PREREQUISITI e NON SOLO, per CALCOLO delle PROBABILITÀ

versione di settembre 2024

In questi appunti vengono ricordati alcuni dei prerequisiti e requisiti necessari per affrontare il corso base di Calcolo delle Probabilità
Si tratta di brani tratti da diversi appunti:

Corso propedeutico di Matematica DispenseCorsoPropedeutico_4.pdf
di Dino Boccaletti, Lamberto Lamberti, Luigi Stazi e con la collaborazione di Enrico Casadio Tarabusi

Istituzioni di Mathematiche dispensePaper.pdf
di Piero D'Ancona e Marco Manetti

Introduzione al Calcolo delle Probabilità
di Fabio Spizzichino e Giovanna Nappo
esistono varie versioni, reperibili dai corsi e-learning Sapienza della professoressa Nappo, l'ultima nel corso di Calcolo delle Probabilità (canale 1) a.a. 2024-25

Indice

1 Elementi di teoria degli insiemi

1.1 Introduzione

La Matematica moderna si differenzia da quella classica per un più elevato grado di astrazione: il suo principale interesse è rivolto non tanto a ciò che i singoli oggetti sono: numeri, equazioni, vettori, operazioni, ..., quanto piuttosto alle regole che essi soddisfano; si produce così, da un lato, una notevole economia di pensiero, che consente di applicare una teoria, già stabilita per degli oggetti singoli, ad altri apparentemente molto lontani, e, dall'altro, consente di stabilire analogie insospettate nei vari campi. Riportiamo, a tal proposito, un passo tratto dal volume di Courant - Robbins: *Che cos'è la Matematica*, Ed. Boringhieri:

Attraverso i secoli, i matematici hanno considerato gli oggetti del loro studio, quali ad esempio numeri, punti, ecc., come cose esistenti di per sé. Poiché questi enti hanno sempre sfidato ogni tentativo di un'adeguata descrizione, lentamente sorse nei matematici del XIX secolo l'idea che la questione del significato di questi oggetti come cose sostanziali, se pure ha un senso, non lo avesse nel campo della matematica. Le uniche affermazioni rilevanti che li riguardano non si riferiscono alla realtà sostanziale, e stabiliscono soltanto delle relazioni tra gli oggetti matematicamente non definiti e le regole che governano le operazioni con essi. Nel campo della scienza matematica, non si può, e non si deve discutere ciò che i punti, le rette, i numeri sono effettivamente: ciò che importa e ciò che corrisponde a fatti verificabili sono la struttura e le relazioni, che due punti determinano una retta, che i numeri si combinano secondo certe regole per formare altri numeri, ecc. Uno dei più importanti e fruttuosi risultati dello sviluppo postulazionale moderno è stata una chiara indagine della necessità di rendere astratti i concetti della matematica elementare.

1.2 Prime definizioni

Dopo tali premesse, visto che gli oggetti matematici sono stati svuotati di un preciso significato concreto, è naturale fissare l'attenzione su insiemi astratti, cioè costituiti di elementi la cui natura non interessa.

Un insieme astratto è da intendersi come un concetto primitivo, cioè non descrivibile mediante altri più elementari. Sono sinonimi di insieme le parole famiglia, classe, totalità, ecc.; ogni insieme verrà generalmente indicato con lettere maiuscole: A, B, $\ldots$; inoltre ognuno di essi si penserà formato da elementi di un insieme universale o insieme ambiente S nel quale tutti sono immersi.

> Nell'ambito del Calcolo delle Probabilità di solito si usa il simbolo Ω per l'insieme universale, e si usa la parola Spazio Campionario, o Spazio dei campioni, o Spazio degli eventi elementari.

Come la nozione di insieme, è da intendersi come primitiva la nozione di appartenenza ad un insieme; l'appartenenza di un elemento x ad un insieme A si indica con $x \in A$ o anche $A \ni x$ che si legge:

$$A \text{ contiene } x$$

Se x non appartiene ad A, si scrive $x \notin A$, o anche $A \not\ni x$.

Un insieme A può essere individuato in duplice modo: o mediante le proprietà che caratterizzano i suoi elementi, o elencando, ove possibile, gli elementi che lo compongono, senza tener conto dell'ordine.

Ad esempio l'insieme dei numeri primi compresi tra 10 e 20 può essere descritto come l'insieme costituito dai numeri 11, 13, 17, 19. In simboli si scrive

$$\{11,\ 13,\ 17,\ 19\}$$

mettendo gli elementi 11, 13, 17 e 19 tra due parentesi graffe.

Siano A e B due insiemi, si dice che A è un sottoinsieme di B (o A è contenuto in B), e si scrive

$$A \subset B, \quad \text{o anche} \quad B \supset A,$$

se ogni elemento di A è anche elemento di B:

$$A \subset B \quad \Leftrightarrow \quad (\forall x \in A \Rightarrow x \in B);$$

ATTENZIONE: su alcuni testi si usa la notazione

$$A \subset B \quad \text{per indicare che } A \text{ è un sottoinsieme di } B,$$

e

$$A \subsetneq B, \quad \text{per indicare che } A \text{ è un sottoinsieme proprio di } B$$

In altri testi (come ad esempio negli Appunti Spizzichino-Nappo) si una invece una notazione diversa:

$$A \subseteq B \quad \text{per indicare che } A \text{ è un sottoinsieme di } B,$$

e

$$A \subset B, \quad \text{per indicare che } A \text{ è un sottoinsieme proprio di } B$$

Dovete sempre controllare quale convenzione usa il testo che state leggendo.

La precente formula $A \subset B \quad \Leftrightarrow \quad (\forall x \in A \Rightarrow x \in B)$ va letta nel seguente modo: *"L'insieme A è un sottoinsieme di B se e solo se per ogni x appartenente ad A, ne segue che x appartiene a B"* in quanto

il simbolo	$\Leftrightarrow$	si legge	***se e solo se***,
il simbolo	$\forall$	si legge	***per ogni*** o ***qualsiasi***
il simbolo	$\Rightarrow$	si legge	***implica che***.

Tabella 1 Alcuni simboli matematici.

I due insiemi A e B si dicono coincidenti se e solo se

$$A \subset B \quad \text{e} \quad B \subset A \quad \text{e in tal caso si scrive} \quad A = B.$$

Se $A \subset B$, senza che sia $B = A$, si dice che A è un sottoinsieme proprio di B.

Un comodo modo di raffigurare gli insiemi è attraverso i diagrammi di Eulero-Venn: si traccia in un piano una linea chiusa, e si immagina l'insieme in questione come costituito dai punti indicati all'interno della regione così individuata.

1.3 Operazioni tra insiemi

Dati due o più insiemi, se ne possono costruire altri. Precisamente, dati A e B, si chiama unione di A e B l'insieme $A \cup B$, costituito da tutti gli elementi che verificano **almeno una** delle due seguenti condizioni

$$(i)\ x \in A \quad \text{oppure} \quad (ii)\ x \in B$$

cioè

$$A \cup B = \{x : \ x \in A \text{ e/o } x \in B\}.$$

ESEMPIO: siano $A = \{a, c, d, e, i\}$ e $B = \{b, c, e, g, h\}$, allora

$$A \cup B = \{a, c, d, e, i, b, g, h\}.$$

Si osservi che anche gli elementi che soddisfano entrambe le due condizioni appartengo ad $A \cup B$.

La nozione di unione si generalizza a più insiemi in modo ovvio.

Siano A, B e C tre insiemi, si pone

$$A \cup B \cup C = \{x : \ x \in A \text{ e/o } x \in B, \text{ e/o} x \in C\}$$

A parole $A \cup B \cup C$ è l'insieme i cui elemente appartangono ad almeno uno degli insiemi A, B e C.

Valgono le seguenti proprietà, di verifica immediata
1: $A \cup B = B \cup A$
2: $A \cup (B \cup C) = (A \cup B) \cup C = A \cup B \cup C$
3: $A \cup A = A$
4: $A \cup B \supset B$
5: $A \cup B = B \quad \Leftrightarrow \quad B \supset A$.

Si chiama intersezione di A e B l'insieme $A \cap B$ costituito dagli elementi che appartengono sia ad A, sia a B:

$$A \cap B = \{x : \ x \in A \quad \text{e} \quad x \in B\}.$$

ESEMPIO: siano $A = \{a, c, d, e, i\}$ e $B = \{b, c, e, g, h\}$, allora

$$A \cap B = \{c, e\}.$$

La nozione di intersezione, come la precedente, si generalizza immediatamente a più insiemi.

Siano A, B e C, tre insiemi,

$$A \cap B \cap C = \{x : \ x \in A, \ x \in B, \ x \in C\}.$$

Si noti che la virgola ha la stessa funzione della congiunzione "e".

Valgono le seguenti proprietà :
6: $A \cap B = B \cap A$
7: $A \cap (B \cap C) = (A \cap B) \cap C = A \cap B \cap C$
8: $A \cap A = A$
9: $A \cap B \subset A$
10: $A \cap B = A \quad \Rightarrow \quad A \subset B$.

Teorema 1.1. Unione e intersezione verificano le seguenti proprietà distributive:
proprieta distributiva dell'intersezione rispetto all'unione

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \tag{1}$$

e proprietà distributiva dell'unione rispetto all'intersezione

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \tag{2}$$

da cui, per $B = A$,

$$A \cup (A \cap C) = A, \quad A \cap (A \cup C) = A.$$

Dimostrazione. Occupiamoci della relazione (1) (proprietà distributiva dell'intersezione rispetto all'unione)

> Schema della dimostrazione della (1): si inizia mostrando che
> $$A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$$
> ovvero che
> $$x \in A \cup (B \cap C) \quad \text{implica che} \quad x \in (A \cup B) \cap (A \cup C)$$
> Successivamente si dimostra che
> $$(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$$
> ovvero che
> $$x \in (A \cup B) \cap (A \cup C) \quad \text{implica che } x \in A \cup (B \cap C)$$

Se x appartiene all'insieme a primo membro nella (1) allora

$$x \in A, \quad \text{oppure} \quad x \text{ appartiene contemporaneamente a } B \text{ e } C;$$

in entrambi i casi x appartiene al secondo membro, sicché il primo insieme è contenuto nel secondo, ovvero $x \in A \cup (B \cap C)$

> Riscritto in formule il precedente ragionamento diventa
> $$x \in A \quad \Rightarrow \quad x \in A \cup (B \cap C)$$
> $$x \in A \quad \Rightarrow \quad x \in A \cup (B \cap C)$$

Facciamo ora vedere che anche il secondo insieme della (1) è contenuto nel primo insieme.
Sia dunque x appartenente al secondo insieme, ossia

$$x \in (A \cup B) \cap (A \cup C)$$

allora esso appartiene contemporaneamente ad $A \cup B$ e ad $A \cup C$, ossia, in formule

$$x \in A \cup B, \quad \text{e} \quad x \in A \cup C;$$

se appartiene ad A, allora appartiene anche all'insieme a primo membro, ossia $x \in A \cup (B \cap C)$;
se invece x non appartiene ad A, allora deve appartenere contemporaneamente a B e C, e dunque alla loro intersezione, e quindi x deve appartenere anche ad $A \cup (B \cap C)$.

> Riscritto in formule il precedente ragionamento diventa:
> Per ogni $x \in (A \cup B) \cap (A \cup C)$ sono possibili solo due casi: o $x \in A$ o $x \notin A$ (e un caso esclude l'altro caso)
>
> $$x \in A \quad \Rightarrow \quad x \in A \cup (B \cap C)$$
>
> Poiché
> $$\Big[(x \in A \cup B) \text{ e } (x \notin A)\Big] \quad \Rightarrow \quad x \in B,$$
> e similmente
> $$\Big[(x \in A \cup C) \text{ e } (x \notin A)\Big] \quad \Rightarrow \quad x \in C,$$
> si ha
> $$\Big[\big(x \in (A \cup B) \cap (A \cup C)\big) \text{ e } x \notin A\Big] \quad \Rightarrow \quad \big[(x \in B) \text{ e } (x \in C)\big] \quad \Leftrightarrow \quad x \in B \cap C;$$
> e infine, chiaramente,
> $$x \in B \cap C \quad \Rightarrow \quad x \in A \cup (B \cap C)$$

La relazione (2) (la proprietà distributiva dell'unione rispetto all'intersezione) si dimostra in modo analogo, verificando cioè le due inclusioni:

$$A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C), \quad A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$$

$\square$

In questi appunti, come è usuale, il simbolo $\square$ indica la fine della Dimostrazione: in altri testi si può trovare, con lo stesso significato l'acronimo CDD, Come Dovevasi Dimostrare, o QED, Quod Erat Demonstrandum, usato specialmente nei testi di lingua inglese.

Si chiama insieme vuoto, e si indica con $\emptyset$, l'insieme che non contiene alcun elemento. Ad esempio, tale è l'insieme delle soluzioni reali dell'equazione

$$x^2 = -4,$$

oppure l'insieme dei numeri primi compresi tra 32 e 36.
Si ha
$$A \cup \emptyset = A, \quad A \cap \emptyset = \emptyset, \quad \forall\, A.$$

Differenza e differenza simmetrica di due insiemi.
L'insieme differenza tra l'insieme A e l'insieme B è l'insieme $A \setminus B$ costituito dagli elementi di A che non appartengono a B:
$$A \setminus B := \{x : \ x \in A \text{ e } x \notin B\} = A \cap \overline{B};$$
esso è detto anche il complemento di B in A.
Valgono le ovvie proprietà

$$A \setminus B = A \setminus (A \cap B), \quad A \subset B \ \Leftrightarrow \ A \setminus B = \emptyset, \quad A = (A \setminus B) \cup (A \cap B) = (A \cap \overline{B}) \cup (A \cap B), \quad A \setminus A = \emptyset.$$

> ESEMPIO: siano $A = \{a, c, d, e, i\}$ e $B = \{b, c, e, g, h\}$, allora
> $$A \setminus B = \{a, c, d, e, i\} \setminus \{b, c, e, g, h\} = \{a, d, i\},$$
> $$A \setminus (A \cap B) = \{a, c, d, e, i\} \setminus \{c, e\} = \{a, d, i\}.$$

La differenza simmetrica $A \triangle B$ è l'insieme costituito dagli elementi di A o B privato degli elementi comuni:

$$A \triangle B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A) \text{ quindi } A \triangle B = B \triangle A.$$

Inoltre

$$A \triangle B = \emptyset \quad \Leftrightarrow \quad A = B.$$

ESEMPIO: siano $A = \{a, c, d, e, i\}$ e $B = \{b, c, e, g, h\}$, allora

$$A \triangle B = \{a, c, d, e, i\} \triangle \{b, c, e, g, h\} = \{a, d, i, b, g, h\} = B \triangle A.$$

Se S è l'insieme universale[1], (ossia se tutti gli insiemi che stiamo considerando sono sottoinsiemi di S) ed A è un insieme (ossia $A \subset S$), l'insieme complementare[2] $\overline{A}$ di A, è definito come

$$\overline{A} := S \setminus A.$$

ESEMPIO

$$S = \mathbb{R}, \quad A = \{x : 0 < x < 1\} \;\Rightarrow\; \overline{A} = \{x \in \mathbb{R} : \; x \leq 0 \text{ o } x \geq 1\} = \{x \leq 0\} \cup \{x \geq 1\}.$$

Valgono le proprietà

$$\overline{\overline{A}} = A, \quad \overline{S} = \emptyset, \quad \overline{\emptyset} = S,$$

a parole: il complementare del complementare di un insieme coincide con l'insieme di partenza, il complementare dell'insieme universo è l'insieme vuoto, il complementare dell'insieme vuoto è l'insieme universo.

Valgono anche le seguenti semplici proprietà che discendono dalla regola *tertium non datur*:
dato un insieme A nell'insieme universo S, per ogni $x \in S$ sono possibili solo i seguenti due casi:

$$(1) \quad x \in A, \qquad\qquad (0) \quad x \notin A$$

ovvero, equivalentemente

$$(1) \quad x \in A, \qquad\qquad (0) \quad x \in \overline{A}$$

Si osservi che

$$A \cap \overline{A} = \emptyset, \quad A \cup \overline{A} = S.$$

[1] Nel calcolo delle probabilità invece di insieme universale si parla di spazio campionario Ω.
[2] E' importante sapere che in molti testi si usa anche la notazione A^c, al posto di $\overline{A}$, per indicare l'insieme complementare.

Se, oltre ad A, è dato un secondo insieme B nell'insieme universo S, per ogni $x \in S$ sono possibili solo i seguenti quattro casi:

$$\begin{array}{llll} (1,1) & x \in A \text{ e } x \in B & (1,0) & x \in A \text{ e } x \in \overline{B} \\ (0,1) & x \in \overline{A} \text{ e } x \in B & (0,0) & x \in \overline{A} \text{ e } x \in \overline{B} \end{array}$$

equivalentemente

$$\begin{array}{llll} (1,1) & x \in A \cap B & (1,0) & x \in A \cap \overline{B} \\ (0,1) & x \in \overline{A} \cap B & (0,0) & x \in \overline{A} \cap \overline{B} \end{array}$$

Si osservi che gli insiemi
$H_0 = \overline{A} \cap \overline{B}$, $H_1 = \overline{A} \cap B$, $H_2 = A \cap \overline{B}$, $H_3 = A \cap B$ sono disgiunti a due a due, ossia

$$H_0 \cap H_1 = H_0 \cap H_2 = H_0 \cap H_3 = H_1 \cap H_2 = H_1 \cap H_3 = H_2 \cap H_3 = \emptyset,$$

e la loro unione coincide con l'insieme universo, ossia

$$H_0 \cup H_1 \cup H_2 \cup H_3 = S.$$

Una famiglia finita di sottoinsiemi di S

$$\mathcal{H} = \{H_1, H_2, ..., H_m\}$$

tali che disgiunti a due a due e la loro unione coincide con S

$$H_i \cap H_j = \emptyset, \text{ per ogni } i, j \in \{1, 2, ..., m\} \text{ con } i \neq j, \quad \text{e} \quad \bigcap_{i=1}^{m} H_i = \Omega$$

è detta **partizione** (finita) di S.

Le famiglie

$$\{A, \overline{A}\} \quad \text{e} \quad \{A \cap B, A \cap \overline{B}, \overline{A} \cap B, \overline{A} \cap \overline{B}\}$$

delle note precedenti sono esempi di partizioni.

La nozione di partizione si estende anche al caso di famiglie numerabili:

$$\mathcal{H} = \{H_1, H_2, ..., H_m, ...\} = \{H_i,\ i \geq 1\}$$

è una partizione (numerabile) di S se e solo se

$$H_i \cap H_j = \emptyset, \text{ per ogni } i, j \geq 1 \text{ interi con } i \neq j, \quad \text{e} \quad \bigcap_{i=1}^{\infty} H_i = \Omega$$

Come sappiamo nell'ambito del Calcolo delle Probabilità l'insieme universo S è detto spazio campionaio e si usa il simbolo Ω. Nel caso in cui Ω sia finito o infinito numerabile, i sottoinsiemi di Ω rappresentano degli eventi.
Se A e B rappresentano due eventi (che per semplicità di notazione continuiamo a denotare con A e B) e $A \cap B = \emptyset$, si dice che i due eventi A e B sono **incompatibili**, mentre se H_i, per $i = 1, 2, ..., m$ (o per $i \geq 1$) rappresentano degli eventi e godono della proprietà che la loro unione è tutto Ω si dice che gli eventi H_i sono **esaustivi**.
Con questa terminologia una famiglia $\mathcal{H} = \{H_1, H_2, ..., H_m\}$ o $\mathcal{H} = \{H_i,\ i \geq 1\}$ è una **partizione** (dell'evento certo) se e solo se gli eventi H_i sono **incompatibili a due a due** e sono **esaustivi**.
A volte si usa anche dire che gli eventi H_i **formano una partizione** (dell'evento certo) se e solo se sono esaustivi e incompatibili a due a due.

Teorema 1.2 (Regole di De Morgan). Unione, intersezione e passaggio al complementare verificano le relazioni

$$\overline{A \cap B} = \overline{A} \cup \overline{B}, \quad \overline{A \cup B} = \overline{A} \cap \overline{B}.$$

Basta dimostrare solo la prima relazione, ossia

$$\overline{A \cap B} = \overline{A} \cup \overline{B}.$$

Infatti la seconda relazione si ottiene applicando la prima ai complementari di A e B, per cui si ottiene che

$$\overline{(\overline{A} \cap \overline{B})} = \overline{\overline{A}} \cup \overline{\overline{B}}, \quad \Leftrightarrow \quad \overline{(\overline{A} \cap \overline{B})} = A \cup B,$$

dove l'equivalenza deriva dalla proprietà che il complementare del complementare di un insieme è l'insieme stesso.
A questo punto basta considerare i complementari di ambo i membri dell'ultima uguaglianza

$$\overline{\overline{(\overline{A} \cap \overline{B})}} = \overline{A \cup B} \quad \Leftrightarrow \quad \overline{A} \cap \overline{B} = \overline{A \cup B}.$$

Dimostrazione. Se x appartiene al primo insieme, ossia $x \in \overline{A \cap B}$, allora x è un elemento di S che non appartiene ad A e B contemporaneamente, e pertanto verifica una delle seguenti condizioni:

$a)$ x non appartiene ne' ad A ne' a B;	$\Leftrightarrow$	$x \in \overline{A} \cap \overline{B}$,	si osservi che	$\overline{A} \cap \overline{B} \subset \overline{A} \cup \overline{B}$
$b)$ x appartiene ad A ma non a B;	$\Leftrightarrow$	$x \in A \cap \overline{B}$	si osservi che	$A \cap \overline{B} \subset \overline{B} \subset \overline{A} \cup \overline{B}$
$c)$ x appartiene a B ma non ad A;	$\Leftrightarrow$	$x \in B \cap \overline{A}$	si osservi che	$\overline{A} \cap B \subset \overline{A} \subset \overline{A} \cup \overline{B}$

in ognuno di questi casi appartiene all'insieme a secondo membro e dunque il primo insieme è contenuto nel secondo.

Si osservi che i tre casi $a)$, $b)$ e $c)$ si escludono a vicenda.

Viceversa, se x appartiene al secondo insieme, ossia $x \in \overline{A} \cup \overline{B}$, vale una delle seguenti condizioni
(i) x sta nel complementare di A,
(e dunque non appartiene ad A, e quindi nemmeno all'intersezione di A con B),

$$x \in \overline{A} \quad \Leftrightarrow \quad x \notin A \quad \Rightarrow \quad x \notin A \cap B \quad \Leftrightarrow \quad x \in \overline{A \cap B}$$

o
(ii) x sta nel complementare di B,
(e dunque non appartiene ad B, e quindi nemmeno all'intersezione di A con B),

$$x \in \overline{B} \quad \Leftrightarrow \quad x \notin B \quad \Rightarrow \quad x \notin A \cap B \quad \Leftrightarrow \quad x \in \overline{A \cap B}$$

o, infine
(iii) x sta nel complementare di entrambi (ossia x è sia nel complementare di A che nel complementare di B)
(e dunque non appartiene ad A e nemmemo a B, e quindi nemmeno all'intersezione di A con B);

$$x \in \overline{A} \cap \overline{B}, \quad \Rightarrow \quad x \notin A \quad \Rightarrow \quad x \notin A \cap B \quad \Leftrightarrow \quad x \in \overline{A \cap B}$$

in ogni caso appartiene al primo insieme, ossia al complementare di $A \cap B$, e in conclusione il secondo insieme, $\overline{A} \cup \overline{B}$ è contenuto nel primo.

Si osservi che i tre casi (i), (ii) e (iii) non si escludono a vicenda. Si potrebbero equivalentemente considerare i seguenti tre casi, che si escludono a vicenda, considerando che

$$\overline{A} \cup \overline{B} = (\overline{A} \cap B) \cup (\overline{B} \cap A) \cup (\overline{A} \cap \overline{B})$$

Pertanto i due insiemi coincidono. $\square$

Le regole di De Morgan si generalizzano al caso di più insiemi:

$$\overline{A \cap B \cap C \cap ...} = \overline{A} \cup \overline{B} \cup \overline{C} \cup ...$$

$$\overline{A \cup B \cup C \cup ...} = \overline{A} \cap \overline{B} \cap \overline{C} \cap ...$$

o, più in generale e sinteticamente, per ogni insieme I e collezione di sottoinsiemi di S, si ha

$$\overline{\bigcup_{i \in I} A_i} = \bigcap_{i \in I} \overline{A}_i$$

Dato un insieme A contenente n elementi, si definisce insieme delle parti l'insieme che ha come elementi i sottoinsiemi di A, compresi l'insieme stesso e l'insieme vuoto.

ESEMPIO: Per l'insieme $A = \{1, 2, 3\}$, l'insieme delle parti è l'insieme

$$\mathcal{P}(A) = \big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\big\}$$

Esercizio 1.4.
(1) Dimostrare che $A \cup B = \emptyset \quad \Rightarrow \quad A = \emptyset$ e $B = \emptyset$.
(2) Dimostrare che se $A \cup B = A \cup C$, non necessariamente $B = C$ (non vale la legge di cancellazione)
(3) $(A \cup B) \cap C = A \cup (B \cap C)$?
(4) Si considerino l'insieme A dei numeri interi divisibili per 3, l'insieme B dei numeri interi divisibili per 5, l'insieme C dei numeri interi divisibili per 20.
Determinare $A \cap B$, $A \cup B$, $A \cap B \cap C$, $A \cup B \cup C$, $(A \cap B) \cup C$, $(A \cup B) \cap C$.
(5) Dimostrare che $(A \cup B) \cap \overline{B} = A \quad \Leftrightarrow \quad A \cap B = \emptyset$.

1.4 I numeri naturali.

È consuetudine indicare con $\mathbb{N}$ l'insieme dei numeri naturali:

$$\mathbb{N} = \{1, 2, 3, ...\}$$

Va detto che in alcuni testi $\mathbb{N}$ denota l'insieme $\{0, 1, 2, 3, ...\}$, ovvero viene incluso lo zero. Per evitare confusione, quando lo zero è incluso scriveremo $\mathbb{N} \cup \{0\}$ oppure $\mathbb{N}_0$.

Nell'insieme dei numeri naturali sono definite le ordinarie operazioni di somma e di prodotto, le quali, ad ogni coppia di numeri naturali, associano ancora un numero naturale: si dice che l'insieme $\mathbb{N}$ è chiuso rispetto alle operazioni anzidette.
Per poter definire anche la sottrazione, bisogna introdurre l'insieme $\mathbb{Z}$ degli interi relativi:

$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$$

ed infine, per dar senso all'operazione di divisione, l'insieme $\mathbb{Q}$ dei numeri razionali, cioè l'insieme delle frazioni, intese come rapporto di numeri interi, con l'avvertenza che il denominatore sia diverso da zero:

$$\mathbb{Q} = \left\{\frac{a}{b} : \ a \in \mathbb{Z},\, b \in \mathbb{Z},\, b \neq 0\right\}$$

Unitamente ai numeri irrazionali, gli insiemi precedenti costituiscono l'insieme $\mathbb{R}$ dei numeri reali.

1.5 Prodotto cartesiano

Dati due insiemi A e B, si chiama prodotto cartesiano di A per B, nell'ordine, l'insieme $A \times B$ costituito dalle coppie ordinate (a, b) con $a \in A$ e $b \in B$. Sottolineiamo che le coppie sono ordinate, nel senso che, ad esempio, si deve intendere $(a, b) \neq (b, a)$ per $a \neq b$.

I due prodotti cartesiani $A \times B$, $B \times A$ sono in genere diversi. Ad esempio, se $A = \{1, 2\}$ e $B = \{3, 4, 5\}$ si ha

$$A \times B = \{(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5)\},$$

mentre

$$B \times A = \{(3, 1), (3, 2), (4, 1), (4, 2), (5, 1), (5, 2)\}.$$

L'insieme delle coppie ordinate di numeri reali si indica con $\mathbb{R} \times \mathbb{R}$; se poi si introduce su un piano un sistema di coordinate cartesiane ortogonali, si può rappresentare la coppia (a, b) come il punto di coordinate (a, b).

Per generalizzazione, l'insieme

$$\mathbb{R}^n = \overbrace{\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R} \times \mathbb{R}}^{n \text{ volte}},$$

prodotto cartesiano dell'insieme dei numeri reali per sé stesso, n volte, è l'insieme delle n-ple ordinate di numeri reali.

Esercizio 2.1. Dimostrare che

$$(A \cap B) \times C = (A \times C) \cap (B \times C), \quad (A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D).$$

1.6 Funzioni

Siano A ed B due insiemi: si dice che f è una funzione, o un'applicazione di A in B

$$f : \ A \to B; \quad x \mapsto f(x)$$

se essa costituisce un procedimento, una legge, che ad ogni elemento $x \in A$ associa uno ed un solo elemento y di B.

Se l'insieme A è finito basta anche elencare tutte le associazioni: ad esempio se $A = \{a, c, d, e, i\}$ e $B = \{b, c, e, g, h\}$, ecco due funzioni di A in B:

$$\begin{array}{ll} f_1 : \ A \to B & f_2 : \ A \to B \\ \quad a \mapsto f_1(a) = c & \quad a \mapsto f_2(a) = c \\ \quad c \mapsto f_1(c) = b & \quad c \mapsto f_2(c) = b \\ \quad d \mapsto f_1(d) = b & \quad d \mapsto f_2(d) = g \\ \quad e \mapsto f_1(e) = g & \quad e \mapsto f_2(e) = h \\ \quad i \mapsto f_1(i) = b & \quad i \mapsto f_2(i) = e \end{array}$$

L'elemento che corrisponde ad x viene indicato con $f(x)$, ed $f(x)$ è detto **immagine** di x tramite f. Il fatto che ad ogni x corrisponda un solo y si esprime dicendo che la corrispondenza definita da f è univoca. L'insieme A si chiama **dominio** della funzione f, l'insieme B dove la funzione assume i valori si chiama **codominio** della funzione f.

Esempio 1.1.
(1) Sia $A = \mathbb{R} \setminus \{0\}$, $B = \mathbb{R}$; la corrispondenza $f : \ A \to B$ definita da $f(x) = 1/x$ è una funzione;
(2) Sia $A = [-1, 1]$, $B = [0, 1]$; la $f : \ A \to B$ definita da $f(x) = x^2$ è una funzione;
(3) Sia $A = [0, 1]$, $B = [-1, 1]$, la legge che associa ad ogni $x \in [0, 1]$ i valori di $y \in [-1, 2]$ tali che $y^2 = x$,

non determina una funzione $f:\ A \to B$, dato che, al medesimo $x \neq 0$ vengono associati due valori di y.

Una funzione $f:\ A \to B$ è detta
• **suriettiva** se ogni $y \in B$ è immagine di almeno un $x \in A$:

$$f:\ A \to B \quad \text{è suriettiva se } \ \text{per ogni } y \in B, \ \text{esiste } x \in A \text{ tale che } f(x) = y;$$

in formule

$$f:\ A \to B \quad \text{è suriettiva se } \ \forall\, y \in B,\ \exists\, x \in A:\ f(x) = y;$$

• **iniettiva** se elementi distinti di A hanno immagini distinte in B:

$$f:\ A \to B \quad \text{è iniettiva se } \ (x_1, x_2 \in A, \ \text{con } x_1 \neq x_2) \text{ implica che } f(x_1) \neq f(x_2).$$

in formule

$$f:\ A \to B \quad \text{è iniettiva se } \ (x_1, x_2 \in A,\ x_1 \neq x_2) \ \Rightarrow\ f(x_1) \neq f(x_2).$$

La grafia	$\exists x \in A$	sostituisce l'affermazione	*esiste* $x \in A$.
Il simbolo il simbolo analogo	$\exists$ $\nexists$	si legge si legge	*esiste*, *non esiste*.
Il simbolo dei due punti	:	spesso sostituiscono la frase	*tali che* o *tale che*.

Tabella 2 simboli

La funzione f_1 della nota precedente non è ne' suriettiva ne' iniettiva, mentre la funzione f_2 è sia suriettiva che iniettiva. Queste funzioni hanno una particolare importanza.

Si dice che una funzione $f:\ A \to B$ è
• una corrispondenza **biunivoca** o una funzione **biettiva** se f è contemporaneamente suriettiva ed iniettiva: ossia
(i) elementi distinti di A hanno per immagine punti distinti di B,
(ii) ogni elemento di $y \in B$ è immagine di uno e uno solo elemento $x \in A$.

L'insieme delle immagini dei punti x al variare di x in A è detto **immagine di** A **tramite** f, e si indica con:

$$f(A) = \{y \in B:\ \exists x \in A, \text{con}\, y = f(x)\}$$

L'insieme $f(A)$ è un sottoinsieme di B, ed è un sottoinsieme proprio se f non è suriettiva.
Per ogni sottoinsieme $I \subset B$ del codominio si definisce la **controimmagine di** I **tramite** f come l'insieme dei punti $x \in A$ tali che $f(x)$ appartiene a I

$$f^{-1}(I) = \big\{x \in A:\ f(x) \in I\big\}$$

Siano $A = \{a, c, d, e, i\}$ e $B = \{b, c, e, g, h\}$, e sia $f:\ A \to B$, definita da

$$\begin{gathered} a \mapsto f(a) = c \\ c \mapsto f(c) = b \\ d \mapsto f(d) = b \\ e \mapsto f(e) = g \\ i \mapsto f(i) = b \end{gathered}$$

Mentre B è il codominio di f, l'immagine di A tramite f, ossia l'insieme $f(A)$, è dato da:

$$f(A) = \{y \in B:\ \exists x \in A, \text{con}\, y = f(x)\} = \{b, c, g\} \subsetneq B,$$

Inoltre si ha che $f^{-1}(\{c, g\}) = \{a, e\}$, $f^{-1}(\{e, h\}) = \emptyset$, $f^{-1}(\{b\}) = \{c, d, i\}$

Osservazione 1.2. A volte si indica come codominio di f l'insieme $f(A)$ stesso: è chiaro che, con questa definizione, f è (automaticamente) suriettiva.

Esempio 1.3.
(1) La funzione $f: \ x \mapsto sin(x)$,
con dominio $A = [0, 2\pi]$ e codominio $B = \mathbb{R}$, **non è ne' suriettiva ne' iniettiva**:
non è suriettiva perché, ad esempio,
non esiste nessun $x \in A$ tale che $\sin(x) = 2$, inoltre l'immagine di f è $f(A) = \sin([0, 2\pi]) = [-1, 1] \subsetneq \mathbb{R}$,
e non è iniettiva perché, ad esempio, $\sin(0) = \sin(\pi) = 0$.
con dominio $A = [0, 2\pi]$ e codominio $B = [-1, 1]$ è suriettiva, ma non è iniettiva;
con dominio $A = [-\pi/2, \pi/2]$ e codominio $B = [-1, 1]$ è invece sia suriettiva che iniettiva
(2) La funzione $f: \ A \to B$, ove $A = B = \mathbb{N}$, che associa ad ogni numero naturale il suo quadrato non è suriettiva: esistono in $B = \mathbb{N}$ numeri che non sono quadrati di numeri naturali;
(3) La corrispondenza tra ciascun punto di un segmento verticale illuminato da una lampada e la sua ombra è biunivoca (si suppone che la lampada sia posta sufficientemente in alto e non sia sul prolungamento del segmento).

Funzione inversa
Se $f: \ A \to B$ è biettiva, ogni $y \in B$ è immagine di uno e un solo $x \in A$; ha senso allora considerare la funzione inversa
$$f^{-1}: \ B \mapsto A$$
la quale associa ad ogni $y \in B$ il punto $x \in A$ tale che $f(x) = y$; si scrive
$$y \mapsto x = f^{-1}(y).$$
Pertanto, nella corrispondenza inversa, la y diventa la variabile indipendente, mentre la x funge da variabile dipendente.

ESEMPIO: Siano $A = \{a, c, d, e, i\}$ e $B = \{b, c, e, g, h\}$. La seguente funzione$f$ è biunivoca e la sua inversa si ottiene immediatamente (sostanzialmente "*invertendo le frecce* $\mapsto$")

$f: \ A \to B$	$f^{-1}: \ B \to A$
$a \mapsto f(a) = c$	$c \mapsto f^{-1}(c) = a$
$c \mapsto f(c) = b$	$b \mapsto f^{-1}(b) = c$
$d \mapsto f(d) = g$	$g \mapsto f^{-1}(g) = d$
$e \mapsto f(e) = h$	$h \mapsto f^{-1}(h) = e$
$i \mapsto f(i) = e$	$e \mapsto f^{-1}(e) = i$

4. La cardinalità

I numeri naturali rappresentano l'operazione del contare: *fissato un insieme A, quanti elementi ha l'insieme A?*
Un elemento, due, tre,..., 1000, ecc.
Dopo aver contato gli elementi di due insiemi si riconosce, a volte, che....
...hanno lo stesso numero di elementi, e si riconosce anche che tra i due insiemi si può stabilire una corrispondenza biunivoca.

La cardinalità di un insieme A è quindi n se e solo se si può mettere in corrispondenza biunivoca con l'insieme $\{1, 2, ..., n\}$.

Si usa il simbolo $|A|$ per indicare il numero degli elementi di A, ossia $|A|$ è la cardinalità dell'insieme A.

L'insieme $A = \{a, c, d, e, i\}$ ha cardinalità 5 e si può mettere in corrispondenza biunivoca con l'insieme $\{1, 2, 3, 4, 5\}$ (anche in più di un modo):

$$\begin{aligned} f_1 : A &\to \{1,2,3,4,5\} \\ a &\mapsto 1 \\ c &\mapsto 2 \\ d &\mapsto 3 \\ e &\mapsto 4 \\ i &\mapsto 5 \end{aligned} \qquad\qquad \begin{aligned} f_2 : A &\to \{1,2,3,4,5\} \\ a &\mapsto 3 \\ c &\mapsto 2 \\ d &\mapsto 5 \\ e &\mapsto 4 \\ i &\mapsto 1 \end{aligned}$$

L'insieme $\mathbb{N}$ dei numeri naturali è infinito, e tutti gli insiemi che si possono mettere in corrispondenza biunivoca con $\mathbb{N}$ si dicono numerabili.

Una volta incontrati insiemi non finiti la domanda

dato un insieme non finito A, quanti elementi ha l'insieme A?

può essere *imbarazzante* e non è chiaro immediatamente come rispondere. Invece il valutare se due insiemi (anche non finiti) abbiano lo stesso numero di elementi appare ragionevole e viene tradotta nel chiedere che esista una corrispondenza biunivoca tra loro, ma conduce a *scoperte* sorprendenti:

Ad esempio, sia A l'insieme dei numeri naturali pari, l'insieme $\mathbb{N}$ dei numeri naturali ed A possono essere messi in corrispondenza biunivoca fra loro:
· ad ogni $n \in \mathbb{N}$ facciamo corrispondere il numero pari $2n \in A$,
· ad ogni $p \in A$ facciamo corrispondere la sua metà $p/2 \in \mathbb{N}$.

Sia per insiemi finiti che per insiemi infiniti, l'esistenza di corrispondenze biunivoche tra due insiemi A e B viene sintetizzata nella frase A e B hanno la stessa cardinalità. Quindi, ad esempio $\mathbb{N}$ e l'insieme A dei numeri naturali pari hanno la stessa cardinalità: la sorpresa consiste nel fatto che A è un sottoinsieme proprio di $\mathbb{N}$:

$$A \subset \mathbb{N}, \quad A \neq \mathbb{N}.$$

Da questo esempio impariamo che gli insiemi infiniti possono avere la stessa cardinalità pur essendo uno sottinsieme proprio dell'altro, circostanza che invece è impossibile nel caso finito.

Cardinalità del prodotto cartesiano di insiemi finiti

Dati due insiemi A e B due insiemi finiti, con $|A| = n$ e $|B| = m$ allora il prodotto cartesiano $A \times B$ ha cardinalità $n \cdot m$, in formule

$$|A \times B| = |A| \cdot |B|$$

Questa proprietà discende immediatamente dal fatto che, se indiciamo con

$$A = \{a_1, a_2, ..., a_n\}, B = \{b_1, b_2, ..., b_m\}$$

tutti gli elementi del prodotto cartesiano $A \times B$ si possono mettere in una tabella di n righe ed m colonne:

$$\begin{array}{ccccc} (a_1, b_1) & (a_1, b_2) & \cdots & \cdots & (a_1, b_m) \\ (a_2, b_1) & (a_2, b_2) & \cdots & \cdots & (a_2, b_m) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (a_n, b_1) & (a_n, b_2) & \cdots & \cdots & (a_n, b_m) \end{array}$$

che chiaramente è composta da $n \cdot m$ coppie.

Questa proprietà si estende al caso di prodotti cartesiani, ossia dati A, B e C tre insiemi finiti si ha

$$|A \times B \times C| = |A| \cdot |B| \cdot |C|$$

e ancora più in generale dati ℓ insiemi finiti A_1, A_2,..., A_ℓ, si ha

$$|A_1 \times A_2 \times \cdots \times A_\ell| = |A_1| \cdot |A_2| \cdots |A_\ell|$$

ESEMPIO: siano $A_1 = A_2 = \cdots = A_\ell = A = \{0, 1\}$ Allora il prodotto cartesiano $A_1 \times A_2 \times \cdots \times A_\ell$ si scrive anche come A^ℓ, e si ha

$$A^\ell = \big\{(x_1, x_2, ..., x_\ell) : \; x_i \in \{0, 1\}, \, \forall\, i = 1, 2, ..., \ell\big\}$$

e

$$|A^\ell| = |A|^\ell = 2^\ell$$

Quando $A_1 = A_2 = \cdots = A_\ell = A$, può essere interessante pensare al prodotto cartesiano

$$A_1 \times A_2 \times \cdots \times A_\ell = \underbrace{A \times A \times \cdots \times A}_{\ell\,\text{volte}} = A^\ell$$

come la famiglia delle funzioni con dominio $\{1, 2, ..., \ell\}$ e codominio A. Infatti ogni elemento del prodotto cartesiano individua naturalmente una funzione e viceversa.

Per capire il legame tra A^ℓ e le funzioni da $\{1, 2, ..., \ell\}$ all'insieme A, facciamo un esempio: sia $A = \{a, b, c, d\}$ ed $\ell = 3$.
All'elemento $(a, a, b) \in A^3$ possiamo associare la funzione

$$f : \; \{1, 2, 3\} \to A; \quad 1 \mapsto f(1) = a, \quad 2 \mapsto f(2) = a, \quad 3 \mapsto f(3) = b$$

Viceversa data una funzione

$$g : \; \{1, 2, 3\} \to A; \quad 1 \mapsto g(1) = d, \quad 2 \mapsto g(2) = a, \quad 3 \mapsto g(3) = c$$

possiamo associare l'elemento $(d, a, c) \in A^3$.

4.1. L'insieme delle parti.

Assegnato un insieme A indichiamo con $\mathcal{P}(A)$ l'insieme dei sottoinsiemi di A.

Così, ad esempio, se $A = \{1, 2, 3\}$ riesce

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Nel caso degli insiemi finiti vale il seguente semplice risultato:

se un insieme finito A ha cardinalità n allora $\mathcal{P}(A)$ ha cardinalità 2^n.

L'insieme delle parti di $A = \{a_1, \cdots, a_n\}$ ha cardinalità 2^n

Denotiamo con $\mathcal{P}(\{a_1, \cdots, a_n\})$ l'insieme delle parti di $A = \{a_1, \cdots, a_n\}$. Per mostrare che $|\mathcal{P}(\{a_1, \cdots, a_n\})| = 2^n = 2^{|A|}$ possiamo procedere come segue: $\mathcal{P}(\{a_1, \cdots, a_n\})$ è in corrispondenza biunivoca con l'insieme delle funzioni $g : \{a_1, \cdots, a_n\} \mapsto \{0, 1\}$. La corrispondenza è data da $G \longleftrightarrow g = \mathbf{1}_G$, dove

$$\mathbf{1}_G(a_i) = 1, \qquad se \quad a_i \in G$$

$$\mathbf{1}_G(a_i) = 0, \qquad se \quad a_i \notin G.$$

Queste ultime sono tante quanti sono gli elementi del prodotto cartesiano di $\{0, 1\} \times \{0, 1\} \times \cdots \{0, 1\}$ (n volte) e sono quindi 2^n.
Per capire meglio la corrispondenza poniamo $n = 4$ e consideriamo, ad esempio, il sottoinsieme $G = \{a_1, a_3\}$:

$$\{a_1, a_3\} \qquad \Longleftrightarrow \qquad \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 0 & 1 & 0 \end{pmatrix} \qquad \Longleftrightarrow \qquad (1, 0, 1, 0) \in \{0, 1\}^4.$$

Ancora, ad esempio $(0, 0, 0, 0)$ corrisponde all'insieme vuoto, e $(1, 1, 1, 1)$ a tutto $A = \{a_1, a_2, a_3, a_4\}$. Nel caso generale di $A = \{a_1, a_2, \ldots, a_n\}$, la corrispondenza tra i sottoinsiemi di A e gli elementi di $\{0, 1\}^n$ dovrebbe essere quindi chiara, e di conseguenza l'uguaglianza $|\mathcal{P}(\{a_1, \cdots, a_n\})| = 2^n$.

Esiste un teorema che afferma che, dato un insieme A, finito o infinito, $\mathcal{P}(A)$ ha cardinalità maggiore di quella di A, ovvero che non esistono corrispondenze biunivoche tra A e $\mathcal{P}(A)$.

Tra le conseguenze di tale teorema, nel caso degli insiemi infiniti, c'è il risultato di Cantor relativo all'esistenza di insiemi di cardinalità comunque grandi:
• l'insieme $A = \mathcal{P}(\mathbb{N})$ delle parti di $\mathbb{N}$ ha cardinalità maggiore di quella di $\mathbb{N}$,
• l'insieme $B = \mathcal{P}(A)$ delle parti di $A = \mathcal{P}(\mathbb{N})$ ha cardinalità maggiore di quella di A, ecc. ecc.

1.7 Calcolo Combinatorio

Le nozioni di calcolo cambinatorio necessari si possono trovare negli appunti Introduzione al Calcolo delle Probabilità di Spizzichino e Nappo e in particolare nelle sezioni "Calcolo combinatorio: primi elementi", "Alcune proprieta dei coefficienti binomiali", "Approfondimenti sui primi elementi di calcolo combinatorio", "Approfondimenti di Calcolo Combinatorio". In questi appunti C_k^n denota il numero delle combinazioni[3] di n elementi di classe k.
Invece D_k^n denota il numero delle disposizioni di [4] di n elementi di classe k.
Infine $P_m = D_m^m$ è il numero delle permutazioni [5] di m elementi.

È importante sapere che molte formule di calcolo combinatorio si possono ottenere "a parole", ossia anche senza usare formule matematiche, come ad esempio

$$C_0^n = C_n^n = 1, \text{ e } \quad C_k^n = C_{n-k}^n, \quad C_k^n = C_k^{n-1} + C_{k-1}^{n-1}, \quad P_k \cdot C_k^n = D_k^n, \qquad 1 \leq k \leq n-1.$$

[3]Una combinazione di n elementi di classe k è una k-pla di elementi distinti di un insieme di cardinalità n, senza tenere conto dell'ordine, o equivalentemente un sottoinsieme di cardinalità k di un insieme con n elementi.

[4]Una disposizione di n elementi di classe k è una k-pla di elementi distinti di un insieme di cardinalità n, in cui si tiene conto dell'ordine.

[5]Una permutazione di m elementi è uno dei possibili modi di ordinare gli m elementi di un insime, ovvero è semplicemente una disposizione di m elelemnti di classe m

Alcuni esempi di quanto appena detto si possono trovare nella sezione "Approfondimenti sui primi elementi di calcolo combinatorio", alla cui fine si trova il seguente cenno al Principio fondamentale del calcolo combinatorio, che permette di calcolare

$$D_k^n = \overbrace{n(n-1)(n-2)\cdots(n-(k-1))}^{k \text{ fattori}} = \frac{n!}{(n-k)!},$$

e quindi

$$P_m = m!, \quad C_k^n = \frac{D_k^n}{P_k} = \frac{n!}{k!(n-k)!} =: \binom{n}{k}.$$

Principio fondamentale del calcolo combinatorio

Come nel caso del calcolo della cardinalità dell'insieme delle Disposizioni, ossia del numero D_k^n delle disposizioni senza ripetizione, può accadere che gli elementi di un insieme G possano essere determinati con in h passi uno dopo l'altro, e in modo che per ciascun passo il numero delle possibili scelte sia un numero prefissato: al primo passo ci siano m_1 scelte possibili, al secondo passo ce ne siano m_2, . . . , all'h-simo passo ce ne siano m_h. Se inoltre accade che sequenze distinte delle h scelte determinano elementi distinti dell'insieme G, in altre parole due sequenze diverse di scelte danno luogo a due elementi diversi di G, allora

$$|G| = m_1 \cdot m_2 \cdots m_h.$$

Non diamo una dimostrazione formale di questa affermazione, detta appunto **Principio fondamentale del calcolo combinatorio** è spesso usato ma bisogna stare attenti a controllare bene che effettivamente le h scelte diverse diano effettivamente luogo ad elementi diversi, altrimenti si può incorrere in errori.

In questa sezione aggiungiamo il seguente esempio, particolarmente interessante.

Esempio 1.1. *Dimostrare che*

$$C_k^n \cdot k = n \cdot C_{k-1}^{n-1} = C_{k-1}^n \cdot (n-1)$$

usando il seguente esempio:
In un condominio con n proprietari contare il numero dei modi in cui si può scegliere una giunta di k ($k < n$) condomini di cui uno sia il presidente.

metodo 1) si scelgono i k membri della giunta e poi si sceglie il presidente

metodo 2) si sceglie prima il presidente e poi i rimanenti $k-1$ membri della giunta

metodo 3) si scelgono prima i $k-1$ membri della giunta (NON presidenti) e tra i rimanenti si sceglie il presidente

Si consiglia poi di controllare che la formula precedente permette di usare le seguenti ugualianze

$$\binom{n}{k} \cdot k = n \cdot \binom{n-1}{k-1} = \binom{n}{k-1} \cdot (n-1).$$

Infine di fondamentale importanza è anche la formula della potenza del binomio (formula di Newton):

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

2 Formule base di Matematica

2.1 Proprietà distributiva della somma rispetto al prodotto

Richiamo: PROPRIETÀ DISTRIBUTIVA DELLA SOMMA RISPETTO AL PRODOTTO

Dati R ed S interi ($R,\ S \geq 1$), e $a_1, \dots, a_R$ e $b_1, \dots, b_S$, numeri reali, la sommatoria di tutti i prodotti del tipo $a_r\, b_s$ coincide con il prodotto delle somme di a_r per le somme di b_r:

$$\sum_{r=1}^{R} \sum_{s=1}^{S} a_r b_s = \left(\sum_{r=1}^{R} a_r \right) \left(\sum_{s=1}^{S} b_s \right)$$

Infatti basta osservare che

$$\begin{aligned}
\textstyle\sum_{r=1}^{R} \sum_{s=1}^{S} a_r b_s &= a_1 b_1 + a_1 b_2 + \cdots + a_1 b_S \\
&+ a_2 b_1 + a_2 b_2 + \cdots + a_2 b_S \\
&+ \cdots \\
&+ a_R b_1 + a_R b_2 + \cdots + a_R b_S \\
\\
&= a_1 (b_1 + b_2 + \cdots + b_S) + a_2 (b_1 + b_2 + \cdots + b_S) \\
&+ \cdots + a_R (b_1 + b_2 + \cdots + b_S) \\
\\
&= \textstyle\sum_{r=1}^{R} a_r \left(\sum_{s=1}^{S} b_s \right) = \left(\sum_{s=1}^{S} b_s \right) \left(\sum_{r=1}^{R} a_r \right).
\end{aligned}$$

2.2 Progressioni aritmetiche

Una successione di numeri

$$a_0, a_1, a_2, \dots, a_n, \dots$$

è detta **progressione aritmetica** se e solo se la differenza tra un qualunque elemento e quello che lo precede sia costante, ovvero sempre la stessa

$$a_k - a_{k-1} = d, \quad \Leftrightarrow \quad a_k = a_{k-1} + d \qquad \forall\, k \geq 1.$$

Il numero d viene detto **ragione della progressione aritmetica** e a_0 viene detto termine iniziale
Il valore degli elementi a_k della progressione dipendo solo da a_0 e d (oltre che da k):

$$a_k = a_0 + kd$$

infatti $a_1 = a_0 + d$, $\quad a_2 = a_1 + d = (a_0 + d) + d = a_0 + 2d$, $\quad a_3 = a_2 + d = (a_0 + 2d) + d = a_0 + 3d$, ...
e per induzione

$$a_k = a_0 + kd \quad \text{implica} \quad a_k = a_{k-1} + d = (a_0 + (k-1)d) + d = a_0 + kd$$

Per calcolare la somma dei primi termini di una progressione aritmentica osserviamo che

$$a_0 + a_1 + \cdots + a_n = a_0 + (a_0 + d) + (a_0 + 2d) + \cdots + (a_0 + nd) = (n+1)\, a_0 + (0 + 1 + 2 + \cdots + n)\, d$$

e quindi basta conoscere la somma dei primi numeri interi, per ottenere che

$$a_0 + a_1 + \cdots + a_n = (n+1)\, a_0 + \frac{n(n+1)}{2}\, d$$

Somma dei primi numeri interi

Ricordiamo qui il fatto che in generale

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

La dimostrazione si ottiene facilmente per induzione, ma conviene pensare al seguente ragionamento:

$$\sum_{k=1}^{n} k = 1 + 2 + \cdots + (n-1) + n = n + (n-1) + \cdots + 2 + 1$$

e quindi, da una parte

$$\big[1 + 2 + \cdots + (n-1) + n\big] + \big[n + (n-1) + \cdots + 2 + 1\big] = 2\sum_{k=1}^{n} k$$

dall'altra

$$\begin{array}{ccccccccccc}
1 & + & 2 & + & \cdots & + & (n-1) & + & n & = & \sum_{k=1}^{n} k \\
+ & & + & & + & & + & & + & & + \\
n & + & (n-1) & + & \cdots & + & 2 & + & 1 & = & \sum_{k=1}^{n} k \\
\hline
(n+1) & + & (n+1) & + & \cdots & + & (n+1) & + & (n+1) & = & n(n+1)
\end{array}$$

da cui

$$2\sum_{k=1}^{n} k = n(n+1).$$

Va però detto che, più in generale[6]

$$\sum_{k=m}^{M} a_k = \frac{(a_m + a_M)(M-m+1)}{2} = \frac{\big(2\,a_0 + (m+M)\,d\big)(M-m+1)}{2}$$

[6] Per verificare questa formula si può procedere in diversi modi: ad esempio, con un ragionamento analogo a quello per ottenere la somma dei primi numeri interi

$$\begin{aligned}
\sum_{k=m}^{M} a_k &= \frac{1}{2}\,[(a_m + a_{m+1} + \cdots + a_M) + (a_M + a_{M-1} + \cdots a_m)] \\
&= \frac{1}{2}\,[(a_m + a_M) + (a_{m+1} + a_{M-1}) + \cdots (a_M + a_m)] = \frac{1}{2}\sum_{k=0}^{M-m} (a_{m+k} + a_{M-k}).
\end{aligned}$$

Osserviamo che gli $M - m + 1$ addendi $a_{m+k} + a_{M-k}$, per $k = m, m+1, \ldots, M$, sono tutti uguali: infatti $a_{m+k} = a_0 + (m+k)d$ e $a_{M-k} = a_0 + (M-k)d$, e quindi si ha che $a_{m+k} + a_{M-k} = 2\,a_0 + (m+M)\,d = a_m + a_M$, e in conclusione:

$$\sum_{k=m}^{M} a_k = \frac{(a_m + a_M)(M-m+1)}{2} = \frac{\big(2\,a_0 + (m+M)\,d\big)(M-m+1)}{2}$$

2.3 Progressioni geometriche

Una successione di numeri

$$a_0,\ a_1,\ a_2,\ \ldots,\ a_n,\ \ldots$$

è detta **progressione geometrica** se e solo se è costante il rapporto q tra ogni termine e quello che lo precede:

$$\frac{a_k}{a_{k-1}} = q \quad \Leftrightarrow \quad a_k = q\, a_{k-1}, \qquad \forall\, k \geq 1.$$

Il numero q viene detto **ragione della progressione geometrica** e a_0 viene detto termine iniziale.
Il valore degli elementi a_k della progressione dipendo solo da a_0 e q (oltre che da k):

$$a_k = a_0\, q^k$$

infatti $a_1 = a_0\, q \quad a_2 = a_1\, q = (a_0\, q)\, q = a_0\, q^2 \quad a_3 = a_2\, q = (a_0\, q^2)\, q = a_0\, q^3$, ... e per induzione

$$a_{k-1} = a_0\, q^{k-1} \quad \text{implica} \quad a_k = a_{k-1}\, q = (a_0\, q^{k-1})\, q = a_0\, q^k$$

Per ottenere la somma dei primi termini di una progressione geometrica con dato iniziale a_0, basta ricordare che per $q \neq 1$ si ha

$$\sum_{k=0}^{n} a_k = \sum_{k=0}^{n} a_0\, q^k = a_0 \sum_{k=0}^{n} q^k = a_0\, \frac{1 - q^{n+1}}{1-q} = a_0\, \frac{q^{n+1} - 1}{q-1}.$$

Somma dei primi termini di una progressione geometrica, con $a_0 = 0$

Ricordiamo qui il fatto che in generale

$$s_n(q) := \sum_{k=0}^{n} q^k = \frac{1 - q^{n+1}}{1-q} = \frac{q^{n+1} - 1}{q-1}, \qquad \forall\, q \neq 1$$

La dimostrazione si ottiene facilmente per induzione, ma conviene pensare al seguente ragionamento:

$$s_{n+1}(q) = \overbrace{1 + q + q^2 + \cdots + q^n}^{=s_n(q)} + q^{n+1} \quad \text{e} \quad s_{n+1}(q) = 1 + \overbrace{q + q^2 + \cdots + q^n + q^{n+1}}^{=q\, s_n(q)}$$

da cui

$$s_{n+1}(q) = s_n(q) + q^{n+1} \quad \text{e} \quad s_{n+1}(q) = 1 + q\, s_n(q)$$

e quindi,

$$s_n(q) + q^{n+1} = 1 + q\, s_n(q) \;\Leftrightarrow\; s_n(q) - q\, s_n(q) = 1 - q^{n+1} \;\Leftrightarrow\; s_n(q)\,(1-q) = 1 - q^{n+1},$$

e quindi per ogni $q \neq 1$ si ottiene $s_n(q) = \dfrac{1 - q^{n+1}}{1-q}$.
Infine osserviamo che il caso $q = 1$ è immediato in quanto $s_n(1) = \sum_{k=0}^{n} 1^k = n + 1$.

Va anche detto che, più in generale, si ha[7]

$$\sum_{k=m}^{M} a_k = a_0\, q^m\, \frac{1 - q^{M-m+1}}{1-q} = a_0\, \frac{q^m - q^{M+1}}{1-q} = a_0\, \frac{q^{M+1} - q^m}{q-1}.$$

---

[7] Infatti: $\displaystyle \sum_{k=m}^{M} a_k = a_0 \sum_{k=m}^{M} q^k \overset{k:=h+m}{=} a_0 \sum_{h=0}^{M-m} q^{h+m} = a_0 \sum_{h=0}^{M-m} q^h q^m = a_0\, q^m \sum_{h=0}^{M-m} q^h = a_0\, q^m\, \frac{1 - q^{M-m+1}}{1-q}$

oppure

$$\sum_{k=m}^{M} a_k = \sum_{k=0}^{M} a_k - \sum_{k=0}^{m-1} a_k = a_0 \left[\frac{1 - q^{M+1}}{1-q} - \frac{1 - q^m}{1-q} \right] = a_0\, \frac{q^m - q^{M+1}}{1-q}$$

2.4 Serie geometrica e serie delle sue derivate prime e seconde

Consideriamo qui solamente la serie i cui termini sono una progressione geometrica del tipo $a_k = x^k$, con termine iniziale $a_0 = 1$: il caso generale si deduce immediatamente da questo.
Si ha che

$$\text{la serie} \qquad \sum_{k=0}^{\infty} x^k \quad \begin{cases} \text{diverge a } +\infty & \text{per } x \geq 1 \\ \text{converge (assolutamente) a } \dfrac{1}{1-x} & \text{per ogni } x \text{ tale che } -1 < x < 1 \text{ (ovvero } |x| < 1) \\ \text{non converge} & \text{per } x \leq -1 \end{cases}$$

La serie geometrica, pensata come funzione di x, è il prototipo delle serie di potenze e il suo raggio di convergenza è quindi pari a 1 e inoltre la convergenza è uniforme in ogni intervallo chiuso e limitato contenuto in $(-1, 1)$.
Per le proprietà delle serie di potenze, sappiamo che la serie delle derivate ha lo stesso raggio di convergenza

$$\sum_{k=0}^{\infty} \frac{d}{dx} x^k = \frac{d}{dx} \sum_{k=0}^{\infty} x^k = \frac{d}{dx} \frac{1}{1-x} = \frac{d}{dx}(1-x)^{-1} = -(1-x)^{-2} \frac{d}{dx}(1-x) = \frac{1}{(1-x)^2}, \qquad |x| < 1.$$

Tenendo conto che $\frac{d}{dx} x^k = k\, x^{k-1}$, otteniamo quindi che

$$\sum_{k=1}^{\infty} k\, x^{k-1} = \sum_{k=1}^{\infty} \frac{d}{dx} x^k = \sum_{k=0}^{\infty} \frac{d}{dx} x^k = \frac{1}{(1-x)^2}, \qquad |x| < 1,$$

dove, nella seconda uguaglianza, abbiamo usato il fatto che, per $k = 0$ la derivata di $x \mapsto x^k = x^0 \big(= 1 \big)$ è nulla.

In modo analogo, e tenendo conto che

$$\frac{d^2}{dx^2}(1-x)^{-1} = \frac{d}{dx}(1-x)^{-2} = 2\,(1-x)^{-3} = \frac{1}{(1-x)^3}, \qquad |x| < 1,$$

si ottiene che

$$\sum_{k=1}^{\infty} k(k-1)\, x^{k-2} = \sum_{k=0}^{\infty} \frac{d^2}{dx^2} x^k = \sum_{k=0}^{\infty} \frac{d^2}{dx^2} x^k = \frac{1}{(1-x)^3}, \qquad |x| < 1,$$

dove abbiamo usato il fatto che le derivate seconde di $x \mapsto x^0 = 1$ e $x \mapsto x^1 = x$ sono entrambe nulle.

2.5 Serie esponenziale e serie delle sue derivate prime e seconde

La serie esponenziale è la serie di potenze

$$\sum_{k=0}^{\infty} \frac{x^k}{k!}$$

che si ottiene come serie di Mac Laurin (ossia serie di Taylor in $x_0 = 0$) della funzione esponenziale $x \mapsto f(x) := e^x$. Infatti le derivate k-sime di $f(x)$ concidono tutte con la funzione stessa, ossia, $f^{(k)}(x) = e^x$, per cui $f^{(k)}(0) = e^0 = 1$ e quindi la serie di Mac Laurin è appunto

$$\sum_{k=0}^{\infty} \frac{f^{(k)}(0)}{k!}\, x^k = \sum_{k=0}^{\infty} \frac{x^k}{k!}.$$

Si dimostra inoltre che la serie converge alla funzione stessa, ossia

$$\sum_{k=0}^{\infty} \frac{x^k}{k!} = e^x, \qquad \forall\, x \in \mathbb{R}.$$

Il raggio di convergenza di questa serie è quindi infinito e la convergenza è uniforme in ogni intervallo limitato: per questo motivo la somma della serie delle derivate è la derivata della somma della serie e quindi

$$\sum_{k=1}^{\infty} k\, \frac{x^{k-1}}{k!} = \sum_{k=0}^{\infty} \frac{d}{dx} \frac{x^k}{k!} = \frac{d}{dx} \sum_{k=0}^{\infty} \frac{x^k}{k!} = \frac{d}{dx} e^x = e^x \qquad \forall\, x \in \mathbb{R},$$

dove abbiamo usato il fatto che la derivata di $x \mapsto x^0 = 1$ è nulla.
Inoltre, similmente al caso precedente,

$$\sum_{k=2}^{\infty} k(k-1)\, \frac{x^{k-2}}{k!} = \sum_{k=0}^{\infty} \frac{d^2}{dx^2} \frac{x^k}{k!} = \frac{d^2}{dx^2} \frac{x^k}{k!} = \frac{d^2}{dx^2} e^x = e^x \qquad \forall\, x \in \mathbb{R},$$

dove abbiamo usato il fatto che le derivate seconde di $x \mapsto x^0 = 1$ e $x \mapsto x^1 = x$ sono entrambe nulle.

3 Teorema fondamentale del calcolo integrale

3.1 Enunciato del teorema fondamentale

In questa sezione diamo solo l'enunciato (senza dimostrazione) di uno dei più importanti risultati del calcolo integrale.

Teorema 3.1 (Teorema fondamentale del calcolo)**.** *Sia $f : [a, b] \to \mathbb{R}$ una funzione continua e consideriamo la funzione $G : [a, b] \to \mathbb{R}$ definita come*

$$G(x) = \int_a^x f(t)\, dt.$$

Allora la funzione G è continua in $[a, b]$, è derivabile in (a, b) e la sua derivata e uguale a

$$G'(x) = f(x), \qquad \textit{per ogni } x \in (a, b).$$

Inoltre se $F : [a, b] \to \mathbb{R}$ è una primitiva di f sull'intevallo $[a, b]$, ovvero F è continua in $[a, b]$, è derivabile in (a, b) ed è tale che

$$F'(x) = f(x) \qquad \textit{per ogni } x \in (a, b),$$

allora vale la formula

$$\int_a^x f(t)\, dt = F(b) - F(a).$$

4 Vettori e matrici

Questa sezione sarà utile quando si parlerà delle Catene di Markov.

4.1 Definizioni e prodotto di matrici (da scrivere)

4.2 Autovalori e autovettori (da scrivere)