2.4 Permutazioni e calcolo combinatorio

Per ogni numero naturale n, le funzioni biiettive dall'insieme $\{1, 2, \ldots, n\}$ in se stesso si dicono *permutazioni*. Questo nome si deve al fatto che una tale funzione deve assegnare a ogni numero tra 1 e n un numero tra 1 e n evitando ripetizioni (altrimenti non sarebbe iniettiva) e in modo che tutti compaiano come immagini (altrimenti non sarebbe suriettiva): quindi, essa non fa altro che "cambiare l'ordine" degli elementi $1, 2, \ldots, n$. Ad esempio, se $n = 3$, un esempio di funzione biiettiva da $\{1, 2, 3\}$ in se stesso si ottiene ponendo

$$f(1) = 3$$
$$f(2) = 1$$
$$f(3) = 2$$

oppure

$$f(1) = 3$$
$$f(2) = 2$$
$$f(3) = 1$$

che scambia 3 e 1 tra loro lasciando fisso 2.

Si noti che anche la funzione identica su $\{1, 2, \ldots, n\}$, essendo chiaramente una funzione biiettiva, è una permutazione in base alla definizione data.

In generale, se ho un insieme $A = \{a_1, a_2, \ldots a_n\}$ con n elementi chiameremo *permutazione di* A (o *permutazione di* $a_1, a_2, \ldots, a_n$) una funzione biiettiva $\{1, 2, \ldots, n\} \to A$, ad esempio se $A = \{a, b, c\}$, la funzione $f : \{1, 2, 3\} \to \{a, b, c\}$ definita da

$$f(1) = b$$
$$f(2) = a$$
$$f(3) = c$$

è una permutazione di a, b, c.

Quante sono le possibili permutazioni di n elementi $a_1, a_2, \ldots, a_n$?
Essendo una permutazione una funzione biiettiva $\{1, 2, \ldots, n\} \to \{a_1, a_2, \ldots a_n\}$, dare una permutazione significa semplicemente scegliere le immagini di $1, 2, \ldots, n$ in modo che la funzione così definita sia iniettiva e suriettiva.
Ora, come immagine $f(1)$ di 1 possiamo prendere uno qualunque degli elementi $a_1, a_2, \ldots, a_n$, quindi abbiamo n possibili scelte; per ognuna di queste,

come immagine $f(2)$ di 2 possiamo prendere uno qualunque degli elementi $a_1, a_2, \ldots, a_n$ purchè diverso da quello già scelto come immagine di 1 (altrimenti la funzione costruita non sarebbe iniettiva e non sarebbe una permutazione): quindi per i primi due elementi abbiamo $n(n-1)$ possibili scelte. Andando avanti, vediamo che come immagine di 3 abbiamo $n-2$ possibili scelte (uno qualunque degli n elementi $a_1, a_2, \ldots, a_n$ tranne i due già scelti come immagini di 1 e di 2), una per ognuna delle $n(n-1)$ scelte già fatte per le immagini dei primi due, quindi $n(n-1)(n-2)$ possibilità in tutto, e continuando così fino all'immagine di n, che sarà obbligatoriamente l'ultimo elemento rimasto dopo le scelte dei precedenti, si vede che le scelte possibili come immagini di $1, 2, \ldots, n$ che diano una funzione biiettiva sono

$$n(n-1)(n-2)(n-3)\cdots 1 \tag{2.14}$$

ovvero n moltiplicato per tutti i numeri naturali precedenti escluso lo zero. Il numero che compare nella (2.14) si dice *fattoriale di* n e si denota con il simbolo $n!$.

Ad esempio,

$$1! = 1$$

$$2! = 2 \cdot 1 = 2$$

$$3! = 3 \cdot 2 \cdot 1 = 6$$

$$4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$$

$$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$$

Per convenzione, si pone inoltre $0! = 1$.

Come si vede, il fattoriale di n cresce molto rapidamente all'aumentare di n. Ad esempio, elenchiamo esplicitamente tutte le $3! = 6$ permutazioni di 3 elementi a, b, c:

$$\begin{array}{ccccccccc} 1 & \mapsto & a & 1 & \mapsto & b & 1 & \mapsto & c \\ 2 & \mapsto & b & 2 & \mapsto & a & 2 & \mapsto & b \\ 3 & \mapsto & c & 3 & \mapsto & c & 3 & \mapsto & a \end{array}$$

$$\begin{array}{ccccccccc} 1 & \mapsto & a & 1 & \mapsto & b & 1 & \mapsto & c \\ 2 & \mapsto & c & 2 & \mapsto & c & 2 & \mapsto & a \\ 3 & \mapsto & b & 3 & \mapsto & a & 3 & \mapsto & b \end{array}$$

Il calcolo del numero di permutazioni di un insieme con n elementi fa parte del cosiddetto *calcolo combinatorio*, che si occupa di contare i modi per ordinare, raggruppare o scegliere gli elementi di insiemi finiti, sotto condizioni date.

Vediamo alcuni altri problemi tipici del calcolo combinatorio, nei quali vedremo che il fattoriale ha un ruolo fondamentale.

(1) Supponiamo di voler contare quante sono le possili permutazioni di n elementi in cui però alcuni di essi sono uguali tra loro.

Un esempio familiare di tale situazione si ha quando si vogliono considerare tutti i possibili anagrammi di una parola in cui alcune lettere si ripetono, ad esempio la parola "PAPPA": in tale parola compaiono due lettere in cui una (la A) si ripete due volte e l'altra (la P) si ripete tre volte, per un totale di 5 elementi in tutto (non distinti tra loro). Quanti sono gli anagrammi di tale parola?

Iniziamo con l'osservare che il numero totale di permutazioni possibili delle 5 lettere di tale parola è $5! = 120$, in quanto abbiamo visto sopra che $n!$ è il numero di permutazioni di un insieme di n elementi.

Tuttavia, questo non significa che esistono 120 possibili anagrammi di tale parola: infatti, in queste 120 permutazioni troveremo ogni anagramma di PAPPA ripetuto tante volte quante sono le permutazioni che scambiano solo le A tra loro o solo le P tra loro, perché tali permutazioni non modificano l'anagramma. Quante sono per ogni anagramma dato queste permutazioni che non lo modificano? abbiamo $2! = 2$ permutazioni delle due A tra loro e, per ciascuna di queste, $3! = 6$ permutazioni delle tre P tra loro, ovvero in tutto $2!3! = 12$ permutazioni che in realtà non cambiano un anagramma dato.

Quindi, il numero totale di permutazioni trovate, 120, va diviso per il numero di queste permutazioni che non cambiano l'anagramma corrispondente, cioè 12: il numero di anagrammi distinti della parola PAPPA è quindi $120/12 = 10$:

PAPPA, AAPPP, PPPAA, APAPP, PAAPP, PAPAP, APPAP, PPAAP, APPPA, PPAPA

In generale, supponiamo di avere s elementi distinti in cui il primo si ripete k_1 volte, il secondo k_2 volte, e così via fino all'ultimo che si ripete k_s volte, per un totale di $k_1 + k_2 + \cdots + k_s = n$ elementi non distinti tra loro (quindi ad esempio per la parola PAPPA sarebbe $s = 2$, $k_1 = 2$, $k_2 = 3$ e $n = k_1 + k_2 = 5$): esattamente come per il ragionamento fatto sopra, le possibili permutazioni di questi n elementi distinti sono $n!$, ma questo numero va diviso per il numero di permutazioni che non cambia veramente la configurazione trovata, che sono le permutazioni che scambiano i k_1 elementi che si ripetono tra loro, i k_2 che si ripetono tra loro, e così via fino all'ultimo gruppo di k_s elementi. Esattamente come

abbiamo visto nel nostro esempio, tali permutazioni sono $k_1!k_2!\cdots k_s!$ (per ognuna delle $k_1!$ permutazioni del primo gruppo di elementi uguali, ne abbiamo $k_2!$ del secondo gruppo, $k_3!$ del terzo e così via).

In conclusione, il numero di permutazioni di n elementi in cui c'è un gruppo di k_1 elementi uguali, un altro di k_2 elementi uguali, e così via fino a k_s elementi uguali (si parla di *permutazioni con ripetizione*, per distinguerle dalle permutazioni usuali in cui gli elementi sono tutti distinti, dette anche *permutazioni semplici*) è

$$\frac{n!}{k_1!k_2!\cdots k_s!} \tag{2.15}$$

dove $k_1 + k_2 + \cdots + k_s = n$.

Questo numero è anche detto *coefficiente polinomiale*.

Si noti che se gli elementi fossero tutti distinti senza ripetizioni, questo vorrebbe dire che $k_1 = k_2 = \cdots = k_s = 1$, e nella (2.15) rimarrebbe $n!$, che infatti è come sappiamo il numero di permutazioni di n elementi distinti.

(2) Un'altra importante domanda a cui il calcolo combinatorio risponde è la seguente: dato un insieme X di n elementi e scelto un $k \leq n$, quanti sono i sottoinsiemi di X formati da k elementi?

Ad esempio, se $X = \{a, b, c\}$ (quindi $n = 3$) e $k = 2$, i sottoinsiemi di X con 2 elementi sono

$$\{a, b\}, \{a, c\}, \{b, c\}$$

Si noti che dal momento che un sottoinsieme è determinato dai suoi elementi indipendentemente dall'ordine in cui li mettiamo, il problema può essere riformulato nel modo seguente: in quanti modi diversi possiamo scegliere k elementi da un insieme di n (senza ripetizioni e senza tener conto dell'ordine)? Con una terminologia tipica del calcolo combinatorio, si dice anche che vogliamo sapere quante sono le *combinazioni semplici di n elementi di classe k.*

Rispondiamo ora alla domanda. Se X ha n elementi, e dobbiamo scegliere k elementi distinti tra questi n per formare un sottoinsieme S, per il primo elemento di S abbiamo n possibili scelte (uno qualunque degli elementi di X); per ognuna di queste n scelte, il secondo elemento può essere scelto tra $n - 1$ (tutti gli elementi di X tranne quello già scelto): quindi per i primi due elementi abbiamo $n(n-1)$ possibili scelte.

Per ognuna di queste, abbiamo $n-2$ possibilità per il terzo elemento (tutti gli elementi di X tranne i 2 già scelti), quindi $n(n-1)(n-2)$ possibilità per i primi 3 elementi; $n(n-1)(n-2)(n-3)$ per i primi 4, e in generale se dobbiamo arrivare a k saranno $n(n-1)(n-2)\cdots(n-k+1)$.

Tuttavia, questo numero non è ancora la risposta corretta: ad esempio, per $n=3$ e $k=2$ come nell'esempio di sopra, otterremmo $n(n-1) = 3\cdot 2 = 6$, mentre abbiamo visto che ci sono solo tre sottoinsiemi!

Questo perché, nel ragionamento appena fatto, ci sono scelte diverse del primo, del secondo etc. fino al k -esimo elemento che però danno lo stesso sottoinsieme: ad esempio se in $\{a,b,c\}$ scegliamo a come primo e b come secondo, oppure b come primo a a come secondo, otteniamo chiaramente lo stesso sottoinsieme di due elementi $\{a,b\}$: e non ci sono altre scelte che danno questo stesso sottoinsieme, perché sono solo 2 le permutazioni possibili dei suoi due elementi.

In generale, lo stesso sottoinsieme di k elementi può essere ottenuto mediante esattamente $k!$ scelte diverse, ovvero tante quante sono le possibili permutazioni dei suoi elementi.

Concludiamo che, per avere il numero effettivo di sottoinsiemi di k elementi da un insieme di n, il numero $n(n-1)(n-2)\cdots(n-k+1)$ delle scelte che si possono fare va diviso per il numero $k!$ di scelte che in realtà danno gli stessi elementi disposti in ordine diverso, e quindi è

$$\frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}$$

Tale numero può essere riscritto come segue: moltiplicando numeratore e denominatore per $(n-k)(n-k-1)\cdots 2\cdot 1$, ovvero $(n-k)!$, si trova

$$\frac{n(n-1)(n-2)\cdots(n-k+1)(n-k)(n-k-1)\cdots 2\cdot 1}{k!(n-k)!}$$

Ma ora il numeratore è il prodotto di tutti i naturali da n fino ad arrivare a 1, ovvero $n!$. Quindi otteniamo

$$\frac{n!}{k!(n-k)!} \tag{2.16}$$

L'espressione (2.16) appena scritta si denota $\binom{n}{k}$ e si chiama *coefficiente binomiale*[8].

[8]In effetti, la (2.16) è un particolare caso del coefficiente polinomiale (2.15) quando

Ad esempio, se $n = 3$ e $k = 2$, troviamo $\binom{n}{k} = \frac{3!}{2!1!} = \frac{6}{2} = 3$, in accordo con l'esempio di sopra in cui abbiamo trovato esattamente 3 sottoinsiemi di due elementi in un insieme con 3 elementi.

Il coefficiente binomiale compare in molte importanti formule della matematica, quindi è importante conoscerne le proprietà. Ad esempio, si ha

$$\binom{n}{k} = \binom{n}{n-k} \tag{2.17}$$

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \tag{2.18}$$

(come vedremo tra poco, la seconda ci permette di calcolare rapidamente i coefficienti binomiali al crescere di n senza usare la definizione).

Per dimostrare la (2.17), basta scrivere il secondo membro in base alla definizione stessa di binomiale, cioè la (2.16) con $n - k$ al posto di k:

$$\binom{n}{n-k} = \frac{n!}{(n-k)![n-(n-k)]!} = \frac{n!}{(n-k)!(n-n+k)!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$$

Dimostriamo ora la (2.18): si ha per definizione di binomiale

$$\binom{n-1}{k} + \binom{n-1}{k-1} = \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)![(n-1)-(k-1)]!} =$$

$$= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!}. \tag{2.19}$$

Per sommare le due frazioni, osserviamo che $k!(n-k)!$ è un multiplo comune dei denominatori: infatti, tale numero si ottiene moltiplicando il primo denominatore per $n-k$ (che moltiplicato per $(n-1-k)!$ lo fa diventare $(n-k)!$), ma anche moltiplicando il secondo denominatore per k (che moltiplicato per $(k-1)!$ lo fa diventare $k!$). Usando allora

$s = 2$ (da cui binomiale): infatti, in tal caso la (2.15) diventa $\frac{n!}{k_1!k_2!}$ con $k_1 + k_2 = n$, ovvero $k_2 = n - k_1$: quindi possiamo riscriverlo come $\frac{n!}{k_1!(n-k_1)!}$ che è, a parte il k_1 al posto di k, proprio la (2.16).

$k!(n-k)!$ come multiplo comune, possiamo sommare le frazioni mettendo tutto allo stesso denominatore (esattamente come quando si fa la somma di due frazioni numeriche) e otteniamo che la (2.19) è uguale a

$$\frac{(n-k)\cdot(n-1)! + k\cdot(n-1)!}{k!(n-k)!}$$

ovvero, mettendo in evidenza $(n-1)!$ nei due addendi a numeratore,

$$\frac{[(n-k)+k]\cdot(n-1)!}{k!(n-k)!} = \frac{n\cdot(n-1)!}{k!(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

proprio come volevamo dimostrare.

Come abbiamo accennato, la (2.18) ci permette di calcolare velocemente i coefficienti binomiali al crescere di n: se disponiamo per ogni $n = 0, 1, 2, \ldots$ i coefficienti binomiali $\binom{n}{k}$ al variare di $k = 0, 1, \ldots, n$ in riga, ovvero

	$(k=0)$	$(k=1)$	$(k=2)$	$(k=3)$	$(k=4)$	$(k=5)$
$(n=0)$	$\binom{0}{0}$					
$(n=1)$	$\binom{1}{0}$	$\binom{1}{1}$				
$(n=2)$	$\binom{2}{0}$	$\binom{2}{1}$	$\binom{2}{2}$			
$(n=3)$	$\binom{3}{0}$	$\binom{3}{1}$	$\binom{3}{2}$	$\binom{3}{3}$		
$(n=4)$	$\binom{4}{0}$	$\binom{4}{1}$	$\binom{4}{2}$	$\binom{4}{3}$	$\binom{4}{4}$	
$(n=5)$	$\binom{5}{0}$	$\binom{5}{1}$	$\binom{5}{2}$	$\binom{5}{3}$	$\binom{5}{4}$	$\binom{5}{5}$
			$\ldots$			

allora la (2.18) ci dice che un'entrata $\binom{n}{k}$ della tabella (che si trova all'incrocio di riga n-esima e colonna k-esima) si ottiene sommando l'entrata sopra di lei, che si trova nella stessa colonna, la k-esima, ma una riga sopra, la $(n-1)$-esima (ovvero il coefficiente binomiale $\binom{n-1}{k}$) più l'entrata che si trova a sinistra di quest'ultima, cioè sempre nella riga sopra, la $(n-1)$-esima, e nella colonna di un passo più a sinistra, la $(k-1)$-esima (ovvero il coefficiente $\binom{n-1}{k-1}$).

A questo punto, conoscendo le prime due righe (in quanto $\binom{0}{0} = \binom{1}{0} = \binom{1}{1} = 1$) con questa regola si ricostruiscono rapidamente tutte le entrate della tabella:

	$(k=0)$	$(k=1)$	$(k=2)$	$(k=3)$	$(k=4)$	$(k=5)$
$(n=0)$	1					
$(n=1)$	1	1				
$(n=2)$	1	2	1			
$(n=3)$	1	3	3	1		
$(n=4)$	1	**4**	**6**	4	1	
$(n=5)$	1	5	**10**	10	5	1
			$\dots$			

(ad esempio, abbiamo messo in evidenza in grassetto il fatto che il 10 dell'ultima riga è stato ottenuto sommando il 6 sopra di lui più il 4 a sinistra del 6).

La tabella appena scritta si dice anche *triangolo di Tartaglia*.

I coefficienti ottenuti servono, tra le altre cose, per calcolare le potenze $(a+b)^n$ di un binomio: infatti, vale la formula

$$(a+b)^n =$$
$$= \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-2}a^2b^{n-2} + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

che può essere scritta

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k \tag{2.20}$$

(dove il simbolo $\sum$, simbolo di sommatoria, indica che dobbiamo sommare tutti gli addendi del tipo $\binom{n}{k}a^{n-k}b^k$ con k che varia da 0 a n).

Ad esempio, applicando questa formula e guardando i coefficienti della tabella si trova

$$(a+b)^2 = a^2 + 2ab + b^2$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$
$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$

Dimostreremo la (2.20) nel prossimo paragrafo, usando un metodo detto *induzione*.

(3) Un altro problema tipico del calcolo combinatorio è il seguente: dato un insieme X con n elementi, e scelto un $k \leq n$, in quanti modi possiamo scegliere k distinti elementi da X tenendo conto dell'ordine? (diversamente da quanto visto in (2) per i sottoinsiemi di k elementi dove l'ordine degli elementi non conta).

Ad esempio, se $X = \{a, b, c\}$ (cioè $n = 3$) e scegliamo $k = 2$, abbiamo le seguenti possibilità:

$$ab, ba, ac, ca, bc, cb$$

In calcolo combinatorio si dice che vogliamo determinare il numero delle *disposizioni semplici di n elementi di classe k.*

La risposta a questa domanda è facile se si tiene conto di quanto già detto per risolvere il problema (2): lì abbiamo visto che il numero di sottoinsiemi di k elementi presi da X è $n(n-1)(n-2)\cdots(n-k+1)$ diviso per $k!$ (il numero di permutazioni dei k elementi del sottoinsieme) perché ordinamenti diversi di questi elementi danno lo stesso sottoinsieme.

Dal momento che qui vogliamo invece tener conto dell'ordine, non dobbiamo dividere per $k!$ e il numero cercato è semplicemente

$$n(n-1)(n-2)\cdots(n-k+1).$$

Allo scopo di scrivere questo numero in una forma più conveniente, moltiplichiamolo e dividiamolo per $(n-k)(n-k-1)\cdots 2\cdot 1$ (ovvero $(n-k)!$) ottenendo

$$n(n-1)(n-2)\cdots(n-k+1) =$$
$$= \frac{n(n-1)(n-2)\cdots(n-k+1)(n-k)(n-k-1)\cdots 2\cdot 1}{(n-k)!} = \frac{n!}{(n-k)!}$$

(4) Se nel problema (3) ammettiamo anche le ripetizioni otteniamo le cosiddette *disposizioni con ripetizione di n elementi di classe k.*

Ovvero, dato un insieme X con n elementi, e scelto un $k \leq n$, ci chiediamo in quanti modi possiamo scegliere k elementi da X, eventualmente con ripetizioni e tenendo conto dell'ordine.

Ad esempio, se $X = \{a, b, c\}$ (cioè $n = 3$) e $k = 2$, abbiamo le seguenti possibilità:

$$aa, bb, cc, ab, ba, ac, ca, bc, cb$$

In questo caso, la risposta è particolarmente semplice: il primo elemento può essere scelto in n modi (può essere un qualunque elemento di X), il secondo anche (non dobbiamo escludere il primo già scelto perché sono ammesse ripetizioni) e così via per tutti gli altri: quindi abbiamo $n \cdot n \cdot \cdots \cdot n = n^k$ possibilità, tenendo conto anche dell'ordine.

Si osservi che nello scegliere k elementi da X ammettendo ripetizioni e tenendo conto dell'ordine, stiamo equivalentemente considerando tutte le k-uple ordinate di elementi di X, ovvero l'insieme prodotto cartesiano X^k di X per se stesso k volte: ad esempio per l'insieme $X = \{a, b, c\}$ considerato sopra, si ha

$$X^2 = \{(a, a), (b, b), (c, c), (a, b), (b, a), (a, c), (c, a), (b, c), (c, b)\}$$

e si vede bene che dare le coppie ordinate o le disposizioni con ripetizione è sostanzialmente la stessa cosa.

(5) Infine, consideriamo le cosiddette *combinazioni con ripetizione di n elementi di classe k*: rispetto alle combinazioni semplici, ovvero i sottoinsiemi di k elementi, studiate in (2), ammettiamo anche le ripetizioni: più precisamente, dato un insieme X con n elementi, e scelto un $k \leq n$, ci chiediamo in quanti modi possiamo scegliere k elementi da X, eventualmente con ripetizioni, ma sempre senza tener conto dell'ordine come nelle combinazioni semplici.

Ad esempio, se $X = \{a, b, c\}$ (cioè $n = 3$) e $k = 2$, abbiamo le seguenti possibilità:

$$aa, bb, cc, ab, ac, bc$$

Notiamo che dare una di queste combinazioni significa semplicemente dire il numero di volte che si ripete a, il numero di volte che si ripete b e il numero di volte che si ripete c, con la condizione che la somma di questi tre numeri deve essere 2, perché in tutto dobbiamo avere solo 2 elementi (questi numeri possono essere anche 0, ad esempio in aa, a si ripete 2 volte, b zero volte e c zero volte; in bc, a si ripete 0 volte, b una volta e c una volta).

Possiamo rappresentare allora ognuna di queste combinazioni come uno schema del tipo

$$* * \cdots * \circ * * \cdots * \circ * * \cdots *$$

dove il numero di asterischi della prima serie ci dice quante volte si ripete a, il numero di asterischi della seconda serie (dopo il primo cerchietto) ci dice quante volte si ripete b, e il numero di asterischi della terza serie (quelli dopo il secondo cerchietto) ci dice quante volte si ripete c.

Ad esempio, ab è rappresentato da $* \circ * \circ$ (il primo asterisco ci dice che a si ripete una volta, il secondo che b si ripete una volta, e l'assenza di asterischi dopo il secondo cerchietto significa che c si ripete 0 volte, ovvero non compare nella combinazione); cc invece è rappresentato da $\circ \circ **$ (nessun asterisco prima del primo cerchietto significa che a si ripete 0 volte, nessun asterisco tra il primo e il secondo cerchietto significa che b si ripete 0 volte, 2 asterischi dopo il secondo cerchietto significano che c si ripete 2 volte).

In generale, se l'insieme X ha n elementi, avremo n serie di asterischi, separate da $n-1$ cerchietti, e il numero totale di asterischi deve essere k.

La nostra domanda equivale allora a chiedere: quanti possibili schemi di questo tipo con k asterischi e $n-1$ cerchietti possiamo formare?

Tali schemi saranno tanti quanti i modi diversi di permutare gli asterischi e i cerchietti tra loro, che essendo in tutto $k+n-1$, sono $(k+n-1)!$, diviso per il numero di permutazioni che lasciano invariato uno schema dato, ovvero quelle che permutano i cerchietti tra loro e gli asterischi tra loro: essendoci k asterischi, le permutazioni che permutano gli asterischi tra loro sono $k!$ mentre essendoci $n-1$ cerchietti, le permutazioni che permutano i cerchietti tra loro sono $(n-1)!$. Quindi dobbiamo dividere il numero totale di permutazioni per $k!(n-1)!$, ottenendo

$$\frac{k+n-1}{k!(n-1)!} = \binom{k+n-1}{k}$$

2.5 L'induzione

Come abbiamo anticipato sopra, dimostreremo in questo paragrafo la formula (2.20) con un metodo detto *induzione*, che ora illustriamo.

Quando un teorema afferma che una certa formula o una certa proprietà P valgono per ogni numero naturale n (ad esempio, nel caso della formula (2.20), stiamo affermando che si tratta dello sviluppo di $(a+b)^n$ per ogni n), esso può essere dimostrato provando i due seguenti fatti:

(1) la proprietà P vale per $n = 0$

(2) ogniqualvolta la P vale per un certo numero n, allora vale per il suo successivo $n + 1$ (scriveremo $P(n) \Rightarrow P(n + 1)$)

Questi due fatti, insieme, garantiscono che l'affermazione è vera per ogni numero naturale: intuitivamente, quello che succede è che se da (1) sappiamo che l'affermazione vale per $n = 0$, applicando la (2) sappiamo che essa deve valere per il suo successivo, cioè $n = 1$; ma se vale per $n = 1$, sempre dalla (2) deduciamo che vale per il suo successivo $n = 2$, e così via. Rigorosamente, il fatto che questo meccanismo a catena impichi che l'affermazione è vera per l'insieme infinito di tutti i numeri naturali dipende dagli assiomi che definiscono i numeri naturali stessi, ma questo va oltre lo scopo di questo corso.

Osservazione 2.26. Il metodo si applica anche quando si vuole dimostrare che una certa proprietà P vale non per ogni naturale ma a partire da un $n_0 \in \mathbb{N}$ dato: in tal caso, bisogna dimostrare che

(1) la proprietà P vale per n_0

(2) ogniqualvolta la P vale per un certo numero n, allora vale per il suo successivo $n + 1$ (scriveremo $P(n) \Rightarrow P(n + 1)$)

Prima di usare tale metodo per dimostrare la (2.20), vediamo qualche esempio preliminare significativo.

(1) La somma dei numeri naturali da 0 a n vale $\frac{n(n+1)}{2}$, ovvero, usando il simbolo di sommatoria,

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2} \tag{2.21}$$

Per dimostrare per induzione che questa formula vale per ogni numero naturale $n \in \mathbb{N}$, verifichiamo prima che essa vale per $n = 0$: infatti, in tal caso la sommatoria contiene solo 0, mentre dall'altra si ha $\frac{0(0+1)}{2} = 0$, quindi l'uguaglianza è verificata.

Ora, supponiamo di sapere che la formula (2.21) vale per n, e dimostriamo che essa vale per $n+1$, ovvero dimostriamo che

$$\sum_{k=0}^{n+1} k = \frac{(n+1)[(n+1)+1]}{2} = \frac{(n+1)(n+2)}{2} \tag{2.22}$$

Si ha chiaramente

$$\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) \tag{2.23}$$

Ma poiché stiamo supponendo che la formula (2.21) valga per n (si chiama *ipotesi induttiva*), possiamo sostituire $\sum_{k=0}^{n} k$ con $\frac{n(n+1)}{2}$, e quindi la (2.23) si scrive

$$\sum_{k=0}^{n+1} k = \frac{n(n+1)}{2} + (n+1)$$

Ma, svolgendo i conti, il secondo membro è uguale a

$$\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+2)(n+1)}{2}$$

e quindi abbiamo dimostrato la (2.22), come volevamo.

(2) Per ogni numero naturale $n \geq 1$, si ha

$$2^{n-1} \leq n! \tag{2.24}$$

Dimostriamo anche questa formula per induzione, nella versione vista nell'Osservazione 2.26: poichè vogliamo mostrare che essa vale per ogni $n \geq 1$, iniziamo con il dimostrare che essa vale per $n = 1$: infatti, sostituendo $n = 1$ in (2.24) si trova da un lato $2^{1-1} = 2^0 = 1$ e dall'altro $1! = 1$, ovvero $1 \leq 1$, che è vera.

Ora, come prevede il metodo di induzione, supponiamo che la (2.24) sia valida per un certo n e dimostriamo che essa vale per $n+1$, ovvero

$$2^{(n+1)-1} \leq (n+1)! \tag{2.25}$$

Si ha chiaramente $2^{(n+1)-1} = 2^n = 2 \cdot 2^{n-1}$, e allora poiché stiamo supponendo che valga la $2^{n-1} \leq n!$ possiamo scrivere

$$2^{(n+1)-1} = 2 \cdot 2^{n-1} \leq 2 \cdot n! \leq (n+1) \cdot n! = (n+1)!$$

dove nell'ultima disuguaglianza abbiamo sfruttato il fatto che per ogni $n \geq 1$ si ha $2 \leq n+1$. La (2.25) è dimostrata.

Osservazione 2.27. Quando si dimostra per induzione che una certa proprietà P vale per ogni numero naturale maggiore o uguale di un numero di partenza n_0, dopo aver dimostrato che $P(n_0)$ è vera, bisogna stare attenti che l'implicazione $P(n) \Rightarrow P(n+1)$ sia valida effettivamente per ogni $n \geq n_0$.
Ad esempio, si consideri la disuguaglianza

$$2^n \geq n^2 \tag{2.26}$$

e supponiamo di voler dimostrare che essa è vera per tutti i numeri naturali. Chiaramente, tale disuguaglianza è vera per $n = 0$ in quanto si riduce a $2^0 = 1 \geq 0^2 = 0$, che è vera.
Ora, come prevede l'induzione, supponiamo che la formula sia vera per n (ipotesi induttiva) e dimostriamo che essa vale per $n+1$, ovvero che

$$2^{(n+1)} \geq (n+1)^2 \tag{2.27}$$

Usando l'ipotesi induttiva $2^n \geq n^2$, si ha

$$2^{(n+1)} = 2 \cdot 2^n \geq 2 \cdot n^2$$

e quindi per dimostrare la (2.27) basterebbe mostrare che $2n^2 \geq (n+1)^2$, ovvero $2n^2 \geq n^2 + 2n + 1$, che portando tutto a primo membro equivale alla disuguaglianza

$$n^2 - 2n - 1 \geq 0 \tag{2.28}$$

Ora, ricordiamo che una generica disuguaglianza di secondo grado $ax^2 + bx + c \geq 0$ è verificata per $x \geq x_1$ e $x \leq x_2$ se a è positivo, e per $x_1 \leq x \leq x_2$ se a è negativo, dove x_1 e x_2 sono le soluzioni di $ax^2 + bx + c = 0$.
Nel nostro caso, come si vede usando la nota formula risolutiva $x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$, si vede che $n^2 - 2n - 1 = 0$ ha come soluzioni $n = 1 - \sqrt{2}$ e $n = 1 + \sqrt{2}$, quindi la nostra disuguaglianza (2.28) è verificata per $n \geq$

$1 + \sqrt{2} \sim 2,4$ e $n \leq 1 - \sqrt{2} \sim -0,4$. Siccome stiamo lavorando nei naturali, il primo numero naturale per cui la disuguaglianza è verificata è 3: quindi l'implicazione $P(n) \Rightarrow P(n+1)$ che stiamo dimostrando è vera solo per $n \geq 3$, ovvero pur essendo $P(0)$ vera non possiamo partire da 0 per innescare il meccanismo dell'induzione. Come minimo, dobbiamo partire da 3, tuttavia, $P(3)$ non è vera: infatti, sostituendo $n = 3$ in (2.26) si ottiene $2^3 \geq 3^2$, cioè $8 \geq 9$.
Sostituendo $n = 4$ vediamo invece che $2^4 \geq 4^2$ (cioè $16 \geq 16$), ovvero $P(4)$, è vera, quindi non solo possiamo usarlo come punto di partenza dell'induzione, ma sapendo anche che per $n \geq 4$ la $P(n) \Rightarrow P(n+1)$ è vera, la formula risulta dimostrata per induzione per $n \geq 4$.

Dimostriamo finalmente la (2.20) per induzione.
Intanto, tale formula è vera per $n = 0$, in quanto da una parte $(a+b)^0 = 1$, dall'altra si ha $\sum_{k=0}^{0} \binom{0}{k} a^{0-k} b^k = \binom{0}{0} a^0 b^0 = 1$.
Supponiamo ora che la formula valga per n, ovvero

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \tag{2.29}$$

(ipotesi induttiva) e dimostriamo che vale quando sostituiamo n con $n+1$, ovvero

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k \tag{2.30}$$

Poiché $(a+b)^{n+1} = (a+b)(a+b)^n$, possiamo usare l'ipotesi induttiva e scrivere

$$(a+b)^{n+1} = (a+b) \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = a \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k + b \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k. \tag{2.31}$$

Ora, possiamo portare l'a e il b che moltiplicano rispettivamente la prima e la seconda sommatoria all'interno delle sommatorie stesse, in quanto in generale per le sommatorie vale[9] la proprietà $c \sum_{j=1}^{N} x_j = \sum_{j=1}^{N} c x_j$. Si ottiene quindi

$$\sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1}.$$

[9]Infatti, si ha $c \sum_{j=1}^{N} x_j = c(x_1 + x_2 + \cdots + x_N) = c x_1 + c x_2 + \cdots + c x_N = \sum_{j=1}^{N} c x_j$, dove abbiamo applicato la proprietà distributiva nella seconda uguaglianza.

Per motivi che saranno chiari nei passaggi successivi, separiamo ora dalla prima sommatoria il termine corrispondente a $k = 0$, cioè $\binom{n}{0}a^{n+1-0}b^0 = a^{n+1}$, e dalla seconda sommatoria il termine che corrisponde a $k = n$, cioè $\binom{n}{n}a^{n-n}b^{n+1} = b^{n+1}$:

$$a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n+1-k}b^k + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k}b^{k+1} + b^{n+1}$$

Ora usiamo un trucco spesso usato quando si ha a che fare con sommatorie: nella seconda sommatoria denotiamo $k + 1 = h$ (ovvero $k = h - 1$) e usiamo h come nuovo indice di sommatoria. Quando $k = 0$, si ha $h = 1$ e quando $k = n-1$ si ha $h = n$. Cambiati in questo modo gli estremi della sommatoria e sostituito ovunque in tale sommatoria $k = h - 1$, si ha

$$a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n+1-k}b^k + \sum_{h=1}^{n} \binom{n}{h-1} a^{n-h+1}b^h + b^{n+1}$$

A questo punto, dal momento che l'indice di una sommatoria può essere denotato in qualunque modo, ridenominiamo h come k:

$$a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n+1-k}b^k + \sum_{k=1}^{n} \binom{n}{k-1} a^{n-k+1}b^k + b^{n+1}$$

Dopo queste trasformazioni, entrambe le sommatorie centrali hanno l'indice k che varia sempre da 1 a n e in entrambe compare $a^{n-k+1}b^k$, moltiplicato nella prima per $\binom{n}{k}$ e nella seconda per $\binom{n}{k-1}$: quindi possiamo raggrupparle, usando la proprietà[10] generale delle sommatorie $\sum_{j=1}^{N} x_j + \sum_{j=1}^{N} y_j = \sum_{j=1}^{N}(x_j + y_j)$ e mettendo in evidenza $a^{n-k+1}b^k$:

$$a^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1} \right] a^{n+1-k}b^k + b^{n+1}$$

A questo punto, all'interno della parentesi quadra possiamo usare la proprietà (2.18) del coefficiente binomiale, che ci dice che $\binom{n}{k}+\binom{n}{k-1} = \binom{n+1}{k}$, ottenendo

$$a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^{n+1-k}b^k + b^{n+1}$$

[10]Infatti, $\sum_{j=1}^{N} x_j + \sum_{j=1}^{N} y_j = (x_1 + x_2 + \cdots + x_N) + (y_1 + y_2 + \cdots + y_N)$ che, usando le proprietà associativa e commutativa della somma, che ci permettono di permutare e accorpare gli addendi come vogliamo, è uguale a $(x_1 + y_1) + (x_2 + y_2) + \cdots + (x_N + y_N) = \sum_{j=1}^{N}(x_j + y_j)$.

Ora, possiamo inglobare di nuovo gli addendi a^{n+1} e b^{n+1}, che nei passaggi precedenti avevamo separato, all'interno della sommatoria centrale: infatti, $a^{n+1} = \binom{n+1}{0} a^{n+1-0}b^0$ e $b^{n+1} = \binom{n+1}{n+1} a^{n+1-(n+1)}b^{n+1}$: quindi perchè nella sommatoria siano compresi anche a^{n+1} e b^{n+1} basta aggiungere $k = 0$ e $k = n + 1$, ottenendo finalmente

$$\sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k}b^k$$

Abbiamo quindi dimostrato la (2.30) partendo dall'ipotesi che fosse vera la (2.29), quindi come afferma il principio d'induzione la formula è vera per ogni n.

Osservazione 2.28. Segnaliamo un'altra formulazione del principio di induzione, spesso usata nelle dimostrazioni. Una proprietà P risulterà dimostrata per ogni naturale n se si dimostra che

(1) la proprietà P vale per 0

(2) se la P vale per ogni $0 \leq k \leq n$, allora vale per $n + 1$

2.6 L'insieme delle permutazioni come gruppo

In questo paragrafo vogliamo considerare l'insieme delle permutazioni di $\{1, 2, \ldots, n\}$, che da ora denoteremo S_n, assieme all'operazione di composizione di funzioni, e studiarne le proprietà, non diversamente da quello che si fa quando si considera ad esempio l'insieme dei numeri naturali $\mathbb{N}$, assieme a un'operazione (ad esempio la somma o il prodotto) e se ne studiano le proprietà.

Prima di fare ciò, dobbiamo però essere sicuri che quando componiamo due permutazioni otteniamo ancora una permutazione. Non avrebbe infatti senso studiare le proprietà di questa operazione su S_n se succedesse che quando la applichiamo rischiamo di ottenere qualcosa che non sta più in S_n, allo stesso modo in cui non ha senso per esempio studiare le proprietà della sottrazione su $\mathbb{N}$ quando non sempre questa operazione si può fare in questo insieme (pur essendo 2 e 5 numeri naturali, 2-5 non è un numero naturale).

Dal momento che una permutazione per definizione è una funzione biiettiva da $X = \{1, 2, \ldots, n\}$ in sè, basta mostrare che la composizione di due funzioni biiettive è ancora biiettiva. Questo segue dal seguente risultato generale.

Lemma 2.29. Siano $f : X \to Y$ e $g : Y \to Z$ due funzioni. Allora

(1) se f e g sono iniettive, anche $g \circ f$ è iniettiva

(2) se f e g sono suriettive, anche $g \circ f$ è suriettiva

Dal lemma segue come corollario che se ho due funzioni biiettive f e g, che per definizione sono sia iniettive che suriettive, allora la loro composizione è sia iniettiva che suriettiva, e quindi biiettiva: ovvero, la composizione di funzioni biiettive è biiettiva, come volevamo.
Dimostriamo ora il Lemma 2.29.

(1) Per dimostrare che $g \circ f : X \to Z$ è iniettiva, dobbiamo mostrare che per ogni $x_1, x_2 \in X$, se $(g \circ f)(x_1) = (g \circ f)(x_2)$ allora $x_1 = x_2$.

Ma, per definizione di composizione, $(g \circ f)(x_1) = (g \circ f)(x_2)$ significa $g(f(x_1)) = g(f(x_2))$: da questa uguaglianza, siccome g è iniettiva segue che $f(x_1) = f(x_2)$, e siccome f è iniettiva a sua volta da quest'ultima segue $x_1 = x_2$, come volevamo.

(2) Per dimostrare che $g \circ f : X \to Z$ è suriettiva dobbiamo dimostrare che per ogni $z \in Z$ esiste un $x \in X$ tale che $(g \circ f)(x) = z$. Ora, dal momento che $g : Y \to Z$ è suriettiva, per ogni $z \in Z$ esiste un $y \in Y$ tale che $z = g(y)$; a sua volta, dal momento che y appartiene al codominio di $f : X \to Y$ che è anch'essa per ipotesi suriettiva, esiste un $x \in X$ tale che $y = f(x)$. Sostituendo allora $y = f(x)$ in $z = g(y)$ si ottiene $z = g(f(x))$, ovvero per definizione di composizione $z = (g \circ f)(x)$, come volevamo.

Ora che siamo sicuri che la composizione di permutazioni sia ancora una permutazione, e quindi che l'operazione di composizione sia ben definita sull'insieme S_n delle permutazioni, possiamo studiarne le proprietà.
Ad esempio, sappiamo già che la composizione di funzioni è associativa (si veda la (2.11)); sappiamo anche che in generale la composizione non è commutativa, e non è difficile mostrare un esempio di permutazioni che non commutano, ad esempio sull'insieme $\{1, 2, 3\}$ se definiamo f e g come segue

$$\begin{array}{ccc} 1 & \mapsto & 2 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & 3 \end{array}$$
$$f$$

$$\begin{array}{ccc} 1 & \mapsto & 3 \\ 2 & \mapsto & 2 \\ 3 & \mapsto & 1 \end{array}$$
$$g$$

allora si ha

$$\begin{array}{ccc} 1 & \mapsto & 2 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 1 \end{array}$$
$$g \circ f$$

mentre

$$\begin{array}{ccc} 1 & \mapsto & 3 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & 2 \end{array}$$
$$f \circ g$$

Un'altra proprietà della composizione sull'insieme S_n è che in S_n esiste un elemento neutro per tale operazione: come abbiamo visto a pagina 47, l'elemento neutro per la composizione è la funzione identica id_X, che appartiene all'insieme S_n delle permutazioni di $X = \{1, 2, \ldots, n\}$ in quanto tale funzione è chiaramente biiettiva. Per semplicità di notazione, da questo momento in poi denoteremo la funzione identica semplicemente id.

Infine, essendo ogni permutazione una funzione $f : X \to X$ biiettiva, essa, come abbiamo visto nella Proposizione 2.25, è invertibile, ovvero esiste una funzione $g : X \to X$ tale che $g \circ f = f \circ g = id$.
Chiaramente, anche la funzione g inversa di f è biiettiva, perché le uguaglianze $g \circ f = f \circ g = id$ ci dicono che anche lei è invertibile (ha f come sua inversa): quindi anche g, l'inversa di f, che da questo momento denoteremo f^{-1}, è una permutazione di X.
In altre parole S_n contiene per ogni permutazione anche la sua inversa.

Le proprietà che stiamo mettendo in evidenza rientrano in quelle elencate nella seguente, importantissima

Definizione 2.30. Sia G un insieme, sul quale è definita un'operazione (che denotiamo $\cdot$) Se valgono le tre seguenti

(i) l'operazione è associativa, ovvero per ogni $g_1, g_2, g_3 \in G$ si ha $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$

(ii) esiste un elemento neutro, ovvero esiste un $u \in G$ per cui $g \cdot u = u \cdot g = g$ per ogni $g \in G$

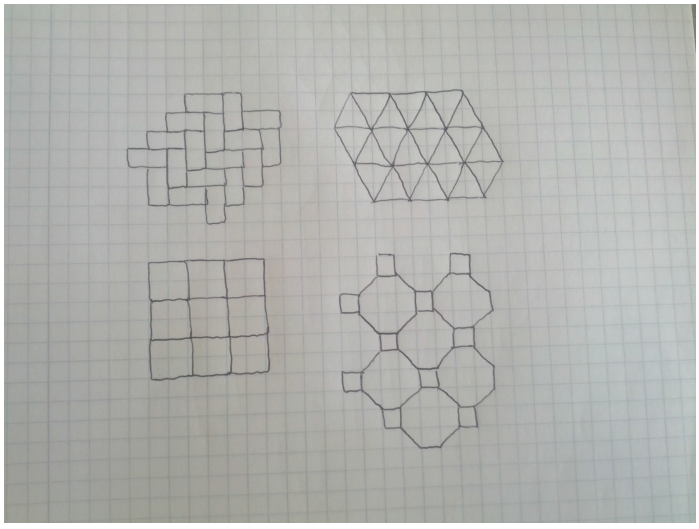
(iii) ogni $g \in G$ ha un inverso in G, ovvero esiste $g^{-1} \in G$ tale che $g \cdot g^{-1} = g^{-1} \cdot g = u$

allora G, con l'operazione $\cdot$, si dice un *gruppo* (si usa anche scrivere che $(G, \cdot)$ è un gruppo).
Se l'operazione $\cdot$ gode anche della proprietà commutativa (ovvero $g_1 \cdot g_2 = g_2 \cdot g_1$) allora $(G, \cdot)$ si dice *gruppo commutativo* (o *gruppo abeliano*).

Quindi $(S_n, \circ)$ (l'insieme delle permutazioni dotato dell'operazione di composizione) è un gruppo (non abeliano).

Esempio 2.31. Un altro esempio di gruppo, stavolta abeliano, è $(\mathbb{Z}, +)$, ovvero l'insieme degli interi dotato dell'operazione di somma: l'elemento neutro è il numero 0, e l'inverso di ogni numero intero n è semplicemente $-n$.
Invece, $(\mathbb{Z}, \cdot)$, cioè sempre l'insieme degli interi ma dotato della moltiplicazione, non è un gruppo: pur essendo valide la proprietà associativa e l'esistenza dell'elemento neutro (in questo caso il numero 1), non è vero che ogni elemento di $\mathbb{Z}$ ha un inverso rispetto alla moltiplicazione (ad esempio, l'inverso di 2 è $\frac{1}{2}$, che è un razionale non intero).

Esempi di gruppi si trovano numerosi in ogni campo della matematica e nelle sue applicazioni. Ad esempio, in geometria, data una figura nel piano l'insieme delle trasformazioni che lasciano la figura invariata mandandola in se stessa (ad esempio, dato un quadrato la rotazione di 90 gradi attorno al centro del quadrato manda il quadrato in sè) forma un gruppo, detto *gruppo di simmetria della figura*. Questa definizione si estende anche a figure non limitate, ad esempio i motivi geometrici illlimitati, spesso usati nelle decorazioni o in architettura, che ricoprono in maniera regolare il piano per ripetizione di un motivo



sono figure infinite con un loro gruppo di simmetria, e grazie alla teoria dei gruppi si può dimostrare che esistono solo 17 possibili gruppi di simmetria di tali motivi.
Infine, la nozione di gruppo si rivela fondamentale in tutta la fisica contemporanea: grazie alla teoria dei gruppi si è riusciti a prevedere l'esistenza di particelle elementari che poi sono state effettivamente osservate.

Mettiamo ora in evidenza un'altra importante differenza tra il gruppo delle permutazioni $(S_n, \circ)$ e quello degli interi $(\mathbb{Z}, +)$: in $\mathbb{Z}$ ogni elemento può essere scritto usando solo il numero 1 o il suo inverso -1 e l'operazione $+$:

$$2 = 1 + 1, 3 = 1 + 1 + 1, 4 = 1 + 1 + 1 + 1, \dots$$

$$-2 = (-1) + (-1), -3 = (-1) + (-1) + (-1), \dots$$

$$0 = 1 + (-1)$$

In questo senso, quindi, è sufficiente un elemento a *generare* tutto $\mathbb{Z}$. Questo è un caso particolare della seguente

Definizione 2.32. Dato un gruppo $(G, \cdot)$, si dice che $g_1, g_2, \dots, g_s$ *generano* G (o *sono generatori di* G) se ogni elemento di G può essere scritto come prodotto dei g_i e dei loro inversi.

Quindi 1 è un generatore di $\mathbb{Z}$, che ha la caratteristica di essere generato da un solo elemento (si dice che è *un gruppo ciclico*).
Si ha invece che il gruppo S_n non è ciclico, a meno che $n = 2$ (in questo caso, infatti, S_2 contiene solo l'identità id e la permutazione f che scambia 1 e 2, che genera id in quanto $f \circ f = id$).
Troveremo ora un insieme di generatori del gruppo S_n.

Più precisamente, chiamiamo *trasposizioni* le permutazioni di S_n che scambiano tra loro due elementi lasciando fissi tutti gli altri: ad esempio, in S_4, la permutazione

$$1 \mapsto 1$$

$$2 \mapsto 3$$

$$3 \mapsto 2$$

$$4 \mapsto 4$$

è una trasposizione (scambia tra loro 2 e 3 lasciando fissi 1 e 4).
Mostreremo ora che qualunque permutazione può essere scritta come composizione di trasposizioni: questo mostrerà che le trasposizioni generano il gruppo S_n.

Per farlo, procederemo in modo costruttivo mostrando su un esempio come effettivamente data una permutazione si può trovare la sua decomposizione in trasposizioni: consideriamo la seguente permutazione σ in S_6:

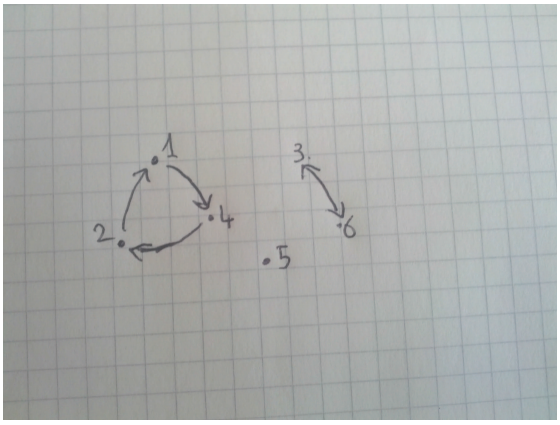
$$1 \mapsto 4$$
$$2 \mapsto 1$$
$$3 \mapsto 6$$
$$4 \mapsto 2$$
$$5 \mapsto 5$$
$$6 \mapsto 3$$

Procediamo come segue: la permutazione manda 1 in 4, 4 in 2, e 2 nuovamente in 1: questi tre elementi vengono quindi permutati tra loro in quello che si chiama un *ciclo di lunghezza 3*.
Usiamo la notazione (1 4 2) per denotare tale ciclo (ogni numero che appare nel ciclo viene mandato nel successivo, e l'ultimo viene rimandato nel primo).
Andiamo ora a vedere il primo elemento rimasto fuori da questo ciclo, cioè 3: questo viene mandato in 6, e 6 viene mandato in 3: quindi questi due elementi vengono permutati tra loro in un ciclo di lunghezza 2, che seguendo la notazione di sopra denotiamo (3 6) (si noti che un ciclo di lunghezza 2 è una trasposizione).
Infine, l'ultimo elemento che rimane fuori dai cicli trovati è 5, che viene fissato dalla permutazione, quindi non appartiene a nessun ciclo[11].
La nostra permutazione è quindi scrivibile come *composizione di cicli disgiunti*:

$$\sigma = (3\ 6)(1\ 4\ 2) \tag{2.32}$$

(spesso da questo momento per facilità di notazione ometteremo il simbolo di composizione) e agisce sugli elementi $1, 2, 3, 4, 5, 6$ come nel disegno seguente

[11] O, volendo, possiamo interpretarlo come un ciclo di lunghezza 1 e denotarlo (5), ma in generale lo si omette.



Ora, il nostro obiettivo è decomporre però ogni permutazione in trasposizioni: se riusciamo a mostrare che ogni ciclo può essere decomposto in trasposizioni avremo raggiunto lo scopo. In effetti, dato un ciclo $(a_1\ a_2\ \cdots\ a_k)$ di lunghezza k, si può dimostrare che si ha sempre

$$(a_1\ a_2\ \cdots\ a_{k-1}\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})\cdots(a_1\ a_2) \tag{2.33}$$

Non diamo una dimostrazione generale di tale fatto: limitiamoci a illustrarlo con un esempio. Il nostro ciclo (1 4 2) in base alla (2.33) si dovrebbe decomporre come (1 2)(1 4): verifichiamolo esplicitamente: ricordando che le permutazioni si applicano da destra a sinistra, si ha che (1 2)(1 4) agisce su 1,2,4 come segue:

$$\begin{array}{ccccc} 1 & \mapsto & 4 & \mapsto & 4 \\ 2 & \mapsto & 2 & \mapsto & 1 \\ 4 & \mapsto & 1 & \mapsto & 2 \\ & (1\ 4) & & (1\ 2) & \end{array}$$

cioè esattamente come il ciclo (1 4 2) che manda $1 \mapsto 4$, $4 \mapsto 2$, $2 \mapsto 1$.
In conclusione, la (2.32) può essere riscritta come

$$\sigma = (3\ 6)(1\ 2)(1\ 4)$$

e come si vede è prodotto di trasposizioni.

Quello che abbiamo mostrato è un modo per determinare la decomposizione di una permutazione in trasposizioni, tuttavia si può vedere che tale decomposizione non è in generale unica. Ad esempio, è facile verificare che la permutazione

$$\begin{array}{ccc} 1 & \mapsto & 3 \\ 2 & \mapsto & 4 \\ 3 & \mapsto & 1 \\ 4 & \mapsto & 2 \end{array}$$

si decompone sia come (1 3)(2 4) che come (1 4)(1 2)(4 3)(1 4).
Tuttavia, un importante risultato, che non dimostriamo, afferma che *il numero di trasposizioni in cui si decompone una permutazione data è o sempre pari o sempre dispari.* Alla luce di ciò, possiamo dare la seguente

Definizione 2.33. Una permutazione si dice *pari* (risp. *dispari*) se si decompone in un numero pari (risp. dispari) di trasposizioni.

Ad esempio, anche l'identità id è una permutazione pari in quanto possiamo realizzarla come prodotto di una qualunque trasposizione τ per se stessa: $\tau \circ \tau = id$ (in quanto τ scambia due elementi tra loro lasciando gli altri fissi, e riapplicando τ gli unici due elementi scambiati vengono di nuovo scambiati tornando alla situazione iniziale.), quindi due trasposizioni.

Osserviamo che se componiamo due permutazioni σ e σ' entrambe pari, il risultato sarà ancora una permutazione pari: infatti, se la prima si decompone in $2k$ trasposizioni

$$\sigma = \tau_1 \tau_2 \cdots \tau_{2k}$$

e la seconda in $2l$ trasposizioni

$$\sigma' = \tau'_1 \tau'_2 \cdots \tau'_{2l}$$

allora si ha chiaramente

$$\sigma\sigma' = \tau_1 \tau_2 \cdots \tau_{2k} \tau'_1 \tau'_2 \cdots \tau'_{2l}$$

cioè $\sigma\sigma'$ si decompone come prodotto di $2k + 2l = 2(k + l)$ trasposizioni, ed è quindi anche lei una permutazione pari.
Inoltre, se ho una permutazione σ pari, anche la sua inversa σ^{-1} sarà una permutazione pari: infatti, se $\sigma = \tau_1 \tau_2 \cdots \tau_{2k-1} \tau_{2k}$, dimostriamo che la sua inversa è

$$\sigma^{-1} = \tau_{2k} \tau_{2k-1} \cdots \tau_2 \tau_1 \tag{2.34}$$

cioè il prodotto delle stesse trasposizioni ma nell'ordine inverso (quindi sempre un numero pari).
Questo fatto è conseguenza del seguente risultato, che ci dice come calcolare l'inversa di un prodotto in un gruppo in generale:

Lemma 2.34. Sia G un gruppo e siano $g_1, g_2, \ldots, g_k \in G$. Allora

$$(g_1 g_2 \cdots g_k)^{-1} = g_k^{-1} \cdots g_2^{-1} g_1^{-1} \tag{2.35}$$

Prima di dimostrare il lemma, osserviamo che da esso segue subito la (2.34): infatti, in base al lemma si ha che l'inversa di $\tau_1 \tau_2 \cdots \tau_{2k-1} \tau_{2k}$ è $\tau_{2k}^{-1} \tau_{2k-1}^{-1} \cdots \tau_2^{-1} \tau_1^{-1}$; ma come abbiamo già osservato sopra, per qualunque trasposizione τ si ha $\tau \circ \tau = id$, che significa che τ ha come inversa se stessa, ovvero $\tau^{-1} = \tau$. Quindi $\tau_{2k}^{-1} \tau_{2k-1}^{-1} \cdots \tau_2^{-1} \tau_1^{-1} = \tau_{2k} \tau_{2k-1} \cdots \tau_2 \tau_1$, che dimostra la (2.34).

Ora dimostriamo il lemma. In base alla definizione di inversa basta vedere se moltiplicando $g_1 g_2 \cdots g_{k-1} g_k$ con $g_k^{-1} g_{k-1}^{-1} \cdots g_2^{-1} g_1^{-1}$ si ottiene l'elemento neutro:

$$(g_1 g_2 \cdots g_{k-1} g_k)(g_k^{-1} g_{k-1}^{-1} \cdots g_2^{-1} g_1^{-1}) =$$

(per associatività dell'operazione in un gruppo, possiamo disporre le parentesi come vogliamo)

$$= (g_1 g_2 \cdots g_{k-1})(g_k g_k^{-1})(g_{k-1}^{-1} \cdots g_2^{-1} g_1^{-1}) = \tag{2.36}$$

Ma la parentesi centrale $g_k g_k^{-1}$ è uguale all'elemento neutro u, quindi la (2.36) si riduce a

$$= (g_1 g_2 \cdots g_{k-1}) u (g_{k-1}^{-1} \cdots g_2^{-1} g_1^{-1}) = \tag{2.37}$$

ovvero, tenendo conto della definizione di elemento neutro,

$$= (g_1 g_2 \cdots g_{k-1})(g_{k-1}^{-1} \cdots g_2^{-1} g_1^{-1}). \tag{2.38}$$

A questo punto possiamo nello stesso modo eliminare g_{k-1}: infatti, sempre per associatività la (2.38) si scrive

$$= (g_1 g_2 \cdots)(g_{k-1} g_{k-1}^{-1})(\cdots g_2^{-1} g_1^{-1}) = \tag{2.39}$$

e come prima la parentesi centrale si elimina in quanto $g_{k-1} g_{k-1}^{-1} = u$. Continuando così, si eliminano via via tutti i fattori del prodotto, fino a che non rimane solo $g_1 g_1^{-1} = u$. La dimostrazione è conclusa[12].

Quanto detto mostra in effetti che l'insieme delle permutazioni pari in S_n, che si denota A_n, può essere considerato un gruppo a sè, in quanto quando

[12] Dovremmo verificare anche che $(g_k^{-1} g_{k-1}^{-1} \cdots g_2^{-1} g_1^{-1})(g_1 g_2 \cdots g_{k-1} g_k) = u$, ma i calcoli sono analoghi.

compongo due elementi di A_n rimango in A_n (cioè l'operazione di composizione è ben definita dentro A_n), l'elemento neutro sta dentro A_n e l'inversa di ogni elemento di A_n sta ancora dentro A_n.
Un gruppo più piccolo G' contenuto in un gruppo più grande G si dice *sottogruppo di* G (si intende che devono essere gruppi rispetto alla stessa operazione). Quindi A_n è un sottogruppo di S_n.

Notiamo che invece il sottoinsieme di S_n costituito dalle permutazioni dispari non forma un sottogruppo: basterebbe già il fatto che l'elemento neutro id (che come abbiamo osservato sopra è una permutazione pari) non sta in tale sottoinsieme, ma possiamo anche notare che il prodotto di due permutazioni dispari non è più dispari in quanto se $\sigma = \tau_1\tau_2\cdots\tau_{2k+1}$ e $\sigma' = \tau'_1\tau'_2\cdots\tau'_{2l+1}$, allora $\sigma\sigma' = \tau_1\tau_2\cdots\tau_{2k+1}\tau'_1\tau'_2\cdots\tau'_{2l+1}$ risulta essere prodotto di $(2k+1)+(2l+1) = 2(k+l+1)$ trasposizioni, cioè un numero pari.

Osservazione 2.35. Un'importante applicazione delle proprietà dei gruppi A_n e S_n in matematica è stata la dimostrazione del fatto che *non esiste una formula risolutiva generale per risolvere le equazioni di grado superiore al quarto*, ovvero nessuna formula generale che permetta di trovare le radici di un polinomio di grado $d \geq 5$: la dimostrazione, che fa parte della cosiddetta teoria di Galois, fa uso del fatto che a ogni polinomio di grado n si può associare un gruppo, opportunamente definito, che permuta le sue radici, quindi si può pensare come un sottogruppo del gruppo delle permutazioni S_n. La risolubilità dell'equazione determinata da tale polinomio corrisponde a una particolare proprietà di questi gruppi di permutazioni che, come si dimostra, S_n e A_n non hanno se $n \geq 5$.