MATEMATICA (GRATUITA) PER LE SCUOLE SUPERIORI

FUORI PROGRAMMA

In questo contributo sono proposti argomenti che né le Indicazioni Nazionali (Licei) né le Linee Guida (Tecnici e Professionali) contemplano. Ciò non di meno, questi argomenti, o semplicemente qualcuno di essi, potrebbero interessare studenti particolarmente motivati allo studio della matematica. Gli argomenti sono scollegati fra loro, anche se in qualche misura sono connessi a contenuti affrontati nel "testo base", costituendone a volte un vero e proprio approfondimento e/o ampliamento.
Qui appreso forniamo l'indice di tali argomenti: ciascuno ne farà l'uso che ritiene più appropriato.
In linea di massima gli argomenti trattati sono rivolti agli studenti che frequentano gli ultimi anni della scuola superiore, ma qualcuno di essi (come, per esempio: argomenti 3, 4, 5) potrebbe essere affrontato anche a livello di biennio con le dovute cautele.

Indice degli argomenti affrontati:

1 – Affinità.

1.1 È noto che un'**affinità** (o **trasformazione affine**) ha equazioni:

[1] $$\mathbf{x' = a\,x + b\,y + c, \quad y' = a'\,x + b'\,y + c',}$$

oppure, scritte in forma matriciale:

[1′] $$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a & b \\ a' & b' \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} c \\ c' \end{bmatrix}$$

dove a, b, c, a', b', c' sono numeri reali qualunque, purché $a\,b' - a'\,b \neq 0$.

Si potrebbe dimostrare (cosa che però non facciamo) che:

Ogni affinità:

- **conserva l'allineamento dei punti; vale a dire che trasforma rette in rette;**
- **conserva il parallelismo delle rette; vale a dire che trasforma rette parallele in rette parallele;**
- **trasforma una conica di un dato tipo in una conica dello stesso tipo; vale a dire: un'ellisse in un'ellisse** (la circonferenza è considerata una particolare ellisse)**, una parabola in una parabola, un'iperbole in un'iperbole.**

Al fine di comprendere come opera un'affinità invitiamo a risolvere il seguente esercizio.

ESERCIZIO. In un piano riferito ad un sistema di assi cartesiani ortogonali (Oxy), è assegnato il pentagono ABCDE di vertici A(0,0), B(2,0), C(2,1), D(1,2), E(0,1). Disegnarlo assieme al suo trasformato A'B'C'D'E' in base all'affinità di equazioni: x'=2x+2, y'=x+y.

Il numero reale non nullo **k=ab'–a'b** si chiama ***modulo*** dell'affinità. Se k>0 l'affinità è *diretta* (conserva il verso degli angoli), se k<0 l'affinità è *speculare* (inverte il verso degli angoli).

TEOREMA. **Se S rappresenta l'area di una figura geometrica ed S' l'area della figura trasformata in base all'affinità di modulo k, si ha:**

$$\frac{S'}{S} = |k|\,.$$

DIMOSTRAZIONE. Dimostriamo la proprietà con riferimento al triangolo, ma la proprietà è generale.

Sia allora un triangolo ABC. Scegliamo il sistema di riferimento cartesiano (Oxy) in modo che si abbia (Fig. 1.1): A(0, 0), B(p, 0), C(m, n), con p>0 ed n>0. La sua area è evidentemente:

$$S = \frac{1}{2}\,|p||n|\,.$$

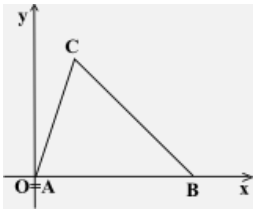

FIG. 1.1

I punti A', B', C' trasformati di A, B, C in base alle equazioni [1] hanno coordinate:

$$x_{A'}=c\,,\ y_{A'}=c'; \quad x_{B'}=ap+c\,,\ y_{B'}=a'p+c'; \quad x_{C'}=am+bn+c\,,\ y_{C'}=a'm+b'n+c'$$

Si trova che:

$$A'B'=|p|\sqrt{a^2+a'^2}\,; \quad \text{la retta } A'B' \text{ ha equazione: } a'x-ay+(ac'-a'c)=0; \quad d(C', A'B')=\frac{|n|\,|ab'-a'b|}{\sqrt{a^2+a'^2}}\,.$$

Pertanto, essendo ab'–a'b uguale al modulo k dell'affinità, l'area S' del triangolo A'B'C' è:

$$S' = \frac{1}{2}\cdot A'B'\cdot d(C',A'B') = \frac{1}{2}\cdot|p|\sqrt{a^2+a'^2}\cdot\frac{|n||k|}{\sqrt{a^2+a'^2}} = \frac{1}{2}|p||n||k|.$$

Dunque effettivamente: $\frac{S'}{S} = |k|$.

Si capisce che se k=±1 risulta S'=S, vale a dire che l'affinità conserva l'area della superficie. Ogni affinità siffatta si definisce *affinità equivalente* o *equiaffinità*.

1.2 Dal precedente teorema discende una conseguenza importante che riguarda l'area dell'ellisse.

In un piano, riferito ad un sistema monometrico di assi cartesiani ortogonali (Oxy), sia assegnata la circonferenza di equazione:

$$x^2 + y^2 = r^2.$$

Considerata l'affinità di equazioni:

[2] $$x' = h\,x,\ \ y' = k\,y,$$

dove h, k sono numeri reali non nulli, il suo modulo è m=h k.

Poiché da quelle equazioni si ricava:

$$x=\frac{x'}{h}\ ,\ \ y=\frac{y'}{k}\ ,$$

la circonferenza viene trasformata dall'affinità nell'ellisse:

$$\frac{x'^2}{h^2}+\frac{y'^2}{k^2}=r^2$$

di semiassi: a=|h|r, b=|k|r.

Chiamata A l'area racchiusa dall'ellisse ed S l'area del cerchio, per la formula dimostrata sopra si ha:

$\frac{A}{S} = |hk|$. Pertanto: $\frac{A}{S} = \frac{a}{r}\cdot\frac{b}{r} = \frac{ab}{r^2}$. Siccome $S = \pi r^2$, allora $A = \pi r^2 \cdot \frac{ab}{r^2}$, ossia: $\mathbf{A = \pi ab}$.

Formula, quest'ultima, che fornisce l'area racchiusa dall'ellisse o, come anche si dice, l'***area dell'ellisse***.

NOTA BENE. Le affinità di equazioni [2] sono denominate ***dilatazioni***, anche se in realtà a volte sono *dilatazioni* vere e proprie, altre volte sono invece *contrazioni*. Per esempio, applicate ad un segmento AB, esse ne determinano di norma un *allungamento* (se il trasformato A'B' di AB è tale che A'B'>AB) o un *accorciamento* (se A'B'<AB). Nel caso particolare in cui:

- |h|≠1 e k=1 si ha una *dilatazione nella direzione dell'asse* x, nel verso positivo se h>0, in quello negativo se h<0;
- h=1 e |k|≠1 si ha una *dilatazione nella direzione dell'asse* y, nel verso positivo se k>0, in quello negativo se k<0.

Si comprende meglio quanto qui detto risolvendo il seguente esercizio.

ESERCIZIO. Nel piano, riferito ad un sistema di assi cartesiani ortogonali (Oxy), è assegnato il triangolo OAB i cui vertici A e B hanno coordinate nell'ordine (1,0) e (0,2). Disegnare il triangolo e i suoi trasformati in base alle affinità di equazioni: 1) $\{x'=2x,\ y'=y\}$, 2) $\left\{x'=x,\ y'=-\frac{1}{2}y\right\}$.

Disegnare anche la circonferenza di equazione $x^2+y^2=1$ e la sua trasformata in base alle stesse equazioni.

1.3 Occupiamoci adesso della risoluzione di qualche esercizio sulle affinità. È richiesta una minima collaborazione da parte di chi legge.

ESERCIZIO 1. Riferito il piano ad un sistema di assi cartesiani ortogonali (Oxy), determinare le equazioni dell'affinità che trasforma i punti A(1,–1), B(2,1), C(–1,0) nei punti A'(0,1), B'(0,0), C'(–1,0) rispettivamente.

RISOLUZIONE. La generica affinità ha equazioni:

$$x' = a\,x + b\,y + c\ ,\ \ \ y' = a'x + b'y + c'\ ,$$

dove a, b, c, a', b', c' sono numeri reali tali che ab'–a'b≠0.

Il fatto che essa trasformi il punto A(1,–1) nel punto A'(0,1) implica le seguenti condizioni:

$$0 = a - b + c\ ,\ \ \ 1 = a' - b' + c'\ ;$$

analogamente, poiché essa trasforma B(2,1) in B'(0,0) deve risultare:

$$0 = 2\,a + b + c\ ,\ \ \ 0 = 2\,a' + b' + c'\ ,$$

e poiché trasforma C(–1,0) in C'(–1,0) deve risultare:

$$-1 = -a + c\,, \quad 0 = -a' + c'\,.$$

Risolto il sistema delle tre equazioni nelle incognite a, b, c e quello delle tre equazioni nelle incognite a', b', c', si trova:

$$a = \frac{2}{5}\,,\ \ b = -\frac{1}{5}\,,\ \ c = -\frac{3}{5}\,; \qquad a' = \frac{1}{5}\,,\ \ b' = -\frac{3}{5}\,,\ \ c' = \frac{1}{5}\,.$$

Pertanto l'affinità ha le seguenti equazioni:

$$x' = \frac{2}{5}\,x - \frac{1}{5}\,y - \frac{3}{5}\,, \qquad y' = \frac{1}{5}\,x - \frac{3}{5}\,y + \frac{1}{5}\,.$$

Si tratta di una generica affinità di modulo $k = \frac{2}{5}\cdot\left(-\frac{3}{5}\right) - \left(-\frac{1}{5}\right)\cdot\frac{1}{5} = -\frac{1}{5}$.

ESERCIZIO 2. Riferito il piano ad un sistema di assi cartesiani ortogonali (Oxy), determinare l'affinità che trasforma la retta di equazione x–y=0 in quella di equazione x+y=0 e la seconda nella prima.

RISOLUZIONE. La generica affinità ha equazioni:

$$x' = a\,x + b\,y + c\,, \quad y' = a'x + b'y + c'\,,$$

dove a, b, c, a', b', c' sono numeri reali tali che ab'–a'b≠0.

Per trovare la trasformata della retta x–y=0 dobbiamo prima di tutto esprimere, nelle precedenti equazioni, x ed y per mezzo di x' ed y', risolvendo il sistema delle due equazioni nelle indeterminate x ed y. Si ottiene:

$$x = \frac{b'x' - by' + bc' - b'c}{ab' - a'b}\,, \quad y = -\frac{a'x' - ay' + ac' - a'c}{ab' - a'b}\,.$$

In base a queste formule, l'equazione x–y=0 viene trasformata nella seguente equazione:

$$(b'x - by' + bc' - b'c) + (a'x' - ay' + ac' - a'c) = 0$$

ovvero, ritornando alle coordinate correnti x, y e semplificando:

$$(a'+b')\,x - (a+b)\,y + (a+b)\,c' - (a'+b')\,c = 0.$$

Affinché questa equazione coincida con l'equazione x+y=0 deve risultare:

$$(a+b)\,c' - (a'+b')\,c = 0, \quad a'+b' = k, \quad a+b = -k,$$

essendo k una costante di proporzionalità. Dunque deve risultare:

[*i*] $$c'+c = 0, \quad a'+b' = k, \quad a+b = -k.$$

L'affinità assegnata trasforma inoltre la retta x+y=0 nella seguente:

$$(b'x - by' + bc' - b'c) - (a'x' - ay' + ac' - a'c) = 0$$

ovvero, ritornando alle coordinate correnti x, y e semplificando:

$$(-a'+b')\,x + (a-b)\,y + (-a+b)\,c' + (a'-b')\,c = 0.$$

Affinché questa equazione coincida con l'equazione x–y=0 deve risultare:

$$(-a+b)\,c' + (a'-b')\,c = 0, \quad -a'+b' = h, \quad a-b = -h,$$

essendo h un'altra costante di proporzionalità. Dunque deve risultare:

[*ii*] $$c'-c = 0, \quad -a'+b' = h, \quad a-b = -h.$$

Associando opportunamente le sei equazioni [*i*] e [*ii*] e risolvendo si trova:

$$c = c' = 0\,,\ \ a = -\frac{h+k}{2}\,,\ \ b = \frac{h-k}{2}\,,\ \ a' = \frac{k-h}{2}\,,\ \ b' = \frac{h+k}{2}\,.$$

Vale a dire:

$$c = c' = 0, \quad a' = -b, \quad b' = -a.$$

Pertanto l'affinità ha le seguenti equazioni:

$$x' = a\,x + b\,y, \quad y' = -\,b\,x - a\,y,$$

purché sia $a^2 - b^2 \neq 0$. Il suo modulo è $b^2 - a^2$.

In particolare:

- se a=1 e b=0 l'affinità assume le seguenti equazioni:

$$x' = x, \quad y' = -y\,;$$

si tratta della simmetria assiale rispetto all'asse x;

- se a=–1 e b = 0 le equazioni diventano queste:

$$x' = -x, \quad y' = y\ ;$$

si tratta della simmetria assiale rispetto all'asse y.

ESERCIZIO 3. Considerata la seguente trasformazione geometrica:

(A) $$x' = 2\,y\ , \quad y' = x - y\ ,$$

stabilirne la natura e determinarne gli elementi uniti.

RISOLUZIONE. Si tratta di una generica affinità di modulo k = –2.

Ricerchiamo i suoi punti uniti. Per questo bisogna risolvere il sistema delle seguenti equazioni:

$$x = 2\,y\ , \quad y = x - y\ .$$

È un sistema indeterminato che ammette le infinite soluzioni (x, x/2), $\forall x \in \mathbb{R}$. Il che vuol dire che tutti i punti di coordinate (x, x/2), cioè i punti della retta r di equazione x=2y, sono punti uniti. La retta r è naturalmente retta unita.

Vediamo se l'affinità ha altre rette unite. A questo proposito consideriamo la generica retta di equazione:

(B) $$m\,x + n\,y + p = 0\ ,$$

dove m, n non sono contemporaneamente nulli.

La sua trasformata in base alle (A) è la retta di equazione:

(C) $$n\,x + (2m-n)\,y + p = 0\ .$$

Bisogna distinguere due casi:

- Se $p \neq 0$ la (B) e la (C) coincidono se risulta:

$$n = m \quad \text{e} \quad 2\,m - n = n$$

ossia $n = m \neq 0$.

Per cui le rette di equazione:

$$m\,x + m\,y + p = 0\ , \ \text{ossia:}\ \ x + y + h = 0\ \ (h \neq 0),$$

sono rette unite della trasformazione.

- Se p=0 la (B) e la (C) coincidono se risulta: $\frac{n}{m} = \frac{2m-n}{n}$, ossia: $2m^2 - mn - n^2 = 0$. Da qui, risolvendo rispetto ad m, segue: m=n oppure m=–n/2.

Nel primo caso (m=n) si ottiene la retta unita: x+y=0; nel secondo (m=–n/2) si ritrova la retta x=2y.

In definitiva l'affinità in esame ha le seguenti rette unite:

- la retta x=2y, che è anche luogo di punti uniti;
- il fascio di rette parallele x+y+h=0, $\forall h \in \mathbb{R}$.

1.4 Concludiamo questa parte con una classificazione delle affinità in base ai suoi punti uniti.

Detto che le affinità che hanno come punto unito l'origine del sistema di riferimento sono chiamate ***centro-affinità***, quali sono le loro equazioni?

Adesso dimostriamo due proprietà.

PROPRIETÀ 1. **Se un'affinità ha uniti due punti distinti A, B allora ogni punto della retta AB è unito.**

DIMOSTRAZIONE. Nel piano cartesiano (Oxy) consideriamo l'affinità (α) di equazioni:

$$x' = a\,x + b\,y + c\ , \quad y' = a'\,x + b'\,y + c'\ .$$

Se i punti $A(x_A,y_A)$ e $B(x_B,y_B)$ sono uniti allora risulta:

$$a\,x_A + b\,y_A + c = x_A\ , \quad a'\,x_A + b'\,y_A + c' = y_A\ ;$$
$$a\,x_B + b\,y_B + c = x_B\ , \quad a'\,x_B + b'\,y_B + c' = y_B\ .$$

Indicato ora con C un qualsiasi punto della retta AB, distinto da A e da B, risulta: $\overrightarrow{AC} = k\,\overrightarrow{AB}$. Pertanto le coordinate x_C, y_C sono:

$$x_C = k\,(x_B - x_A) + x_A\,, \quad y_C = k\,(y_B - y_A) + y_A\,.$$

Il punto C', trasformato di C, ha allora coordinate $x_{C'}$, $y_{C'}$ tali che:

$$x_{C'} = a\,[k\,(x_B - x_A) + x_A] + b\,[k\,(y_B - y_A) + y_A] + c = k\,[(a\,x_B + b\,y_B) - (a\,x_A + b\,y_A)] + (a\,x_A + b\,y_A + c) =$$
$$= k\,[(x_B - c) - (x_A - c)] + x_A = k\,(x_B - x_A) + x_A = x_C\,;$$

analogamente $y_{C'} = y_C$.

Insomma il punto C', trasformato di un qualsiasi punto C della retta AB, coincide con C: è punto unito. [c.v.d.]

PROPRIETÀ 2. **Se un'affinità ha uniti tre punti non allineati allora tutti i punti del piano sono uniti, per cui l'affinità è l'identità.**

DIMOSTRAZIONE. Siano A, B, C i tre punti uniti non allineati per l'affinità (α) nel piano.

Intanto i punti delle rette AB, BC, CA sono punti uniti per la precedente proprietà 1.

Considerato ora un generico punto P non appartenente ad alcuna delle tre rette suddette, accade almeno una delle tre situazioni seguenti:

- la retta PA seca la retta BC (nel punto unito X),
- la retta PB seca la retta CA (nel punto unito Y),
- la retta PC seca la retta AB (nel punto unito Z).

Tanto per fissare le idee, supponiamo che si verifichi la prima situazione: ciò significa che il punto P appartiene alla retta AX; ma questa – essendo retta di due punti uniti (A ed X) – ha unito ogni suo punto e quindi anche P.

Perciò ogni punto del piano è punto unito. [c.v.d.]

Da quanto su esposto si desume che:

Ogni affinità, diversa dall'identità, a seconda dei punti uniti che la caratterizzano, appartiene ad una ed una soltanto delle seguenti famiglie:

- **A1 : affinità senza punti uniti;**
- **A2 : affinità con uno ed un solo punto unito;**
- **A3 : affinità con due punti uniti.**

Le affinità A3 hanno evidentemente una retta unita luogo di punti uniti: si chiamano **affinità omologiche** (o **omologie affini**); la retta di punti uniti si dice ***asse dell'omologia***.

Naturalmente un'affinità omologica può avere altre rette unite, oltre alla retta di punti uniti. Tali rette, però, non possono essere luoghi di punti uniti, altrimenti si cadrebbe in contraddizione con la precedente proprietà 2.

In ogni caso vale la seguente proprietà che non dimostriamo.

PROPRIETÀ 3. **Considerata un'affinità omologica nel piano, ogni retta che congiunge due punti corrispondenti (non uniti) appartiene allo stesso fascio di rette parallele.**

La direzione di tali rette si dice ***direzione dell'omologia***.

Per esempio, ritornando per un momento al precedente esercizio 2, possiamo concludere che l'affinità di equazioni:

$$x' = 2\,y\,, \quad y' = x - y\,,$$

ivi considerata, è un'affinità omologica avente per asse la retta di equazione x=2y e per direzione quella individuata dalla retta di equazione x+y=0.

In effetti ogni punto P(a, b) e il suo trasformato P'(2b, a–b) in base all'affinità in questione appartengono ad una retta parallela alla retta di equazione x–y=0.

1.5 Proponiamo, per concludere, la risoluzione di alcune questioni sulle affinità.

[Il piano s'intende riferito ad un sistema di assi cartesiani ortogonali (Oxy)]

1. Disegnare i punti A, B, C e i loro trasformati A', B', C' in base all'affinità di equazioni:

$$x' = 2x - 1,\ y' = x + y + 1,$$

sapendo che:

a) $A(1,-1)$, $B(2,0)$, $C(0,1)$. b) $A(-2,0)$, $B(-4,-1)$, $C(1,2)$. c) $A\left(1,\frac{1}{2}\right)$, $B(2,2)$, $C(0,-1)$.

[**R**. a) A'(1,1), B'(3,3), C'(–1,2); ...]

2. Disegnare la retta r e la sua trasformata r' in base all'affinità di equazioni:

$$x' = -x + y,\ y' = x - 2y,$$

sapendo che r ha equazione:

a) $x = 0$. b) $y = 0$. c) $y = x$. d) $2x-y+1 = 0$.

[**R**. a) $2x+y = 0$; ... ; d) $3x+y-1 = 0$]

3. Sono date le affinità di equazioni:

$$x' = (k+1)x - y + 1,\quad y' = -\frac{1}{2}kx + 2y,$$

dove k è un parametro reale.

a) Stabilire se le equazioni suddette rappresentano un'affinità per ogni k.
b) Dimostrare che ognuna delle affinità assegnate ha un punto unito.
c) Trovare se fra di esse ve ne sono di quelle che trasformano la retta $2x+3y+1=0$ in una retta parallela.

$\left[\mathbf{R}.\ \text{a) } k \neq -\frac{4}{3},\ \text{b) } \left(-\frac{2}{k},-1\right),\ \text{c) Non ce ne sono}\right]$

4. Sono date le affinità di equazioni:

$$x' = (k+1)\,x + k\,y - 1\,,\quad y' = (k-1)\,x + k\,y + 2\,k\,,$$

dove k è un parametro reale.

a) Stabilire se per qualche valore di k le equazioni suddette non rappresentano un'affinità.
b) Dimostrare che tra quelle assegnate vi sono due affinità equivalenti.
c) Dopo aver disegnato il triangolo ABC di vertici A(1,0), B(2,0), C(2,1) e i suoi trasformati in base a ciascuna delle due affinità equivalenti, verificare che effettivamente i tre triangoli hanno la stessa area.

$\left[\mathbf{R}.\ \text{a) } k=0;\ \text{b) } k=\pm\frac{1}{2}\ ;\ \ldots\right]$

5. Dimostrare che le affinità che mutano in sé l'iperbole $xy=k$ hanno equazioni del tipo:

$$x' = mx,\ y' = \frac{1}{m}y \qquad \text{oppure del tipo} \qquad x' = my,\ y' = \frac{1}{m}x$$

dove m è un numero reale diverso da 0.

6. Scrivere le equazioni dell'affinità (A) che ha come punti uniti i punti O(0,0) e A(1,0) e trasforma il punto B(1,1) nel punto C(0,2).
Trovare i punti uniti e le rette unite di (A).
Tra le rette unite determinare quella che divide il quadrilatero OABC in due parti, di cui quella che contiene il vertice O è metà dell'altra.
La maggiore di queste due parti è trasformata dall'affinità in una regione R: calcolarne l'area.

[**R**. $x'=x-y$, $y'=2y$; $y=0$: retta unita luogo di punti uniti, $x+y=h$ ($h\in\mathbb{R}$): rette unite; $x+y=1$; A(R)=2]

7. Disegnare il quadrilatero di vertici A(0,1), B(1,2), C(0,3), D(–1,2) e quello di vertici A'(2,0), B'(4,0), C'(4,1), D'(2,1). Dopo aver verificato che si tratta di due parallelogrammi, dimostrare che sono figure affini, trovando le equazioni di un'affinità che trasforma il primo quadrilatero nel secondo, e precisamente quelle dell'affinità che associa ai vertici del primo quadrilatero quelli del secondo in base alla seguente tabella: $\begin{pmatrix} A & B & C & D \\ A' & B' & C' & D' \end{pmatrix}$.
Di tale affinità determinare gli eventuali punti uniti. Stabilire inoltre se ha o non ha rette unite.

$\left[\mathbf{R}.\ x' = x + y + 1,\ y' = -\frac{1}{2}x + \frac{1}{2}y - \frac{1}{2};\ \ldots\right]$

8. Si considerino le trasformazioni geometriche di equazioni:

$$x' = a\,x + 2\,y + b\,,\quad y' = -\,x + (a-1)\,y\,,$$

dove a, b sono numeri reali.

Fra le trasformazioni date determinare la trasformazione T che ha come punto unito il punto A(1,–1). Di essa studiare la natura e stabilire se ha altri punti uniti e se ha rette unite.
Considerato poi il triangolo OAB, dove O è l'origine del sistema di riferimento e B(0,2), determinare le equazioni dei suoi lati e calcolarne l'area.
Determinare infine le equazioni dei lati del triangolo trasformato di OAB in base alla T e calcolare inoltre l'area di questo triangolo.

[**R**. x' = x+2y+2, y' = – x; generica affinità, nessun altro punto unito, nessuna retta unita; ...]

9. È assegnata l'ellisse (H) di equazione:

$$x^2 + 2y^2 - 1 = 0\,.$$

Verificare che la traslazione di equazioni: {X=x+1, Y=y–2} la trasforma nell'ellisse (K) di equazione:

$$x^2 + 2y^2 - 2x + 8y + 8 = 0\,.$$

Stabilire poi se esistono altre affinità che trasformino l'ellisse (H) nell'ellisse (K).
RISOLUZIONE (traccia). La risoluzione della seconda parte comporta qualche difficoltà, per questo, al fine di favorire lo studente che avesse voglia di risolvere questa questione, proponiamo una traccia di risoluzione.
Si considerano le equazioni di una generica affinità:

X=ax+by+c, Y=mx+ny+p,

dove a, b, c, m, n p sono parametri reali con an–bm≠0.
Dopo aver espresso x, y in funzione di X, Y, si sostituiscono i valori trovati nell'equazione di (H) e, una volta ritornati alle coordinate correnti x,y, si ottiene la trasformata dell'equazione di (H). Si impone la condizione che questa trasformata sia identicamente uguale all'equazione di (K). Tale condizione si traduce nel seguente sistema di equazioni nelle incognite a, b, c, m, n p:

$$\begin{cases} 2m^2 + n^2 = 1 \\ 2am + bn = 0 \\ 2a^2 + b^2 = 2 \\ (2am + bn)p - c = -1 \\ 2p - 2acm - bcn = -4 \\ a^2n^2 + b^2m^2 - 2p^2 - 2abmn + 2bcnp + 4acmp - 1 = -8 \end{cases}$$

Risolto questo sistema si trovano infinite soluzioni ripartite in due categorie:

(1) c=1, p=–2, m=$-\frac{b}{2}$, n=a; (2) c=1, p=–2, m=$\frac{b}{2}$, n=–a,

sotto la condizione che risulti: $2a^2+b^2=2$.
Sotto questa condizione si hanno pertanto le affinità di equazioni seguenti:

(A') : X=ax+by+1, Y=$-\frac{b}{2}$x+ay–2; (A") : X=ax+by+1, Y=$\frac{b}{2}$x–ay–2.

Le prime hanno modulo 1 e perciò sono affinità dirette, le seconde hanno modulo –1 e dunque sono affinità speculari. Entrambe sono affinità equivalenti.
Si può constatare che fra le infinite affinità trovate c'è ovviamente la traslazione di cui si fa menzione nella traccia, vale a dire la traslazione di equazioni {X=x+1, Y=y–2}, ottenute dalle (A') per a=1 e b=0.
Ci sono poi le seguenti altre 3 isometrie:

- isometria di equazioni {X=–x+1, Y=–y–2}, ottenute dalle (A') per a=–1 e b=0; si tratta della composizione della traslazione di componenti (1,–2) con la simmetria centrale o, se si preferisce, della simmetria rispetto al centro di coordinate (1/2, –1);
- glissosimmetria [1] di equazioni {X=x+1, Y=–y–2}, ottenute dalle (A") ponendo a=1, b=0.
- glissosimmetria di equazioni {X=–x+1, Y=y–2}, ottenute dalle (A") ponendo a=–1, b=0.

[1] Ricordiamo che una *glissosimmetria* è un'isometria che si ottiene componendo una traslazione di vettore non nullo con una simmetria assiale.

Per ciascuna delle 4 isometrie suddette il lettore è invitato a rappresentare le due ellissi (H) e (K), evidenziando in particolare il triangolo ABC di vertici $A(1,0)$, $B(-1,0)$, $C\left(\frac{\sqrt{2}}{2}, \frac{1}{2}\right)$ inscritto nell'ellisse (H) e il suo trasformato $A_1B_1C_1$ inscritto nell'ellisse (K).
Per valori di a, b tali che $|a|\neq 1$ (e perciò $b\neq 0$), si hanno affinità generiche che, come abbiamo già specificato, sono in ogni caso affinità equivalenti.
Una particolare di queste affinità, considerata a titolo di esempio, è quella che si ottiene dalle (A") ponendo $b=-\sqrt{2}$ e perciò a=0, vale a dire l'affinità di equazioni:

$$X = -\sqrt{2}\,y + 1\,, \quad Y = -\frac{\sqrt{2}}{2}x - 2\,.$$

Essa trasforma l'ellisse (H) nell'ellisse (K) ovviamente e il triangolo ABC considerato sopra (Fig. 1.2) nel triangolo A'B'C' di vertici $A'\left(1, -\frac{\sqrt{2}}{2} - 2\right)$, $B'\left(1, \frac{\sqrt{2}}{2} - 2\right)$, $C'\left(1 - \frac{\sqrt{2}}{2}, -\frac{5}{2}\right)$.

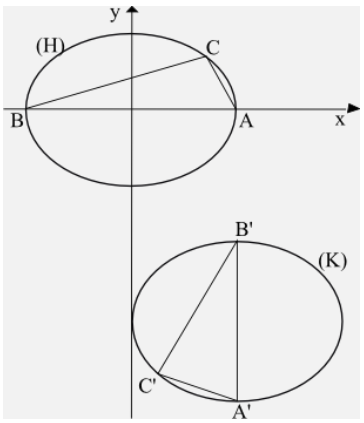

FIG. 1.2

2 – Geodetiche.

2.1 Fissati due punti A e B su una superficie piana, si sa che il percorso più breve per andare da A a B, ammesso che sia possibile muoversi in ogni direzione, è la retta AB.

E se i punti A e B sono due punti qualsiasi di una superficie sferica? Prova a verificare che succede se la sfera è una palla di gomma. Segna sulla sua superficie due qualsiasi punti e prova a congiungerli con un tratto che abbia la minima lunghezza possibile: noterai anzitutto che il percorso da A a B non può avvenire in linea retta e, in secondo luogo, che il cammino più breve si realizza lungo il più piccolo degli archi di circonferenza massima passante per i due punti [(2)]. Ogni altro tratto che unisce i due punti, effettuato sempre sulla superficie sferica, è più lungo di questo. E se i due punti sono situati su un cilindro? O su un cono? Risponderemo fra breve, ma intanto prova da solo a cercare una risposta.

Il problema di "***tracciare la linea di minimo percorso, fra due punti, su una superficie***" fu posto da Johann Bernoulli (1667-1748) nel 1697. Queste linee furono poi chiamate ***geodetiche*** da Pierre Simon de Laplace (1749-1827) nel 1798 e studiate in maniera approfondita da Bernhard Riemann (1826-1866).

Possiamo, dunque, assumere la seguente definizione:

<u>Geodetica</u> è la linea che realizza, su una data superficie,
il minimo percorso fra due punti assegnati.

Alcuni esempi.

a) Le geodetiche di un piano sono le rette passanti per i due punti.

b) Le geodetiche di un angolo diedro $\widehat{\alpha\beta}$ passanti per i due punti A e B sono:
- le rette passanti per i due punti se essi appartengono alla stessa faccia;
- le spezzate AOB, dove O è il punto dello spigolo RS del diedro tale che AÔR=BÔS, se i due punti A e B non appartengono alla stessa faccia (Fig. 2.1a): per rendersene conto è sufficiente distendere il diedro in modo che le sue facce diventino due semipiani opposti (Fig. 2.1b)

c) Le geodetiche di una superficie sferica sono le circonferenze massime passanti per i due punti.

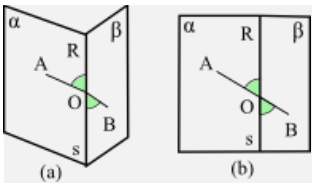

FIG. 2.1

Proponiamo a chi legge di risolvere il seguente esercizio.
Una scatola ha la forma di un parallelepipedo rettangolo con la base superiore ovviamente aperta. Questa base è un quadrato di lato lungo 8 cm. Una formica si trova nella posizione P, nella parte esterna della scatola, su uno spigolo laterale, alla distanza di 5 cm dalla base superiore. Nella posizione Q, situata all'interno della scatola sullo spigolo opposto al precedente, ad una distanza di 7 cm dalla base superiore, c'è rimasto un cristallo di zucchero. Calcolare quale traiettoria deve seguire la formica per recarsi da P a Q percorrendo il cammino più breve e calcolare inoltre la lunghezza di tale traiettoria.

[**R**. Conviene sviluppare il parallelepipedo su un piano e poi … ricordi il problema di Erone?
La traiettoria di minima lunghezza misura 20 cm]

[2] Ricordiamo che una **circonferenza massima** è quella che si ottiene sezionando la superficie sferica con un piano passante per il suo centro.

2.2 Occupiamoci adesso delle geodetiche di un cilindro circolare retto.
Se i due punti, fra i quali si vuole tracciare la geodetica, appartengono ad una generatrice, la geodetica è la generatrice medesima.
Se i due punti sono situati su una circonferenza contenuta in un piano perpendicolare all'asse di rotazione, la geodetica è la circonferenza medesima.
Se i due punti sono situati sulla superficie cilindrica in posizioni diverse dalle due esaminate sopra, le geodetiche sono le cosiddette ***eliche cilindriche*** (chiamate anche ***eliche circolari***).
Per capire di cosa si tratti, invitiamo a seguire le considerazioni che andiamo ad esporre.
Consideriamo un punto P in moto uniforme su una circonferenza di centro O, contenuta in un piano perpendicolare all'asse di rotazione del cilindro. Supponiamo poi che contemporaneamente il piano della circonferenza subisca un moto traslatorio uniforme secondo la direzione dell'asse del cilindro.
Nel moto risultante dei due moti suddetti (entrambi uniformi, uno rotatorio e uno traslatorio), il punto P descrive una linea giacente sul cilindro circolare: questa linea è per l'appunto una **elica cilindrica** (Fig. 2.2).
L'asse di rotazione e il raggio del cilindro si dicono *asse* e *raggio* dell'elica.

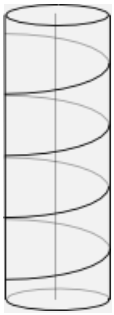

FIG. 2.2

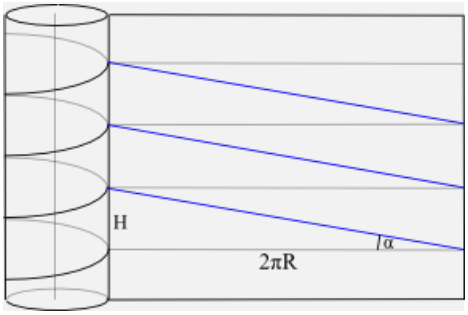

FIG. 2.3

Immaginando di sviluppare il cilindro su un piano, ogni spira dell'elica si distende secondo un segmento di retta e tutti i segmenti ottenuti sono paralleli ed equidistanti (Fig. 2.3). Da ciò si comprende che l'elica cilindrica interseca ogni generatrice del cilindro secondo un angolo costante ed è inclinata di un angolo costante (complementare del primo) rispetto ad ogni piano perpendicolare all'asse di rotazione: la tangente di quest'ultimo angolo si chiama *pendenza* (o *inclinazione*) dell'elica.
Ogni generatrice del cilindro circolare, inoltre, è intersecata più volte da un'elica e la distanza fra due qualsiasi intersezioni consecutive è costante: si chiama *passo* dell'elica.
Se si indica con α l'angolo costante secondo cui l'elica interseca ogni piano perpendicolare al suo asse di rotazione, con R il raggio dell'elica e con H il suo passo (Fig. 2.3), la pendenza dell'elica, tan α, è tale che si ha evidentemente: $\tan\alpha = \frac{H}{2\pi R}$.
A seconda del valore di α vi sono due posizioni limite dell'elica cilindrica: 1) se α=0°, l'elica "degenera" in una circonferenza; 2) se α=90°, l'elica "degenera" in un segmento di retta.
Facciamo notare poi che la proiezione ortogonale di un'elica cilindrica su un piano perpendicolare al suo asse è una circonferenza e ciò è del tutto evidente. Meno evidente è che la proiezione ortogonale su un piano parallelo all'asse è una sinusoide.
Osserviamo, infine, che un'elica cilindrica può essere *destrorsa* (detta anche *oraria*) o *sinistrorsa* (detta anche *antioraria* come quella di figura 2.3) a seconda del verso di rotazione.
In natura è possibile trovare soggetti la cui struttura richiama l'elica cilindrica. Il più famoso è costituito dalla molecola di DNA (acido desossiribonucleico), che di solito presenta una struttura a doppia elica circolare (Fig. 2.4).

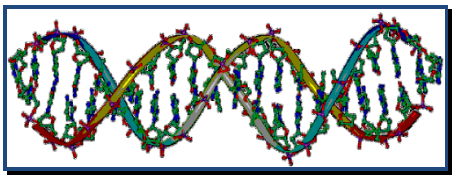

FIG. 2.4

Proponiamo un paio di esercizi.

1) Un'elica circolare si avvolge per tre giri attorno ad un cilindro alto 2 m. Sapendo che intercetta ogni generatrice del cilindro secondo un angolo di 60°, determinare la lunghezza dell'elica. [**R**. 4 m]

2) Un'elica circolare, lunga 4π m, si avvolge per 4 volte attorno ad un cilindro di raggio 0,3 m. Calcolare l'ampiezza dell'angolo secondo cui interseca ogni generatrice del cilindro, approssimato al secondo.

[**R**. 36°52'12"]

2.3 Nel caso del cono circolare retto si possono fare considerazioni analoghe a quelle del cilindro.

Se i due punti, fra i quali si vuole tracciare la geodetica, appartengono ad una generatrice, la geodetica è la generatrice medesima.

Se i due punti sono situati su una circonferenza contenuta in un piano perpendicolare all'asse di rotazione, la geodetica è la circonferenza medesima.

Se i due punti sono situati sulla superficie conica in posizioni diverse dalle due esaminate sopra, le geodetiche sono ancora delle *eliche*, chiamate ***eliche coniche*** (Fig. 2.5).

Su di esse ci limitiamo a dire che intersecano le generatrici del cono secondo angoli di ampiezza costante e la distanza fra due spire consecutive dell'elica si chiama ancora *passo*, ma la sua misura diminuisce via via che ci si avvicina al vertice del cono, che però non si raggiunge mai.

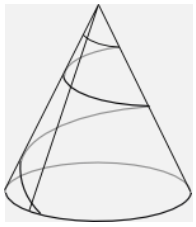

FIG. 2.5

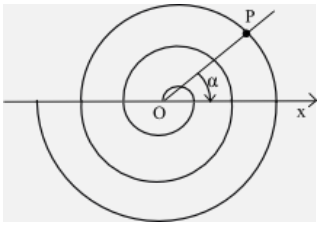

FIG. 2.6

Notiamo inoltre che la proiezione ortogonale di un'elica conica su un piano perpendicolare all'asse di rotazione è una particolare curva, chiamata *spirale di Archimede*. È definita in questo modo: è il luogo geometrico dei punti P la cui distanza da un punto fisso O è direttamente proporzionale all'ampiezza dell'angolo descritto dalla semiretta OP mentre ruota intorno ad O (Fig. 2.6).

Anche un'elica conica può essere *destrorsa* (detta anche *oraria*, come quella di figura 2.5) o *sinistrorsa* (detta anche *antioraria*) a seconda del verso di rotazione.

Ed anche dell'elica conica esistono in natura esseri viventi che ne richiamano la struttura. Uno di essi è una conchiglia, della quale si sono trovati dei fossili che risalgono al periodo del Cenomaniano, Cretaceo superiore, circa 95 milioni di anni fa: il suo nome è *Turrilites costatus* (Fig. 2.7).

FIG. 2.7

3 – Operazioni e strutture algebriche.

3.1 Com'è noto, l'addizione e la moltiplicazione sono operazioni definite nell'insieme dei numeri naturali, nel senso che, addizionando o moltiplicando due numeri naturali qualsiasi, si ottengono ancora numeri naturali.
In generale:
Si chiama **operazione (binaria) definita** in un dato insieme A (o **legge di composizione interna** ad A o **operazione interna** ad A) una funzione di A×A in A,
vale a dire una relazione che ad ogni coppia ordinata di elementi di A associa uno ed un solo elemento di A.
Questo elemento è detto il *risultato* dell'operazione e, in base alla medesima definizione di operazione, esso è unico.
Gli elementi della coppia si dicono *termini* dell'operazione.
Per denotare un'operazione si usano, oltre ai simboli consueti $+$, $\cdot$, $-$, $:$, vari altri simboli come per esempio i seguenti:

$$\divideontimes \quad \circ \quad \perp \quad \oplus \quad \otimes \quad \text{ed altri ancora}$$

e per indicare che alla coppia ordinata $(x,y)\in A\times A$ l'operazione "$\divideontimes$" associa $z\in A$ si scrive: $x\divideontimes y=z$ e, se l'operazione è un'operazione generica non meglio identificata, si legge : « x composto con y è uguale a z ». Chiaramente, se l'operazione è accertata, come per esempio: "+", $x\divideontimes y=z$ diventa $x+y=z$ e si legge « x più y è uguale a z ».
L'insieme A, nel quale è definita una determinata operazione, si dice ***chiuso*** rispetto a quell'operazione.
L'insieme $\mathbb{Q}$ dei razionali è chiuso rispetto all'addizione? Lo è rispetto alla divisione?

Un'operazione, definita in un dato insieme può godere di importanti proprietà. Le andiamo ad analizzare.

- L'operazione $\perp$, definita nell'insieme A, si dice **commutativa** (o che **gode della proprietà commutativa**) se, comunque si prendano $x,y\in A$, risulta:
$$x \perp y = y \perp x\,.$$
L'insieme, in tal caso, si dice *commutativo* o *abeliano* [3] rispetto a quell'operazione.
Chi legge è invitato a fornire esempi di insiemi commutativi rispetto ad un'operazione definita in essi ed esempi di insiemi non commutativi.
La proprietà commutativa consente di parlare di "risultato dell'operazione" senza precisare l'ordine con cui si prendono i due termini. Precisazione che è invece indispensabile se l'operazione non è commutativa.
- L'operazione $\perp$, definita nell'insieme A, si dice **associativa** (o che **gode della proprietà associativa**) se, comunque si prendano $x,y,z\in A$, risulta:
$$(x \perp y) \perp z = x \perp (y \perp z)\,.$$
Chi legge è invitato a fornire esempi di insiemi in cui un'operazione definita è associativa ed esempi in cui non lo è.
Se l'operazione $\perp$, definita nell'insieme A, è associativa, acquista significato la scrittura $x\perp y\perp z$, indicando essa indifferentemente l'uno o l'altro dei risultati uguali $(x\perp y)\perp z$ oppure $x\perp(y\perp z)$. Se, al contrario, l'operazione non fosse associativa allora la scrittura $x\perp y\perp z$ sarebbe ambigua e perciò non avrebbe significato, a meno che non si faccia qualche convenzione al riguardo.
Ricordiamo, per esempio, che per convenzione la scrittura a:b:c sta per (a:b):c.
- Un insieme A, in cui è definita l'operazione $\perp$ si dice dotato di **elemento neutro** (o **elemento indifferente**) rispetto a quell'operazione se, indicato con u tale elemento e preso un qualsiasi elemento $x\in A$, risulta:
$$x \perp u = u \perp x = x\,.$$
Alcuni esempi:
  - nell'insieme $\mathbb{N}$ dei numeri naturali, 0 è elemento neutro rispetto all'addizione, mentre 1 lo è rispetto alla moltiplicazione;
  - nell'insieme P(A) delle parti di un insieme A, l'insieme vuoto $\varnothing$ è elemento neutro rispetto all'operazione di unione, mentre lo stesso insieme A è elemento neutro rispetto all'operazione di intersezione;

[3] Da Niel H. Abel, matematico norvegese, 1802-1829.

- nell'insieme delle affinità piane, l'identità è elemento neutro rispetto all'operazione prodotto di due trasformazioni.

Vale il seguente teorema, di cui forniamo anche la dimostrazione.

TEOREMA. **Se un insieme A è dotato di elemento neutro rispetto all'operazione ⊥, in esso definita, tale elemento è unico**.

DIMOSTRAZIONE. Indicato con u l'elemento neutro, supponiamo che oltre ad esso ci sia in A un secondo elemento neutro u', ovviamente rispetto alla medesima operazione ⊥. Allora si ha:

$$u \perp u' = u \quad \text{ed} \quad u \perp u' = u'.$$

Di conseguenza, in virtù dell'unicità del risultato dell'operazione, deve essere u=u'.

- Dato un insieme A dotato di elemento neutro u rispetto all'operazione ⊥, definita in A, può accadere che, preso un elemento x∈A, esista x'∈A tale che:

$$x \perp x' = x' \perp x = u\,.$$

Se questo accade, gli elementi x ed x' si dicono l'uno **simmetrico** dell'altro rispetto a ⊥.

Cosa si può dire della simmetrizzabilità degli elementi dell'insieme ℕ dei numeri naturali rispetto alle operazioni addizione e moltiplicazione? Cosa degli elementi dell'insieme ℝ dei numeri reali?

- Sia un insieme A in cui è definita l'operazione ⊥. Se esiste in A un elemento z, tale che per ogni a∈A risulti:

$$a \perp z = z \perp a = z\,,$$

tale elemento z si dice **elemento assorbente** (o **elemento nullifico**) rispetto a ⊥.

Alcuni esempi:
- nell'insieme ℝ dei numeri reali, 0 è elemento assorbente rispetto alla moltiplicazione;
- nell'insieme delle matrici quadrate dello stesso ordine, la matrice nulla è elemento assorbente rispetto all'operazione prodotto;
- nell'insieme ℕ dei numeri naturali 1 è elemento assorbente rispetto all'operazione "massimo comune divisore".

- Dato un insieme A in cui è definita l'operazione ⊥, un elemento a ∈A, si dice:
  - **regolare a destra** rispetto a ⊥ se, comunque si prendano x,y ∈A, risulta:
  $$a \perp x = a \perp y \;\rightarrow\; x = y\,;$$
  - **regolare a sinistra** rispetto a ⊥ se, comunque si prendano x,y∈A, risulta:
  $$x \perp a = y \perp a \;\rightarrow\; x = y\,;$$
  - **regolare** rispetto a ⊥ se lo è sia a destra sia a sinistra.

Se ogni elemento di A è regolare rispetto all'operazione ⊥, definita in A (o se lo è solamente a destra o solamente a sinistra) si dice allora che per l'operazione ⊥ vale la **regola si semplificazione** in A (o che vale solo a destra o solo a sinistra).

Cosa si può dire dell'insieme ℚ dei razionali riguardo alla regola di semplificazione delle operazioni addizione, moltiplicazione, sottrazione e divisione?

- In un insieme A siano definite due operazioni ⊕ e ⊙, che si leggono rispettivamente "più cerchiato" e "punto cerchiato". Presi tre qualsiasi elementi x,y,z ∈A, si dice che:
  - ⊙ è **distributiva a sinistra** rispetto a ⊕ se risulta: x⊙(y⊕z)=(x⊙y)⊕(x⊙z);
  - ⊙ è **distributiva a destra a** rispetto a ⊕ se risulta: (y⊕z)⊙x=(y⊙x)⊕(z⊙x);
  - ⊙ è **distributiva** rispetto a ⊕ se lo è sia a destra sia a sinistra.

Alcuni esempi:
- nell'insieme P(A) delle parti di A, l'operazione unione è distributiva rispetto all'intersezione e questa è distributiva rispetto a quella;
- nell'insieme ℚ dei razionali la moltiplicazione è distributiva rispetto all'addizione, mentre l'addizione non lo è rispetto alla moltiplicazione, né a destra né a sinistra;
- nell'insieme $\mathbb{Q}_0$ dei razionali non nulli, la divisione è distributiva a destra rispetto all'addizione ma non lo è a sinistra.

3.2 Quando in un insieme A sono definite una o più operazioni interne si dice che l'insieme è *strutturato* (o *dotato di struttura*) e l'insieme, preso assieme alla sua operazione interna (o alle sue operazioni interne) si dice che è una **struttura algebrica**. L'insieme è chiamato ***sostegno*** della struttura. La struttura algebrica avente per sostegno l'insieme A ed operazione interna $\perp$ si rappresenta con la coppia ordinata $(A, \perp)$.

Una struttura algebrica assume nomi diversi a seconda che si consideri rispetto ad una sola operazione o a due operazioni ed a seconda delle proprietà di cui le operazioni medesime godono. Noi fermeremo la nostra attenzione sulle seguenti strutture algebriche: monoide, gruppo, anello, corpo.

- Un **monoide** è una struttura algebrica con una sola operazione interna che sia associativa e rispetto alla quale il sostegno della struttura abbia l'elemento neutro.
  Se poi l'operazione è anche commutativa il monoide si dice *abeliano* (o *commutativo*).
- Un **gruppo** è un monoide nel quale ogni elemento ammette il simmetrico rispetto all'operazione che lo caratterizza.
  Se poi l'operazione è anche commutativa il gruppo si dice *abeliano* (o *commutativo*).
- Un **anello** è una struttura algebrica, rappresentata dalla terna ordinata $(A, \perp, \divideontimes)$, con due operazioni interne tale che:
  - la struttura $(A, \perp)$ è un gruppo abeliano;
  - la seconda operazione $\divideontimes$ è associativa;
  - la seconda operazione $\divideontimes$ è distribuita rispetto alla prima $\perp$.

  Se poi anche la seconda operazione $\divideontimes$ è commutativa, l'anello si dice *abeliano* (o *commutativo*).
- Un **corpo** è una struttura algebrica, rappresentata dalla terna ordinata $(A, \perp, \divideontimes)$, con due operazioni interne tale che:
  - la struttura $(A, \perp)$ è un gruppo abeliano; sia u l'elemento neutro;
  - la struttura algebrica $(A_u, \divideontimes)$ è un gruppo, essendo $A_u = A - \{u\}$;
  - la seconda operazione $\divideontimes$ è distribuita rispetto alla prima $\perp$.

  Se poi anche la seconda operazione $\divideontimes$ è commutativa, il corpo si dice *abeliano* (o *commutativo*). Un corpo commutativo è chiamato anche ***campo***.

Alcuni esempi:

- le strutture $(\mathbb{N},+)$ e $(\mathbb{N},\cdot)$ sono modelli di monoidi abeliani;
- le strutture $(P(A), \cup)$ e $(P(A), \cap)$ – dove A è un qualsiasi insieme è $\cup$ e $\cap$ sono le note operazioni di unione e intersezione – sono modelli di monoidi abeliani;
- le strutture $(\mathbb{Q}, +)$ e $(\mathbb{Q}_0,\cdot)$ sono modelli di gruppi abeliani, *additivo* il primo, *moltiplicativo* il secondo;
- un modello di anello commutativo è l'*anello degli interi* $(\mathbb{Z}, +, \cdot)$;
- indicato con $\mathbb{Z}[x]$ l'insieme dei polinomi nell'indeterminata x, con coefficienti nell'insieme $\mathbb{Z}$ degli interi, la struttura algebrica $(\mathbb{Z}[x], +, \cdot)$ è ancora un modello di anello commutativo: è denominato *anello dei polinomi* nell'indeterminata x con coefficienti in $\mathbb{Z}$;
- tra i modelli di campo ricordiamo il *campo razionale* $(\mathbb{Q}, +,\cdot)$, il *campo reale* $(\mathbb{R}, +,\cdot)$ e il *campo complesso* $(\mathbb{C}, +,\cdot)$. Sono tutti ovviamente corpi commutativi.

Le strutture algebriche godono di importanti proprietà. Ne prendiamo in esame alcune.

TEOREMA 1. **In ogni gruppo ciascun elemento ha un solo simmetrico**.

DIMOSTRAZIONE. Sia $(A,*)$ un gruppo generico di elemento neutro u e sia x un qualunque elemento di A. Sappiamo, per definizione di gruppo, che x ammette un simmetrico rispetto a $*$: sia x'. Vale a dire che si ha:

$$x * x' = x' * x = u \ .$$

Ci proponiamo di dimostrare che x' è l'unico simmetrico di x rispetto all'operazione del gruppo. Se esistesse un altro elemento simmetrico di x, mettiamo x", dovrebbe essere: $x * x'' = x'' * x = u$. Risulterebbe pertanto, in virtù delle proprietà del gruppo:

$$x' = u * x' = (x'' * x) * x' = x''*(x * x') = x'' * u = x'' \ .$$

In conclusione, ogni elemento di A ammette un solo simmetrico rispetto all'operazione del gruppo.

TEOREMA 2. **Se la struttura algebrica $(\mathbf{A},*)$ è un gruppo allora vale la regola di semplificazione.**
Vale a dire che, comunque si prendano x,y,a ∈A, risulta:

$$a * x = a * y \;\rightarrow\; x = y\,, \qquad x * a = y * a \;\rightarrow\; x = y\,.$$

DIMOSTRAZIONE. Indicato con u l'elemento neutro di A e chiamato a' il simmetrico di a, si ha in successione:

$$a * x = a * y \;\rightarrow\; a' * (a * x) = a' * (a * y) \;\rightarrow\; (a' * a) * x = (a' * a) * y \;\rightarrow\; u * x = u * y \;\rightarrow\; x = y\,;$$
$$x * a = y * a \;\rightarrow\; (x * a) * a' = (y * a) * a' \;\rightarrow\; x * (a * a') = y * (a * a') \;\rightarrow\; x * u = y * u \;\rightarrow\; x = y\,.$$

Come volevasi dimostrare.
Si capisce che, se il gruppo è commutativo, le due righe di dimostrazione si identificano.

TEOREMA 3. **In un corpo $(\mathbf{A},\perp,\divideontimes)$ l'elemento neutro u rispetto alla prima operazione $\perp$ è elemento assorbente rispetto alla seconda $\divideontimes$.**
Vale a dire che, per ogni x∈A, risulta: $x * u = u * x = u$.
DIMOSTRAZIONE. Indicato con x' il simmetrico di x rispetto a $*$, per le proprietà del corpo $(A,\perp,\divideontimes)$, compresa la regola di semplificazione rispetto all'operazione $*$, si ha di seguito:

$$x' \perp u = x' \;\rightarrow\; x * (x' \perp u) = x * x' \;\rightarrow\; (x * x') \perp (x * u) = (x * x') \perp u \;\rightarrow\; x * u = u\,;$$
$$u \perp x' = x' \;\rightarrow\; (u \perp x') * x = x' * x \;\rightarrow\; (u * x) \perp (x' * x) = u \perp (x' * x) \;\rightarrow\; u * x = u\,.$$

In definitiva risulta: $x * u = u * x = u$. [c.v.d.]

NOTA BENE. Il teorema vale anche nel caso in cui la struttura è un anello, ma la dimostrazione va condotta con considerazioni diverse da quelle su esposte. Non ce ne occupiamo.

3.3 Proponiamo adesso alcuni esercizi da risolvere.

1. Considerata l'operazione "massimo comune divisore" che per comodità indichiamo con "Δ", dimostrare che l'insieme ℕ dei numeri naturali è chiuso rispetto ad essa. Studiare quindi la struttura algebrica (ℕ,Δ). Si tratta di qualche struttura particolare?
2. Indicato con M_3 l'insieme dei movimenti che mutano un triangolo equilatero in se stesso e indicata con "∘" l'operazione "prodotto", dimostrare che l'insieme è chiuso rispetto all'operazione considerata. Studiare quindi la struttura algebrica $(M_3, \circ)$, dimostrando che si tratta di un gruppo non commutativo.
   Dimostrare inoltre che, fra gli elementi di M_3 ce ne sono alcuni che a loro volta formano un gruppo commutativo, chiamato *sottogruppo* del gruppo originario.
3. Studiare le affinità, le similitudini e le isometrie piane rispetto alla teoria dei gruppi.
4. Si consideri il seguente insieme:
   $$\mathcal{F} = \left\{x \mid x = \frac{2a+1}{2b+1}\right\},$$
   dove a, b sono numeri interi qualsiasi. Dopo aver dimostrato che esso è chiuso rispetto all'ordinaria moltiplicazione, dimostrare che la struttura algebrica $(\mathcal{F}, \cdot)$ è un gruppo commutativo. Qual è l'elemento neutro?
5. Sia l'operazione "$*$" tale che:
   $$x * y = x + y + 1\,,$$
   dove x, y sono numeri interi qualsiasi. Dimostrare che l'insieme ℤ degli interi è chiuso rispetto ad essa e dimostrare che la struttura algebrica $(\mathbb{Z}, *)$ è un gruppo commutativo. Qual è l'elemento neutro?

3.4 Siano a, b numeri interi qualsiasi e sia m un qualunque numero naturale non nullo. Il numero a si dice *congruo* di b rispetto al *modulo* m se esiste un intero k tale che:

$$a - b = km\,.$$

Si scrive:

$$a \equiv b \pmod{m}$$

e si legge: «a è congruo di b rispetto al modulo m».
Per esempio: 7 è congruo di 4 rispetto al modulo 3, 2 è congruo di 10 rispetto al modulo 4. Lasciamo a chi legge la verifica di ciò.

La relazione "$\Re$" tale che:

$$a\Re b \text{ se e solo se } a \equiv b \pmod{m}$$

si chiama relazione di *congruenza* rispetto al modulo m.

> La teoria che si occupa in maniera completa di questa questione è conosciuta come ***aritmetica modulare***. Fu creata dal matematico tedesco C. F. Gaus (1777-1855), il quale ne tratta diffusamente nella sua opera *Disquisitiones Arthmeticae* (1801). Ha interessanti applicazioni non solo nella teoria dei numeri ma anche in altri campi, come, tanto per fare un esempio, la sicurezza di Internet.
> Per quanto concerne il discorso più generale sull'algebra e, in particolare, sulle strutture algebriche, dopo la creazione del concetto di "gruppo", dovuta al francese Évariste Galois (1811-1832), i contributi più importanti sono venuti dall'inglese Arthur Cayley (1821-1895) e dalla tedesca Emmy Noether (1882-1935), considerata "la madre della moderna algebra astratta".

Per tornare alla relazione di congruenza, si dimostra facilmente (compito che lasciamo a chi legge) che essa è riflessiva, simmetrica e transitiva; è pertanto una relazione di equivalenza. Di conseguenza, opera una partizione dell'insieme $\mathbb{Z}$ dei numeri interi in classi di equivalenza, ciascuna delle quali è formata da tutti i numeri naturali congrui fra loro rispetto al modulo m.

Poiché ogni classe di equivalenza può essere rappresentata da un suo qualsiasi elemento, è conveniente scegliere quale suo rappresentante il minore di tali elementi. E questo, per ogni elemento, altro non è che il resto della divisione dell'elemento medesimo per il numero m. Di modo che l'insieme delle classi di equivalenza è individuato dall'insieme dei resti delle divisioni dei numeri interi per il numero m. Cosicché, indicato con la scrittura $\mathbb{Z}/m$ tale insieme, detto ***insieme delle classi di resto modulo m***, si ha:

$$\mathbb{Z}/m = \{[0],\ [1],\ [2],\ \ldots,\ [m-1]\},$$

oppure, scrivendo per comodità gli elementi di tale insieme senza le parentesi:

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

In figura (Fig. 3.1) è sintetizzata la procedura su descritta, quantunque riferita al caso particolare m=3.

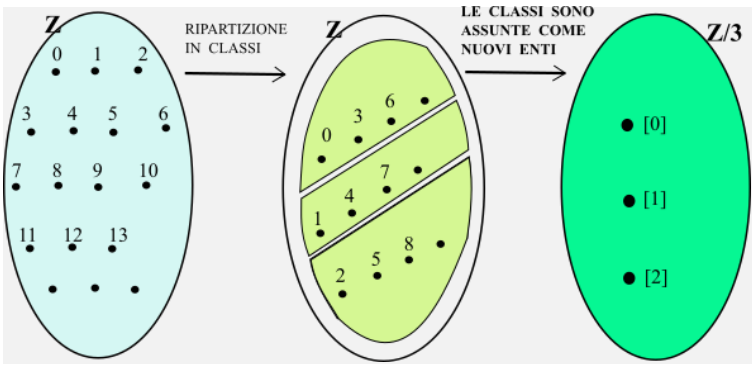

FIG. 3.1

Nell'insieme $\mathbb{Z}/m$ si possono introdurre due operazioni, che chiamiamo "addizione cerchiata" e "moltiplicazione cerchiata", indicate rispettivamente con i simboli "$\oplus$" e "$\odot$" tali che:

$$a \oplus b = a+b, \quad a \odot b = a \cdot b.$$

Per esempio, nell'insieme $\mathbb{Z}/3$:

$$2 \oplus 1 = 3 = 0, \quad 2 \odot 2 = 4 = 1.$$

Le due operazioni, per il modo stesso in cui sono state definite, godono delle medesime proprietà di cui godono le corrispondenti operazioni in $\mathbb{Z}$, vale a dire che sono commutative, associative e rispetto a ciascuna di esse, l'insieme $\mathbb{Z}/m$ ammette l'elemento neutro, che è evidentemente 0 per l'operazione "$\oplus$" e 1 per l'operazione "$\oplus$". Ma tali operazioni godono anche di altre proprietà.

Infatti, ogni elemento dell'insieme $\mathbb{Z}/m$ ammette il simmetrico rispetto a "$\oplus$", come mostra un'apposita tabella (Tab. 3.1) ancorché costruita per m=5.
Per quanto riguarda invece l'operazione "$\odot$", ogni elemento dell'insieme $\mathbb{Z}/m-\{0\}$ ammette il simmetrico rispetto ad essa se e solo se il numero m è un numero primo, come mostrano due apposite tabelle (Tab. 3, a/b), quantunque costruite, la prima per m=4 e la seconda per m=5.
Con riferimento alla tabella 2/a, possiamo constatare che si ha $2\odot 2=0$. Questo fatto, vale a dire che possa essere uguale a 0 il prodotto di due numeri diversi da 0, si verifica ogni volta che m è un numero pari. I numeri a, b tali che $a\odot b=0$ si chiamano *divisori dello zero*.

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

TAB. 3.1

$\odot$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

(a)

$\odot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(b)

TAB. 3.2

A questo punto proponiamo a chi legge la risoluzione dei seguenti esercizi:
- dimostrare che la struttura algebrica $(\mathbb{Z}/m,\ \oplus)$ è un gruppo commutativo, qualunque sia $m\in\mathbb{N}_0$; di ogni elemento indicare il simmetrico rispetto a $\oplus$;
- dimostrare che la struttura algebrica $(\mathbb{Z}/m-\{0\},\ \odot)$ è un monoide commutativo se m è un numero naturale pari diverso da 0, è invece un gruppo commutativo se m è un numero naturale dispari; nel secondo caso, di ogni elemento indicare il simmetrico rispetto a $\odot$;
- cosa si può concludere riguardo alla struttura algebrica $(\mathbb{Z}/m,\ \oplus,\ \odot)$?

3.5 Se si esaminano i diversi modelli di monoidi, gruppi, anelli e corpi che abbiamo presentato passo dopo passo nelle righe precedenti, si constata una circostanza interessante: mentre abbiamo fornito esempi di gruppi commutativi e di gruppi non commutativi, gli esempi riguardanti monoidi, anelli e corpi sono tutti di strutture commutative; per essi nessun esempio di strutture non commutative. In realtà non è semplicissimo trovarne. Ebbene, ci proponiamo adesso di colmare questa lacuna.

- Consideriamo al riguardo l'insieme M delle matrici quadrate del 2° ordine, con coefficienti in $\mathbb{Q}$, strutturato con le due operazioni "somma" (simbolo +) e "prodotto" (simbolo ×). Si dimostra che le strutture algebriche (M,+), (M,×) e (M,+,×) sono nell'ordine un gruppo commutativo, un monoide non commutativo e un anello non commutativo. Dimostrazione che lasciamo a chi legge queste righe, limitandoci a fornire qualche semplice ragguaglio.

Come, per esempio, il fatto che l'elemento neutro rispetto a + e l'elemento nutro rispetto a × sono rispettivamente le cosiddette *matrice nulla* e *matrice unità*, ossia:

$$\begin{Vmatrix} 0 & 0 \\ 0 & 0 \end{Vmatrix} \qquad \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}$$

e che la matrice simmetrica della matrice $\begin{Vmatrix} a & b \\ c & d \end{Vmatrix}$ è la cosiddetta *matrice opposta* $\begin{Vmatrix} -a & -b \\ -c & -d \end{Vmatrix}$.

La struttura (M,+,×) è forse un corpo? Affinché lo sia, dovrebbe esistere di ogni matrice non nulla la matrice simmetrica rispetto a ×. Vale a dire che, presa una qualsiasi matrice non nulla $\begin{Vmatrix} a & b \\ c & d \end{Vmatrix}$, dovrebbe esistere la matrice $\begin{Vmatrix} x & y \\ z & t \end{Vmatrix}$ tale che risulti:

$$\begin{Vmatrix} a & b \\ c & d \end{Vmatrix} \times \begin{Vmatrix} x & y \\ z & t \end{Vmatrix} = \begin{Vmatrix} x & y \\ z & t \end{Vmatrix} \times \begin{Vmatrix} a & b \\ c & d \end{Vmatrix} = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}$$

Poiché:

$$\begin{Vmatrix} a & b \\ c & d \end{Vmatrix} \times \begin{Vmatrix} x & y \\ z & t \end{Vmatrix} = \begin{Vmatrix} ax+bz & ay+bt \\ cx+dz & cy+dt \end{Vmatrix} \quad \text{e} \quad \begin{Vmatrix} x & y \\ z & t \end{Vmatrix} \times \begin{Vmatrix} a & b \\ c & d \end{Vmatrix} = \begin{Vmatrix} xa+yc & xb+yd \\ za+tc & zb+td \end{Vmatrix}$$

Dovrebbe dunque risultare:

$$\begin{cases} ax + bz = 1 \\ ay + bt = 0 \\ cx + dz = 0 \\ cy + dt = 1 \end{cases}$$

e la soluzione di questo sistema nelle indeterminate x, y, z, t dovrebbe soddisfare il sistema:

$$\begin{cases} ax + cy = 1 \\ bx + dy = 0 \\ az + ct = 0 \\ bz + dt = 1 \end{cases}$$

Ora, il primo sistema ammette soluzione (una ed una soltanto) se e solo se risulta $\Delta = ad - bc \neq 0$ e, sotto questa condizione, la soluzione è la seguente:

$$x = \frac{d}{\Delta}, \quad y = -\frac{b}{\Delta}, \quad z = -\frac{c}{\Delta}, \quad t = \frac{a}{\Delta}.$$

E questa quaterna soddisfa anche il secondo sistema, come si può verificare.

Pertanto, solamente sotto la condizione che sia $\Delta = ad - bc \neq 0$, ogni matrice $\begin{Vmatrix} a & b \\ c & d \end{Vmatrix}$ ammette la matrice simmetrica rispetto all'operazione ×. Sotto questa condizione, la matrice $\begin{Vmatrix} a & b \\ c & d \end{Vmatrix}$ si dice *regolare*.

Indicato allora con M_r l'insieme delle matrici regolari del 2° ordine e controllato che è chiuso rispetto alle solite operazioni + e ×, si può concludere che la struttura algebrica $(M_r, +, \times)$ è un corpo non commutativo.

La verifica di tutto è lasciata per esercizio a chi legge.

- Un altro modello di corpo non commutativo è costituito dai cosiddetti *quaternioni di Hamilton* [(4)].

Per comprendere di cosa si tratti, generalizziamo il concetto di numero complesso e consideriamo al riguardo gli enti i, j, k per i quali vale l'operazione "·" come definita in tabella (Tab. 3.2).

·	i	j	k
i	-1	-k	j
j	k	-1	-i
k	-j	i	-1

TAB. 3.2

Si chiamano *quaternioni di Hamilton* (con componenti razionali) entità del tipo:

$$a + bi + cj + dk$$

dove a, b, c, d $\in \mathbb{Q}$, mentre i, j, k sono enti che si comportano come descritto nella precedente tabella.

Detto per inciso, **i numeri complessi sono casi particolari di quaternioni**: basta porre c=d=0.

Nell'insieme H dei quaternioni di Hamilton si possono definire due operazioni, somma (simbolo +) e prodotto (simbolo ·), i cui risultati si ottengono considerando i loro termini come polinomi di 1° grado nelle indeterminate i, j, k con coefficienti in $\mathbb{Q}$ e operando con essi con le ordinarie addizione e moltiplicazione, ma con l'accorgimento di sostituire ai prodotti i·i, i·j, i·k, ecc., i risultati esplicitati dalla tabella suddetta (Tab. 3).

Dimostrare che la struttura (H, +, ·) è un corpo non commutativo. Qual è l'elemento neutro rispetto alla prima operazione? Quale rispetto alla seconda? Qual è il simmetrico di a+bi+cj+dk rispetto a +? Quale il simmetrico rispetto a · ?

[4] Hamilton, William Rowan, astronomo e matematico tedesco, 1821-1881.

4 – Spazi vettoriali.

4.1 Prendiamo in esame l'insieme V dei vettori piani e l'operazione "somma" (+), Sappiamo, non solo che questa operazione è definita in V, ma pure che è commutativa e associativa, che rispetto ad essa esiste in V l'elemento neutro (è il vettore nullo $\vec{0}$) e infine che ogni vettore $\vec{v}$ ammette il simmetrico $-\vec{v}$ rispetto ad essa. In altri termini, la struttura (V,+) è un gruppo commutativo.
È altresì noto che, una volta definito opportunamente il prodotto $k\vec{v}$ di un numero reale k per il vettore $\vec{v}$, risultano dimostrate le seguenti proprietà:

$$1\vec{v} = \vec{v}\,, \quad \alpha(\beta\vec{v}) = (\alpha\beta)\vec{v}\,, \quad (\alpha+\beta)\vec{v} = \alpha\vec{v} + \beta\vec{v}\,, \quad \alpha(\vec{v}+\vec{w}) = \alpha\vec{v} + \alpha\vec{w}\,,$$

dove $\vec{v}$, $\vec{w}$ sono vettori qualsiasi e α, β sono numeri reali qualsiasi [5].

Ebbene, se invece di vettori piani, gli elementi di un insieme V sono "oggetti" qualsiasi per i quali valgano però tutte le proprietà su elencate per i vettori piani, si ottiene una nuova struttura algebrica, chiamata "spazio vettoriale sul corpo reale". Pertanto:

Uno **spazio vettoriale sul corpo reale** è un insieme V di oggetti – chiamati ***vettori*** e indicati simbolicamente con lettere sormontate da una freccia ($\vec{v}$) oppure sottolineate ($\underline{v}$) o infine scritte in grassetto ($\boldsymbol{v}$) – dotato di due operazioni, una detta *somma* e l'altra *prodotto per uno scalare*, tali che:
- rispetto alla somma (simbolo +) l'insieme V acquisisca la struttura di gruppo commutativo;
- rispetto al prodotto per uno scalare si ha la seguente definizione: presi un qualsiasi vettore $\vec{v}$ ed un qualsiasi numero reale α (detto *scalare*), l'operazione restituisce ancora un vettore, indicato con la scrittura $\alpha\vec{v}$; questa operazione deve poi soddisfare alle seguenti proprietà:

  $$1\vec{v} = \vec{v}\,, \quad \alpha(\beta\vec{v}) = (\alpha\beta)\vec{v}\,, \quad (\alpha+\beta)\vec{v} = \alpha\vec{v} + \beta\vec{v}\,, \quad \alpha(\vec{v}+\vec{w}) = \alpha\vec{v} + \alpha\vec{w}\,,$$

  dove $\vec{v}$, $\vec{w}$ sono vettori qualsiasi e α, β sono numeri reali qualsiasi.

Si capisce che i vettori piani, strutturati con le due operazioni suddette costituiscono un modello di spazio vettoriale sul corpo reale. Così come, del resto, i vettori dello spazio ordinario.

4.2 Ma questi non sono gli unici modelli. Ne andiamo ad elencare alcuni altri, invitando il lettore a verificare che effettivamente si tratta di modelli di spazio vettoriale sul corpo reale:
- insieme dei numeri complessi, strutturato con l'ordinaria addizione e con il prodotto di un numero reale per un numero complesso;
- insieme delle matrici quadrate di uno stesso ordine, strutturato con l'ordinaria addizione e con il prodotto di un numero reale per una matrice;
- insieme dei polinomi in una indeterminata con coefficienti reali, strutturato con l'ordinaria addizione e con il prodotto di un numero reale per un polinomio;
- insieme delle funzioni $f(x) = ae^{hx} + be^{kx}$, dove a, b sono parametri reali qualsiasi e h, k sono numeri reali prefissati, strutturato con l'ordinaria addizione e con il prodotto di un numero reale per una funzione;
- insieme delle funzioni reali di una variabile reale, continue in un intervallo]a,b[, strutturato con l'ordinaria addizione e con il prodotto di un numero reale per una funzione.

[5] Cfr.: Testo base, Unità 34: Nozioni di calcolo vettoriale.

5 – Isomorfismo aritmetico.

5.1 Chi avrà occasione di seguire corsi universitari di Matematica (e ci auguriamo che ce ne siano fra chi ci legge), avrà modo di sentire parlare di *morfismi*. Non si tratta di una parolaccia né di un tipo particolare di droga. Il termine deriva dal greco *morphé* e significa *forma*. Ne diamo la definizione:

Date due struttura algebriche $(A,*)$ e $(B,\perp)$, si definisce ***morfismo*** una funzione f di A in B tale che, quali che siano x, y ∈ A, risulti:

$$f(x*y) = f(x) \perp f(y)\ .$$

In realtà ci sono diversi tipi di morfismi, dei quali non ci interessa occuparci in questa sede. Ci interessa tuttavia un particolare tipo di morfismo, il cosiddetto *isomorfismo*.

Ebbene un morfismo prende il nome di ***isomorfismo*** quando la funzione f è biiettiva. Vale a dire che stabilisce una corrispondenza biunivoca fra gli elementi di A e quelli di B.
Due strutture algebriche, fra le quali sussiste un isomorfismo, si dicono ***isomorfe***. Pertanto:
Due strutture algebriche (A,∗) e (B,⊥) si dicono ***isomorfe*** se esiste una biiezione f di A in B tale che, comunque si scelgano x, y in A, risulti: f(x∗y)=f(x)⊥f(y).

Qualche esempio per chiarire.
Consideriamo due strutture algebriche $(A,*)$ e $(B,\perp)$. Supponiamo che esista una biiezione f di A in B. Detti x, y due qualsiasi elementi di A, evidentemente risulta che anche $x*y$ appartiene ad A. I corrispondenti in B di tali elementi – x, y, $x*y$ – sono chiaramente (Fig. 5.1): $f(x), f(y), f(x*y)$.

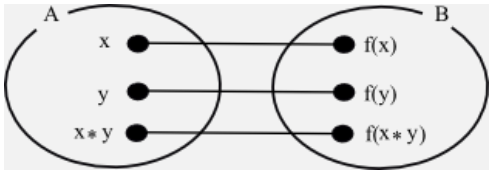

FIG. 5.1

Si pone una domanda: risulta f(x∗y)=f(x)⊥f(y) oppure risulta f(x∗y)≠f(x)⊥f(y)? La risposta è: dipende.

Consideriamo al riguardo due situazioni particolari.

- Siano le strutture algebriche (ℕ,+) ed (ℕ, ×). L'applicazione f : n→n, ∀n∈ℕ, è evidentemente una biiezione di ℕ in ℕ. Se a, b sono due qualsiasi elementi di ℕ, in genere risulta f(a+b)≠f(a)×f(b).

Infatti f(a+b)=a+b, mentre f(a)×f(b)=a×b. E, di norma: a+b≠a×b.
Una figura (Fig. 5.2), dove abbiamo posto a=2 e b=3, visualizza questo fatto.

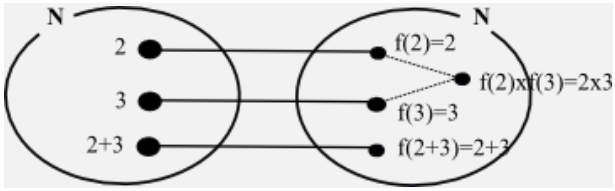

FIG. 5.2

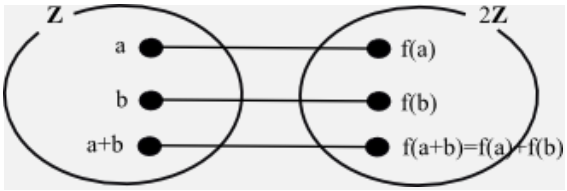

FIG. 5.3

- Siano le strutture algebriche (ℤ,+) e (2ℤ,+), dove 2ℤ è l'insieme degli interi pari. L'applicazione f : z→2z, ∀z∈ℤ, è una biiezione di ℤ in 2ℤ. Se a, b sono due qualsiasi elementi di ℤ, risulta f(a+b)=f(a)+f(b) (Fig. 5.3). Infatti:

$$f(a+b) = 2(a+b) = 2a+2b = f(a)+f(b).$$

Dunque, mentre le strutture (ℕ,+) ed (ℕ,×) non sono isomorfe, lo sono invece le strutture (ℤ,+) e (2ℤ,+).

Il nostro interesse per le strutture isomorfe proviene dal fatto che l'isomorfismo, e in particolare quello fra strutture numeriche, ci permette di dar significato pieno ed esauriente alla scrittura:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}\ .$$

Cosa che in unità del prodotto base abbiamo già fatto, per la verità, ma con qualche concessione al rigore logico. Andiamo a vedere in che modo.

5.2 L'importanza di sapere che due strutture sono isomorfe è sottolineata dal seguente teorema.

TEOREMA. **Siano date due strutture algebriche isomorfe. Se l'operazione di una di esse gode di certe proprietà (commutativa, associativa, …) anche l'operazione dell'altra struttura gode delle stesse proprietà.**
DIMOSTRAZIONE. Siano $(A,*)$ e $(B,\perp)$ due strutture algebriche isomorfe. Questo implica che:

esiste una biiezione f di A in B; $f(x*y)=f(x)\perp f(y)$, $\forall x,y\in A$.

Fermiamo l'attenzione su una delle proprietà di cui eventualmente gode l'operazione "$*$" in A, per esempio la proprietà associativa e facciamo vedere che anche l'operazione "$\perp$" in B gode della stessa proprietà.
Dunque, $\forall x,y,z\in A$:

$$(x*y)*z=x*(y*z) \rightarrow f\big((x*y)*z\big)=f\big(x*(y*z)\big) \rightarrow f(x*y)\perp f(z)=f(x)\perp f(y*z) \rightarrow$$
$$\rightarrow (f(x)\perp f(y))\perp f(z)=f(x)\perp\big(f(y)\perp f(z)\big).$$

Come volevasi dimostrare. Analogamente per altre eventuali proprietà.

5.3 Se l'isomorfismo tra due strutture algebriche è importante, addirittura fondamentale è l'*isomorfismo aritmetico*, perlomeno nell'operazione di allargamento degli insiemi numerici, nel passaggio cioè da $\mathbb{N}$ a $\mathbb{Z}$ a $\mathbb{Q}$ a $\mathbb{R}$ a $\mathbb{C}$.

L'isomorfismo aritmetico è un'idea del matematico siciliano **Michele Cipolla** (1880-1947).

L'isomorfismo aritmetico è in realtà un doppio isomorfismo fra due strutture algebriche. Lo precisiamo meglio.

Due strutture algebriche $(A,*,\cdot)$ e $(B,+,\cdot)$ si dicono in ***isomorfismo aritmetico*** se esiste una funzione f di A in B che stabilisca fra le due strutture due isomorfismi, ognuno rispetto a ciascuna operazione. Vale a dire (Fig. 5.4):

f è una biiezione di A in B; $f(x+y)=f(x)+f(y)$ e $f(x\cdot y)=f(x)\cdot f(y)$, $\forall x,y\in A$.

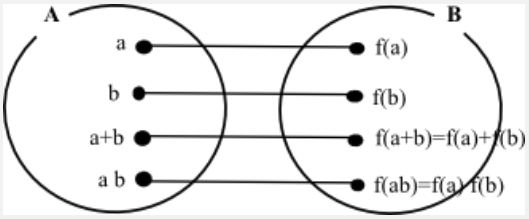

FIG. 5.4

Per esempio, le strutture algebriche $(\mathbb{N},+,\cdot)$ e $(\mathbb{Z}^+,+,\cdot)$, dove $\mathbb{Z}^+$ è l'insieme degli interi non negativi, sono in isomorfismo aritmetico. Infatti:

- esiste una biiezione f di $\mathbb{N}$ in $\mathbb{Z}^+$: basta porre $f(n)=+n$, $\forall n\in\mathbb{N}$;
- inoltre, $\forall x,y\in\mathbb{N}$, risulta:
  $f(x+y)=+(x+y)=(+x)+(+y)=f(x)+f(y)$, $f(x\cdot y)=+(x\cdot y)=(+x)\cdot(+y)=f(x)\cdot f(y)$.

Considerato, invece, l'insieme $2\mathbb{N}$ dei numeri naturali pari e constatato che è chiuso sia rispetto all'ordinaria addizione sia rispetto all'ordinaria moltiplicazione, si dimostra facilmente (compito che lasciamo a chi legge) che le due strutture algebriche $(\mathbb{N},+,\cdot)$ e $(2\mathbb{N},+,\cdot)$ non sono in isomorfismo aritmetico.

A questo punto, in virtù del teorema dimostrato sopra, possiamo concludere con la seguente affermazione:

Due strutture algebriche in isomorfismo aritmetico hanno la stessa aritmetica.

Cioè, posto che le due operazioni siano le ordinarie addizione e moltiplicazione, le due strutture presentano le stesse proprietà formali sia rispetto all'addizione sia rispetto alla moltiplicazione. Inoltre, cosa che può essere dimostrata agevolmente, se la moltiplicazione è distributiva rispetto all'addizione in una delle due strutture lo è anche nell'altra.

Questo fatto – la circostanza cioè che l'aritmetica che vale in una struttura algebrica si conserva in un'altra in isomorfismo aritmetico con essa – unito alla corrispondenza biunivoca che sussiste fra i sostegni delle due strutture – permette di ritenere IDENTICHE le strutture medesime, anche se in realtà sono concettualmente distinte, e pertanto di identificare ogni elemento del sostegno di una di esse con il corrispondente elemento del sostegno dell'altra.

È per l'appunto in virtù dell'isomorfismo aritmetico che sussiste fra le strutture $(\mathbb{N},+,\cdot)$ e $(\mathbb{Z}^+,+,\cdot)$, che possiamo identificare l'insieme $\mathbb{N}$ con l'insieme $\mathbb{Z}^+$, ponendo $+a=a$, $\forall a\in\mathbb{N}$, e concludere che $\mathbb{N}\subset\mathbb{Z}$.
Allo stesso modo possiamo concludere che si ha:

$$\mathbb{Z}\subset\mathbb{Q}\,,\quad \mathbb{Q}\subset\mathbb{R}\,,\quad \mathbb{R}\subset\mathbb{C}\,.$$

Inclusioni valide tutte non esattamente, ma a meno di un isomorfismo aritmetico.
Al contrario, riprendendo le due strutture $(\mathbb{N},+,\cdot)$ e $(2\mathbb{N},+,\cdot)$, considerate poco sopra, il fatto evidenziato che non siano in isomorfismo aritmetico – anche se, occorre sottolinearlo, sono isomorfe le due strutture $(\mathbb{N},+)$ e $(2\mathbb{N},+)$ – non permette di identificare i due insiemi sostegno $\mathbb{N}$ e $2\mathbb{N}$. Cosa che, ad onor del vero, non ha nulla di sorprendente. Caso mai, sarebbe stato sorprendete il risultato contrario, che cioè essi fossero identificabili.
Ma questo controesempio evidenzia che l'isomorfismo aritmetico fra due strutture algebriche è, quando c'è, qualcosa di veramente notevole.

6 – Analogie strutturali.

6.1 Le strutture algebriche e con esse le strutture d'ordine, pur essendo le grandi strutture della matematica, non sono le sole strutture che meritino attenzione. E in effetti, benché non apertamente dichiarate, strutture di vario tipo sono utilizzate anche nel corso degli studi secondari. Lo scopo, forse non chiaramente esplicitato ma non per questo meno importante, è di riuscire a cogliere eventuali analogie strutturali.
Proprio sull'analogia delle strutture vogliamo fare però un'ultima riflessione, per dire che, quando si medita su una determinata struttura, lo si fa ragionando a volte sulla struttura astratta a volte su un suo particolare modello. Ma non è esattamente la stessa cosa e qui intendiamo richiamare l'attenzione del lettore sul diverso punto di vista di chi ragiona sul modello rispetto a chi invece ragiona sulla struttura astratta.
Lo facciamo mutuando da un aneddoto raccontato dalla matematica polacca Zofia Krigowska [(6)] (1904-1988).

In una casa sono invitate alcune persona a cena. Indicato con G l'insieme degli ospiti (ospitati e ospitanti) seduti a tavola, consideriamo le due seguenti relazioni:

- H = relazione di vicinanza: xHy se e solo se x è seduto a fianco di y;
- S = relazione "essere dello stesso sesso": xSy se e solo se x è dello stesso sesso di y.

Le due relazioni godono di alcune proprietà. Precisamente: H è simmetrica, mentre S è riflessiva, simmetrica e transitiva.
Il padrone di casa dispone poi le persone in modo che siano rispettate le due condizioni seguenti:

- Ogni persona ne ha una seduta di fianco alla sua destra e una seduta di fianco alla sua sinistra;
- Due persone dello stesso sesso non sono attigue (cioè non sono sedute l'una di fianco all'altra).

Proprietà e condizioni possono essere formalizzate nel modo seguente:

1) $xHy \rightarrow yHx$, $\forall x,y \in G$;
2) xSx , $\forall x \in G$;
3) $xSy \rightarrow ySx$, $\forall x,y \in G$;
4) $(xSy \wedge ySz) \rightarrow xSz$, $\forall x,y,z \in G$;
5) $\forall x \in G, \exists y,z \in G, y \neq z \wedge xHy \wedge xHz$;
6) $xSy \rightarrow x\overline{H}y$, $\forall x,y \in G$.

Immaginiamo adesso che due persone – A e B – nessuna delle quali presente alla cena, siano chiamate ad esaminare la situazione, ma da angolazioni diverse:

- A ha ricevuto le informazioni 1-6, scritte su un foglietto, e gli è stato spiegato il significato dei simboli;
- anche B ha ricevuto le informazioni 1-6, scritte su un foglietto, ma senza che gli sia stato spiegato il significato dei simboli.

Entrambe le persone A e B comprendono la simbologia matematica ed entrambe sono chiamate a trarre conclusioni sulle caratteristiche dell'insieme G e delle relazioni H ed S. Quali possono essere queste conclusioni?

6.2 La persona A è portata a trarre le sue conclusioni proprio sulla base del significato dei simboli. In particolare:

- in base alle proprietà 5) e 6) conclude che in G vi sono persone di entrambi i sessi e pertanto il numero complessivo delle persone presenti a cena deve essere PARI;
- in base alle proprietà 2) e 6) trae la conclusione banale che "nessuno è seduto di fianco a se stesso".

6.3 Il punto di osservazione di B è più delicato, ma nello stesso tempo è più interessante. Egli non ha alcun motivo per ritenere che le informazioni trovate casualmente si riferiscano a un particolare modello e si trova perciò costretto a

[6] Zofia Krigowska, *Cenni di didattica della matematica*, 1, Bologna, Pitagora, 1979.

ragionare sul possibile significato dei simboli stessi – in particolare G, H, S – per poter trarre delle conclusioni. Scopre così molte situazioni interessanti alle quali si adattano le informazioni 1-6. Ne indichiamo alcune:

- G = insieme di persone sedute attorno ad un tavolo
  H : xHy se e solo se x è seduto di fianco a y
  S : xSy se e solo se x è parente di y;
- G = insieme $\mathbb{N}/m$ dei resti modulo m (m naturale non nullo)
  H : xHy se e solo se $|x - y|=1$
  S : xSy se e solo se $|x - y|$ è pari;
- G = insieme $\mathbb{Z}$ degli interi
  H : xHy se e solo se $|x - y|=1$
  S : xSy se e solo se $x - y$ è pari;
- G = insieme dei vettori piani
  H : xHy se e solo se $|x|=|y| \wedge$ (x ortogonale a y)
  S : xSy se e solo se x è parallelo a y.

Insomma la persona B conclude che le informazioni 1-6 definiscono un certo tipo di struttura di cui sono possibili svariati modelli, non necessariamente isomorfi.
Se egli vuole scoprire altre proprietà della struttura non lo farà certamente riferendosi ad un modello particolare ma si riferirà alla struttura astratta. Così per esempio scoprirà anch'egli che $x\overline{H}x, \forall x \in G$, ma non concluderà certamente che il numero degli elementi di G è pari, dal momento che l'insieme G potrebbe essere infinito, nel qual caso non avrebbe alcun senso dire che il numero dei suoi elementi è pari.
Per concludere, sia A sia B ragionano in modo deduttivo, ma A lo fa in relazione ad un modello, col rischio di commettere errori, C al contrario lo fa in relazione alla struttura astratta e perciò non può sbagliare.
Questo vale sempre:
Un ragionamento condotto su un particolare modello di una struttura può portare a conclusioni errate, nel senso che esse valgono in quel modello ma potrebbero non valere in generale; invece il ragionamento condotto sulla struttura astratta porta a conclusioni che valgono in generale, ossia in ogni modello della struttura medesima.

7 – Numeri algebrici e numeri trascendenti.

7.1 A varie riprese nel testo base abbiamo accennato ai numeri algebrici e ai numeri trascendenti [7]. Qui ci proponiamo un minimo di approfondimento dell'argomento a beneficio di chi volesse saperne di più.
Segnaliamo in via preventiva che ci tornerà utile la celebre formula di Eulero [8]: $e^{\pi i} = -1$.

7.2 Ripartiamo dalle definizioni di numero algebrico e numero trascendente.
Prendiamo in considerazione al riguardo la più generale equazione algebrica (o polinomiale) di grado n, che per comodità riscriviamo qui appresso:

(1) $$\boldsymbol{a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n = 0}$$

dove i coefficienti a_i (con $a_0 \neq 0$) sono numeri reali qualsiasi. Se tali coefficienti sono in particolare numeri razionali, è possibile moltiplicare entrambi i membri dell'equazione per il massimo comune divisore dei coefficienti. In questo modo l'equazione diventa a coefficienti interi. Ebbene tali equazioni svolgono un ruolo fondamentale nelle definizioni di numero algebrico e numero trascendente. Infatti:

Un numero (reale o complesso) si dice ***algebrico*** se esiste qualche equazione algebrica (o polinomiale) a coefficienti interi di cui esso è soluzione. Altrimenti si dice **trascendente**.

È semplice controllare che sono algebrici i seguenti numeri:

$$0,\ 1,\ \sqrt{2},\ i,\ \alpha,\ \varphi,$$

dove i è l'unità immaginaria, α è la sezione aurea dell'unità, φ è il numero aureo, vale a dire:

$$i = \sqrt{-1},\quad \alpha = \frac{\sqrt{5}-1}{2}\ ,\quad \varphi = \frac{\sqrt{5}+1}{2}.$$

Essi sono, infatti, soluzioni nell'ordine delle seguenti equazioni polinomiali:

$$x = 0,\ \ x - 1 = 0,\ \ x^2 - 2 = 0,\ \ x^2 + 1 = 0,\ \ x^2 + x - 1 = 0,\ \ x^2 - x - 1 = 0.$$

È ugualmente facile spiegare che ogni numero razionale è algebrico e che ogni numero irrazionale del tipo $\sqrt{q}$, dove q è un qualsiasi numero razionale, è un numero algebrico. Spiegazioni, queste, che lasciamo a chi legge.
S'intuisce insomma che i numeri algebrici sono infiniti. Vale precisamente il seguente teorema, che però non dimostriamo.

TEOREMA. I numeri algebrici (supponiamo reali, ma il discorso vale ugualmente se sono complessi) formano un insieme infinito numerabile.

Sono ora evidenti alcuni fatti:
- l'insieme dei numeri reali è non numerabile: esattamente è un insieme che ha la potenza del continuo [9];
- tale insieme è formato dall'unione di due insiemi: quello dei numeri (reali) algebrici e quello dei numeri (reali) trascendenti;
- l'insieme dei numeri (reali) algebrici è numerabile.

Ne consegue il seguente corollario.

COROLLARIO. L'insieme dei numeri (reali) trascendenti è non numerabile (precisamente ha la potenza del continuo).

7.3 Il teorema e il corollario precedenti assicurano che ci sono infinitamente più numeri trascendenti che algebrici. Ma da qui a trovare dei numeri trascendenti il passo non fu breve. Di fatto, fino alla metà dell'Ottocento si supponeva

[7] Cfr.: Testo base, Unità 43: Equazioni polinomiali, N° 43.5; Unità 52: Funzioni esponenziali e logaritmiche, N° 52.6.
[8] Cfr.: Testo base, Unità 59: Successioni e progressioni, N° 59.3.2.
[9] Cfr.: Testo base, Unità 54: Insiemi numerici e infinito, N° 53.3.4.

che i numeri "e", base dei logaritmi naturali e il celebre "π" fossero numeri trascendenti, ma senza poterlo provare. E soprattutto non c'era cognizione di altri numeri trascendenti.

Una prima svolta si ebbe nel 1844, allorché il matematico francese **Joseph Liouville** (1809-1882) dimostrò l'esistenza di numeri trascendenti, dei quali fornì una costruzione. Ma tra di essi non figuravano ancora né il numero e né π.
La svolta decisiva si ebbe nel 1882, quando il matematico tedesco **Carl Louis Ferdinand von Lindemann** (1852-1939) – riprendendo un precedente risultato, ottenuto nel 1873 dal francese **Charles Hermite** (1822-1901) – pubblicò un teorema che, generalizzato nel 1885 dal tedesco **Karl Weierstrass** (1815-1897), permette di stabilire immediatamente che sia il numero e sia π sono numeri trascendenti.

Noi possiamo solo limitarci all'enunciato del teorema, la cui dimostrazione è piuttosto complessa.

TEOREMA (di Lindemann-Weierstrass). Se $\alpha_1, \alpha_2, \dots, \alpha_n$ sono numeri algebrici distinti (reali o complessi) e $k_1, k_2, \dots, k_n$ sono numeri interi non tutti nulli, allora l'espressione:

(2) $$\boldsymbol{k_1 e^{\alpha_1} + k_2 e^{\alpha_2} + k_3 e^{\alpha_3} + \cdots + k_n e^{\alpha_n}}$$

non può essere nulla.

Da questo teorema discendono due corollari che assicurano che sia il numero e sia π sono numeri trascendenti.

COROLLARIO 1. **Il numero e è trascendente**.
DIMOSTRAZIONE. Se la precedente espressione (2) non è mai nulla per i valori dei parametri lì specificati, allora il numero e non può essere soluzione di alcuna delle equazioni (1). Esso, pertanto, non può essere algebrico. Non può che essere trascendente.

COROLLARIO 2. **Il numero π è trascendente**.
DIMOSTRAZIONE. Riprendiamo la celebre formula di Eulero:

$$e^{\pi i} + 1 = 0\,.$$

Il suo primo membro si può considerare come un caso particolare dell'espressione (2). Basta assumere nella (2): $n = 2,\ k_1 = 1,\ k_2 = 1,\ \alpha_1 = \pi i,\ \alpha_2 = 0$. Ora, dato che l'espressione $k_1 e^{\alpha_1} + k_2 e^{\alpha_2}$ è uguale a 0 e dato che k_1, k_2 sono numeri interi e 0 è un numero algebrico, il numero πi non può essere algebrico (se lo fosse l'espressione in esame sarebbe diversa da 0 per il teorema di Lindemann). Deve essere perciò trascendente. D'altro canto il fattore i è un numero algebrico. Di conseguenza π non può che essere trascendente.

Un ulteriore passo fondamentale, nella ricerca di numeri trascendenti, fu fatto nel 1934, allorché il sovietico **Aleksandr Osipovič Gelfond** (1906-1968) e il tedesco **Theodor Schneider** (1911-1988), l'uno separatamente e indipendentemente dall'altro, dimostrarono un teorema idoneo allo scopo.

Anche adesso ci limitiamo a fornire solo l'enunciato del teorema, noto come "teorema di Gelfond-Schneider".

TEOREMA (di Gelfond-Schneider). Se a è un qualsiasi numero algebrico, diverso da 0 e da 1, e se b è un qualsiasi numero algebrico non razionale, allora a^b è un numero trascendente.

Il teorema permette evidentemente di costruire innumerevoli numeri trascendenti, quali per esempio i seguenti:

$$2^{\sqrt{2}},\quad \sqrt{2}^{\sqrt{2}},\quad \sqrt{2}^{\sqrt{3}},\quad \sqrt{3}^{\sqrt{2}},\quad i^i,\quad i^{-2i}$$

e infiniti altri.
Anche il numero e^π è trascendente. Basta osservare che dalla formula di Eulero seguono in successione queste altre:

$$e^{\pi i} = -1,\quad \left(e^{\pi i}\right)^{-i} = (-1)^{-i}\,,\quad e^{-\pi i^2} = (i^2)^{-i},\quad e^\pi = i^{-2i}$$

e che i^{-2i} è un numero trascendente.

Al giorno d'oggi non sappiamo ancora se π^e è un numero algebrico o trascendente. Così come non lo sappiamo dei numeri 2e, 2^π e di molti altri.

Un particolare numero, del quale ancora oggi non si è riusciti a stabilire se è algebrico o trascendente (né addirittura se è razionale o irrazionale), è il numero γ, così definito:

$$\gamma = \lim_{n\to\infty}\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}-\ln n\right).$$

È noto come ***costante di Eulero-Mascheroni***. Il suo valore, approssimato per difetto alla 5ª cifra decimale è 0,57721.

Mentre di Eulero più volte ci siamo occupati nel testo base e nelle varie integrazioni, Mascheroni compare qui per la prima volta. Per questo vogliamo parlarne, anche se brevemente.

Lorenzo Mascheroni fu un insigne matematico italiano, nato a Bergamo nel 1750 e morto a Parigi nel 1800. Tra i suoi molti contributi alla matematica ci piace ricordare due sue opere:

- *Adnotationes ad calculum integralem Euleri* (1790-1792), opera nella quale egli calcolò le prime 32 cifre decimali della costante che porta il suo nome; ma si scoprì circa un decennio più tardi che solo le prime 19 erano esatte. Egli sostenne che la costante in questione fosse un numero razionale (di conseguenza sarebbe anche un numero algebrico). Ma senza poterlo provare.
- *La geometria del compasso*, opera pubblicata nel 1797, nella quale egli dimostrò che i problemi geometrici risolubili con riga e compasso possono essere risolti col solo compasso.

8 – Variabili aleatorie discrete in due dimensioni.

8.1 Siano X e Y due variabili aleatorie discrete definite sullo stesso spazio campionario Ω. Si chiama **variabile aleatoria doppia** (o **bidimensionale**), e si indica con (X,Y), la funzione, definita su $\mathbb{R}^2$, che ad ogni evento ω∈Ω associa la coppia ordinata (x,y), dove x=X(ω), y=Y(ω).

Può essere interessante calcolare la probabilità della coppia ordinata (x,y), che indichiamo con p(x,y), ossia:

$$p(x,y) = p(X=x \text{ e } Y=y).$$

Diciamo subito che di norma non è possibile calcolare p(x,y) conoscendo le probabilità p(X=x) e p(Y=y). Bisogna percorrere altre strade.

Per comodità di ragionamento lo facciamo riferendoci ad un caso concreto. In particolare consideriamo l'esperimento consistente nel lancio, eseguito per 3 volte, di una moneta "testa/croce", le cui facce abbiano la stessa probabilità di uscire, vale a dire 1/2. Lo spazio Ω degli eventi di questa nuova variabile è il seguente insieme, dove T sta per "testa" e C sta per "croce":

$$\Omega = \{TTT,\ TTC,\ TCT,\ TCC,\ CTT,\ CTC,\ CCT,\ CCC\}$$

ed ogni evento elementare ha probabilità 1/8 di verificarsi.

Possiamo prendere in considerazione le due variabili aleatorie X e Y definite sullo stesso spazio Ω, tali che:

X = numero di teste uscite, Y = numero di variazioni T/C o C/T nel passaggio da un lancio al successivo.

Osserviamo anzitutto che si ha la situazione sintetizzata nella seguente tabella (Tab. 8.1):

Ω	TTT	TTC	TCT	TCC	CTT	CTC	CCT	CCC
X	3	2	2	1	2	1	1	0
Y	0	1	2	1	1	2	1	0

TAB. 8.1

Questa tabella permette di calcolare p(x,y) per qualsiasi valore di x e y, attribuito rispettivamente alla variabile X e alla variabile Y. Per esempio:

$$p(3,1) = p(X=3 \text{ e } Y=1) = 0,\quad p(1,2) = p(X=1 \text{ e } Y=2) = 1/8,\quad p(1,1) = p(X=1 \text{ e } Y=1) = 2/8.$$

Ebbene, tutte le probabilità p(x,y) possono essere riportate in un'apposita tabella a doppia entrata (Tab. 8.2), la quale fornisce quella che si chiama **distribuzione congiunta** (o **distribuzione doppia**) delle variabili X e Y.

TAB. 8.2 – Distribuzione congiunta delle variabili aleatorie X e Y, definite in tabella 8.1

Y / X	0	1	2	p(X=x)
0	1/8	0	0	1/8
1	0	2/8	1/8	3/8
2	0	2/8	1/8	3/8
3	1/8	0	0	1/8
p(Y=y)	2/8	4/8	2/8	1

Nell'ultima colonna figura la distribuzione di probabilità di X, mentre nell'ultima colonna figura quella di Y.

Osserviamo che risulta:

$$p(X=0)=1/8,\quad p(Y=0)=2/8,\quad p(X=0 \text{ e } Y=0)=1/8,$$

e pertanto:

$$p(X=0 \text{ e } Y=0) \neq p(X=0)\cdot p(Y=0),$$

a conferma di quanto già detto, che di norma p(X=x e Y=y) ≠ p(X=x)·p(Y=y).

In generale, considerate due generiche variabili aleatorie discrete X e Y, definite sullo stesso spazio campionario Ω:

(1) $$X = \begin{pmatrix} x_1 & x_2 & \dots & x_m \\ p_1 & p_2 & \dots & p_m \end{pmatrix},\quad Y = \begin{pmatrix} y_1 & y_2 & \dots & y_n \\ q_1 & q_2 & \dots & q_n \end{pmatrix}$$

ovviamente con $\sum_{i=1}^{m} p_i = 1$ e $\sum_{i=1}^{n} q_i = 1$, la loro distribuzione congiunta può essere rappresentata come nella tabella 8.3, dove con p_{ik} si è indicata la probabilità $p(x_i,y_k)$:

TAB. 8.3 – Distribuzione congiunta delle variabili aleatorie X e Y, definite dalle (1)						
Y / X	y_1	y_2	y_3	…	y_n	p(X=x)
x_1	p_{11}	p_{12}	p_{13}	…	p_{1n}	$p(X=x_1)$
x_2	p_{21}	p_{22}	p_{23}	…	p_{2n}	$p(X=x_2)$
x_3	p_{31}	p_{32}	p_{33}	…	p_{3n}	$p(X=x_3)$
…	…	…	…	…	…	…
x_m	p_{m1}	p_{m2}	p_{m3}	…	p_{mn}	$p(X=x_m)$
p(Y=y)	$p(Y=y_1)$	$p(Y=y_2)$	$p(Y=y_3)$	…	$p(Y=y_n)$	1

La funzione che ad ogni coppia (x,y), con $x \in \{x_1, x_2, \ldots, x_m\}$ e $y \in \{y_1, y_2, \ldots, y_n\}$, associa la probabilità p(x,y) è detta ***funzione di probabilità congiunta*** di X e Y.
È chiamata pure ***funzione di probabilità doppia*** (o ***bivariata***) di X e Y.
Che la variabile doppia (X,Y) sia effettivamente una variabile aleatoria è giustificato dal fatto che ogni probabilità $p_{ik}=p(x_i,y_k)$ è non negativa e la somma di tutte le probabilità p_{ik} è uguale ad 1.
La distribuzione di X, evidenziata anche nell'ultima colonna della tabella che fornisce la distribuzione congiunta di X e Y, e la distribuzione di Y, evidenziata invece nell'ultima riga della stessa tabella, si dicono rispettivamente ***distribuzione marginale di*** X e ***distribuzione marginale di*** Y.

8.2 Prendiamo in considerazione un secondo esempio concreto. Precisamente consideriamo l'esperimento consistente nel lancio di una moneta "testa/croce" e di un "dado" a forma di tetraedro regolare con le facce numerate da 1 a 4. Con un particolare: che tanto la moneta quanto il dado siano truccati. Esattamente:

- la probabilità che nel lancio della moneta esca "testa" è 3/5, mentre è 2/5 quella che esca "croce";
- la probabilità che nel lancio del dado esca "1" è 2/5 [10], mentre quella che esca ogni altro degli altri tre numeri è 1/5.

Lo spazio Ω degli eventi di questa nuova variabile è il seguente insieme, dove T sta per "testa" e C per "croce":

$$\Omega = \{T1, T2, T3, T4, C1, C2, C3, C4\}.$$

Prendiamo in considerazione le due seguenti variabili aleatorie X e Y, definite sullo stesso spazio Ω:
X = 1 se esce T e 2 se esce C nel lancio della moneta;
Y = numero che contrassegna la faccia uscita nel lancio del dado.
Osserviamo subito che si ha la situazione sintetizzata nella seguente tabella (Tab. 8.4), dove sono indicate anche le probabilità P(x,y) degli eventi (X,Y):

Ω	T1	T2	T3	T4	C1	C2	C3	C4
X	1	1	1	1	2	2	2	2
Y	1	2	3	4	1	2	3	4
p(x,y)	$\frac{3}{5}\cdot\frac{2}{5}$	$\frac{3}{5}\cdot\frac{1}{5}$	$\frac{3}{5}\cdot\frac{1}{5}$	$\frac{3}{5}\cdot\frac{1}{5}$	$\frac{2}{5}\cdot\frac{1}{5}$	$\frac{2}{5}\cdot\frac{1}{5}$	$\frac{2}{5}\cdot\frac{1}{5}$	$\frac{2}{5}\cdot\frac{1}{5}$

TAB. 8.4

Oltre a constatare che le probabilità p(x,y) sono tutte non negative, si controlla agevolmente che la somma delle probabilità p(x,y) è uguale a 1. In simboli:

$$\sum_x \sum_y p(x,y) = 1\,.$$

[10] Si capisce che nel caso del dado, per la sua conformazione, per "faccia uscita" s'intende quella coperta.

La prima sommatoria indica che la somma è estesa a tutti gli x, la seconda che è estesa a tutti gli y. Tutto ciò per concludere che la variabile doppia (X,Y) è effettivamente una variabile aleatoria.
Costruiamo allora la distribuzione congiunta delle variabili X e Y (Tab. 8.5), evidenziando anche le loro distribuzioni marginali, che forniscono le distribuzioni di probabilità di X e di Y:

TAB. 8.5 – Distribuzione congiunta delle variabili aleatorie X e Y, definite in tabella 8.4

Y / X	1	2	3	4	p(X=x)
1	6/25	3/25	3/25	3/25	3/5
2	4/25	2/25	2/25	2/25	2/5
p(Y=y)	2/5	1/5	1/5	1/5	1

Osserviamo che risulta:

$$p(X=1) = 3/5, \quad p(Y=1) = 2/5, \quad p(X=1 \text{ e } Y=1) = 6/25$$

e pertanto:

$$p(X=1 \text{ e } Y=1) = p(X=1) \cdot p(Y=1).$$

E così accade per ogni coppia (X=x, Y=y), come si può facilmente controllare. Vale a dire:

$$p(X=x \text{ e } Y=y) = p(X=x) \cdot p(Y=y).$$

Ci sono allora situazioni (come nel secondo esempio) in cui, per ogni coppia (x,y), la probabilità di (X=x e Y=y) è uguale al prodotto delle probabilità di (X=x) e di (Y=y) e ci sono situazioni (come nel primo esempio) in cui questo non accade per ogni coppia.
Nel primo caso le due variabili casuali X e Y si dicono ***dipendenti***, nel secondo si dicono ***indipendenti***.
Accade che, se sono indipendenti i singoli eventi (X=x) e (Y=y), per ogni coppia (x,y), come nel secondo esempio, allora le variabili X e Y sono indipendenti
In questo caso, evidentemente, la distribuzione congiunta delle due variabili X e Y si costruisce facilmente a partire dalle distribuzioni della probabilità di X e di Y.

8.3 Proponiamo alcuni esercizi su questa prima parte dell'argomento.

ESERCIZIO 1. Siano X e Y due variabili aleatorie, la cui distribuzione di probabilità congiunta è rappresentata nella tabella sottostante (Tab. 8.6).
a) Spiegare perché la variabile doppia (X,Y) è una variabile aleatoria.
b) Determinare le distribuzioni delle probabilità (marginali) di X e di Y.
c) Stabilire se le due variabili sono indipendenti.

Y / X	3	4	5	6
1	3/125	7/125	6/125	4/125
2	3/125	7/125	6/125	4/125
3	3/50	7/50	6/50	4/50
4	3/100	7/100	6/100	4/100
5	3/250	7/250	6/250	4/250

TAB. 8.6

ESERCIZIO 2. Si lancia un dato (a forma di cubo) con le facce numerate da 1 a 6, aventi la stessa probabilità di uscire. Si considerino le due variabili aleatorie X e Y, definite sullo stesso spazio Ω={1, 2, 3, 4, 5, 6}, tali che:
- X è uguale al numero uscito se è un multiplo di 2, altrimenti è uguale a 0;
- Y è uguale al numero uscito se è un multiplo di 3, altrimenti è uguale a 0.

a) Costruire la distribuzione congiunta di X e Y.

b) Determinare le distribuzioni delle probabilità (marginali) di X e di Y.
c) Stabilire se le due variabili sono indipendenti.

ESERCIZIO 3. Siano X e Y due variabili aleatorie, la cui distribuzione di probabilità congiunta è rappresentata nella tabella sottostante (Tab. 8.7).

a) Spiegare perché la variabile doppia (X,Y) è una variabile aleatoria.
b) Determinare le distribuzioni delle probabilità (marginali) di X e di Y.
c) Stabilire se le due variabili sono indipendenti.

Y / X	3	4	5
1	1/6	0	1/3
2	1/6	1/3	0

TAB. 8.7

8.4 Come nel caso di una sola variabile aleatoria A si definisce, oltre alla distribuzione di probabilità, anche la media (indicata con M(A) o E(A) o anche μ_A) e la varianza (indicata con var(A)), anche nel caso di una variabile aleatoria doppia si può fare lo stesso, ma con differenze considerevoli rispetto al caso unidimensionale. Ovviamente la variabile aleatoria doppia deve essere definita in modo chiaro e non equivoco.
Così, per esempio, se X e Y sono due variabili aleatorie, sono ben definite le seguenti variabili doppie:

$$X+Y,\ \ XY,\ \ 2X+Y^2,\ \ 2X-XY.$$

Media.
Incominciamo ad occuparci della media di una variabile aleatoria bidimensionale.
Ebbene, indicata con Z(X,Y) una generica funzione di una variabile aleatoria doppia (X,Y) e indicata con p(x,y) la probabilità di (X=x e Y=y), risulta:

$$\mu_Z = M(Z) = \sum_x \sum_y Z(x,y) \cdot p(x,y)\,.$$

Al fine di fornire un esempio, riprendiamo la variabile doppia (X,Y), dove X e Y sono definite sullo spazio Ω descritto nella precedente tabella 1 e consideriamo la funzione:

$$Z = X+Y.$$

Calcoliamo M(Z) ricorrendo direttamente alla formula precedente, che adesso assume questa forma:

$$\mu_Z = M(Z) = \sum_x \sum_y (x+y) \cdot p(x,y)\,.$$

Pertanto, tenendo presente la tabella 8.5 della distribuzione congiunta di X e Y, si ha:

$$\begin{aligned} M(Z) = {} & (0+0)\cdot\frac{1}{8} + (0+1)\cdot 0 + (0+2)\cdot 0 + \\ & +(1+0)\cdot 0 + (1+1)\cdot\frac{2}{8} + (1+2)\cdot\frac{1}{8} + \\ & +(2+0)\cdot 0 + (2+1)\cdot\frac{2}{8} +\cdot (2+2)\cdot\frac{1}{8} + \\ & +(3+0)\cdot\frac{1}{8} + (3+1)\cdot 0 + (3+2)\cdot 0 = \frac{1}{2}+\frac{3}{8}+\frac{3}{4}+\frac{1}{2}+\frac{3}{8} = \frac{5}{2}\,. \end{aligned}$$

In questo caso, in verità, potevamo giungere al risultato utilizzando direttamente la tabella 1. Ricordando allora che tutti gli eventi elementari hanno probabilità 1/8, avremmo ottenuto:

$$M(Z) = \{(3+0)+(2+1)+(2+2)+(1+1)+(2+1)+(1+2)+(1+1)+(0+0)\}\cdot\frac{1}{8} = \frac{5}{2}.$$

Ovviamente come prima.

Si possono dimostrare le due seguenti proprietà, valide quali che siano le variabili casuali X, Y:

(2) **M(X+Y) = M(X)+M(Y), M(aX+bY) = a M(X) + b M(Y),**

essendo a, b parametri reali.
La prima di esse è in realtà un caso particolare della seconda. Basta porre in quest'ultima: a=b=1.

La prima delle due precedenti relazioni può essere subito verificata sempre con riferimento alla particolare situazione correlata alla tabella 5. Riguardo alla seconda proponiamo di verificarla per la variabile 3X+2Y. ancora con riferimento alla tabella 5

Covarianza.

Per quanto concerne la varianza, a differenza del caso unidimensionale, non esiste una formula universale per il calcolo della varianza di una qualsiasi variabile aleatoria doppia (X,Y). Esistono tuttavia formule idonee in alcuni casi specifici e, in particolare, nei due casi dei quali andiamo ad occuparci e che sono i seguenti:

$$Z = X+Y, \qquad Z = aX+bY,$$

dove a, b sono parametri reali.
Prima di occuparci della varianza, però, dobbiamo introdurre un nuovo concetto, quello di covarianza.
La *covarianza* di due variabili casuali X, Y (si indica con cov(X,Y) o anche con σ_{xy}) fornisce una misura dell'intensità con cui le due variabili variano congiuntamente. Essa è uguale alla media dei prodotti degli scarti delle due variabili dalle loro rispettive medie, vale a dire:

$$\sigma_{xy} = \mathrm{cov}(X,Y) = M[(X - \mu_X)(Y - \mu_Y)].$$

Si dimostra che si ha:

$$\mathrm{cov}(X,Y) = M(XY) - \mu_X\mu_Y\,.$$

Vale inoltre il seguente teorema.

TEOREMA. Se le variabili aleatorie X e Y sono indipendenti allora cov(X,Y)=0.

DIMOSTRAZIONE. Se X e Y sono indipendenti allora, com'è noto, per ogni coppia (x,y), si ha: p(x,y)=p(x)p(y).
Pertanto, essendo: $M[(X-\mu_X)(Y-\mu_Y)] = \sum_x\sum_y(x-\mu_X)(y-\mu_Y)p(x,y)$, si ha:

$$\mathrm{cov}(X,Y) = \sum_x\sum_y(x-\mu_X)(y-\mu_Y)p(x)p(y) = \sum_x(x-\mu_X)p(x)\cdot\sum_y(y-\mu_Y)p(y)\,.$$

D'altro canto, il primo fattore nell'ultima espressione è il valor medio degli scarti della variabile X dalla sua media e sappiamo che è uguale a 0. E così pure per il secondo fattore. Dunque, in definitiva: cov(X,Y)=0. [c.v.d.]

Per una verifica si può calcolare la covarianza di X e Y con riferimento alle variabili la cui distribuzione congiunta è riportata in tabella 8.5

ATTENZIONE! Il teorema enuncia una condizione sufficiente:

se X e Y sono indipendenti allora cov(X,Y)=0.

Ma la condizione non è necessaria. Ossia:

se cov(X,Y)=0 non è detto che X e Y siano indipendenti.

Per provarlo basta un esempio. E questo è fornito dalle variabili X e Y, la cui distribuzione congiunta è riportata in tabella 2. Cosa che chi legge può verificare agevolmente.

Varianza.

Possiamo andare adesso alla ricerca della formula per la varianza di X+Y.

$$\mathrm{var}(X+Y) = M([(X+Y)-(\mu_X+\mu_Y)]^2) = M([(X-\mu_X)+(Y-\mu_Y)]^2) =$$
$$= M[(X-\mu_X)^2 + (Y-\mu_Y)^2 + 2(X-\mu_X)(Y-\mu_Y)].$$

Considerato che sia $(X-\mu_X)^2$ sia $(Y-\mu_Y)^2$ sia infine $2(X-\mu_X)(Y-\mu_Y)$ sono variabili casuali, per la seconda delle formule (2) si ha:

$$\mathrm{var}(X+Y) = M[(X-\mu_X)^2] + M[(Y-\mu_Y)^2] + 2M[(X-\mu_X)(Y-\mu_Y)]$$

e infine:

$$\mathbf{var(X+Y) = var(X) + var(Y) + 2\,cov(X,Y)}.$$

Analogamente:

$$\mathbf{var(aX + bY) = a^2\, var(X) + b^2\, var(Y) + 2\, a\, b\, cov(X, Y)}.$$

Anche adesso la prima formula è un caso particolare della seconda. Basta porre in quest'ultima a=b=1.

Al fine di fornire un esempio, facciamo riferimento alla distribuzione di probabilità congiunta rappresentata nella precedente tabella 8.7 e poniamo l'attenzione sulle variabili doppie X+Y e 2X+3Y, e anche sulle variabili XY e (X,Y) ma solo perché sono utili nel calcolo di cov(X,Y).
Dopo alcuni calcoli elementari si trovano i valori sintetizzati nella tabella sottostante (Tab 8.8).

Variabile	X	Y	XY	(X,Y)	X+Y	2X+3Y
Media	3/2	4	35/6	---	11/2	15
Covarianza	---	---	---	–1/6	---	---
Varianza	1/4	2/3	---	---	7/12	5

TAB. 8

Ovviamente, se si sa che le variabili X, Y sono indipendenti, essendo in tal caso cov(X,Y)=0, risulta:

var(X+Y) = var(X) + var(Y), var(aX+bY) = a var(X) + b var(Y).

Verificare ciò con riferimento alle variabili X, Y la cui distribuzione congiunta è riportata in tabella 8.5.

8.5 Proponiamo alcuni esercizi su questa seconda parte dell'argomento.

ESERCIZIO 1. Siano X e Y due variabili aleatorie, la cui distribuzione di probabilità congiunta è rappresentata nella tabella sottostante (Tab. 8.9).

a) Spiegare perché la variabile doppia (X,Y) è una variabile aleatoria.
b) Stabilire se le due variabili sono indipendenti.
c) Calcolare cov(X,Y).
d) La risposta al precedente punto b) e il valore trovato per cov(X,Y) suggeriscono qualcosa?
e) Calcolare var(X+Y) e var(X–2Y).

Y / X	0	2	4
0	1/10	3/10	1/10
2	1/5	1/10	1/5

TAB. 8.9

ESERCIZIO 2. Risolvere lo stesso esercizio precedente ma con riferimento alle variabili aleatorie X e Y, la cui distribuzione di probabilità congiunta è rappresentata nella tabella sottostante (Tab. 8.10).

Y / X	0	2	4
0	1/8	1/8	1/4
2	1/8	3/8	0

TAB. 8.10

ESERCIZIO 3. Si lanciano due "dadi" a forma di tetraedro regolare, ciascuno dei quali ha le facce numerate da 1 a 4. Uno dei due dadi è "onesto", nel senso che tutte le facce hanno la stessa probabilità di uscire. L'altro è truccato e precisamente è uguale a 2/5 la probabilità che esca la faccia "1", mentre le altre facce hanno la stessa probabilità di uscire.

a) Dopo aver costruito lo spazio Ω degli eventi, si considerino le seguenti variabili aleatorie:

X è uguale a 0 se nel dado onesto esce "1" ed è uguale ad 1 in ogni altro caso;

Y è uguale al numero che contrassegna la faccia uscita nel dado truccato.

b) Costruire la distribuzione congiunta di X e Y.

c) Calcolare M(X+Y) e var(X+Y).

[**R**. … , c) 2,95; 1,55]

8.6 La covarianza di due variabili casuali X e Y può assumere in teoria qualsiasi valore reale, per cui è impossibile trarne qualche significato interessante, a parte riconoscere se è positiva, negativa o nulla, e tirare le conclusioni. In particolare:

- Se cov(X,Y)>0 – il che accade quando $X-\mu_X$ e $Y-\mu_Y$ hanno segno concorde – allora X e Y tendono a variare in modo concorde appunto, vale a dire che, se una di esse tende ad assumere valori maggiori del proprio valor medio, anche l'altra lo fa; e così pure per valori minori del valor medio.
- Se cov(X,Y)<0 – il che accade quando $X-\mu_X$ e $Y-\mu_Y$ hanno segno discorde – allora X e Y tendono a variare in modo discorde appunto, vale a dire che, se una di esse tende ad assumere valori maggiori (risp.: minori) del proprio valor medio, l'altra tende ad assumere valor minori (risp.:maggiori) del proprio valor medio.
- Se cov(X,Y)=0 non si può concludere nulla circa la tendenza delle due variabili rispetto alle relative medie.

Per una migliore comprensione di quanto stiamo esponendo può far comodo considerare un piano cartesiano ortogonale in cui si prendono i valori x della variabile casuale X sull'asse delle ascisse e i valori y di Y su quello delle ordinate, e rappresentare le coppie (x,y), ottenendo così una "nuvola" di punti che va sotto il nome di ***diagramma a dispersione*** della variabile casuale doppia (X,Y).

Ebbene, a seconda del segno di cov(X,Y), si ottengono orientativamente grafici del tipo rappresentato nella figura sottostante (Fig. 8.1).

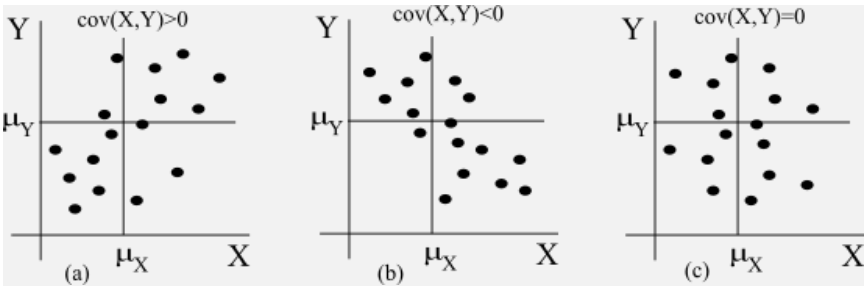

FIG. 8.1

Ad ogni buon conto, un coefficiente che – meglio e più efficacemente della covarianza, ma pur tuttavia da essa dipendente – permette di valutare l'intensità con cui due variabili aleatorie X e Y variano congiuntamente, è il **coefficiente di correlazione lineare** ρ(X,Y), così definito:

$$\boldsymbol{\rho(X,Y) = \frac{cov(X,Y)}{\sigma(X)\cdot\sigma(Y)}}$$

dove σ(X) e σ(Y) sono le deviazioni standard delle due variabili.

Siccome è possibile dimostrare che $|cov(X,Y)| \le \sigma(X)\cdot\sigma(Y)$, tale coefficiente varia tra –1 e +1, estremi inclusi. Vale a dire:

$$-1 \le \rho(X,Y) \le +1\,.$$

Inoltre, essendo σ(X) e σ(Y) entrambi positivi, è evidente che ρ(X,Y) è maggiore, minore o uguale a 0 quando lo è rispettivamente cov(X,Y). Per cui, ρ(X,Y)>0 o ρ(X,Y)<0 o ρ(X,Y)=0 a seconda che il diagramma a dispersione della variabile aleatoria (X,Y) sia rispettivamente del tipo (a) o (b) o (c) di figura 15.

Casi particolari si hanno quanto ρ(X,Y)=±1. In tali casi i punti del diagramma a dispersione tendono ad assemblarsi intorno ad una retta (Fig. 8.2).

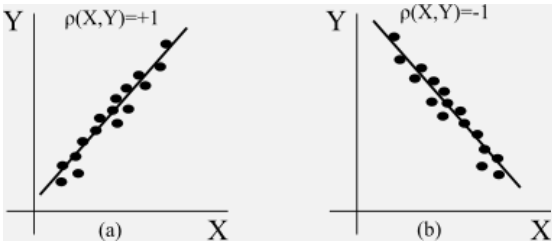

FIG. 8.2

8.7 Anche su quest'ultima parte proponiamo alcuni esercizi.

ESERCIZIO 1. Siano X e Y due variabili aleatorie, la cui distribuzione di probabilità congiunta è rappresentata nella tabella sottostante (Tab. 8.11).

a) Spiegare perché la variabile doppia (X,Y) è una variabile aleatoria.
b) Costruire il relativo diagramma a dispersione, comprensivo delle rette $X=\mu_X$ e $Y=\mu_Y$.
c) Calcolare il coefficiente di correlazione lineare di (X,Y).

Y / X	1	3	5	7
2	0,06	0,09	0,09	0,06
4	0,04	0,06	0,06	0,04
6	0,04	0,06	0,06	0,04
8	0.06	0,09	0,09	0,04

TAB. 8.11

ESERCIZIO 2. Risolvere lo stesso esercizio precedente, ma con riferimento alle variabili aleatorie X e Y, la cui distribuzione di probabilità congiunta è rappresentata nella tabella sottostante (Tab. 8.12).

Y / X	2	4	6	8
1	0,04	0,04	0,02	0
3	0,08	0,05	0,04	0,03
5	0,11	0,10	0,05	0,04
7	0,17	0,11	0,09	0,04

TAB. 8.12

ESERCIZIO 3. Si consideri l'esperimento del lancio, eseguito per 4 volte, di una moneta "T/C" truccata in modo che la probabilità che esca T sia 2/5 mentre quella che esca C sia 3/5.

a) Costruire lo spazio campionario Ω.
b) Considerate le due seguenti variabili aleatorie definite sullo stesso spazio Ω:

X = numero di T uscite nei quattro lanci,
Y = numero di variazioni T/C o C/T nel passaggio da un lancio al successivo,

costruire la tabella che fornisce la distribuzione congiunta di X e Y.

c) Costruire il diagramma a dispersione di (X,Y), comprensivo delle rette $X=\mu_X$ e $Y=\mu_Y$.
d) Calcolare il coefficiente di correlazione lineare di (X,Y).

9 – La legge dei grandi numeri.

9.1 Riprendiamo la legge empirica del caso, che, com'è noto, è una legge suggerita dall'esperienza.

LEGGE EMPIRICA DEL CASO. La frequenza (relativa) f_N di un evento casuale, di probabilità p in senso classico, pur variando al variare del numero N delle prove, eseguite tutte nelle medesime condizioni, al crescere di N si approssima alla probabilità p dell'evento benché non in modo regolare.
La differenza $|f_N–p|$ si approssima a 0 (ma non in modo regolare).

Ricordiamo che a suo tempo [11] è stata assunta come base per la valutazione frequentista della probabilità. Capita, e non di rado, di sentirla chiamare *legge dei grandi numeri*. Non c'è nulla di strano o di sbagliato, a condizione di non confonderla con altre leggi dei grandi numeri, che sono però dei teoremi e perciò dimostrabili all'interno della teoria della probabilità.

> Uno di questi è il teorema di Bernoulli, noto anche come *legge debole dei grandi numeri*. Prende il nome dal matematico che per primo lo formulò, vale a dire lo svizzero **Jakob Bernoulli** (1654-1705). Questa legge compare nel suo libro dal titolo *Ars conjectandi* (*L'arte della congettura*), pubblicato alcuni anni dopo la sua morte, nel 1713.

TEOREMA DI BERNOULLI. In una serie di N prove un evento, che in ciascuna di esse ha la probabilità p di presentarsi, si presenti effettivamente n volte. La probabilità P che il numero $|f_N–p|$, dove $f_N=n/N$, sia inferiore ad un numero positivo assegnato ε tende a 1 quando N tende a infinito. In simboli:

$$\lim_{N\to\infty} P(|f_N–p| < \varepsilon) = 1\,.$$

In termini non formali, il teorema potrebbe essere enunciato in questo modo: «È assai improbabile che, in seguito ad un numero molto grande di prove, la frequenza di un evento sia significativamente diversa dalla probabilità del medesimo».
Il teorema di Bernoulli, al fine di rendere più comprensibile il suo significato, è spesso enunciato in modo impreciso, dicendo che:

"quando il numero delle prove tende a infinito, la differenza $|f_N–p|$ tende a 0"

e quindi, traendo dal teorema una conclusione del tutto ingiustificata, si afferma che:
"la frequenza di un evento A tende alla probabilità di A quando il numero delle prove cresce indefinitamente" [12].
In effetti, sotto questa forma non appare ben chiara la differenza tra il teorema di Bernoulli e la legge empirica del caso e si può essere indotti erroneamente a ritenere equivalenti le due leggi, che in realtà svolgono ruoli diversi e nessuna di esse può sostituire l'altra [13]. Ritorneremo su questi concetti, ma dopo aver dimostrato il teorema di Bernoulli.

9.2 Bernoulli dimostrò il teorema con un procedimento del quale non ci occupiamo. Facciamo vedere invece come il teorema sia una immediata conseguenza di una relazione, nota come "disuguaglianza di Bienaymé-Čebyšëv".

> La relazione sarebbe stata pubblicata un secolo e mezzo dopo la pubblicazione del teorema di Bernoulli e precisamente nel 1853 dallo statistico francese Irénée-Jules Bienaymé (1796-1878) e riscoperta una decina d'anni più tardi dal matematico russo Pafnutij L'vovič Čebyšëv (1821-1894).

[11] Cfr.: Unità 13: Probabilità: un primo approccio, N° 2.3.
[12] Cfr.: Boris V. Gnedenko, Teoria della probabilità, Roma, Editori Riuniti, 1987, pag. 213.
[13] Cfr.: Guido Castelnuovo, *Calcolo delle probabilità*, vol. I, Bologna, Zanichelli, 1961, pag. 104.

Teorema di Bienaymé-Čebyšëv. Detto μ il valor medio di una variabile aleatoria X e σ la deviazione standard, la probabilità P che un valore di X appartenga all'intervallo]μ–kσ, μ+kσ[, dove k è un qualsiasi numero reale positivo, è almeno $1-\frac{1}{k^2}$. In simboli:

$$P[\mu - k\sigma < X < \mu + k\sigma] \geq 1 - \frac{1}{k^2}.$$

DIMOSTRAZIONE. Sia la variabile aleatoria:

$$X = \begin{pmatrix} x_1 & x_2 & \dots & x_N \\ p_1 & p_2 & \dots & p_N \end{pmatrix}.$$

Indicati con $y_1, y_2, \dots, y_N$ i valori assunti dallo scarto Y=X–μ, la deviazione standard σ è tale che:

$$\sigma^2 = \sum_{i=1}^{N} p_i {y_i}^2 .$$

Ammettiamo, per comodità di ragionamento, che gli scarti $y_1, y_2, \dots, y_N$ siano tali da risultare:

$$|y_1| \leq |y_2| \leq \dots \leq |y_N|.$$

Fissata una costante positiva ε, alcuni scarti potranno essere tali che $|y_i|<\varepsilon$, altri invece tali che $|y_i|\geq\varepsilon$. Supponiamo che questi ultimi siano gli scarti seguenti:

$$y_{k+1}, y_{k+2}, \dots, y_N .$$

Se, ora, nella precedente espressione di σ^2, poniamo 0 al posto di y_i quando i≤k e poniamo ε quando i>k, l'espressione al secondo membro diventa $\varepsilon^2 \sum_{i=k+1}^{N} p_i$ e il suo valore è minore di quello originario, per cui si ha:

$$\varepsilon^2 \sum_{i=k+1}^{N} p_i < \sigma^2.$$

L'espressione $\sum_{i=k+1}^{N} p_i$ esprime evidentemente la probabilità che lo scarto Y assuma uno dei valori $y_{k+1}, y_{k+2}, \dots, y_N$, cioè di quei valori che, presi in valore assoluto, sono maggiori o uguali a ε. Dunque, indicata con Q questa probabilità, vale a dire la probabilità di avere uno scarto appartenente all'intervallo]–∞,–ε]∪[+ε, +∞[, si ha:

$$Q<\frac{\sigma^2}{\varepsilon^2};$$

di conseguenza, la probabilità P di avere uno scarto y_i tale che $-\varepsilon<y_i<+\varepsilon$, cioè la probabilità contraria di Q, essendo P=1–Q, è tale che:

$$P \geq 1 - \frac{\sigma^2}{\varepsilon^2}.$$

Posto ora ε=kσ, dove k è un numero reale certamente positivo, possiamo concludere che si ha:

$$P[-k\sigma < X - \mu < +k\sigma] \geq 1 - \frac{1}{k^2}, \text{ vale a dire: } P[\mu - k\sigma < X < \mu + k\sigma] \geq 1 - \frac{1}{k^2}.$$

È così dimostrata la disuguaglianza di Bienaymé-Čebyšëv.

9.3 Il teorema di Bernoulli è, come già detto, un'immediata conseguenza di questa disuguaglianza.

DIMOSTRAZIONE DEL TEOREMA DI BERNOULLI. Supponiamo che la variabile aleatoria X sia la frequenza f_N della variabile binomiale B_N, ossia:

$$X = f_N = \frac{1}{N} B_N .$$

In tal caso il valor medio μ e la deviazione standard σ di X, posto q=1–p, sono tali che:

$$\mu = \frac{1}{N} \cdot Np = p, \quad \sigma^2 = \frac{1}{N^2} \cdot Npq = \frac{pq}{N};$$

dunque:

$$P[p-\varepsilon < f_N < p+\varepsilon] \geq 1 - \frac{p\,q}{N\,\varepsilon^2}$$

e, di conseguenza, osservando che $\frac{p\,q}{N\,\varepsilon^2}$ tende a 0 quando N→∞, si ha:

$$\lim_{N\to\infty} P[p-\varepsilon < f_N < p+\varepsilon] \geq 1\ ;$$

siccome la probabilità P non può essere maggiore di 1 e poiché scrivere $p-\varepsilon<f_N<p+\varepsilon$ è lo stesso che scrivere $|f_N-p|<\varepsilon$, si ha:

$$\lim_{N\to\infty} P(|f_N-p| < \varepsilon) = 1.$$

Esattamente come enuncia il teorema di Bernoulli, che così risulta dimostrato.

9.5 Riassumiamo.

La legge empirica del caso afferma in modo "intuitivo" che, in una successione di N prove, in ognuna delle quali si ha un successo con probabilità costante p, la frequenza dei successi ottenuti tende a p quando N tende a infinito. Ma non dice in che modo, quantitativamente, tale frequenza si accosta a p.

Il teorema di Bernoulli, per parte sua, specifica che in N prove, in ognuna delle quali si ha un successo con probabilità costante p, è da aspettarsi, con probabilità sempre più prossima ad 1, che la differenza $|f_N-p|$ sia minore di un numero ε, anche arbitrariamente piccolo, al crescere indefinitamente del numero N.

Un esempio per cogliere meglio il significato di quanto detto.

ESERCIZIO. Si lancia per N=6.000 volte un dado con le facce numerate da 1 a 6, aventi la stessa probabilità di uscire. Calcolare la probabilità che la differenza tra la frequenza (relativa) delle volte in cui esce la faccia "6" e la probabilità che in un lancio esca tale faccia, sia in valore assoluto minore di 1/120.

RISOLUZIONE. La probabilità P che si verifichi l'evento in questione è tale che si ha:

$$P(|f_N - p| < \varepsilon) \geq 1 - \frac{p\,q}{N\,\varepsilon^2}$$

dove f_N è la frequenza incognita, N=6.000, p=1/6 e q=5/6, mentre ε=1/120. Siccome allora:

$$1 - \frac{p\,q}{N\,\varepsilon^2} = 1 - \frac{\frac{1}{6}\cdot\frac{5}{6}}{6.000\cdot\left(\frac{1}{120}\right)^2} = \frac{2}{3} \approx 66{,}66\%$$

la probabilità cercata è almeno il 66,66% .

In conclusione: in 6.000 lanci del dado, la probabilità che la frequenza (relativa) f_N dei successi si discosti da p di meno di 1/120, è almeno del 66,66% .

In realtà, metodi più accurati permettono di ottenere un valore molto più preciso di quello trovato sopra. Uno di questi metodi è il ricorso alla distribuzione binomiale o alla distribuzione normale.

Al riguardo, indicando con n il numero di successi, cioè il numero di volte in cui, nei 6.000 lanci, esce "6", osserviamo che si ha in successione:

$$|f_N - p| < \varepsilon \ \rightarrow\ \frac{1}{6} - \frac{1}{120} < \frac{n}{6.000} < \frac{1}{6} + \frac{1}{120} \ \rightarrow\ 950 < n < 1050\,.$$

Cosicché:

$$P(|f_N - p| < \varepsilon) = P[950 < n < 1050].$$

Si trova, eventualmente con un idoneo software matematico, che questa probabilità vale circa 91,67% .

I risultati ottenuti utilizzando il teorema di Bernoulli, in verità, non sono granché soddisfacenti sotto l'aspetto quantitativo, ma sono meglio del niente che ci dà la legge empirica del caso, la quale ci dice al più che la frequenza si approssima alla probabilità, ma senza specificare in che modo.

D'altro canto, i risultati ottenuti mediante il teorema di Bernoulli, pur sempre insoddisfacenti, migliorano ovviamente con l'aumentare del numero delle prove e solo per un numero estremamente grande (al limite infinito) diventano soddisfacenti. Per averne un'idea più precisa, raccogliamo in un'apposita tabella (Tab. 9.1) i valori di

$P(|f_N-p|<\varepsilon)$, riferendoci allo stesso esempio precedente, in cui p=1/6, q=5/6, ε=1/120, ma con valori di N via via crescenti riportati nella prima riga della tabella. Nella seconda riga sono riportati i valori minimi che può assumere P, calcolati mediante il teorema di Bernoulli, mentre nella terza riga sono riportati i valori di P calcolati utilizzando la distribuzione normale. Osserviamo che, mentre la frequenza (relativa) f_N risulta sempre compresa tra 19/120 e 21/120, la frequenza assoluta n, vale a dire il numero di successi negli N lanci, varia al variare di N: gli intervalli entro cui varia n sono riportati nella quarta riga della tabella.

N =	1.200	2.400	3.600	4.800	6.000	7.200	8.400	9.600	10.800	12.000
P ≥	–0,6	0,1666	0,4444	0,5833	0,6666	0,7222	0,7618	0,7916	0,8148	0,8333
P =	0,5614	0,7267	0,8203	0,8787	0,9167	0,9422	0,9596	0,9715	0,9799	0,9857
n	tra 190 e 210	tra 380 e 420	tra 570 e 630	tra 760 e 840	tra 950 e 1.050	tra 1.140 e 1.260	tra 1.330 e 1.470	tra 1.520 e 1.680	tra 1.710 e 1.890	tra 1.900 e 2.100

TAB. 9.1

Richiamiamo l'attenzione sul primo valore di P ottenuto per mezzo del teorema di Bernoulli (N=1.200): risulta che P deve essere almeno uguale a –0,6, addirittura un valore negativo, il che consente soltanto di dire che la probabilità P cercata, che non può essere negativa, è almeno uguale a 0. Francamente un'informazione del tutto pleonastica.

Proponiamo a chi legge un esercizio simile al precedente.

ESERCIZIO. Si lancia per N volte una moneta T/C, le cui facce hanno la stessa probabilità di uscire. Calcolare la probabilità che la differenza tra la frequenza (relativa) delle volte in cui esce la faccia "T" e la probabilità che in un lancio esca quella faccia, sia in valore assoluto minore di 1/100, per i seguenti valori di N: 1.000, 2.000, 3.000, 4.000, 5.000, 6.000, 7.000, 8.000, 9.000, 10.000. Compilare una tabella simile alla precedente, utilizzando un idoneo software matematico.

9.6 Un'ultima riflessione per concludere.

Che si tratti della legge empirica del caso o del teorema di Bernoulli, spesso nel linguaggio di tutti i giorni se ne fa un uso improprio oltre che scorretto.

Un esempio illustra ciò che intendiamo dire.

Supponiamo allora che da 170 estrazioni del Lotto non esca il numero 90 sulla ruota di Napoli e che questo numero sia quello che fa registrare il massimo ritardo. Chiamando in causa la legge dei grandi numeri, si conclude che conviene giocare il numero 90 sulla ruota di Napoli perché è quello che nella prossima estrazione ha la maggiore probabilità di uscire.

È un falso ragionamento.

La probabilità che in una qualunque estrazione esca il 90 è esattamente uguale a quella degli altri numeri, indipendentemente da ciò che è successo nelle precedenti estrazioni. Come direbbero i probabilisti, "i numeri non hanno memoria". D'altro canto, né la legge empirica del caso né il teorema di Bernoulli forniscono informazioni su una singola estrazione.

Di fatto, la legge empirica del caso ci dice solamente che, al crescere indefinitamente del numero delle estrazioni, la frequenza (relativa) dell'evento si approssima alla probabilità. ancorché in modo irregolare. Mentre il teorema di Bernoulli ci dice che, al crescere indefinitamente del numero delle estrazioni, è sempre più prossima all'unità la probabilità che la differenza $|f_N-p|$ diventi piccola quanto si vuole.

Ma, lo ribadiamo, né la legge empirica del caso né il teorema di Bernoulli ci forniscono informazioni di sorta su una singola estrazione. Quindi quello che accadrà nella prossima estrazione non può essere spiegato chiamando in causa l'una o l'altro.

10 – Asintoti curvilinei.

10.1 Nel "testo base" – U68: Studio di una funzione, N° 68.2.4 – parlando degli asintoti di una curva di equazione y=f(x), abbiamo fornito alcune indicazioni utili al tracciamento del grafico della funzione, relative al caso in cui la curva presenta "rami parabolici". Indicazioni che però non abbiamo dimostrato.
Qui ci proponiamo di approfondire l'argomento, almeno nel caso in cui la funzione sia una *funzione razionale fratta*, ossia una funzione f(x) tale che sia:

$$f(x) = \frac{A(x)}{B(x)},$$

essendo A(x) e B(x) polinomi nell'indeterminata x con coefficienti reali, non aventi fattori comuni.

10.2 Incominciamo con una definizione di carattere generale.

Sia f(x) una funzione reale di variabile reale definita in un intorno di $+\infty$ [rispettivamente: $-\infty$]. Se risulta:

[1] $$f(x) = g(x) + h(x), \text{ con } \lim_{x\to+\infty} h(x) = 0 \quad \left[\text{risp.: } \lim_{x\to-\infty} h(x) = 0\right],$$

allora si dice che la curva k' di equazione y=g(x) è una **curva asintotica** (o semplicemente un **asintoto**) per la curva k di equazione y=f(x) per $x\to+\infty$ [risp.: $x\to-\infty$].
In particolare:
- se k' è asintoto di k per $x\to+\infty$, allora k' si dice *asintoto destro*;
- se k' è asintoto di k per $x\to-\infty$, allora k' si dice *asintoto sinistro*;
- se k' è asintoto di k sia destro sia sinistro, allora k' si dice *asintoto completo*.

Soffermiamoci sul caso particolare in cui f(x) è una funzione razionale fratta, ossia f(x)=A(x)/B(x), dove A(x) e B(x) sono polinomi in x con coefficienti reali, di gradi rispettivamente g_A e g_B . Indicando con Q(x) e R(x) rispettivamente il polinomio quoziente e il polinomio resto della divisione di A(x) per B(x), si ha:

$$\frac{A(x)}{B(x)} = Q(x) + \frac{R(x)}{B(x)},$$

dove i gradi g_Q e g_R dei polinomi Q(x) e R(x) sono tali che:

$$g_Q = g_A - g_B \quad \text{e} \quad g_R < g_B .$$

Questo implica anzitutto che:

$$\lim_{x\to\pm\infty} \frac{R(x)}{B(x)} = 0 ,$$

per cui la curva k' di equazione y=Q(x) è un asintoto completo per la curva k di equazione y=A(x)/B(x).
Inoltre l'asintoto k' è esattamente una parabola di ordine g_Q. Ossia: una retta se $g_Q\leq1$, una parabola propriamente detta se $g_Q=2$, una parabola cubica se $g_Q=3$, e così via.
Un paio di esempi.
1) Consideriamo la curva k di equazione:

$$y = \frac{x^3+1}{x}.$$

Constatato che risulta:

$$\frac{x^3+1}{x} = x^2 + \frac{1}{x} \quad \text{e} \quad \lim_{x\to\pm\infty} \frac{1}{x} = 0 ,$$

concludiamo che la parabola k' di equazione $y = x^2$ è un asintoto completo per la curva k (Fig. 10.1).

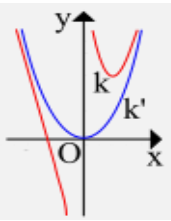

FIG. 10.1

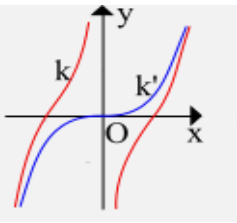

FIG. 10.2

2) Consideriamo la curva k di equazione:

$$y = \frac{x^4 - 4}{x}.$$

Constatato che risulta:

$$\frac{x^4 - 4}{x} = x^3 - \frac{4}{x} \quad \text{e} \quad \lim_{x \to \pm\infty} \frac{4}{x} = 0\,,$$

concludiamo che la parabola cubica k' di equazione $y = x^3$ è un asintoto completo per la curva k (Fig. 10.2).

10.3 La disamina del caso in cui f(x) non è una funzione razionale presenta complicazioni di cui non possiamo occuparci. Ci limitiamo a fornire solamente un esempio, giusto per dare un'idea delle difficoltà cui si va incontro.

Sia allora la curva k di equazione $y = \sqrt{x^2 - 1}$. In seguito a qualche tentativo, si può stabilire che si ha:

$$\sqrt{x^2 - 1} = x - \frac{1}{x + \sqrt{x^2 - 1}} \quad \text{e} \quad \lim_{x \to +\infty} \frac{1}{x + \sqrt{x^2 - 1}} = 0$$

e inoltre:

$$\sqrt{x^2 - 1} = -x - \frac{1}{-x + \sqrt{x^2 - 1}} \quad \text{e} \quad \lim_{x \to -\infty} \frac{1}{-x + \sqrt{x^2 - 1}} = 0\,.$$

Ragion per cui la retta di equazione $y = x$ è un asintoto destro per k, mentre la retta di equazione $y = -x$ è un asintoto sinistro.

Lasciamo a chi legge il disegno del grafico che evidenzia quanto detto.

10.4 Quando, nel testo base, abbiamo accennato al comportamento di una curva e di un suo asintoto rettilineo, abbiamo detto che, da un certo punto in poi la curva e il suo asintoto tendono ad avvicinarsi sempre più, senza mai soprapporsi. Ebbene questo vale anche per l'asintoto curvilineo e ne vogliamo dare una esauriente spiegazione.

Incominciamo con una definizione.

Si dice *distanza di un punto* P *da una curva* h l'estremo inferiore dell'insieme delle distanze di P dai punti di h. Ossia, indicata con dist (P,h) questa distanza:

$$\text{dist}\,(\mathrm{P}, \mathrm{h}) = \inf\{\,\text{dist}\,(\mathrm{P}, \mathrm{Q}),\ \ \forall \mathrm{Q} \in \mathrm{h}\,\}\,.$$

Chiaramente se h è una retta allora dist (P,h) è la lunghezza del segmento perpendicolare condotto da P ad h.

Vale il seguente teorema.

TEOREMA. Se k' è un asintoto destro per la curva k allora $\lim_{x \to +\infty} \text{dist}\,(\mathrm{P}, \mathrm{k}') = 0$, dove P è un punto di k. Analogamente, se k' è un asintoto sinistro per la curva k allora $\lim_{x \to -\infty} \text{dist}\,(\mathrm{P}, \mathrm{k}') = 0$, dove P è un punto di k.

DIMOSTRAZIONE. Ci soffermiamo sul caso dell'asintoto destro. La dimostrazione è analoga nel caso dell'asintoto sinistro.

Siano allora y=f(x) l'equazione della curva k e sia possibile scomporre f(x) in modo che risulti g(x)+h(x), con h(x)→0 per x→+∞. Questo significa che la curva k' di equazione y=g(x) è l'asintoto destro di k.

Ora, un generico punto P di k ha coordinate (x, f(x)), D'altro canto, se Q è un qualsiasi punto di k', risulta per definizione dist (P,k')≤dist (P,Q). In particolare, se Q(x, g(x)), risulta:

$$\text{dist}\,(\mathrm{P},\mathrm{Q}) = |f(x) - g(x)| = |(g(x) + h(x)) - g(x)| = |h(x)|, \text{ con } h(x) \to 0 \text{ per } x \to +\infty.$$

E pertanto: $0 \leq \text{dist}(P,k') \leq |h(x)|$. Da qui, per il teorema del confronto, segue $\lim_{x \to +\infty} \text{dist}(P, k') = 0$. Come si voleva dimostrare.

In base al teorema testé dimostrato, possiamo dunque affermare che, da un certo punto in poi, la curva e il suo asintoto tendono ad avvicinarsi sempre più, ma senza sovrapporsi.

La cosa peraltro è ben visualizzata dai due grafici precedenti (Figg. 10.1 e 10.2).