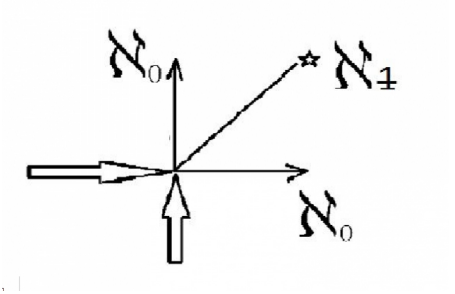
Omaggio a Umberto Cibien

(*mio amico fraterno*)
(PARTE TERZA)

Voglio ricordarti così, come quando eravamo giovani e forti, quando le nostre menti viaggiavano alla velocità della luce su teorie delle quali solo in poche persone al mondo sono state in grado di compiere le nostre evoluzioni! Come acrobati eravamo in grado di far compiere alle nostre intelligenze dei voli sui più complicati concetti, come anime gemelle giocavamo sui campi della conoscenza! Adesso hai calcolato con estrema precisione l'integrale della gaussiana della parte concernete la tua permanenza su questo pianeta, lo hai fatto per liberarti in una geodetica esistenziale dove neanche i limiti della libertà saranno in grado di contenere il tuo spirito. Sarai sempre con me, nella mia mente e nel mio cuore. Adesso è grande il mio dolore, ma lo saprò superare! Torneremo ancora a giocare!
Ciao Umberto Cibien!



LE MATEMATICHE PURE

Qui troverete una serie di articoli dedicata ad uno degli argomenti più affascinanti delle matematiche pure: la teoria degli insiemi infiniti, dovuta principalmente a ***Georg Cantor***.
Sarà un percorso lungo, e all'inizio forse noioso.
Parleremo di insiemi, corrispondenze, relazioni di equivalenza in modo semplice ed intuitivo, fino ad arrivare a dimostrare che gli insiemi infiniti non sono tutti ugualmente numerosi, ma esisto vari livelli (ordini) di infinito.
Gli articoli sono alla portata di tutti (o quasi); ho cercato di usare il minimo formalismo .
La trattazione introduttiva è minima, ed è quella che serve per arrivare al risultato finale.
Non è mia presunzione tenere delle lezioni di matematica pura, ma solo divulgare un argomento forse poco noto, che chi vuole potrà approfondire.
L'obiettivo è anche quello di rendere più simpatica la tanto odiata matematica che a volte ci è stata propinata come un ammasso informe di tecniche di calcolo senza alcun riferimento storico-culturale.
In realtà la matematica è fantasia e intuizione.
Il percorso che porta a un risultato non è mai lineare: ci sono intuizioni, errori, aggiustamenti, risultati intermedi.
Vedremo cosa si inventa Cantor per dimostrare che i numeri razionali (le frazioni) sono tanti quanti i numeri naturali (0,1,2,3,4,5,...), fra l'altro restando sorpreso egli stesso del risultato.

In questa fase della trattazione verranno toccati vari argomenti attinenti il contesto del discorsoe gli argomenti sarannno suddivisi per parti.

1. Parte prima:relazioni e classi di equivalenza
2. Parte seconda:la definizione di numero cardinale
3. Parte terza: I gruppi della matematica moderna
4. Parte quarta:altri esempi di gruppi
5. Parte quinta: I gruppi liberi 1/2
6. Parte quinta: I gruppi liberi 2/2
7. Parte sesta:i campi algebrici
8. Parte settima: Il campo dei numeri complessi 1/2
9. Parte settima: Il campo dei numeri complessi 2/2
10. Parte ottava: i punti impropri della geometria proiettiva
11. Parte nona: il gruppo delle curve ellittiche 1/2
12. Parte nona: il gruppo delle curve ellittiche 2/2

Relazioni e classi di equivalenza

Le relazioni e le classi di equivalenza aprono un altro capitolo estremamente importante della teoria degli insiemi.
Tramite le classi di equivalenza è stato possibile formalizzare correttamente le definizioni di numero intero, razionale ed altro ancora.
In poche parole costruire una base solida della matematica.
Prima di parlare di relazioni di equivalenza, devo introdurre un altro concetto che riguarda gli insiemi:

La partizione di un insieme.

Una partizione di un insieme **X** è una divisione di **X** in sottoinsiemi, dette classi della partizione, che "***coprono***" **X** senza sovrapporsi.
Tali sottoinsiemi sono non vuoti, ovvero hanno almeno un elemento.

Dall'immagine è chiaro di cosa stiamo parlando: abbiamo dei sottoinsiemi (non vuoti) di un insieme A che sono disgiunti (comunque ne prendiamo due, non hanno elementi in comune) e tali che la loro unione dia tutto X.
Facciamo comunque un esempio : sia **A ={0,1,23,4,5,6,7,8,9,10}** ;

I tre sottoinsiemi:
B={0,1,2,3,4}; **C={5,6,7,8}**; **D={9,10}**; costituiscono una partizione di **A**
Infatti non sono vuoti, non hanno elementi in comune e la loro unione dà tutto **A**.

Relazioni tra gli elementi di un insieme.

Consideriamo un insieme qualsiasi; potremmo prendere per esempio gli abitanti di una certa città.
Questi sono gli elementi di un certo insieme.
Ma cosa può legarli fra loro? Una relazione.
Prendiamo due elementi **a** e **b**.
Per esempio:
"***a è sposato con b***" è una relazione. "**a è figlio di b**" rappresenta un' altra relazione fra due elementi dell'insieme.
Non farò una trattazione formale delle relazioni, che esula dagli obiettivi che vogliamo raggiungere.
Tratteremo inoltre solo relazioni definite fra elementi di uno stesso insieme **A**.
Possiamo anche pensare di rappresentare una relazione tramite una tabella:

A	a1	a2	a3	a4
a1				*
a2	*			
a3		*		
a4			*	

Infatti una relazione altro non è che un sottoinsieme di **A x A** (insieme prodotto di **A**), ovvero formato dalle coppie che stanno appunto in relazione fra loro.

Le proprietà delle Relazioni di equivalenza.

Un tipo particolare di relazione fra due elementi di uno stesso insieme è quella di equivalenza, che ha delle particolari caratteristiche (o proprietà).
(Se **a** è in relazione di equivalenza con **b** scriveremo a $\sim$ b)
Una relazione si dice di equivalenza se sono valide le seguenti proprietà:

Proprietà riflessiva:

a $\sim$ a (ovvero **a** è in relazione con se stesso)

Proprietà simmetrica:

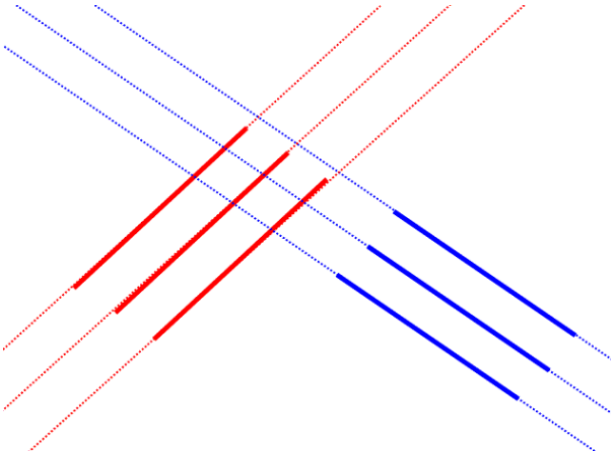
se a $\sim$ b allora b $\sim$ a (se **a** è in relazione con **b**, allora anche **b** è in relazione con **a**)

Proprietà transitiva:

se **a** $\sim$ **b e b** $\sim$ **c** allora **a** $\sim$ **c** (se a è in relazione con **b**, **b** è in relazione con **c**, allora **a** è in relazione con **c**)
Notiamo che per il fatto che è riflessiva, una relazione di equivalenza è definita su tutto **A**; infatti c'è sempre almeno un elemento che è in relazione con **x**, ed è **x** stesso.

Esempi.

"*a è figlio di b* " **non** è una relazione di equivalenza; non vale infatti la proprietà simmetrica (se **a** è figlio di **b**, **b** non può essere figlio di **a**) e nemmeno quella riflessiva (**a** non può essere figlio) di se stesso.
*Invece se **A** è l'insieme delle rette nel piano, il parallelismo fra rette è una relazione di equivalenza.*
Infatti;
Proprietà riflessiva: una retta è parallela a se stessa.
Proprietà simmetrica: se a è parallela a b, chiaramente b è parallela ad a.
Proprietà transitiva: se a è parallela a b, e b è parallela a c, allora a è parallela a c.



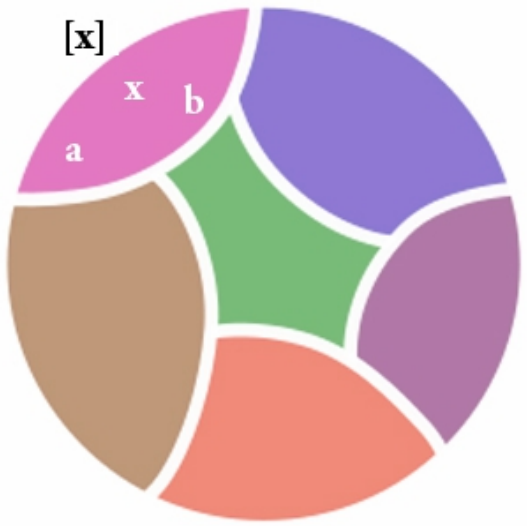
Consideriamo l'insieme delle automobili di una certa città.
La relazione "hanno lo stesso colore" è una relazione di equivalenza.
Proprietà riflessiva: infatti **a** ha lo stesso colore di **a.**
Proprietà simmetrica: se **a** e **b** hanno lo stesso colore, lo stesso dicasi per **b** e **a**
Proprietà transitiva: se **a** e **b** hanno lo stesso colore, e **b** e **c** hanno lo stesso colore, allora anche **a** e **c** hanno lo stesso colore.

Classi di equivalenza.

Un sottoinsieme di **A** che contiene tutti e soli gli elementi equivalenti a un qualche elemento **x** di **A** prende il nome di ***classe di equivalenza*** di **x** per la relazione $\sim$.

Si indica una classe di equivalenza con: **[x]**.

In una classe di equivalenza tutti gli elementi in essa contenuti sono tra loro equivalenti.



Classi di equivalenza di automobili con lo stesso colore

Se torniamo all'esempio delle macchine dello stesso colore, e supponiamo che **x** sia una macchina di colore fucsia , allora l'insieme delle macchine di colore fucsia è costituito da **{x,a,b}** e lo indichiamo con **[x]**.
La scelta del rappresentante, in questo caso **x**, non conta; se prendiamo **a** o **b**, la classe (colore) non cambia.
Volevo dimostrare formalmente quanto asserito sopra:

Se x $\sim$y allora [x]=[y]

Scegliamo un elemento $z \in [x]$, allora **z**$\sim$**x**. Ma **x**$\sim$**y** ma allora per la proprietà transitiva **z**$\sim$**y**, quindi $z \in [y]$, quindi $[x] \subseteq [y]$ (tutti gli elementi di **[x]** appartengono a **[y]**.
Allo stesso modo prendiamo un $w \in [y]$, allora **w**$\sim$**y**; per la proprietà simmetrica **y**$\sim$**x** e per la transitiva **w**$\sim$**x** dunque $w \in [x]$ quindi $[y] \subseteq [x]$. Pertanto **[x]=[y].**

Insieme quoziente di una relazione di equivalenza.
L'insieme delle classi di equivalenza su **A** si chiama **insieme quoziente** di **A** per la relazione $\sim$, e viene talvolta indicato con l'espressione **A /** $\sim$.
Si dimostra che esso rappresenta una partizione di **A** (per non appesantire il discorso ho messo la dimostrazione in appendice).
Il nome (quoziente) deriva dal fatto che agendo sulle classi dividiamo l'insieme.
Sempre nel caso delle macchine, l'insieme quoziente non è altro che l'insieme di tutti i colori delle macchine di una certa città.
Nel caso di parallelismo fra rette, la classe non è che la direzione della retta nel piano.
L'insieme quoziente è invece l'insieme di tutte le direzioni possibili.
Nel prossimo articolo useremo il concetto di classe di equivalenza per definire la cardinalità dell'insieme senza contare i suoi elementi.

Appendice

Questa appendice è un po' formale; chi vuole una dimostrazione rigorosa del fatto che l'insieme quoziente è una partizione di **A** la legga pure, ma non è necessaria per comprendere i prossimi argomenti.

L'insieme quoziente è una partizione di A.
Riscriviamo la definizione di classe di equivalenza in modo un po' più formale.
[x]={$y \in A$ tali che **y** $\sim$ **x** } ricordiamo che questi sono **sottoinsiemi** di **A**.
Ricordiamo anche che abbiamo dimostrato che: **Se x** $\sim$ **y allora [x]=[y]**
Dobbiamo dimostrare tre cose:

1 **La classe [x] non è mai vuota**
Infatti , dato un x appartenente ad A, per la proprietà simmetrica x $\sim$ x. quindi **[x]** contiene almeno un elemento.

2 **Se [x] , [y] sono le classi di x,y , la loro intersezione è vuota, oppure coincidono.**

Supponiamo che l'intersezione fra **[x]** e **[y]** dia l'elemento **z**, allora **z** $\sim$ **x** (perché (**z** appartiene a **[x]**), **x** $\sim$ **z** (per la proprietà simmetrica) **z** $\sim$**y** (perché **z** appartiene anche a **[y]** per la transitiva abbiamo che **x** $\sim$ **y** .

Ma abbiamo dimostrato sopra che **se x $\sim$ y allora [x]=[y] ,** quindi coincidono.

3) L'unione di tutte le classi dà l'insieme A
l'unione di tutte le classi è contenuta in : $\bigcup [x] \subseteq A$ (sono sottoinsiemi di **A**)
Non è possibile che $\bigcup [x] \subset A$ ovvero : se l'unione fosse contenuta propriamente in **A**, allora esisterebbe un **x** appartenente ad **A** tale che **x** non è in relazione con nessun **y** appartenente ad **A**, ma sappiamo che **x** $\sim$ **x** per la proprietà riflessiva.

La definizione di numero Cardinale

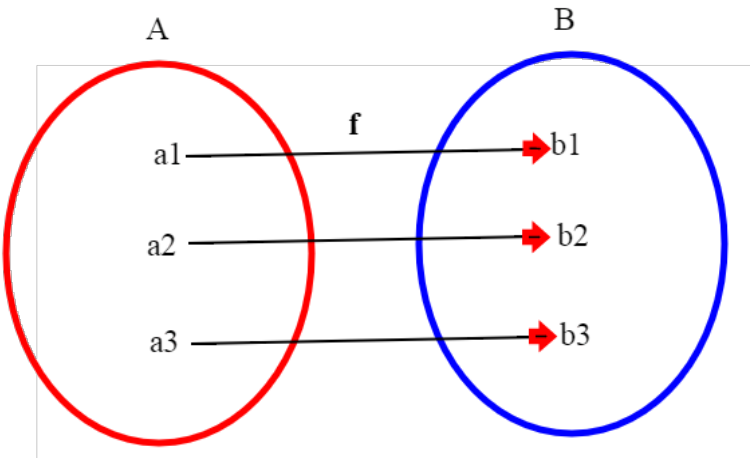
In questo articolo ci proponiamo di dare la definizione di numero cardinale usando il concetto di classe di equivalenza visto nell'articolo precedente. Questo modo di definire i concetti astratti come classi di equivalenza risale a Friedric Ludwig Gottlob Frege matematico, logico e filosofo tedesco, padre della logica matematica moderna ed è molto usato nella teoria degli insiemi.
Potrebbe servire leggere prima questo articolo “Corrispondenze e funzioni”.
Pensiamo agli insiemi che possono essere messi in corrispondenza biunivoca fra di loro.
Questa è una relazione di equivalenza.

Proprietà riflessiva

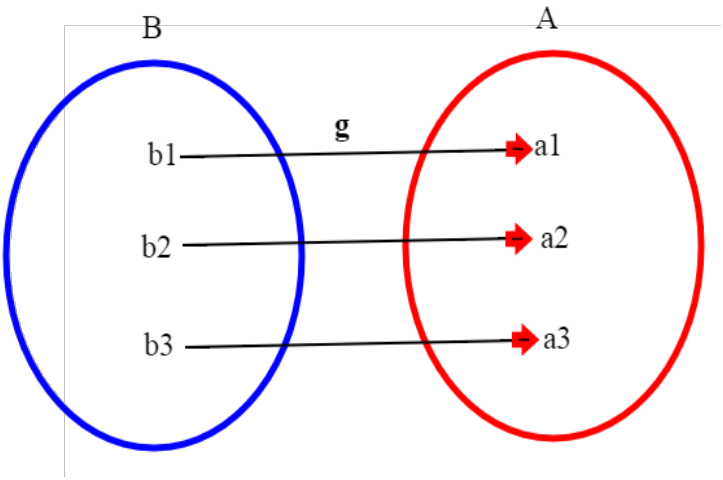
Chiaramente **A** può essere messo in corrispondenza biunivoca con se stesso. (mando ogni elemento **a** di **A** in **a** (**a--->a**)

Proprietà simmetrica

Se **A** è in corrispondenza biunivoca con **B**, allora **B** è in corrispondenza biunivoca con **A**.



Corrispondenza diretta da A a B

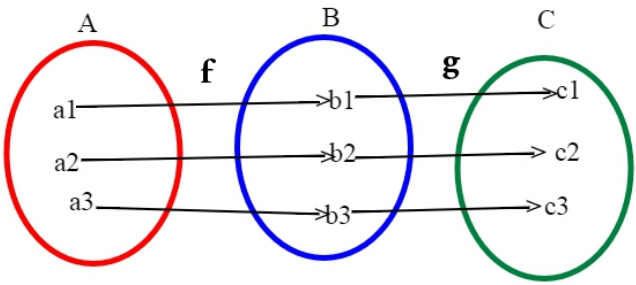


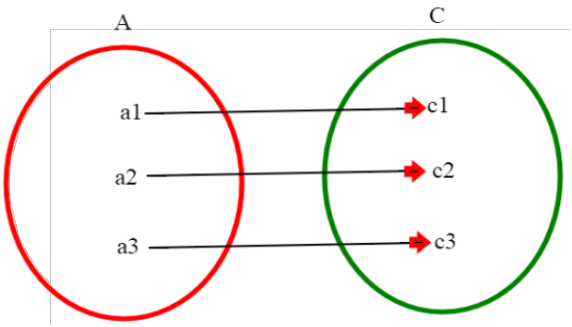
Corrispondenza inversa da B a A

Se **A** è in corrispondenza biunivoca con **B**, la funzione **f** che va da **A** a **B** copre tutto **B** e manda elementi distinti in elementi distinti; costruiamo una **g** che invece va da **B** in **A**; dato un **b** appartenente a **B** sappiamo che **b=f(a)** (notiamo che questo **a** è unico, perché **f** è iniettiva) , quindi poniamo **g(b)=a**.
Il fatto poi che **a** sia unico ci assicura che **g** sia una funzione, ovvero che associ ad ogni elemento del dominio uno e **un solo** elemento del codominio.
g si chiama **funzione inversa di f**, e si indica con f^{-1}.

Proprietà transitiva

se **A** è in corrispondenza biunivoca con **B**, e **B** è in corrispondenza biunivoca con **C**, allora **A** è in corrispondenza biunivoca con **C**.





Per dimostralo rigorosamente basta definire una terza funzione **z** (che va da **A** a **C**) in questo modo:

z(a)=g(f(a)); questa funzione si chiama **funzione composta** di **f** e **g**.
(esempio: **a1-->b1---->c1**)

1) **z è iniettiva.**
infatti se **a1**$\neq$**a2**, essendo **f** iniettiva, **f(a1)**$\neq$**f(a2)** e quindi essendo anche **g** iniettiva **g(f(a1))**$\neq$ **g(f(a2)).**

2) **z è suriettiva**.
Infatti se prendiamo un qualsiasi **c** che appartiene a **C**, sappiamo (**g** è suriettiva) che esiste un **b** tale che **c=g(b)**; ma anche **f** è suriettiva, quindi esiste un **a** tale che **f(a)=b**; **z(a)=g(b)=g(f(a))**.

Quindi è una **relazione d'equivalenza**.
Nel caso della relazione di equivalenza fra insiemi che possono essere messi in corrispondenza biunivoca, la classe non è altro che il **numero Cardinale** dell'insieme.
Nel caso finito esso non è altro che quello che abbiamo sempre chiamato numero di elementi di un insieme; ma Cantor estese questa definizione anche agli insiemi infiniti.

Gruppi della matematica moderna

Continuiamo il nostro percorso sui prerequisiti fondamentali delle matematiche pure.
Dopo esserci occupati di relazioni di equivalenza, fondamentali in ogni settore delle matematiche astratte, e di funzioni biunivoche (definizione di numero cardinale) ci occuperemo di una struttura molto nota e molto usata nella matematica moderna, quella di **gruppo.**

Un po' di storia

Lo studio dei gruppi è cominciato in Francia all'inizio dell'800, in relazione alla ricerca di formule risolutive per le equazioni algebriche, e ha riguardato inizialmente i gruppi finiti di permutazioni,iniziati da ***Évariste Galois*** negli

anni 1830.
In seguito a contributi provenienti da altri settori della matematica come la teoria dei numeri e la geometria, la nozione di gruppo fu generalizzata e definita stabilmente attorno al 1870.
Prima di dare la definizione di gruppo, alcuni concetti preliminari.

Operazione binaria interna

Dato un insieme **A**, una operazione binaria interna altro non è che una corrispondenza che ha come dominio l'insieme prodotto di **A**, e come codominio **A**; se indichiamo con ***** tale corrispondenza: $* : A \times A \to A$, essa associa alla coppia **(a,b)** il risultato di una certa operazione che indichiamo con **a*b**
(in pratica **a*b=*(a,b)**.
E' importante notare che il risultato dell'operazione resta all'interno dell'insieme; questa è la proprietà basilare di ciò che stiamo definendo, il fatto appunto che gli elementi di un insieme formano proprio un "**gruppo**".
Se ad esempio consideriamo l'operazione **"-"** ovvero la sottrazione **(a-b)**, essa è ***una operazione binaria interna*** se come insieme **A** prendiamo **Z** (interi);
Ma ***se come insieme prediamo quello dei numeri naturali N questo non è vero*** (se **a<b, a-b<0** che ***non è un numero naturale***.

Proprietà dell'operazione binaria interna

Proprietà associativa

Se a,b,c sono elementi di A, allora (a*b)*c=a*(b*c)
Cosa vuole dire? Vuol dire che è indifferente se abbiamo tre elementi **a,b,c**, ***eseguire prima l'operazione fra a e b e tale risultato comporlo con c***, oppure comporre **a** con il risultato dell'operazione con **b** e **c**.
Lo abbiamo visto con i numeri e le usuali operazioni fin dalle scuole elementari; se devo fare **1+5+2** è indifferente fare **1+5=6**, e poi **6+2=8**, oppure **5+2=7**, **1+7=8**.
Questo non è sempre vero; basti pensare alla sottrazione definita nei numeri relativi. In essa ad esempio fare **(1-5)-2** che dà **-6** non è la stessa cosa che fare **1-(-5-2)** che dà **8**.

Elemento neutro

Esistenza di un elemento **e** appartenente ad **A**, tale che **e*a=a*e=a *qualsiasi sia a appartenente ad A***.
Pensando ai numeri, se l'operazione è la somma, l'elemento neutro è lo zero **(a+0=a)**, se invece consideriamo la moltiplicazione **e**=1 **(a*1=a)**.

Inverso

Esistenza di un elemento a^{-1} detto inverso, che sia tale che $a^{-1} * a = a * a^{-1} = e$, qualsiasi sia **a**.
Sempre nel caso numerico, **se l'operazione è la somma e siamo nell'insieme Z l'inverso di a è -a (a+-a=0)**; **se l'operazione è il prodotto** e siamo nell'insieme **Q dei razionali**, **l'inverso di a è proprio quello che chiamiamo inverso**, ovvero $a^{-1} = \frac{1}{a}$, infatti il prodotto dà **1** (dobbiamo però limitarci ai numeri $a \neq 0$ per avere un gruppo, ossia considerare **Q\{0})**.

Commutatività

L'operazione * è detta commutativa, se qualsiasi siano **a,b** appartenenti ad **a**, **a*b=b*a**.
La somma e il prodotto di numeri interi sono operazioni commutative; la sottrazione no.

Definizione di gruppo

Dato un insieme **A** in cui sia **definita una operazione binaria interna ***, diciamo che la coppia **(A,*)** è un ***gruppo*** se l'operazione * soddisfa le seguenti condizioni:

1. * è associativa
2. per * esiste l'elemento neutro
3. per ogni **A** esiste l'inverso

se inoltre vale anche la proprietà commutativa, il gruppo si dice ***abeliano*** (o commutativo).
L'ordine di un gruppo **A** (identifichiamo il gruppo con l'insieme in cui è de-

finita l'operazione *) non è altro che la **cardinalità dell'insieme A**; nel caso **A** sia finito è il numero di elementi di **A**, altrimenti è la cardinalità che abbiamo visto negli infiniti di Cantor.
La cardinalità di A si indica sempre con |A|.

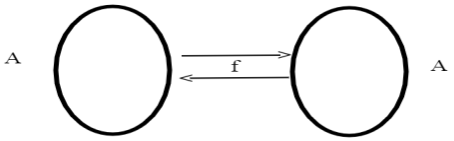
Un piccolo esercizio: ***in un gruppo l'inverso di un elemento è unico***.
Supponiamo per assurdo di avere due inversi per a;indichiamo con **a',a''** i due inversi di **a**.
allora
$$a'' = a'' \cdot e = a'' \cdot (a \cdot a') = (a'' \cdot a) \cdot a' = e \cdot a' = a'$$
dove la terza eguaglianza vale per la proprietà associativa. Dunque **a''=a'**.
Vi lascio verificare che l'insieme **Z** degli interi con l'usuale somma **(Z,+)** è un gruppo, anzi è un gruppo abeliano (commutativo).
Così pure $(Q - \{0\}, \cdot)$ ossia **Q** privato dello zero con l'usuale moltiplicazione è un gruppo abeliano.
Per noi sarà più interessante trattare gruppi non numerici.
Cominciamo dai gruppi **simmetrici**, in quanto lo studio dei gruppi partì proprio da qui.
Prima un'altra definizione.

Sottogruppi

Se (G, °) è un gruppo, un sottogruppo di G è una struttura (H, °), dove H è un sottoinsieme di G, chiuso rispetto alla operazione ° definita in G e contenente e_G e l'inverso di ogni suo elemento.
Si ha così che (H, °) è un gruppo e $e_H = e_G$.

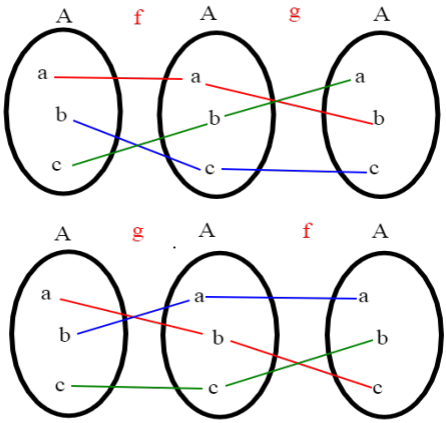
I gruppi simmetrici

Dato un insieme A, consideriamo (tutte)le funzioni biunivoche **f: A--->A**



(per un chiarimento dettagliato sulle funzioni biunivoche vedere l'articolo sulla definizione di numero cardinale)

Chiamiamo S_A l'insieme di queste funzioni biunivoche.
Prendiamo adesso come operazione tra due funzioni **°:**S_A**X**S_A--->S_A, la composizione di due funzioni biunivoche **f,g**. **f°g** è una funzione che è anch'essa biunivoca, quindi l'operazione **°** è una operazione interna.
Se ho tre funzioni **f,g,h** ovviamente è indifferente applicare **f** a **g°h** oppure **f°g** ad **h**; , infatti qualsiasi sia **x**, f°**(g°h)(x) =f(g(h(x))=f°g(h(x))** quindi vale la proprietà associativa.
La funzione **i** che manda ogni elemento in se stesso (***identità***) è l'elemento neutro, in quanto se mandiamo un elemento **a** in **b** e poi applichiamo ancora **i** otteniamo ancora **b**; quindi componendo **f** con **i** ottengo **f**; lo stesso se compongo **i** con **f**.
Data una qualsiasi funzione **f** biunivoca, esiste la funzione inversa (potete verificarlo sempre nella parte dedicata alla definizione di numero cardinale) che chiamiamo f^{-1}; se componiamo $f^{-1} \cdot f = i$, e anche se componiamo $f \cdot f^{-1} = i$; quindi per ogni f esiste l'elemento l'inverso.
Quindi S_A è un gruppo.
Non è un gruppo abeliano se il numero di elementi di **A** è maggiore o uguale a tre; se componiamo **f°g** in generale non otteniamo la stessa cosa di **g°f.**



Le applicazioni biunivoche di un insieme **A** in se stesso si chiamano anche permutazioni; possiamo pensare infatti ad una applicazione biunivoca come ad una applicazione che sposta gli elementi di uno stesso insieme in posizioni diverse; se l'insieme è **A={1,2,3,..n}** i gruppi corrispondenti si denotano con **Sn**.
Dalla definizione di fattoriale possiamo trovare l'ordine del gruppo **Sn**, che è uguale a **n!**.
Infatti il fattoriale di un numero **n** altro non è che il numero di permutazioni di un insieme con **n** elementi.
Per rappresentare una permutazione α in **Sn**, possiamo usare la scrittura:

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

torniamo al caso **n=2**; usando questa rappresentazione, essendo **2!=2**, esplicitiamo le due permutazioni:

$I = \begin{pmatrix} 1,2 \\ 1,2 \end{pmatrix}$ (identità) e $\tau = \begin{pmatrix} 1,2 \\ 2,1 \end{pmatrix}$ se scriviamo una tabella per le composizioni possibili (qualcosa che ricorda la tabella Pitagorica), otteniamo:

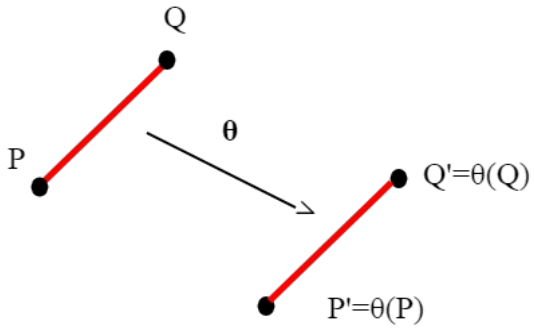
∘	I	τ
I	I	τ
τ	τ	I

Vediamo da qui che il gruppo S2 è abeliano.

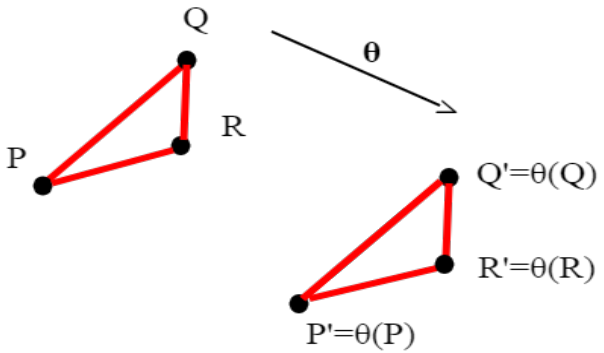
Il gruppo delle isometrie piane

Il concetto di isometria.
Una isometria (dal greco ἴσος, isos, che significa uguale) è una nozione che generalizza quella di movimento rigido di un oggetto o di una figura geometrica.
Consideriamo il piano Euclideo; se per isometria intendiamo una funzione che generi un movimento rigido, essa necessariamente conserva le distanze, e quindi applicata ad un ente geometrico, ne conserva la forma.

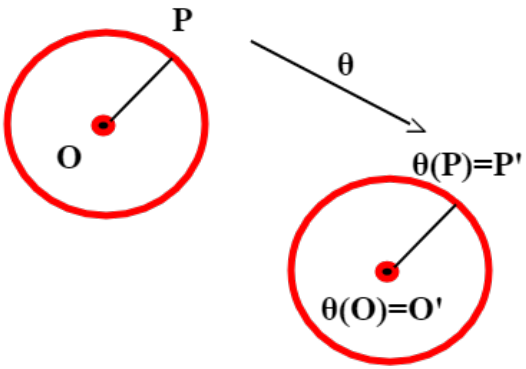
Più in dettaglio, se Indichiamo con $\mathbb{P}$ l'insieme dei punti de piano euclideo e con θ una applicazione biunivoca θ: $\mathbb{P}$--->$\mathbb{P}$, diremo che θ è un 'isometria se per ogni coppia di punti **P,Q**, chiamati θ**(P)=P' e** θ**(Q)=Q'** i punti corrispondenti, **PQ=P'Q'** (intendiamo con **PQ** la lunghezza del segmento con estremi **P** e **Q**).



i segmenti **PQ,P'Q'** sono congruenti, perché l'isometria conserva le distanze, o come preferite, genera un movimento rigido nel piano.
Se consideriamo tre punti **P,Q,R e** θ**(P)=P',** θ**(Q)=Q',** θ**(R)=R'** i due triangoli **PQR** e **P'Q'R'** sono congruenti avendo i tre lati uguali (terzo criterio). Essendo θ un isometria;



Una isometria trasforma un triangolo in un triangolo congruente, essendo i rispettivi lati congruenti. Se il triangolo degenera in un segmento, lo farà anche la sua immagine
Pertanto se **R** appartiene alla retta **PQ** anche **R'** appartiene alla retta **P'Q'**. Di conseguenza, ogni isometria trasforma rette in rette.
Trasforma poi circonferenze in circonferenze dello stesso raggio; infatti se **c** è una circonferenza di raggio **r**, essa è il luogo geometrico dei punti equidistanti da un punto(centro) **O**, ossia i punti **P** del piano per cui **PO=r**; consideriamo allora l'immagine **O'=θ(O)** di **O**; se **P** è un punto di **c**, **PO=r**, ma allora **P'O'=PO=r**, quindi **P'=θ(P)** , immagine di **P**, appartiene alla circonferenza di centro **O'** e raggio **r**.



Chiamiamo H l'insieme delle isometrie.
H con l'operazione ° di composizione è un sottogruppo del gruppo delle biiezioni (applicazioni biunivoche) del piano in sé (in particolare **H** è un gruppo).

Dimostrazione.

Dalla definizione di sottogruppo:

1. esistenza elemento neutro;Ovviamente, I ∈H. (l'identità conserva le distanze, ovvero è una isometria).

2. La composizione di due isometrie è una isometria. Siano **f, g** $\in$**H** e siano **P, Q** due punti. Posto **P'** = **f(P), Q'** = **f(Q), P"** = **g(P'), Q"** = **g(Q')**, si ha **P"Q"** ≡ **P'Q'**, perché **g** è un'isometria, **P'Q'** ≡ **PQ**, perché **f** è un'isometria, quindi **P"Q"** ≡ **PQ**. Ma allora anche **g°f**, che trasforma **P** in **P"** e **Q** in **Q"**, è un'isometria.

3. L'inversa f di una isometria è una isometria. Se f manda **P** in **P'** e **Q** in **Q'**, essendo **PQ** ≡ **P'Q'**, anche **f-1**, che porta **P'** in **P** e **Q'** in **Q**, è un'isometria.

(chiaramente la proprietà associativa è vera per definizione, perché una isometria è anche una applicazione biunivoca, e per le applicazioni biunivoche è valida).
Ci fermiamo qui come esempi di gruppi; visto che sono state ampiamente trattate in questo sito, mi piacerebbe se qualcuno provasse a verificare che ***le trasformazioni di Lorentz*** (con l'operazione di composizione) formano un gruppo.
Questo fa capire come la struttura di gruppo sia applicabile anche alla fisica.

Altri esempi di gruppi

Proseguiamo lo studio dei gruppi, analizzando due gruppi fondamentali costruiti su **Z**; le classi di resto modulo **n** (un valido esempio anche per approfondire il concetto di equivalenza) e il gruppo prodotto.
Poi la verifica del fatto che anche le trasformazioni di Lorentz formano un gruppo,che era stato proposta ai lettori nell'articolo precedente.

Le classi di resto modulo n: $\mathbb{Z}_n$**.**

Nell'insieme **Z** dei relativi, consideriamo la seguente relazione di equivalenza(le relazioni di equivalenza le abbiamo viste nella parte relativa alle relazioni e alle classi di equivalenza):
$a \sim b$: a è equivalente a **b** se **a,b** danno lo stesso resto divisi per un certo **n** fissato.
Ricordiamo che la divisione fra interi è la soluzione di un problema; dati a ,**n,** dividere a per **n** equivale **a** trovare due interi **q,r** tali che **a=nq+r** con **r<n**.
Vogliamo trovare un altro metodo per esprimere questa relazione.

Sia ad esempio **n=3**; siano **a,b** due numeri interi.
a=3x+r1
b=3y+r2
supponiamo che **a,b** abbaino lo stesso resto; allora **r1=r2.**
a-b=3x-3y+r1-r2=3(x-y); quindi per essere equivalenti la loro differenza deve essere multiplo di 3.
Abbiamo trovato un modo più comodo per verificare se due elementi sono equivalenti.
Verifichiamo le tre proprietà che caratterizzano le relazioni di equivalenza:

proprietà riflessiva: $a \sim a$, essendo a-a=0 e quindi multiplo di 3

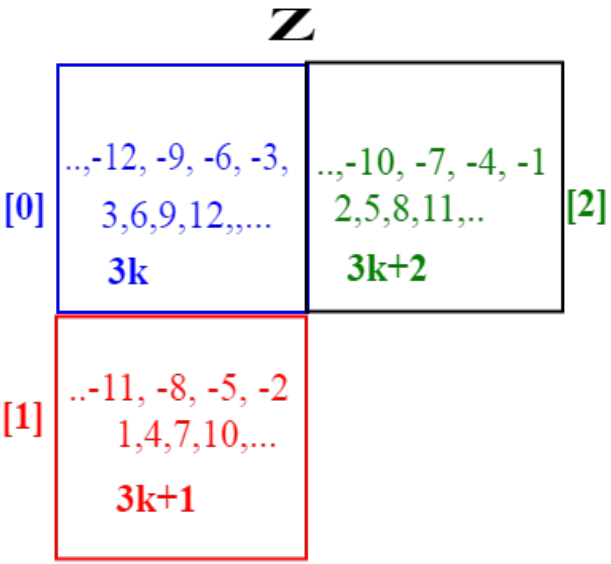
proprietà simmetrica: se $a \sim b$**,** a-b=3m, b-a=-3m quindi $b \sim a$

proprietà transitiva: se$a \sim b$ allora a-b=3m, se $b \sim c$ allora b-c=3n

ma allora **a-c=b+3m +3n-b=3(m-n)** , quindi $a \sim c$

Lo stesso vale per **n** generico.

Quindi essendo $\sim$ una relazione di equivalenza, possiamo considerare l'insieme quoziente, ovvero l'insieme delle classi di equivalenza.
Ricordiamo che le classi di equivalenza costituiscono una partizione dell'insieme (in questo caso **Z**).
Per rappresentare una classe,possiamo prendere uno qualsiasi dei suoi elementi come rappresentante.
Nel caso **n=3** possiamo considerare come rappresentanti i numeri **0,1,2** che altro non sono che i resti possibili.
Infatti 0 diviso 3 dà quoziente 0 e resto 0, 1 diviso 3 dà quoziente 0 e resto 1, 2 diviso 3 dà quoziente 0 e resto 2.



***Z** è unione delle classi **[0],[1],[2]**, che sono disgiunte, essendo una partizione .*

Per **n** generico avremo **0,1,2,..n-1**, quindi **n** classi.
Indichiamo con $\mathbb{Z}_n$ tale insieme quoziente.
Più precisamente l'insieme quoziente è costituito dalle classi $\mathbb{Z}_n$**={ [0],[1], [2],[3], ...[n-1]}.**
Per **n=3, 0,1,2,3** non sono altro che dei rappresentanti delle classi.
Per esempio la classe **[1]** ha come elementi **1,4,7,10,...)** ma non dimentichiamoci anche i numeri negativi **(...,-11, -8, -5, -2)**.
Infatti tutti divisi per 3 danno resto 1.
Nell'insieme quoziente, per definire un gruppo dobbiamo definire una operazione interna, ovvero una corrispondenza di $\mathbb{Z}_n$**x**$\mathbb{Z}_n$--->$\mathbb{Z}_n$.

Definiamo la somma fra due elementi **[a]** e **[b]** come la classe del resto della divisione di **a+b** per **n**.

Tale operazione così definita è interna; infatti tornando all'esempio **n=3**, il resto di **a+b** (diviso per **3**) qualsiasi siano **a,b** è sempre un numero minore di **3**, che quindi appartiene ad una delle classi **[0],[1],[2],[3];** è una buona definizione, ovvero è sensata, in quanto non dipende da quali rappresentanti scegliamo per le classi di **a,b**.
Supponiamo per esempio (caso **n=3**) **[1]+[2]=[1+2]=[3]=[0]**; se cambiamo rappresentanti **[4]+[5]=[4+5]=[9]=[0]**.
In generale, **[a]+[b]=[a+b]**; se $a \sim a', b \sim b'$, **[a']+[b']=[a'+b']** ma **a-a'=kn**, **b-b'=zn**, **a+b=a'+kn+b'+zn=a'+b'+n(k+z)**, **a+b-(a'+b')=n(k+z)** quindi per la definizione dell'equivalenza **[a+b]=[a'+b']**.
Verifichiamo le tre condizioni per fare di $\mathbb{Z}_n$un **gruppo**.
La proprietà associativa deriva immediatamente dalla proprietà associativa di **Z**; se facciamo infatti
([a]+[b]) +[c]=[a+b] +[c]=[(a+b)+c]=[a+(b+c)] = [a]+([b] +[c])

Qualsiasi sia **[a]**, l'elemento neutro è la classe **[0]**; infatti:
[a] +[0]=[a+0]=[a]; l'inverso di **[a]** è la classe di **[-a]**, infatti **[a]+[-a]=[a-a]=[0]**.
L'operazione è poi commutativa :**[a]+[b]=[a+b]=[b+a]=[b]+[a]** quindi $\mathbb{Z}_n$ è un gruppo abeliano.

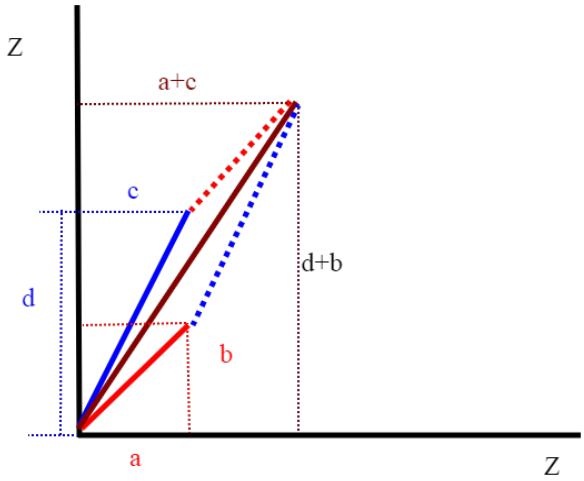
Il gruppo Z x Z

Z x Z con la seguente operazione interna **(a,b)+(c,d)=(a+c,b+d)** è gruppo.

0) Proprietà associativa:
[(a,b)+(c,d)]+(e,f)=(a,b)+[(c,d)+(e,f)]
Potete intuirlo immediatamente dal fatto che su **Z** l'operazione di somma è associativa. Infatti **[(a,b)+(c,d)]+(e,f)=(a+c,b+d) +(e,f)=(a+c+e,b+d+f)= (a,b)+(c+e,d+f)=(a,b)+[(c,d)+(e,f)]**.

1) Chiusura rispetto all'operazione interna:
(a,b) ∈ Z x Z, (c,d) ∈ ZxZ => (a+c,b+d) ∈ Z x Z
perché **Z** è gruppo additivo , come tale è chiuso rispetto all'addizione , cioè sulla prima componente si ha **a ∈Z**, **c ∈Z=>a+c ∈Z** e idem sulla seconda componente **b ∈Z**, **d ∈Z =>b+d ∈Z.**

2)esistenza dell'elemento neutro;
cerchiamo una coppia **(e1,e2)** tale che, qualsiasi siano **a,b** si abbia:
(a,b)+ (e1,e2) =((e1,e2) +(a,b)=(a,b) basta prendere **(e1,e2)=(0,0).**



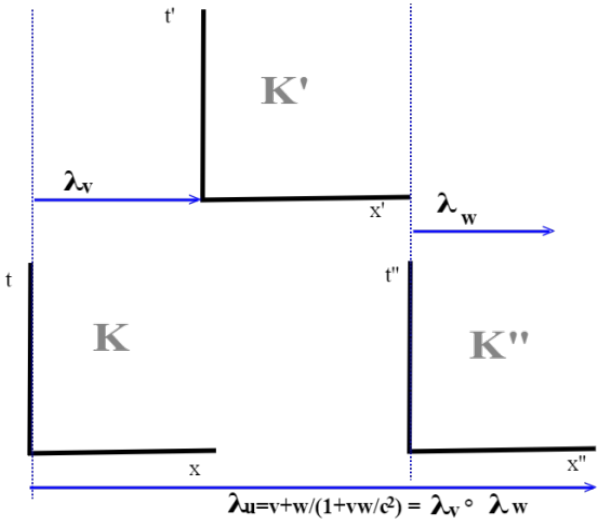
3) Inverso; qualsiasi sia l'elemento (a,b) di Z x Z se consideriamo (-a,-b) si ha:
(a,b)+(-a,-b)=(-a,-b)+(a,b)=(0,0)
L'operazione è poi commutativa:
(a,b)+(c,d)=(a+c,b+d)=(c+a,d+b)=(c,d)+(a,b).

Il gruppo delle trasformazioni di Lorentz

Da un punto di vista strettamente matematico, le trasformazioni di **Lorentz** sono delle funzioni di **R x R--->R x R** che associano ad una coppia **(x,t)** la coppia **(x',t')** con la seguente legge:

1) $\begin{cases} x' = \gamma(v)(x - vt)) \\ t' = \gamma(v)(t - \frac{v}{c^2}x) \end{cases}$

dove $\gamma(v) = \frac{1}{\sqrt{1 - \frac{v^2}{c^2}}}$ è un parametro che dipende dalla sola velocità **v**, velocità relativa fra i due sistemi.
Quindi chiamando **L**'insieme delle trasformazioni di Lorentz in uno spazio-tempo bidimensionale, esse dipendono da un solo parametro, **v;L={**λ_v**}.** Possiamo dunque scrivere $\lambda_v : R \times R \to R \times R$, dove la funzione λ_v è espressa dalla 1).
Osserviamo innanzitutto che essendo le λ_v delle funzioni, possiamo considerare la loro composizione.
La composizione di funzioni in ogni caso è associativa, lo abbiamo visto nel primo articolo sui gruppi.
Verifichiamo adesso che le trasformazioni di Lorentz formano un gruppo. Dobbiamo dimostrare che l'operazione composizione è interna, ovvero °:
L x L --->L, $(\lambda_w, \lambda_v) \to \lambda_u$;
la funzione composta, che per ora indichiamo con $f = \lambda_w \circ \lambda_v$ sarà una funzione **f: R x R-->R x R**; non sappiamo ancora se si tratti di una trasformazione di Lorentz, dobbiamo dimostrarlo.



Abbiamo tre sistemi inerziali, **K,K',K''**; **K'** si muove rispetto a **K** con velocità **v, K''** si muove rispetto a **K'** con velocità **w**; per calcolare le coordinate di un punto (evento) in **K''** in funzione di quelle in **K** possiamo operare in due modi;
il primo è quello di calcolare prima la trasformazione di Lorentz da **K** a **K'**:

$$\begin{cases} x' = \gamma(v)(x - vt)) \\ t' = \gamma(v)(t - \frac{v}{c^2}x) \end{cases}$$

poi riapplicare la trasformazione da **K'** a **K''**,

$$\begin{cases} x'' = \gamma(w)(x' - wt')) \\ t'' = \gamma(w)(t' - \frac{w}{c^2}x') \end{cases}$$

per esprimere la funzione composta dobbiamo legare **(x'',t'')** a **(x,t)**, per cui nella seconda dobbiamo sostituire a **x',t'** le espressioni in funzione di **x,t**:

$$\begin{cases} x'' = \gamma(w)[\gamma(v)(x - vt) - w\gamma(v)(t - \frac{v}{c^2})] \\ t'' = \gamma(w)(\gamma(v))[t - \frac{v}{c^2}) - \frac{w}{c^2}(x - vt)] \end{cases}$$

Per quanto complessa, otteniamo una associazione fra **f: (x,t)--->(x'',t'')**.
L'altro modo, è quello di applicare direttamente una trasformazione di Lorentz fra **Ke K''**,(sistemi inerziali in moto relativo con velocità **u**) che chiamiamo λ_u**: (x,t)--->(x'',t'')**; chiaramente le due funzioni devono dare gli stessi valori su ogni coppia **(x,t)**, quindi **f=**λ_u; quindi **f** ha la forma di una trasformazione di Lorentz.
Quale sia la velocità **u** lo scopriamo subito: conosciamo già la legge di composizione di due velocità **v,w** che è $u = \dfrac{v + w}{1 + \frac{vw}{c^2}}$;

Quindi:

$$\lambda_v \circ \lambda_w = \lambda_u = \lambda_{\frac{v+w}{1+\frac{vw}{c^2}}}.$$

Qual'è l'elemento neutro? è la trasformazione con velocità relativa uguale a zero,ossia λ_0 (i due sistemi sono in quiete).

L'inversa? la trasformazione con **w=-v**.

Lo possiamo capire subito così:

$$\lambda_v \circ \lambda_{-v} = \lambda_u = \lambda_{\frac{v+-v}{1-\frac{v^2}{c^2}}} = \lambda_0$$ oppure

pensando al fatto che se **K'** si allontana da **K** con velocità **v** mentre **K''** si avvicina a **K'** con velocità **v** allora **K,K''** sono in quiete relativa.

Quindi abbiamo verificato tutte le condizioni della definizione di gruppo.

I Gruppi liberi

Questo articolo è un po' più difficile di quelli trattati finora, in quanto richiede una certa astrazione.
Vedremo come generare un gruppo partendo da un insieme.
Qualcuno si chiederà a cosa può servire una cosa del genere.. vi anticipo solo che è di fondamentale importanza per comprendere uno dei più importanti paradossi della matematica moderna, quello di Banach-Tarski.
Negli articoli precedenti abbiamo definito la struttura di gruppo, oggetto fondamentale dell'algebra moderna.
Ci chiediamo se è possibile generare in qualche modo un gruppo, partendo da alcuni dei suoi elementi.
Chi conosce gli spazi di vettori, vede immediatamente una analogia; in tali spazi combinando dei vettori fra di essi, si possono ottenere tutti i vettori ; se poi scegliamo dei vettori particolari (ad esempio tre vettori fra loro ortogonali nello spazio tridimensionale) sappiamo che possiamo ottenere tutti i vettori dello spazio. E in tal caso tali vettori si dicono indipendenti.
Nel caso di gruppo si parlerà invece di generatori di gruppi e di generatori liberi.

Generatori di gruppi

Consideriamo un gruppo **G** e un suo sottoinsieme $X \subseteq G$; su **G** è definita una certa operazione; consideriamo tutte le combinazioni di questa operazione applicata ad elementi di **X**; chiaramente non tutti gli elementi combinati apparterranno ad **X** (senz'altro appartengono a **G**).
Chiamiamo $\langle X \rangle$ il più piccolo (minimo) sottogruppo di **G** che contenga **X**.

Per dirlo più formalmente: $\langle X \rangle = \left\{ x_1^{\alpha_1} \cdot x_2^{\alpha_2} \ldots . x_n^{\alpha_n} \right\}$ dove $x_1, \ldots, x_n$ sono elementi di **X** e $\alpha_1 \ldots . \alpha_n$ numeri interi relativi; infatti questo equivale a considerare direttamente anche gli inversi di x_i con un loro esponente.
Chiariamo meglio nel dettaglio cosa conveniamo con la scrittura sopra.
Se $\alpha = 0, x^{\alpha} = e$
se $\alpha > 0, x^{\alpha} = x \cdot x \cdot \ldots x : \alpha$ volte
se $\alpha < 0, x^{\alpha} = x^{-1} \cdot x^{-1} \cdot \ldots x^{-1} : -\alpha$ volte
Se $\langle X \rangle$**=G, X** si dice insieme generatore del gruppo **G**.
Se **X** è un generatore di **G**, qualsiasi sia **g** appartenente a **G, g** si scrive come $g = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \ldots . x_n^{\alpha_n}$.

Notiamo che con il puntino (·) abbiamo indicato l'operazione interna in **G**, (volevo cioè sottolineare che non indica un prodotto), e con ***e*** l'elemento neutro generico.
Infatti In **Z** la scrittura assume un altra forma *(con il +)* e so che questo può generare confusione.
esempio: chiariamo meglio cos'è il secondo membro di $\langle X \rangle = \left\{ x_1^{\alpha_1} \cdot x_2^{\alpha_2} \ldots . x_n^{\alpha_n} \right\}$ quando consideriamo **Z** con l'addizione usuale l'operazione da considerare è la somma, "+";potremmo pensare di generare **Z** usando come generatore **X={1}** in questo caso la scrittura 1^{α} vuole semplicemente dire **1+1...+1+ 1** α volte se α>0, 1^{α} vuole dire, **-1-1...-1** -α volte se α**<0**, sappiamo infatti che qualsiasi numero intero **z** si può pensare come somma di **z** volte **1** se **z** è positivo, -**z** volte -**1** se **z** è negativo. Quindi **X={1}** genera **Z**.

Gruppi finitamente generati e gruppi ciclici

Un gruppo si dice finitamente generato (o ***n-generato***) quando **X** è un insieme finito.
Un gruppo con un solo generatore si dice gruppo ciclico.
Prendiamo come esempio $\mathbb{Z}$**(*interi relativi***) con l'addizione usuale; è finitamente generato, anzi è ciclico, $\mathbb{Z} = \langle 1 \rangle$, ossia è generato dal solo elemento **1** come abbiamo visto sopra.
Vediamo altri esempi con gruppi **(**$\mathbb{Z}_n$**, Z x Z)** che abbiamo conosciuto nell'articolo precedente dove venivano esposti altri esempi di gruppi:

Il gruppo $\mathbb{Z}_n$ (classi di resti modulo n).

Consideriamo $\mathbb{Z}_n$; se con **[1]** indichiamo la classe degli interi che divisi per **n** danno **1** come resto, $\mathbb{Z}_n$ è ciclico; **[1]** è il generatore del gruppo.
Infatti **[1] +[1]=[2], [1] +[1]+[1]=[3], [1]+[1]+...+[1] n** volte dà **[n]=0]** (infatti **n** diviso **n** dà resto **0**).

Il gruppo Z x Z

Z x Z ha come generatori **(1,0) (0,1)**; infatti **(a,b)=(1+...1,0) + (0,1+...1)** nel caso siano entrambi positivi; facilmente si vede anche negli altri casi.

Gruppi liberi (parte prima)

Sia **X** un insieme di generatori di un gruppo **G**; sappiamo allora che ogni elemento **g** può essere scritto nella forma:
$g = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \ldots . x_n^{\alpha_n}$ con gli x_i appartenenti a **X**, e gli α_i interi relativi.
La scrittura sopra non è in generale univoca, nel senso che esistono più sequenze che possono dare come risultato **X**, basti pensare che se una sequenza realizza **g**, anche la sequenza a cui aggiungiamo $x^{-1} \cdot x = e$ (**e** ***elemento neutro***) realizza **g**.
Ad esempio se **G=Z** per generare 4 possiamo usare **(1+1+1+1)** ma anche **(1+1+1+1) -1+1** .
Potremmo pensare di evitare quel tipo di scritture, contenenti sequenze di un elemento e il suo inverso.
Ma in ogni caso non saremmo mai sicuri.
Diamo la seguente definizione:
Un insieme di generatori **X** di un gruppo **G** si dice **libero** se , comunque si scelga una sequenza $x_1, x_2, \ldots, x_n$,con $x_i \neq x_{i+1}$,$x_i \in X$, e con $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$, si abbia:
$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \ldots . x_n^{\alpha_n} = e$; (***e elemento neutro di G***) solo nel caso che gli α_i **siano tutti nulli.**
Conseguenza di questa definizione è che sotto queste ipotesi ogni elemento $g \neq e$ si scrive in modo unico nella forma: $g = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \ldots . x_n^{\alpha_n}$,con $x_i \neq x_{i+1}$ e con $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}, \alpha_i \neq 0$.

Consideriamo per semplicità che i generatori siano **2**, ovvero **n=2** (è solo per visualizzare meglio le operazioni).
Supponiamo per assurdo che **g** abbia due espressioni diverse, ovvero che si possa scrivere :
$g = x_1^{\alpha_1} \cdot x_2^{\alpha_2} = x_1^{\beta_1} \cdot x_2^{\beta_2}$
utilizziamo adesso le due diverse espressioni per esprimere g e il suo inverso:
$g = x_1^{\alpha_1} \cdot x_2^{\alpha_2}$
dico che $g^{-1} = x_2^{-\beta_2} \cdot x_2^{-\beta_1}$; infatti:
$g \cdot g^{-1} = x_1^{\beta_1} \cdot x_2^{\beta_2}\ x_2^{-\beta 2} \cdot x_1^{-\beta 1}$ = $x_1^{\beta_1} \cdot e \cdot x_1^{-\beta 1} = x_1^{\beta_1}\ x_1^{-\beta 1} = e$, quindi $x_2^{-\beta_2} \cdot x_1^{-\beta_1}$ è proprio l'inverso di **g**.
Per trovare l'inverso di **g** partendo dalla sua espressione, abbiamo dovuto considerare gli inversi dei singoli fattori scritti nell'ordine inverso; questo è necessario perchè il gruppo **G** non è in generale commutativo.
Combiniamo adesso le due espressioni, una in funzione di α, l'altra in funzione di β:
1)**e**=$g \cdot g^{-1} = x_1^{\alpha_1} \cdot x_2^{\alpha_2}\ x_2^{-\beta 2} \cdot x_1^{-\beta 1} = x_1^{\alpha_1} \cdot x_2^{\alpha_2 - \beta 2} \cdot x_1^{-\beta 1}$;
se fosse $\alpha_2 \neq \beta_2$ potremmo scrivere **e** come e come combinazione di x_1, x_2 con un esponente ($\alpha_2 - \beta_2$) non nullo ma questo va contro l'ipotesi.
Allora deve essere $\alpha_2 = \beta_2$.
La 1) diventa: $e = g \cdot g^{-1} = x_1^{\alpha_1} \cdot x_2^0 \cdot x_1^{-\beta 1} = x_1^{\alpha_1 - \beta 1}$; ma allora anche $\alpha_1 = \beta_1$, altrimenti l'esponente di x_1 sarebbe non nullo.
Dunque $\alpha_i = \beta_i$ qualsiasi sia i e quindi le due espressioni di **g** coincidono.
Un gruppo G si dice libero se ammette un insieme libero di generatori.
Il gruppo **Z** che come abbiamo visto è un gruppo generato da **{1}** è un gruppo libero.
Facciamo attenzione che qui l'operazione interna è l'addizione, e l'elemento neutro lo zero.
Applichiamo il risultato sopra; non è possibile scrivere 0 sommando degli **1** in nessun modo.
Anche **Z x Z** con generatori **(1,0)** e **(0,1)** è libero; infatti non si può scrivere **(0,0)** come combinazione di somme di **(1,0)** e **(0,1)** in alcune modo.

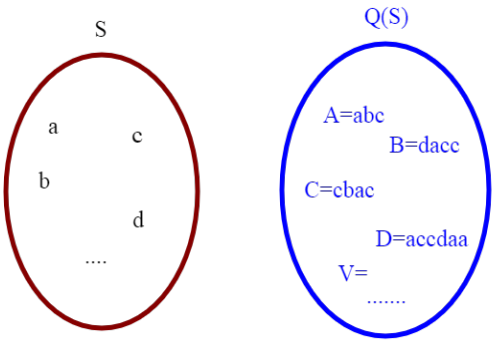
Se **n(1,0)+m(0,1)=(0,0)**, allora **(n,m)=0**, quindi **n=0,m=0** .
Gli esempi di gruppi liberi non sono purtroppo molti; vedremo però nel prossimo articolo come costruire un gruppo libero partendo da un insieme qualsiasi.

Gruppi liberi (seconda parte)

Nell'articolo precedente abbiamo parlato di generatori di gruppi e di gruppi liberi.
Vogliamo ora provare l'esistenza di questi gruppi, senza ricorrere ad un esempio "reale".

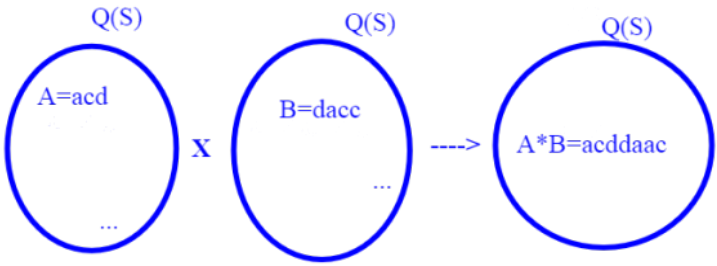
Costruzione di un gruppo libero

Non è molto facile trovare esempi di gruppi liberi, però c'è un procedimento astratto per costruirli.
Consideriamo un insieme **S** qualsiasi.
Vogliamo da questo insieme costruire (***generare***) un gruppo.
Sia **S={a,b,c,d,...}**.
Consideriamo tutte le sequenze (finite) ottenute combinando elementi di **S** in questo modo : **acd, abd, daac,** ecc..



Dato un qualsiasi insieme **S**, costruiamo su di esso un'altro insieme **Q(s)**,

costituito da tutte le parole che si possono formare usando come alfabeto **S**.
Con **V** indichiamo la parola vuota.
Chiamiamo queste combinazioni o sequenze semplicemente parole.
Definiamo **Q(S)** come l'insieme di tutte queste parole.
Notiamo che se anche **S** è finito, **Q(S)** è infinito.
Infatti possiamo ripetere indefinitamente uno stesso simbolo quante volte vogliamo: **abccccc,abccccccccccccc.....** ottenendo tutte parole diverse.
Indichiamo le parole con delle lettere maiuscole ; **A=abc**, **B=cda**, ecc.
Definiamo (***inventiamo)*** una operazione interna fra le parole di **Q(S)**, in questo modo:
***: Q(S) x Q(S)---> Q(S)** che (*per esempio*) ad **A=acd**, **B=daac** associa **A*B=acddaac**, ossia scrive semplicemente una sequenza dopo l'altra.



Chiamiamo $giustapposizione^{(1)}$ questa operazione.
La **giustapposizione** di parole è una operazione interna (componendo due parole si ottiene ancora una parola) ed inoltre è associativa .
Sia **C=abd** una terza parola.
Infatti è la stessa cosa comporre prima **A** con **B** e poi con **C** oppure **A** con **B** con **C**:
(A*B)*C=(acddaac)*abd=acddaacabd=(acd)*(daacabd)
quindi l'operazione * è associativa.
Non è commutativa : A*B=acddaac$\neq$daacacd=B*A.
Come elemento neutro prendiamo la sequenza vuota di lettere, che indichiamo con **V**.
Chiaramente combinando qualsiasi sequenza con la sequenza vuota ottenia-

mo la sequenza stessa.
Quindi **V** è proprio l'elemento neutro per questa operazione.

---

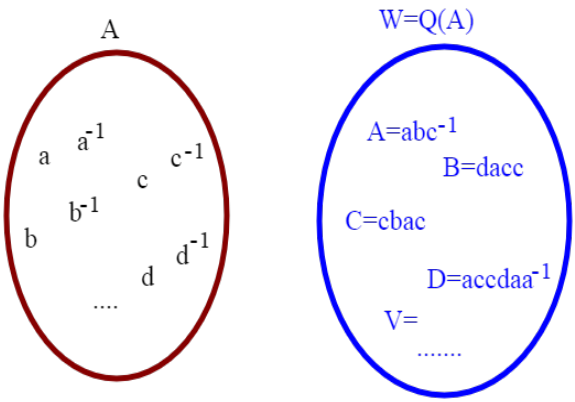
(1) *Giustapposizione*: In linguistica, composizione di parole fondata sul semplice allineamento, senza che si stabilisca un rapporto di subordinazione dell'una all'altra o di entrambe a un'unità sintattica sottintesa.

Nell'algebra astratta, un monoide è una struttura algebrica dotata dell'operazione binaria associativa e di un elemento neutro.

Q(S) è un monoide.

Per definire un gruppo questo ancora non basta; dobbiamo trovare per ogni elemento un inverso.
Dobbiamo in qualche modo ampliare l'insieme **S**; per ogni elemento ***a*** di **S**, prendiamo un elemento che chiamiamo a^{-1}; per adesso questi elementi non hanno niente di particolare, a parte il fatto che per ogni ***a*** ne esiste uno ed uno solo.
Li chiamiamo al limite *cancellatori*.
Come si può intuire tali elementi avranno il ruolo di essere gli inversi delle stringhe semplici, formate da una sola lettera, ma non abbiamo ancora risolto il problema degli inversi di ogni sequenza.
Abbiamo così ampliato l'insieme **S={a,b,c,d,....** a
A={$a, a^{-1}, b, b^{-1}, c, c^{-1}, d, d^{-1}$}.
A viene anche chiamato alfabeto di **S**.

Prendiamo in considerazione gli elementi di **W=Q(A)** che adesso conterranno anche i nuovi simboli.



Sugli elementi **w** di **W** definiamo i seguenti due tipi di operazione: (1) inserimento in **w** di una coppia di termini consecutivi del tipo xx^{-1} oppure $x^{-1}x$

(2) cancellazione in **w** di una coppia di termini consecutivi del tipo xx^{-1} oppure xx^{-1}
Diciamo che due parole **w1;w2** appartenenti a **W** sono equivalenti, e scriviamo $w_1 \sim w_2$, se **w2** si ottiene da **w1** mediante una successione finita di operazioni del tipo **(1)** o **(2)**.
Conveniamo inoltre che tali termini possano essere inseriti in qualsiasi punto di una parola, anche all'inizio o alla fine.
w=abc; parole equivalenti a **w** sono ad esempio:

$$x^{-1}xabcxx^{-1}, abx^{-1}xcxx^{-1}, abcx^{-1}x$$

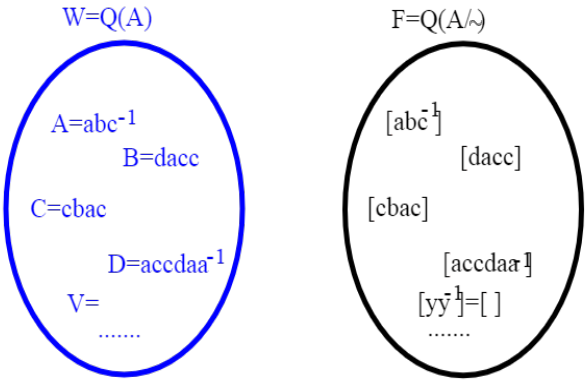
la relazione è riflessiva:
$w \sim w$;
infatti se a **w** prima aggiungiamo $x^{-1}x$ e poi togliamo $x^{-1}x$ otteniamo ancora **w**
Esempio:**w=abc** , $abc \sim abcxx^{-1} \sim abc$
è simmetrica:
se $w_1 \sim w_2$ allora $w_2 \sim w_1$; infatti se **w2** si ottiene da **w1** mediante

una sequenze di operazioni di *tipo **1,2*** se per ogni operazione poi facciamo l'opposta su **w2** (nel senso che se era un inserimento facciamo una cancellazione e viceversa), allora da **w2** otteniamo ancora **w1**.
esempio: $w1 = abc, w2 = abcx^{-1}x$; se adesso togliamo $x^{-1}x$ da **w2** otteniamo proprio **w1=abc**;
è transitiva; se $w_1 \sim w_2$, $w_2 \sim w_3$, allora $w_1 \sim w_3$; infatti se con operazioni del ***tipo 1,2*** da **w1** otteniamo **w2**, e se con operazioni del ***tipo 1,2*** da **w2** otteniamo **w3**, allora con una certa sequenza di tali operazioni da **w1** otteniamo **w3**.
Esempio:$w1 = abc, w2 = abcx^{-1}x$;
$w3 = yy^{-1}w2 = yy^{-1}abcxx^{-1} = yy^{-1}w1xx^{-1}$

Indichiamo allora con **[w]** la classe di equivalenza di **w**; se **V** è la stringa vuota, **[V]=[**$x^{-1}x$**]=[**xx^{-1}**]** qualsiasi sia **x**; (***su V abbiamo effettuato un operazione di tipo 1***).
Consideriamo adesso l'insieme quoziente; possiamo pensare alle parole ridotte, ovvero non contenenti sequenze del tipo xx^{-1} che tanto rappresentano la sequenza nulla.
Così gli elementi ridotti si potranno rappresentare tali elementi del quoziente (classi), così come le frazioni di **Q** (**numeri razionali**) possono essere pensate come ridotte ai minimi termini.

Definizione di un'operazione sull'insieme quoziente.

A questo punto è importante notare che per la costruzione del gruppo ci siamo spostati prima da **Q(S)** a **Q(A)**, e adesso sull'insieme quoziente di **Q(A)** rispetto alla relazione di equivalenza che abbiamo introdotto. Tale insieme si indica con **F=**$Q(A)/\sim$



Per costruire il gruppo siamo costretti a passare all'insieme quoziente della nostra relazione di equivalenza.

Sull'insieme quoziente definiamo l'operazione fra classi semplicemente così:
[w1]*[w2]=[w1w2] che si legge così: il risultato dell'operazione fra le due classi, corrisponde alla classe della ***giustapposizione*** fra due rappresentanti qualsiasi.
Perché ha senso questa definizione? Perchè non dipende dai rappresentanti che scegliamo.Infatti se $w_1' \sim w_1, w_2' \sim w_2,$ allora:
$w_1'w_2' \sim w_1w_2$.
Vediamo con un esempio: $w_1' = xx^{-1}w_1, w_2' = xx^{-1}w_2yy^{-1}$, $w_1'w_2' = xx^{-1}w_1xx^{-1}w_2yy^{-1}$ ma il secondo membro è equivalente a w_1w_2 per come abbiamo definito tale relazione.
Ci fermiamo qui per non appesantire troppo il discorso; nel prossimo articolo dimostreremo che con l'operazione che abbiamo definito sopra $Q(A)/\sim$ diventa un gruppo libero.

I campi algebrici

Definizione di campo algebrico

Dopo i gruppi affrontiamo un'altra struttura algebrica fondamentale: **I campi**.
Senza saperlo sono qualcosa che conosciamo già molto bene.
Consideriamo i numeri reali; in essi abbiamo una operazione di somma che fa di essi un gruppo ***commutativo*** (o ***Abeliano***). quindi (**R,+**) ovvero **R** con l'operazione + ***è un gruppo*** (*con 0 elemento neutro*).
Consideriamo un'altra operazione in **R**, che è il prodotto.
Anche rispetto a questa operazione **R** è un gruppo (*con 1 elemento neutro*), a condizione di togliere lo zero.
Sappiamo infatti che tutti gli elementi di **R** hanno un inverso rispetto alla moltiplicazione a parte lo zero; non esiste infatti un numero che moltiplicato per **0** dia **1**.
Quindi **(R\{0},*)** è anche un gruppo commutativo rispetto alla moltiplicazione.
C'è poi un altra proprietà che riguarda le operazioni **+,*** definite in **R**; il fatto che la moltiplicazione sia distributiva rispetto alla addizione; questo significa che qualsiasi siano **a,b,c** :
a*(b+c)= a*b + a*c.
***Un insieme in cui esistano due operazioni con tali proprietà è detto* Campo.**
Voi mi direte; va bè è qualcosa che effettivamente sapevamo già.
Ma i matematici cercano sempre di estendere e generalizzare e di guardare oltre.
Facciamo un esempio.
Consideriamo una curva, tipo la circonferenza di raggio unitario. essa è definita dalle coppie **(x,y)** di **numeri reali**, soluzioni dell'equazione:
$x^2 + y^2 = 1$; ma è veramente necessario considerare le soluzioni reali? ***No!.***
Potremmo considerare anche solo le soluzioni razionali, come abbiamo fatto nella soluzione del Quiz su Fermat.
In pratica per calcolare i valori di quel polinomio in due variabili **(x,y)** abbiamo solo bisogno di un **Campo;** anche i numeri razionali privati dello zero **(Q\{0})** costituiscono un campo con le operazioni **+,***.

Cosa cambia? che in generale risolvendo in un altro campo l'equazione non abbiamo più una "curva" nel vero senso della parola, che sottintende "continua".
E' per questo motivo che sarebbe meglio parlare di equazioni in generale, a volte tralasciando il significato geometrico.
Per poter manipolare correttamente le equazioni, abbiamo bisogno dell'opposto, dell'inverso e di altre proprietà dei numeri.
Quando dico che per trovare **x+a=0** porto a destra cambiando di segno, altro non faccio che sommare ad ambo i membri ***l'opposto di a***, ottenendo **x=-a**; questo è possibile se siamo in un gruppo additivo.
Allo stesso modo dividere ambo i membri per trovare **ax=d** è possibile se esiste ***il reciproco di a*** (naturalmente pe $a \neq 0$), ovvero a^{-1}.
Per non parlare che la proprietà distributiva è necessaria per fare i raccoglimenti o i prodotti fra polinomi.
Un campo soddisfa ampiamente a queste necessità.

Il campo degli interi modulo p(Zp) con p primo

Un campo molto famoso e che ci servirà quando parleremo delle "curve" (equazioni) ellittiche è il ***campo degli interi modulo p***, **Zp**; questo è un campo a patto però che ***p sia un numero primo.***
Che **Zp** sia un gruppo con l'operazione + (***n in generale***) lo abbiamo visto quando abbiamo parlato dei gruppi.
Ricordiamo che in pratica gli elementi di **Zn** sono numeri che danno lo stesso resto se divisi per **n**.
Vogliamo dimostrare che se **n** è primo **Zp** è un gruppo anche rispetto ad una operazione di prodotto (*) se escludiamo lo zero, e che rispetto a tale operazione vale la proprietà distributiva.
Definiamo il prodotto in questo modo, sempre usando le classi di equivalenza:
definiamo il prodotto fra due elementi **[a]** e **[b]** come ***la classe del resto della divisione di a*b per p***.
Tale operazione così definita è compatibile con la relazione di equivalenza:
[a]*[b]=[a*b].
Vediamolo con un esempio; consideriamo **p=5**, quindi **Z5**;
[1]*[2]=[1*2]=[2]; se prendiamo un altro rappresentante per la **classe [1]**, ad esempio **6**, e per la classe **[2]**, ad esempio **7:**
[1]*[2]=[6*7]=[42]=[2] essendo **5*8=40** e quindi ***due è il resto della divisione di 42 per 5***; quindi la definizione di moltiplicazione non dipende dai

rappresentanti scelti per la classe. E la proprietà distributiva?
Se ad esempio consideriamo:
[2] *([3]+[4]) =[2]*([3+4])=[2]*[7]=[2]*[2]=[4]
mentre invece **[2]*[3] +[2]*[4]=[6]+[8]=[1]+[3]=[4]**, quindi sono la stessa cosa.
Questo in generale è valido anche se **p** non è primo; però in tal caso **Zp** non è un gruppo rispetto alla moltiplicazione.
L'elemento neutro è chiaramente **[1]**; Consideriamo **n=4**, cioè **Z4**.
Gli elementi di **Z4** sono **[0],[1],[2],[3]**.
Se prendiamo ad esempio **[2]**, vediamo che ***non esiste*** $[2]^{-1}$, ***ovvero un numero che moltiplicato per [2] dia [1]***.
infatti:
[2]*[0]=[0] [2]*[1]=[2] [2]*[2]=[4]=[0] [2]*[3]=[6]=[2]; quindi ***non c'è nessun elemento che moltiplicato per [2] dia [1]***.
Quindi in generale Zn **non** è un gruppo rispetto alla moltiplicazione, e quindi non è un campo.
Più difficile è dimostrare che se **p *è primo***, allora **Zp** è un gruppo moltiplicativo e ***quindi Zp è anche un campo***.
Però se prendiamo per buona la seguente ***identità di Bezout***:

d = a · x + b · y

dove **a,b, x, y** sono numeri interi e **d** è il ***massimo comun divisore*** di **a,b**,;
Sostanzialmente tale identità afferma che **d *può sempre essere espresso come combinazione lineare di* a,b**.
Prendiamo ad esempio **a=16**, **b=6**.
Il ***massimo comun divisore è 2***, essendo $a = 2^4$, **b=3 * 2.**
Quindi **d=2**; **2=18-16=-1*16+3*6=-1*a+3*b**; quindi **x=-1**, **y=3**.
Per gli appassionati dei numeri ho messo a fine pagina una giustificazione dell'identità.
Consideriamo adesso **Zp** con **p** primo; dobbiamo dimostrare che ogni $[a] \neq [0]$ ha un inverso moltiplicativo in **Zp**; essendo $[a] \neq [0]$, a non è multiplo di **p** (infatti diviso per **p** non dà resto zero); **p** è primo , quindi il **M.C.D. di (a,p) =1**
ma allora per l'identità di Bezout descritta sopra, **d=1** ed esistono **x,y** in **Z**, tali che:
1=x*a+ y*p; quindi **a*x=1-y*p** questo vuol dire che **a*x** diviso **p** dà resto 1 quindi **[a*x]=[a]*[x]=[1]**;

pertanto $[x] = [a]^{-1}$.

"Curve" con punti finiti.

Essendo dunque **Zp** con **p** primo un campo, possiamo su di esso studiare le soluzioni di certe equazioni polinomiali.
Consideriamo su Z5 l'equazione $x^2 + y^2 = 1$ (qui in realtà al posto di **1** dovremmo scrivere **[1]**) .
Tale equazione ha infinite soluzioni sia in **R** che in **Q**, come abbiamo visto. E in **Z5**? Essendo **Z5** un insieme finito, tali saranno anche le soluzioni.
Per dimostrarlo usiamo un metodo assolutamente banale, che però è alla base di quanto fatto da ***Wiles*** e compagni con le equazioni ellittiche.
Facciamo una tabella di tutte le coppie possibili di **x,y**: (i valori possibili sono i ***resti della divisione per 5***, che vanno dunque da **0** a **4**).
Mettiamo un **X** se la coppia è una soluzione dell'equazione, altrimenti non mettiamo niente.

	0	1	2	3	4
0		X			X
1	X				
2					
3					
4	X				

$x^2 + y^2 = 1$

(0,0) no, essendo **0 *0+ 0*0=0**$\neq$**1**
(1,0)=1 si essendo **1*1+0*0=1+0=1**, quindi anche **(0,1)** va bene.
(**1,1)=2**,no e così via.
Sembra che stiamo giocherellando con i numeri; in realtà per certe curve c'è un profondo legame fra le soluzioni in **Zp** e le soluzioni nel caso dei numeri razionali;
il metodo sopra è alla base della ***Congettura di Birch e Swinnerton-Dyer***, uno dei problemi più difficili della matematica, e ancora senza soluzione

completa, ma solo in certi casi particolari.
Ma lo vedremo meglio quando parleremo di curve (equazioni) ellittiche.

Addendum

Giustificazione dell'identità di Bezout:un problema aritmetico, risolvibile con un algoritmo, noto come algoritmo di Euclide esteso.
Procediamo con un esempio numerico; consideriamo i due numeri:
294 e **144 e** proponiamoci di risolvere per primo il seguente problema:
Trovare il MCD(204,144) ; con MCD indichiamo naturalmente il massimo comun divisore.
Dubito che qualcuno lo abbia usato alle scuole inferiori, di solito si usa la scomposizione in fattori (comuni, con il minimo esponente).
L'algoritmo è chiamato "***algoritmo di Euclide***", perchè sembra sia stato il primo a trovarlo, anche se applicato ai segmenti e formulato in modo leggermente diverso.
Dividiamo il più grande **(294)** per il più piccolo **(144)**, troveremo un quoziente e un resto, che di solito si indicano con **q,r**.

1. **) 204 = 144 · 1 + 60 (q=1,r=60)**

dividiamo adesso iterativamente il divisore per il resto:

2) **144 = 60 · 2 + 24 (q1=2,r1=24)**
3) **60 = 24 · 2 + 12 (q2=2, r2=12)**
4) **24 = 12 · 2 + 0 (q3=2,r3=0)**

E' da notare che ad ogni iterazione il resto successivo **r** è strettamente minore del resto precedente **60>24>12**; dovendo poi essere **r>=0** ad un certo punto deve necessariamente annullarsi.
Il massimo comun divisore è l'ultimo resto non nullo, ovvero 12 nel nostro caso.
Infatti, guardando le eguaglianze sopra, si vede che 12 le divide tutte, e quindi divide anche 204 e 144.
Infatti dalla 4) si sa che 12 divide 24, ma allora dividendo sia 24 che 12 per la 3) divide il 60; dividendo 60 e 24 divide 144 per la 2) e per la 1) divide anche 204.
(se un numero divide ambo i termini di una somma, allora divide la somma stessa)

Se riprendiamo adesso le divisioni eseguite sopra ed esplicitiamo il resto otteniamo:

60 = 204 + 144 · (−1)

24 = 144 + 60 · (−2)

12 = 60 + 24 · (−2)

Oltre ad essere un divisore comune, 12 è anche il massimo ; se infatti ***d*** è un altro divisore di **204** e **144** essendo **60 = 204 + 144 · (−1)** allora **d** divide anche 60 (se un numero è divisore di ambo i termini di una differenza allora è divisore anche della differenza); per lo stesso motivo è divisore anche di 24 e 12.
Dividendo anche il 12 significa che 12 è più grande di ***d*** *oppure uguale*, quindi 12 è il massimo.
Vogliamo ora esprimere 12, che è il MCD (204,144) come combinazione lineare di 204 e 144.
Sostituiamo ora nell'ultima identità **(12 = 60 + 24 · (−2))** il numero 24 con la sua combinazione lineare di **144 e 60** (penultima identità)

12 = 60 + 24 · (−2) ; ma **24** = 144 + 60 · (−2).

quindi :
12=60 + [144 + 60 · (−2)] · (−2)=144 · (−2) + **60** · 5;

ma **60** = 204 + 144 · (−1)

allora: 12=144 · (−2) + [204 + 144 · (−1)] · 5

Quindi: **12=204 · 5 + 144 · (−7) (12 MCD, x=58, y=-7)**

Per chi non fosse ancora convinto, accenno una dimostrazione non troppo formale, con le lettere al posto dei numeri.
E' un po' più difficile; può bastare l'esempio numerico.

Supponendo **a>b** cominciamo a dividere **a** per **b**:

- 1)$a = b \cdot q_0 + r_0$ con $0 \leq r_0 < b$
- 2) $b = r_0 \cdot q_1 + r_1$ con $0 \leq r_1 < r_0$
- 3)$r_0 = r_1 \cdot q_2 + r_2$ con $0 \leq r_2 < r_1$

. . .

n) $r_{n-2} = r_{n-1} \cdot q_n + r_n$ con $0 \leq r_n < r_{n-1}$

n+1)$r_{n-1} = r_n \cdot q_{n+1} + 0$

notiamo come nel caso numerico che:

$0 \leq .. < r_n < r_{n-1} < \ldots < r_2 < r_1 < r_0$

Questa è una successione (finita) strettamente decrescente i cui termini non possono mai diventare negativi; quindi prima o poi deve annullarsi.
Seguendo il ragionamento dell'esempio numerico,vediamo che l'ultimo resto non nullo r_n **divide a e b**; infatti oltre a stesso r_n divide r_{n-1} quindi dalla n) divide anche r_{n-2} e così via, risalendo la catena si arriva a vedere che r_n divide sia **a** che **b**, quindi è un divisore comune.
Per vedere che è il massimo esplicitiamo il resto come abbiamo fatto nel caso numerico.

- 1)$r_0 = a - b \cdot q_0$
- 2) $r_1 = b - r_0 \cdot q_1$
- 3) $r_2 = r_0 - r_1 \cdot q_2$

. . .
n) $r_n = r_{n-2} - r_{n-1} \cdot q_n$

Se **d** è un divisore di **a** e **b** allora , per la 1) è divisore anche di r_0 quindi per la 2) anche di r_1 e per la 3) di r_2; e così via fino ad arrivare a r_n,; essendo **d** divisore anche di r_n che è il nostro divisore comune trovato , ***allora*** r_n ***è il massimo divisore comune di a,b.***
E ***l'identità di Bezout***? Vogliamo dimostrare che r_n**=ax+by**, ovvero l'ultimo resto diverso da zero; sappiamo che $r_n = r_{n-2} - r_{n-1} \cdot q_n$, che è in nostro MCD; r_n è espresso come combinazione lineare a coefficienti interi di r_{n-1} e di r_{n-2}. Poichè r_{n-1} è a sua volta combinazione lineare a

coefficienti interi di r_{n-2} e di r_{n-3}, si scrive r_n come combinazione lineare di r_{n-2} e di r_{n-3}.

Infatti:
$r_n = r_{n-2} - r_{n-1} \cdot q_n$
$r_{n-1} = r_{n-3} - r_{n-2} \cdot q_{n-1}$
sostituendo nella prima la seconda identità:
$r_n = r_{n-2} - (r_{n-3} - r_{n-2} \cdot q_{n-1})) \cdot q_n$
Continuando in questo modo si arriva a scrivere (con qualche difficoltà ma solo di scrittura formale) r_n come combinazione lineare di **a** e **b**.
Questo significa proprio che r_n=**ax+by**.
Torniamo un attimo indietro; se ricordiamo come abbiamo fatto per dimostrare che ogni elemento di **Zp** con p primo ammette inverso:
1=x*a+ y*p; quindi **a*x=1-y*p** questo vuol dire che ***a*x diviso p dà resto 1*** quindi **[a*x]=[a]*[x]=[1]**; cioè $[x] = [a]^{-1}$.
Notiamo che applicando l'algoritmo sopra abbiamo anche un metodo per trovare **x**, ovvero l'inverso di **a**.

Il campo C dei numeri complessi-Parte prima

Un altro campo algebrico che è necessario introdurre è quello dei numeri complessi.
Essi rappresentano un insieme con una struttura molto ricca; non sono solo numeri con delle proprietà algebriche complete (rappresentano infatti un campo algebrico) ma con ulteriori proprietà geometriche, o meglio ancora,vettoriali.
Basti pensare che in essi la somma rappresenta anche una somma vettoriale, e il prodotto una rotazione di un vettore di un certo angolo unitamente alla dilatazione/contrazione del modulo.
Ma la cosa più importante è la chiusura algebrica che essi comportano; nel campo dei complessi una qualsiasi equazione algebrica ha **sempre** soluzioni.
Seguendo le moderne strutture algebriche non avremo difficoltà ad introdurre tali numeri senza dover parlare di "numeri immaginari" se non sotto un profilo storico.
Non so ancora bene come inquadrare questo articolo; l'insieme C dei complessi ha una struttura algebrica di campo, e quindi è un esempio che rientra nelle matematiche pure; d'altronde per chi non lo ha mai visto, bisogna richiamare le operazioni fondamentali, la forma trigonometrica ed esponenziale dei numeri complessi; non troverete però una accurata didattica, che esula dai nostri obiettivi.
Alla fine del secondo articolo metterò dei link per chi vuole esercitarsi a fondo.
A noi serviranno solo le proprietà e i metodi fondamentali che riguardano tali numeri, per introdurre concetti avanzati quali le ***forme modulari****,* ***la funzione zeta di Riemann****, ed altro ancora.*

I numeri complessi come estensione dei reali.

Gli insiemi numerici si sono evoluti dai ***numeri naturali*** ai ***numeri reali*** come successive estensioni atte a risolvere dei problemi algebrici ben precisi.

1. Da **N** a **Z**: ovvero dai numeri naturali agli interi relativi; Z si può vedere come una estensione dei naturali atta a risolvere il seguente problema: ***dati due numeri a,b con a<b, trovare un numero che sottratto ad a dia b***.

Si chiede cioè di risolvere la seguente equazione: **b=a-x**.
Esmpio: **5=2-x**; **x *non può essere un numero naturale***, infatti deve valere **-3**.
Bisogna uscire dall'ambito dei numeri naturali, dove il problema non ha soluzione, ed estenderli ad un nuovo insieme, quello degli interi con segno.

2. Da **Z** a **Q**, ovvero dai numeri relativi ai razionali.
   Si sa che in **Z**, l'equazione **ax=b** ha soluzioni se **b** è divisibile per **a**; se non lo è dobbiamo uscire dai numeri relativi ed estenderli ai razionali, ovvero alle frazioni.
   In tal modo sappiamo che l'equazione ha soluzione **x=b/a**.
   Esempio: **2x=3** non ha soluzioni all'interno dei numeri interi, infatti **x=3/2** è la soluzione, ***che è un numero razionale***.
3. Da **Q** a **R**; sappiamo che non esiste un numero razionale soluzione dell'equazione: $x^2 = 2$; per farlo dobbiamo uscire dai razionali ed estenderli ad un nuovo insieme , quello dei ***numeri reali***, dove ***oltre ai razionali troviamo anche gli irrazionali***, tipo $\sqrt{2}$, che è proprio una soluzione dell'equazione $x^2 = 2$.
   Se adesso io vi dicessi che voglio estendere **R** ad un nuovo insieme in cui risolvere l'equazione $x^2 = -1$ voi mi direste che è impossibile ; un numero elevato al quadrato non può dare un numero negativo perché più per più da più e meno per meno anche.
   Ma alla fine ,concettualmente, questa estensione sarebbe si diversa dalle altre, ma perché impossibile? Si tratterebbe di aggiungere dei numeri il cui quadrato dia un numero negativo.
   Basterà definire in modo opportuno le operazioni di somma e prodotto, come è stato fatto nelle altre estensioni.

Definizione (moderna) di numero complesso.

Definiamo un ***numero complesso*** come ***l'insieme delle coppie*** **(a,b)** di numeri reali, in cui siano definite certe operazioni.
Quindi intanto diciamo che un numero complesso è un elemento di **R x R**; Quando però abbiamo a che fare con i numeri, vogliamo mantenere le proprietà formali delle operazioni; ***essendo R un campo***, anche l'estensione deve essere un campo.
Daremo adesso la definizione di due operazioni ,che chiamiamo somma e prodotto, ma che sono soltanto due operazioni interne all'insieme; le chia-

miamo in tal modo per analogia,e per definire gli elementi **neutri** come **0** (somma) e **1**(prodotto); ma queste operazioni sono diverse dalle somme e i prodotti che conosciamo, pur derivando da combinazioni di esse.

Definizione di somma:

(a,b)+(c,d)=(a+c,b+d)

L'insieme **R x R** diventa un gruppo additivo con questa operazione.
Infatti l'operazione è commutativa:
(a,b)+(c,d)=(a+c,b+d)=(c+a,d+b)=(c,d)+a,b) essendo la s***omma commutativa in R.***

associatività:
(a,b)+(c,d)+(e,f)=(a+c,b+d)+(e,f)=(a+c+e,b+d+f)=(a,b)+ (c+e,b+f) essendo ***associativa in R***.
Esiste un elemento neutro rispetto la somma, ed è **(0,0)**; infatti
(a,b)+(0,0)=(a+0,b+0)=(a,b)
ogni elemento ha l'opposto:
opposto di (a,b) è (-a,-b); infatti:
(a,b)+ (-a,-b)=(a-a,b-b)=(0,0)
quindi è un gruppo rispetto alla somma.

Distinguiamo due differenti notazioni; se pensiamo a **C=R x R**, indichiamo con **0** l'elemento ***neutro di C rispetto alla somma***, che poi viene e***spresso come (0,0) in R x R.***

Definizione di prodotto:

(a,b)*(c,d)=(ac-bd,ad+bc)

Vediamo per prima cosa che questa definizione l'operazione di prodotto è distributiva rispetto alla somma:
(a,b)*[(c,d)+(c1,d1)]=(a,b)*(c+c1,d+d1)=
=(a(c+c1)-b(d+d1),a(d+d1)+b(c+c1))=
=(ac+ac1-bd-bd1,ad+ad1,bc+bc1)=
=(a,b)(c,d)+(a,b)(c1,d1).

L'operazione è commutativa:

$$z_1 * z_2 = (a_1, b_1) * (a_2, b_2)$$

$$= (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1)$$; essendo il ***prodotto commutativo in R***:

$$= (a_2 a_1 - b_2 b_1, b_2 a_1 + b_1 a_2) = z_2 * z_1$$

ed è associativa:

$$z_1 * (z_2 * z_3) = (z_1 * z_2) * z_3$$

La dimostrazione non è per niente difficile, ma molto noiosa.
Basta applicare la definizione di prodotto. Chi vuole provarci...
Con questa definizione, **R x R \{(0,0)}** diventa un gruppo moltiplicativo, avente **1**= **(1,0)** come elemento neutro. (anche qui indichiamo l'elemento neutro per il prodotto con **1** se pensato come elemento di **C**, in **R x R** dobbiamo indicarlo con **(1,0)**)
Infatti **(1,0)(c,d)=(1*c-o*d,1*d+0*c)=(c,d)**.
Notiamo poi che **-1**=**(-1,0)** (opposto di **-1**)
Un po' più difficile è provare l'esistenza dell'inverso per ogni numero diverso dallo **0**, cioè da **(0,0)**.
Per far ciò è necessario introdurre ***il concetto di coniugato***, e di modulo di un numero complesso.
Ma andiamo per ordine.

Forma algebrica

Un' altra notazione per i numeri complessi; la forma algebrica
Sia dato un piano cartesiano (ossia un piano con un sistema di coordinate cartesiane).
Allora ad ogni numero complesso **z=(a,b)**si può associare il punto del piano **P** avente coordinate **a** e **b**.
Tale corrispondenza è biunivoca (ossia ad ogni numero complesso **z** si associa un unico punto **P** ed ad ogni punto corrisponde un unico numero complesso).

Se ad ogni numero reale **a** associamo il numero complesso

a-->(a,0)

abbiamo una applicazione di **R--> R x R**
Possiamo osservare che le operazioni di somma e prodotto di numeri reali corrispondono alle rispettive operazioni dei numeri complessi associati.
Ossia, se **a,b**, sono numeri reali allora:
se a ------>(a,0) ,b------>(b,0)
allora: **a+b------>(a,0) + (b,0)=(a+b,0)** per la definizione di somma
ab-------->(a,0) * (b,0)=(ab,0) per la definizione di prodotto.
***Quindi l'insieme dei numeri reali può essere considerato come il sottoinsieme dei numeri complessi che consiste delle coppie del tipo* (a,0)**.
Osserviamo che il numero complesso **(o,b)** si può scrivere come **(0,b)=(b,0)*(0,1)** Basta applicare infatti la definizione di prodotto:

(b,0)*(0,1)=0*0-0*1,b*1+b*0)=(0,b)

Quindi ogni numero complesso z=(a,b) si può scrivere nella forma:

$$z=(a,0)+(0,b) =(a,0)+(0,1)*(b,0) \quad 1)$$

l'equazione 1) ci dice che ogni numero complesso si può scrivere come somma di **(a,0)** e del prodotto di **(b,0)** per l'elemento **(0,1)**.
Poniamo per definizione **i=(0,1)** e sostituiamolo nella 1):
Usando adesso l'identificazione dei numeri reali **a,b** con le coppie **(a,0), (b,0)** ed applicando la formula sopra otteniamo che ogni numero complesso **z=(a,b)** può essere scritto nella forma, anche detta forma algebrica:

$$z=a+ib$$

In questa forma risulta più facile fare i calcoli, perché ci riduciamo alla somma e prodotto di polinomi, che sappiamo far bene tutti.
Teniamo conto anche dell'identità fondamentale:

$$i^2 = -1$$

(infatti: $i^2 = i * i = (0,1) * (0,1)$***=(0*0-1*1,0*1+1*0)=(-1,0)=-1***)**

Possiamo infatti verificare facilmente che:
fare **(a,b)+(c,d)** con la definizione di somma , ovvero **(a+c,b+d)** equivale, usando i polinomi, a fare:
a+ib + c + id= a+c + i(b+d)

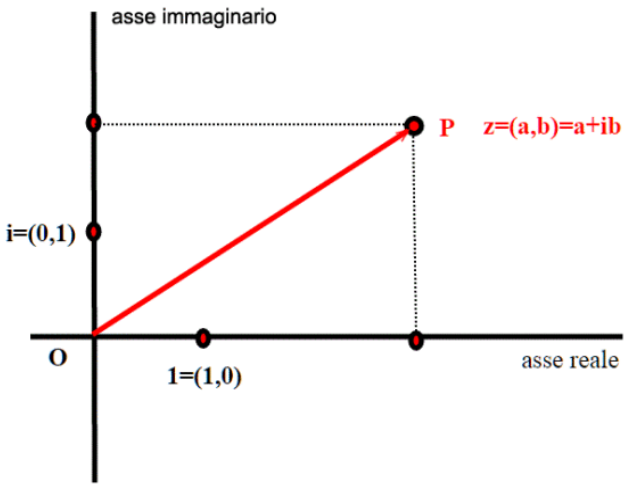
Per quanto riguarda il prodotto, sappiamo che con la notazione a coppie vale:
(a,b)*(c,d)=(ac-bd,ad+bc)
se uso la nuova forma:
(a+ib)*(c+id)=ac+iad +ibc+i*i bd)=ac -bd + i(ad+bc) dove abbiamo usato anche il fatto che **i*i=-1**

Dato il numero complesso **z=a+ib** per motivi storici continueremo a chiamare **a** parte reale e **b** parte immaginaria di **z, i** unità immaginaria.
Si usa anche indicare **a=Re(z), b=IM(z).**

Esempio di calcolo:

(1+i)(2-i)=2-i+2i-i*i=2+i+1=3+i
(non vorrei essere ripetitivo ; in questa notazione somme e prodotti di numeri complessi non dovrebbero essere un problema, perchè si riducono al calcolo con monomi e polinomi e tenendo conto anche del fatto che $i^2 = -1$)

Il piano dei numeri complessi (piano di Argand-Gauss)



Essendo i numeri complessi identificabili con coppie di numeri reali, è naturale rappresentarli graficamente come punti del piano cartesiano.
Quindi, facendo riferimento alla figura , il numero complesso **z=a+ib** verrà rappresentato dal punto di coordinate **(a,b)**.
In particolare l'origine **(0,0)** rappresenta il numero complesso **0**, il punto **(1,0)** rappresenta il numero complesso **1=1+0i**, il punto **(0,1)** rappresenta il numero complesso **i=0+1i**.
I punti dell'asse **x** del piano complesso corrispondono ai numeri reali **(x,0)=x+0i**.
Per cui l'asse **x** è chiamato asse reale.

I punti dell'asse **y** corrispondono ai numeri immaginari puri **(0,y)=0+iy** per cui l'asse **y** è chiamato asse immaginario.

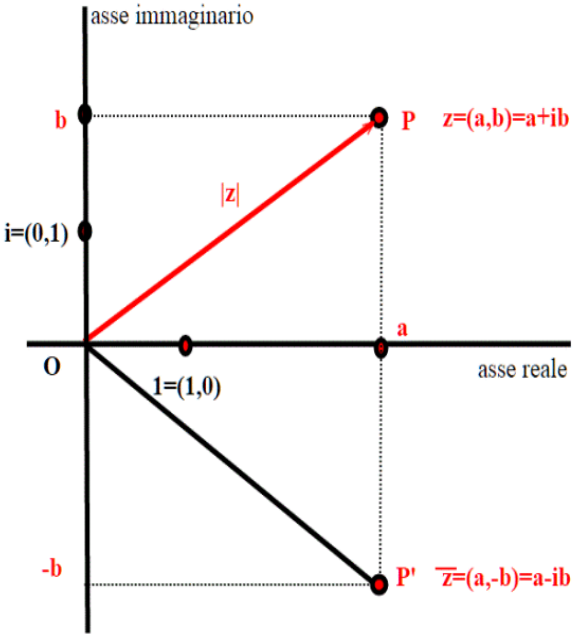
Coniugato e modulo di un numero complesso

Si definisce coniugato di **(a,b)** la coppia **(a,-b)**, ovvero in notazione algebrica:
coniugato di z=a+ib---> a-ib che si indica con $\overline{z}$.
Esempio di coniugati:
z=2+i, $\overline{z}$=2-i
z=2i; $\overline{z}$=-2i
z=a, $\overline{z}$=a qualsiasi sia **a** appartenente a **R**.

se invece consideriamo la quantità:

$$z * \overline{z} = (a + ib) * (a - ib) = a^2 - aib + aib - i^2b^2 = a^2 + b^2$$

(che è chiaramente un numero reale) questa, ***per il teorema di Pitagora***, altro non è che il quadrato del modulo del vettore che rappresenta **z** nel piano complesso.



osserviamo che:

1. nella rappresentazione sul piano, il coniugato è il simmetrico rispetto all'asse reale.
2. la somma di un numero con il suo coniugato dà un numero con sola parte reale $z + \overline{z} = a + ib + a - ib = 2a$
3. Il prodotto di un numero per il suo coniugato (abbiamo visto sopra) dà il quadrato del modulo.

Notiamo che il modulo di un numero complesso è nullo se (soltanto se) z=(0,0)=**0.**
Infatti $a^2 + b^2 = 0$
se (e solo se) **a=0, b=0** essendo **a,b** numeri reali.
Siamo adesso in grado di risolvere il seguente problema: ***dato un z qualsiasi, trovare il suo inverso***, ovvero un $z^{-1} : z * z^{-1} = 1$
abbiamo visto sopra che $z * \overline{z} = (a + ib) * (a - ib) = a^2 + b^2$,
quindi $\frac{z * \overline{z}}{a^2 + b^2} = 1$.

dunque $z^{-1} = \frac{\overline{z}}{a^2 + b^2}$

(notare che nel caso ***z sia reale***, **b=0**, $z^{-1} = \frac{a}{a^2} = \frac{1}{a}$, come deve essere
nel caso **z** sia puramente immaginario invece :
a=0, **z=ib**; $\overline{z}$**=-ib**; $z^{-1} = \frac{\overline{z}}{0^2 + b^2} = \frac{-ib}{b^2} = \frac{-i}{b}$)
quindi l' insieme che abbiamo definito è effettivamente un **campo.**

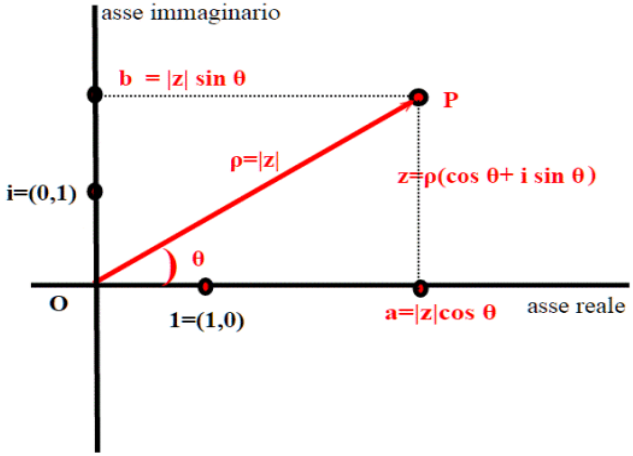
Esempio di calcolo dell'inverso.

Sia **z=2+3i;** $\overline{z}$**=2-3i**; $|z|^2 = a^2 + b^2 = 4 + 9 = 13$
$z^{-1} = \frac{\overline{z}}{|z|^2} = \frac{2 - 3i}{13}$; verifichiamo che $zz^{-1} = 1$:
$(2 + 3i)(2 - 3i)\frac{1}{13} = \frac{4 - 6i + 6i - 9i^2}{13} = \frac{13}{13} = 1$

Nel campo C dei numeri complessi l'equazione:
$x^2 = -1$ ammette come soluzioni $x = \pm i$; quindi abbiamo raggiunto il nostro scopo.
Ma c'è ben altro; il **Teorema fondamentale dell'algebra** dice ben di più:
Nel campo dei numeri complessi **C** l'equazione di grado **n** (***con n>=1***):
$a_n^{x^n} + a_{n-1}x^{n-1} + ...a_1 x = 0$
ha sempre n soluzioni, a patto che vengano contate con la loro molteplicità.
Ma questo cosa vuol dire? Chiariamolo con un esempio: $(x-2)^2 = 0$ ha una sola soluzione, ma che interviene con ***molteplicità due***, in pratica **2** è due volte soluzione dell'equazione, che si può anche scrivere come:
(x-2)(x-2)=0.
La dimostrazione di questo teorema (che è intuitivo, vista l'estensione che abbiamo fatto da **R a C**) è per noi fuori portata (***almeno per ora***).

Forma trigonometrica

Espressione di un numero complesso in forma trigonometrica o coordinate polari.
Vogliamo ora dare una espressione dei numeri complessi usando la trigonometria e le coordinate polari.
Torniamo al nostro piano complesso; un numero complesso rappresenta un vettore, che quindi possiamo rappresentare in coordinate polari:



dal disegno si vede già l'espressione trigonometrica del numero complesso; comunque, essendo :
z=a+ib
a=|z|cos (θ), b=|z| sin(θ), allora **z=a+ib=|z|cos (θ) +i|z| sin(θ)**;
se adesso chiamiamo ρ il modulo **|z|** del numero complesso, abbiamo:

$$z = \rho(cos(\theta) + isin(\theta));$$

$$\rho = \sqrt{a^2 + b^2}$$

Se siamo **nel primo quadrante** (cioè se **a>0, b>0**) si ha poi :

$$\frac{b}{a} = \frac{\rho \cdot sin\theta}{\rho \cdot cos\theta} = tg\theta; \theta = arctg(\frac{b}{a})$$

Altrimenti ricavare l'angolo sarà un problema che riguarda sempre l'arcotangente ma che avrà diverse soluzioni a seconda dei segni di di **a,b,** ovvero della posizione di **(a,b)** ***nel relativo quadrante***.
(Osserviamo che l'argomento di **z** è definito a meno di multipli interi di 2π tale è infatti la periodicità di seno e coseno).

esempio:
Sia z=1+i; vogliamo scriverlo in forma trigonometrica. Calcoliamo per primo il modulo, $|z| = \sqrt{a^2 + b^2} = \sqrt{1+1} = \sqrt{2}$;

$$\theta = arctg(\frac{b}{a}) = arctg(\frac{1}{1}) = arctg(1) = \frac{\pi}{2}$$

quindi la forma trigonometrica (o in coordinate polari) risulta:

$$z = \sqrt{2}(sin\frac{\pi}{2} + cos\frac{\pi}{2})$$

Il problema inverso è in ogni caso più semplice, basta calcolare seno, coseno di un angolo noto e poi moltiplicare per il modulo.

Prodotto di numeri complessi in forma polare.

Abbiamo visto che è possibile scrivere un numero complesso in questa forma:
$z = \rho(cos(\theta) + isin(\theta))$; ρ è il modulo **|z|** del numero complesso, mentre θ si scrive anche come **arg(z) (**θ**=arg(z)).**
Vogliamo adesso dimostrare che , dati **z1,z2**, se consideriamo il loro prodotto **z1* z2**,si ha:
|z1*z2|=|z1|*|z2| ovvero il modulo del prodotto è il prodotto dei moduli.
arg(z1*z2)=arg(z1) + arg(z2) ovvero l'argomento del prodotto è la somma degli argomenti.
Scriviamo i due numeri nella loro forma trigonometrica:

$$z_1 = \rho_1(cos\theta + isin\theta); z_2 = \rho_2(cos\alpha + isin\alpha)$$

$$z_1 \cdot z_2 = \rho_1(cos\theta + isin\theta)\rho_2(cos\alpha + isin\alpha) = \rho_1 \cdot \rho_2[cos\theta cos\alpha - sin\theta sin\alpha + i(cos\alpha sin\theta + sin\alpha sin\theta)]$$

Ma dentro alle parentesi quadre abbiamo due termini, uno reale che rappresenta lo sviluppo del coseno di una somma di angoli, mentre la parte immaginaria è lo sviluppo del seno di una somma di angoli.
Per concludere abbiamo:

$$z_1 \cdot z_2 = \rho_1 \cdot \rho_2[cos(\theta + \alpha) + isin(\theta + \alpha)]$$

che confrontata con questa:

$$z = \rho(cos(\theta) + isin(\theta))$$

Ci dice che il numero complesso ottenuto dal prodotto ha come modulo il prodotto dei moduli e come argomento la somma degli argomenti.
Per ora ci fermiamo qui; la prossima volta useremo questo risultato per esprimere la potenza di un numero complesso; vedremo poi un altro bellissimo modo per rappresentare un numero complesso.

Il campo C dei numeri complessi-Parte seconda

Riprendiamo il discorso sui numeri complessi; dopo aver dimostrato che ***C è un campo***, abbiamo visto alcune proprietà :

1. coniugato di un numero complesso
2. modulo di un numero complesso
3. metodo per trovare il reciproco di un numero complesso
4. Forma trigonometrica di un numero complesso
5. prodotto di due numeri complessi in forma trigonometrica

Applichiamo quest'ultima per dimostrare la **formula di De Moivre**:

$$(cos\theta + i \cdot sin\theta)^n = cos(n\theta) + i \cdot sin(n\theta)$$ 1)

metodo molto elegante per calcolare la potenza n-esima di un numero complesso semplicemente considerando un multiplo dell'angolo in rappresentazione trigonometrica.

Sia $z = cos\theta + i \cdot sin\theta$; sappiamo che il modulo di **z**,è **|z|=1**.

Vogliamo applicare il principio d'induzione.

Per **n=1 la 1)** è vera:

$$z^1 = cos(1 \cdot \theta) + i \cdot sin(1 \cdot \theta)$$

supponiamola vera per **n-1:**

$$z^{n-1} = cos((n-1) \cdot \theta) + i \cdot sin((n-1) \cdot \theta)$$

e dimostriamola per **n**:

$$z^n = z^{n-1} \cdot z = cos\big((n-1) \cdot \theta\big) + i \cdot sin\big((n-1) \cdot \theta\big) \cdot \big(cos\theta + i \cdot sin\theta\big)$$

Sappiamo, dall'articolo precedente, che l'argomento del prodotto è la somma degli argomenti.

Calcoliamo tale somma degli argomenti:

$$(n-1)\cdot\theta+\theta=n\cdot\theta$$

$z^n=cos(n\cdot\theta)+i\cdot sin(n\cdot\theta)$ che dà proprio la 1).

Newton e la funzione esponenziale.

Forse pochi sanno che la funzione esponenziale di base ***e*** è stata definita in un modo particolare da Newton.
Noi tutti oggi sappiamo che la derivata di e^x è ancora e^x; questo ci basta per affermare che soluzione dell'equazione differenziale:
$Df(x)=f(x)$
(se il termine equazione differenziale può spaventare pensiamo in questo caso semplicemente ad una equazione in cui l'incognita è una funzione la cui derivata è uguale alla funzione stessa) è proprio la funzione e^x.
Questo ci è stato insegnato alle superiori, ricavando le derivate fondamentali fra cui proprio quella di e^x, a cui ci si arriva tramite il limite fondamentale :

$$lim_{z\to 0}\frac{a^z-1}{z}=\ln(a)$$

essendo **ln(e)=1** (***logaritmo naturale***) nel caso la base della potenza sia ***e***, si ha:

$$lim_{z\to 0}\frac{e^z-1}{z}=\ln(e)=1$$

per calcolare la derivata di e^x basta scrivere il rapporto incrementale:

$$De^x=\lim_{h\to 0}\frac{e^{x+h}-e^x}{h}=\lim_{h\to 0}\frac{e^h-1}{h}\cdot e^x=1\cdot e^x=e^x$$

La soluzione dell'equazione non varia se moltiplichiamo e^x per una costante, quindi la soluzione generica è $f(x)=x_0\cdot e^x$, dove x_0 altro non è che il valore della funzione per **x=0**, essendo $e^0=1$, ovvero x_0**=f(0)**.

Queste sono cose che sappiamo però oggi; ai tempi di Newton non si sapevano tutte queste cose sulla funzione esponenziale.

Vediamo come procede invece Newton.
Il suo problema è quello di risolvere l'equazione differenziale: **Df(x)=f(x)**; ovvero trovare una funzione che sia uguale alla sua derivata.
E qui interviene il genio incomparabile di Newton: definisce una funzione proprio così, tramite l'equazione differenziale!
Newton procede allora così: ***la funzione non può essere un polinomio***, perché quando si deriva un polinomio si abbassa di uno il grado (quindi la funzione non potrebbe essere uguale alla sua derivata); però possiamo pensare ad un polinomio infinito, ovvero a una serie.
Continuiamo con il ragionamento di Newton; la nostra soluzione sarà una certa funzione, ma ogni funzione (sotto determinate condizioni) può espressa come una serie del tipo:

$$f(x) = \sum_{n=0}^{\infty} c_n x^n$$

Le costanti c_n sono date dallo sviluppo di **Taylor - Mc Laurin.**

$$c_0 = f(0); c_1 = Df(0); c_2 = \frac{D^2 f(0)}{2!}; ...; c_n = \frac{D^n f(0))}{n!}$$

e questa è una cosa;
ma il fatto che la derivata della funzione coincida con la funzione stessa, provoca questa catena:

$$Df(x) = f(x)$$
$$D^2 f(x) = Df(x)$$

...

$D^{n+1} f(x) = D^n f(x)$ che porta a:

$$D^{n+1} f(x) = D^n f(x) = ...Df(x) = f(x)$$

in particolare, se calcoliamo in zero le derivate successive, si ha:

$$D^{n+1} f(0) = D^n f(0) = ...Df(0) = f(0);$$

tornando adesso ai coefficienti dello sviluppo, essendo $c_n = \frac{D^n f(0)}{n!}$
ma essendo il valore della derivata n-esima indipendente da n ed uguale a **f(0)**, otteniamo che $c_n = \frac{f(0)}{n!}$ qualsiasi sia **n**;

*(notiamo che **f(0)** è un valore arbitrario, nei problemi di fisica è quello che si definisce valore iniziale).*

Quindi possiamo , nella serie $f(x) = \sum_{n=0}^{\infty} c_n x^n$; raccogliere **f(0)**, ottenendo:

$f(x) = \sum_{n=0}^{\infty} c_n x^n = f(0) \cdot \sum_{n=0}^{\infty} \frac{x^n}{n!}$; bene allora definiamo :

$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ e di conseguenza, calcolando la funzione in 1:

$$e^1 = \sum_{n=0}^{\infty} \frac{1^n}{n!} = \sum_{n=0}^{\infty} \frac{1}{n!} = 1 + \frac{1}{2} + \frac{1}{3!} + \frac{1}{4!} + ... = e$$

quindi abbiamo anche definito il numero ***e***, oltre a un metodo per calcolarlo.

Definizione di esponenziale complesso.

Il fatto di aver definito e^x come somma di una serie in campo reale, ci permette di estendere in modo naturale la definizione nel campo complesso: Definiamo esponenziale complesso la funzione:

$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$ dove **z** è un numero complesso.

Questo ha senso perché l'insieme dei numeri complessi è un campo, e in esso sono definite le operazioni di somma, prodotto, elevamento a potenza, rapporto.

Richiami sullo sviluppo in serie di seno e coseno

(in tutti questi esempi prendiamo per buono il fatto che le serie che trattiamo convergano, ovvero che abbiamo somma finita, per qualsiasi valore della variabile **x**)

Ricordando l'espressione della serie :

$$f(x) = \sum_{n=0}^{\infty} c_n x^n$$

Le costanti c_n sono date dallo sviluppo di **Taylor- Mc Laurin**

$$c_0 = f(0); c_1 = Df(0); c_2 = \frac{D^2 f(0)}{2!}; ...; c_n = \frac{D^n f(0))}{n!}$$

se consideriamo la funzione **sin(x)**, avremo:

$$c_0 = sin(0) = 0; c_1 = cos(0) = 1; c_2 = \frac{-sin(0)}{2} = 0; c_3 = -\frac{cos(0)}{6} = -\frac{1}{6}.$$

....

per cui $sin(x) = x - \frac{x^3}{6} + \frac{x^5}{120} + ...$

Vogliamo ora esprimere il termine generico della serie con una espressione funzione di **n;** notiamo il coefficiente del termine pari è nullo perché (lasciando per ora da parte i segni) partendo dal seno, se derivo una volta ottengo il coseno, se derivo due volte ottengo il seno; siccome devo calcolare la funzione in zero, il seno di zero è zero.
Il coefficiente pari dunque è nullo, quello dispari è unitario ma il segno parte da **1** (**cos(0)**) poi diventa **-1** (**-cos(0)=-1**) e così via.

Sappiamo poi che a denominatore abbiamo il fattoriale dell'esponente.

Il termine generico della serie è pertanto $\frac{(-1)^n}{(2n+1)!} x^{2n+1}$ come potete verificare sostituendo a **n** i valori **0,1,2,ecc**.
Infatti:

$$\frac{(-1)^0}{(2 \cdot 0 + 1)!} x^{2 \cdot 0 + 1} = \frac{1}{(1)!} x^1 = x$$ per **n=0**

$$\frac{(-1)^1}{(2 \cdot 1 + 1)!} x^{2 \cdot 1 + 1} = -\frac{x^3}{3!} = -\frac{x^3}{6}$$ per **n=1**

$$\frac{(-1)^2}{(2\cdot 2+1)!}x^{2\cdot 2+1} = \frac{x^5}{5!} = \frac{x^5}{120}$$ per **n=2** e così via.

Quindi in definitiva possiamo scrivere:

$$sin(x) = \sum_0^\infty \frac{(-1)^n}{(2n+1)!}x^{2n+1}$$

Analogo discorso vale per il coseno; qui sono invece i termini pari ad essere diversi da zero.

$$cos(x) = 1 - \frac{x^2}{2} + \frac{x^4}{4!} + ...(-1)^n \frac{x^{2n}}{(2n)!}$$

in questo caso il termine generale è $(-1)^n \frac{x^{2n}}{(2n)!}$

calcoliamo i primi valori.

$(-1)^0 \frac{x^0}{(0)!} = 1$ per **n=0**

$(-1)^1 \frac{x^2}{(2)!} = \frac{x^2}{2}$ per **n=1**

$(-1)^2 \frac{x^{2\cdot 2}}{(2\cdot 2)!} = \frac{x^4}{4!}$ per **n=4**

l'espressione compatta diventa:

$$cos(x) = \sum_{n=0}^{\infty}(-1)^n \frac{x^{2n}}{(2n)!}$$

Riassumendo: lo sviluppo di **sin(x)** mi dà tutte le *potenze dispari*, quello di **cos(x)** tutte le *potenze pari*.
In entrambi i casi, la potenza viene divisa per il fattoriale dell'esponente.

Viene in mente una cosa; sovrapponendo (sommando) le due serie si ottiene una serie di potenze per così dire "completa":

$1 + x - \frac{x^2}{2} - \frac{x^3}{6} + \frac{x^4}{4!} + \frac{x^5}{120} + \ldots$ che assomiglia molto allo sviluppo in serie dell'esponenziale:

$1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{4!} + \frac{x^5}{120} + \ldots$ a parte i segni.

Forse è stata proprio questa somiglianza a spingere ***Eulero*** nel cercare una relazione fra esponenziale e funzioni trigonometriche; ma per trovarla non bastavano i numeri reali, doveva cercarla nei numeri complessi.

La formula di Eulero

La formula di Eulero è (***assieme all'identità di Eulero*** che vedremo appena dopo) una delle formule più belle della matematica.
Essa esprime il legame fra la funzione esponenziale di base ***e*** *(numero di* ***Nepero****)* in C e la forma trigonometrica di un numero complesso; supponiamo che x sia un numero reale,
allora *ix* è un numero complesso (immaginario puro); la funzione :
e^{ix}
sarà una funzione a valori complessi ; infatti è somma della serie:

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

Sappiamo poi che qualsiasi numero complesso si può scrivere in forma trigonometrica come:
$cosx + isinx$; ebbene la formula di Eulero ci dice che:
$e^{ix} = cosx + isinx$
Dimostriamo la formula partendo dalla definizione di esponenziale complesso.

Abbiamo definito l'esponenziale complesso come:

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

Consideriamo adesso un numero complesso immaginario puro, ovvero **z=iy**.

$$e^{iy} = \sum_{n=0}^{\infty} \frac{i^n y^n}{n!}$$

(abbiamo semplicemente scritto **iy** al posto di **z** nello sviluppo)

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!})$$

Spezziamo adesso la serie $\sum_{n=0}^{\infty} \frac{i^n y^n}{n!}$ in due parti (esponenti pari e esponenti dispari) $\sum_{n=0}^{\infty} \frac{i^n y^n}{n!} = \sum_{n=0}^{\infty} \frac{i^{2n} y^{2n}}{(2n)!} + \sum_{n=0}^{\infty} \frac{i^{2n+1} y^{2n+1}}{(2n+1)!}$ 1);

nel primo addendo abbiamo infatti tutte le potenze pari :

$$\sum_{n=0}^{\infty} \frac{i^{2n} y^n}{(2n)!} = 1 + \frac{i^2 y^2}{2} + \frac{i^4 y^4}{4!} + \ldots$$

nel secondo $\sum_{n=0}^{\infty} \frac{i^{2n+1} y^{2n+1}}{(2n+1)!} = i + \frac{i^3 y^3}{3!} + \frac{i^5 y^5}{5!} + \ldots$

tutte le potenze dispari (basta sostituire ad n i valori **0,1,2,3,...**)

osserviamo che $i^{2n} = (i^2)^n = (-1)^n$

mentre $i^{2n+1} = i \cdot i^{2n} = i \cdot (-1)^n$

quindi possiamo riscrivere la 1) :

1. $$\sum_{n=0}^{\infty} \frac{i^n y^n}{n!} = \sum_{n=0}^{\infty} \frac{(-1)^n y^{2n}}{(2n)!} + i \cdot \sum_{n=0}^{\infty} \frac{(-1)^n) y^{2n+1}}{(2n+1)!}$$

Usiamo adesso i due sviluppi di seno e coseno che abbiamo calcolato sopra:

$$cos(x) = \sum_{n=0}^{\infty}(-1)^n \frac{x^{2n}}{(2n)!}; sin(x) = \sum_{0}^{\infty} \frac{(-1)^n}{(2n+1)!}x^{2n+1};$$

confrontando con la formula sopra otteniamo subito che:

$$e^{iy} = \sum_{n=0}^{\infty} \frac{i^n y^n}{n!} = cos(x) + isin(x))$$

Identità di Eulero.

Eccoci arrivati all'identità di **Eulero**; essa non è altro che un caso particolare della formula:

$e^{ix} = cosx + isinx$
quando $x = \pi$; la formula diventa:

$e^{i\pi} = cos\pi + isin\pi = -1 + 0 = -1$ ovvero:

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

L' identità di Eulero resta una delle formule più belle della matematica.
Richard Feynman disse che questa formula era straordinaria perché legava fra di loro le maggiori entità della matematica: il ***numero zero*** (*elemento neutro per la somma)*, il ***numero uno***, (*identità per il prodotto)*; il ***numero irrazionale p-greco*** e il ***numero irrazionale e; l'unità immaginaria i, la somma e l'elevamento a potenza.***

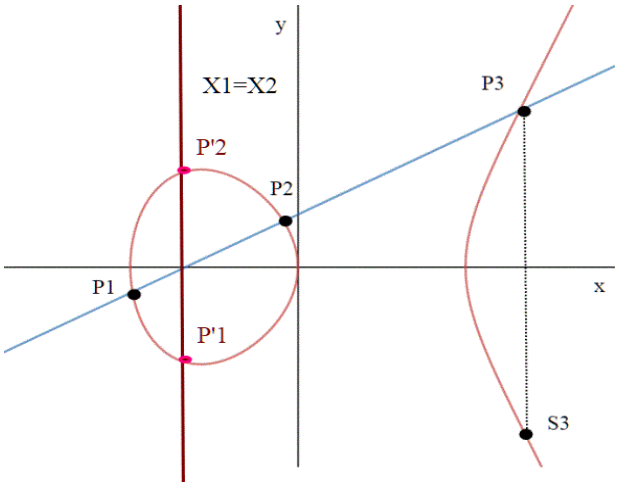
Ndr: l*a trattazione teorica permette di affrontare tutte le problematiche di base sui numeri complessi.*
La didattica vera e propria esula dagli obiettivi di questi articoli.
Per chi non li ha mai visti, per impratichirsi sarebbe meglio esercitarsi.

I punti impropri della geometria proiettiva

Si può partire dalla equazione generale di una curva ellittica che è la seguente:

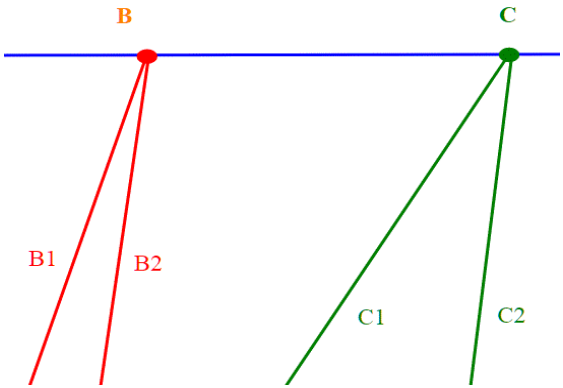
$$y^2 = x^3 + ax + b$$

Prossimo nostro obiettivo sarà quello di dimostrare che con questa operazione i punti della curva formano un gruppo, se aggiungiamo però a tale insieme un punto che non è nel piano, anche se appartiene alla curva.
Tale punto è detto "**punto all'infinito**".
Ricordo brevemente come abbiamo definito l'operazione: si considerano due punti della curva (che possono anche coincidere) e si traccia la retta per quei due punti (nel caso coincidano è la tangente); detto **P3** il terzo punto in qui la retta incontra la curva (e abbiamo dimostrato che esiste), costruiamo il simmetrico rispetto all'asse delle **x**; tale punto è il risultato dell'operazione.
Tutto questo è valido se **x1<>x2**; nel caso **x1=x2** (e $y_1 \neq y_2$) la retta diventa parallela all'asse delle **y** e sembra non intersecare più la curva.
In realtà possiamo pensare che la intersechi all'infinito

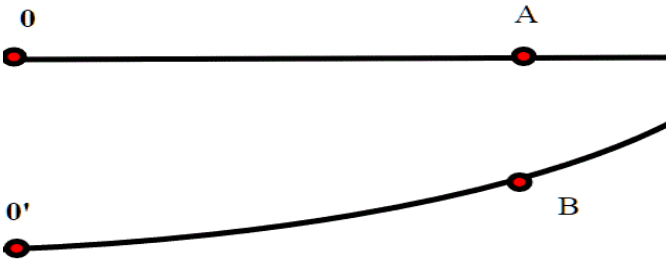


I punti all'infinito della geometria proiettiva

La geometria proiettiva nasce dall'esigenza di unificare determinati discorsi in ambito geometrico; succede infatti di trattare delle dimostrazioni la cui soluzione può ad esempio dipendere dall'intersezione fra due rette; sappiamo che due rette si intersecano se non sono parallele, quindi all'interno di determinate dimostrazioni dovremmo distinguere una casistica, e ciò in matematica non va bene.
Si supera lo scoglio passando ad un altro tipo di piano, detto proiettivo, in cui due rette hanno sempre intersezione, anche se sono parallele. Tali punti di intersezione si dicono punti impropri.
Comincio il discorso sui punti impropri delle geometria proiettiva servendomi di un articolo molto bello sui punti all'infinito nel piano ,che potete trovare a questo indirizzo http://www.infinitoteatrodelcosmo.it/2013/10/10/1-zero-e-infinito/.
Consiglio di leggerlo per chi affronta per la prima volta questo tipo di discorsi.
Riassumendo in poche parole tale articolo, dall'osservazione che rette parallele in realtà prospetticamente si incontrano all'orizzonte in un punto e che diverse coppie di rette parallele si incontrano sempre all'infinito ma in punti distinti, possiamo introdurre una nuova categoria di punti, detti punti impropri, che altro non rappresentano che la direzione di tali rette.
Procedendo in tale modo, anche le rette parallele avranno una intersezione; tale intersezione è proprio un punto improprio.

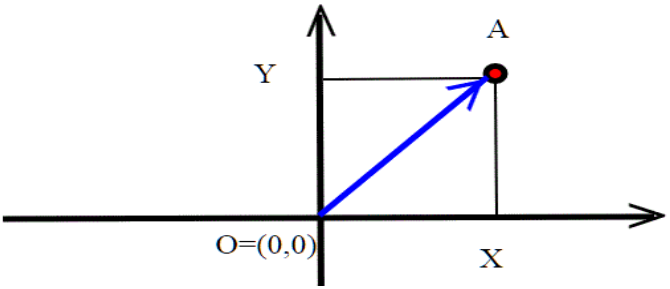


Le rette **B1** e **B2** sono parallele; prospetticamente parlando si intersecano in un punto **B** *all'infinito*; **C1** e **C2** sono anch'esse parallele, ma non a **B1**, **B2**; si intersecano in un altro punto **C**; i punti **B** e **C** si trovano su una retta detta retta impropria.



Un breve discorso sulle dimensioni

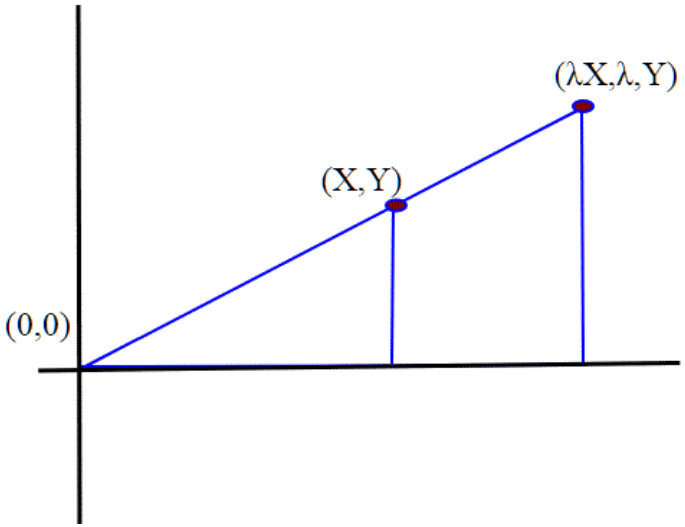
In matematica, non esiste una definizione di dimensione che comprenda adeguatamente tutte le situazioni in cui vorremmo farne uso.
Si supera il concetto quando si parla di spazio vettoriale, che noi però non abbiamo trattato.
Possiamo però pensare alla dimensione usando le coordinate; per individuare un punto sulla retta basta una coordinata (fissato **O** altro non è che la distanza **OA**); si dirà in questo caso che la retta ha dimensione 1.
Possiamo però estendere questo discorso anche ad una linea curva; stabilendo una origine, possiamo individuare il punto con una coordinata (***detta curvilinea***) che altro non è che la lunghezza dell'arco **OB**.
Nel piano servono due coordinate per individuare un punto; qui abbiamo dimensione 2.



Esistono anche qui altri oggetti con dimensione due; in una superficie si possono infatti trattare coordinate curvilinee; anche qui servono due coordinate per individuare un punto.
La dimensione di un oggetto geometrico è quindi il numero minimo di coordinate che servono per individuare un suo punto.

Le coordinate proiettive: La retta proiettiva

Consideriamo le coppie del piano **R x R**, escludendo **(0,0)**; sappiamo cosa rappresenta una coppia **(X,Y)**;
Un vettore che parte da **(0,0)** e arriva in **(X,Y)**.
Consideriamo i vettori con coordinate proporzionali ovvero vettori del tipo **(X,Y)**, **(λX,λY)** con **λ<>0**.
Tutti tali vettori hanno in comune la direzione .
Possiamo vederlo dal fatto che formano triangoli simili:



Ricordate le relazioni d'equivalenza? A mio avviso sono il modo più completo per introdurre gli spazi proiettivi.

Definiamo una relazione d'equivalenza in **R x R**, (con **(X;Y)**$\neq$**(0,0)** in questo modo:

$(X,Y) \sim (X',Y')$ se (e solo se) $(X,Y) = \lambda(X',Y')\, \lambda \neq 0$;

Per vedere che è una relazione d'equivalenza dobbiamo verificare che:

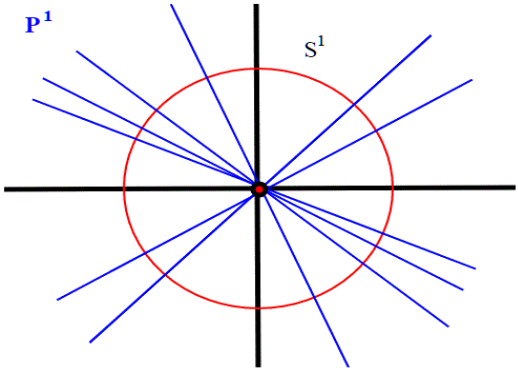
1. è riflessiva
2. èsimmetrica
3. è transitiva

per dimostrare la 1 : (X,Y)=$1 \cdot (X,Y)$

2 : se $(X,Y) = \lambda(X',Y')$ e $\lambda \neq 0, \frac{1}{\lambda}(X,Y) = (X',Y')$

3: se $(X,Y) = \lambda(X',Y')$ e $(X',Y') = \mu(X'',Y'')$
allora $(X,Y) = \lambda\mu(X'',Y'')$

L'insieme delle classi di equivalenza (***insieme quoziente***) si chiama **retta proiettiva** e si indica con $P^1(R)$.
Possiamo pensare di identificare tutte le direzioni con i punti di un cerchio di raggio unitario centrato nell'origine:



L'insieme di tutte le direzioni corrisponde proprio ai punti sul cerchio (considerando uguali quelli antipodali; qui stiamo parlando di direzione, non ci interessa il verso).
Ecco perché abbiamo escluso in punto **(0,0)**; il **vettore nullo non individua nessuna direzione.**
Il punto **(1,2)** ha indifferentemente coordinate **(1,2), (2,4), (-1,-2,), (-2,-4)** ecc.
Tali coordinate prendono il nome di coordinate proiettive omogenee.
Se adesso pensiamo di dividere la prima coordinata per la seconda otteniamo **1/2** in ogni caso.
In generale tutte le coppie **(X,Y)** se **Y**$\neq$**0** possono essere identificate con **(X/Y,1)**; quindi ogni punto può essere identificato da **(K,1)** (che quindi è un ***oggetto geometrico di dimensione 1***).
Questo genera una corrispondenza biunivoca fra $P^1(R)$ privato del punto **(X,0)** e la retta reale.
Nella retta R ogni punto può essere individuato solo da **X**; questa si chiama semplicemente coordinata, come sappiamo.
Riassumendo:

1. ***Spazio proiettivo*** $P^1(R)$; ogni punto viene individuato da due coordinate dette proiettive omogenee
2. ***Retta reale*** **R**; per individuare un punto basta una coordinata.
   Tale coordinata di solito si chiama ***coordinata affine***, o non omogenea.

Esiste una corrispondenza biunivoca fra $P^1(R)$ in cui escludiamo il punto **(X,0)** e la retta **R**.
Si può pensare di estendere questa corrispondenza a tutto $P^1(R)$ in tal modo; aggiungendo a **R** un punto, detto punto infinito.
Quindi $P^1(\mathbb{R}) \cong \mathbb{R} \bigcup \{\infty\}$.
Tale infinito salta fuori, intuitivamente, da una divisione per zero.

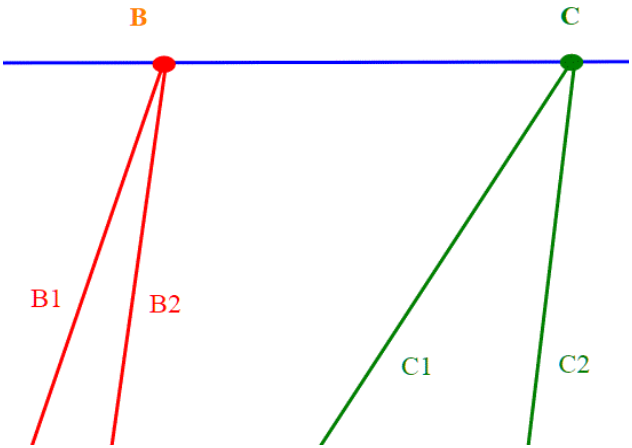
Il piano proiettivo

Consideriamo adesso l'insieme **R x R xR**, ovvero delle terne di numeri reali **(X,Y,Z)** supponiamo inoltre che **(X,Y,Z)**$\neq$**(0,0,0)**.
Tutti i vettori (***punti)*** uscenti dall'origine individuano una direzione.
Escludiamo il vettore nullo perché non individua nessuna direzione.

Definiamo una relazione in tal modo: $(X, Y, Z) \sim (X', Y', Z')$ se (e solo se) $(X, Y, Z) = \lambda(X', Y', Z'), \lambda \neq 0$.
Questa è ancora una relazione d'equivalenza, come nel caso precedente di **RxR**.
La classe di equivalenza di questa relazione è costituita dalle terne con coordinate proporzionali; tale classe prende il nome di punto proiettivo.
Per rappresentare la classe, sappiamo che possiamo prendere qualsiasi rappresentante; per esempio **(6,4,18) , (12,8,36) , (3,2,9)** sono tutte terne equivalenti.
Si definisce **piano proiettivo**, e si indica con $P^2(R)$ l'insieme quoziente di tale relazione d'equivalenza, ovvero l'insieme di tutte le classi.
Consideriamo adesso le terne **(X,Y,Z)** dove **Z**$\neq$**0**; possiamo dividere per **Z** (ovvero moltiplicare per **1/Z**);
(N.B. : abbiamo diviso per **Y**, supponendo **Y**$\neq$**0**; questa è una scelta arbitraria, avremmo potuto dividere per **X** o per **Y** e il succo del discorso non cambierebbe, è solo una scelta di notazione).
La terna **(X/Z,Y/Z,1)** è equivalente alla terna **(X,Y,Z)**.
Poniamo adesso **X/Z=K**, **Y/Z=K'** e otteniamo che il generico punto (con **Z** $\neq$**0**) può essere indicato con **(K,K',1)**.
La generica terna di questo tipo è in corrispondenza biunivoca con **R x R**; questo tipo di punti si chiamano "**punti finiti**" o "***punti propri***" e corrisponde in pratica al nostro piano usuale.
Questo oggetto geometrico ha dimensione quindi 2.
Per ottenere tutto il piano proiettivo, ai punti finiti vanno aggiunti quindi soltanto i punti con **Z = 0**.
Se **Z = 0** le classi di equivalenza che si ottengono sono del tipo **[X ,Y , 0]** con **X** e **Y** non entrambi nulli: il loro insieme si identifica * pertanto con la retta proiettiva **P1(R)** e viene detto retta all'infinito e i suoi punti **[X , Y , 0]** sono detti punti all'infinito.
Possiamo concludere che il piano proiettivo altro non è che l'unione del piano usuale con la retta all'infinito.
*(infatti, se Z=0, $(X, Y, 0) \sim (X, Y, 0)$ se e solo se $(X, Y, 0) = \lambda(X, Y, 0)$ e questo se e solo se $(X, Y) = \lambda(X, Y)$; ma questo identifica la retta proiettiva.)

Per concludere questo breve discorso, vediamo che il piano proiettivo $P^2(R)$ è un oggetto un po' strano.

Di solito uno oggetto geometrico è l'insieme dei suoi punti; qui, invece è anche l'unione di un piano (***spazio di dimensione 2***) con una retta (***spazio di dimensione 1***) che sono insiemi disgiunti.
Abbiamo formalizzato in pratica ciò che si intuiva dalla figura 1:



Il piano proiettivo è l'unione fra il piano usuale e la retta impropria, che contiene tutti i punti all'infinito

Piano proiettivo e piano affine

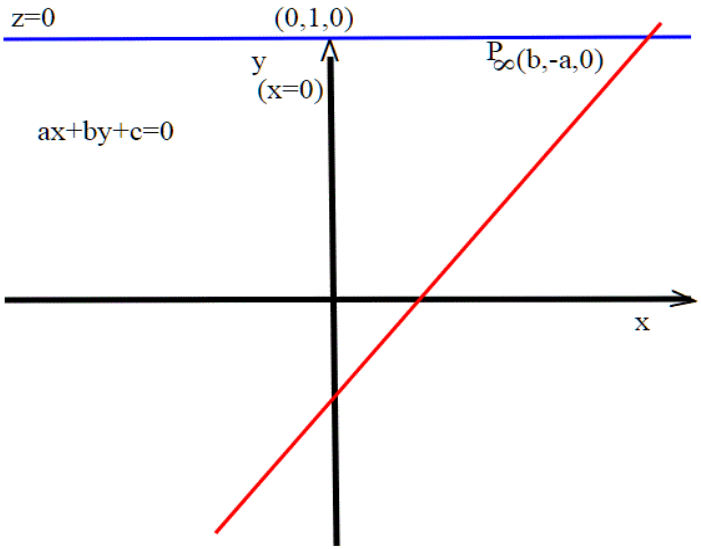
Tanto per puntualizzare ed evitare confusione nei prossimi discorsi: il piano proiettivo è l'insieme di tutti i punti con coordinate proiettive (***classi della relazione di equivalenza***); certi punti si possono anche esprimere con coordinate non omogenee, o affini.
Sono i punti usuali di **R x R**, che possiamo identificare anche con ***il piano Euclideo***.
Tale piano prende anche il nome di **piano affine**.
Nel piano proiettivo abbiamo in più i punti impropri, quelli con coordinata omogenea **Z=0**, che non possiamo trasformare con coordinate affini, non potendo dividere per zero.
Tali punti però possono essere messi in corrispondenza biunivoca con una retta proiettiva, come visto sopra.

Equazione della retta e punti della retta proiettiva $P^1(R)$*.*

Siamo partiti da un piano ed arrivati ad una retta, i cui punti coincidono con le direzioni delle rette del piano passanti per l'origine.
Ma nel piano, con le coordinate abituali, qual'è l'equazione di una retta? Consideriamo rette per l'origine, quindi l'equazione sarà: **ax+by=0**.
Chiaramente, se moltiplichiamo per un valore <> **0**, l'equazione rimane sempre vera.
Questa retta corrisponde ad un punto (***direzione***) di $P^1(R)$; quale sarà? Semplicemente il punto di coordinate omogenee **(b,-a).**
Facciamo ora uno sforzo in più e andiamo nel piano affine (quello solito, tanto per capirsi).
L'equazione di una retta sarà **ax+by+c=0**; la sua direzione (o ***punto improprio***) sarà il punto di coordinate omogenee **(b,-a,0)**; consideriamo due retta parallele, ad esempio **2x+4y+3=0. 2x+4y+7=0**
Il punto improprio (direzione) di entrambe sarà **(4,-2,0)**.
Se guardiamo adesso alle rette come immerse nel piano proiettivo, le loro equazioni si trasformano passando da coordinate affini a coordinate omogenee:
x--->X/Z,y--->Y/Z; le equazioni (siamo nel piano affine , **Z<>0**) diventano:

2X/Z+4Y/Z+3=0
2X/Z+4Y/Z+7=0
2X+4Y+3Z=0
2X+4Y+7Z=0

Notiamo che il punto **(4,-2,0)** appartiene ad entrambi le rette; basta infatti sostituire:
2*4-4*2+3*0=0
2*4-4*2+7*0=0; quindi appartiene all'intersezione delle due rette.
Nel piano proiettivo, due rette parallele si incontrano in un punto improprio. Che due rette non parallele si incontrino sempre in un punto lo sappiamo già; quindi nel piano proiettivo due rette si incontrano sempre.
Che punto improprio ha l'asse **y**? Be', la sua equazione è **x=1* x=0**, quindi **(b,-a,0)=(0,1,0)** (sarebbe **-1**, ma moltiplichiamo per **-1** ottenendo un punto equivalente).



Questo disegno non deve farci ingannare; ***la retta blue dove si interseca la retta rossa non è una retta parallela all'asse delle x***; ***è la retta all'infinito***.

Equazioni algebriche omogenee.

Una equazione algebrica è rappresentata da un polinomio in una o più variabili di cui si cercano le radici. Essa è determinata da una espressione del tipo F(x,y)=0 (se per esempio siamo in due variabili).
Un equazione algebrica omogenea è un'equazione algebrica in più variabili i cui termini hanno tutti lo stesso grado.
Facciamo un esempio:

$x^2 - xy + y^2 = 0$ è un equazione algebrica omogenea in due variabili.

La particolarità delle equazioni omogenee è che ammettono sempre una soluzione banale, quella in cui le variabili sono tutte nulle.

Se prendiamo infatti la nostra equazione e sostituiamo a **x,y** i valori **0,0** otteniamo:

$$0^2 - 0 \cdot 0 + 0^2 = 0$$

Notiamo una cosa; se una equazione omogenea ha una soluzione, allora ne ha infinite. Prendiamo sempre come esempio l'equazione:

$x^2 - 2xy + y^2 = 0$ che ha come soluzione la coppia **(1,1)** allora preso un λ qualsiasi, **λ(1,1)=(λ,λ)**,

$$\lambda^2 - 2\lambda \cdot \lambda + \lambda^2 = 2\lambda^2 - 2\lambda^2 = 0$$

Questo ci ricorda subito i discorsi fatti sulle coordinate omogenee; se studiamo quindi delle equazioni nel piano proiettivo, dobbiamo **per forza** trattare equazioni omogenee.

Equazione generica di una curva ellittica nel piano proiettivo

Abbiamo visto nell'introduzione che per studiare in modo completo una curva ellittica da punto di vista algebrico (legge gruppale) abbiamo bisogno dei punti all'infinito; quindi possiamo pensare di usare il piano proiettivo; ma nel piano proiettivo ci sono le coordinate omogenee, quindi anche la forma generale dell'equazione ellittica deve essere omogenea.
Studiamo quindi le equazioni del tipo*:

$Y^2Z = X^3 + aXZ^2 + bZ^3$ **1)**

(nota *: l'equazione è stata semplificata usando trasformazioni un particolare sistema di coordinate; ciò comunque nulla toglie alla validità del discorso)
qualcuno mi dirà; cos'è questa cosa così complicata? non assomiglia affatto all'equazione:

$y^2 = x^3 + ax + b$ **2)**

ed ha una variabile in più, Z.

Ma se ricordiamo il legame fra coordinate omogenee e coordinate affini, vediamo che infondo sono la stessa cosa.
Infatti se siamo nel piano affine, un punto si individua con due coordinate, **(x,y)**.
Vediamo che la 2) altro non è che la 1) eseguendo un cambio di coordinate da proiettive a coordinate affini (o non omogenee).
Sappiamo infatti che nel caso il punto sia nel piano affine, la coordinata **Z** è

diversa da zero; dividiamo allora la 1) per Z^3:

$$\frac{Y^2 Z}{Z^3} = \frac{X^3}{Z^3} + \frac{aX Z^2}{Z^3} + \frac{bZ^3}{Z^3}$$

$$\frac{Y^2}{Z^2} = \frac{X^3}{Z^3} + \frac{aX}{Z} + b$$

sappiamo che $\frac{Y}{Z} = y; \frac{X}{Z} = x$; se sostituiamo otteniamo proprio la 2):

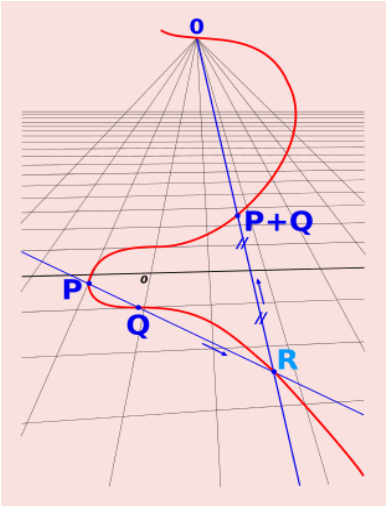
$$y^2 = x^3 + ax + b.$$

Però adesso che siamo nel piano proiettivo possiamo risolvere il problema del punto all'infinito; come fare per trovare i punti all'infinito della curva? Facile,basta intersecarla con la retta proiettiva, ovvero la retta all'infinito. Tale retta sappiamo che ha equazione Z=0

Si tratta quindi di risolvere il sistema:

$$\begin{cases} Y^2 Z = X^3 + aX Z^2 + bZ^3 \\ Z = 0 \end{cases}.$$

che dà come unica soluzione **X=0**.
Quindi abbiamo **Z=0** e **X=0**.
Questo unico punto, che chiameremo $\ominus$ ha quindi coordinate omogenee **(0,X,0)**, con **X<>0**.
Infatti sappiamo che **(0,0,0)** non appartiene al piano proiettivo.
Possiamo dividere per **X** essendo **X<>0**, ottenendo $\ominus$**=(0,1,0)**.
Cosa rappresenta $\ominus$? Sappiamo che il punto improprio **(b,-a,0)** è la direzione della retta **ax+by+c=0**.
Quindi **(b,-a,0)=(0,1,0)** dà **b=0**; quindi **ax=0**, **a<>0**, **x=0**.
Questa è la direzione delle rette parallele all'asse delle **y**, come abbiamo visto anche sopra.

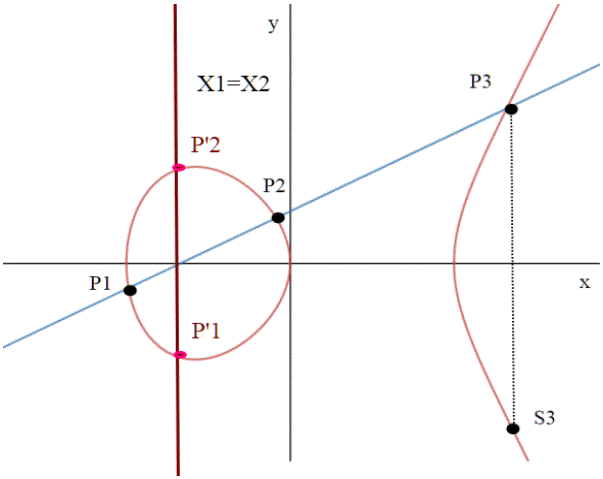


un'immagine molto suggestiva che ci fa intuirecome la curva ellittica intersechi la retta impropria all'infinito.

Quindi oltre ai punti affini soluzioni della 2) la curva ellittica ha anche un altro punto (improprio) che chiamiamo $\ominus$, o anche punto all'infinito.
Siamo adesso in grado di dare una definizione più precisa di somma fra punti della curva:
Siano **P; Q** due punti appartenenti alla curva, e sia **L** la retta per **P** e **Q**.
(Se **P = Q**, allora **L** è la retta tangente in **P** a **E**).
Sia **R** il terzo punto di intersezione di **L** con **E** e sia **L'** la retta passante per **R** e $\ominus$.
Allora **L'** interseca **E** in **R;**$\ominus$ e in un terzo punto che denotiamo con **P + Q**.
Questa nuova definizione di somma comprende anche quella data in precedenza, ed è valida sempre, anche la retta per **P** e **Q** dovesse essere parallela all'asse delle **y**.
Ma questo e anche la verifica che con questa operazione abbiamo creato un gruppo, lo vedremo in dettaglio la prossima volta.

Il gruppo delle curve ellittiche, parte prima

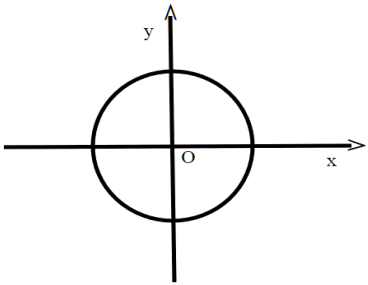
Riprendiamo il discorso sulle curve ellittiche; nell' articolo precedente, abbiamo trovato il punto all'infinito di una curva ellittica di equazione generica: $y^2 = x^3 + ax + b$; esso coincide con il punto all'infinito dell'asse delle **y**; questo ci fa capire che la curva all'infinito è tangente all'asse delle **y**.
Adesso volevo evidenziare meglio il fatto che la curva ellittica **non è una** funzione ma un luogo geometrico di punti.
Una funzione infatti per ogni valore della **x** ha un solo valore dell'**y**; si vede anche dal grafico che nel caso delle curve ellittiche ciò non è vero sempre.



L'operazione che abbiamo definito sui punti della curva , che dati due punti trova il risultato S3 come indicato nel disegno, è valida sia nel caso che la retta passi per due punti distinti, oppure sia verticale (il punto diventa il punto improprio $\ominus$ o punto all'infinito).
Nel quiz sulle curve ellittiche:
(http://www.infinitoteatrodelcosmo.it/2017/03/21/soluzione-al-quiz-il-fantasma-di-galois/) abbiamo fatto in dettaglio i calcoli nel caso **x1<>x2** per trovare il terzo punto **S3.**
Nel caso la retta per **P1,P2** sia verticale sappiamo che il punto è $\ominus$; ci manca da trovare il punto nel caso **P1=P2** e **y1=y2**, ovvero quando la retta è tangente alla curva.
Ma procediamo per gradi.

Le funzioni implicite.

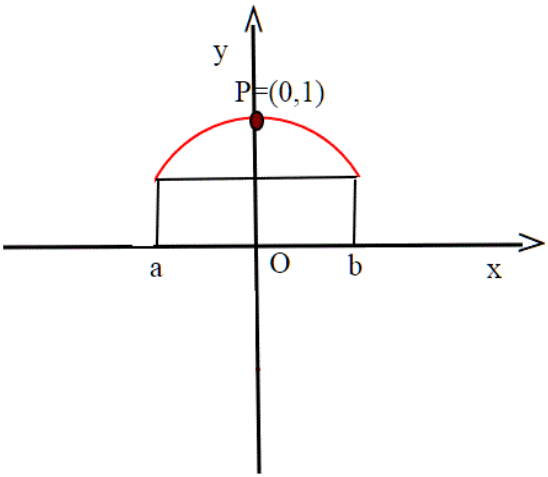
Le curve ellittiche sono un esempio di funzioni definite implicitamente .
Ma per capirlo meglio, cominciamo da un caso più semplice; una circonferenza con centro nell'origine e di raggio unitario.



Come tutti sappiamo, tale circonferenza ha equazione $x^2 + y^2 = 1$.
Ma guardiamo adesso la cosa da un punto di vista diverso; consideriamo la funzione di due variabili:
$F(x, y) = x^2 + y^2 - 1$; tale funzione è definita su tutto **RxR--->R**.
Consideriamo adesso solo i valori per cui **F(x,y)=0**;
Tali valori definiscono proprio la circonferenza di sopra.
Infatti:
$F(x, y) = x^2 + y^2 - 1 = 0$; cioè $x^2 + y^2 = 1$.

Cosa vuol dire questo discorso? Che data una funzione di due variabili, i punti in cui la funzione si annulla definiscono un luogo geometrico, che può essere o meno una curva.

Ci chiediamo se, almeno localmente, tutte le soluzioni dell'equazione **F(x,y)=0** si possono rappresentare tramite una funzione della sola **x** oppure tramite una funzione della sola **y**, ovvero se esiste una funzione **f** tale che **F(x, f(x)) = 0** o esiste una funzione **g** tale che **F(g(y), y) = 0**.
Torniamo alla nostra circonferenza, e consideriamo il punto **P(0,1)** che vi appartiene, e che quindi è soluzione dell'equazione **F(x,y)=0**

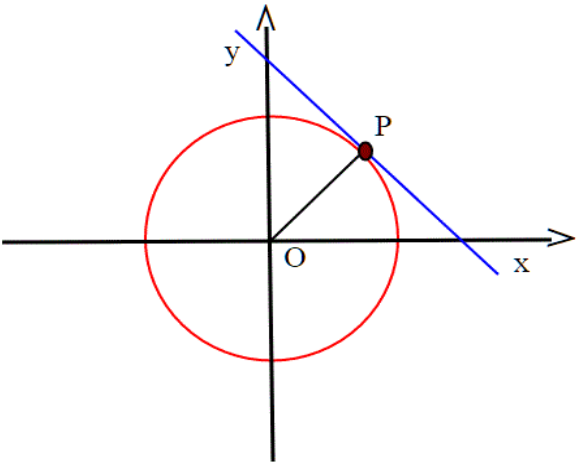


Possiamo, attorno al punto, possiamo rappresentare localmente le soluzioni tramite i punti del tipo $(x, \sqrt{1-x^2})$, quindi in questo caso f sarà proprio $f(x) = \sqrt{1-x^2}$.
Possiamo dire dunque che **F(x,y)** definisce in modo implicito una funzione **f(x)**.
Questo naturalmente accade sotto determinate condizioni; nel caso sopra sappiamo che nell'intervallo **(a,b) y** è sempre positiva, quindi per risolvere l'equazione $y^2 = 1 - x^2$ possiamo prendere solo la radice positiva, e ottenere proprio $y = f(x) = \sqrt{1-x^2}$.

Trovare la derivata di una funzione definita implicitamente

Supponiamo adesso di dover trovare la tangente alla circonferenza in un punto **P**; supponiamo :

$$P = (1/\sqrt{2}, 1/\sqrt{2}) x = y = 1/\sqrt{2}.$$



Ci sono più metodi per trovare il coefficiente angolare della retta tangente in quel punto, ma questo probabilmente non lo avete mai visto. Sappiamo che sulla circonferenza:

1. $y^2 = 1 - x^2$; quello che noi dobbiamo trovare è il rapporto $\frac{dy}{dx}$; deriviamo rispetto a x ambo i termini della 1.:

$2y \cdot \frac{dy}{dx} = -2x$; il termine di sinistra è la derivata della funzione composta y^2.

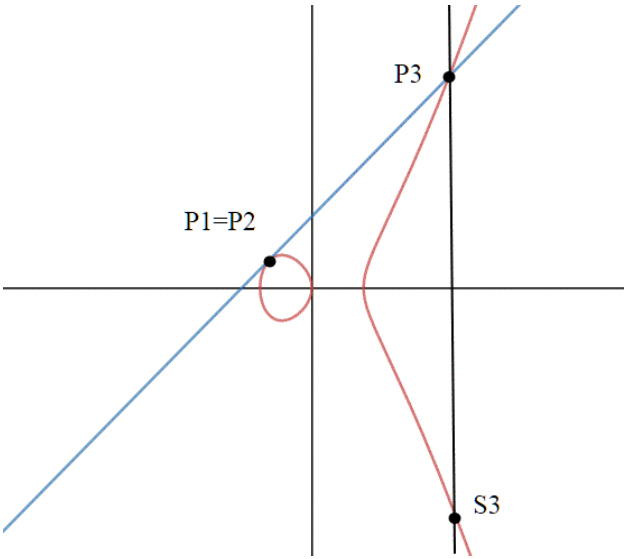
Ricordiamo che la derivata di una funzione composta è data da:
f(g(x))'=f'(g(x))* g'(x)

quindi $\frac{dy}{dx} = -\frac{2x}{2y}$; $\frac{dy}{dx} = -\frac{x}{y}$; quindi se $x = y = \sqrt{2}$ come nel nostro caso, tale derivata o coefficiente angolare vale -1.
Questo metodo è un po' brutale, ma evita di dovere parlare del Teorema del

Dini sulle funzioni implicite la cui dimostrazione è fuori portata.
E' da notare poi che questa espressione ($\frac{dy}{dx} = -\frac{x}{y}$) non ci dà una funzione esplicitata, ma solo un metodo di calcolo per trovare la derivata di una funzione definita implicitamente in un punto.

Calcolo della tangente ad una curva ellittica

Torniamo adesso alle nostre ellittiche; per la definizione di somma resta fuori il caso in cui **P1=P2**, ovvero la retta è tangente.
Escludiamo per adesso il caso in cui tale tangente sia parallela all'asse delle **y**, ovvero sia verticale.
Possiamo allora applicare lo stesso metodo che abbiamo applicato alla circonferenza.



Nel caso i due punti coincidano, la retta da cercare per prima è quella tangente alla curva in **P1=P2**.
Il passo successivo sarà quello di trovare **P3**, poi **S3**.

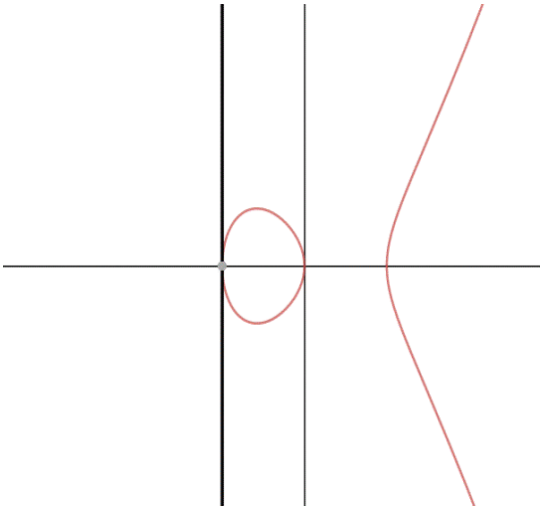
$y^2 = x^3 + ax + b$; derivando ambo i membri rispetto a **x**:

$2y\frac{dy}{dx} = 3x^2 + a$; supponiamo che **y<>0**; abbiamo allora.

$\frac{dy}{dx} = \frac{3x^2 + a}{2y}$: se vogliamo adesso il coefficiente angolare della retta in **P1**, basta che sostituiamo le sue coordinate:

$m = \frac{3x_1^2 + a}{2y_1}$. e abbiamo finito.

Se **y1=0**, la retta tangente è verticale; in tal caso si definisce in questo caso **P1+P1=⊖.**



Nel caso la retta sia verticale, come abbiamo visto nel'articolo sui punti impropri l'intersezione con la curva è all'infinito.

La tangente interseca infatti la curva in $\ominus$; se da lì tracciamo la retta per $\ominus$ e $\ominus$ otteniamo ancora $\ominus$.
Ci chiediamo ora una cosa; questa tangente esiste sempre? La sua espressione è(coefficiente angolare):
$\frac{dy}{dx} = \frac{3x^2 + a}{2y}$: se **y=0** abbiamo visto che la tangente è parallela all'asse delle **y.**
Ma allora in quale caso perde di significato? Bè, quando si annullano contemporaneamente numeratore e denominatore.
Quindi **y=0**, $3x^2 + a = 0$. ma se **y=0**, allora anche $y^2 = x^3 + ax + b = 0$

$$\begin{cases} x^3 + ax + b = 0 \\ 3x^2 + a = 0 \end{cases}$$

moltiplichiamo la prima equazione per **3** e la seconda per **x**:

$$\begin{cases} 3x^3 + 3ax + 3b = 0 \\ 3x^3 + ax = 0 \end{cases}$$

sottraendo membro a membro otteniamo:

$$2ax + 3b = 0; x = -\frac{3b}{2a}$$

sostituiamo adesso il valore di x nella $3x^2 + a = 0$ ottenendo:

$\frac{27b^2}{4a^2} + a = 0$; quindi

1) $27b^2 + 4a^3 = 0$

I punti in cui succede questo si dicono singolari e le curve per cui vale la 1) sono dette anch'esse singolari.

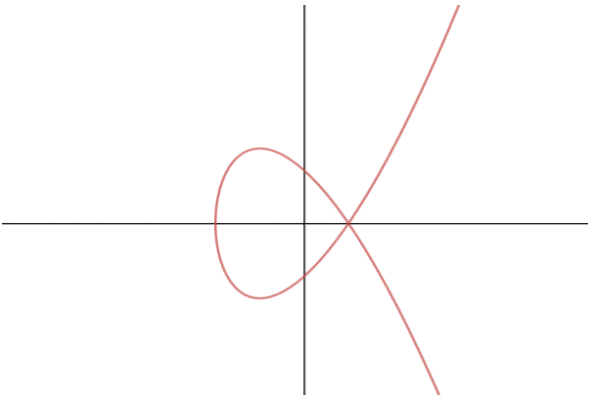
Questa espressione è anche detta discriminante della curva ellittica.

Esempi di curve singolari.

$y^2 = x^3 - 3x + 2 = (x-1)^2(x+2)$; nel punto 1 ha una radice doppia e la curva ha una singolarità;

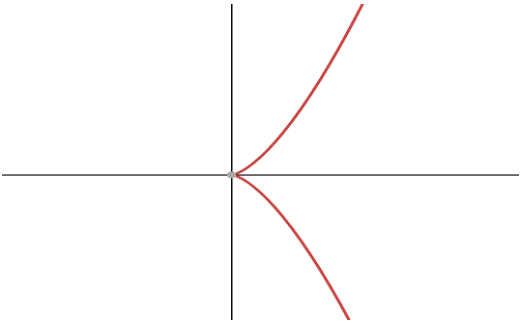
infatti:

$$\Delta = 27b^2 + 4a^3 = 27 \cdot 4 - 4 \cdot 3^3 = 0, x = \frac{-3b}{2a} = \frac{-6}{-6} = 1$$



Una curva di questo tipo è detta **nodo.**

$y^2 = x^3$; in questo caso la radice doppia è in zero, anzi è addirittura tripla.



Una curva di questo tipo si dice **cuspide.**

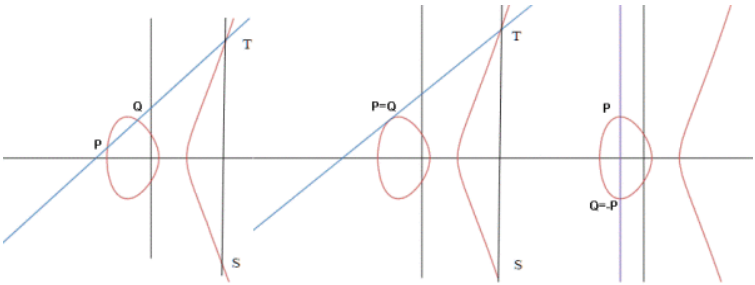
Per avere un gruppo, ovvero affinchè sia sempre possibile trovare **P+Q**, la curva deve quindi soddisfare la condizione:
$\Delta = 27b^2 + 4a^3 \neq 0.$

Nel prossimo articolo faremo un riassunto tutto quello che è stato fatto sulle curve ellittiche, e arriveremo a dimostrare che con l'operazione di somma descritta ogni curva forma un gruppo.

Il gruppo delle curve ellittiche, parte seconda

Riassumiamo in breve quello che abbiamo visto finora sulle curve ellittiche.

1. Sulle curve ellittiche definite da equazioni del tipo $y^2 = x^3 + ax + b$, è possibile definire una operazione di composizione interna.
   Se chiamiamo **E** l'insieme dei punti di una curva ellittica, tale operazione dunque è definita in: **E x E--->E**, e può essere interpretata in modo grafico in questo modo, pensando anche a tutti e tre i casi possibili.



Si considerano due punti **P, Q** sulla curva; si traccia la retta per i due punti, che nel caso i due punti siano coincidenti diventa la tangente; si trova la terza intersezione **T** e poi si traccia la verticale passante per **T** trovando così **S**; **P+Q=S**.
T esiste sempre come abbiamo visto nel quiz:

http://www.infinitoteatrodelcosmo.it/2017/03/21/soluzione-al-quiz-il-fantasma-di-galois/
Il caso limite, quando **P** e **Q** stanno su una retta verticale, lo abbiamo studiato in coordinate proiettive; in tal caso la retta per **P** e **Q** interseca la curva all'infinito, il punto improprio Θ.
Estendendo quindi **E** aggiungendo Θ si ottiene proprio un insieme con una legge di composizione interna.
Per dire che **E** è un gruppo dobbiamo provare che:
L'operazione è associativa, commutativa, esiste un elemento neutro e per ogni elemento abbiamo un opposto.
Che l'operazione sia commutativa discende dalla definizione; scambiando **P** con **Q** otteniamo come **P+Q** sempre **S** e nel caso verticale sempre Θ.
Per quanto riguarda l'associatività darò un accenno in appendice ad una sua giustificazione.
Chi sarà l'elemento neutro? Cerchiamo un elemento **N** tale che **P+N=P** qualsiasi sia **P** (basta questo, essendo commutativa, **P+N=N+P**).
Proviamo che N=Θ.
Se facciamo infatti **P+**Θ, dobbiamo considerare la retta passante per **P** e Θ, che interseca appunto la curva in Θ (all'infinito).
Quindi **P+**Θ**=P**.
Notiamo poi che se consideriamo i punti **P** e **Q** sulla verticale, ovvero con **Xp=Xq, P+Q=**Θ.
Infatti la verticale interseca la curva in Θ. Quindi **P+Q=**Θ; questo significa che **Q=-P**.
Quindi abbiamo trovato anche l'opposto di un punto **P**.
In definitiva, la curva con l'operazione così definita è proprio un gruppo.

Gli algoritmi di calcolo; punti distinti

Nel quiz http://www.infinitoteatrodelcosmo.it/2017/03/21/soluzione-al-quiz-il-fantasma-di-galois/
abbiamo calcolato anche il procedimento per il primo caso, quello di due punti distinti.
Indicando con **(x1,y1)** le coordinate di **P**, **(x2,y2)** le coordinate di **Q**, e con **(x3,y3)** le coordinate di **P+Q=S**,
in definitiva si aveva:

$$x_3 = m^2 - x_1 - x_2 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2$$

$$y_{S3} = -m(x_3 - x_1) + y_1 = -\frac{y_2 - y_1}{x_2 - x_1} \cdot (x_3 - x_1) + y_1$$

Punti coincidenti

Nell'ultimo articolo avevamo calcolato il coefficiente m nel caso di tangenza, ovvero di due punti coincidenti:

$$m = \frac{3x_1^2 + a}{2y_1}$$

Basta sostituire ad **m** il suo valore valore per ottenere **S** nel caso di tangenza, ovvero di **P=Q**:, e tener conto che **x1=x2,y1=y2**

$$x_3 = m^2 - x_1 - x_2 = m^2 - 2x_1$$

$$x_3 = m^2 - 2x_1 = (\frac{3x_1^2 + a}{2y_1})^2 - 2x_1$$

$$y_{S3} = -m(x_3 - x_1) + y_1$$

$$y_{S3} = -m(x_3 - x_1) + y_1 = -\frac{3x_1^2 + a}{2y_1} + y_1.$$

Notare che se sappiamo fare **P+P**, sappiamo fare anche **P+P+P**, **P+P+P+P**,...ecc.

In generale sappiamo quindi fare **nP=P+P+....P n** volte

Punti su retta verticale

Nel caso verticale, ovviamente **x1=x2**; ne segue che :

$$y_1^2 = x_1^3 + ax_1 + b$$

essendo **x1=x2**:

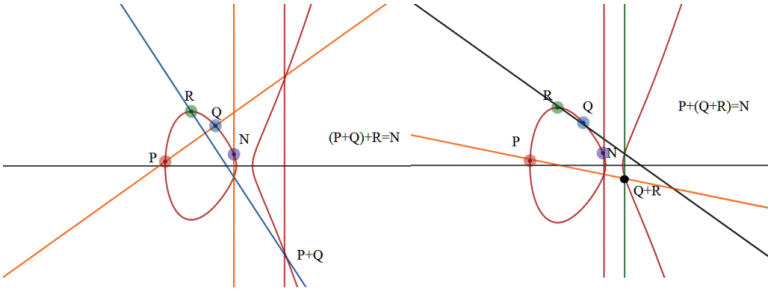
$$y_2^2 = x_1^3 + ax_1 + b$$

essendo **y1<>y2** ne segue **y1=-y2**, quindi l'opposto di **(x1,y1) è (x1,-y1)**.

Naturalmente questi algoritmi, che non implicano nessun ragionamento, possono essere eseguiti anche da un computer.
Abbiamo dunque concluso che l'insieme dei punti di una curva ellittica con il punto improprio come zero costituisce un gruppo vero e proprio.
Finora abbiamo considerato le curve con infiniti punti, definite cioè sui numeri reali.
La prossima volta vedremo come fare le stesse operazioni su un campo finito, tipo **Zp** (interi modulo p con p primo).
Sarà una cosa molto interessante e divertente, e ci porterà verso la crittografia moderna.

Appendice:

giustificazione intuitiva della proprietà associativa.
La dimostrazione formale della proprietà associativa, comporta delle tecniche riguardanti le soluzioni di equazioni polinomiali molto avanzate.
Tuttavia, volevo dare solo una giustificazione grafica di tale proprietà; si tratta di trovare graficamente **(P+Q)+R, P +(Q+R)**, e poi verificare che sono uguali ad un certo punto, chiamiamolo **N**.



clicca sull'immagine per ingrandirla.
Nello schema sono rappresentati i due modi diversi per calcolare la somma di tre punti;in entrambi i casi si vede che coincidono con il punto **N**.
Questa non è chiaramente non è una dimostrazione valida.
Chi vuole può provare a disegnarne altri casi, (io ho usato desmos).
Chi ancora non è soddisfatto può provare ad usare le due formule:

$$x_3 = m^2 - x_1 - x_2 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2$$

$$y_{S3} = -m(x_3 - x_1) + y_1 = -\frac{y_2 - y_1}{x_2 - x_1} \cdot (x_3 - x_1) + y_1$$

applicandole alle due somme fatte in ordine diverso, e vedere se coincidono.

Confesso che non ho provato, ma immagino che vengano fuori dei conti brutali.
Se qualcuno lo fa mi avvisi, così lo aggiungiamo all'articolo.

Ndr: ***Purtroppo Umberto non potrà più leggere i nostri commenti, ma spero che L'Universo trovi il modo di renderlo compartecipe alla scrittura dell'Evoluzione!***
Romeo