ALGEBRA I – MODULO PROF. VERARDI

Prerequisiti[1]**:** insiemi, funzioni, relazioni d'equivalenza e d'ordine, operazioni e loro proprietà, conoscenze di base dei numeri naturali ed interi. Nozioni tratte dagli altri insegnamenti del I anno svolti in parallelo.

Contenuto:

§ 1 I numeri naturali: preistoria; sistemi di numerazione; gli assiomi di Peano, operazioni in **N**, potenze, divisori e multipli, ordinamenti, il principio del minimo. Nozione di monoide. Divisione col resto, massimo comune divisore e minimo comune multiplo, algoritmo euclideo, numeri primi e teorema fondamentale dell'aritmetica.

§ 2 I numeri interi relativi come numeri naturali col segno: ordinamento, valore assoluto e segno, operazioni; l'anello dei numeri interi. Divisibilità in **Z**: varianti rispetto ad **N**, identità di Bézout.

§ 3 Calcolo combinatorio: equipotenza, insiemi numerabili, insiemi finiti e loro numero di elementi; principio di addizione e conseguenze; principio di moltiplicazione, funzioni tra insiemi finiti, funzioni iniettive e biiettive; anagrammi; coefficienti binomiali, formula di Newton e triangolo aritmetico.

§ 4 Il gruppo simmetrico come gruppo delle unità del monoide delle funzioni da un insieme a se stesso; equipotenza di insiemi e isomorfismo dei gruppi simmetrici. Il caso finito: il gruppo S_n, rappresentazione e calcoli in S_n; permutazioni disgiunte; cicli e teorema di fattorizzazione in cicli disgiunti; ordine di una permutazione; le trasposizioni come generatori di S_n; permutazioni pari e dispari; il sottogruppo alterno; il teorema di Cayley. Il sottogruppo di Klein di S_4. Alcuni problemi di rappresentazione.

[1] Per alcuni prerequisiti sono disponibili schede da vecchi corsi di Algebra.

§ 1 – I NUMERI NATURALI

I *numeri naturali* sono entrati nella vita degli esseri umani (di Cro-Magnon) almeno 30.000 anni fa sotto forma di file (o *stringhe*) finite di *tacche*:

1 = I 2 = II 3 = III e così via.

Lo *zero* è l'assenza di tacche. E' un metodo che dal punto di vista teorico permette di capire facilmente le operazioni ed il confronto.

- L'*ordinamento* è evidente: si sovrappongono le due file di tacche e quella che "sporge" è maggiore dell'altra.
- *Addizionare* non è altro che giustapporre:

  III+IIII = IIIIIII

  e così ogni numero è somma di tanti 1 quante sono le sue tacche.
- *Sottrarre* è eliminare dal minuendo tante tacche quante sono espresse dal sottraendo, purché sia minore o uguale al minuendo:

  IIIII - II = III
- *Moltiplicare* è addizionare successivamente lo stesso numero di tacche:

  III × II = II+II+II = IIIIII
- *Dividere* è sottrarre successivamente il divisore dal dividendo, finché possibile: il *quoziente* è il numero delle sottrazioni, il *resto* è quel che rimane alla fine.

Le proprietà sono quasi immediate. In particolare, persino uno scoglio concettuale come la divisione per zero è facile: sottrarre zero tacche da un numero dato non lo cambia mai, si può proseguire all'infinito e non si ha un quoziente ed un resto, perciò non ha senso dividere per zero.

Questo metodo si pensa sia stato il primo ad essere utilizzato nella storia della rappresentazione dei numeri: infatti il più antico ritrovamento consiste in un osso di lupo, risalente proprio a 30.000 anni fa circa, con incise una successione di tacche a distanza all'incirca costante l'una dall'altra e con una tacca più lunga in corrispondenza di cinque tacche corte.

Tuttavia, questo approccio non è soddisfacente per un uso pratico: i numeri come tacche diventano presto ingestibili e le esigenze di calcolo e di

introduzione di nuovi insiemi di numeri (per misurare e non solo per contare) richiedono una razionalizzazione dei numeri naturali ed una loro diversa rappresentazione. Nascono allora, circa 4.000 anni fa i sistemi di numerazione.

Per *sistema di numerazione* si intende l'insieme dei simboli e delle regole che consentono di rappresentare graficamente i numeri e di leggerli. Un sistema di numerazione è quindi una sequenza di nomi di numeri, o numerali, utilizzata per *enumerare*, ossia per attribuire ad ogni elemento di un insieme finito un nome, che dipende dall'ordine con il quale prendiamo in considerazione tale elemento. Sin dai primi tentativi di enumerazione, l'uomo ha capito la necessità di attribuire nomi ai numeri seguendo regole e non in modo arbitrario, ed ha escogitato nel corso della storia diversi metodi di rappresentazione dei numeri attraverso la scrittura. Tali metodi si dividono in due categorie principali: i *metodi senza base* e quelli *con base*.

Del primo tipo è il metodo delle tacche, già visto, ma anche il rappresentare ogni numero con un simbolo diverso e senza nessi logici fra i simboli. Quest'ultimo metodo è sicuramente inefficiente perché privo di organicità e perché non permette le fasi di memorizzazione e trasmissione del processo del contare.

I Romani introdussero una notazione per evitare di scrivere successivamente più di 3 simboli uguali. Per fare questo furono introdotti simboli per le potenze di 10 ed altri simboli per "unità intermedie", e una notazione sottrattiva. Il suo supporto grafico è costituito da 7 lettere dell'alfabeto latino :

I = 1, V = 5, X =10, L = 50, C = 100 , D = 500 M = 1000.

Per rappresentare un numero venivano scritte le lettere in ordine decrescente dei loro valori, che venivano sommati, ma per evitare la ripetizione di 4 lettere uguali fu inventata la seguente regola: se una lettera di valore inferiore è collocata alla sinistra di una lettera di valore superiore, i due valori vanno sottratti; se è collocata alla destra i due valori vanno sommati. In questo modo otteniamo ad esempio: XL = 40 e LX = 60. L'efficienza computazionale è bassissima e la rappresentazione di numeri altri assai complicata.

Il progresso decisivo fu la notazione posizionale. Questo metodo è utilizzato da quasi tutti i popoli, facendo riferimento alla base 10 e usando attualmente i simboli 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 come cifre, combinate secondo le seguenti regole:

- i primi nove interi positivi sono rappresentati da 1, 2, 3, 4, 5, 6, 7, 8, 9
- il successivo di 9 si scrive 10
- il successivo rappresentato da n cifre si scrive nel seguente modo: se l'ultima cifra non è 9 si sostituisce questa con la sua successiva; se l'ultima cifra è 9 si sostituisce 9 con 0 e l'intero rappresentato dalle n-1 prime cifre col suo successivo.

Questo metodo ha origini indo-arabiche ed è usato non tanto per la motivazione dei simboli, quanto per la sua sistematicità e per la sua elevata efficienza computazionale. I sistemi posizionali si sono sviluppati gradualmente, in concomitanza con l'uso di "unità di ordine

superiore" (decine, centinaia, dozzine, lustri…) rese necessarie dall'espansione del sistema dei numerali verso numeri sempre più grandi.

Tuttavia, questo poter eseguire le operazioni in modo efficiente non basta. Infatti, non consente di dimostrare le proprietà delle operazioni o calcolare somme di un numero variabile di termini ottenuti con regole predeterminate (per esempio, la somma dei numeri da 0 ad n, o dei loro quadrati). Occorre allora un approccio simile a quello usato da Euclide per la geometria: una specie di gioco, in cui ci sono delle pedine con cui giocare, delle regole per incominciare a giocare e delle altre per proseguire nel gioco. Per Euclide, le pedine erano punti, rette, piani; le regole erano i postulati e la regola per proseguire era di dover usare solo i postulati e i risultati già raggiunti. Gli attrezzi per giocare sono le regole della logica accettate unanimemente.

Tra i tentativi di ricreare i numeri naturali con questo metodo si distingue quello proposto da Giuseppe Peano, un matematico torinese di fine ottocento. La sfida che ci proponiamo è vedere se questo suo approccio sia sufficiente a restituirci tutte le proprietà che le stringhe di tacche dei nostri antenati ci hanno abituato a considerare vere.

In questa sezione si richiama la definizione secondo Peano dell'insieme $\mathbf{N} = \{0, 1, 2, ...\}$ dei numeri naturali; successivamente si introducono le operazioni di addizione e moltiplicazione di $\mathbf{N}$ e le relative relazioni d'ordine e ne sono descritte le proprietà principali.

Assiomi di Peano. L'insieme $\mathbf{N}$ dei numeri naturali può essere definito mediante gli assiomi di Peano, che, con il linguaggio degli insiemi, tradurremo nel modo seguente:

I. $\mathbf{N}$ contiene un elemento, indicato con 0.

II. E' definita una funzione iniettiva $\sigma : \mathbf{N} \xrightarrow{1\text{–}1} \mathbf{N}$, la cui immagine è $\mathbf{N} \setminus \{0\}$

III. Per ogni $M \subseteq \mathbf{N}$, se $0 \in M$ e se per ogni $n \in M$ anche $\sigma(n) \in M$, allora $M = \mathbf{N}$.

In altre parole, la III postula che ogni sottoinsieme M contenente lo zero e che sia *chiuso* rispetto a σ coincide con $\mathbf{N}$.

Per ogni $n \in \mathbf{N}$, l'elemento $\sigma(n)$ è detto *successivo* di n. Dalla proprietà II segue che **N** è infinito. Si può provare inoltre che ogni insieme con queste proprietà è equipotente ad **N** e viene detto *numerabile*.

La proprietà III si chiama *principio d'induzione* e si usa in definizioni e dimostrazioni che coinvolgano una variabile $n \in \mathbf{N}$.

Le *dimostrazioni per induzione* seguono lo schema seguente: si debba provare un'affermazione P(n) che abbia senso per ogni numero naturale.

a) Si dimostra innanzitutto che è vera P(0).
b) Si dimostra che l'essere vera P(n) (*ipotesi induttiva*) implica che è vera $P(\sigma(n))$.

In tal modo l'insieme M dei numeri n per i quali P(n) è vera contiene 0 e per ogni $n \in M$ contiene anche $\sigma(n)$. Dunque, per il principio d'induzione, $M = \mathbf{N}$.

Analogamente, la proprietà III serve per definire nozioni, secondo lo schema seguente (*definizioni ricorsive*): si debba definire una nozione, che denoteremo con D(n), e che abbia senso per ogni numero naturale.

a) Si definisce esplicitamente D(0).
b) Supposta definita D(n), si definisce mediante essa $D(\sigma(n))$.

In tal modo l'insieme M dei numeri n per i quali D(n) è definita contiene 0 e per ogni $n \in M$ contiene anche $\sigma(n)$. Dunque, per il principio d'induzione, $M = \mathbf{N}$.

A volte si parte da un numero n_0 anziché da 0. In tal caso, l'affermazione P(n) sarà provata solo per ogni $n \geq n_0$. Analogamente per le definizioni D(n).

Osservazione. In alcuni casi, per dimostrare un'affermazione P(n) si segue uno schema un po' diverso, detto *II principio d'induzione*:

a) si dimostra P(0)
b) supposto vero P(k) per ogni $k \leq n$, si dimostra $P(\sigma(n))$.

Esempi di dimostrazioni per induzione e di definizioni ricorsive si troveranno nel seguito. Incominciamo con il definire le operazioni.

Addizione. Su **N** si può definire ricorsivamente la *somma* di un numero m con un numero n qualsiasi, nel modo seguente:

$$\begin{cases} m+0=m \\ m+\sigma(n)=\sigma(m+n) \end{cases}$$

In tal modo, per la proprietà III, per ogni m∈**N** la *somma* m+n è definita per ogni n∈**N**. Posto 1 = σ(0), si ottiene subito, per ogni m∈**N**:

$$\sigma(m) = \sigma(m+0) = m+\sigma(0) = m+1.$$

Chiamiamo *addizione* l'operazione $+ : \mathbf{N}^2 \to \mathbf{N}$, $+ : (m,n) \mapsto m+n$, che associa a una coppia ordinata (m, n) di numeri naturali la loro somma.

PROPOSIZIONE 1.1. - L'addizione possiede le proprietà seguenti:

a) *associativa*: per ogni a, b, c∈**N** risulta: (a+b)+c = a+(b+c);

b) *elemento neutro*: per ogni a∈**N** si ha a+0 = 0+a = a;

c) *commutativa*: per ogni a, b∈**N** risulta a+b = b+a.

Dimostrazione. a) L'uguaglianza è vera per c = 0, risultando (a+b)+0 = a+b = a+(b+0).

Supponendola provata per c = n (ipotesi induttiva), dimostriamo che è vera per c = σ(n) nel modo seguente:

(a+b)+c = (a+b)+ σ(n) =

(per la definizione di +) = σ((a+b)+n) =

(per l'ipotesi induttiva) = σ(a+(b+n)) =

(per la definizione di +) = a+σ(b+n) =

(ancora per la definizione di +) = a+(b+σ(n)) = a+(b+c),

come si voleva.

b) Per definizione di + si ha a+0 = a. L'uguaglianza 0+a = a è vera ovviamente per a = 0. Supponendola provata per a = n, se a = σ(n) si ha:

$$0+a = 0+\sigma(n) = \sigma(0+n) = \sigma(n) = a.$$

c) La dimostrazione della proprietà commutativa è più complessa, perché occorre procedere per induzione rispetto ad entrambi gli addendi. Per b) la proprietà è vera se a = 0. Sia vera per a = n e dimostriamo che è vera per a = σ(n). Per questo procediamo per induzione rispetto a b.

E' vera per definizione di + se b = 0. Sia vera per b = m. Per b = σ(m) si ha allora:

$$a+b = \sigma(n)+ \sigma(m) = \sigma(\sigma(n)+m) =$$

(per l'ipotesi induttiva su b) $= \sigma(m+\sigma(n)) = \sigma(\sigma(m+n)) =$

(per l'ipotesi induttiva su a) $= \sigma(\sigma(n+m)) = \sigma(n+\sigma(m)) =$

(ancora per l'ipotesi induttiva su a) $= \sigma(\sigma(m)+n) = \sigma(m)+ \sigma(n) = b+a,$

così come si voleva.

Col linguaggio dell'algebra possiamo concludere che la terna (**N**, +, 0) risulta un *monoide* commutativo. Esso possiede inoltre le seguenti proprietà:

PROPOSIZIONE 1.2. - Ulteriori proprietà dell'addizione.

a) Per ogni a, b∈**N**, se a+b = 0 allora a = b = 0.

b) *Legge di cancellazione*: per ogni a, b, c∈**N**, se a+b = a+c allora b = c.

c) Per ogni a, b∈**N**, una e, se a ≠ b, una sola delle due equazioni: $\begin{cases} a + x = b \\ b + y = a \end{cases}$, nelle incognite x, y∈**N**, ha soluzione, ed in tal caso ne ha una sola.

Dimostrazione. Sia a ≠ 0. Per induzione su b proviamo che a+b ≠ 0. Innanzi tutto, a+0 = a ≠ 0. Sia a+b ≠ 0. Allora a+σ(b) = σ(a+b) ≠ 0 perché 0∉σ(**N**).

Pertanto, può essere a+b = 0 solo se a = 0, ma allora b = 0+b = 0 implica b = 0.

b) Sia a+b = a+c. Se a = 0 si ha b = c. Sia vero per a = n. Allora, per a = σ(n) si ha: a+b = σ(n)+b = σ(n+b), e analogamente a+c = σ(n+c). Perciò, da a+b = a+c segue σ(n+b) = σ(n+c), da cui, per la iniettività di σ, si ha n+b = n+c. Per l'ipotesi induttiva segue allora b = c.

c) Per induzione rispetto a b proviamo che una delle due equazioni ha soluzione. Se b = 0 allora si ha y = a. Sia vero per b = n. Sia ora b = n+1. Se si aveva a+x = n, allora a+(x+1) = n+1 = b. Invece nel caso n+y = a, se y = 0 si ha anche a+0 = a, per cui siamo nel caso precedente; se y ≠ 0, allora y appartiene all'immagine di σ e quindi esiste z tale che z+1 = σ(z) = y.

Allora b+z = (n+1)+z = n+(1+z) = n+y = a.

Se risulta contemporaneamente a+x = b e b+y = a, per la proprietà associativa si ha: b+0 = b = a+x = (b+y)+x = b+(y+z), quindi per la legge di cancellazione si ha y+z = 0, ma per a) si ha y = z = 0 e quindi b = a. La soluzione è unica per la legge di cancellazione.

Sottrazione. Se risulta a+d = b, si pone b-a = d e d si chiama *differenza* di b ed a. In particolare si ha a-a = 0.

Moltiplicazione. Si definisce ricorsivamente l'operazione di *moltiplicazione* · definendo dapprima il *prodotto* di un m per un n qualsiasi, nel modo seguente (ricordando che σ(n) = n+1):

$$\text{per ogni m, n}\in\mathbf{N},\ \begin{cases} m\cdot 0 = 0 \\ m\cdot(n+1) = m\cdot n + m \end{cases}.$$

Di conseguenza, per esempio, m·1 = m·(0+1) = m·0+m = m, ecc. Solitamente il *prodotto* di m per n si denota con mn, anziché con m·n. La moltiplicazione è l'operazione che ad ogni coppia (m,n) associa il prodotto m·n

PROPOSIZIONE 1.3. - Proprietà della moltiplicazione.

1) *Elemento assorbente*: per ogni a∈**N**, 0·a = a·0 = 0
2) *Elemento neutro*: per ogni a∈**N** si ha a·1 = 1·a = a.
3) *Distributiva* rispetto al +: per ogni a, b, c∈**N** risulta $\begin{cases}(a+b)c = ac+bc \\ a(b+c) = ab+ac\end{cases}$
4) *Associativa*: per ogni a, b, c∈**N** risulta (ab)c = a(bc)
5) *Commutativa*: per ogni a, b∈**N** risulta ab = ba.

Dimostrazione. 1) Basta provare che si ha 0·a = 0. E' vera per a = 0. Sia vera per a, allora $0\cdot\sigma(a) = 0\cdot a + 0 = 0+0 = 0$, quindi è vero anche per $\sigma(a)$.

2) $a\cdot 1 = a\cdot\sigma(0) = a\cdot 0 + a = 0 + a = a$. Invece, $1\cdot 0 = 0$ e, supposto 1·a = a, allora si ha $1\cdot\sigma(a) = 1\cdot a + 1 = a + 1 = \sigma(a)$ e anche la 2) è dimostrata.

3) Vediamo la prima uguaglianza, ossia la *distributività a sinistra*. Se c = 0 entrambi i membri sono nulli, quindi per c = 0 l'uguaglianza è vera. Sia c un numero per il quale l'uguaglianza è vera. Allora, usando la definizione di prodotto, l'ipotesi su c e le proprietà della somma, si ha:

$$(a+b)\cdot\sigma(c) = (a+b)\cdot c + (a+b) = a\cdot c + b\cdot c + a + b =$$
$$= (a\cdot c + a) + (b\cdot c + b) = a\cdot\sigma(c) + b\cdot\sigma(c)$$

Vediamo la *distributività a destra*. Se a = 0 è vera. Sia vera per un a∈**N**; allora, usando questa informazione, la proprietà di 1 e la prima uguaglianza, si ha:

$$\sigma(a)\cdot(b+c) = (a+1)\cdot(b+c) = a\cdot(b+c)+(b+c) = ab+ac+b+c =$$

$$= (a\cdot b+1\cdot b)+(a\cdot c+1\cdot c) = (a+1)\cdot b+(a+1)\cdot c = \sigma(a)\cdot b+\sigma(a)\cdot c$$

4) Per induzione su c: se c = 0 è vero. Sia c un numero per il quale si ha (ab)c = a(bc). Allora, per la proprietà distributiva e l'ipotesi induttiva si ha:

$$(ab)\cdot\sigma(c) = (ab)\cdot c+ab = a\cdot(bc)+ab = a\cdot(bc+b) = a\cdot(b\cdot\sigma(c))$$

Quindi è vero anche per $\sigma(c)$.

5) E' vero se b = 0. Sia b tale che ab = ba. Allora:

$$a\cdot\sigma(b) = a\cdot b+a = b\cdot a+1\cdot a = (b+1)\cdot a = \sigma(b)\cdot a$$

Pertanto anche la terna (**N**, ·, 1) risulta un monoide commutativo. Esso possiede inoltre le seguenti proprietà:

PROPOSIZIONE 1.4. - Ulteriori proprietà della moltiplicazione.

a) L'unico elemento dotato di *inverso* è 1, cioè per ogni a, b∈**N**, se ab = 1 allora a = b = 1.

b) *Legge di annullamento del prodotto*: per ogni a, b∈**N** si ha ab = 0 se e solo se a = 0 oppure b = 0.

Si osservi che nel monoide (**N**, ·, 1) la *legge di cancellazione* non vale, a causa della presenza dello 0; infatti per ogni a, b si ha a·0 = b·0 = 0. Pertanto da a·0 = b·0 non segue necessariamente a = b.

Consideriamo però il sottoinsieme $\mathbf{N}^+ = \mathbf{N}\setminus\{0\}$: la legge di annullamento del prodotto ha come conseguenza che se a, b∈$\mathbf{N}^+$ anche a·b∈$\mathbf{N}^+$. Poiché inoltre 1∈$\mathbf{N}^+$, possiamo considerare il *sottomonoide* ($\mathbf{N}^+$, ·, 1). Allora:

PROPOSIZIONE 1.5. - Proprietà del monoide ($\mathbf{N}^+$, ·, 1).

a) *Legge di cancellazione*: per ogni a, b, c∈$\mathbf{N}^+$, se ab = ac allora b = c.

b) Per ogni a, b∈$\mathbf{N}^+$ al massimo una delle due equazioni $\begin{cases} a \cdot x = b \\ b \cdot y = a \end{cases}$, nelle incognite x ed y∈$\mathbf{N}^+$, ha soluzione. Tale soluzione, se esiste, è unica (per la legge di cancellazione).

A differenza dell'analoga proprietà dell'addizione, la proprietà 1.5.b della moltiplicazione non contiene l'affermazione dell'esistenza, ma solo dell'unicità dell'eventuale soluzione.

Divisione. Dati a, b∈$\mathbf{N}^+$, se risulta aq = b allora q si dice *quoziente* di "b diviso a" e si pone b:a = q. In particolare, b:b = 1.

Osservazione. Poiché per ogni a ≠ 0 risulta a·0 = 0, si può definire il quoziente di 0 diviso a, ponendo 0:a = 0. Non hanno senso invece le scritture 0:0 ed a:0 in quanto per ogni q∈**N** si ha 0·q = 0.

L'ordine naturale. L'ordine naturale di **N** si può definire a partire dall'addizione, ponendo per ogni a, b∈**N**,

$$a \le b \text{ se esiste } d \in \mathbf{N} \text{ tale che } a+d = b.$$

PROPOSIZIONE 1.6. - Proprietà della relazione ≤:

a) *Proprietà riflessiva*: per ogni a∈**N** si ha a ≤ a.

b) *Proprietà antisimmetrica*: per ogni a,b∈**N**, se a ≤ b e b ≤ a allora a = b.

c) *Proprietà transitiva:* per ogni a, b, c∈**N**, se a ≤ b e b ≤ c allora a ≤ c.

d) *Dicotomia*: per ogni a, b∈**N** si ha ≤ b oppure b ≤ a.

Dimostrazione. a) Per ogni a∈**N** si ha: a+0 = a, quindi a ≤ a.

b) Se a+m = b e b+n = a allora a+(m+n) = a, ed essendo a = a+0, per la legge di cancellazione si ha m+n = 0, da cui segue m = n = 0 e a = b.

c) Da a+m = b, b+n = c segue a+(m+n) = c.

d) Basta applicare la proprietà 1.2.c.

Le prime tre proprietà hanno come conseguenza che (**N**, ≤) è un *insieme ordinato* e la quarta che l'ordine è *totale*. Inoltre, poiché per ogni n∈**N** si ha 0+n = n allora 0 ≤ n. Dunque 0 è il *minimo*. Non c'è invece *massimo*, poiché per

ogni $n \in \mathbf{N}$ si ha $n < n+1$. Inoltre:

PROPOSIZIONE 1.7. - Relazioni tra operazioni ed ordine.

a) Per ogni a, b, $c \in \mathbf{N}$, si ha $a \leq b$ se e solo se $a+c \leq b+c$.

b) Per ogni $n \in \mathbf{N}$, se $n \leq x \leq n+1$ allora $x = n$ oppure $x = n+1$.

Dimostrazione. a) Da $a+m = b$ segue $(a+c)+m = (b+c)$ e viceversa.

b) Se $n < x$ allora $x = n+m$, con $1 \leq m$, quindi $n+1 \leq n+m = x \leq n+1 \Rightarrow x = n+1$.

Sia H un sottoinsieme di **N**. Un elemento $x \in \mathbf{N}$ si dice *minorante* di H se per ogni $h \in H$ si ha $x \leq h$. Si dice *minorante stretto* se per ogni $h \in H$ si ha $x < h$. Un elemento $y \in \mathbf{N}$ si dice *maggiorante* di H se per ogni $h \in H$ si ha $y \geq h$.

PROPOSIZIONE 1.8 a) **(Principio del minimo). -** Ogni sottoinsieme non vuoto H di **N** possiede il minimo.

b) Ogni sottoinsieme non vuoto H che abbia maggioranti ha il massimo.

Dimostrazione. a) Se $0 \in H$ allora 0 è il suo minimo. Sia $0 \notin H$ e sia M(H) l'insieme dei minoranti stretti di H. Innanzitutto, $H \cap M(H) = \varnothing$. Inoltre, $0 \in M(H)$. Se per ogni $x \in M(H)$ si avesse anche $x+1 \in M(H)$ allora, per il principio d'induzione, $M(H) = \mathbf{N}$ ed $H = H \cap \mathbf{N} = H \cap M(H) = \varnothing$, assurdo. Dunque, esiste $x_0 \in M(H)$ tale che $x_0+1 \in H$. Ne segue che x_0+1 è il minimo cercato: infatti ogni altro $h \in H$ è maggiore di x_0, quindi per 1.7.b) è anche $h \geq x_0+1$.

b) Poiché l'insieme dei maggioranti di H non è vuoto, ha il minimo m. Allora ogni elemento minore di m è minore di qualche elemento di H; in particolare, $m-1$ è minore di almeno un elemento di H, ossia $m \in H$ e m è il massimo di H.

L'ordine dalla divisibilità. Eseguiamo una 'traduzione' in notazione moltiplicativa delle nozioni precedenti, per introdurre un ordine in $\mathbf{N}^+$. Definiamo la relazione $|$ (*divide*) in $\mathbf{N}^+$ ponendo:

per ogni a, $b \in \mathbf{N}^+$, $a \mid b$ se esiste $q \in \mathbf{N}^+$ tale che $aq = b$.

Sostituendo $\leq$ con $|$ e 0 con 1 nella proposizione 1.6, mediante le proprietà della moltiplicazione si provano subito le seguenti proprietà:

PROPOSIZIONE 1.9. - Proprietà della relazione |:

a) *Proprietà riflessiva*: per ogni $a \in \mathbf{N}^+$ si ha $a \mid a$.

b) *Proprietà antisimmetrica*: per ogni $a,b \in \mathbf{N}^+$, se $a \mid b$ e $b \mid a$ allora $a = b$.

c) *Proprietà transitiva:* per ogni $a, b, c \in \mathbf{N}^+$, se $a \mid b$ e $b \mid c$ allora $a \mid c$.

Non vale invece la dicotomia: per esempio 2, successivo di 1, non divide il suo successivo 3 e 3 non divide 2, come si può verificare. Queste proprietà ci dicono che $(\mathbf{N}^+, |)$ è un insieme *parzialmente ordinato*. Inoltre, poiché per ogni $n \in \mathbf{N}^+$ si ha $1 \cdot n = n$ allora $1 \mid n$. Dunque 1 è il minimo. Non c'è invece massimo, poiché per ogni $n \in \mathbf{N}^+$ si ha per esempio $n \mid 2n$. L'ordinamento | di $\mathbf{N}^+$ è legato all'ordinamento $\leq$ dalla relazione seguente:

PROPOSIZIONE 1.10. - Per ogni $a, b \in \mathbf{N}^+$, se $a \mid b$ allora $a \leq b$. Inversamente, se $a < b$ allora b non divide a.

Dimostrazione. Sia $b = aq$ e procediamo per induzione rispetto a q. Se $b = a \cdot 1$ allora $a = b$, quindi $a \leq b$. Supponiamo vero il teorema per $q = n$ (ipotesi induttiva) e proviamolo per $q = n+1$. Sia $b = a(n+1) = an+a$: per ipotesi induttiva e per la proposizione 1.7 si ha:

$$a \leq an = an + 0 \leq an+a = b,$$

da cui segue $a \leq b$. Inversamente, se $a < b$ e se fosse $b \mid a$ allora $b \leq a$, assurdo.

Osservazione. Volendo estendere l'ordinamento | a tutto $\mathbf{N}$, si deve porre necessariamente $n \mid 0$ per ogni $n \in \mathbf{N}$, in particolare, $0 \mid 0$. Infatti per ogni $n \in \mathbf{N}$ esiste almeno un elemento $q \in \mathbf{N}$, tale che $nq = 0$: ovviamente, è $q = 0$ (e non è richiesta l'unicità di q). Pertanto $(\mathbf{N}, |)$ oltre al minimo, uguale ad 1, possiede anche il massimo, lo zero. Pertanto, se $a \mid b$ e $b < a$ allora $b = 0$.

Potenze. Nel monoide $(\mathbf{N}^+, \cdot, 1)$ per ogni $a \in \mathbf{N}^+$ e per ogni $n \in \mathbf{N}$ si definisce ricorsivamente la *potenza* a^n nel modo seguente:

$$\begin{cases} a^0 = 1 \\ a^{n+1} = a^n \cdot a \end{cases}.$$

In particolare si ha $a^1 = a$. Per le potenze valgono le seguenti proprietà, che si dimostrano per induzione rispetto ad n:

PROPOSIZIONE 1.11. - Per ogni $a, b \in \mathbf{N}^*$ e per ogni $m, n \in \mathbf{N}$ si ha:

a) $a^m \cdot a^n = a^{m+n}$

b) $(a^m)^n = a^{mn}$

c) $(ab)^n = a^n b^n$

Osservazione. Mentre le prime proprietà dipendono solo dalla definizione di potenza e dalla proprietà associativa della moltiplicazione, la terza dipende in modo essenziale dalla proprietà commutativa: $(ab)^2 = abab = aabb = a^2b^2$.

Quanto sopra detto per le potenze si può ripetere per il monoide $(\mathbf{N}, +, 0)$. Osserviamo che, in notazione additiva, la potenza di base a ed esponente n si scrive *na* anziché a^n, e si ha:

$$\begin{cases} 0a = 0 \\ (n+1)a = na + a \end{cases}.$$

Il numero *na* si chiama *multiplo naturale* di a.

PROPOSIZIONE 1.12. - Altre proprietà di multipli e potenze.

a) Per ogni $n, h, k \in \mathbf{N}$, $n \neq 0$, si ha $h < k$ se e solo se $hn < kn$. In particolare, l'unico multiplo di n che sia minore di n è lo zero.

b) Per ogni $n, h, k \in \mathbf{N}^+$, $n \neq 1$, si ha $h < k$ se e solo se $n^h < n^k$ (o equivalentemente se e solo se n^h divide "propriamente" n^k). In particolare, l'unica potenza di n che sia minore di n (cioè divisore proprio di n) è 1.

Concludiamo questa sezione con la *divisione euclidea*, che si impara nella scuola elementare ed è di solito “la più difficile” tra le operazioni.

PROPOSIZIONE 1.13. Divisione col resto in N. Dati due numeri naturali a, b, con $b \neq 0$, esistono due numeri naturali q, r, univocamente determinati, tali che $\begin{cases} a = b \cdot q + r \\ 0 \leq r < b \end{cases}$.

Dimostrazione: se $a < b$ allora $q = 0$ ed $r = a$. Se $a \geq b$ sia $M = \{a - b \cdot k \mid k \in \mathbf{N}\}$: non è vuoto perché $a \in M$, perciò ha minimo $r \geq 0$. Allora esiste q tale che $r = a - b \cdot q$, e si ha $r < b$, altrimenti $s = r-b = a-(q+1) \cdot b \in M$ e $s < r$, assurdo. Se poi si ha anche $a = b \cdot q' + r'$, con per esempio $r' < r$, allora:

$$b \cdot q + r = b \cdot q' + r' \Rightarrow r - r' = b \cdot (q' - q), \text{ con } q'\text{-}q \geq 1.$$

Ma si ha contemporaneamente $r - r' < r < b \leq b \cdot (q' - q)$, assurdo. Dunque si ha l'unicità di q ed r.

Nota. Per le definizioni ricorsive, a volte accade che esista un $h > 0$ tale che D(n+h) dipenda da D(n), ..., D(n+h-1). In tal caso occorre definire esplicitamente D(0), D(1), ..., D(h-1) (*condizioni iniziali*). Un esempio è dato dai *numeri di Fibonacci*:

$$\begin{cases} a_0 = 1 \\ a_1 = 1 \\ a_{n+2} = a_n + a_{n+1} \end{cases} \Rightarrow \begin{array}{c|cccccccc} n & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline a_n & 1 & 1 & 2 & 3 & 5 & 8 & 13 & 21 \end{array} \ldots$$

Vediamo ora la teoria della divisibilità, ossia le nozioni di massimo comune divisore, minimo comune multiplo, numeri primi, scomposizione in fattori primi: si tratta di concetti noti fin dalla scuola media inferiore, ma sono qui ripresi per presentare le dimostrazioni delle proprietà che conosciamo e vederne delle altre.

Sia $a \in \mathbf{N}^+$. Denotiamo con $D(a)$ l'insieme dei suoi divisori.Si ha $D(1) = 1$, mentre se $a > 1$, $D(a)$ contiene almeno 1 ed a; se $D(a) = \{1, a\}$ allora a si dice primo. Per esempio, sono primi 2 e 3, ma non $4 = 3+1 = 2+2 = 2 \cdot 2$. In ogni caso i divisori di a sono tutti $\leq a$. Sia ora $b \in \mathbf{N}^+$ e consideriamo $D(a) \cap D(b)$: non è vuoto, perché contiene 1, ed è limitato superiormente da a, quindi ha il massimo. Tale

massimo d si chiama massimo comune divisore di a e b, ed è denotato con $d = MCD(a, b)$ o anche solo con $d = (a, b)$.

Analogamente, l'insieme dei multipli comuni ad a e b non è vuoto, perché contiene a·b, quindi ha il minimo, $m = mcm(a, b)$, detto minimo comune multiplo di a e b.

Come trovarli? Non è facile trovare tutti i divisori di a e verificare quali siano anche divisori di b. Eppure esiste un procedimento, che un tempo si insegnava anche nella scuola media, ma che ora è quasi sempre trascurato.

Si noti che se b | a allora MCD(a,b) = b, mcm(a,b) = a.

Il *procedimento euclideo delle divisioni successive* si basa sul lemma seguente:

LEMMA 1.14. Per ogni a, b∈**N**, b ≠ 0, posto a = b·q + r, 0 ≤ r < b, si ha:

a) $D(a) \cap D(b) = D(r) \cap D(b)$.

b) MCD(a, b) = MCD(b, r)

Dimostrazione: a) sia $c \in D(a) \cap D(b)$: allora esistono a', q' tali che $a = c \cdot a'$, $b = c \cdot b'$. Allora $r = a - b \cdot q = c \cdot (a' - b' \cdot q)$, quindi $c \in D(r), \Rightarrow c \in D(r) \cap D(b)$. Il viceversa è analogo.

b) segue da a).

Ne segue il seguente *algoritmo euclideo delle divisioni successive*: supposto a ≥ b e posto d = MCD(a, b),

$a = b \cdot q_1 + r_1$,	$0 \le r_1 < b$:	se $r_1 = 0$ allora $d = b$
$b = r_1 \cdot q_2 + r_2$,	$0 \le r_2 < r_1$:	se $r_2 = 0$ allora $d = r_1$
$r_1 = r_2 \cdot q_3 + r_3$,	$0 \le r_3 < r_2$:	se $r_3 = 0$ allora $d = r_2$
.....	.....	.....

Il procedimento termina dopo un numero finito di passi, poiché i resti decrescono ad ogni passo. L'ultimo resto non nullo r_n è il MCD(a,b) cercato.

Esempio: $18 = 12 \cdot 1 + 6$; $12 = 6 \cdot 2 + 0 \Rightarrow MCD(18, 12) = 6$

Osserviamo che $r_{n-1} = r_n \cdot q_{n+1} = d \cdot q_{n+1} \Rightarrow D(d) = D(r_n) = D(r_n) \cap D(r_{n-1})$. Per il lemma 1.14, si ha allora:

$$D(d) = D(r_n) = D(r_n) \cap D(r_{n-1}) = \ldots = D(r) \cap D(b) = D(a) \cap D(b)$$

Ossia, ogni divisore comune di a e b è anche divisore di d. Questo consente una diversa definizione di MCD(a,b), più "intrinseca" ed esportabile anche agli interi o a strutture non ordinate totalmente, come i polinomi:

Siano a, b∈**N**. Un elemento d∈ **N** si dice *massimo comune divisore* di a e b se:

i. è un divisore di a e di b (*divisore comune*)
ii. è multiplo di ogni altro divisore comune (*massimo)*

In modo analogo, è immediato dimostrare che il minimo comune multiplo m di a e b divide ogni altro divisore comune s: dividendo s per m si ha $s = m \cdot q + r,\ 0 \le r < m$. Poiché $D(s) \cap D(m) = D(m) \cap D(r)$, allora r è a sua volta multiplo di a e b, quindi, per la minimalità di m, deve essere r = 0 e m |s.
Pertanto, si può definire il mcm anche così:

Un elemento m∈X si dice *minimo comune multiplo* di a e b se:

i. è un multiplo di a e di b (*multiplo comune*)
ii. è divisore di ogni altro multiplo comune (*minimo)*

Per trovare mcm(a, b) si può usare la relazione: MCD(a,b)·mcm(a,b) = a·b.

Abbiamo visto che un numero p > 1 si dice primo se D(p) = {1, p}. La più antica testimonianza della loro presenza nella cultura umana è su un osso di babuino di circa 7.000 anni fa, su cui sono incise prima 11 tacche, poi 13, poi 17, poi 19, ossia i numeri primi fra 10 e 20.

Euclide caratterizzò i numeri primi p nel modo seguente: se p divide a·b, divide almeno uno dei fattori. Ossia:

LEMMA 1.15. Un numero $p > 1$ è primo se e solo se per ogni a, b$\in \mathbf{N}^+$, $p \in D(a \cdot b) \Leftrightarrow p \in D(a) \cup D(b)$.

Dimostrazione. Sia $d = MCD(a \cdot b, b \cdot p)$. Allora b e p dividono d. Sia $d = b \cdot u$. Allora esiste s tale che $b \cdot p = d \cdot s = b \cdot (u \cdot s)$. Essendo $b \neq 0$, si può semplificare, e così si ottiene $p = u \cdot s$. Poiché p è primo, allora $\begin{cases} u = 1 \\ s = p \end{cases}$ oppure $\begin{cases} u = p \\ s = 1 \end{cases}$. Nel primo caso, p divide $d = b$; nel secondo, $d = b \cdot p$ divide $a \cdot b$, quindi esiste r tale che $a \cdot b = d \cdot r = b \cdot p \cdot r$. Dividiamo per b ed otteniamo $a = p \cdot r$, ossia $p \mid a$.
Viceversa, valga per p la proprietà euclidea. Allora se $p = h \cdot k$, p divide il prodotto $h \cdot k$, quindi $p \mid h$ oppure $p \mid k$. Ma h e k dividono p, quindi nel primo caso, $h = p$ e $k = 1$; nel secondo, $h = 1$ e $k = p$. Perciò $D(p) = \{1, p\}$.

Che ruolo hanno i numeri primi? Sono i *generatori* del monoide $(\mathbf{N}^+, \cdot, 1)$, ossia:

TEOREMA 1.16 (Teorema fondamentale dell'aritmetica). Ogni $n \in \mathbf{N}^+$ o è 1 o è primo o si può scrivere in uno ed un solo modo come prodotto di fattori primi, a parte l'ordine dei fattori stessi.
Dimostrazione. Per assurdo supponiamo falso il teorema. Allora l'insieme dei controesempi non è vuoto e perciò ha il minimo, che chiameremo m: non è 1, perché per 1 il teorema vale; non è primo perché per i primi il teorema vale, perciò è prodotto di due numeri r, s minori di m e quindi maggiori di 1. Ma essendo questi numeri minori di m, per essi il teorema vale, ossia sono primi o prodotto di primi; ne segue che anche m è prodotto di primi. Dato che m è un controesempio, ed ha la fattorizzazione, non ha l'unicità: si può scrivere cioè $m = p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s$, con i p_i, q_j primi. Allora p_r divide il prodotto $q_1 \cdot q_2 \cdot \ldots \cdot q_s$, quindi divide uno dei fattori, che a meno di riordini possiamo supporre sia q_s. Anche quest'ultimo è primo, quindi ha per divisori solo 1 e se stesso. Dato che $p_r > 1$, si ha $q_s = p_r$. Ma allora si possono semplificare, e rimane: $m' = p_1 \cdot p_2 \cdot \ldots \cdot p_{r-1} = q_1 \cdot q_2 \cdot \ldots \cdot q_{s-1} < m$. Allora per m' il teorema vale, quindi r-1 = s-1 e anche per ogni i, $1 \leq i \leq r-1$, a meno di riordini, si ha $p_i = q_i$. Ma allora anche per m il teorema vale, contro l'ipotesi che m fosse un

controesempio. Perciò m non esiste, ed il teorema è vero per ogni numero naturale ≥ 1.

Quanti sono i numeri primi? Ci sono tante domande sui primi senza risposta, ma almeno questa l'ha trovata Euclide:

TEOREMA 1.17. (Euclide) Esistono infiniti numeri primi

Dimostrazione. Dimostriamo che ogni insieme finito P di primi non li contiene tutti. Basta considerare il loro prodotto m e sommargli 1: m+1 o è primo, e allora abbiamo trovato un primo fuori di P, oppure è prodotto di primi. Sia p uno di essi: se p appartenesse a P allora dividerebbe sia m sia m+1, e quindi dividerebbe 1 = (m+1)-m, assurdo. Perciò p non appartiene a P e in P in ogni caso non ci sono tutti i numeri primi.

Sia Π l'insieme dei primi. Per ogni $a \in \mathbf{N}^+$, accorpando con l'uso delle potenze i fattori primi uguali e ponendo = 0 gli esponenti dei primi mancanti nella sua scomposizione, possiamo rappresentare a nella forma:

$$a = \prod_{p \in \Pi} p^{\alpha_p}$$

dove gli esponenti sono nulli per tutti i primi p tranne un numero finito.

Ciò posto, se $b = \prod_{p \in \Pi} p^{\beta_p}$, si ha:

$$b \mid a \text{ se e solo se per ogni } p \in \Pi,\ \beta_p \leq \alpha_p.$$

Questa proprietà è nota come "criterio generale di divisibilità", e dipende dalle proprietà delle potenze: posto $\theta_p = \alpha_p - \beta_p$ e $q = \prod_{p \in \Pi} p^{\theta_p}$, segue $a = b \cdot q$. Il viceversa è parimenti immediato.

Ne segue la regola che usualmente si insegna nella scuola secondaria: per ogni a, b non nulli, scritti come sopra, si ha:

$$\mathrm{MCD}(a,b) = \prod_{p\in\Pi} p^{\min\{\alpha_p,\beta_p\}},\ \mathrm{mcm}(a,b) = \prod_{p\in\Pi} p^{\max\{\alpha_p,\beta_p\}}.$$

Esempio: $12 = 2^2\cdot 3 = 2^2\cdot 3^1\cdot 5^0\cdot 7^0\cdot \ldots$, $18 = 3^2\cdot 2 = 2^1\cdot 3^2\cdot 5^0\cdot 7^0\cdot \ldots$

$\mathrm{MCD}(12, 18) = 2^1\cdot 3^1\cdot 5^0\cdot 7^0\cdot \ldots = 6$, $\mathrm{mcm}(12, 18) = 2^2\cdot 3^2\cdot 5^0\cdot 7^0\cdot \ldots = 36$

A questo punto, si pongono due problemi:

a) Scoprire se un dato numero sia primo o no
b) Scomporre un dato numero in un prodotto di primi.

In **N** entrambi i problemi sono aperti e sono sempre oggetto di ricerche, a causa delle applicazioni alla crittografia e quindi alla tutela della segretezza nella trasmissione di informazioni bancarie, militari, politiche. Si hanno numerosi criteri di primalità e di divisibilità, alcuni dei quali sono ben noti ed elementari, ma ce ne sono di ben più sofisticati, alcuni dei quali sono implementati sui programmi matematici più comuni (Mathematica, Maple, Derive, ...)

- (Eratostene?) Se un numero dispari non è divisibile per i numeri dispari minori o uguali alla sua radice quadrata è primo.
- (Fermat-Eulero) Un numero p è primo se e solo se per ogni $a\in\mathbf{N}$, $0 < a < p \Rightarrow a^{p-1} \equiv 1 \pmod p$.
- Un numero è divisibile per 2, 3, 5, 11, ... se e solo se ... (*criteri di divisibilità*)

Se consideriamo l'insieme D(n) dei divisori di un dato $n\in\mathbf{N}$ abbiamo dei problemi di tipo numerico o "configurazionale".

a) Quanti elementi ha D(n)?
b) Come trovare questi elementi?
c) Che cosa ha di particolare un numero n con un numero dispari di divisori?
d) Per quali n l'insieme ordinato (D(n), |) è totamente ordinato?
e) Quali numeri del tipo $2^n - 1$ possono essere primi?

Escludiamo subito il caso di n = 0, perché D(0) = **N.** Negli altri casi, D(n) è finito e le domande hanno una risposta; innanzitutto, scomponiamo n in fattori primi, $n = p_1^{n_1}\cdots p_r^{n_r}$. Applicando il criterio generale di divisibilità si ottiene che ogni divisore k di n ha la forma $k = p_1^{k_1}\cdots p_r^{k_r}$,

con $k_i \le n_i$. Pertanto, n ha esattamente $m = (n_1+1)(n_2+1) \dots (n_r+1)$ divisori. Ciò risponde ai quesiti a) e b) (Si veda anche il capitolo sul calcolo combinatorio).

c) Elenchiamo gli elementi di D(n) in senso crescente: possiamo osservare che se $k \in D(n)$, anche $n/k \in D(n)$, per cui, di norma, i divisori vanno a coppie. Pertanto, se m è dispari, c'è un divisore k che coincide con n/k, dunque $n = k^2$ è un quadrato.

d) Se n fosse multiplo di due primi distinti p e q allora D(n) non sarebbe totalmente ordinato, per cui esiste $k \in \mathbf{N}$ tale che $n = p^k$. Ovviamente, viceversa, per un tal n i divisori sono sempre confrontabili, perché $p^h \mid p^k$ se e solo se $h \le k$.

e) Se $n = r \cdot s$, con $r, s > 1$, allora posto $x = 2^r$ si ha $2^{r \cdot s} - 1 = x^s - 1 = (x-1) \cdot \left(\sum_{i=0}^{s-1} x^i \right)$, cioè $2^n - 1$ non è primo. Allora n deve essere primo. Però non per tutti i primi p il numero $2^p - 1$ è primo: per p = 11 infatti si ha $2^{11} - 1 = 2.047 = 23 \cdot 89$. I primi della forma $2^p - 1$ sono detti *primi di Mersenne*, e non è noto se ce ne siano infiniti o no. Se ne conoscono con milioni di cifre.

I numeri primi si presentano in modo disordinato nella sequenza dei numeri naturali: talvolta ci sono due primi dispari consecutivi, come 3 e 5, 11 e 13, 29 e 31 (*primi gemelli*), e si trovano coppie del genere anche molto grandi.

In compenso, per ogni $n \ge 2$ esistono n numeri consecutivi che non sono primi. Si consideri infatti il prodotto dei numeri da 1 ad n+1, che si denota con (n+1)!. Per ogni k, $2 \le k \le n+1$, il numero (n+1)!+k non è primo, perché è multiplo di k. Pertanto, tra (n+1)!+2 ed (n+1)!+(n+1), estremi compresi, non ci sono numeri primi. Per esempio, per n = 5 si ha (n+1)!+2 = 722, (n+1)!+(n+1) = 726 e nessuno dei 5 numeri 722, 723, 724, 725, 726 è primo. Ma se come n prendiamo un milione di miliardi, il risultato è ancora vero: esistono un milione di miliardi di numeri interi consecutivi, nessuno dei quali è primo.

§ 2 – I NUMERI INTERI

Abbiamo visto che i numeri naturali sono entrati nella vita degli esseri umani di Cro-Magnon sotto forma di stringhe finite di tacche. Possiamo ora fantasticare un pittore del tempo di Altamira o Lascaux, che invece di inciderle su un osso, le voglia dipingere su una parete, e siccome sa usare i colori, ne fa una lista col carboncino ed un'altra con l'ocra rossa. Ovviamente, la stringa vuota non può essere colorata. Poi dispone la stringa vuota al centro, le stringhe nere a destra nel senso solito, e le rosse a sinistra, ma in senso contrario:

… IIIII IIII III II I ø I II III IIII IIIII …

Ha creato un nuovo insieme ordinato totalmente, nel quale i rossi precedono la stringa vuota e i neri la seguono. Non ci sono né minimo né massimo.
Poi, concatena le stringhe, come forse faceva al vero il suo antenato Cro-Magnon, *ma con la condizione che una tacca nera ed una rossa vicine si distruggono a vicenda*. Allora il risultato di una concatenazione è una stringa monocromatica: rossa, se prevalgono le tacche rosse; nera se prevalgono le nere.
L'associatività e la commutatività sono salve, la stringa vuota è l'elemento neutro, ma ora ogni stringa, concatenata con quella della stessa lunghezza ma di colore diverso, dà la stringa vuota. Ossia, ogni stringa ha la *opposta*.
Se fosse esistito, un tal pittore paleolitico avrebbe costruito il primo *gruppo*, e per di più commutativo, o meglio *abeliano*, come si dice in linguaggio tecnico. Un tale gruppo avrebbe avuto dentro di sé due copie identiche del monoide additivo (**N**, + , 0), solo colorate diversamente.

Ovviamente la storia della matematica, ricalcata anche dall'insegnamento elementare e medio, ha percorso una strada diversa: il primo gruppo scoperto è quello dei numeri razionali positivi rispetto alla moltiplicazione.

Come detto a suo tempo, l'uso delle stringhe di tacche non è pratico. Allora procederemo in modo diverso: prese due copie di **N**, al posto del colore,

metteremo davanti ad ogni numero ≠ 0 un segno: + al posto del nero; - al posto del rosso. Avremo allora la situazione seguente:

…	IIIII	IIII	III	II	I	Ø	I	II	III	IIII	IIIII	…
…	-5	-4	-5	-2	-1	0	+1	+2	+3	+4	+5	…

I numeri col + sono detti positivi, quelli col meno negativi.

Otteniamo così il gruppo (**Z**, +) dei numeri *interi* relativi (Z dal tedesco Zahlen, numeri). In esso, l'opposto di un numero x si denota con –x. L'opposto di un positivo è negativo, mentre l'opposto di un negativo è positivo.

Questo gruppo nasce dall'impossibilità di eseguire sempre la sottrazione nell'insieme dei numeri naturali. Qui, infatti, per ogni x,y∈ **Z** si ha x-y = x+(-y), ed ora la sottrazione ha dignità di operazione, perché è sempre possibile eseguirla, anche se ha poche proprietà.

C'è però forte ambiguità, legata alla pluralità di significati che i simboli + e - assumono: per il +, che denota sia i positivi, sia la somma, si conviene di non metterlo come segno, ed usarlo solo per l'addizione; ma il segno – deve essere usato per distinguere i negativi dai positivi, per l'addizione e anche per l'opposto di un numero. Dunque, ben tre significati diversi.

Un confronto tra **N** e **Z** mostra che ora la funzione *successivo* $\sigma(x) = x+1$ è biiettiva, e che ha per inversa la funzione $x \mapsto x-1$. In altri termini, ogni intero è il successivo di un altro.

Ad ogni intero x associamo un intero $|x| \geq 0$, ed un altro intero sign(x)∈{-1, 1}, definiti da:

$$|x| = \begin{cases} x & \text{se } x \geq 0 \\ -x & \text{se } x < 0 \end{cases}, \quad \text{sign}(x) = \begin{cases} 1 & \text{se } x > 0 \\ -1 & \text{se } x < 0 \end{cases}.$$

$|x|$ è il *valore assoluto* o *modulo* di x; sign(x) è il *segno* di x ed è definito solo per $x \neq 0$. Queste due funzioni individuano ogni numero non nullo.

Possiamo esprimere l'*addizione*, che abbiamo costruito sulla falsariga delle tacche bicolori, anche mediante valore assoluto e segno, purché si identifichino i numeri positivi con i numeri naturali. Per ogni x, y∈**Z**, si pone:

- x+0 = 0+x = x

- se $\text{sign}(x) = \text{sign}(y)$ allora $\begin{cases} |x+y| = |x| + |y| \\ \text{sign}(x+y) = \text{sign}(x) \end{cases}$, dove la somma tra valori assoluti è eseguita in **N**;
- se $\text{sign}(x) \neq \text{sign}(y)$ e $|x| = |y|$ allora $x+y = 0$
- se $\text{sign}(x) \neq \text{sign}(y)$ e $|x| > |y|$ allora $\begin{cases} |x+y| = |x| - |y| \\ \text{sign}(x+y) = \text{sign}(x) \end{cases}$
- se $\text{sign}(x) \neq \text{sign}(y)$ e $|x| < |y|$ allora $\begin{cases} |x+y| = |y| - |x| \\ \text{sign}(x+y) = \text{sign}(y) \end{cases}$

Questa, in sintesi, è la regola che si cerca di insegnare nella scuola media. Dedurre da questa le proprietà di gruppo abeliano dell'addizione non è affatto agevole.

La moltiplicazione si basa sull'idea di moltiplicare i moduli come fossero numeri naturali, ed i segni dei due numeri secondo la modalità seguente: il prodotto per 1 agisce come l'identità, mentre il prodotto per -1 agisce come l'opposto.

Di qui nasce la seguente tavola di moltiplicazione, detta *regola dei segni*:

·	1	–1
1	1	–1
–1	–1	1

Si osservi che quella tavola definisce un gruppo abeliano di due elementi.

Allora il prodotto di due numeri ogni $x, y \in \mathbf{Z}$ è definito come segue:

- $x \cdot 0 = 0 \cdot x = 0$.
- Se x, y sono non nulli, $\begin{cases} |x \cdot y| = |x| \cdot |y| \\ \text{sign}(x \cdot y) = \text{sign}(x) \cdot \text{sign}(y) \end{cases}$

Le proprietà di monoide commutativo non sono affatto agevoli da dimostrare. Si ha però la legge d'annullamento del prodotto, dato che il solo numero con modulo nullo è lo zero e la proprietà vale in **N**.

Parimenti, è complicata la proprietà distributiva della moltiplicazione rispetto alla addizione (ma nella scuola media non si fanno dimostrazioni di questo tipo).

Quello che si ottiene con le due operazioni, le loro proprietà, i loro elementi neutri e gli opposti, è un *anello commutativo* $(\mathbf{Z}, +, \cdot, 1)$, che, avendo la legge d'annullamento del prodotto, è anche detto *dominio d'integrità*.

Osserviamo che mentre rispetto all'addizione abbiamo due copie del monoide additivo di **N**, costituite rispettivamente dai numeri ≥ 0 e da quelli ≤ 0, la regola dei segni rompe la simmetria e così solo i numeri ≥ 0 riproducono dentro l'anello **Z** la struttura additiva e moltiplicativa di **N**.

Osserviamo ora che in **Z** ci sono esattamente due elementi invertibili, ossia 1 e –1, e questi formano come detto il gruppo che dà la regola dei segni:

$$\mathbf{Z}^* = \left\{ x \in \mathbf{Z} \;\middle|\; \exists y \in \mathbf{Z},\ x \cdot y = 1 \right\} = \left\{ 1, -1 \right\}$$

Ciò costringe a fare varie modifiche nella teoria della divisibilità.

a) **Divisione col resto**: Come in **N**, dati due interi a, b, con $b \neq 0$, esistono due interi q ed r tali che $a = b \cdot q + r$, con $|r| < |b|$. Se $r \neq 0$, non è unico; lo è se si impone $r \geq 0$. Se no, si trovano due resti, di segno opposto, la cui differenza è $|b|$.

Esempi:

$$\begin{array}{r|l} 11 & -7 \\ \hline 4 & -1 \end{array} \qquad \begin{array}{r|l} -11 & -7 \\ \hline 3 & 2 \end{array} \qquad \begin{array}{r|l} -11 & 7 \\ \hline 3 & -2 \end{array}$$

b) **La divisibilità**. Si può procedere come in **N**, ma c'è la complicazione dei segni: ogni numero $a \in \mathbf{Z}$ non nullo è infatti divisore anche del suo opposto: $a = (-1) \cdot (-a)$.

Per esempio, un numero p non nullo e non invertibile è primo se ha per divisori solo 1, -1, p, -p.

Conviene però pensare ogni numero negativo come ottenuto moltiplicando il suo opposto (che è positivo) per -1. In tal modo, i conti si svolgono sempre con numeri positivi.

Esempio di scomposizione in fattori primi:

$$-18 = (-1) \cdot 18 = (-1) \cdot 2 \cdot 3^2.$$

Valgono allora in **Z** il teorema fondamentale dell'aritmetica, l'algoritmo euclideo e l'esistenza ed unicità del MCD e del mcm (se scelti positivi).

c) Gli ordinamenti. L'ordine $\leq$ in **Z** si può anche definire ponendo $x \leq y$ se $y-x$ è positivo. Invece, la relazione "divide" non è una relazione d'ordine in quanto non è antisimmetrica: se x divide y e y divide x allora $y = \pm x$.

C'è però un vantaggio a lavorare in **Z** anziché in **N** per la teoria della divisibilità:

PROPOSIZIONE 2.1. (**Identità di Bézout**). Se $d = MCD(a,b)$ in **Z**, esistono $u, v \in \mathbf{Z}$ tali che $a \cdot u + b \cdot v = d$.

Dimostrazione. Questi due coefficienti u, v si ottengono dal procedimento euclideo delle divisioni successive; innanzitutto,

$$a = b \cdot q_1 + r_1 \text{ Þ } r_1 = u_1 a + v_1 b, \text{ con } u_1 = 1 \text{ e } v_1 = -q_1;$$

allora, per induzione su i, supposto $r_j = u_j a + v_j b$ per ogni $j \leq i$, e $r_{i-1} = r_i q_{i+1} + r_{i+1}$ allora

$$r_{i+1} = (u_{i-1} - q_{i+1} u_i) a + (v_{i-1} - q_{i+1} v_i) b$$

Pertanto, poiché d è uno di questi resti, vale anche per lui la stessa espressione come combinazione lineare di a e b.

Si può costruire uno schema che riproduca direttamente il procedimento induttivo visto sopra, fornendo sia d sia i coefficienti u e v.

a	b	$r_0 = r$	r_1	r_2	…
1	0	$u_0 = 1 - 0 \cdot q_0$	$u_1 = 0 - u_0 \cdot q_1$	$u_2 = u_0 - u_1 \cdot q_2$	
0	1	$v_0 = 0 - 1 \cdot q_0$	$v_1 = 1 - v_0 \cdot q_1$	$v_2 = v_0 - v_1 \cdot q_2$	
	$q_0 = q$	q_1	q_2	q_3	

Esempio con a = 120 e b = 85:

120	85	35	15	5	0
1	0	1	-2	5	-17
0	1	-1	3	-7	24
	1	2	2	3	

Si osservi che si ha:

35=120·1+85·(-1)	15=120·(-2)+83·3	5=120·5+85·(-7)	0=120·(-17)+83·24

L'ultimo resto non nullo è 5, quindi 5 = MCD(120, 85) = 120·5 + 85·(-7)

COROLLARIO 2.2. a) Due numeri interi a, b non nulli sono coprimi (ossia MCD(a,b) = 1) se e solo se esistono u, v interi tali che $a \cdot u + b \cdot v = 1$.

b) Sia d = MCD(a,b). Posto a = d·a', b = d·b' allora MCD(a',b') = 1.

Dimostrazione. a) I due numeri a, b sono coprimi se MCD(a, b) = 1, quindi per l'algoritmo euclideo esistono u, v interi tali che $a \cdot u + b \cdot v = 1$. Inversamente, posto d = MCD(a, b), se esistono u, v interi tali che $a \cdot u + b \cdot v = 1$, allora necessariamente d divide 1, quindi è uguale ad 1, per cui a e b sono coprimi.

b) Siano u, v tali che $a \cdot u + b \cdot v = d$. Dividiamo per d ambo i membri ed otteniamo $a' \cdot u + b' \cdot v = 1$, quindi per a) si ha MCD(a',b') = 1.

COROLLARIO 2.3. Lemma di Euclide. Dati tre numeri interi a, b, c, se a divide bc e MCD(a,b) = 1, allora a divide c.

Dimostrazione. Sia bc = aq. Per il corollario 2.2. esistono u, v interi tali che $1 = a \cdot u + b \cdot v$. Allora, moltiplicando ambo i membri per c, otteniamo:

$$c = a \cdot (cu) + (bc) \cdot v = a \cdot (cu + qv)$$

NOTA. Ovviamente, Euclide non dimostra in questo modo la proprietà, ma con ragionamenti simili a quelli ben più faticosi usati a suo tempo per caratterizzare i numeri primi in **N**. Da questo lemma, per altro, segue subito la caratterizzazione euclidea dei numeri primi.

§ 3. – CALCOLO COMBINATORIO

In questa sezione si suppongono noti i numeri naturali e si usano per contare gli elementi di certi insiemi finiti, ossia esploriamo il *calcolo combinatorio* elementare. Il problema generale è la determinazione del numero di elementi di certi insiemi finiti conoscendo il numero d'elementi di certi altri insiemi finiti. Ricordiamo che due insiemi A e B si dicono *equipotenti* se esiste una biiezione $f : A \xrightarrow{1-1}{su} > B$. L'equipotenza possiede le proprietà riflessiva, simmetrica e transitiva. Se A è equipotente a B scriviamo $A \cong B$.

Gli insiemi equipotenti ad **N** si dicono *numerabili*. Si può dimostrare che un insieme è infinito se e solo se contiene un sottoinsieme numerabile. Esempi di insiemi numerabili sono i sottoinsiemi di **N** non limitati superiormente, ma anche l'insieme **Z** degli interi o l'insieme **Q** dei numeri razionali. Invece, l'insieme $\wp(\mathbf{N})$ dei sottoinsiemi di **N** e l'insieme **R** dei numeri reali sono infiniti, ma non numerabili.

Siano $n \in \mathbf{N}$, $n > 0$, ed $\mathbf{N}_n = \{i \in \mathbf{N} \mid 1 \le i \le n\}$. Sia poi X un insieme. Diremo che X è *finito* se $X = \varnothing$ oppure se esiste $n \in \mathbf{N}$ tale che $\mathbf{N}_n \cong X$.

Ci sono vari modi di introdurre il numero di elementi di un insieme finito, ed ogni autore ha le sue preferenze. A me piace il modo seguente, basato su un lemmma di unicità.

LEMMA 3.1. Per ogni $m, n \in \mathbf{N}$, non nulli, se $\mathbf{N}_m$ ed $\mathbf{N}_n$ sono equipotenti allora $n = m$.

Dimostrazione. Procediamo per induzione rispetto ad m. Siano $\mathbf{N}_m$ ed $\mathbf{N}_n$ equipotenti e sia $f : \mathbf{N}_m \xrightarrow{1-1}{su} > \mathbf{N}_n$. Se m = 1, allora n = 1, altrimenti $\mathbf{N}_n = \{k \in \mathbf{N} \mid 1 \le k \le n\} \supset \{f(1)\}$, e viceversa. Sia m > 1 (quindi n > 1), sia vero il lemma per m-1 e dimostriamo che è vero anche per m.

Sia $u = f^{-1}(n) \in \mathbf{N}_m$. Poniamo $g : \mathbf{N}_{m-1} \to \mathbf{N}_n$, $g(k) = \begin{cases} f(k) & k < u \\ f(k+1) & k \ge u \end{cases}$. Allora:

$$\mathrm{im}(g) = \mathrm{im}(f) \setminus \{f(u)\} = \mathbf{N}_n \setminus \{n\} = \mathbf{N}_{n-1}$$

Inoltre, g è iniettiva. Infatti, $\forall h,k \in \mathbf{N}_{m-1}$, se g(h) = g(k) allora:

- Se sono entrambi minori di u, si ha f(h) = f(k) quindi h = k.

- Se sono entrambi maggiori di u, allora f(h+1) = f(k+1) implica h+1 = k+1 ossia h = k.
- Altrimenti, se k < u ≤ h, allora f(k) = f(h+1) implica $k = h+1 > h > k$, assurdo.

Pertanto, $g : \mathbf{N}_{m-1} \xrightarrow{1-1\ su} \mathbf{N}_{n-1}$.

L'ipotesi induttiva implica allora m-1 = n-1, ossia m = n.

Questo lemma giustifica la seguente definizione. Siano X un insieme ed n un numero naturale non nullo. Se X = ø poniamo $|X| = 0$. Sia X ≠ ø; se X è equipotente ad $\mathbf{N}_n$ poniamo $|X| = n$. Chiameremo $|X|$ *numero di elementi* di X.

PROPOSIZIONE 3.2. Sia X un insieme finito, $|X| = n$.

a) Ogni insieme Y equipotente ad X ha lo stesso numero n di elementi.

b) Per ogni $A \subseteq X$ si ha $|A| \leq n$.

Dimostrazione. a) Se X è vuoto, anche Y è vuoto, quindi |X| = |Y| = 0. Sia X non vuoto; |X| = n significa che esiste $f : \mathbf{N}_n \xrightarrow{1-1\ su} X$. X ≅ Y significa che esiste $g : X \xrightarrow{1-1\ su} Y$, allora $g \circ f : \mathbf{N}_n \xrightarrow{1-1\ su} Y$ e quindi |Y| = n.

b) Se X = ø allora A = ø. Sia X ≠ ø; |X| = n significa che esiste $f : \mathbf{N}_n \xrightarrow{1-1\ su} X$. Consideriamo l'immagine $f^{-1}(A) \subseteq \mathbf{N}_n$ di A rispetto alla biiezione inversa. Allora $|A| = |f^{-1}(A)|$ e $f^{-1}(A)$ è costituito da numeri naturali distinti compresi tra 1 ed n, quindi sono al massimo n. Pertanto, |A| ≤ n.

Qui vedremo alcuni problemi classici in una formulazione che fa uso della teoria degli insiemi. Ciascuno di essi fornisce lo strumento per risolvere il problema successivo.

PROBLEMA I. Siano A e B insiemi finiti, e sia A∩B = ∅. Calcolare |A∪B|.

TEOREMA 3.3. - In queste ipotesi si ha |A∪B| = |A| + |B|.

Dimostrazione. Poniamo |A| = k, |B| = n. Se k = 0 oppure n = 0 allora è banale. Altrimenti esistono $\varphi : \mathbf{N}_k \xrightarrow{1\text{-}1\ su} A$, $\psi : \mathbf{N}_n \xrightarrow{1\text{-}1\ su} B$. Definiamo ora una funzione $\Phi : \mathbf{N}_{k+n} \xrightarrow{1\text{-}1\ su} A \cup B$ ponendo, per ogni $i \in \mathbf{N}_{k+n}$,

$$\Phi(i) = \begin{cases} \varphi(i) & \text{se } i \le k \\ \psi(i-k) & \text{se } i > k \end{cases}$$

Poiché φ e ψ sono funzioni e $A \cap B = \varnothing$, anche Φ è una funzione ed è anche una biiezione.

COROLLARIO 3.4 – a) **Principio di addizione.** - Siano $A_1, \ldots, A_r$ insiemi finiti a due a due disgiunti. Allora $\left|\bigcup_{i=1}^{r} A_i\right| = \sum_{i=1}^{r} |A_i|$.

b) *Principio dei cassetti*: se A è un insieme con n elementi e $\wp = \{C_1, \ldots, C_m\}$ è una partizione di A con $m < n$ blocchi, allora esiste $i \in \{1, 2, \ldots, r\}$ tale che $|C_i| > 1$.

Dimostrazione. a) Per induzione su r, se r = 2 è vero per il teorema 3.3. Supponiamo il teorema vero per r (≥ 2) e proviamo che di conseguenza è vero per r+1.

Posto $B = \bigcup_{i=1}^{r} A_i$, si ha $B \cap A_{r+1} = \varnothing$ e $|B| = \sum_{i=1}^{r} |A_i|$, dunque per il teorema 3.3 si ha

$$|B \cup A_{r+1}| = \sum_{i=1}^{r} |A_i| + |A_{r+1}| = \sum_{i=1}^{r+1} |A_i|.$$

b) Se in un insieme A con n elementi consideriamo una partizione $\wp = \{C_1, \ldots, C_m\}$, allora A è unione disgiunta delle componenti $C_1, \ldots, C_m$. Ne segue $|A| = \left|\bigcup_{i=1}^{m} C_i\right| = \sum_{i=1}^{m} |C_i|$.

In particolare, poiché ogni componente ha almeno un elemento, allora $|A| = \sum_{i=1}^{m} |C_i| \ge \sum_{i=1}^{m} 1 = m = |\wp|$. Di conseguenza, n > m implica che per almeno uno dei "cassetti" sia $|C_i| > 1$.

COROLLARIO 3.5. Siano A e B insiemi finiti. Se esiste $f : A \xrightarrow{su} B$ allora $|A| \ge |B|$.

Dimostrazione. Consideriamo la relazione di equivalenza $\Re_f$ in A, associata ad f, secondo la quale sono in relazione due elementi x ed y se f(x) = f(y). Essendo f suriettiva esiste una biiezione F tra l'insieme quoziente $A/\Re_f$, che è una partizione di A, e il codominio B, che associa ad ogni classe $[a]_{\Re_f}$ l'elemento $f(a)$. Dunque, $|A/\Re_f| = |B|$. Per quanto precede, però, $|A| \geq |A/\Re_f|$, perciò $|A| \geq |B|$.

COROLLARIO 3.6. Siano $|A| = k$, $|B| = n$, $C \subseteq A$, $|C| = r$.

a) $|A \setminus C| = k-r$.

b) Sia $C = A \cap B$, allora $|A \cup B| = k+n-r$.

Dimostrazione. a) La coppia $\{C, A \setminus C\}$ è una partizione di A, quindi per il principio di addizione si ha $|A| = |C| + |A \setminus C|$, da cui segue $|A \setminus C| = |A| - |C| = k-r$.

b) La terna $\{C, A \setminus C, B \setminus C\}$ è una partizione di $A \cup B$, quindi

$$|A \cup B| = |A \cap B| + |A \setminus C| + |B \setminus C| = r + (k - r) + (n - r) = k + n - r$$

Denotiamo con $A \times B$ il prodotto cartesiano di A per B, cioè l'insieme di tutte le coppie ordinate (a, b), con $a \in A$ e $b \in B$.

PROBLEMA II. Siano A e B insiemi finiti. Calcolare $|A \times B|$.

TEOREMA 3.7. Si ha $|A \times B| = |A| \cdot |B|$.

Dimostrazione. Se A oppure B è vuoto allora è banale. Altrimenti osserviamo che $A \times B = \bigcup_{a \in A} (\{a\} \times B)$, e che tutti gli insiemi $\{a\} \times B$ sono a due a due disgiunti ed equipotenti a B. Infatti, $a \neq a' \Rightarrow (a, b) \neq (a', b')$ per tutti i b, b'∈B, quindi $(\{a\} \times B) \cap (\{a'\} \times B) = \varnothing$. Inoltre, per ogni a∈A, la funzione $f_a : B \to \{a\} \times B$, $f_a : b \mapsto (a, b)$, risulta biiettiva, perciò $\{a\} \times B$ è equipotente a B. Per il corollario 8.3.4 si ha quindi:

$$|A \times B| = \left| \bigcup_{a \in A} (\{a\} \times B) \right| = \sum_{a \in A} |\{a\} \times B| = \sum_{a \in A} |B| = |A| \cdot |B|$$

perché somma di $|A|$ addendi uguali a $|B|$.

Il prodotto cartesiano degli insiemi $A_1, A_2, \ldots, A_n$, $n > 2$ è definito induttivamente: $A_1 \times \ldots \times A_n = (A_1 \times \ldots \times A_{n-1}) \times A_n$. I suoi elementi sono detti *liste* o *n-uple ordinate*, e denotati con $(a_1, a_2, \ldots, a_n)$.

COROLLARIO 3.8. Il principio di moltiplicazione. Se A_1, ..., A_k sono insiemi finiti, allora $|A_1 \times \ldots \times A_k| = \prod_{i=1}^{k} |A_i|$.

Dimostrazione. Procediamo per induzione rispetto a k. Per k = 2 l'asserto è il teorema 3.7. Sia k ≥ 3, allora si ha $A_1 \times \ldots \times A_k = (A_1 \times \ldots \times A_{k-1}) \times A_k$. Per ipotesi induttiva, $|A_1 \times \ldots \times A_{k-1}| = \prod_{i=1}^{k-1} |A_i|$ e, per il teorema 3.7, si ottiene:

$$|A_1 \times \ldots \times A_k| = |(A_1 \times \ldots \times A_{k-1}) \times A_k| = \left(\prod_{i=1}^{k-1} |A_i| \right) \cdot |A_k| = \prod_{i=1}^{k} |A_i|$$

NOTA. Il *principio di moltiplicazione* afferma che se per la lista $(a_1, a_2, \ldots, a_n)$ ci sono: n_1 possibilità per a_1, n_2 possibilità per a_2, e così via, in tutto ci sono $n_1 \cdot n_2 \cdot \ldots \cdot n_k$ liste distinte. In particolare, se A_1, ... , A_k sono tutti uguali ad un insieme A con n elementi, ci sono in tutto n^k liste distinte (k = lunghezza della lista, n = numero di scelte per ogni casella).

PROBLEMA III. Siano A e B insiemi finiti non vuoti. Calcolare $|B^A|$, ovvero il numero di funzioni f:A→B.

TEOREMA 3.9. Risulta $|B^A| = |B|^{|A|}$.

Dimostrazione. Sia $A = \{a_1, a_2, \ldots, a_k\}$. Ogni f:A→B si può rappresentare mediante la tabella

x	a_1	a_2	⋯	a_k
$f(x)$	$f(a_1)$	$f(a_2)$	⋯	$f(a_k)$

, ossia, in definitiva, mediante la lista $(f(a_1), f(a_2), \ldots, f(a_k))$. Quest'ultimo oggetto è un elemento del prodotto cartesiano B^k. Inversamente, dato un

qualunque elemento $(b_1, b_2, \ldots, b_k) \in B^k$, la tabella $\begin{array}{c|ccccc} x & a_1 & a_2 & \cdots & a_k \\ \hline y & b_1 & b_2 & \cdots & b_k \end{array}$ definisce una funzione f:A→B. Allora la corrispondenza Φ che ad ogni funzione f:A→B associa la lista $(f(a_1), f(a_2), \ldots, f(a_k)) \in B^k$ è una biiezione da B^A a B^k. Quest'ultimo ha $|B|^k = |B|^{|A|}$ elementi, quindi risulta proprio $|B^A| = |B|^{|A|}$.

ESEMPI 3.10.

3.10.A. - Quante parole di 3 lettere si possono scrivere con l'alfabeto $\{a, c, g, t\}$?

Ogni parola è una lista di lettere. Nel nostro caso, le lettere sono tre, e per ciascuna ci sono 4 possibilità, quindi $4 \cdot 4 \cdot 4 = 4^3 = 64$ parole.

3.10.B. - Sia |A| = n. Quante operazioni diverse, ossia funzioni $* : A \times A \to A$, si possono definire su A? Poiché $|A \times A| = n^2$, le operazioni possibili sono $n^{(n^2)}$. Per esempio, se n = 2, ci sono $2^4 = 16$ operazioni distinte.

COROLLARIO 3.11. Sia U un insieme finito, |U| = n; allora $|\wp(U)| = 2^n$.

Dimostrazione. Sia X⊆U; definiamo la seguente funzione associata ad X, detta *funzione caratteristica* di X: $\varepsilon_X : U \to \{0,1\}$, $\varepsilon_X : x \mapsto \begin{cases} 0 & \text{se } x \notin X \\ 1 & \text{se } x \in X \end{cases}$.

Definiamo ora la funzione $\varepsilon : \wp(U) \to \{0,1\}^U$, $\varepsilon : X \mapsto \varepsilon_X$. Tale funzione è una biiezione, e allora dal teorema 3.8 segue l'asserto.

PROBLEMA IV. Siano A e B due insiemi finiti non vuoti. Calcolare il numero delle funzioni iniettive $f : A \xrightarrow{1\text{-}1} B$.

Se |A| = k e |B| = n tale numero si denota con $D_{n,k}$ e viene anche chiamato *numero delle disposizioni senza ripetizioni* di n oggetti a k a k. Il problema si può porre anche per |A| = 0: in tal caso fra A e B vi è solo la *funzione vuota*, che è iniettiva. Pertanto $D_{n,0} = 1$ per ogni $n \geq 0$.

LEMMA 3.12. Siano A e B insiemi finiti. Se esiste $f : A \xrightarrow{1-1} B$ allora $|A| \le |B|$.

Dimostrazione. Poiché f è iniettiva allora la co-restrizione di f ad f(A) ⊆ B è biiettiva da A ad f(A). Pertanto, A è equipotente ad f(A). Allora, $|A| = |f(A)| \le |B|$.

TEOREMA 3.13. Risulta $D_{n,k} = \begin{cases} 0 & \text{se } k > n \\ \prod_{i=0}^{k-1}(n-i) & \text{se } 0 \le k \le n \end{cases}$.

Dimostrazione. Sia |B| = n. Se |A| = k > n, allora per il lemma si ha $D_{n,k} = 0$. Sia k ≤ n. Ogni $f : A \xrightarrow{1-1} B$ si può rappresentare mediante la lista $(f(a_1), f(a_2), \ldots, f(a_k))$, dove gli elementi sono tutti distinti. Allora, mentre $f(a_1)$ è un elemento qualunque di B, $f(a_2) \in B \setminus f(a_1)$, che ha n-1 elementi, $f(a_3) \in B \setminus \{f(a_1), f(a_2)\}$, che ha n-2 elementi, e così via. La conclusione segue ora dal principio di moltiplicazione.

Poniamo 0! = 1, e per ogni n > 0 poniamo n! = (n-1)!·n. Il simbolo n! si legge "n *fattoriale* ".

PROPOSIZIONE 3.14. – a) Sia X un insieme finito non vuoto, |X| = n. Sia S_X l'insieme delle permutazioni su X. Allora $|S_X| = n!$

b) Risulta $D_{n,k} = \dfrac{n!}{(n-k)!}$ per ogni $0 \le k \le n$.

Dimostrazione. a) Le permutazioni di X sono biiezioni da X a se stesso, perciò ce ne sono $D_{n,n}$. Quest'ultimo numero coincide proprio con n!

b) Si ha $D_{n,k} = \dfrac{D_{n,k} \cdot (n-k)!}{(n-k)!} = \dfrac{n!}{(n-k)!}$.

GLI ANAGRAMMI. Anagrammare una parola significa permutarne le lettere. Se la parola ha n lettere distinte, ci sono n! anagrammi. Per esempio, la parola *cane* ha 4! = 24 anagrammi. Non tutti hanno significato in Italiano, ma non importa: ogni linguaggio usa solo una piccola parte delle infinite parole che si possono scrivere col suo alfabeto.

Ma se ci sono lettere ripetute, ossia con frequenza maggiore di 1?

Per esempio, la parola *mamma* non cambia se si permutano (in 3! = 6 modi) le tre *m* oppure (in 2! = 2 modi) le due *a*. Allora, gli anagrammi della *mamma* sono in tutto $\frac{5!}{3!\cdot 2!} = \frac{5\cdot 4\cdot 3\cdot 2\cdot 1}{3\cdot 2\cdot 1\cdot 2\cdot 1} = \frac{5\cdot 4}{2\cdot 1} = 10$. La formula generale, per una parola di lunghezza n e con r lettere distinte di frequenze f_i, $1 \le i \le r$, è $\frac{n!}{f_1!f_2!\cdots f_r!}$.

PROBLEMA V. Sia X un insieme finito con n elementi. Trovare il numero $C_{n,k}$ di sottoinsiemi di X aventi k elementi. Tale numero è anche chiamato numero delle *combinazioni senza ripetizione* di n oggetti a k a k.

TEOREMA 3.15. Si ha $C_{n,0} = 1$, e, per $0 \le k < n$, $C_{n,k} = \frac{n!}{k!\cdot(n-k)!}$.

Dimostrazione. Elenchiamo gli n elementi di X in un ordine qualsiasi, ma fissato: $X = \{x_1, \ldots, x_n\}$. Sia Y un sottoinsieme con k elementi, e rappresentiamo Y mediante una lista di lunghezza n, in cui all'i-esimo posto mettiamo la lettera V se $x_i \in Y$, la lettera F se $x_i \notin Y$. Allora, Y è una lista, assimilabile ad una parola, costituita solo da k lettere V ed n-k lettere F. Per esempio, X produce la parola con tutti V; il vuoto ø la parola con tutti F.
Ogni insieme con k elementi produce una parola con lo stesso numero k di lettere V ed n-k lettere F, ossia una parola che è un anagramma della parola di Y. Siamo allora nella stessa situazione della *mamma*: avremo $\frac{n!}{k!\cdot(n-k)!}$ anagrammi, quindi $C_{n,k} = \frac{n!}{k!\cdot(n-k)!}$ sottoinsiemi con k elementi.

Poniamo $\binom{n}{k} = C_{n,k} = \frac{n!}{k!\cdot(n-k)!}$. Questo simbolo si chiama *coefficiente binomiale*, ed è, lo ricordiamo, un **numero intero**.

PROPOSIZIONE 3.16. Siano n, k due numeri interi ≥ 0 e sia $k \le n$.

a) $\binom{n}{0} = \binom{n}{n} = 1$.

b) $\binom{n}{k} = \binom{n}{n-k}$.

c) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Dimostrazione. Sia X un insieme con n elementi.

a) $\binom{n}{0}$ è il numero di sottoinsiemi di X con 0 elementi, ossia vuoti, e ce n'è uno solo. Analogamente, di sottoinsiemi di X con n elementi c'è solo X.

b) Per ogni sottoinsieme di X con k elementi c'è il complementare con n-k elementi. Pertanto,

$$\binom{n}{k} = \binom{n}{n-k}.$$

c) Si fissi un elemento x di X. Ogni sottoinsieme Y di X con k elementi è di uno dei due tipi seguenti:

- Y non contiene x: è un sottoinsieme con k elementi di X\{x}, che ha n-1 elementi; di questi Y quindi ce ne sono $\binom{n-1}{k}$;
- Y contiene x: allora Y\{x} è un sottoinsieme con k-1 elementi di X\{x}, che ha n-1 elementi; di questi Y quindi ce ne sono $\binom{n-1}{k-1}$

In totale quindi ci sono $\binom{n-1}{k}+\binom{n-1}{k-1}$ sottoinsiemi Y con k elementi.

Le proprietà a) e c) consentono di costruire un noto triangolo, detto in Italia "Triangolo di Tartaglia", , ma è preferibile chiamarlo *triangolo aritmetico*. Il termine all'incrocio della riga n-esima con la colonna k-esima è $\binom{n}{k}$, ed è ottenuto sommando i termini $\binom{n-1}{k-1}$ ed $\binom{n-1}{k}$, che lo sovrastano nella riga precedente. La somma dei termini della riga n-esima dà il numero di sottoinsiemi di un insieme con n elementi, che sappiamo essere 2^n.

$n \setminus k$	0	1	2	3	4	5	6	7	2^n
0	1								$1 = 2^0$
1	1	1							$2 = 2^1$
2	1	2	1						$4 = 2^2$
3	1	3	3	1					$8 = 2^3$
4	1	4	6	4	1				$16 = 2^4$
5	1	5	10	10	5	1			$32 = 2^5$
6	1	6	15	20	15	6	1		$64 = 2^6$
7	1	7	21	35	35	21	7	1	$128 = 2^7$

COROLLARIO 3.17. - *Formula di Newton* - Siano x e y due numeri reali ed n∈**N**.

Allora $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.

Dimostrazione. Se n = 0 oppure n = 1 il risultato è immediato.

Sia n ≥ 2: $(x+y)^n = (x+y)(x+y)\cdots(x+y)$, e lo sviluppo del secondo membro è la somma dei monomi ottenuti scegliendo un termine da ogni fattore x+y, dunque ogni tal monomio è del tipo $x^{n-k}y^k$, ed è ottenuto scegliendo y da k degli n fattori x+y ed x dagli altri n-k. Pertanto per ognuno degli $\binom{n}{k}$ insiemi di k fattori x+y vi è un monomio $x^{n-k}y^k$; riducendo i termini simili, il coefficiente di questo monomio diviene $\binom{n}{k}$.

NOTA. Posto x = y = 1, dalla formula di Newton si riottiene il numero 2^n di sottoinsiemi di un insieme con n elementi.

Esempio 3.18. Il numero di possibili sestine nel superenalotto si ottiene considerando che da un insieme di n = 90 numeri sostanzialmente se ne estraggono k = 6, distinti. Allora il numero cercato è:

$$C_{90,6} = \binom{90}{6} = \frac{90!}{6!\cdot 84!} = \frac{90\cdot 89\cdot 88\cdot 87\cdot 86\cdot 85}{6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1} = 622.614.630.$$

Esempio 3.19 Un allenatore sta scegliendo la formazione per la prossima partita.

Ha a disposizione: 3 portieri, 8 difensori, 6 centrocampisti e 5 attaccanti.

La squadra sarà composta da: un portiere, 4 difensori, 3 centrocampisti e 3 attaccanti.

Quante possibili formazioni diverse potrebbe allestire?

Portiere	Difesa	Centrocampo	Attacco
$\binom{3}{1} = 3$	$\binom{8}{4} = 70$	$\binom{6}{3} = 20$	$\binom{5}{3} = 10$

Pertanto, potrebbe allestire ben 3•70•20•10 = 42.000 formazioni diverse!

§ 4 – I GRUPPI SIMMETRICI

In questa sezione si danno per note alcune nozioni sui gruppi, apprese nell'altro modulo del corso. In particolare, le nozioni di ordine di un elemento, sottogruppo, gruppi e sottogruppi ciclici, potenze in un gruppo.

PREMESSE SUI MONOIDI. Ricordo che un monoide è una *struttura algebrica* $\left(M,\cdot,1_M\right)$ in cui l'operazione binaria $\cdot$ è associativa ed 1_M ne è l'elemento neutro. Abbiamo visto già gli esempi dei monoidi additivo e moltiplicativo costruiti su **N**. Vediamo uno degli esempi più importanti.

I monoidi di funzioni: sia X un insieme non vuoto e sia X^X l'insieme delle funzioni da X in sé; definiamo in X^X l'operazione $\circ$ di composizione: è noto che è associativa e che ha per elemento neutro la *funzione identità* id_X che ad ogni $x \in X$ associa se stesso. Il monoide $\left(X^X,\circ,\mathrm{id}_X\right)$ è il *monoide delle funzioni di X*. Se X ha n elementi, dal calcolo combinatorio sappiamo che esso possiede n^n elementi.

Una nozione che si può introdurre in un monoide è quella di *potenza*. Sia $\left(M,\cdot,1_M\right)$ un monoide e sia $x \in M$. Poniamo $\forall n \in \mathbf{N}, \begin{cases} x^0 = 1_M \\ x^{n+1} = x^n \cdot x \end{cases}$.

Valgono per le potenze le due proprietà seguenti:

$$\forall x \in M, \forall m,n \in \mathbf{N}, \begin{cases} x^n \cdot x^m = x^{n+m} \\ \left(x^n\right)^m = x^{nm} \end{cases}.$$

Si noti che $\forall x,y \in M,\ \left(x\cdot y\right)^n = x^n \cdot y^n\ \forall n \in \mathbf{N}$ vale se $x\cdot y = y\cdot x$, altrimenti in generale no. Queste proprietà si dimostrano per induzione rispetto ad n.

Un monoide $\left(M,\cdot,1_M\right)$ si dice *commutativo* se $\forall x,y \in M,\ x\cdot y = y\cdot x$. Un esempio è (**N**,+,0).

Un monoide $(M,\cdot,1_M)$ si dice *idempotente* se $\forall x \in M,\ x \cdot x = x$. Un esempio è (**N**,mcm,1), dove mcm denota il minimo comune multiplo. Un altro esempio è, per ogni insieme X, $(\wp(X),\cup,\varnothing)$.

Elementi invertibili: un elemento $x \in M$ si dice invertibile se esiste $x' \in M$ tale che $x \cdot x' = x' \cdot x = 1_M$. In tal caso, x' si dice inverso di x, ed è unico. Infatti, sia x" un altro inverso di x; allora:

$$x'' = x'' \cdot 1_M = x'' \cdot (x \cdot x') = (x'' \cdot x) \cdot x' = 1_M \cdot x' = x'$$

L'inverso di x, se esiste, si denota con x^{-1}.

Un monoide in cui ogni elemento sia invertibile è un *gruppo.* In ogni caso, l'insieme M^* degli elementi invertibili è un gruppo, detto *gruppo delle unità del monoide*. Infatti, contiene l'unità, perché $(1_M)^{-1} = 1_M$; per ogni x,y$\in M^*$ si ha poi: $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$ e $\left(x^{-1}\right)^{-1} = x$, quindi anche x·y ed x^{-1} sono invertibili.

Per un elemento invertibile x si ha anche la seguente proprietà: per ogni n∈**N**, $\left(x^{-1}\right)^n = \left(x^n\right)^{-1}$, quindi si possono definire anche le potenze con esponente negativo, ponendo: per ogni n∈**N**, $x^{-n} = \left(x^{-1}\right)^n = \left(x^n\right)^{-1}$. Si dimostra che valgono le proprietà delle potenze anche per gli esponenti interi.

NOTA. Un monoide può avere l'elemento assorbente, che se è presente in un prodotto, distrugge gli altri fattori: non è invertibile né cancellabile e può essere fastidioso anche definirne la potenza con esponente 0. Perciò, se mai, si escludano i monoidi con elemento assorbente da questi discorsi. Tanto, nei gruppi non ce ne sono.

Un isomorfismo tra due monoidi $(M,\cdot,1_M)$ ed $(H,*,1_H)$ è una funzione biiettiva $f : M \to H$ tale che

$$\begin{cases} \forall x, y \in M, f(x \cdot y) = f(x) * f(y) \\ f(1_M) = 1_H \end{cases}$$

Nel caso dei gruppi la seconda condizione segue dalla prima. Questo giustifica l'uso della notazione abbreviata $(G,\cdot)$ per indicare un gruppo. Vediamo un esempio di due gruppi isomorfi:

+	pari	dispari
pari	pari	dispari
dispari	dispari	pari

e

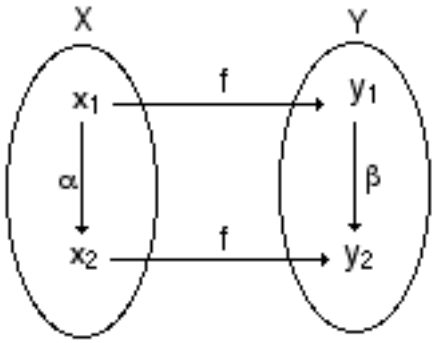
·	1	–1
1	1	–1
–1	–1	1

.

Nel caso del monoide $\left(X^X, \circ, id_X\right)$ delle funzioni da X ad X il gruppo delle unità è detto *gruppo simmetrico* S_X; i suoi elementi sono le biiezioni da X in sé e si chiamano *permutazioni di X*.

LEMMA 4.1. Siano X ed Y due insiemi equipotenti. Allora i gruppi simmetrici S_X ed S_Y sono isomorfi.

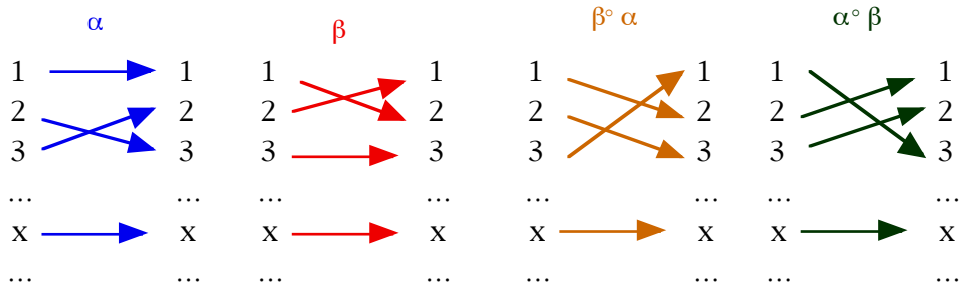
Dimostrazione. Sia f la biiezione tra X ed Y. In riferimento alla figura, data $\alpha \in S_X$, poniamo: $\beta = f \circ \alpha \circ f^{-1}$. Allora $\beta \in S_Y$. Poniamo $\Phi : S_X \to S_Y$, $\Phi(\alpha) = \beta$. Questa è l'isomorfismo cercato. Infatti, ha per inversa la funzione $\beta \mapsto f^{-1} \circ \beta \circ f$, quindi è biiettiva. Poi, per ogni $\alpha, \alpha' \in S_X$ si ha:



$$\Phi(\alpha) \circ \Phi(\alpha') = \left(f \circ \alpha \circ f^{-1}\right) \circ \left(f \circ \alpha' \circ f^{-1}\right) = f \circ (\alpha \circ \alpha') \circ f^{-1} = \Phi(\alpha \circ \alpha')$$

Nel caso finito, siano $n \in \mathbf{N}^+$ ed $\mathbf{N}_n = \left\{ i \in \mathbf{N} \mid 1 \le i \le n \right\}$. Il lemma precedente consente di scegliere come insieme X con n elementi proprio l'insieme $\mathbf{N}_n$, che supporremo ordinato nel modo naturale. Il suo gruppo simmetrico si denota con S_n. Dal calcolo combinatorio sappiamo che ha n! elementi.

Non è difficile verificare che, se n è maggiore di 2, il gruppo $(S_n, \circ)$ non è abeliano. Infatti, sia $X = \{1, 2, 3, \ldots, x, \ldots\}$, dove x è un generico elemento > 3:

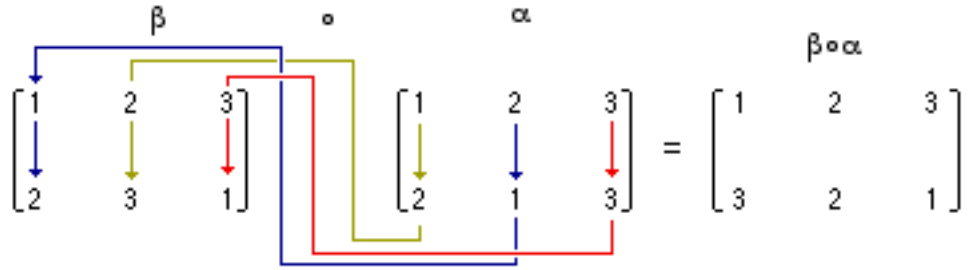


Si ha quindi $\alpha \circ \beta \neq \beta \circ \alpha$ ed il gruppo simmetrico S_n non è abeliano per $n \geq 3$.

La scrittura consueta per rappresentare una permutazione in S_n è la seguente:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \dots & \alpha(n) \end{pmatrix}$$

Per eseguire la composizione di due permutazioni si procede come nell'esempio seguente: siano $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ e calcoliamo $\beta \circ \alpha$.



Per calcolare l'inversa di $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ basta "capovolgerla" e riordinare le colonne: $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \to \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \rho^{-1}$

Calcoliamo ora la tavola di composizione del gruppo simmetrico S_2. Esso ha due soli elementi, $\mathrm{id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. Poiché id è l'elemento neutro, la tavola è necessariamente la seguente:

$\circ$	id	τ
id	id	τ
τ	τ	id

Il gruppo $(S_2, \circ)$ è abeliano ed è isomorfo ai due gruppi con due elementi visti più sopra, ossia il gruppo dei segni di **Z** e il gruppo del pari/dispari.

Un po' più complicata è la tavola di composizione del gruppo S_3. I suoi $6 = 3!$ elementi sono:

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},\ \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Dobbiamo calcolare $6^2 = 36$ prodotti, che riempiono una tabella 6×6. Poiché id è l'elemento neutro, 11 di questi sono immediati: per ogni α si ha $\mathrm{id} \circ \alpha = \alpha,\ \alpha \circ \mathrm{id} = \alpha$, quindi restano 25 prodotti. Anche gli inversi sono immediati, quindi collochiamo subito le altre cinque caselle contenenti l'identità id. Restano 20 prodotti. Calcolandoli pazientemente, otteniamo:

$\circ$	id	ρ_1	ρ_2	τ_1	τ_2	τ_3
id	id	ρ_1	ρ_2	τ_1	τ_2	τ_3
ρ_1	ρ_1	ρ_2	id	τ_3	τ_1	τ_2
ρ_2	ρ_2	id	ρ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	id	ρ_1	ρ_2
τ_2	τ_2	τ_3	τ_1	ρ_2	id	ρ_1
τ_3	τ_3	τ_1	τ_2	ρ_1	ρ_2	id

Si può risparmiare tempo? Osservando la tavola, vediamo che in ogni riga ed in ogni colonna ogni elemento del gruppo compare una ed una sola volta. Vale cioè la *legge di cancellazione*. Questa è una proprietà che hanno tutti i gruppi. Ricordandolo da subito, avremmo potuto calcolare solo qualche prodotto e riempire le caselle rimanenti in modo automatico. Infatti, nella seconda riga, dove ci sono già $\rho_1 \circ \mathrm{id} = \rho_1,\ \rho_1 \circ \rho_2 = \mathrm{id}$, si calcolano $\rho_1 \circ \rho_1 = \rho_2$, $\rho_1 \circ \tau_1 = \tau_3$, dopo di ché restano da collocare τ_1 e τ_2. Quest'ultimo non può occupare la penultima casella, cioè la casella (2,5), perché è già presente nella penultima colonna, al primo posto, quindi deve andare nella (2,6). Allora nella casella (2,5) ci va τ_1. E così via…

Ricordiamo una nozione sui gruppi: l'insieme delle potenze ad esponente intero relativo di un elemento x si denota con $\langle x \rangle$. Il numero di elementi di questo insieme si chiama *ordine* o *periodo* di x e si denota con $|x|$. Se $|x| = n$, si ha $n = \min\left\{ h \in \mathbf{N}^+ \,\middle|\, x^h = 1_G \right\}$. In tal caso si ha: $\langle x \rangle = \left\{ x^0 = 1_G,\ x^1, \ldots,\ x^{n-1} \right\}$.

Infine, se $|x| = n$, si ha $x^k = 1 \Leftrightarrow n$ divide k.

Se due elementi di un gruppo G hanno ordini rispettivamente m ed n, che cosa si può dire dell'ordine del prodotto? In generale non si può dire nulla. Però, se $a, b \in G$ commutano ed hanno ordini finiti, allora $|a \cdot b|$ divide $m = \mathrm{mcm}(|a|, |b|)$.

Infatti, $(a \cdot b)^m = a^m \cdot b^m = 1_G \cdot 1_G = 1_G$. Però in generale non vale l'uguaglianza.

Infatti, se $|a| = k > 1$, preso $b = a^{-1}$, anche $|b| = k$, quindi il mcm degli ordini è k, mentre $|a \cdot b| = 1$. Tuttavia:

PROPOSIZIONE 4.2. Siano G un gruppo ed $a, b \in G$ tali che $\begin{cases} a \cdot b = b \cdot a \\ \langle a \rangle \cap \langle b \rangle = \{1_G\} \end{cases}$. Siano $\begin{cases} h = |a| \\ k = |b| \end{cases}$, $\begin{cases} m = \mathrm{mcm}(h,k) \\ n = |a \cdot b| \end{cases}$. Allora m = n.

Dimostrazione. Abbiamo già visto che n divide m. Dimostriamo che m divide n.

$1_G = (a \cdot b)^n = a^n \cdot b^n \Rightarrow \underbrace{a^n}_{\in\langle a\rangle} = \underbrace{(b^n)^{-1}}_{\in\langle b\rangle}$. Ma $\langle a \rangle \cap \langle b \rangle = \{1_G\}$, dunque $\begin{cases} a^n = 1_G \\ b^n = 1_G \end{cases}$ quindi

$\begin{cases} h \text{ divide } n \\ k \text{ divide } n \end{cases}$ e di conseguenza anche m = mcm(h,k) divide n. Ne segue n = m.

Torniamo ora al gruppo simmetrico S_n, $n \geq 2$, e cerchiamo altre sue proprietà, tra cui gli ordini dei suoi elementi.

Due permutazioni si dicono *disgiunte* se ciascuna fissa gli oggetti spostati dall'altra.

LEMMA 4.3. Siano $\alpha, \beta \in S_n$ disgiunte, allora $\alpha \circ \beta = \beta \circ \alpha$. Inoltre, $|\alpha \circ \beta| = \mathrm{mcm}(|\alpha|, |\beta|)$.

Dimostrazione. Dimostriamo che per ogni $i \in \{1, 2, \ldots, n\}$ si ha $\alpha \circ \beta(i) = \beta \circ \alpha(i)$. Esaminiamo i soli tre casi possibili.

- Se $\alpha(i) = i = \beta(i)$ allora $\begin{cases} \alpha \circ \beta(i) = \alpha(\beta(i)) = \alpha(i) = i \\ \beta \circ \alpha(i) = \beta(\alpha(i)) = \beta(i) = i \end{cases} \Rightarrow \alpha \circ \beta(i) = \beta \circ \alpha(i)$.
- Se $\alpha(i) = j \neq i$ allora β li fissa entrambi, essendo disgiunta da α, pertanto:

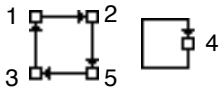
  $$\begin{cases} \alpha \circ \beta(i) = \alpha(\beta(i)) = \alpha(i) = j \\ \beta \circ \alpha(i) = \beta(\alpha(i)) = \beta(j) = j \end{cases} \Rightarrow \alpha \circ \beta(i) = \beta \circ \alpha(i)$$

- Se $\beta(i) = j \neq i$ allora α li fissa entrambi, e si procede allo stesso modo.

L'altra affermazione segue da 4.2, dato che le potenze non banali di α e di β sono disgiunte, quindi solo l'identità è potenza di entrambe.

Sia r un intero positivo, $2 \le r \le n$ e siano dati r elementi distinti $i_1,\dots,i_r \in \{1,2,\dots,n\}$. Col simbolo $(i_1,\dots,i_r)$ denoteremo la permutazione γ che per ogni k, $1 \le k \le n\text{-}1$ porta i_k in i_{k+1}, mentre porta i_r in i_1 e lascia fisso ogni altro oggetto diverso da questi. Questa permutazione si chiama *ciclo* di lunghezza r. Vediamo un ciclo di lunghezza 4 in S_5, con accanto una possibile traduzione grafica:

$$\begin{pmatrix}1&2&3&4&5\\2&5&1&4&3\end{pmatrix} = (1253)$$



Lo stesso ciclo si può scrivere in più modi: $(1253) = (2531) = (5312) = (3125)$, ma se ci accordiamo di cominciare dall'oggetto più piccolo tra quelli spostati, ossia, in questo caso, da 1, abbiamo l'unicità della rappresentazione.

Inoltre, in un prodotto di cicli disgiunti, conveniamo di ordinare i fattori, che come sappiamo commutano, in modo che i loro elementi iniziali siano in ordine crescente. Chiameremo questa *forma standard* del prodotto.

I cicli hanno un ruolo importante nel gruppo simmetrico, simile a quello che hanno i numeri primi in **N**. Si ha infatti:

TEOREMA 4.4. Ogni permutazione diversa dall'identità in S_n o è un ciclo oppure si esprime come prodotto di cicli disgiunti, e questa fattorizzazione è unica se in forma standard.

Dimostrazione. Per illustrare la dimostrazione è utile premettere un esempio, che inoltre spiega come ottenere praticamente la fattorizzazione. Sia $\alpha \in S_9$,

$$\alpha = \begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&3&5&8&6&2&7&9&4\end{pmatrix}$$

Il primo elemento spostato da α è il 2. Abbiamo così:

$$2 \xrightarrow{\alpha} 3 \xrightarrow{\alpha} 5 \xrightarrow{\alpha} 6 \xrightarrow{\alpha} 2$$

che ci fornisce il primo fattore $\gamma_1 = (2356)$, ciclo di lunghezza quattro.

Dopo l'1, fissato ed il 2 e il 3, che fanno parte del ciclo γ_1, c'è il 4:

$$4 \xrightarrow{\alpha} 8 \xrightarrow{\alpha} 9 \xrightarrow{\alpha} 4$$

ed otteniamo un secondo ciclo $\gamma_2 = (489)$, di lunghezza tre.

Gli elementi 5, 6 fanno parte di cicli già considerati. Il primo elemento non ancora trattato è il 7, che è fissato da α, poi l'8 ed il 9 già considerati.

Allora diciamo che $\alpha = \gamma_1 \circ \gamma_2$. Infatti, i due elementi 1, 7 fissati da α sono fissati anche dai due cicli. Quindi anche da $\gamma_1 \circ \gamma_2$. Si ha poi: $\begin{cases} \alpha(2) = 3 \\ \gamma_1 \circ \gamma_2(2) = \gamma_1(\gamma_2(2)) = \gamma_1(2) = 3 \end{cases}$, e più in generale per ogni i = 2, 3, 5, 6 si ha $\gamma_1 \circ \gamma_2(i) = \gamma_1(\gamma_2(i)) = \gamma_1(i) = \alpha(i)$. Infine, per ogni i = 4, 8, 9 si ha $\gamma_1 \circ \gamma_2(i) = \gamma_1(\gamma_2(i)) = \gamma_1(\alpha(i)) = \alpha(i)$. Allora si ha proprio $\alpha = \gamma_1 \circ \gamma_2$.

Tra le due possibilità $\alpha = \gamma_1 \circ \gamma_2 = \gamma_2 \circ \gamma_1$ scegliamo la prima, in cui il primo oggetto spostato dal I fattore è minore del primo oggetto spostato dal II.

Dimostrazione del teorema: per assurdo supponiamo ci siano dei controesempi. Tra questi ne scegliamo uno, α, che sposti il *minimo* numero di oggetti.

Se α non spostasse oggetti, allora α = id, per la quale il teorema è vero. Dunque, ne sposta. Sia i_1 il più piccolo oggetto spostato da α. Abbiamo la seguente successione:

$$i_1 \xrightarrow{\alpha} i_2 \xrightarrow{\alpha} \dots \xrightarrow{\alpha} i_k \xrightarrow{\alpha} \dots$$

Poiché il numero totale n di oggetti è finito, la successione non può proseguire all'infinito trovando oggetti sempre diversi. Pertanto esiste un minimo $m \geq 2$ tale che $i_{m+1} = \alpha(i_m)$ coincide con uno degli oggetti già trovati: $i_{m+1} = i_k$, $k \leq m$.

Se per assurdo fosse $k > 1$ allora $\alpha(i_m) = i_k = \alpha(i_{k-1})$, che essendo α iniettiva implicherebbe $i_m = i_{k-1}$, contro la minimalità di m. Pertanto, k = 1. Allora consideriamo il ciclo $\gamma_1 = (i_1 i_2 \dots i_m)$. Per ciascuno di questi m oggetti si ha $\gamma_1(i_k) = \alpha(i_k)$. Ogni altro oggetto, anche se spostato da α, è fissato da γ_1. L'inverso ${\gamma_1}^{-1}$ del ciclo γ_1 agisce sugli oggetti i_k come α^{-1} e fissa gli altri oggetti. Poniamo allora $\beta = \gamma_1^{-1} \circ \alpha$. Ogni oggetto fissato da α è fissato anche da ${\gamma_1}^{-1}$, ma inoltre $\beta(i_k) = \gamma_1^{-1} \circ \alpha(i_k) = \gamma_1^{-1}(\alpha(i_k)) = \alpha^{-1}(\alpha(i_k)) = i_k$, quindi β fissa anche tutti gli m oggetti i_k. Dunque, β sposta meno oggetti di α, e quindi per β il teorema vale:

esistono $\gamma_2,\ldots,\gamma_r$, cicli disgiunti, tali che $\gamma_1^{-1}\circ\alpha=\beta=\gamma_2\circ\ldots\circ\gamma_r$. Ordiniamo i fattori in forma standard. Allora per β vale anche l'unicità della fattorizzazione.

Di qui segue $\gamma_1^{-1}\circ\alpha=\beta=\gamma_2\circ\ldots\circ\gamma_r$. Questi cicli operano sugli oggetti spostati da β, quindi fissano a loro volta gli oggetti i_k. Ne segue che sono disgiunti da γ_1. Allora $\gamma_1^{-1}\circ\alpha=\gamma_2\circ\ldots\circ\gamma_r\Rightarrow\alpha=\gamma_1\circ\gamma_2\circ\ldots\circ\gamma_r$, prodotto di cicli disgiunti. Ma allora, essendo un controesempio al teorema, per α non deve valere l'unicità. Ossia, si può scrivere (in forma standard) $\alpha=\delta_1\circ\delta_2\circ\ldots\circ\delta_s=\gamma_1\circ\gamma_2\circ\ldots\circ\gamma_r$.

Però, il più piccolo oggetto spostato da α è i_1, che è spostato da δ_1 in $i_2=\alpha(i_1)=\gamma_1(i_1)$; analogamente, per ogni $k<m$ si ha:

$$\delta_1(i_k)=\alpha(i_k)=i_{k+1}=\gamma_1(i_k)\ \text{ e }\ \delta_1(i_m)=\alpha(i_m)=\gamma_1(i_m)=i_1$$

Ne segue $\delta_1=\gamma_1$, quindi $\delta_2\circ\ldots\circ\delta_s=\delta_1^{-1}\circ\alpha=\gamma_1^{-1}\circ\alpha=\beta=\gamma_2\circ\ldots\circ\gamma_r$.

Ma per β vale l'unicità, quindi $s=r$ e anche per ogni $j=2,\ldots,r$ si ha $\delta_j=\gamma_j$. Pertanto anche per α vale l'unicità, contro l'ipotesi che sia un controesempio. Allora α non esiste ed il teorema è vero per ogni elemento di S_n.

Applichiamo ora il risultato precedente per ottenere informazioni sul periodo di una permutazione. Il primo caso è quello di un ciclo, per il quale si ha un semplice risultato: il periodo di un ciclo è uguale alla sua lunghezza. Si ha infatti:

LEMMA 4.5. Sia $\gamma=(i_1,\ldots,i_m)\in S_n$, allora $|\gamma|=m$.

Dimostrazione. Per ogni $k\in\mathbf{N}$, $1\le k\le m-1$ si ha $i_{k+1}=\gamma^k(i_1)$, quindi $\gamma^k\neq id$. Ma $\gamma^m(i_1)=\gamma(\gamma^{m-1}(i_1))=\gamma(i_m)=i_1$. Ne segue $\gamma^m(i_2)=\gamma^m(\gamma(i_1))=\gamma(\gamma^m(i_1))=\gamma(i_1)=i_2$, e così via. Ogni altro oggetto fissato da γ lo è anche dalle sue potenze, quindi anche da γ^m, perciò $\gamma^m=id$. Allora $|\gamma|=m$.

COROLLARIO 4.6. Sia $\alpha\in S_n$, $\alpha=\gamma_1\circ\gamma_2\circ\ldots\circ\gamma_r$ prodotto di cicli disgiunti. Allora $|\alpha|=\mathrm{mcm}(|\gamma_1|,|\gamma_2|,\ldots,|\gamma_r|)$

Dimostrazione. Procediamo per induzione rispetto ad r. Se $r = 1$ è ovviamente vero. Sia $r > 1$ e poniamo $\beta = \gamma_2 \circ \ldots \circ \gamma_r$. Le due permutazioni β e γ_1 sono disgiunte, quindi commutano ed inoltre, operando su oggetti distinti, non hanno potenze uguali se non l'identità. Pertanto, sono soddisfatte le condizioni della Proposizione 4.3. e si ha: $|\alpha| = \mathrm{mcm}(|\gamma_1|, |\beta|)$. Poiché $\beta = \gamma_2 \circ \ldots \circ \gamma_r$ è prodotto di r-1 cicli disgiunti, per ipotesi induttiva si ha $|\beta| = \mathrm{mcm}(|\gamma_2|, \ldots, |\gamma_r|)$, quindi $|\alpha| = \mathrm{mcm}(|\gamma_1|, |\beta|) = \mathrm{mcm}(|\gamma_1|, |\gamma_2|, \ldots, |\gamma_r|)$.

Due problemi interessanti, ma difficili e in un certo senso inversi l'uno dell'altro, sono:

I. Qual è il massimo periodo m degli elementi di S_n?

II. Dato un intero positivo $m \geq 2$, qual è il minimo intero positivo n tale che in S_n ci sia un elemento di periodo m?

Nel primo problema si tratta di esprimere n come somma di interi positivi aventi il minimo comune multiplo massimo possibile. Nel secondo, si tratta alla fine di scomporre m in fattori la cui somma sia minima.

Per esempio, se n = 10 si può scrivere 10 = 5+3+2, quindi c'è un elemento $\alpha = (12345) \circ (678) \circ (9\ 10)$ di periodo $\mathrm{mcm}(5,3,2) = 30$. Si può fare di meglio?

Sia m = 42. Allora $\underbrace{42}_{42} = \underbrace{2 \cdot 21}_{23} = \underbrace{3 \cdot 14}_{17} = \underbrace{6 \cdot 7}_{13} = \underbrace{2 \cdot 3 \cdot 7}_{12}$, pertanto in S_{12} c'è un elemento di periodo 42, $\alpha = (1234567) \circ (8\ 9\ 10) \circ (11\ 12)$. E per n < 12 esiste?

L'insieme dei cicli, dunque, *genera* il gruppo simmetrico S_n, nel senso che ogni elemento diverso dall'identità o è un ciclo o è prodotto di cicli. Ma quanti sono i cicli? Per $2 \leq k \leq n$ si comincia con lo scegliere $\{i_1, \ldots, i_k\} \subseteq \mathbf{N}_n$, e si può fare la scelta in $C_{n,k} = \binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$ modi diversi. Con quei k elementi, scelto come elemento iniziale di ogni ciclo il minimo di questi k elementi, gli altri k-1 si possono disporre tutti i modi possibili, ossia $(k-1)!$ Allora, il principio di moltiplicazione ci dà $(k-1)! \cdot \frac{n!}{k! \cdot (n-k)!} = \frac{n!}{k \cdot (n-k)!} = \frac{D_{n,k}}{k}$ cicli di lunghezza k.

Allora, in tutto ci sono $\sum_{k=2}^{n} \frac{D_{n,k}}{k}$ cicli.

ESEMPIO 4.7. Per n = 4 ci sono sei cicli di lunghezza 2, otto di lunghezza 3, sei di lunghezza 4; dunque, in tutto, 20 cicli su 24 permutazioni. Le restanti quattro formano il sottogruppo $K = \{id, (12)\circ(34), (13)\circ(24), (14)\circ(23)\}$, detto *sottogruppo di Klein* di S_4.

Tale sottogruppo è anche *normale* in S_4, ossia per ogni $\beta \in S_4$ si ha $\beta \circ K = K \circ \beta$, dove $\beta \circ K = \{\beta \circ \alpha \mid \alpha \in K\}$ e analogamente per $K \circ \beta$. Se denotiamo con a, b, c i tre elementi $\neq$ id, si ha la tavola seguente, che dice che K non è ciclico.

$\circ$	id	a	b	c
id	id	a	b	c
a	a	id	c	b
b	b	c	id	a
c	c	b	a	id

Se per un sottogruppo K di un gruppo G e per ogni $x \in G$ si ha $Kx = xK$ allora K si dice sottogruppo *normale* di G. Per un gruppo abeliano tutti i sottogruppi sono normali. Per un gruppo non abeliano, invece, sono normali il sottogruppo banale $\{1_G\}$ e G stesso, ma per un sottogruppo proprio l'essere normale è una proprietà rara. Per indicare che K è un sottogruppo normale in G si scrive $K \triangleleft G$.

Non si può fare di meglio? Certo. Chiamiamo *trasposizione* un ciclo di lunghezza 2. Abbiamo dapprima un lemma:

LEMMA 4.8. a) Ogni ciclo di lunghezza m > 2 è prodotto di m-1 trasposizioni.

b) Ogni permutazione è prodotto di trasposizioni.

Dimostrazione. a) Si ha $\gamma = (i_1 i_2 \dots i_m) = (i_1 i_m)\circ(i_1 i_{m-1})\circ\cdots\circ(i_1 i_2)$

b) Si ha innanzi tutto $id = (12)\circ(12)$ e $(ij) = (ij)\circ(ij)\circ(ij)$. Sia $\alpha \neq$ id una permutazione che non sia una trasposizione. Si scomponga α in prodotto di cicli disgiunti: ciascun ciclo o è una trasposizione oppure è prodotto di trasposizioni, da cui l'asserto.

ESEMPIO 4.9.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 3 & 5 & 8 & 6 & 2 & 7 & 9 & 4 \end{pmatrix} = (2356)\circ(489) = (26)\circ(25)\circ(23)\circ(49)\circ(48)$$

Ma si ha anche $\alpha = (17)\circ(26)\circ(25)\circ(23)\circ(17)\circ(49)\circ(48)$, ossia il numero dei fattori non è univocamente determinato da α.

OSSERVAZIONE 4.10. Il lemma precedente dice che il gruppo simmetrico S_n, oltre ad essere generato dall'insieme dei cicli, lo è anche dall'insieme delle trasposizioni. Queste ultime sono soltanto $\binom{n}{2} = \frac{n\cdot(n-1)}{2}$. Si può dimostrare che S_n si può generare anche con solo *due elementi*: i cicli $(12\ldots n)$ ed (12).

La fattorizzazionbe mediante trasposizioni non è unica, ma qualcosa di unico c'è. Sia $\alpha = \tau_1\circ\tau_2\circ\ldots\tau_r$, prodotto di r trasposizioni. Sappiamo dall'Algebra Lineare che se in una matrice quadrata scambiamo di posto due colonne, il determinante cambia segno. Partiamo dalla matrice identità $I_n = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & 1 \end{bmatrix}$ ed applichiamo dapprima alle sue colonne lo scambio τ_r, poi alla matrice ottenuta lo scambio τ_{r-1}, e così via, fino ad ottenere alla fine una matrice M_α, il cui determinante è $(-1)^r$ e che in definitiva è quella ottenuta applicando alle colonne di I_n la permutazione α. Sia ora $\alpha = t_1\circ t_2\circ\ldots t_s$ un'altra fattorizzazione di α come prodotto di trasposizioni; procedendo come prima, si ottiene di nuovo la matrice M_α, il cui determinante è ora $(-1)^s$. Dato che il determinante è unico, deve essere $(-1)^r = (-1)^s \Rightarrow r \equiv s \pmod 2$. Ossia abbiamo dimostrato il seguente:

LEMMA 4.11. Se scomponiamo $\alpha \in S_n$ in un prodotto di trasposizioni, anche se il numero dei fattori cambia, non cambia la sua parità: se una permutazione è prodotto di un numero pari di trasposizioni, non è prodotto di un numero dispari di trasposizioni.

Chiamiamo *pari* le permutazioni prodotto di un numero pari di trasposizioni, e *dispari* le altre.

NOTE. A) Per trovare se una $\alpha \in S_n$ è pari o dispari, la scomponiamo dapprima in cicli disgiunti: $\alpha = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_r$, con $r \geq 1$, $|\gamma_k| = m_k$, $1 \leq k \leq r$. Poniamo poi

$N(\alpha) = \sum_{k=1}^{r} (m_k - 1) = \sum_{k=1}^{r} m_k - r$ = differenza tra il numero degli elementi spostati da α e il numero dei suoi cicli. Poniamo poi per completezza N(id) = 0. Allora α è pari se $N(\alpha)$ è pari; in caso contrario è dispari.

B) In alcuni testi si parla del *segno* di una permutazione $\alpha \in S_n$; possiamo considerarlo semplicemente come il determinante della matrice M_α. In definitiva, per una $\alpha \in S_n$ sono equivalenti:

a) $N(\alpha)$ è pari
b) $\text{sign}(\alpha) = 1$
c) α è prodotto di un numero pari di trasposizioni.

Denotiamo con A_n l'insieme delle permutazioni pari di S_n. Si ha:

TEOREMA 4.12. a) A_n costituisce un sottogruppo di S_n,
b) $|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$
c) $A_n \lhd S_n$

Dimostrazione. a) L'identità è pari, quindi $\in A_n$. Date $\alpha,\beta \in A_n$, esistono trasposizioni τ_i, t_j, $1 \leq i \leq 2h$, $1 \leq j \leq 2k$, tali che $\begin{cases} \alpha = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2h} \\ \beta = t_1 \circ t_2 \circ \cdots \circ t_{2k} \end{cases}$. Allora, $\alpha \circ \beta = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2h} \circ t_1 \circ t_2 \circ \cdots \circ t_{2k}$ è prodotto di 2h+2k trasposizioni, quindi è pari. Infine, $\alpha^{-1} = \tau_{2h} \circ \tau_{2h-1} \circ \cdots \circ \tau_1$ è pari. Pertanto, $A_n \leq S_n$.

b) Poniamo $\tau = (12)$, che è dispari. Allora ogni $\beta \in A_n \circ \tau$ è dispari perché prodotto di 2h+1 trasposizioni. Dunque ci sono almeno $|A_n \circ \tau| = |A_n|$ permutazioni dispari. D'altra parte, se β è una permutazione dispari, prodotto di 2k+1 trasposizioni, allora $\alpha = \beta \circ \tau$ è pari, perché prodotto di 2k+2 trasposizioni; pertanto $\beta = \alpha \circ \tau \in A_n \circ \tau$ e quindi le permutazioni dispari appartengono tutte al *laterale* $A_n \circ \tau = \{\alpha \circ \tau \mid \alpha \in A_n\}$. Ne segue che tutti gli elementi fuori di A_n, ossia quelli di $S_n \setminus A_n$, costituiscono il laterale $A_n \circ \tau$, equipotente ad A_n. Ma allora,

$$n! = |S_n| = |A_n| + |S_n \setminus A_n| = 2 \cdot |A_n| \Rightarrow |A_n| = \frac{|S_n|}{2} = \frac{n!}{2}.$$

c) Come sopra, anche il laterale sinistro $\tau \circ A_n$ è costituito da tutte le permutazioni dispari, quindi $\tau \circ A_n = A_n \circ \tau$. Il solo altro laterale di A_n è se stesso, dunque tutti i suoi (due) laterali destri coincidono con i corrispondenti laterali sinistri ed A_n è normale in S_n.

NOTA. Come detto, ogni gruppo contiene come sottogruppi normali il sottogruppo banale $\{1_G\}$ e se stesso. Se G non è abeliano, i sottogruppi normali di solito sono rari. Nel gruppo simmetrico S_n c'è anche il sottogruppo alterno A_n e, con la sola eccezione del caso $n = 4$, questi sono gli unici sottogruppi normali. Per $n = 4$ c'è anche il sottogruppo di Klein. La teoria di Galois mostra l'importanza di questa scarsità di sottogruppi normali nella impossibilità di trovare formule risolutive per radicali delle equazioni algebriche di grado ≥ 5.

Il seguente risultato mostra l'importanza dei gruppi simmetrici S_n: nel loro "ventre" sono contenuti sottogruppi isomorfi ad ogni gruppo d'ordine n.

TEOREMA 4.13. (Cayley). Sia G un gruppo d'ordine n. Allora G è isomorfo ad un sottogruppo del gruppo simmetrico S_n.

Dimostrazione. Ad ogni $a \in G$ associamo la funzione $f_a : G \to G$, definita da: $f_a(x) = a \cdot x$. La legge di cancellazione assicura che è iniettiva e quindi anche suriettiva, essendo G finito. Allora $f_a \in S_G$, gruppo simmetrico sull'insieme G. La funzione $\rho : G \to S_G$, definita da $\rho(a) = f_a$ è iniettiva, dato che: $\rho(a) = \rho(a') \Rightarrow f_a = f_{a'} \Rightarrow a = f_a(1_G) = f_{a'}(1_G) = a'$.

Inoltre, per ogni a, a', x∈G, $\rho(a \cdot a')(x) = f_{a \cdot a'}(x) = (a \cdot a') \cdot x = a \cdot (a' \cdot x) = f_a(f_{a'}(x)) =$

$= \rho(a) \circ \rho(a')(x) \Rightarrow \rho(a \cdot a') = \rho(a) \circ \rho(a')$. Allora, ρ è un isomorfismo tra G e la sua immagine $\rho(G)$ in S_G, che è isomorfo ad S_n. Dunque, in S_n c'è un sottogruppo d'ordine n isomorfo a G.