Algebra

Simone Lidonnici

7 maggio 2024

Indice

1

Relazioni di equivalenza

Definizione di relazione

Una relazione ρ da un insieme A ad un insieme B è un sottoinsieme di $A \times B$:

$$\rho \subseteq A \times B$$

In cui:

$$\mathrm{Dom}(\rho) = \{a \in A | \exists b \in B | a\rho b\}$$
$$\mathrm{Im}(\rho) = \{b \in B | \exists a \in A | a\rho b\}$$

Una relazione da A a B è una funzione se:

- $\mathrm{Dom}(\rho) = A$
- $\forall a \in A\ \exists! b \in B | a\rho b$

Data una relazione si può definire la su inversa:

$$\rho^{-1} \subset B \times A = \{(b, a) \in B \times A | a\rho b\}$$

Se ρ è una funzione non è detto che ρ^{-1} lo sia.

Relazione di equivalenza

Una relazione $\rho \subseteq A \times A$ è una relazione di equivalenza se è:

- Riflessiva: $a\rho a\ \forall a \in A$
- Simmetrica: $a\rho b \implies b\rho a$
- Transitiva: $a\rho b \wedge b\rho c \implies a\rho c$

1.1 Classi di equivalenza

Insieme quoziente

Data una relazione di equivalenza ρ e preso un elemento $a \in A$, tutti gli elementi che sono in relazione con a appartengono ad un insieme chiamato **classe di equivalenza** di a:

$$[a] = \{b \in A | b\rho a\} \subseteq A$$

L'insieme di tutte le classi di equivalenza $\{[a] | a \in A\}$ è detto **insieme quoziente** per ρ e la sua cardinalità è il numero di classi di equivalenza esistenti e si indica con $\frac{A}{\rho}$.

Uguaglianza tra classi di equivalenza

Date due classi di equivalenza $[a]$ e $[b]$, queste due classi sono uguali solo se a è in relazione con b.

$$[a] = [b] \iff a\rho b$$

Dimostrazione:
$[a] = [b] \implies b \in [b] \implies b \in [a] \implies b\rho a \iff a\rho b$
Dimostrazione inversa:
$\forall c \in [a] \implies c\rho a \wedge a\rho b \implies c\rho b \implies c \in [b] \implies [a] \subseteq [b]$
$\forall c \in [b] \implies c\rho b \wedge b\rho a \implies c\rho a \implies c \in [a] \implies [b] \subseteq [a]$
$[a] \subseteq [b] \wedge [b] \subseteq [a] \implies [a] = [b]$

1.2 Partizione di un insieme

Definizione di partizione

Dato un insieme A, una **partizione** di A è una collezione di sottoinsiemi di A per cui:

- $A_\alpha \subseteq A$
- $A_\alpha \cap A_\beta \neq \emptyset \iff \alpha = \beta$
- $A_\alpha \cup A_\beta \cup ... \cup A_\omega = A$

Quindi un qualsiasi insieme quoziente creato da una relazione di equivalenza su A è una partizione di A.

1.3 Relazioni di ordine parziale e totale

Relazione di ordine parziale

Una relazione è di ordine parziale se è:

- Riflessiva
- Antisimmetrica: $a\rho b, b\rho a \implies a = b$
- Transitiva
- Alcuni elementi non possono essere messi in relazione tra di loro

Relazione di ordine totale

Una relazione è di ordine totale se è:

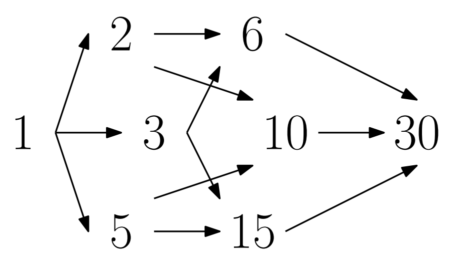
- Riflessiva
- Antisimmetrica: $a\rho b, b\rho a \implies a = b$
- Transitiva
- Tutti gli elementi sono in relazione tra di loro: $\forall a, b \in A \implies a\rho b \lor b\rho a$

1.3.1 Diagramma di Hasse

Preso un insieme (A, ρ) parzialmente ordinato, un elemento a è **coperto** da b e viceversa:

$$a \prec b \iff \nexists x | a\rho x \land x\rho b$$

Per rappresentare graficamente queste relazioni si usa il **diagramma di Hasse**.
Esempio:
$A = \{\text{divisori di } 30\} \subseteq \mathbb{N}$
$A = \{1, 2, 3, 5, 6, 10, 15, 30\}$
$a\rho b \implies$ a divide b $\implies a|b$



2

Numeri naturali

2.1 Terna di Peano

Terna di Peano

Una terna di Peano è una terna $(\mathbb{N}, s, 0)$ in cui:

- $\mathbb{N}$ è un insieme(non inteso i numeri reali)
- s è una funzione $s : \mathbb{N} \to \mathbb{N}$ per cui:
  - $s(0) = 1$
  - $s(n)$ è detto successivo di n
- $0 \in \mathbb{N}$

e che rispetta la seguenti caratteristiche:

- s è iniettiva
- $0 \notin Im(s)$
- Se $U \subseteq \mathbb{N} \wedge 0 \in U \wedge (k \in U \implies s(k) \in U) \implies U = \mathbb{N}$

Si dimostra che se $(\mathbb{N}', s', 0')$ è un'altra terna di Peano allora esiste una funzione sia iniettiva che biettiva:

$$\varphi : \mathbb{N} \to \mathbb{N}' | \varphi(0) = 0' \wedge \varphi(s(n)) = s'(\varphi(n))$$

2.2 Principio del buon ordinamento

Principio del buon ordinamento

Sia $(\mathbb{N}, s, 0)$ una terna di Peano con $n, m \in \mathbb{N}$:

$$n \leq m \iff n = m \vee m = s(s(s(...s(n))))$$

Questa è una relazione di ordine totale.
Da questa relazione possiamo definire il principio del buon ordinamento:

$$\forall X \subseteq \mathbb{N}, X \neq \emptyset \; \exists \text{ un minimo}$$

Da questo teorema possiamo definire:

- Somma
- Prodotto

Inoltre l'insieme $\mathbb{N}$ con relazioni di maggiore uguale, somma e prodotto $(\mathbb{N}, \leq, +, \cdot)$ gode di tutte le proprietà base della matematica.

2.2.1 Definizione di somma

La somma è una funzione $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ che data una coppia di numeri restituisce la somma:

$$f : (n, m) \to n + m$$

La somma ha delle proprietà:

1. $0 + b = b \ \forall b \in \mathbb{N}$
2. $s(a) + b = s(a + b)$

2.2.2 Definizione di prodotto

Il prodotto è una funzione $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ che da una coppia di numeri restituisce il prodotto:

$$f : (n, m) \to n \cdot m$$

Il prodotto a delle proprietà:

1. $0 \cdot b = 0 \ \forall b \in \mathbb{N}$
2. $s(a) \cdot b = a \cdot b + b$

3
Strutture algebriche

Una struttura algebrica è composta da un insieme X e da una o più operazioni binarie, che sono applicazioni:

$$\star : X \times X \to X$$

Esempi:
$(\mathbb{Z}, +)$ è un insieme con un'operazione binaria
$(\mathbb{Z}, \cdot)$ è un insieme con un'operazione binaria

Ci sono diversi tipi di strutture algebriche notevoli:

1. Semigruppo
2. Gruppo
3. Anello
4. Campo

3.1 Semigruppo

Definizione di semigruppo

Un semigruppo è composto da un insieme e da un'operazione $\star$ verificante:

1. $\star$ è associativa: $(s \star s') \star s'' = s \star s' \star s''$
2. esiste un'elemento neutro: $\exists e \in S | e \star s = s \ \forall s$
3. Se $s \star s' = s' \star s$ il semigruppo $(S, \star)$ è commutativo

Un semigruppo generico si scrive $(A, \star)$.

Esempio:
$(\mathbb{N}, +)$ è un semigruppo commutativo avente 0 come elemento neutro

3.2 Gruppo

Definizione di gruppo

Un gruppo è composto da un insieme e da un'operazione $\star$ verificante:

1. $\star$ è associativa: $(s \star s') \star s'' = s \star s' \star s''$
2. esiste un'elemento neutro: $\exists e \in S | e \star s = s \; \forall s$
3. $\forall s \in S \; \exists s' | s \star s' = e = s' \star s$
4. Se $s_1 \star s_2 = s_1 \star s_2 \; \forall s_1, s_2$ il gruppo $(S, \star)$ è commutativo

Un gruppo generico si scrive $(A, \star)$.

Esempio:
$(\mathbb{Z}, +)$ è un gruppo commutativo avente 0 come elemento neutro

3.2.1 Gruppo simmetrico

Definizione di gruppo simmetrico

Dato un insieme X scrivo $S(X)$ l'insieme di tutte le funzioni **biettive** su X:

$$S(X) = \{f : X \to X \text{ biettive}\}$$

Preso $X = [1, n]$, quindi con n elementi, $S(X)$ si scrive S_n ed è un gruppo simmetrico su n elementi.

S_n è composto da permutazioni:

$$S_n = S(\{1, ..., n\}) = \{\sigma : \{1, ..., n\} \to \{1, ..., n\} \text{ biettiva}\}$$

una permutazione σ viene rappresentata come:

$$\sigma : \begin{cases} 1 \to \sigma(1) \\ ... \\ n \to \sigma(n) \end{cases} \implies \begin{pmatrix} 1 & ... & n \\ \sigma(1) & ... & \sigma(n) \end{pmatrix}$$

La cardinalità di S_n: $|S_n| = n!$
Esempio:
$S_3 = \{Id, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$
$|S_3| = 3! = 6$

3.3 Unicità dell'elemento neutro e inverso

Unicità dell'elemento neutro

Dato $s \in S$, l'elemento e tale che:

$$s \star e = s = e \star s \forall s$$

è detto elemento **neutro** ed è unico.
Si denota come 1_S.
Dimostrazione:
Sia $\tilde{e}$ un altro elemento neutro allora:
$\tilde{e} \star e = e = e \star \tilde{e}$ perché $\tilde{e}$ è elemento neutro
$e \star \tilde{e} = \tilde{e} = \tilde{e} \star e$ perché e è elemento neutro
Quindi $e = \tilde{e}$

Inverso

Dato $s \in S$, l'elemento s^{-1} tale che:

$$s \star s^{-1} = e = s^{-1} \star s$$

si dice **reciproco** o **inverso** di s ed è unico.

3.4 Anello

Definizione di anello

Un anello è un insieme dotato di due operazioni $\star, \odot$ con le proprietà:

1. $(A, \odot)$ è un gruppo commutativo con O_A elemento neutro
2. $\star$ è associativa
3. Valgono le proprietà distributive: $(a \odot a') \star b = (a \star b) \odot (a' \star b)$
4. Se $\star$ è commutativo allora l'anello è commutativo
5. Se $\exists u \in A | a \star u = a = u \star a$ allora l'anello è unitario

Un anello privo di divisori dello 0 è un **anello di divisione**.
Un anello generico si scrive $(A, \odot, \star)$.

In un anello risulta sempre:

1. $a \cdot 0 = 0$
2. $a \cdot (-b) = -ab = -a \cdot b$
3. $-a(-b) = ab$

4. $a(b - c) = ab - ac$

Dominio di integrità

Un anello commutativo unitario e privo di divisori dello 0 viene anche detto **dominio di integrità** se:

$$a \star b = O_A \implies a = O_A \vee b = O_A$$

$(\mathbb{Z}, +, \cdot, 0, 1)$ è un dominio di integrità.
In un dominio di integrità vale la legge di cancellazione:

$$ca = cb \implies a = b \; \forall c \neq 0$$

Insieme delle unità

In ogni anello unitario si definisce un gruppo chiamato insieme delle unità:

$$u(A) = \{a \in A | \exists a' | aa' = 1 = a'a\}$$

In $\mathbb{Z}$, $u(\mathbb{Z}) = \{\pm 1\}$.
Il prodotto di due elementi di $u(A)$ appartiene ad $u(A)$:

$$a, b \in u(A) \implies a \cdot b \in u(A)$$

Dimostrazione:
Siano a', b' gli inversi moltiplicativi di a, b.
$a'b'$ inverso di $ab \implies (a'b')(ab) = b'(aa')b = b' \cdot 1 \cdot b = bb' = 1$

3.5 Campo

Definizione di campo

Un campo è un anello commutativo unitario con la seguente proprietà:

$$\forall k \in \mathbb{K}, k \neq 0 \; \exists k' | kk' = 1$$

Si può anche dire:

$$u(\mathbb{K}) = \mathbb{K} \backslash \{0\}$$

Un campo generico si scrive $(\mathbb{K}, +, \cdot)$.

3.5.1 Campo dei numeri razionali

L'insieme dei numeri razionali è definito come:

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z} \backslash \{0\}) / \rho$$

In cui la relazione di equivalenza è:

$$(a, b)\rho(c, d) \implies ad = bc \implies \frac{a}{b} = \frac{c}{d}$$

Gli elementi di $\mathbb{Q}$ sono $[(a,b)]$:
$0 = [(0,1)] = [(0,a)] \forall a \neq 0$
$1 = [(1,1)] = [(a,a)] \forall a \neq 0$
$\mathbb{Q}$ ha 2 operazioni, un elemento neutro additivo e un elemento neutro moltiplicativo, quindi $(\mathbb{Q}, +, \cdot)$ è un anello commutativo unitario. Inoltre è anche un campo perché:

$$[(a,b)] \cdot [(b,a)] = [(ab, ba)] = [(1,1)] = 1$$

$\mathbb{Z}$ sottoinsieme di $\mathbb{Q}$

$\mathbb{Z}$ si definisce come un sottoinsieme di $\mathbb{Q}$ grazie a un'applicazione iniettiva φ:

$$\mathbb{Z} \xrightarrow{\varphi} \mathbb{Q}$$
$$a \xrightarrow{\varphi} (a,1)$$

tale che:

$$\varphi(x +_{\mathbb{Z}} x') = \varphi(x) +_{\mathbb{Q}} \varphi(x) = (x + x', 1)$$
$$\varphi(x \cdot_{\mathbb{Z}} x') = \varphi(x) \cdot_{\mathbb{Q}} \varphi(x') = (xx', 1)$$

$\mathbb{Z}$ è in biezione con un sottoinsieme di $\mathbb{Q}$, cioè $\{[(a,1)], a \in \mathbb{Z}\}$ e questo insieme in $\mathbb{Q}$ è un anello.
Se chiamiamo $a^{-1} = [(1,a)]$ l'inverso di a allora possiamo scrivere tutti gli elementi di $\mathbb{Q}$ come ab^{-1}:

$$[(a,b)] = [(a,1)][(1,b)] = ab^{-1} = \frac{a}{b}$$

3.5.2 Campo dei numeri complessi

Considerando $\mathbb{R}^2 = \{(x,y) | x, y \in \mathbb{R}\}$ e introducendo due operazioni:

- Somma:
$$(x,y) + (x',y') = (x + x', y + y') \text{ con elemento neutro } (0,0)$$
- Prodotto:
$$(x,y)(x',y') = (xx' - yy', xy' + x'y) \text{ con elemento neutro } (1,0)$$

L'inverso di un elemento $(x,y) \neq (0,0)$:

$$(x,y)^{-1} = (\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2})$$

$\mathbb{R}$ sottoinsieme di $\mathbb{C}$

$\mathbb{R}$ si definisce come sottoinsieme di $\mathbb{C}$ grazie a un'applicazione iniettiva φ:

$$\mathbb{R} \xrightarrow{\varphi} \mathbb{C}$$
$$x \xrightarrow{\varphi} (x, 0)$$

tale che:

$$\varphi(x +_{\mathbb{R}} x') = \varphi(x) +_{\mathbb{C}} \varphi(x')$$
$$\varphi(x \cdot_{\mathbb{R}} x') = \varphi(x) \cdot_{\mathbb{C}} \varphi(x')$$

Teorema fondamentale dell'algebra

Ogni equazione algebrica con coefficienti in $\mathbb{C}$ di grado n ammette n soluzioni, non per forza diverse.
Inoltre $\mathbb{C}$ è algebricamente chiuso.

4
Numeri interi

Partendo dall'insieme dei numeri naturali $\mathbb{N}$ costruiamo un'estensione.
Consideriamo $\mathbb{N} \times \mathbb{N}$ e introduciamo una relazione di equivalenza:

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

$\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\rho =$ classi di equivalenza
Ogni (n, m) fa parte di una tra 2 classe di equivalenza:

$$\begin{cases} (n, m) \in [(a, 0)] & n > m \\ (n, m) \in [(0, a)] & n < m \end{cases} \implies \begin{cases} n + 0 = m + a & a = n - m \\ n + a = m + 0 & a = m - n \end{cases}$$

$\mathbb{Z} = (\mathbb{Z}^+ = \{[(a, 0)]|a \in \mathbb{N}\backslash\{0\}\}) + (\mathbb{Z}^- = \{[(0, a)]|a \in \mathbb{N}\backslash\{0\}\}) + (0 = [(0, 0)])$

4.1 Definizione di somma e prodotto

Nei numeri interi la definizione di somma e prodotto sono:

$$[(n, m)] + [(n', m')] = [(n + n', m + m')]$$
$$[(n, m)] \cdot [(n', m')] = [(nn' + mm', nm' + mn')]$$

Inoltre:

1. $n + m = [(n + m, 0)] = [(n, 0)] + [(m, 0)]$
2. $n \cdot m = [(nm, 0)] = [(n, 0)] \cdot [(m, 0)]$
3. $[(n, 0)] + [(0, n)] = 0$
4. $[(n, m)] \cdot [(1, 0)] = [(n, m)]$

Teorema sul resto della divisione

Dati $a, b \in \mathbb{Z}$ con $b \neq 0$:

$$\exists!(q, r) \in \mathbb{Z} \times \mathbb{Z} | a = bq + r$$
$$0 \leq r \leq |b|$$

In cui:

- $a =$ dividendo
- $b =$ divisore
- $q =$ quoziente
- $r =$ resto

Dimostrazione:
Supponiamo $b \geq 0$ e $S = \{a - bx \geq 0, x \in \mathbb{Z}\}$
Se $x = -|a| \implies a - bx = a + b|a| \geq 0 \implies b|a| \geq -a \implies S \neq \emptyset$
Applico il principio del buon ordinamento a S e chiamo r il minimo di S
$r = a - bx \implies a = bq + r$
$r \in S \implies r \geq 0$
Per assurdo $r \geq |b| = b \implies r - b \geq 0 \implies a - bq - b \geq 0 \iff a - b(q + 1) \geq 0 \implies r - b \in S \implies r - b < r \implies$ impossibile

4.2 Numeri primi

Definizione di numero primo

Un numero $p \geq 2$ è primo se i suoi divisori sono solo $\pm 1, \pm p$:

$$\underbrace{p = xy, x \in u(\mathbb{Z}) \implies y \in u(\mathbb{Z})}_{\text{definizione di elemento irriducibile in } (\mathbb{Z},+,\cdot)}$$

Se p è un numero primo:

$$\underbrace{p|xy \wedge p \nmid x \implies p|y}_{\text{definizione di elemento primo in } (\mathbb{Z},+,\cdot)}$$

Dato un elemento $a \in (A, +, \cdot)$:

$$a \text{ primo} \implies a \text{ irriducibile}$$
$$a \text{ irriducibile} \not\Longrightarrow a \text{ primo}$$

4.3 Massimo comun divisore (MCD)

Divisibilità di un numero

Dati $a, b \in \mathbb{Z}$:

$$a|b \iff \exists c \in \mathbb{Z}|b = ac$$

Ha le seguenti proprietà:

1. a ha sempre come divisori $\pm 1, \pm a$
2. $a|0 \ \forall a \in \mathbb{Z}$
3. $0|a \iff a = 0$
4. $a|1 \iff a = \pm 1$
5. Se $a|b$ e $a|c \implies a|(bx + cy) \ \forall x, y$

Definizione di MCD

Dati $(a, b) \in \mathbb{Z} \times \mathbb{Z}, (a, b) \neq (0, 0)$:

$$\exists! d \geq 1| \begin{cases} d|a \text{ e } d|b \\ d'|a \text{ e } d'|b \end{cases} \implies d'|d$$

d è l'unico MCD.
Dimostrazione:
$S = \{ax + by > 0 | x, y \in \mathbb{Z}\} \subseteq \mathbb{N}^*$
$S \neq \emptyset \xRightarrow{\text{buon ordinamento}} \exists d | d \geq x \ \forall x \in S$
$d = ax_0 + by_0$ è il MCD di a e b e $d \geq 1$
$ax + by = dq + r$ con $0 \leq r < d$
$ax + by = (ax_0 + by_0)q + r \implies r = a(x - x_0 q) + b(y - y_0 q)$
Per assurdo $r \in S$ e $r > 0 \implies r < d$ che è il minimo quindi impossibile
Quindi $d|(ax + by) \implies d|a$ e $d|b$

4.3.1 Proprietà

Il minimo comune multiplo ha le seguenti proprietà:

1. $a|b \implies \text{MCD}(a, b) = |a| \ \forall a \neq 0$
2. $\text{MCD}(a, \pm a) = |a|$
3. $\text{MCD}(a, 0) = |a|$
4. $\text{MCD}(\pm 1, b) = 1$
5. $\text{MCD}(ab, ac) = |a| \cdot \text{MCD}(b, c) \ \forall a, b, c \in \mathbb{Z}$
6. $\text{MCD}(a, b) = d \implies \text{MCD}(\frac{a}{d}, \frac{b}{d}) = 1$

Due numeri $a, b \neq (0,0)$ con $\text{MCD}(a,b) = 1$ si dicono **comprimi**.

Lemma di Euclide

Dati $a, b, c \in \mathbb{Z}$:

$$a|bc \wedge \text{MCD}(a,b) = 1 \implies a|c$$

4.3.2 Calcolare il MCD (Algoritmo euclideo)

Dati $a \geq b > 0$ con $a, b \in \mathbb{N}$ per calcolare il $\text{MCD}(a,b)$ seguiamo:

1. $a = bq_1 + r_1 \implies \text{MCD}(a,b) = \text{MCD}(b, r_1)$
   $0 \leq r_1 < b \to \begin{cases} r_1 = 0 \implies \text{MCD}(a,b) = b \\ r_1 > 0 \implies \text{vado al punto 2} \end{cases}$
2. $b = r_1 q_2 + r_2 \implies \text{MCD}(b, r_1) = \text{MCD}(r_1, r_2)$
   $0 \leq r_2 < r_1 \to \begin{cases} r_2 = 0 \implies \text{MCD}(r_1, r_2) = r_1 \\ r_2 > 0 \implies \text{vado al punto 3} \end{cases}$
3. $r_1 = r_2 q_3 + r_3 \implies \text{MCD}(r_1, r_2) = \text{MCD}(r_2, r_3)$
   $0 \leq r_3 < r_2 \to \begin{cases} r_3 = 0 \implies \text{MCD}(r_2, r_3) = r_2 \\ r_3 > 0 \implies \text{vado al punto 4} \end{cases}$

Così abbiamo una successione strettamente decrescente in cui:

$$b > r_1 > r_2 > ... > r_n > r_{n+1} = 0$$
$$\exists n | r_{n+1} = 0 \implies \text{MCD}(a,b) = \text{MCD}(r_n, 0) = r_n$$

Quindi:

$$\text{MCD}(a,b) = \text{MCD}(b, r_1) = \text{MCD}(r_1, r_2) = ... = \text{MCD}(r_n, 0) = r_n$$

Inoltre possiamo trovare:

1. $r_n = r_{n-2} - q_n r_{n-1}$
2. $r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$
3. $\ldots$
4. $r_2 = b - q_2 r_1$
5. $r_1 = a - q_1 b$

Determino tramite il lemma di Bezout x_0 e y_0:

$$r_n = ax_0 + by_0$$

Esempi:
$a = -123$
$b = -39$
$\text{MCD}(-123, -39) = \text{MCD}(123, 39)$

1. $\underbrace{123}_{a} = \underbrace{39}_{b} \cdot \underbrace{3}_{q_1} + \underbrace{6}_{r_1}$
2. $\underbrace{39}_{b} = \underbrace{6}_{r_1} \cdot \underbrace{6}_{q_2} + \underbrace{3}_{r_2}$
3. $\underbrace{6}_{r_1} = \underbrace{3}_{r_2} \cdot \underbrace{2}_{q_3} + \underbrace{0}_{r_3} \implies \text{MCD}(-139, -39) = r_2 = 3$

Per trovare x_0 e y_0:

1. $\underbrace{3}_{r_2} = \underbrace{39}_{b} - \underbrace{6}_{q_2} \cdot \underbrace{6}_{r_1}$
2. $\underbrace{3}_{r_2} = \underbrace{39}_{b} - \underbrace{6}_{q_2} \cdot (\underbrace{123}_{a} - \underbrace{3}_{q_1} \cdot \underbrace{39}_{b}) = -6 \cdot 123 + 19 \cdot 39 =$
   $6 \cdot -123 + (-19 \cdot -39) \implies x_0 = 6, y_0 = -19$

4.4 Minimo comune multiplo

Definizione di mcm

Dati due numeri $a, b \in \mathbb{Z}$:

$$\text{mcm}(a, b) = h$$

Con:

1. $a|h \wedge b|h$
2. Se $a|h' \wedge b|h' \implies h|h'$

Ha delle proprietà:

1. $\text{mcm}(a, 0) = 0$
2. $\text{mcm}(a, \pm 1) = |a|$
3. $\text{mcm}(a, b) = 0 \implies a = 0 \vee b = 0$

4.5 Teorema fondamentale dell'aritmetica

Teorema fondamentale dell'aritmetica

In $\mathbb{N}$:

$$\forall n \in \mathbb{N}, n \geq 2 \implies n \text{ è prodotto di numeri primi}$$
$$n = p_1^{h_1} \cdot p_2^{h_2} \cdot \ldots \cdot p_s^{h_s} \text{ con } s \geq 1, h_i \geq 1$$

In $\mathbb{Z}$:

$$\forall n \in \mathbb{Z}, n \notin [1, -1] \implies n \text{ è prodotto di numeri primi}$$
$$n = (\pm 1) \cdot p_1^{h_1} \cdot p_2^{h_2} \cdot \ldots \cdot p_s^{h_s} \text{ con } s \geq 1, h_i \geq 1$$

Dati due numeri a, b e ammettendo 0 come esponente i due numeri possono sempre essere scritti come prodotto degli stessi numeri primi:

$$a = q_1^{l_1} \cdot \ldots \cdot q_j^{l_j}$$
$$b = q_1^{m_1} \cdot \ldots \cdot q_j^{m_j}$$

Quindi possiamo trovare il $\text{MCD}(a, b)$ e il $\text{mcm}(a, b)$:

$$\text{MCD}(a, b) = q_1^{d_1} \cdot \ldots \cdot q_j^{d_j} \text{ con } d_i = \min(l_i, m_i)$$
$$\text{mcm}(a, b) = q_1^{c_1} \cdot \ldots \cdot q_j^{c_j} \text{ con } c_i = \max(l_i, m_i)$$

4.6 Teoremi su MCD e mcm

MCD per mcm

Dati $a, b \in \mathbb{Z}, (a, b) \neq (0, 0)$:

$$|ab| = \text{MCD}(a, b) \cdot \text{mcm}(a, b)$$

Esistenza dei numeri primi

Esistono infiniti numeri primi.
Dimostrazione per assurdo:
Supponiamo per assurdo che siano finiti: Numeri primi $= \{p_1, p_2, \ldots, p_n\}$
Considero $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$
a fattorizzabile $\implies \exists p_j$ t.c. $p_j | a \implies \exists t | a = tp_j \implies$
$p_j(-(p_1 \cdot \cdots \cdot p_{j-1} \cdot p_{j+1} \cdot \ldots \cdot p_n) + t) = 1 \implies p_j | 1$ impossibile

5

$\mathbb{Z}_n$

Creazione di $\mathbb{Z}_n$

$\mathbb{Z}/_n\mathbb{Z}$ è l'insieme contenenti le classi di equivalenza rispetto alla relazione:

$$a\rho b \iff a - b = kn$$

Scrivendo come $[a]$ la classe che contiene a possiamo scrivere:

$$\mathbb{Z}/_n\mathbb{Z} = \{[0] = [n], [1] = [n+1], ..., [n-1] = [-1]\}$$

$\mathbb{Z}/_n\mathbb{Z} = \mathbb{Z}_n$ e la sua cardinalità è di n elementi.
Un elemento in $\mathbb{Z}_n$ può essere scritto come $[a]_n$
$(\mathbb{Z}_n, +, \cdot)$ è un anello.

5.1 Definizione di somma e prodotto

In $\mathbb{Z}_n$ viene definita la somma:

$$[n] + [m] = [n + m]$$

Dimostrazione:
$\begin{cases} a\rho a' \\ b\rho b' \end{cases} \iff \begin{cases} a - a' = kn \\ b - b' = hn \end{cases} \implies (a+b)\rho(a'+b') \implies (a+b)-(a'+b') = (a-a')+(b-b') = (k+h)n$

In $\mathbb{Z}_n$ viene definita il prodotto:

$$[n] \cdot [m] = [n \cdot m]$$

Dimostrazione:
$(ab)\rho(a'b') \implies ab - a'b' = (a' + kn)(b' + hn) - a'b' = (a'h + b'k + hkn)n$

5.2 Insieme delle unità

In $\mathbb{Z}_n$ il gruppo $u(\mathbb{Z}_n)$:

$$u(\mathbb{Z}_n) = \begin{cases} \mathbb{Z}_n \backslash \{0\} & n \text{ primo} \\ n \cdot \prod_{j=1}^{k} (1 - \frac{1}{p_j}) & n \text{ non primo} \end{cases}$$

In cui p_j è il j-esimo numero primo che compone n.
In $\mathbb{Z}_n$ questo insieme rappresenta anche quello degli invertibili ed è uguale all'insieme dei numeri coprimi con n:

$$u(\mathbb{Z}_n) = \{1 \leq k < n | \, \text{MCD}(k, n) = 1\}$$

5.2.1 Funzione e teorema di Eulero

Funzione di Eulero

La funzione di Eulero φ:

$$\varphi : \mathbb{N} \to \mathbb{N}$$
$$n \to |u(\mathbb{Z}_n)|$$

Rappresenta il numero di elementi coprimi con n, quindi anche la cardinalità dell'insieme delle unità in $\mathbb{Z}_n$.
Dato un numero fattorizzato in numeri primi $n = p_1^{r_1} \cdot ... \cdot p_s^{r_s}$:

$$\varphi(n) = (p_1^{r_1} - p_1^{r_1-1}) \cdot ... \cdot (p_s^{r_s} - p_s^{r_s-1})$$

Teorema di Eulero

Dato un $n \geq 2, a \in \mathbb{Z}$ con $\text{MCD}(a, n) = 1$:

$$a^{\varphi(n)} \equiv 1 \quad (n) \iff [a^{\varphi(n)}]_n = [1]_n$$

Esempio:
Calcolare le ultime 2 cifre di 123^{123}
Dobbiamo calcolare $[123^{123}]_{100} = [123]_{100}^{123} = [23]_{100}^{123}$
Applico Eulero:
$\varphi(100) = \varphi(5^2 \cdot 2^2) = (5^2 - 5)(2^2 - 2) = 40$
$23^{40} = 1(100) \implies [23]_{100}^{123} = [23^{40\cdot 3+3}]_{100} = [23^3]_{100} = [12167]_{100} = 67$

5.3 Equazioni congruenziali

Le equazioni congruenziali si dividono in 3 casi:

- Caso 1 in $\mathbb{Z}$:

$$ax + by = c$$

  Risolvibile se $\text{MCD}(a, b)|c$:

$$\text{Soluzioni}=\begin{cases} x = x_0 \cdot \frac{c}{\text{MCD}(a,b)} + b't \\ y = y_0 \cdot \frac{c}{\text{MCD}(a,b)} - a't \end{cases} \qquad \forall t \in \mathbb{Z}$$

$$b' = \frac{b}{MCD(a, b)}$$

$$a' = \frac{a}{MCD(a, b)}$$

  (x_0, y_0) si trovano con l'algoritmo euclideo

- Caso 1 in $\mathbb{Z}_n$:
$$ax \equiv b \mod n$$
Risolvibile se $\text{MCD}(n,a)|b$:
$$\text{Soluzioni} = x_0 \cdot \frac{b}{\text{MCD}(n,a)} + \frac{n}{\text{MCD}(n,a)} \cdot t$$
$$\forall t \in [0, \text{MCD}(n,a) - 1]$$
x_0 lo trovo con l'algoritmo euclideo
Il numero di soluzioni è $\text{MCD}(n,a)$

- Caso particolare(trovare l'inverso di un numero a) in $\mathbb{Z}_n$:
$$ax \equiv 1 \mod n$$
Risolvibile se $\text{MCD}(n,a) = 1$:
$$\text{Soluzione} = x_0$$

Esempi:
$15x \equiv 18 \mod 24$

1. $24 = 15 + 9$
2. $15 = 9 + 6$
3. $9 = 6 + 3$
4. $6 = 3 \cdot 2 + 0 \implies \text{MCD}(24, 15) = 3|18$

Trovo x_0:
$3 = 9 - 6 = (24 - 15) - (15 - (24 - 15)) = 15 \cdot -3 + 24 \cdot 2 \implies x_0 = -3$
Soluzioni $= -3 \cdot \frac{18}{3} + \frac{24}{3}k = -18 + 8k = 6 + 8k$

$121x \equiv 22\ (33)$
$\text{MCD}(121, 33) = 11|22$
$121x \equiv 22\ (33) \iff 11x \equiv 2\ (3) \iff 2x \equiv 2\ (3) \implies x_0 = 1$
Soluzioni $= 1 + \frac{33}{11}k = 1 + 3k$

5.3.1 Sistemi di equazioni congruenziali

Un sistema di equazioni congruenziali, scritti:
$$\begin{cases} a_1 x \equiv b_1 \quad (n_1) \\ ... \\ a_s x \equiv b_s \quad (n_s) \end{cases}$$
Ammette soluzione se:
$$\text{MCD}(a_i, n_i)|b_i \wedge \text{MCD}(n_i, n_j) = 1$$
Quindi possiamo ricongiungerlo a un sistema di tipo cinese:
$$\begin{cases} x_1 \equiv c_1 \quad (r_1) \\ ... \\ x_s \equiv c_s \quad (r_s) \end{cases} |\ \text{MCD}(r_i, r_j) = 1\ \forall i \neq j$$

In cui:
$r_i = \frac{n_i}{\text{MCD}(a_i,n_i)}$
$c_i = \frac{b_i}{\text{MCD}(a_i,n_i)} \cdot \underbrace{(\frac{a_i}{\text{MCD}(a_i,n_i)})^{-1}}_{\text{inverso di (...)(} \bmod r_i)}$
Questo sistema ha una sola soluzione in $(\mod r_1 \cdot r_2 \cdot ... \cdot r_s)$
Per risolverla scriviamo:
$R = r_1 \cdot r_2 \cdot ... \cdot r_s$ con $R_k = \frac{R}{r_k}$
Risolviamo $R_k x = c_k(r_k)$ e troviamo x_k
La soluzione dell'intero sistema:

$$\tilde{x} = R_1x_1 + ... + R_sx_s$$

Esempio:
$\begin{cases} 8x \equiv 3(5) \\ 8x \equiv 3(7) \\ 8x \equiv 3(11) \end{cases}$
Le singole equazioni sono risolvibili perché:
$\text{MCD}(8,5) = 1|3$
$\text{MCD}(8,7) = 1|3$
$\text{MCD}(8,11) = 1|3$
Il sistema è risolvibile perché:
$\text{MCD}(5,7) = 1$
$\text{MCD}(7,11) = 1$
$\text{MCD}(11,5) = 1$
Il sistema si riconduce a:
$\begin{cases} x \equiv 3 \cdot 2(5) \\ x \equiv 3 \cdot 1(7) \\ x \equiv 3 \cdot 7(11) \end{cases} \xRightarrow{\text{faccio diventare tutti } c_i < n_i} \begin{cases} x \equiv 1(5) \\ x \equiv 3(7) \\ x \equiv 10(11) \end{cases}$
Calcoliamo R_k:
$R = 5 \cdot 7 \cdot 11$
$R_1 = 7 \cdot 11$
$R_2 = 5 \cdot 11$
$R_3 = 5 \cdot 7$
La soluzione quindi è:
$\tilde{x} = R_1x_1 + R_2x_2 + R_3x_3$
$77x_1 \equiv 1(5) \implies 2x_1 \equiv 1(5) \implies x_1 = 3$
$55x_2 \equiv 3(7) \implies 6x_2 \equiv 3(7) \implies -1x_2 \equiv 3(7) \implies x_2 = 4$
$35x_3 \equiv 10(11) \implies 2x_3 \equiv 10(11) \implies x_3 = 5$
$\tilde{x} = 77 \cdot 3 + 55 \cdot 4 + 35 \cdot 5 = 626$

5.3.2 Trasformare equazioni singole in sistemi

Data un'equazione congruenziale:

$$ax \equiv b \quad (n)$$

se n non è primo possiamo fattorizzarlo come:

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot ... \cdot p_n^{r_n}$$

e possiamo scrivere l'equazione come un sistema:

$$\begin{cases} ax \equiv b \quad (p_1^{r_1}) \\ ax \equiv b \quad (p_2^{r_2}) \\ \ldots \\ ax \equiv b \quad (p_n^{r_n}) \end{cases}$$

in cui:

$$\tilde{x}(\text{soluzione del sistema}) = x(\text{soluzione dell'equazione})$$

Esempio:

$$6x \equiv 7 \quad (24) \implies \begin{cases} 6x \equiv 7 \quad (8) \\ 6x \equiv 7 \quad (3) \end{cases}$$

5.4 Piccolo teorema di Fermat

Piccolo teorema di Fermat

Dati p numero primo e $a \in \mathbb{Z}$:

$$a^p \equiv a \quad (p)$$

Dimostrazione per induzione:

1. Caso base:
   $a = 0 \implies 0^p \equiv 0 \ (p)$
2. Passo induttivo:
   Suppongo vero che $a^p \equiv a \ (p)$
3. Dimostrazione induttiva:
   $(a+1)^p \equiv (a^p + 1) \ (p) = (a+1) \ (p)$

Se $\text{MCD}(a, p) = 1$:

$$a^{p-1} \equiv 1 \ (p)$$

Se n è primo allora:

$$u(\mathbb{Z}_n) = \mathbb{Z}_{(n-1)} \iff \mathbb{Z}_n \backslash \{0\} = \{1, a, a^2, ..., a^{n-2}\}$$

6
Teoria dei gruppi

6.1 Sottogruppo

Definizione di sottogruppo

Dato un gruppo $(G, \star)$, un insieme $S \subseteq G$ è un sottogruppo se:

1. $\forall s_1, s_2 \in S \implies s_1 \star s_2^{-1} \in S$
2. $\forall s \in S \implies s^{-1} \in S$

Si denota come $S \leq G$. G viene detto **gruppo ambiente**.

Esempi:
$(\mathbb{R}^* = \mathbb{R} \backslash \{0\}, \cdot) \implies (\mathbb{R}^{>0}, \cdot)$ è un sottogruppo

$(\mathbb{Z}, +) \implies {}_n\mathbb{Z} = \{nk, k \in \mathbb{Z}\} \subseteq \mathbb{Z}$ è un sottogruppo

$(\mathbb{Z}_n, +) \implies d|n \implies \underbrace{\{[d], [2d], ..., [n-d], [n] = [0]\}}_{k \text{ elementi}} \subseteq \mathbb{Z}_n$ è un sottogruppo

Cardinalità dei sottogruppi

Dato $(\mathbb{Z},+)$ e H sottogruppo:

$$H \leq (\mathbb{Z},+) \implies \exists n|_n\mathbb{Z} = H$$
$$H \leq (Z_n,+) \implies \exists d|(d|n)|\{[d],[2d],...,[n-d],[0]\} = H_d = H$$

Preso $\mathbb{Z}_n$ gli H_d sono tutti i sottoinsiemi di $\mathbb{Z}_n$.
Scritto $n = kd$:

$$|H_d| = k$$

Dimostrazione:

1. $H \leq (\mathbb{Z},+)$:
   - $H \cap \mathbb{N}^+ \neq \emptyset \implies \exists n \text{ minimo}|n \in H \cap \mathbb{N}^+ \implies {}_n\mathbb{Z} = \{nk|k \in \mathbb{Z}\} \subseteq H$
   - $\forall a \in H \implies r = a - qn \implies r \in H, r \geq 0 \implies r = 0 \implies a = qn \implies H \subseteq {}_n\mathbb{Z}$

   Dati $H \subseteq {}_n\mathbb{Z} \wedge {}_n\mathbb{Z} \subseteq H \implies H = {}_n\mathbb{Z}$

2. $H \leq (\mathbb{Z}_n,+)$:
   $H' = \{a \in \mathbb{Z}|[a] \in H\} \implies 0, n \in H' \implies H' \neq \emptyset, H \leq \mathbb{Z}$
   $a, b \in H' \implies [a],[b] \in H \xRightarrow{H \leq \mathbb{Z}_n} [a]-[b] \in H \iff a - b \in H'$
   $H' \leq (Z,+) \xRightarrow{(1)} \exists d \in \mathbb{Z}|H' = {}_d\mathbb{Z} \xRightarrow{n \in H} d|n \implies H = H_d$

6.2 Omomorfismi

Definizione di omomorfismo

Un omomorfismo è una mappa tra gruppi:

$$\varphi : (G, \star_1) \to (H, \star_2)$$

che preserva le operazioni dei due gruppi, cioè:

$$\varphi(g \star_1 h) = \varphi(g) \star_2 \varphi(h)$$

Un omomorfismo se è biunivoco è un **isomorfismo**.
L'immagine di φ è un sottogruppo di H:

$$Im(\varphi) = \{\varphi(g), g \in G\}$$

Se φ è iniettiva:

$$\operatorname{Ker}\varphi = \{g \in G|\varphi(g) = 1_H\} = \{1_H\} \equiv \varphi^{-1}(1_H)$$

Per ogni gruppo $(G, \star)$ esiste inoltre una mappa iniettiva $\varphi : (A, \star) \to (S(A), \circ)$ che preserva le operazioni.

$$\varphi(g \star g') = \varphi(g) \circ \varphi(g')$$

Esempio:
Abbiamo un gruppo $(G, \star)$ con $G = \{a, b, c\}$ e $c = 1$ (1 è il simbolo per indicare l'elemento neutro).
Possiamo creare una tabella di moltiplicazione:

$\star$	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

G è commutativo e $G = \{1, a, a^2 | a^3 = 1\}$, quindi $(G, \star)$ è isomorfo a $(\mathbb{Z}_3, +)$

Teorema di isomorfismo

Data una funzione:

$$f : G \to G' \implies G/\operatorname{Ker}(f) \underbrace{\simeq}_{\text{isomorfo}} Im(f)$$

Dimostrazione:
Presa la mappa:

$$\begin{aligned} \pi : G &\to G/H \\ a &\to Ha \end{aligned}$$

π è un omomorfismo di gruppi.
$\pi(aa') = H(aa') = Ha \star Ha' = \pi(a) \star \pi(a')$
$a \rho_f a' \iff f(a) = f(a') \iff f(a)(f(a'))^{-1} = 1_G \xLeftrightarrow{f \text{ omo}} f(a(a)^{-1}) \iff a(a)^{-1} \in \operatorname{Ker}(f) \iff G/\operatorname{Ker}(f) = G/\rho_f$

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & G' \\ G/\rho_f \arrow[r, "F"] & Im(f) \arrow[u, "i\text{=inclusione}"'] \end{tikzcd}$$

$F(Ha) = f(a)$
F è un omomorfismo di gruppi perché:

$$F(Ha \star Hb) = F(Hab) = f(ab) = f(a)f(b) = F(Ha) \cdot F(Hb)$$

6.2.1 Gruppo degli automorfismi

Dato un gruppo G il gruppo degli **automorfismi** su G:

$$\operatorname{Aut}(G) = \{\varphi : G \to G \text{ isomorfismi}\}$$

preso un $x \in G$:

$$\gamma_x : G \to G$$
$$g \to \gamma_x(g) = xgx^{-1}$$

γ_x è un isomorfismo di gruppi.
Questi isomorfismi sono componibili cioè:

$$\gamma_x \gamma_y = \gamma_{xy}$$
$$\gamma_x(\gamma_y(a)) = \gamma_x(yay^{-1}) = xyay^{-1}x^{-1} = \gamma_{xy}$$

Il nucleo di γ:

$$\text{Ker}(\gamma) = \{x \in G | \gamma_x = Id : G \to G\} = \{x \in G | xax^{-1} = a \; \forall a \in G\}$$

Questo gruppo viene chiamato **centro** di G e Ker $\trianglelefteq G$.
Se G è commutativo allora $G = \text{Ker}(G)$.

6.3 Gruppi ciclici

Generatore di un gruppo ciclico

Dato un gruppo G e un elemento $g \in G$ e $t \in \mathbb{Z}$:

$$< g >= g^t = \begin{cases} 1_G & t = 0 \\ \underbrace{g \star \dots \star g}_{t \text{ volte}} & t > 0 \\ \underbrace{g^{-1} \star \dots \star g^{-1}}_{|t| \text{ volte}} & t < 0 \end{cases}$$

g^t è un sottogruppo di G e si dice che G è generato da g.
L'ordine di g è uguale:

$$o(g) = \min(\{n \geq 1 | g^n = 1_G = \text{elemento neutro}\})$$

Se questo minimo non esiste allora g ha ordine ∞.

Definizione di gruppo ciclico

Dato un gruppo $(G, \star)$ è ciclico se:

$$\exists g \in G | G =< g >$$

Se $H \leq G$ ciclico allora H è ciclico:

$$\exists h \in H | H =< h >$$

Se G è **ciclico** allora è anche **commutativo**.

Esempio:
$(\mathbb{Z}, +)$ è ciclico perché $\mathbb{Z} =< 1 >=< -1 >$
$\mathbb{Z}$ è anche l'unico gruppo ciclico con $o(g) = \infty$

6.3.1 Struttura dei gruppi ciclici

I gruppi ciclici posso essere di due tipi:

$$G =< g > \implies \begin{cases} o(g) = \infty \\ o(g) = n \end{cases}$$

1. Caso 1:

$$\varphi : \mathbb{Z} \to G$$
$$m \to g^m$$

   φ è un isomorfismo, cioè è sia iniettiva che suriettiva.
   Dimostrazione:

   - $o(g) = \infty \implies \operatorname{Ker} \varphi = \{m \in \mathbb{Z} | g^m = 1_G\} = \{0\} \implies \varphi$ è iniettiva
   - $< g >= \{g^t | t \in \mathbb{Z}\} \implies g^k = \varphi(k) \implies \varphi$ è suriettiva

2. Caso 2:

$$\varphi : \mathbb{Z}_n \to G$$
$$[m] \to g^m$$

   φ è ben definita:

$$[m]_n = [m']_n \iff m' = m + nk \implies g^{m'} = g^{m+nk} = g^m \cdot 1_G = g_m$$

   φ è un isomorfismo quindi $|G| = |\mathbb{Z}_n|$.
   Dimostrazione:
   $G = \{1, g, g^2, ..., g^{n-1}\} \implies \varphi$ è suriettiva e iniettiva

6.4 Teorema di Lagrange

6.4.1 Gruppi generici

Definizione di classi laterali

Dato un gruppo G e $H \leq G$:

- la **classe laterale sinistra** associata ad $a \in G$:

$$aH = \{a \star k, k \in H\} \subseteq G$$

- La **classe laterale destra**:

$$Ha = \{k \star a, k \in H\} \subseteq G$$

Se G non è commutativo:

$$aH \neq Ha$$

Dimostrazione:
Esiste una biezione:

$$H \rightarrow aH$$
$$h \rightarrow ah$$

Quindi:
$|H| = |aH|$ e $\{a_1 H, a_2 H, ..., a_i H\}$ sono classi laterali sinistre distinte.

$|G| = n \implies n = \sum_{j=i}^{i} |a_j H| \implies G = \bigcup_{j=1}^{i} (a_j H)$

$|H| = |aH| \implies n = i \cdot H$

Esempio:
S_3

$H = \{1, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\}$

$H \leq S_3, a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$aH = \{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\}$

$Ha = \{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\}$

Partizioni di classi laterali

Dati $a, b \in G$:

- Le classi laterali sinistre formano una partizione di G, $\mathcal{L}_s$ con proprietà:
  1. $aH = bH \iff a^{-1}b \in H$
  2. $a, b \in G \implies aH = bH \vee aH \cap bH = \emptyset$
  3. $\forall x \in G\ \exists a \in G | x \in aH$

  La partizione $\mathcal{L}_s$ definisce una relazione ρ_s:

  $$a\rho_s b \iff \exists g \in G | a, b \in gH$$

  Quindi:

  $$a\rho_s b \iff a^{-1}b \in H$$
  $$a\rho_s b \iff aH \cap gH \neq \emptyset \wedge bH \cap gH \neq \emptyset \iff aH = gH = bH$$

- Le classi laterali destre formano una partizione di G, $\mathcal{L}_d$ con proprietà:
  1. $Ha = Hb \iff a^{-1}b \in H$
  2. $a, b \in G \implies Ha = Hb \vee Ha \cap Hb = \emptyset$
  3. $\forall x \in G\ \exists a \in G | x \in Ha$

  La partizione $\mathcal{L}_d$ definisce una relazione ρ_d:

  $$a\rho_d b \iff \exists g \in G | a, b \in Hg$$

  Quindi:

  $$a\rho_d b \iff a^{-1}b \in H$$
  $$a\rho_d b \iff Ha \cap Hg \neq \emptyset \wedge Hb \cap Hg \neq \emptyset \iff Ha = Hg = Hb$$

6.4.2 Gruppi finiti

Teorema di Lagrange

Dato un gruppo G con $o(g) = n$ con $H \leq G$:

$$|H| \underbrace{\mid}_{\text{divide}} |G|$$

Preso un k:

$$\forall k|k|n \ \exists! H \leq G||H| = k$$
$$H =< g^{\frac{n}{k}} >$$

Se $h|k$:

$$< g^{\frac{n}{h}} > \leq < g^{\frac{n}{k}} >$$

6.5 Sottogruppi normali

Definizione di sottugruppo normale

Dato un gruppo G e $H \leq G$, H è un **sottogruppo normale** se:

$$H \trianglelefteq G \iff \rho_d = \rho_s \iff aH = Ha \ \forall a \in G$$

Per controllare se H è normale:

$$H \trianglelefteq G \iff aha^{-1} \in H \ \forall a \in G, \forall h \in H$$

Se G è commutativo allora ogni $H \leq G$ è normale.
Dimostrazione:

$$H \trianglelefteq G \implies aH = Ha \implies \begin{cases} ah = h'a & \text{per un qualche } h' \\ ha = ah'' & \text{per un qualche } h'' \end{cases} \implies \begin{cases} aha^{-1} = h' \in H \\ a^{-1}ha = h'' \in H \end{cases}$$

$$aha^{-1} = h' \implies ah = h'a \implies \begin{cases} aH \subseteq Ha \\ Ha \subseteq aH \end{cases}$$

Data una funzione f:

$$f : G \to G' \implies \mathrm{Ker}(f) = \{g \in G | f(g) = 1_G\} \trianglelefteq G$$

6.5.1 Gruppo quoziente per un sottogruppo normale

In un gruppo G finito il numero di classi laterali destre è uguale al numero di classi laterali sinistre, questo gruppo è il gruppo quoziente e si denota G/H. Il numero di queste classi laterali determina l'indice di H in G che si denota come $[G : H]$. L'indice può essere anche calcolato come $\frac{|G|}{|H|}$.
Inoltre:

$$[G : H] \cdot |H| = |G|$$

Dimostrazione:

$$\begin{aligned} \varphi : \mathcal{L}_d(H) &\to \mathcal{L}_s(H) \\ Ha &\to a^{-1}H \end{aligned}$$

φ è biettiva quindi ha un inverso:

$$\begin{aligned} \varphi^{-1} : \mathcal{L}_s(H) &\to \mathcal{L}_d(H) \\ aH &\to Ha^{-1} \end{aligned}$$

Relazione di equivalenza compatibile

Una relazione di equivalenza ρ è compatibile con l'operazione in un gruppo G se:

$$\left.\begin{matrix} a\rho a' \\ b\rho b' \end{matrix}\right\} \implies ab\rho a'b'$$

Se ρ è compatibile allora nell'insieme delle classi di equivalenza G/ρ:

$$[a] \star [b] = [a \cdot b]$$

Quindi $(G/\rho, \star)$ è un gruppo con elemento neutro 1_G e inverso di $[b] = [b^{-1}]$.
Anche $(G/H, \star) = (G/\rho_d, \star) = (G/\rho_s, \star)$ è un gruppo con elemento neutro H e inverso di $aH = a^{-1}H$.

7

Permutazioni

7.1 Supporto di una permutazione

Definizione di supporto

Presa una permutazione $\sigma \in S_n$ il supporto di σ:

$$\text{Supp}(\sigma) = \{j \in \{1, .., n\} | \sigma(j) \neq j\}$$

Preso un elemento esterno al supporto:

$$x \in [\{1, ..., n\} - \text{Supp}(\sigma)] \implies \sigma(x) = x$$

Prese due mappe σ, τ:

$$\text{Supp}(\sigma) \cap \text{Supp}(\tau) = \emptyset \implies \sigma\tau = \tau\sigma$$

Esempi:

- Trasposizione con 2 elementi:

$$\sigma(i, j) \implies \begin{cases} 1 \to 1 \\ ... \\ i \to j \\ j \to i \\ ... \\ n \to n \end{cases} \implies \text{Supp}(\sigma) = \{i, j\} \implies o(\sigma) = 2$$

- Trasposizione con k elementi:

$$\sigma(j_1, ..., j_k) \implies \begin{cases} 1 \to 1 \\ ... \\ j_1 \to j_2 \\ j_2 \to j_3 \\ ... \\ j_n \to j_1 \\ ... \\ n \to n \end{cases} \implies \text{Supp}(\sigma) = \{j_1, ..., j_k\} \implies o(\sigma) = k$$

7.2 Decomposizione di una permutazione

Ogni permutazione σ può essere scritta in modo unico come un prodotto di cicli (freccie che collegano un elemento a se stesso attraverso altri elementi) con supporto disgiunto a coppie:

$$\sigma = \sigma_1 \cdot ... \cdot \sigma_k | \operatorname{Supp}(\sigma_i) \cap \operatorname{Supp}(\sigma_j) = \emptyset$$

L'ordine di una permutazione σ data la sua decomposizione:

$$d_j = o(\sigma_j) = \text{numero di elementi in } \sigma_j$$
$$o(\sigma) = \text{mcm}(d_1, ..., d_k)$$

Esempio:
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 4 & 1 & 2 \end{pmatrix}$
Può essere decomposta in 3 cicli:

- $1 \to 3 \to 5 \to 1 = (1\ 3\ 5)$
- $2 \to 6 \to 2 = (2\ 6)$
- $4 \to 4 = (4)$

Quindi possiamo scrivere σ (si omettono gli elementi da soli):
$\sigma = (1\ 3\ 5)(2\ 6) \implies \operatorname{Supp}(\sigma) = \{1, 2, 3, 5, 6\}$
$\text{mcm}(3, 2) = 6$

7.3 Coniugazioni

Elementi coniugati in un gruppo

Dato un gruppo G, diciamo che x è coniugato a y se:

$$\exists g \in G | x = gyg^{-1} = \gamma_g(y)$$

Se in S_n coniughiamo una permutazione σ ad un'altra permutazione τ:

$$\tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1}) \cdot ... \cdot (\tau\sigma_k\tau^{-1})$$

Per ogni $\sigma_i = \{j_1^i, ..., j_k^i\}$:

$$\tau(j_1, ..., j_k)\tau^{-1} \to \begin{cases} j \xrightarrow{\tau^{-1}} j_t \xrightarrow{\sigma} j_{t+1} \xrightarrow{\tau} \tau(j_{t+1}) \\ j \xrightarrow{\tau^{-1}} x \notin \{j_1, ..., j_k\} \xrightarrow{\sigma} x \xrightarrow{\tau} j \end{cases}$$

Il risultato quindi è:

$$\tau\sigma_i\tau^{-1} = (\tau(j_1)\tau(j_2)...\tau(j_k))$$

Il risultato ha lo stesso ordine di σ:

$$o(\tau\sigma\tau^{-1}) = o(\sigma)$$

Esempio:
$\sigma = (1\ 3\ 5)(2\ 6)$
$\tau = (1\ 2\ 3\ 4\ 5\ 6)$
$\tau^{-1} = (1\ 6\ 5\ 4\ 3\ 2)$
$\tau\sigma\tau^{-1} = [\tau(1\ 3\ 5)][\tau^{-1} \cdot \tau(2\ 6)\tau^{-1}] = [\tau(1)\tau(3)\tau(5)][\tau(2)\tau(6)] = (2\ 4\ 6)(3\ 1)$

Coniugazione tra due permutazioni

Prese due permutazioni $\sigma, \sigma' \in S_n$, se sono divise in cicli della stessa lunghezza allora sono coniugati:

$$\sigma = \sigma_1 ... \sigma_k \implies d_j = o(\sigma_j) | i < j \implies d_i < d_j$$
$$\sigma' = \sigma'_1 ... \sigma'_k \implies d'_j = o(\sigma'_j) | i < j \implies d'_i < d'_j$$
$$d_j = d'_j \ \forall j \in [1, k] \implies \sigma \text{ coniugato con } \sigma'$$

Esempio:
$\sigma = (1\ 3\ 5)(2\ 6)(4)$
$\sigma' = (2\ 3\ 5)(1\ 4)(6)$
Quindi τ sarà:
$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 6 & 5 & 4 \end{pmatrix} \implies (1\ 2)(4\ 6)$

7.4 Decomposizione in trasposizioni

Una permutazione σ può essere divisa in un prodotto di trasposizioni di 2 elementi:

$$\sigma = \tau_1 \cdot ... \cdot \tau_k$$

Questa divisione non è unica al contrario di quella in cicli.
Qualsiasi trasposizione $\tau = (j_1\ j_2)^2 = Id$
Se il numero di trasposizioni è pari si dice che la permutazioni è **pari**, altrimenti si dice **dispari**.
Il gruppo delle permutazioni pari è un sottogruppo e ha indice 2 (quindi è normale):

$$A = \{\sigma : \text{permutazione pari}\} \trianglelefteq S_n$$

Questo sottogruppo si chiama **gruppo alterno**.

8

Sistemi di equazioni lineari

8.1 Matrici

Una matrice $A = m \times n$ con coefficienti in $\mathbb{R}$ è una tabella di m righe e n colonne:

$$A = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{vmatrix}$$

Le righe vengono denotate $A^i = i$-esima riga
Le colonne vengono denotate $A_i = i$-esima colonna

8.1.1 Tipi di matrici

Matrici quadrate e triangolari

Se una matrice ha $m = n$ si dice **quadrata**:

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$$

Una matrice quadrata si dice **triangolare superiore** se:

$$a_{ij} = 0 \quad \forall i > j \implies \begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ 0 & a_{22} & a_{23} & a_{24} & a_{25} \\ 0 & 0 & a_{33} & a_{34} & a_{35} \\ 0 & 0 & 0 & a_{44} & a_{45} \\ 0 & 0 & 0 & 0 & a_{55} \end{vmatrix}$$

Si dice **triangolare inferiore** se:

$$a_{ij} = 0 \quad \forall i < j \implies \begin{vmatrix} a_{11} & 0 & 0 & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 & 0 \\ a_{31} & a_{32} & a_{33} & 0 & 0 \\ a_{41} & a_{42} & a_{43} & a_{44} & 0 \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{vmatrix}$$

Matrici a scala

Una matrice si dice a **scala** se in ogni riga il primo numero diverso da 0 è più a destra della riga precedente:

$$\begin{array}{c} \begin{matrix} j_1 & \dots & j_2 & \dots & \dots & j_3 & \dots & j_r \end{matrix} \\ \begin{vmatrix} p_1 & & & & & & & \\ 0 & 0 & p_2 & & & & & \\ 0 & 0 & 0 & 0 & 0 & p_3 & & \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & p_r \end{vmatrix} \end{array}$$

Ogni indice j_i indica la riga dell'i-esimo pivot.

Matrici simmetriche e antisimmetriche

Una matrice $A = n \times n$ si dice:

- **Simmetrica** se $a_{ij} = a_{ji} \; \forall i, j$
$$\begin{vmatrix} b & a & c \\ a & d & e \\ c & e & f \end{vmatrix}$$
- **Antisimmetrica** se $a_{ij} = -a_{ji} \; \forall i, j$ (la diagonale principale sarà tutta composta da 0)
$$\begin{vmatrix} 0 & a & c \\ -a & 0 & e \\ -c & -e & 0 \end{vmatrix}$$

Matrici trasposte

Presa una matrice quadrata $A = n \times n$ la sua trasposta A^T è una matrice in cui le righe sono scambiate con le colonne, cioè $a_{ij} = a_{ji}$:

$$A = \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} \implies A^T = \begin{vmatrix} a & d & g \\ b & e & h \\ c & f & i \end{vmatrix}$$

8.2 Sistemi lineari come matrici

Dato un sistema di equazioni lineari (di 1° grado):

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{cases}$$

Questo sistema può essere associato alla matrice dei coefficienti del sistema:

$$A = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{vmatrix}$$

I termini noti si possono scrivere in una m-pla:

$$\underline{b} = \begin{vmatrix} b_1 \\ b_2 \\ \dots \\ b_m \end{vmatrix}$$

Le coordinate si possono scrivere in una n-pla:

$$\underline{x} = \begin{vmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{vmatrix}$$

Un sistema si denota con $A\underline{x} = \underline{b}$.

Equivalenza di sistemi lineari

Due sistemi $A\underline{x} = \underline{b}$ e $A'\underline{x} = \underline{b}'$ sono equivalenti se hanno le stesse soluzioni:

$$\Sigma = \{\underline{x} \in \mathbb{R}^n | A\underline{x} = \underline{b}\}$$
$$\Sigma' = \{\underline{x} \in \mathbb{R}^n | A'\underline{x} = \underline{b}'\}$$
$$A\underline{x} = \underline{b} \equiv A'\underline{x} = \underline{b}' \iff \Sigma = \Sigma'$$

8.3 Metodo di Gauss

Teorema alla base del Metodo di Gauss

Dato un sistema lineare $m \times n$:

$$A\underline{x} = \underline{b}$$

Prese due equazioni del sistema:

$$\begin{aligned} \alpha_1 x_1 + ... + \alpha_n x_n = \beta \\ \alpha_1' x_1 + ... + \alpha_n' x_n = \beta' \end{aligned}$$

Questo sistema è equivalente al sistema $\tilde{A}\underline{x} = \tilde{\underline{b}}$ ottenuto sostituendo alla seconda equazione l'equazione:

$$h(\alpha_1 x_1 + ... + \alpha_n x_n) + k(\alpha_1' x_1 + ... + \alpha_n' x_n) = h\beta + k\beta \qquad \forall k \neq 0$$

Dimostrazione per doppia conclusione:

1. $\Sigma \subseteq \tilde{\Sigma}$:
   Prendiamo una n-pla $\underline{y} \in \Sigma$ che soddisfa il sistema e quindi le due equazioni, quindi:
   $\left.\begin{aligned} \alpha_1 y_1 + ... + \alpha_n y_n - \beta = 0 \\ \alpha_1' y_1 + ... + \alpha_n' y_n - \beta' = 0 \end{aligned}\right\} \implies$
   $h(\alpha_1 y_1 + ... + \alpha_n y_n - \beta) + k(\alpha_1' y_1 + ... + \alpha_n' y_n - \beta') = 0 \implies \underline{y}$ soddisfa la nuova equazione $\implies \Sigma \subseteq \tilde{\Sigma}$

2. $\tilde{\Sigma} \subseteq \Sigma$:
   Prendiamo una n-pla $\underline{z} \in \tilde{\Sigma}$ che soddisfa il secondo sistema, quindi:
   $\alpha_1 z_1 + ... + \alpha_n z_n - \beta = 0 \implies \underbrace{h(\alpha_1 z_1 + ... + \alpha_n z_n - \beta)}_{=0} + k(\alpha_1' z_1 + ... + \alpha_n' z_n) =$
   $k\beta' \xRightarrow{k \neq 0} \underline{z}$ soddisfa la nuova equazione $\implies \tilde{\Sigma} \subseteq \Sigma$

8.3.1 Trasformare un sistema quadrato in triangolare

Ogni sistema quadrato è equivalente ad un sistema triangolare superiore o inferiore. Per trasformarlo seguiamo dei passaggi ciclicamente per ogni colonna j:

1. Per ogni colonna j prendiamo il coefficiente sulla diagonale(cioè in posizione a_{ij} con $i = j$) nel caso sia $\neq 0$, sennò scambiamo la riga con la prima riga più in basso nella colonna j in cui il coefficiente è $\neq 0$ e lo chiamiamo $a_{ij} = p_j$

2. Troviamo un valore $k_j = -(\dfrac{a_{i+1,j}}{p_j})$

3. Per ogni valore della matrice $a_{i'j'} | i' > i \land j' \geq j \implies a_{i'j'} = a_{i'j'} + a_{i,j'} \cdot k_j$

4. Cambiamo i valori della matrice $\underline{b}$ con $b_{i'} = b_{i'} + b_i \cdot k_j$

5. Nel caso non tutti i coefficienti sotto p_1 siano 0, ripetiamo il procedimento sempre nella colonna j

Eseguendo questi passi in ciclo arriveremo ad ottenere una matrice triangolare superiore.

8.4 Risolvere un sistema lineare

8.4.1 Soluzioni di un sistema triangolare

Dato un sistema triangolare superiore $T\underline{x} = \underline{b}$ con:

$$T = \begin{vmatrix} t_{11} & t_{12} & t_{13} & ... & t_{1n} \\ 0 & t_{22} & t_{23} & ... & t_{2n} \\ ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & t_{nn} \end{vmatrix} \qquad \underline{b} = \begin{vmatrix} b_1 \\ b_2 \\ ... \\ b_n \end{vmatrix}$$

Possiamo risolvere il sistema trovando x_n e sostituendolo nella riga sopra trovando x_{n-1} e continuando così.
Il sistema ha una sola soluzione se:

$$t_{ii} \neq 0 \quad \forall i = [i, n]$$

Sennò non ammette soluzione o ne ammette infinite (per sapere in quale dei due casi siamo bisogna conoscere gli spazi vettoriali)

8.4.2 Soluzioni di un sistema non quadrato

Dato un sistema non quadrato a scala:

$$\begin{cases} p_1x_1 + a_{12}x_2 + a_{13}x_3 + ... + a_{1n}x_n = b_1 \\ \qquad\qquad\qquad p_2x_3 + ... + a_{2n}x_n = b_2 \\ ... \\ \qquad\qquad\qquad\qquad\qquad p_rx_n = b_n \end{cases}$$

Per risolverlo sposto tutte le variabili non moltiplicate per un p_i dall'altra parte e le considero come parametri $t_1, ..., t_n$ calcolando le altre variabili. Per sostituzione faccio diventare tutte le variabili nella forma $x_i = j_i + \alpha_1 t_1 + ... + \alpha_n t_n$.
Scriviamo poi il risultato sotto forma:

$$\begin{vmatrix} x_1 \\ x_2 \\ ... \\ x_n \end{vmatrix} = \begin{vmatrix} j_1 \\ j_2 \\ ... \\ j_n \end{vmatrix} + t_1 \begin{vmatrix} \alpha_{11} \\ \alpha_{12} \\ ... \\ \alpha_{1n} \end{vmatrix} + ... + t_n \begin{vmatrix} \alpha_{r1} \\ \alpha_{r2} \\ ... \\ \alpha_{rn} \end{vmatrix}$$

Esempio:

$$\begin{cases} x_2 - x_3 + 3x_4 - x_5 + \frac{1}{2}x_6 = 1 \\ 2x_4 - x_6 = 0 \\ x_5 + x_6 = 1 \end{cases}$$

Porto a destra x_3, x_6 (cha non sono pivot):

$$\begin{cases} x_2 + 3x_4 - x_5 = 1 + x_3 - \frac{1}{2}x_6 \\ 2x_4 = x_6 \\ x_5 = 1 - x_6 \end{cases}$$

Rinomino i parametri:

$$\begin{cases} x_1 = t_1 \\ x_3 = t_2 \\ x_6 = t_3 \end{cases}$$

A questo punto risolvo le altre in funzione di questi parametri:

$$\begin{cases} x_2 + 3x_4 - x_5 = 1 + t_2 - \frac{1}{2}t_3 \\ 2x_4 = t_3 \\ x_5 = 1 - t_3 \end{cases} \implies \begin{cases} x_2 = -3(\underbrace{\frac{1}{2}t_3}_{x_4}) + (\underbrace{1 - t_3}_{x_5}) + 1 + t_2 - \frac{1}{2}t_3 \\ x_4 = \frac{1}{2}t_3 \\ x_5 = 1 - t_3 \end{cases}$$

Risolvo tutte le x:

$$\begin{cases} x_1 = t_1 \\ x_2 = 2 + t_2 - 3t_3 \\ x_3 = t_2 \\ x_4 = \frac{1}{2}t_3 \\ x_5 = 1 - t_3 \\ x_6 = t_3 \end{cases}$$

Ora posso cambiarla e scriverla in forma:

$$\begin{vmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{vmatrix} = \begin{vmatrix} 0 \\ 2 \\ 0 \\ 0 \\ 1 \\ 0 \end{vmatrix} + t_1 \begin{vmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{vmatrix} + t_2 \begin{vmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{vmatrix} + t_3 \begin{vmatrix} 0 \\ -3 \\ 0 \\ \frac{1}{2} \\ -1 \\ 1 \end{vmatrix}$$

Proprietà di un sistema a scala

Dato un sistema lineare $A\underline{x} = \underline{b}$ e $S\underline{x} = \underline{b}$ la sua riduzione a scala ha diverse proprietà:

- $\{\underline{x} | A\underline{x} = \underline{b}\} = \{\underline{x} | S\underline{x} = \underline{c}\}$
- $\text{Ker}(A) = \text{Ker}(S)$
- $\text{rg}(A) = \text{rg}(S)$
- Prese le colonne con pivot $S^{j_1}, ..., S^{j_r}$:
  - $\{S^{j_1}, ..., S^{j_r}\}$ è una base per $\text{Im}(S) = \text{Span}(\text{colonne di } S)$
  - $\{A^{j_1}, ..., A^{j_r}\}$ è una base per $\text{Im}(A) = \text{Span}(\text{colonne in } A)$

8.4.3 Tutte le soluzioni di un sistema lineare

Dato un sistema di equazioni lineari $A\underline{x} = \underline{b}$ con:

$$\Sigma = \{\underline{x} | A\underline{x} = \underline{b}\}$$
$$\Sigma_0 = \{\underline{x} | A\underline{x} = \underline{0}\}$$

Trovata una soluzione del sistema $\underline{x}'$, posso trovare tutte le soluzioni:

$$\Sigma = \underline{x}' + \Sigma_0$$

9
Spazi vettoriali

Definizione di spazio vettoriale

Uno **spazio vettoriale** $(V, +, \underline{0}, \cdot)$ su $\mathbb{R}$ se $(V, +, \underline{0})$ è un gruppo commutativo con $+$ operazione interna:

$$+ : V \times V \to V$$
$$(\underline{v}, \underline{w}) \to \underline{v} + \underline{w}$$

Inoltre c'è un'operazione esterna $\cdot$ prodotto scalare:

$$\cdot : \mathbb{R} \times V \to V$$
$$(\alpha, \underline{v}) \to \alpha\underline{v}$$

Il prodotto scalare è commutativo e distributivo.

Esempio:
$(\mathbb{R}^n, +, \underline{0}, \cdot)$

$\underline{x} \in R^n = \begin{vmatrix} x_1 \\ \dots \\ x_n \end{vmatrix}$

$\underline{0} = \begin{vmatrix} 0 \\ \dots \\ 0 \end{vmatrix}$

$\underline{x} + \underline{y} = \begin{pmatrix} x_1 + y_1 \\ \dots \\ x_n + y_n \end{pmatrix}$

$\lambda\underline{x} = \begin{pmatrix} \lambda x_1 \\ \dots \\ \lambda x_n \end{pmatrix}$

9.1 Sottospazi vettoriali

Definizione di sottospazio vettoriale

Dato uno spazio vettoriale V con W sottoinsieme di V, allora W è un **sottospazio vettoriale** di V se:

1. $\forall \underline{w}, \underline{w}' \in W \implies \underline{w} + \underline{w}' \in W$
2. $\forall \underline{w} \in W, \forall \lambda \in \mathbb{R} \implies \lambda \underline{w} \in W$

Si denota come $W \leq V$.

Sottospazio vettoriale di un sistema lineare omogeneo

Data una matrice $A = m \times n$ associata ad un sistema lineare omogeneo, cioè in cui tutti i termini noti sono nulli, allora $\Sigma_0 = \{\underline{x} \in \mathbb{R}^n | A\underline{x} = \underline{0}\}$ è un sottospazio vettoriale di $\mathbb{R}^n$.
Dimostrazione:

1. $\underline{x}, \underline{x}' \in \Sigma_0 \implies \underline{x} + \underline{x}' \in \Sigma_0$:
   Se queste sono due soluzioni allora possiamo dire che:

$$\begin{cases} (a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n) + (a_{11}x'_1 + a_{12}x'_2 + ... + a_{1n}x'_n) = 0 \\ ... \\ (a_{n1}x_1 + a_{n2}x_2 + ... + a_{nn}x_n) + (a_{n1}x'_1 + a_{n2}x'_2 + ... + a_{nn}x'_n) = 0 \end{cases}$$

   Applicando la proprietà distributiva:

$$\begin{cases} a_{11}(x_1 + x'_1) + a_{12}(x_2 + x'_2) + ... + a_{1n}(x_n + x'_n) = 0 \\ ... \\ a_{n1}(x_1 + x'_1) + a_{n2}(x_2 + x'_2) + ... + a_{nn}(x_n + x'_n) = 0 \end{cases}$$

   Quindi $\underline{x} + \underline{x}' \in \Sigma_0$

2. $\underline{x} \in \Sigma_0, \lambda \in \mathbb{R} \implies \lambda \underline{x} \in \Sigma_0$:
   Prendendo il sistema e moltiplicando per λ:

$$\begin{cases} \lambda(a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n) = 0 \\ ... \\ \lambda(a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n) = 0 \end{cases}$$

   Applicando la proprietà distributiva:

$$\begin{cases} \lambda a_{11}x_1 + \lambda a_{12}x_2 + ... + \lambda a_{1n}x_n = 0 \\ ... \\ \lambda a_{m1}x_1 + \lambda a_{m2}x_2 + ... + \lambda a_{mn}x_n = 0 \end{cases}$$

   Quindi $\lambda \underline{x} \in \Sigma_0$

9.2 Combinazioni lineari

E

Esercizi

E.1 Esercizi su $\mathbb{Z}$ e $\mathbb{Z}_n$

E.1.1 Calcolare il MCD e x_0, y_0

$$\text{MCD}(a, b) \text{ con } a \leq b$$

1. Scrivo $b = k_1 a + r_1$
2. Scrivo $a = k_2 r_1 + r_2$
3. Scrivo $r_1 = k_3 r_2 + r_3$
4. Continuo a scrivere $r_{n-1} = k_i r_n + r_{n+1}$ finché $r_{n+1} = 0$ e il $\text{MCD}(a, b) = r_n$

Nel caso di numeri negativi $\text{MCD}(-a, -b) = \text{MCD}(a, b)$

$$x_0, y_0 | a x_0 + b y_0 = \text{MCD}(a, b)$$

1. Scrivo $\text{MCD}(a, b) = r_{n-2} - k_1 r_{n-1}$
2. Sostituisco $r_{n-1} = r_{n-3} - k_2 r_{r-2}$
3. Continuo a sostituire $r_i = r_{i-2} - k_j r_{i-1}$ finché $r_{i-2} = b$ e $r_{i-1} = a$ e l'equazione finale sarà del tipo $\text{MCD}(a, b) = a x_0 + b y_0$

Esempio:
$\text{MCD}(116, 189)$

1. $189 = 116 + 73$
2. $116 = 73 + 43$
3. $73 = 43 + 30$
4. $43 = 30 + 13$
5. $30 = 13 \cdot 2 + 4$
6. $13 = 4 \cdot 3 + 1$
7. $4 = 1 \cdot 4 + 0 \implies \text{MCD}(a, b) = 1$

$1 = 13 - 4 \cdot 3$

1. $= 13 - 3(30 - 13 \cdot 2)$
2. $= -3 \cdot 30 + 7 \cdot 13$
3. $= -3 \cdot 30 + 7 \cdot (43 - 30)$
4. $= 7 \cdot 43 - 10 \cdot 30$
5. $= 7 \cdot 43 - 10 \cdot (73 - 43)$
6. $= -10 \cdot 73 + 17 \cdot 43$
7. $= -10 \cdot 73 + 17(116 - 73)$
8. $= 17 \cdot 116 - 27 \cdot 73$
9. $= 17 \cdot 116 - 27(189 - 116)$
10. $= 34 \cdot 116 - 27 \cdot 189 \implies x_0 = 34, y_0 = -27$

E.1.2 Equazioni diofantee

$$ax + by = c$$

Ha soluzione se $\text{MCD}(a,b)|c$
Trovo x_0 e y_0 tramite il $\text{MCD}(a,b)$
Tutte le soluzioni si trovato con la formula:

$$\text{Soluzioni}=\begin{cases} x = x_0 \cdot \frac{c}{\text{MCD}(a,b)} + b't \\ y = y_0 \cdot \frac{c}{\text{MCD}(a,b)} - a't \end{cases} \qquad \forall t \in \mathbb{Z}$$

$$b' = \frac{b}{\text{MCD}(a,b)}$$

$$a' = \frac{a}{\text{MCD}(a,b)}$$

Esempio:
$34x + 12y = 8$
$34 = 2 \cdot 12 + 10$
$12 = 10 + 2$
$10 = 5 \cdot 2 \implies \text{MCD}(34,12) = 2 \implies$ Risolvibile perchè $\text{MCD}(34,12) = 2|8$

$2 = 12 - 10 = 12 - (34 - 12 \cdot 2) = -34 + 3 \cdot 12 \implies x_0 = -1, y_0 = 3$
Tutti i risultati:

$$\begin{cases} x = -1 \cdot \frac{8}{2} + \frac{12}{2}t \\ y = 3 \cdot \frac{8}{2} + \frac{34}{2}t \end{cases} \implies \begin{cases} x = -4 + 6t \\ y = 12 + 17t \end{cases}$$

E.1.3 Equazioni congruenziali

$$ax \equiv b \mod n$$

Ha soluzione se $\text{MCD}(n, a)|b$
Trovo x_0 tramite il $\text{MCD}(n, a)$

$$\text{Soluzioni} = x_0 \cdot \frac{b}{\text{MCD}(n, a)} + \frac{n}{\text{MCD}(n, a)} \cdot t$$
$$\forall t \in [0, \text{MCD}(n, a) - 1]$$

Esempio:
$16x \equiv 22(6)$
$16 = 6 \cdot 2 + 4$
$6 = 4 + 2$
$4 = 2 \cdot 2 \implies \text{MCD}(16, 6) = 2 \implies$ Risolvibile perché $\text{MCD}(16, 6) = 2|22$

$2 = 6 - 4$
$= 6 - (16 - 6 \cdot 2)$
$= -16 + 6 \cdot 3 \implies x_0 = -1$
Soluzioni:

$$x = -1 \cdot \frac{22}{2} + \frac{6}{2} = -11 + 3t \quad \forall t \in [0, 1]$$

E.1.4 Invertire un numero in $\mathbb{Z}_n$

$$ax \equiv 1 \mod n$$

Ha soluzione se $\text{MCD}(n, a) = 1$
Trovo x_0 tramite il $\text{MCD}(a, b)$

$$\text{Soluzione} = x_0$$

E.1.5 Sistemi di equazioni congruenziali