(matrice) = pivot(matrice orlata) → **sistema risolubile**
  - se pivot(matrice) = numero incognite → **unica soluzione**
  - se pivot(matrice) < numero di incognite → **infty** ^{j} soluzioni e j = incognite - pivot(matrice)
- Un **sistema si dice omogeneo** se b = 0, cioe'se tutti i termini noti sono nulli
- **0 è soluzione di Ax = b ⇔ b = 0**
- **Rouche' Capelli 2:** Sia $A\underline{x} = b$ un sistema
  - se $\underline{b} = \underline{0}$ allora è soluzione del sistema. Inoltre se $\underline{x0}$ e $\underline{x1}$ sono soluzioni, **anche $\alpha\underline{x0} + \beta\underline{x1}$** è soluzione dello stesso sistema
  - se $\underline{b} \neq \underline{0}$ può essere risolubile oppure no. $\underline{x2}$ è soluzione sse $\underline{x0} = \underline{x1} - \underline{x2}$ è soluzione
- il determinante di una matrice triangolare superiore è il prodotto degli elementi sulla diagonale.
- **Teorema di Cramer** permette di calcolare la matrice inversa e le soluzioni di un sistema a matrice quadrata.
- si può trovare la matrice inversa tramite Cramer: ==========>

$$m_{ij} = \frac{(-1)^{i+j} \det(A_{ji})}{\det(A)}$$

- per calcolare **l'inversa di una matrice**, si può usare gauss nel seguente modo:
  - orlare la matrice A con la matrice identità
  - semplificare con gauss la matrice orlata
  - una volta semplificata bisogna rendere la matrice che abbiamo appena semplificato con gli elementi nulli pure sopra la diagonale
  - la matrice che è nell'orlo sarà quella inversa.
- Sia K un campo e V un gruppo abeliano. Un insieme V è detto **spazio vettoriale** se sono definite:
  - **operazione +** : $V \times V \rightarrow V$ $(\underline{v}, \underline{u}) \mapsto \underline{v} + \underline{u}$
  - **funzione *:** $K \times V \rightarrow V$ $(k, \underline{v}) \rightarrow k*\underline{v}$
  - **le operazioni sopra devono rispettare le operazioni del gruppo abeliano e dei campi**

- Sia U un sottoinsieme di V. Si dice che **U è sottospazio vettoriale** se valgono:
    - $\forall \underline{u1}, \underline{u2} \in U \rightarrow \underline{u1} + \underline{u2} \in U$
    - $\forall \underline{u} \in U, \forall k \in K \rightarrow (k\,\underline{u}) \in U$
- **spazio generato è <v> := {$\underline{w} \in V$ tali che $\exists k \in K$ con $w = k\,\underline{v}$}**
- Siano U e V due sottospazi di X, allora **U∩ V è sottospazio vettoriale.** (prende le condizioni di U e V)
- Siano U e V due sottospazi di X, allora **U + V** := **{$\underline{x} \in X$ tali che $\exists \underline{u} \in U$ e $\underline{v} \in V$ tali che $x = \underline{u} + \underline{v}$}** (prende le condizioni in comune)
- dato uno spazio vettoriale V = < hv1, v2, . . . vn> allora < hv1, v2, . . . vn> è un **sistema di generatori per V**
- v1, v2, . . . , vn sono **linearmente indipendenti** se non si possono scrivere come combinazione lineare di altri
- si dice che {v1, v2, . . . , vn} è una **base di V** se:
    - i vettori {v1, v2, . . . , vn} sono un **sistema di generatori di V**
    - i vettori {v1, v2, . . . , vn} sono **indipendenti**
- Sia V uno spazio vettoriale che ammette una base {v1, v2, . . . , vn} formata da n vettori. Allora **ogni altra base di V sarà formata da n vettori**.
- e Diciamo che **V è uno spazio vettoriale finitamente generato** se ammette un insieme finito come insieme di generatori
- **Estrazione della base:** se abbiamo un po' di vettori che generano lo spazio, o abbiamo già una base, oppure stiamo considerando "troppi vettori", quindi ne possiamo **scegliere solo alcuni fra questi per ottenere una base**.
- **Completamento della base:** se abbiamo un po' di vettori indipendenti, o abbiamo già una base, oppure stiamo considerando "troppo pochi vettori", quindi ne **dobbiamo aggiungere altri per ottenere una base.**
- Il **rango di una matrice** è la **dimensione dello spazio vettoriale generato dalle sue colonne** = **n pivot**
- **Formula di Grassman: dim(U) + dim(W) = dim(U ∩ W) + dim(U + W)**
- Sia **V** uno **spazio vettoriale e U un suo sottospazio** allora se **dim(U)=dim(V) → U=V**
- Un'**applicazione lineare** f è determinata dall'immagine dei vettori di una base del dominio. Se conosco l'immagine dei vettori che formano una base del dominio, allora conosco tutta l'applicazione lineare
- se **$f(0_V) = f(0_K\,v1) = 0_K\,f(v1) = 0_W$** allora abbiamo un grande indizio che potrebbe essere lineare
- **ker(f)** = **{ $\underline{v} \in V : f(\underline{v}) = \underline{0_W}\} \subset V \rightarrow$** insieme dei vettori che hanno come immagine 0_W **→ STSP di V**
- **Im(f)** = **{ $\underline{w} \in W : \exists \underline{v} \in V$ con $f(\underline{v}) = \underline{w}\} \subset W \rightarrow$ STSP di W**
- **nullità più rango** = siano V e W due spazi vettoriali su K finitamente generati e f: V→ W un'applicazione lineare. Allora **dim(V) = dim(ker(f)) + dim(Im(f))**
- **applicazione iniettiva** sse **ker(f) = {0_V}.**
- **applicazione suriettiva** sse **Im(f)=W**
- Un'applicazione lineare f si dice **isomorfismo** se è **biiettiva**. L'isomorfismo tra spazi vettoriali è una relazione di equivalenza
- **V è isomorfo a W ⇔ dim(V) = dim(W).**
- ==========
- siano V e W due spazi vettoriali e siano C e D le rispettive basi che hanno dimensione dim(V) e dim(W). Sia f V → W una applicazione lineare. Si chiama **matrice rappresentativa** di f la matrice ${}_D M_C$ costruita cosi:
    - si considera il vettore di base v_i
    - si calcola l'immagine f(v_i) che è un vettore in W
    - si scrive il vettore f(v_i) come combinazione lineare dei vettori della base di D
    - si mettono i coefficienti ottenuti in colonna
    - questa colonna è la i-esima colonna della matrice ${}_D M_C$ (f)

- se si conosce la matrice rappresentativa di un'applicazione lineare, allora **si può trovare il vettore immagine di un vettore dato** semplicemente **moltiplicando fra di loro la matrice rappresentativa e un vettore**: sia $_{D}M_{C}$ la matrice rappresentativa
    - Si scrive il vettore $\underline{v}$ come combinazione lineare di C
    - prendo i coefficienti e li metto in un vettore
    - moltiplico questo vettore per la matrice rappresentativa e ottengo un vettore con i coefficienti della immagine del vettore che cerco.
- la matrice Rappresentativa ci permette di definire subito alcune proprietà:
    - **dim(V) = numero colonne matrice**
    - **dim(W) = numero righe matrice**
    - **dim(Im(f)) = rk(M)**
    - **dIm(ker(f)) = n - rk(M)**
- **Hom (V, W)** = {f : V → W lineari }
- **End (V)** = {f : V → V applicazione lineare } = **Hom(V,V)**
- Sia f endomorfismo di V definito su un campo K e sia $\underline{v} \in V$. Diciamo che $\underline{v} \in V$ è un **autovettore** per f se:
    - $v \neq \underline{0}$
    - esiste $k \in K : f(\underline{v}) = kv$ → se esiste questo vettore allora si dice che k è un **autovalore**
- Sia f : V → V un'applicazione lineare e sia V un K-spazio vettoriale finitamente generato. **La matrice $M_{V}(f)$ è diagonale sse la base V è formata da autovettori.**
- un endomorfismo f di V è **diagonalizzabile** se esiste una base di V **formata tutta da auto-vettori di f**
- **spettro di f** è l'insieme degli autovalori di f. Per vedere se è diagonalizzabile:

  ⇨ **Data una applicazione f: V→V bisogna:**

    - Scegliere una base di V
    - Scrivere la matrice rappresentativa rispetto alla base scelta
    - Si scrive la matrice **$M_{V}(f) - t\ (I)$** (t una variabile e I è matrice identità)
    - si calcola il determinante e le soluzioni di P_f (t) sono gli autovalori e poi (n=dimensione sp. vett)
    - si consideri **n=dim(V)** allora:
        - se P_f (t) = 0 ha **n soluzioni distinte** = **f diagonalizzabile**
        - se P_f (t) = 0 ha **meno di n soluzioni** anche calcolandole con la loro molteplicità allora f **non è diagonalizzabile**
        - se P_f (t) = 0 **ha alcune soluzioni coincidenti**, ma a patto di **contarle con la loro molteplicità ne ha n** allora **non si può sapere** se è diagonalizzabile o meno

- **Molteplicità algebrica a(λ):** molteplicità di λ come soluzione del polinomio $P_f(t)$
- **autospazio di un autovalore:** si chiama **V_λ := {$\underline{v} \in V$ tali che $f(\underline{v}) = \lambda\underline{v}$}** ovvero l'insieme degli autovettori di V relativi all'autovalore λ.
- **Molteplicità geometrica g(λ):** è la dimensione di V_λ ovvero la **dimensione dell'autospazio di un autovalore. Per trovarla:**
    - si prende la matrice **$M_{V}(f) - t\ (I)$** e si sostituisce a t gli autovalori con molteplicità>1
    - si contano i numero di pivot della matrice ottenuta
    - **$g(\lambda) = n - rk(\ M_{V}(f) - t\ (I)\ )$** (dove n = dim(V))