

Algebra

Simone Lidonnici

7 maggio 2024

Indice

1	Relazioni di equivalenza	4
1.1	Classi di equivalenza	5
1.2	Partizione di un insieme	5
1.3	Relazioni di ordine parziale e totale	6
1.3.1	Diagramma di Hasse	6
2	Numeri naturali	7
2.1	Terna di Peano	7
2.2	Principio del buon ordinamento	7
2.2.1	Definizione di somma	8
2.2.2	Definizione di prodotto	8
3	Strutture algebriche	9
3.1	Semigrupp o	9
3.2	Gruppo	10
3.2.1	Gruppo simmetrico	10
3.3	Unicit� dell'elemento neutro e inverso	11
3.4	Anello	11
3.5	Campo	12
3.5.1	Campo dei numeri razionali	12
3.5.2	Campo dei numeri complessi	13
4	Numeri interi	15
4.1	Definizione di somma e prodotto	15
4.2	Numeri primi	16
4.3	Massimo comun divisore (MCD)	17
4.3.1	Propriet�	17
4.3.2	Calcolare il MCD (Algoritmo euclideo)	18
4.4	Minimo comune multiplo	19
4.5	Teorema fondamentale dell'aritmetica	20
4.6	Teoremi su MCD e mcm	20
5	\mathbb{Z}_n	21
5.1	Definizione di somma e prodotto	21
5.2	Insieme delle unit�	21
5.2.1	Funzione e teorema di Eulero	22
5.3	Equazioni congruenziali	22
5.3.1	Sistemi di equazioni congruenziali	23
5.3.2	Trasformare equazioni singole in sistemi	24
5.4	Piccolo teorema di Fermat	25
6	Teoria dei gruppi	26
6.1	Sottogruppo	26
6.2	Omomorfismi	27
6.2.1	Gruppo degli automorfismi	28

6.3	Gruppi ciclici	29
6.3.1	Struttura dei gruppi ciclici	30
6.4	Teorema di Lagrange	31
6.4.1	Gruppi generici	31
6.4.2	Gruppi finiti	33
6.5	Sottogruppi normali	33
6.5.1	Gruppo quoziente per un sottogruppo normale	33
7	Permutazioni	35
7.1	Supporto di una permutazione	35
7.2	Decomposizione di una permutazione	36
7.3	Coniugazioni	36
7.4	Decomposizione in trasposizioni	37
8	Sistemi di equazioni lineari	38
8.1	Matrici	38
8.1.1	Tipi di matrici	38
8.2	Sistemi lineari come matrici	40
8.3	Metodo di Gauss	41
8.3.1	Trasformare un sistema quadrato in triangolare	41
8.4	Risolvere un sistema lineare	42
8.4.1	Soluzioni di un sistema triangolare	42
8.4.2	Soluzioni di un sistema non quadrato	42
8.4.3	Tutte le soluzioni di un sistema lineare	44
9	Spazi vettoriali	45
9.1	Sottospazi vettoriali	46
9.2	Combinazioni lineari	47
9.3	Base di uno spazio vettoriale	47
9.3.1	Indipendenza tra vettori	47
9.3.2	Spazi vettoriali finitamente generati	48
9.3.3	Isomorfismi	49
9.4	Operazioni insiemistiche su sottospazi vettoriali	49
9.5	Sottospazio Somma	50
10	Applicazioni lineari	52
10.1	Applicazioni su spazi vettoriali	53
10.2	Dimensione di un'applicazione	54
11	Operazioni con matrici	55
11.1	Inverso di una matrice	55
11.2	Determinante di una matrice	56
11.2.1	Sviluppo di Laplace	57
11.3	Matrice di una funzione su basi	57
12	Autovalori e autovettori	59
12.1	Trovare gli autovalori	59
12.2	Matrice associata alla funzione	60
12.3	Teorema di indipendenza degli autovettori	60

12.4	Base di autovettori	61
E	Esercizi	62
E.1	Esercizi su \mathbb{Z} e \mathbb{Z}_n	62
E.1.1	Calcolare il MCD e x_0, y_0	62
E.1.2	Equazioni diofantee	63
E.1.3	Equazioni congruenziali	64
E.1.4	Invertire un numero in \mathbb{Z}_n	64
E.1.5	Sistemi di equazioni congruenziali	64
E.1.6	Sistemi di equazioni congruenziali con sostituzione	65
E.1.7	Piccolo teorema di Fermat	66
E.1.8	Sottogruppi di \mathbb{Z}_n	66
E.1.9	Invertibili in \mathbb{Z}_n	67
E.1.10	Teorema di Eulero	67
E.2	Esercizi sulle permutazioni	67
E.2.1	Calcolare il supporto di una permutazione	67
E.2.2	Scrivere in cicli una permutazione	67
E.2.3	Trovare la coniugazione di una permutazione	67
E.2.4	Trovare la permutazione che coniuga	68
E.3	Esercizi sui sistemi di equazioni lineari	68
E.3.1	Passare dai generatori al sistema	68
E.3.2	Passare dal sistema ai generatori	68

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:

$$\text{Dom}(\rho) = \{a \in A \mid \exists b \in B \mid a\rho b\}$$

$$\text{Im}(\rho) = \{b \in B \mid \exists a \in A \mid a\rho b\}$$

Una relazione da A a B è una funzione se:

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

Data una relazione si può definire la su inversa:

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

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 :

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

L'insieme di tutte le classi di equivalenza $\{[a] \mid a \in A\}$ 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:

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

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: $apb, bpa \implies a = b$
- 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: $apb, bpa \implies a = b$
- Transitiva
- Tutti gli elementi sono in relazione tra di loro: $\forall a, b \in A \implies apb \vee bpa$

1.3.1 Diagramma di Hasse

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

$$a \prec b \iff \nexists x | apx \wedge xpb$$

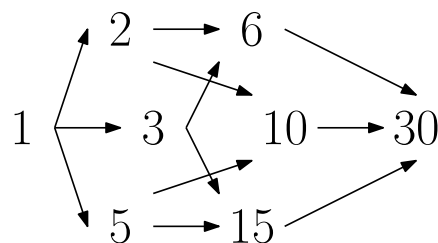
Per rappresentare graficamente queste relazioni si usa il **diagramma di Hasse**.

Esempio:

$$A = \{\text{divisori di } 30\} \subseteq \mathbb{N}$$

$$A = \{1, 2, 3, 5, 6, 10, 15, 30\}$$

$$apb \implies a \text{ divide } b \implies a|b$$



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 $s : \mathbb{N} \rightarrow \mathbb{N}$ 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
- $0 \notin \text{Im}(s)$
- 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:

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

2.2 Principio del buon ordinamento

Principio del buon ordinamento

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

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

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 $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ che data una coppia di numeri restituisce la somma:

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

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 $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ che da una coppia di numeri restituisce il prodotto:

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

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:

$$\star : X \times X \rightarrow X$$

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. Semigrupp
2. Gruppo
3. Anello
4. Campo

3.1 Semigrupp

Definizione di semigrupp

Un semigrupp 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: $\exists e \in S | e \star s = s \star e = s \forall s$
3. Se $s \star s' = s' \star s$ il semigrupp (S, \star) è commutativo

Un semigrupp generico si scrive (A, \star) .

Esempio:

$(\mathbb{N}, +)$ è un semigrupp 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 :

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

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:

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

una permutazione σ viene rappresentata come:

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

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:

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

Insieme delle unità

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

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

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 .

$$a'b' \text{ inverso di } ab \implies (a'b')(ab) = b'(aa')b = b' \cdot 1 \cdot b = bb' = 1$$

3.5 Campo

Definizione di campo

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

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

Si può anche dire:

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

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

3.5.1 Campo dei numeri razionali

L'insieme dei numeri razionali è definito come:

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

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 :

$$\begin{aligned}\mathbb{Z} &\xrightarrow{\varphi} \mathbb{Q} \\ a &\xrightarrow{\varphi} (a, 1)\end{aligned}$$

tale che:

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

\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 $(x, y) \neq (0, 0)$:

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

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

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

$$\begin{aligned}\mathbb{R} &\xrightarrow{\varphi} \mathbb{C} \\ x &\xrightarrow{\varphi} (x, 0)\end{aligned}$$

tale che:

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

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:

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

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

4.1 Definizione di somma e prodotto

Nei numeri interi la definizione di somma e prodotto sono:

$$\begin{aligned} [(n, m)] + [(n', m')] &= [(n + n', m + m')] \\ [(n, m)] \cdot [(n', m')] &= [(nn' + mm', nm' + mn')] \end{aligned}$$

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 $b \neq 0$:

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

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 $a \in (A, +, \cdot)$:

$$a \text{ primo} \implies a \text{ irriducibile}$$

$$a \text{ irriducibile} \not\Rightarrow a \text{ primo}$$

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

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

d è l'unico MCD.

Dimostrazione:

$$S = \{ax + by > 0 | x, y \in \mathbb{Z}\} \subseteq \mathbb{N}^*$$

$$S \neq \emptyset \xrightarrow{\text{buon ordinamento}} \exists d | d \geq x \forall x \in S$$

$$d = ax_0 + by_0 \text{ è il MCD di } a \text{ e } b \text{ e } d \geq 1$$

$$ax + by = dq + r \text{ con } 0 \leq r < d$$

$$ax + by = (ax_0 + by_0)q + r \implies r = a(x - x_0q) + b(y - y_0q)$$

Per assurdo $r \in S$ e $r > 0 \implies r < d$ che è il minimo quindi impossibile

$$\text{Quindi } d|(ax + by) \implies d|a \text{ e } d|b$$

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. $\text{MCD}(a, b) = d \implies \text{MCD}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

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. $a = bq_1 + r_1 \implies \text{MCD}(a, b) = \text{MCD}(b, r_1)$
 $0 \leq r_1 < b \rightarrow \begin{cases} r_1 = 0 \implies \text{MCD}(a, b) = b \\ r_1 > 0 \implies \text{vado al punto 2} \end{cases}$
2. $b = r_1q_2 + r_2 \implies \text{MCD}(b, r_1) = \text{MCD}(r_1, r_2)$
 $0 \leq r_2 < r_1 \rightarrow \begin{cases} r_2 = 0 \implies \text{MCD}(r_1, r_2) = r_1 \\ r_2 > 0 \implies \text{vado al punto 3} \end{cases}$
3. $r_1 = r_2q_3 + r_3 \implies \text{MCD}(r_1, r_2) = \text{MCD}(r_2, r_3)$
 $0 \leq r_3 < r_2 \rightarrow \begin{cases} r_3 = 0 \implies \text{MCD}(r_2, r_3) = r_2 \\ r_3 > 0 \implies \text{vado al punto 4} \end{cases}$

Così abbiamo una successione strettamente decrescente in cui:

$$b > r_1 > r_2 > \dots > r_n > r_{n+1} = 0$$

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

Quindi:

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

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. ...
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:

$$1. a|h \wedge b|h$$

$$2. \text{Se } a|h' \wedge b|h' \implies h|h'$$

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} :

$$\forall n \in \mathbb{N}, n \geq 2 \implies n \text{ è prodotto di numeri primi}$$

$$n = p_1^{h_1} \cdot p_2^{h_2} \cdot \dots \cdot p_s^{h_s} \text{ con } s \geq 1, h_i \geq 1$$

In \mathbb{Z} :

$$\forall n \in \mathbb{Z}, n \notin [1, -1] \implies n \text{ è prodotto di numeri primi}$$

$$n = (\pm 1) \cdot p_1^{h_1} \cdot p_2^{h_2} \cdot \dots \cdot p_s^{h_s} \text{ con } s \geq 1, h_i \geq 1$$

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

$$a = q_1^{l_1} \cdot \dots \cdot q_j^{l_j}$$

$$b = q_1^{m_1} \cdot \dots \cdot q_j^{m_j}$$

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

$$\text{MCD}(a, b) = q_1^{d_1} \cdot \dots \cdot q_j^{d_j} \text{ con } d_i = \min(l_i, m_i)$$

$$\text{mcm}(a, b) = q_1^{c_1} \cdot \dots \cdot q_j^{c_j} \text{ con } c_i = \max(l_i, m_i)$$

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 = $\{p_1, p_2, \dots, p_n\}$

Considero $a = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$

a fattorizzabile $\implies \exists p_j \text{ t.c. } p_j | a \implies \exists t | a = tp_j \implies$

$p_j(-(p_1 \cdot \dots \cdot p_{j-1} \cdot p_{j+1} \cdot \dots \cdot p_n) + t) = 1 \implies p_j | 1$ 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:

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

$\mathbb{Z}/_n\mathbb{Z} = \mathbb{Z}_n$ 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 $u(\mathbb{Z}_n)$:

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

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 :

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

5.2.1 Funzione e teorema di Eulero

Funzione di Eulero

La funzione di Eulero φ :

$$\begin{aligned}\varphi &: \mathbb{N} \rightarrow \mathbb{N} \\ n &\rightarrow |u(\mathbb{Z}_n)|\end{aligned}$$

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 $n = p_1^{r_1} \cdot \dots \cdot p_s^{r_s}$:

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

Teorema di Eulero

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

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

Esempio:

Calcolare le ultime 2 cifre di 123^{123}

Dobbiamo calcolare $[123^{123}]_{100} = [123]_{100}^{123} = [23]_{100}^{123}$

Applico Eulero:

$$\varphi(100) = \varphi(5^2 \cdot 2^2) = (5^2 - 5)(2^2 - 2) = 40$$

$$23^{40} \equiv 1(100) \implies [23]_{100}^{123} = [23^{40 \cdot 3 + 3}]_{100} = [23^3]_{100} = [12167]_{100} = 67$$

5.3 Equazioni congruenziali

Le equazioni congruenziali si dividono in 3 casi:

- Caso 1 in \mathbb{Z} :

$$ax + by = c$$

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

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

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

- Caso 1 in \mathbb{Z}_n :

$$ax \equiv b \pmod{n}$$

Risolubile se $\text{MCD}(n, a) | b$:

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

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 :

$$ax \equiv 1 \pmod{n}$$

Risolubile se $\text{MCD}(n, a) = 1$:

$$\text{Soluzione} = x_0$$

Esempi:

$$15x \equiv 18 \pmod{24}$$

$$1. \quad 24 = 15 + 9$$

$$2. \quad 15 = 9 + 6$$

$$3. \quad 9 = 6 + 3$$

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

Trovo x_0 :

$$3 = 9 - 6 = (24 - 15) - (15 - (24 - 15)) = 15 \cdot -3 + 24 \cdot 2 \implies x_0 = -3$$

$$\text{Soluzioni} = -3 \cdot \frac{18}{3} + \frac{24}{3}k = -18 + 8k = 6 + 8k$$

$$121x \equiv 22 \pmod{33}$$

$$\text{MCD}(121, 33) = 11 | 22$$

$$121x \equiv 22 \pmod{33} \iff 11x \equiv 2 \pmod{3} \iff 2x \equiv 2 \pmod{3} \implies x_0 = 1$$

$$\text{Soluzioni} = 1 + \frac{33}{11}k = 1 + 3k$$

5.3.1 Sistemi di equazioni congruenziali

Un sistema di equazioni congruenziali, scritti:

$$\begin{cases} a_1x \equiv b_1 & (n_1) \\ \dots \\ a_sx \equiv b_s & (n_s) \end{cases}$$

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:

$$\begin{cases} x_1 \equiv c_1 & (r_1) \\ \dots & | \text{MCD}(r_i, r_j) = 1 \quad \forall i \neq j \\ x_s \equiv c_s & (r_s) \end{cases}$$

In cui:

$$r_i = \frac{n_i}{\text{MCD}(a_i, n_i)}$$

$$c_i = \frac{b_i}{\text{MCD}(a_i, n_i)} \cdot \underbrace{\left(\frac{a_i}{\text{MCD}(a_i, n_i)} \right)^{-1}}_{\text{inverso di } (...)(\text{ mod } r_i)}$$

Questo sistema ha una sola soluzione in $(\text{ mod } r_1 \cdot r_2 \cdot \dots \cdot r_s)$

Per risolverla scriviamo:

$$R = r_1 \cdot r_2 \cdot \dots \cdot r_s \text{ con } R_k = \frac{R}{r_k}$$

Risolviamo $R_k x = c_k(r_k)$ e troviamo x_k

La soluzione dell'intero sistema:

$$\tilde{x} = R_1 x_1 + \dots + R_s x_s$$

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:

$$\tilde{x} = R_1 x_1 + R_2 x_2 + R_3 x_3$$

$$77x_1 \equiv 1(5) \implies 2x_1 \equiv 1(5) \implies x_1 = 3$$

$$55x_2 \equiv 3(7) \implies 6x_2 \equiv 3(7) \implies -1x_2 \equiv 3(7) \implies x_2 = 4$$

$$35x_3 \equiv 10(11) \implies 2x_3 \equiv 10(11) \implies x_3 = 5$$

$$\tilde{x} = 77 \cdot 3 + 55 \cdot 4 + 35 \cdot 5 = 626$$

5.3.2 Trasformare equazioni singole in sistemi

Data un'equazione congruenziale:

$$ax \equiv b \pmod{n}$$

se n non è primo possiamo fattorizzarlo come:

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

e possiamo scrivere l'equazione come un sistema:

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

in cui:

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

Esempio:

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

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:

$$a = 0 \implies 0^p \equiv 0 \quad (p)$$

2. Passo induttivo:

$$\text{Suppongo vero che } a^p \equiv a \quad (p)$$

3. Dimostrazione induttiva:

$$(a+1)^p \equiv (a^p + 1) \quad (p) = (a+1) \quad (p)$$

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

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

Se n è primo allora:

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

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:

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

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

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

Cardinalità dei sottogruppi

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

$$H \leq (\mathbb{Z}, +) \implies \exists n | n\mathbb{Z} = H$$

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

Preso \mathbb{Z}_n gli H_d sono tutti i sottoinsiemi di \mathbb{Z}_n .

Scritto $n = kd$:

$$|H_d| = k$$

Dimostrazione:

1. $H \leq (\mathbb{Z}, +)$:

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

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

2. $H \leq (\mathbb{Z}_n, +)$:

$$H' = \{a \in \mathbb{Z} | [a] \in H\} \implies 0, n \in H' \implies H' \neq \emptyset, H \leq \mathbb{Z}$$

$$a, b \in H' \implies [a], [b] \in H \xrightarrow{H \leq \mathbb{Z}_n} [a] - [b] \in H \iff a - b \in H'$$

$$H' \leq (\mathbb{Z}, +) \xrightarrow{(1)} \exists d \in \mathbb{Z} | H' = d\mathbb{Z} \xrightarrow{n \in H} d|n \implies H = H_d$$

6.2 Omomorfismi

Definizione di omomorfismo

Un omomorfismo è una mappa tra gruppi:

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

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:

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

Per ogni gruppo (G, \star) esiste inoltre una mappa iniettiva $\varphi : (G, \star) \rightarrow (S(G), \circ)$ 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:

$$f : G \rightarrow G' \implies G / \text{Ker}(f) \underset{\text{isomorfo}}{\simeq} \text{Im}(f)$$

Dimostrazione:

Presa la mappa:

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

π è un omomorfismo di gruppi.

$$\pi(aa') = H(aa') = Ha \star Ha' = \pi(a) \star \pi(a')$$

$$a \rho_f a' \iff f(a) = f(a') \iff f(a)(f(a'))^{-1} = 1_G \xLeftrightarrow{f \text{ omo}} f(a(a)^{-1}) \iff a(a)^{-1} \in \text{Ker}(f) \iff G / \text{Ker}(f) = G / \rho_f$$

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \pi \downarrow & & \uparrow i=\text{inclusione} \\ G / \rho_f & \xrightarrow{F} & \text{Im}(f) \end{array}$$

$$F(Ha) = f(a)$$

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 :

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

preso un $x \in G$:

$$\begin{aligned}\gamma_x : G &\rightarrow G \\ g &\rightarrow \gamma_x(g) = xgx^{-1}\end{aligned}$$

γ_x è un isomorfismo di gruppi.

Questi isomorfismi sono componibili cioè:

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

Il nucleo di γ :

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

Questo gruppo viene chiamato **centro** di G e $\text{Ker} \trianglelefteq G$.

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 $t \in \mathbb{Z}$:

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

g^t è un sottogruppo di G e si dice che G è generato da g .

L'ordine di g è uguale:

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

Se questo minimo non esiste allora g ha ordine ∞ .

Definizione di gruppo ciclico

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

$$\exists g \in G \mid G = \langle g \rangle$$

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

$$\exists h \in H \mid H = \langle h \rangle$$

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

Esempio:

$(\mathbb{Z}, +)$ è ciclico perché $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

\mathbb{Z} è anche l'unico gruppo ciclico con $o(g) = \infty$

6.3.1 Struttura dei gruppi ciclici

I gruppi ciclici possono essere di due tipi:

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

1. Caso 1:

$$\begin{aligned} \varphi : \mathbb{Z} &\rightarrow G \\ m &\rightarrow g^m \end{aligned}$$

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

Dimostrazione:

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

2. Caso 2:

$$\begin{aligned} \varphi : \mathbb{Z}_n &\rightarrow G \\ [m] &\rightarrow g^m \end{aligned}$$

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:

$$G = \{1, g, g^2, \dots, g^{n-1}\} \implies \varphi \text{ è suriettiva e iniettiva}$$

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 $\{a_1H, a_2H, \dots, a_iH\}$ sono classi laterali sinistre distinte.

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

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

Esempio:

S_3

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

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

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

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

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 :

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

Quindi:

$$\begin{aligned} a\rho_sb &\iff a^{-1}b \in H \\ a\rho_sb &\iff aH \cap gH \neq \emptyset \wedge bH \cap gH \neq \emptyset \iff aH = gH = bH \end{aligned}$$

- 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 :

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

Quindi:

$$\begin{aligned} a\rho_db &\iff a^{-1}b \in H \\ a\rho_db &\iff Ha \cap Hg \neq \emptyset \wedge Hb \cap Hg \neq \emptyset \iff Ha = Hg = Hb \end{aligned}$$

6.4.2 Gruppi finiti

Teorema di Lagrange

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

$$\begin{array}{ccc} |H| & | & |G| \\ & \underbrace{\quad} & \\ & \text{divide} & \end{array}$$

Preso un k :

$$\forall k|n \exists! H \leq G \mid |H| = k$$

$$H = \langle g^{\frac{n}{k}} \rangle$$

Se $h|k$:

$$\langle g^{\frac{n}{h}} \rangle \leq \langle g^{\frac{n}{k}} \rangle$$

6.5 Sottogruppi normali

Definizione di sottogruppo normale

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

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

Per controllare se H è normale:

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

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 :

$$f : G \rightarrow G' \implies \text{Ker}(f) = \{g \in G \mid f(g) = 1_{G'}\} \trianglelefteq G$$

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:

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

φ è biettiva quindi ha un inverso:

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

Relazione di equivalenza compatibile

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

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

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 :

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

Preso un elemento esterno al supporto:

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

Prese due mappe σ, τ :

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

Esempi:

- Trasposizione con 2 elementi:

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

- Trasposizione con k elementi:

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

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:

$$\sigma = \sigma_1 \cdot \dots \cdot \sigma_k \mid \text{Supp}(\sigma_i) \cap \text{Supp}(\sigma_j) = \emptyset$$

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

$$d_j = o(\sigma_j) = \text{numero di elementi in } \sigma_j$$

$$o(\sigma) = \text{mcm}(d_1, \dots, d_k)$$

Esempio:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 4 & 1 & 2 \end{pmatrix}$$

Può essere decomposta in 3 cicli:

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

Quindi possiamo scrivere σ (si omettono gli elementi da soli):

$$\sigma = (1 \ 3 \ 5)(2 \ 6) \implies \text{Supp}(\sigma) = \{1, 2, 3, 5, 6\}$$

$$\text{mcm}(3, 2) = 6$$

7.3 Coniugazioni

Elementi coniugati in un gruppo

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

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

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

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

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

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

Il risultato quindi è:

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

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:

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

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:

$$\sigma = \tau_1 \cdot \dots \cdot \tau_k$$

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 permutazione 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:

$$\begin{array}{cccccccc} j_1 & \dots & j_2 & \dots & \dots & j_3 & \dots & j_r \\ \left| \begin{array}{cccccccc} p_1 & & & & & & & \\ 0 & 0 & p_2 & & & & & \\ 0 & 0 & 0 & 0 & 0 & p_3 & & \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & p_r \end{array} \right| \end{array}$$

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 $a_{ij} = a_{ji}$:

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

Matrici simili

Due matrici A e A' sono simili se:

$$\exists C \text{ invertibile } | A' = C^{-1}AC$$

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:

$$\begin{aligned} \Sigma &= \{\underline{x} \in \mathbb{R}^n \mid A\underline{x} = \underline{b}\} \\ \Sigma' &= \{\underline{x} \in \mathbb{R}^n \mid A'\underline{x} = \underline{b}'\} \\ A\underline{x} = \underline{b} &\equiv A'\underline{x} = \underline{b}' \iff \Sigma = \Sigma' \end{aligned}$$

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:

$$\alpha_1 x_1 + \dots + \alpha_n x_n = \beta$$

$$\alpha'_1 x_1 + \dots + \alpha'_n x_n = \beta'$$

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

$$h(\alpha_1 x_1 + \dots + \alpha_n x_n) + k(\alpha'_1 x_1 + \dots + \alpha'_n x_n) = h\beta + k\beta' \quad \forall k \neq 0$$

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:

$$\left. \begin{aligned} \alpha_1 y_1 + \dots + \alpha_n y_n - \beta &= 0 \\ \alpha'_1 y_1 + \dots + \alpha'_n y_n - \beta' &= 0 \end{aligned} \right\} \implies$$

$$h(\alpha_1 y_1 + \dots + \alpha_n y_n - \beta) + k(\alpha'_1 y_1 + \dots + \alpha'_n y_n - \beta') = 0 \implies \underline{y} \text{ soddisfa la nuova equazione} \implies \Sigma \subseteq \tilde{\Sigma}$$

2. $\tilde{\Sigma} \subseteq \Sigma$:

Prendiamo una n -pla $\underline{z} \in \tilde{\Sigma}$ che soddisfa il secondo sistema, quindi:

$$\alpha_1 z_1 + \dots + \alpha_n z_n - \beta = 0 \implies \underbrace{h(\alpha_1 z_1 + \dots + \alpha_n z_n - \beta) + k(\alpha'_1 z_1 + \dots + \alpha'_n z_n - \beta')}_{=0} =$$

$$k\beta' \xrightarrow{k \neq 0} \underline{z} \text{ soddisfa la nuova equazione} \implies \tilde{\Sigma} \subseteq \Sigma$$

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 $k_j = -\left(\frac{a_{i+1,j}}{p_j}\right)$
3. Per ogni valore della matrice $a_{i'j'} | i' > i \wedge j' \geq j \implies a_{i'j'} = a_{i'j'} + a_{i,j'} \cdot k_j$
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:

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

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:

$$t_{ii} \neq 0 \quad \forall i = [1, n]$$

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:

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

Per risolverlo sposto tutte le variabili non moltiplicate per un p_i dall'altra parte e le considero come parametri t_1, \dots, t_n calcolando le altre variabili. Per sostituzione faccio diventare tutte le variabili nella forma $x_i = j_i + \alpha_1t_1 + \dots + \alpha_nt_n$.

Scriviamo poi il risultato sotto forma:

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

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 (che 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:

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

Risolvero 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:

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

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}, \dots, S^{j_r} :
 - $\{S^{j_1}, \dots, S^{j_r}\}$ è una base per $\text{Im}(S) = \text{Span}(\text{colonne di } S)$
 - $\{A^{j_1}, \dots, A^{j_r}\}$ 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:

$$\begin{aligned}\Sigma &= \{\underline{x} | A\underline{x} = \underline{b}\} \\ \Sigma_0 &= \{\underline{x} | A\underline{x} = \underline{0}\}\end{aligned}$$

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:

$$\begin{aligned} + : V \times V &\rightarrow V \\ (\underline{v}, \underline{w}) &\rightarrow \underline{v} + \underline{w} \end{aligned}$$

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

$$\begin{aligned} \cdot : \mathbb{R} \times V &\rightarrow V \\ (\alpha, \underline{v}) &\rightarrow \alpha \underline{v} \end{aligned}$$

Il prodotto scalare è commutativo e distributivo.

Esempio:

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

$$\underline{x} \in \mathbb{R}^n = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$\underline{0} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

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

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

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:

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

Applicando la proprietà distributiva:

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

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 :

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

Applicando la proprietà distributiva:

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

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

9.2 Combinazioni lineari

Dato uno spazio vettoriale V e un insieme di vettori $\underline{v}_1, \underline{v}_2, \dots, \underline{v}_k$, una **combinazione lineari** in V è:

$$\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 + \dots + \alpha_k \underline{v}_k \quad \alpha_j \in \mathbb{R}$$

Span di un insieme di vettori

Dato un insieme di vettori in uno spazio vettoriale V , lo Span è l'insieme di tutte le possibili combinazioni lineari:

$$\text{Span}(\underline{v}_1, \underline{v}_2, \dots, \underline{v}_k) = \{\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 + \dots + \alpha_k \underline{v}_k \mid \alpha_j \in \mathbb{R}\}$$

Lo Span di un insieme di vettori è uguale allo Span di quell'insieme unito con altri elementi che già appartengono allo Span:

$$\text{Span}(W) = \text{Span}(W \cup \{\underline{a}, \underline{b}, \dots, \underline{n}\}) \iff \{\underline{a}, \underline{b}, \dots, \underline{n}\} \in \text{Span}(W)$$

Lo Span è un sottospazio vettoriale.

9.3 Base di uno spazio vettoriale

9.3.1 Indipendenza tra vettori

Presi k vettori, questi sono linearmente indipendenti se:

$$\alpha_1 \underline{v}_1 + \dots + \alpha_k \underline{v}_k = \underline{0} \implies \alpha_1 = \alpha_2 = \dots = \alpha_k = 0$$

Al contrario se:

$$\exists \alpha_j \neq 0 \mid \alpha_1 \underline{v}_1 + \dots + \alpha_k \underline{v}_k = \underline{0}$$

allora sono linearmente dipendenti.

Sono sempre linearmente dipendenti se:

1. Un qualsiasi vettore $\underline{v}_j = \underline{0}$
2. Un vettore è combinazione lineare degli altri
3. Sono proporzionali, cioè $\exists \alpha \neq 0 \mid \underline{v}_1 = \alpha \underline{v}_2$
4. Un sottoinsieme di j vettori con $j < k$ ha vettori linearmente dipendenti

Base di uno spazio vettoriale

Dato uno spazio vettoriale V un insieme di vettori:

$$B = \{\underline{v}_1, \dots, \underline{v}_k\}$$

è una base per V se:

1. Sono linearmente indipendenti
2. Generano V , cioè $\text{Span}(\underline{v}_1, \dots, \underline{v}_k) = V$

Una base B è un sottoinsieme massimale di vettori lineari indipendenti in V .

Dimostrazione:

Aggiungiamo a B un vettore \underline{v} allora $\underline{v} \in \text{Span}(B) \implies B \cup \underline{v}$ sono linearmente dipendenti.

Esempi:

$$\{\underline{e}_1, \underline{e}_2, \dots, \underline{e}_k\} \subseteq \mathbb{R}^n$$

$$\underline{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \underline{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, \underline{e}_k = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

Questi vettori sono una base di \mathbb{R}^n

$$\{\underline{v}_1, \underline{v}_2\} \subseteq V_O^2$$

Qualsiasi coppia di vettori linearmente indipendenti è una base di V_O^2 .

9.3.2 Spazi vettoriali finitamente generati

Dato uno spazio vettoriale V , esso è **finitamente generato** se:

$$\exists \{\underline{v}_1, \dots, \underline{v}_k\} | \text{Span}(\underline{v}_1, \dots, \underline{v}_k) = V$$

Se è finitamente generato ha almeno una base.

Qualsiasi $\underline{v} \in V$ può essere scritto in modo unico come $\alpha_1 \underline{v}_1 + \dots + \alpha_k \underline{v}_k$.

Esempio:

$\mathbb{R}[X] = V$ non è finitamente generato

$\{p_1, \dots, p_j\}$ un insieme di polinomi con $d_j = \text{grado di } p_j$ e $d = \max(d_1, \dots, d_j)$

Allora $x^{d+1} + 1 \notin \text{Span}(p_1, \dots, p_j)$

Cardinalità uguale fra basi

Dato uno spazio vettoriale V finitamente generato con una base $B = \{\underline{v}_1, \dots, \underline{v}_n\}$ e siano $\{\underline{w}_1, \dots, \underline{w}_k\}$ vettori linearmente indipendenti, allora esistono $n - k$ vettori che aggiunti a $\{\underline{w}_1, \dots, \underline{w}_k\}$ danno una base B' di V .

Due basi dello stesso spazio vettoriale V hanno la stessa cardinalità:

$$|B| = |B'|$$

La dimensione dello spazio V è uguale alla cardinalità della base.

Sottospazi vettoriali di spazi finitamente generati

Dato uno spazio vettoriale V finitamente generato di dimensione n qualsiasi sottospazio vettoriale $W \leq V$:

1. W è finitamente generato
2. Dimensione di W è minore della dimensione di V

Dimostrazione:

Procediamo in modo ciclico:

1. $\underline{w}_1 \in W \implies \begin{cases} \langle \underline{w}_1 \rangle = W \implies W \text{ finitamente generato} \\ \exists \underline{w}_2 \in W \setminus \langle \underline{w}_1 \rangle \implies \underline{w}_2 \text{ lin. indep. da } \underline{w}_1 \end{cases}$
2. $\{\underline{w}_1, \underline{w}_2\} \in W \implies \begin{cases} \langle \underline{w}_1, \underline{w}_2 \rangle = W \implies W \text{ finitamente generato} \\ \exists \underline{w}_3 \in W \setminus \langle \underline{w}_1, \underline{w}_2 \rangle \implies \underline{w}_3 \text{ lin. indep. da } \{\underline{w}_1, \underline{w}_2\} \end{cases}$
3. Continuiamo al massimo fino a quando arriviamo a \underline{w}_n oppure ci fermiamo prima ad un \underline{w}_m con $m < n$

9.3.3 Isomorfismi

Dato uno spazio vettoriale V finitamente generato su \mathbb{K} e B una base di V :

$$\begin{aligned} \varphi_B : \mathbb{K}^n &\rightarrow V \\ \underline{\alpha} = (\alpha_1, \dots, \alpha_k) &\rightarrow \alpha_1 \underline{v}_1 + \dots + \alpha_k \underline{v}_k \end{aligned}$$

La mappa φ è un isomorfismo di \mathbb{K} -spazi vettoriali.

9.4 Operazioni insiemistiche su sottospazi vettoriali

Presi due sottospazi vettoriali:

$$\left. \begin{array}{l} U \leq V \\ W \leq V \end{array} \right\} \implies U \cap W \leq V$$

Dimostrazione:

$$\begin{aligned}
 U \leq V &\implies \left. \begin{array}{l} \forall \underline{u}_1, \underline{u}_2 \in U \\ \forall \lambda_1, \lambda_2 \in \mathbb{R} \end{array} \right\} \implies \lambda_1 \underline{u}_1 + \lambda_2 \underline{u}_2 \in U \\
 W \leq V &\implies \left. \begin{array}{l} \forall \underline{w}_1, \underline{w}_2 \in U \\ \forall \mu_1, \mu_2 \in \mathbb{R} \end{array} \right\} \implies \mu_1 \underline{w}_1 + \mu_2 \underline{w}_2 \in W
 \end{aligned}$$

Queste due cose implicano:

$$\left. \begin{array}{l} \forall \underline{z}_1, \underline{z}_2 \in U \cap W \\ \forall \lambda_1, \lambda_2 \in \mathbb{R} \end{array} \right\} \implies \left\{ \begin{array}{l} \lambda_1 \underline{z}_1 + \lambda_2 \underline{z}_2 \in U \\ \lambda_1 \underline{z}_1 + \lambda_2 \underline{z}_2 \in W \end{array} \right. \implies \lambda_1 \underline{z}_1 + \lambda_2 \underline{z}_2 \in U \cap W$$

A differenza dell'intersezione l'unione di due sottospazi vettoriali $W \leq V, U \leq V$ non è sempre un sottospazio.

9.5 Sottospazio Somma

Presi due sottospazi vettoriali $U \leq V, W \leq V$ e dei rispettivi sistemi di generatori $\{\underline{u}_1, \dots, \underline{u}_k\}$ e $\{\underline{w}_1, \dots, \underline{w}_k\}$ allora $\{\underline{u}_1, \dots, \underline{u}_k, \underline{w}_1, \dots, \underline{w}_k\}$ è un sistema di generatori per $U + W$. Non è detto che questa sia una base.

Formula di Grassmann

Presi due sottospazi vettoriali $U \leq V, W \leq V$:

$$\dim(U \cap W) + \dim(U + W) = \dim(U) + \dim(W)$$

Questo vuol dire che un sistema di generatori di $U + W$ è anche una base se $U \cap W = \underline{0}$

Esempio:

$$V = V_O^3$$

$$U = V_O^2$$

$$W = V_O$$

$$\underbrace{\dim(U \cap W)}_0 + \underbrace{\dim(U + W)}_3 = \underbrace{\dim(U)}_2 + \underbrace{\dim(W)}_1$$

Somma diretta

Presi due sottospazi vettoriali $U \leq V, W \leq V$, V è una somma diretta di U e W se:

- $U \cap W = \underline{0}$
- $U + W = V$

Si scrive come:

$$V = U \oplus W$$

Quindi:

$$\dim(U \oplus W) = \dim(U) + \dim(W)$$

Se $V = U \oplus W$ allora W si dice **supplementare** di U .

Dato qualunque sottospazio $U \leq V$ esistono sempre infiniti supplementari.

Preso un sottospazio vettoriale $U \leq V$ e le relative basi $B_U = \{\underline{u}_1, \dots, \underline{u}_k\}$ e $B_V = \{\underline{v}_1, \dots, \underline{v}_n\}$ tali che $|B_U| = k$ e $|B_V| = n$ con $k < n$, posso trovare $n - k$ vettori $\{\underline{v}_{i_1}, \dots, \underline{v}_{i_{n-k}}\}$ tali che $\{\underline{u}_1, \dots, \underline{u}_k, \underline{v}_{i_1}, \dots, \underline{v}_{i_{n-k}}\}$ è una nuova base di V .

Lo Span di questo insieme di vettori aggiunto è un supplementare di U :

$$W = \text{Span}(v_{i_1}, \dots, v_{i_{n-k}}) \implies U \oplus W = V \implies W \text{ supplementare di } U$$

10

Applicazioni lineari

Definizione di applicazione lineare

Presi due spazi vettoriali $(V, +, \cdot), (W, +, \cdot)$ l'applicazione:

$$T : V \rightarrow W$$

è lineare se:

- $T(\underline{v}_1 + \underline{v}_2) = T(\underline{v}_1) + T(\underline{v}_2)$
- $T(\lambda \cdot \underline{v}) = \lambda \cdot T(\underline{v})$

Questa applicazione collega i vettori nulli e gli inversi tra loro:

$$\begin{aligned} T(\underline{0}_V) &= \underline{0}_W \\ T(-\underline{v}) &= -T(\underline{v}) \end{aligned}$$

Inoltre:

$$T : \mathbb{R} \rightarrow \mathbb{R} \text{ lineare} \iff \exists c \in \mathbb{R} | Tx = cx$$

Esempi:

$$V = W$$

$$T = Id_V$$

$$Id_V(\underline{v}) = \underline{v}$$

$$A \in M_{mn}(\mathbb{R}) = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{mn} \end{vmatrix}$$

$$L_A : \mathbb{R}^n \rightarrow \mathbb{R}^m$$

$$\begin{vmatrix} x_1 \\ \dots \\ x_n \end{vmatrix} \rightarrow \begin{vmatrix} a_{11}x_1 + \dots + a_{1n}x_n \\ \dots \\ a_{n1}x_1 + \dots + a_{nn}x_n \end{vmatrix} = x_1 \begin{vmatrix} a_{11} \\ \dots \\ a_{n1} \end{vmatrix} + \dots + x_n \begin{vmatrix} a_{1n} \\ \dots \\ a_{nn} \end{vmatrix} = x_1 A^1 + \dots + x_n A^n$$

Questa applicazione L_A è lineare (solo se le x solo di grado 1 e non ci sono termini noti) perché:

- $L_A\left(\begin{vmatrix} x_1 \\ \dots \\ x_n \end{vmatrix} + \begin{vmatrix} x'_1 \\ \dots \\ x'_n \end{vmatrix}\right) = L_A\left(\begin{vmatrix} x_1 \\ \dots \\ x_n \end{vmatrix}\right) + L_A\left(\begin{vmatrix} x'_1 \\ \dots \\ x'_n \end{vmatrix}\right)$
- $L_A\left(\lambda \begin{vmatrix} x_1 \\ \dots \\ x_n \end{vmatrix}\right) = \lambda L_A\left(\begin{vmatrix} x_1 \\ \dots \\ x_n \end{vmatrix}\right)$

10.1 Applicazioni su spazi vettoriali

Presi due spazi vettoriali V, W e le loro basi B_V, B_W :

$$\exists! T : V \rightarrow W \text{ lineare } | T(\underline{v}_i) = \underline{w}_i$$

Se due applicazioni:

$$S(\underline{v}_i) = T(\underline{v}_i) \implies S = T$$

Un'applicazione è univocamente determinata dai valori che assume su una base.

Inoltre per ogni $T : V \rightarrow W$ esistono due sottospazi particolari:

1. $\text{Im}(T) \leq W$
2. $\text{Ker}(T) = \{\underline{v} \in V | T(\underline{v}) = \underline{0}_W\} \leq V$

Se T è iniettiva:

$$T \text{ iniettiva} \iff \text{Ker}(T) = \{\underline{0}_V\}$$

Sistema di generatori per $\text{Im}(T)$

Data un'applicazione lineare T con base $B = \{\underline{v}_1, \dots, \underline{v}_n\}$ allora:

$$\text{Im}(T) = \text{Span}(\underbrace{T(\underline{v}_1), \dots, T(\underline{v}_n)}_{\text{Sistema di generatori}})$$

Nel caso di matrici $A \in M_{mn}$ con applicazione $L_A : \mathbb{R}^n \rightarrow \mathbb{R}^m$:
 $\text{Im}(L_A) = \text{Span}(A', \dots, A^n)$

10.2 Dimensione di un'applicazione

Teorema della dimensione

Data un'applicazione lineare T :

$$T : V \rightarrow W$$

$$\dim(V) = \dim(\text{Ker}(T)) + \dim(\text{Im}(T))$$

Osservazioni:

- $\dim(\text{Im}(T)) = \text{rango}(T) = \text{rg}(T)$
- $\text{rg}(T) \leq \dim(W)$
- $\text{rg}(T) \leq \dim(V)$
- $\text{rg}(L_A) = \text{rg}(A) = \dim(\text{Span}(A^1, \dots, A^n)) = \max \text{ numero di colonne lin. ind.}$

Quindi:

1. T iniettiva $\iff \text{rg}(T) = \dim(V)$
2. T suriettiva $\iff \text{rg}(T) = \dim(W)$
3. Se $\dim(V) = \dim(W)$ allora T iniettiva $\iff T$ suriettiva

Teorema di Rouchè-Capelli

Dato un sistema $A\underline{x} = \underline{b}$:

$$A\underline{x} = \underline{b} \text{ è compatibile (risolvibile) } \iff \text{rg}(A) = \text{rg}(A|\underline{b})$$

In cui $A|\underline{b}$ è la matrice ottenuta aggiungendo la colonna dei termini noti.
Questo sistema ha una sola soluzione:

$$\text{Soluzione unica } \iff \text{rg}(A) = n$$

11

Operazioni con matrici

11.1 Inverso di una matrice

Inverso di una matrice

Data una matrice A quadrata la matrice inversa è una matrice B tale che:

$$A \cdot B = \text{Id}$$

In cui l'identità per le matrici è:

$$\text{Id} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

11.2 Determinante di una matrice

Definizione di determinante

Data una matrice quadrata A il **determinante** di A è un'applicazione:

$$\det : A \rightarrow \det(A)$$

$$\det = \sum_{p \in S_n} (-1)^{\sigma(p)} a_{1p(1)} \cdot a_{2p(2)} \cdot \dots \cdot a_{np(n)}$$

In cui $\sigma(p)$ è il numero di trasposizioni dell'elemento p di σ (quanti numeri -1).
Il determinante ha delle proprietà:

1. $\det(A_1, \dots, A_n) = 0$ se ci sono due righe uguali o una riga è nulla
2. $\det(A_1, \dots, \lambda A_i, \dots, A_n) = \lambda \det(A)$
3. $\det(A_1, \dots, A_i + A_j, \dots, A_n) = \det(A_1, \dots, A_i, \dots, A_n) + \det(A_1, \dots, A_j, \dots, A_n)$
4. $\det(\text{Id}) = 1$
5. $\det(A) = \det(A^T)$
6. $\det(A_1, \dots, A_i, A_j, \dots, A_n) = -1 \det(A_1, \dots, A_j, A_i, \dots, A_n)$

Esempi:

$$A = \begin{vmatrix} 2 & 5 \\ 7 & 8 \end{vmatrix}$$

$$\det(A) = 2 \cdot 8 - 5 \cdot 7 = -19$$

$$A = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

$$\sigma = S_3 = \{Id, (12), (13), (23), (123), (132)\}$$

$$\det(A) = a_{11}a_{22}a_{33} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}$$

Unicità del determinante

Data \tilde{d} funzione delle righe di una matrice che gode delle regole del determinante allora:

$$\tilde{d}(A) = \det(A)$$

Inoltre:

$$\text{rg}(A) = n \iff \det(A) \neq 0 \iff A \text{ invertibile}$$

Teorema di Binet

Date due matrici quadrate A, B :

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

In una matrice triangolare il determinante si calcola utilizzando i numeri sulla diagonale p_1, p_2, \dots, p_n :

$$\det(A) = p_1 \cdot p_2 \cdot \dots \cdot p_n$$

11.2.1 Sviluppo di Laplace

Data una matrice quadrata A :

$$\begin{vmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i1} & \dots & a_{ij} & \dots & a_{in} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nj} & \dots & a_{nn} \end{vmatrix}$$

Il complemento algebrico di a_{ij} è la matrice che si ottiene eliminando la i -esima riga e la j -esima colonna e viene scritto come A_{ij} .

Da questo posso calcolare il determinante di A :

$$\det(A) (\text{usando una riga } i) = \sum_{k=1}^n (-1)^{i+k} a_{ik} \det(A_{ik})$$

$$\det(A) (\text{usando una colonna } j) = \sum_{k=1}^n (-1)^{j+k} a_{kj} \det(A_{kj})$$

Esempio:

$$A = \begin{vmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 3 \\ 2 & 1 & 1 & 4 \\ 0 & 2 & 3 & -1 \end{vmatrix}$$

$$\det(A) \stackrel{\text{riga 1}}{=} (-1)^{1+1} 0 \det(A_{11}) + (-1)^{1+2} 1 \det(A_{12}) + (-1)^{1+3} 0 \det(A_{13}) + (-1)^{1+4} 0 \det(A_{14}) =$$

$$-1 \det \begin{vmatrix} 0 & -1 & 3 \\ 2 & 1 & 4 \\ 0 & 3 & -1 \end{vmatrix}$$

11.3 Matrice di una funzione su basi

Data una funzione:

$$F : V \rightarrow W$$

In cui B è la base di V e E è la base di W .

Posso creare una matrice $M_{E,B}(F)$ che è la matrice che ha per j -esima colonna $F(b_j)$ scritta usando la base E .

La matrice della funzione inversa è l'inverso della matrice:

$$M_{B,E}(F^{-1}) = (M_{E,B}(F))^{-1}$$

Preso un'altra funzione:

$$S : W \rightarrow U$$

In cui D è la base di U .

Allora:

$$M_{D,B}(S \circ F) = M_{D,E}(S) \cdot M_{E,B}(F)$$

Cambio di base

Se ho una matrice $M_{B,B}(F)$ e voglio cambiargli la base, cioè acendola diventare $M_{E,E}(F)$:

$$M_{E,E}(F) = M_{E,B}(\text{Id}_V) \cdot M_{B,B}(F) \cdot M_{B,E}(\text{Id}_V)$$

12

Autovalori e autovettori

Definizione di autovettore

Data una funzione lineare:

$$T : V \rightarrow V$$

$\underline{v} \neq \underline{0}$ è un **autovettore** se:

$$T\underline{v} = \lambda\underline{v}$$

Se \underline{v} è un autovettore di autovalore $\lambda \implies \alpha\underline{v}$ è anche un autovettore di autovalore λ .

Definizione di autospazio associato ad un autovalore

Data una funzione l'autospazio associato ad un autovalore λ :

$$V_\lambda = \{\underline{v} \in V | T\underline{v} = \lambda\underline{v}\} = \text{Ker}(T - \lambda \text{Id}_V) \leq V$$

12.1 Trovare gli autovalori

Dato un $\lambda \in \mathbb{K}$ è un autovalore se esiste un autovettore associato, cioè:

$$V_\lambda \neq \{\underline{0}\} \iff \text{Ker}(T - \lambda \text{Id}_V) = \text{Ker}(A - \lambda I_n) \neq \{\underline{0}\} \iff \det(A - \lambda I_n) = 0$$

In cui $A = M_{B,B}(T)$ e $I_n = M_{B,B}(\text{Id}_V) = \text{Id}$.

Il polinomio caratteristico di T e in λ :

$$P_T(\lambda) = \det(A - \lambda I_n)$$

Dato un polinomio in λ e λ_0 una radice del polinomio cioè $P(\lambda_0) = 0$:

$$\exists h \geq 1 | P(\lambda) = (\lambda - \lambda_0)^h F(\lambda)$$

h è la molteplicità algebrica (m_a) di λ_0 .

La molteplicità geometrica (m_g) di $\lambda_0 = \dim(\text{Ker}(T - \lambda_0 \text{Id}_V)) = \dim(V_{\lambda_0})$

Per un qualunque autovettore λ_0 :

$$m_g(\lambda_0) \leq m_a(\lambda_0)$$

12.2 Matrice associata alla funzione

Se esiste una base $B = \{v_1, \dots, v_n\}$ di V costituita da autovettori posso scrivere la matrice associata:

$$M_{B,B}(T) = \begin{vmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{vmatrix}$$

Questa matrice è **diagonale**.

Diagonalizzabilità di una matrice

Una matrice è diagonalizzabile se :

$$m_a(\lambda_i) = m_g(\lambda_i) \quad \forall \lambda_i$$

Oppure se ha tutti autovalori diversi.

Inoltre se una matrice A è simmetrica, cioè $A = A^T$ allora è diagonalizzabile.

12.3 Teorema di indipendenza degli autovettori

Autovettori indipendenti

Data una funzione:

$$T : V \rightarrow V$$

Gli autovettori associati agli autospazi di autovalori diversi sono linearmente indipendenti.

Dimostrazione per induzione:

1. Caso base:

$k = 1 \implies$ un autovettore non può essere nullo

2. Ipotesi induttiva:

Supponiamo vero per $k - 1$ autovettori

3. Passo induttivo:

Dati $\{v_1, \dots, v_k\}$ autovettori

$$\alpha_1 v_1 + \dots + \alpha_k v_k = 0 \implies \alpha_k v_k = -\alpha_1 v_1 - \dots - \alpha_{k-1} v_{k-1}$$

$$T(\alpha_1 v_1 + \dots + \alpha_k v_k) = T(0) = \alpha_1 \lambda_1 v_1 + \dots + \alpha_k \lambda_k v_k = \alpha_1 \lambda_1 v_1 + \dots + \alpha_{k-1} \lambda_{k-1} v_{k-1} + \lambda_k (-\alpha_1 v_1 - \dots - \alpha_{k-1} v_{k-1}) = \alpha_1 (\lambda_1 - \lambda_k) + \dots + \alpha_{k-1} (\lambda_{k-1} - \lambda_k) v_{k-1}$$

Per l'ipotesi induttiva:

$$\alpha_1 (\lambda_1 - \lambda_k) = 0, \dots, \alpha_{k-1} (\lambda_{k-1} - \lambda_k) = 0$$

$$\lambda_i - \lambda_j \neq 0 \implies \alpha_1, \dots, \alpha_{k-1} = 0 \implies \alpha_k = 0$$

12.4 Base di autovettori

Data una funzione f con autovalori $\lambda_1, \dots, \lambda_k$ posso scrivere una base di autovettori di f :

$$B = B(V_1) \cup \dots \cup B(V_k)$$

In cui V_k è l'autospazio associato a λ_k .

E

Esercizi

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

E.1.1 Calcolare il MCD e x_0, y_0

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

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

1. Scrivo $b = k_1a + r_1$
2. Scrivo $a = k_2r_1 + r_2$
3. Scrivo $r_1 = k_3r_2 + r_3$
4. Continuo a scrivere $r_{n-1} = k_nr_n + r_{n+1}$ finché $r_{n+1} = 0$ e il $\text{MCD}(a, b) = r_n$

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

$$x_0, y_0 | ax_0 + by_0 = \text{MCD}(a, b)$$

1. Scrivo $\text{MCD}(a, b) = r_{n-2} - k_1r_{n-1}$
2. Sostituisco $r_{n-1} = r_{n-3} - k_2r_{n-2}$
3. Continuo a sostituire $r_i = r_{i-2} - k_jr_{i-1}$ finché $r_{i-2} = b$ e $r_{i-1} = a$ e l'equazione finale sarà del tipo $\text{MCD}(a, b) = ax_0 + by_0$

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

Data un'equazione del tipo:

$$ax + by = c$$

Ha soluzione se $\text{MCD}(a, b) | c$

Trovo x_0 e y_0 tramite il $\text{MCD}(a, b)$

Tutte le soluzioni si trovano con la formula:

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

Esempio:

$$34x + 12y = 8$$

$$34 = 2 \cdot 12 + 10$$

$$12 = 10 + 2$$

$$10 = 5 \cdot 2 \implies \text{MCD}(34, 12) = 2 \implies \text{Risolubile perchè } \text{MCD}(34, 12) = 2 | 8$$

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

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

Data un'equazione del tipo:

$$ax \equiv b \pmod{n}$$

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

Trovo x_0 tramite il $\text{MCD}(n, a)$

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

Esempio:

$$16x \equiv 22(6)$$

$$16 = 6 \cdot 2 + 4$$

$$6 = 4 + 2$$

$$4 = 2 \cdot 2 \implies \text{MCD}(16, 6) = 2 \implies \text{Risolubile perché } \text{MCD}(16, 6) = 2 | 22$$

$$2 = 6 - 4$$

$$= 6 - (16 - 6 \cdot 2)$$

$$= -16 + 6 \cdot 3 \implies x_0 = -1$$

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

Data un'equazione del tipo:

$$ax \equiv 1 \pmod{n}$$

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

Dato un sistema del tipo:

$$\begin{cases} a_1x \equiv b_1 & (n_1) \\ \dots \\ a_sx \equiv b_s & (n_s) \end{cases}$$

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 (se il sistema è già in questa forma non serve modificarlo ulteriormente):

$$\begin{cases} x_1 \equiv c_1 & (r_1) \\ \dots \\ x_s \equiv c_s & (r_s) \end{cases} \quad | \text{MCD}(r_i, r_j) = 1 \forall i \neq j$$

In cui:

$$r_i = \frac{n_i}{\text{MCD}(a_i, n_i)}$$

$$c_i = \frac{b_i}{\text{MCD}(a_i, n_i)} \cdot \underbrace{\left(\frac{a_i}{\text{MCD}(a_i, n_i)} \right)^{-1}}_{\text{inverso di } (\dots) \pmod{r_i}}$$

Questo sistema ha una sola soluzione in $(\pmod{r_1 \cdot r_2 \cdot \dots \cdot r_s})$

Per risolverla scriviamo:

$$R = r_1 \cdot r_2 \cdot \dots \cdot r_s \text{ con } R_k = \frac{R}{r_k}$$

Risolviamo $R_k x \equiv c_k(r_k)$ e troviamo x_k

La soluzione dell'intero sistema:

$$\tilde{x} = R_1 x_1 + \dots + R_s x_s \pmod{r_1 \cdot \dots \cdot r_s}$$

Esempio:

$$\begin{cases} 16x \equiv 12 & (6) \\ 8x \equiv 9 & (5) \\ 34x \equiv 9 & (7) \end{cases} \Rightarrow \begin{cases} \text{MCD}(16, 6) = 2 | 12 \\ \text{MCD}(8, 5) = 1 | 9 \\ \text{MCD}(34, 7) = 1 | 9 \\ \text{MCD}(6, 5) = 1 \\ \text{MCD}(5, 7) = 1 \\ \text{MCD}(7, 6) = 1 \end{cases} \Rightarrow \text{Il sistema è risolvibile}$$

Lo trasformiamo nel sistema:

$$\begin{cases} x_1 \equiv 6 \cdot (8)^{-1} & (3) \\ x_2 \equiv 9 \cdot (8)^{-1} & (5) \\ x_3 \equiv 9 \cdot (34)^{-1} & (7) \end{cases} \Rightarrow \begin{cases} x_1 \equiv 0 & (3) \\ x_2 \equiv 3 & (5) \\ x_3 \equiv 5 & (7) \end{cases}$$

Con $R = 3 \cdot 5 \cdot 7$

$$\begin{cases} 35x_1 \equiv 0 & (3) \\ 21x_2 \equiv 3 & (5) \\ 15x_3 \equiv 5 & (7) \end{cases} \Rightarrow \begin{cases} 2x_1 \equiv 0 & (3) \\ x_2 \equiv 3 & (5) \\ x_3 \equiv 5 & (7) \end{cases} \Rightarrow \begin{cases} x_1 = 0 \\ x_2 = 3 \\ x_3 = 5 \end{cases}$$

$$\tilde{x} = 35 \cdot 0 + 21 \cdot 3 + 15 \cdot 5 = 138(105) = 33$$

E.1.6 Sistemi di equazioni congruenziali con sostituzione

Dato un sistema del tipo:

$$\begin{cases} x_1 \equiv c_1 & (r_1) \\ \dots & | \text{MCD}(r_i, r_j) = 1 \forall i \neq j \\ x_s \equiv c_s & (r_s) \end{cases}$$

Scrivo $x = c_1 + r_1 t_1$ e lo sostituisco nella seconda equazione:

$c_1 + r_1 t_1 \equiv c_2 \pmod{r_2} \Rightarrow$ Risolvo e trovo t_1 a cui aggiungo $r_2 t_2$ e scrivo la nuova formula nella terza equazione, così via finchè il risultato non sarà nella forma $x = k + r_1 r_2 \dots r_s t_s$ e il risultato sarà semplicemente $x = k$

Esempio:

$$\begin{cases} x \equiv 3 & (5) \\ x \equiv 4 & (7) \\ x \equiv 4 & (11) \end{cases}$$

$$x = 3 + 5t_1 \Rightarrow 3 + 5t_1 \equiv 4 \pmod{7} \Rightarrow 5t_1 \equiv 1 \pmod{7} \Rightarrow t_1 = 3 + 7t_2$$

$$x = 3 + 5(3 + 7t_2) = 18 + 5 \cdot 7t_2 \implies 18 + 5 \cdot 7t_2 \equiv 4 \pmod{11} \implies 2t_2 \equiv 8 \pmod{11} \implies t_2 = 4 + 11t_3$$

$$x = 18 + 5 \cdot 7(4 + 11t_3) = 158 + 5 \cdot 7 \cdot 11t_3 \implies x = 158$$

E.1.7 Piccolo teorema di Fermat

Preso un p primo e un'equazione del tipo:

$$a^{kp+h} \pmod{p}$$

Posso risolverla:

$$a^{kp+h} \pmod{p} = a^{kp} \cdot a^h \pmod{p} = \underbrace{a^p \cdot a^p \cdot \dots \cdot a^p}_{k \text{ volte}} \cdot a^h \pmod{p} = \underbrace{a \cdot a \cdot \dots \cdot a}_{k \text{ volte}} \cdot a^h \pmod{p} = a^k \cdot a^h \pmod{p}$$

Esempio:

$$9^{16} \pmod{7} = 9^{14} \cdot 9^2 \pmod{7} = 9^7 \cdot 9^7 \cdot 9^2 \pmod{7} = 9 \cdot 9 \cdot 9^2 \pmod{7} = 9^4 \pmod{7} = 2$$

Preso un p primo e un $a \mid \text{MCD}(a, p) = 1$ e un'equazione del tipo:

$$a^{k(p-1)+h} \pmod{p}$$

Posso risolverla:

$$a^{k(p-1)+h} \pmod{p} = a^{k(p-1)} \cdot a^h \pmod{p} = \underbrace{a^{p-1} \cdot a^{p-1} \cdot \dots \cdot a^{p-1}}_{k \text{ volte}} \cdot a^h \pmod{p} = \underbrace{1 \cdot 1 \cdot \dots \cdot 1}_{k \text{ volte}} \cdot a^h \pmod{p} =$$

$$a^h \pmod{p}$$

Esempio:

$$3^{39} \pmod{8} = 3^{35} \cdot 3^4 \pmod{8} = 3^{7 \cdot 5} \cdot 3^4 \pmod{8} = 1 \cdot 3^4 \pmod{8} = 81 \pmod{8} = 1$$

E.1.8 Sottogruppi di \mathbb{Z}_n

Dato \mathbb{Z}_n devo trovare tutti sottogruppi:

Per ogni divisore k di n esiste un sottogruppo $\langle [\frac{n}{k}] \rangle$ che contiene tutti numeri del tipo $x \cdot \frac{n}{k}$.

Esempio:

$$\mathbb{Z}_{12}$$

$$k = 1, 2, 3, 4, 6, 12$$

- $\langle [\frac{12}{1}] \rangle = \langle [12] \rangle = \{0\}$
- $\langle [\frac{12}{2}] \rangle = \langle [6] \rangle = \{0, 6\}$
- $\langle [\frac{12}{3}] \rangle = \langle [4] \rangle = \{0, 4, 8\}$
- $\langle [\frac{12}{4}] \rangle = \langle [3] \rangle = \{0, 3, 6, 9\}$
- $\langle [\frac{12}{6}] \rangle = \langle [2] \rangle = \{0, 2, 4, 6, 8, 10\}$
- $\langle [\frac{12}{12}] \rangle = \langle [1] \rangle = \mathbb{Z}_{12}$

E.1.9 Invertibili in \mathbb{Z}_n

Dato \mathbb{Z}_n devo trovare tutti gli invertibili cioè i numeri coprimi con n .

La cardinalità di questo insieme è $\varphi(n)$.

fattorizzo n in numeri primi $p_1^{r_1}, p_2^{r_2}, \dots, p_k^{r_k}$ allora :

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

Esempio:

\mathbb{Z}_{15}

$$\varphi(15) = \varphi(3 \cdot 5) = (3^1 - 3^0) \cdot (5^1 - 5^0) = 8$$

$$u(\mathbb{Z}_{15}) = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

E.1.10 Teorema di Eulero

Data un'equazione del tipo:

$$a^{k\varphi(n)+h} \equiv 1 \pmod{n}$$

Possiamo risolverla:

$$a^{k\varphi(n)+h} \equiv 1 \pmod{n} = a^{k\varphi(n)} \cdot a^h \equiv 1 \cdot a^h \equiv 1 \pmod{n}$$

Esempio:

$$23^{123} \equiv 1 \pmod{100} = 23^{123} \equiv 1 \pmod{100} \implies \varphi(100) = (2^2 - 2^1)(5^2 - 5^1) = 40 \implies 23^{123} \equiv 23^{123 \bmod 40} \pmod{100} = 23^{3 \cdot 40 + 3} \equiv 23^3 \equiv 12167 \equiv 67 \pmod{100}$$

E.2 Esercizi sulle permutazioni

E.2.1 Calcolare il supporto di una permutazione

Data una permutazione σ dobbiamo calcolare tutti i numeri tali che $\sigma(j) \neq j$.

Esempio:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 6 & 5 & 1 \end{pmatrix} \implies \text{Supp}(\sigma) = \{1, 3, 4, 6\}$$

E.2.2 Scrivere in cicli una permutazione

Data una permutazione σ dobbiamo scriverla come un prodotto di cicli con supporto disgiunto tra loro. Per farlo dobbiamo trovare dei cicli che partono da un numero e arrivano allo stesso.

Esempio:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 1 & 3 & 4 \end{pmatrix} = (164)(253)$$

E.2.3 Trovare la coniugazione di una permutazione

Date due permutazioni σ, τ scritte in cicli dobbiamo calcolare la coniugazione di σ , cioè la permutazione $\sigma' = \tau\sigma\tau^{-1}$.

Si calcola facendo $\tau\sigma\tau^{-1} = \tau(\text{Ogni elemento di } \sigma)$

Esempio:

$$\sigma = (134)(256)$$

$$\tau = (126)(345)$$

$$\tau\sigma\tau^{-1} = (\tau(1) \tau(3) \tau(4))(\tau(2) \tau(5) \tau(6)) = (245)(631)$$

E.2.4 Trovare la permutazione che coniuga

Data due permutazioni σ, σ' coniugate tra loro dobbiamo calcolare la permutazione τ tale che $\tau\sigma\tau^{-1} = \sigma'$.

Avendo σ e σ' con divisione in cicli della stessa lunghezza, allora τ collegherà il primo numero di σ con il primo di σ' e così via.

Esempio:

$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 6 & 3 \end{pmatrix} = (12)(356)(4) \\ \sigma' &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 5 & 1 & 6 \end{pmatrix} = (23)(145)(6) \\ \tau &= \begin{cases} (12) \rightarrow (23) \implies \begin{cases} 1 \rightarrow 2 \\ 2 \rightarrow 3 \end{cases} \\ (356) \rightarrow (145) \implies \begin{cases} 3 \rightarrow 1 \\ 5 \rightarrow 4 \\ 6 \rightarrow 5 \end{cases} \\ (4) \rightarrow (6) \implies \{4 \rightarrow 6\} \end{cases} = (123)(465)\end{aligned}$$

E.3 Esercizi sui sistemi di equazioni lineari

E.3.1 Passare dai generatori al sistema

E.3.2 Passare dal sistema ai generatori