CAPITOLO II

STRUTTURE ALGEBRICHE ASTRATTE

1. PRELIMINARI E NOMENCLATURA

Dato un insieme $A \neq \emptyset$, si chiama operazione binaria interna su di esso e si indica col simbolo "$\circ$", una corrispondenza che ad ogni coppia ordinata (a,b) di elementi di A associa uno ed un solo elemento di A, esso viene indicato con

$$a \circ b.$$

Dunque una operazione binaria interna e' una applicazione dell'insieme A x A in A. Il termine interna sta ad indicare che il risultato dell'operazione e' ancora un elemento di A.

L'ente costituito da un insieme non vuoto A , da un insieme di operazioni $\mathcal{O} = \{ o_1, o_2, \ldots \}$ binarie interne o no definite in esso e da un insieme di proprieta' delle operazioni stesse prende il nome di <u>struttura algebrica</u> e si scrive $(A, \mathcal{O})$.

Piu' in generale una <u>operazione parziale n-aria</u> puo' essere pensata come una applicazione :

$$(op_n) : \mathbb{P} \subseteq \mathbb{A}_1 \times \mathbb{A}_2 \times \ldots \times \mathbb{A}_n \dashrightarrow \mathbb{A}$$

Se $\mathbb{P} = \mathbb{A}_1 \times \mathbb{A}_2 \times \ldots \mathbb{A}_n$ l'operazione si dice <u>totale</u>, mentre si dice <u>binaria</u> se n = 2, infine si dice <u>interna</u> se $\mathbb{A} = \mathbb{A}_1 = \mathbb{A}_2 = \ldots = \mathbb{A}_n$.

Una delle piu' semplici strutture algebriche e' quella di gruppoide. Un <u>gruppoide</u> e' una coppia $(A, \circ)$ dove A e' un insieme non vuoto e $(\circ)$ e' una operazione binaria interna su A. In un gruppoide possono esistere degli elementi e_s detti <u>elementi neutri a sinistra</u> con la proprieta' che:

$$\forall\, a \in A \;:\; e_s \circ a = a.$$

Analogamente possono esistere degli elementi e_d, detti <u>elementi neutri a destra</u>, tali che :

$$\forall\, a \in A \;:\; a \circ e_d = a.$$

Utilizzando tavole tipo "tavola pitagorica generalizzata" e' possibile dare i due seguenti esempi di gruppoidi:

(1)

∘	a	b	c
a	a	b	c
b	b	b	b
c	a	b	c

(2)

∘	a	b	c
a	c	a	a
b	c	b	b
c	c	c	c

Nella struttura (1) gli elementi a e b sono elementi neutri sinistri mentre nella (2) b e c sono elementi neutri destri. In altre parole possono esistere molti elementi neutri a sinistra e molti a destra .

Un elemento sia neutro destro che sinistro si chiama <u>elemento neutro</u> (bilatero). Proviamo che:

TEOREMA 1.- (Unicita' dell'elemento neutro) Sia $(A, \circ)$ un gruppoide. Se esistono un elemento neutro destro ed un elemento neutro sinistro allora essi coincidono in un elemento neutro (bilatero) che risulta essere unico.

DIMOSTRAZIONE. Esistono in A due elementi e_s ed e_d tali che:

$$\forall\, a \in A \;:\; e_s \circ a = a.$$

$$\forall\, b \in A \;:\; b \circ e_d = b.$$

Queste relazioni valgono, a maggior ragione, quando sia $a = e_d$ con $b = e_s$. Segue allora: $e_s \circ e_d = e_d$, $e_s \circ e_d = e_s$, e quindi l'asserto.

Dicesi <u>semigruppo</u> ogni gruppoide $(G, \circ)$ nel quale valga la proprieta' associativa, tale cioe' che:

$$(a \circ b) \circ c = a \circ (b \circ c), \quad \forall\, a,b,c \in A.$$

Un semigruppo $(G, \circ)$ che possegga un elemento neutro denotato con e , necessariamente unico per il teorema 1, si dira' un <u>semigruppo unitario</u> . Un elemento a di un semigruppo unitario $(G, \circ)$ si dice <u>invertibile</u> se esiste in G un elemento a' tale che :

$$a \circ a' = a' \circ a = e$$

TEOREMA 2 . In ogni semigruppo unitario $(G, \circ)$ l' inverso di un elemento, se esiste, e' unico.

DIMOSTRAZIONE. Se a' ed a'' sono elementi inversi di a$\in$ G, segue:

$$a \circ a' = a' \circ a = e \;,\; a \circ a'' = a'' \circ a = e.$$

Nell'uguaglianza $a \circ a' = e$ moltiplichiamo a sinistra per a'' e applichiamo la proprieta' associativa, segue:
$(a' \circ a) \circ a'' = a$, cioe' $e \circ a'' = a''$, cioe' $a'' = a$.

TEOREMA 3 . Sia $(G, \circ)$ un semigruppo unitario. Se esiste l'inverso a' di un elemento a di G, allora esiste anche l'inverso dell'inverso (a')' di a, e risulta :

$$(a')' = a$$

DIMOSTRAZIONE . Dalla relazione:

$$a \circ a' = a' \circ a = e \qquad (*)$$

risulta che l'elemento di G, che composto con a' fornisce l'elemento neutro e' esattamente lo stesso 'elemento a ; dunque l'inverso di a' e' a.

OSSERVAZIONE . Questo e' un caso, e il lettore se ne convinca, in cui l'ipotesi formata dalla frase (*) coincide con la tesi anche lei coincidente con la frase (*).

TEOREMA 4. In ogni semigruppo unitario $(G, \circ)$ l'inverso di un prodotto , se esiste, e' uguale al prodotto degli inversi in ordine inverso, cioe':

$$(a_1 \circ a_2 \circ \ldots \circ a_n)' = a'_n \circ a'_{n-1} \circ \ldots \circ a'_2 \circ a'_1 .$$

DIMOSTRAZIONE. Si tratta di provare che il prodotto sia a destra che a sinistra del secondo membro della precedente uguaglianza per l'elemento $a_1 \circ a_2 \circ \ldots \circ a_n$ e' l'elemento neutro e.

Proviamo il teorema per il prodotto a destra. Proviamo che :

$$(*)\ (a_1 \circ a_2 \circ \ldots \circ a_n) \circ (a'_n \circ a'_{n-1} \circ \ldots \circ a'_2 \circ a'_1) = e .$$

Procediamo per induzione. La (*) e'manifestamente vera per n=1.

Supposto dunque la (*) vera per n = k-1, proviamola di conseguenza per n = k. Si ha :

$(a_1 \circ a_2 \circ \ldots \circ a_k) \circ (a'_k \circ a'_{k-1} \circ \ldots \circ a'_1) =$

$= (a_1 \circ a_2 \circ \ldots \circ a_{k-1}) \circ (a_k \circ a'_k) \circ (a'_{k-1} \circ \ldots \circ a'_2 \circ a'_1) =$

$= (a_1 \circ a_2 \circ \ldots \circ a_{k-1}) \circ e \circ (a'_{k-1} \circ \ldots \circ a'_2 \circ a'_1) =$

$= (a_1 \circ a_2 \circ \ldots \circ a_{k-1}) \circ (a'_{k-1} \circ \ldots \circ a'_2 \circ a'_1) = e .$

L'ultima eguaglianza avendosi per l'ipotesi induttiva. La prova con l'elemento inverso a sinistra e' del tutto analoga.

Un semigruppo si dice <u>commutativo</u> o abeliano se l'operazione definita nel semigruppo gode della proprieta' commutativa, cioe':

$$a \circ b = b \circ a \qquad \forall\, a,b \in A$$

Consideriamo ora i seguenti esempi di semigruppi.

ESEMPIO 1.- L'insieme dei numeri naturali, dei numeri interi relativi, dei numeri razionali, dei numeri reali, dei numeri complessi con l'operazione di addizione oppure con l'operazione di moltiplicazione sono semigruppi unitari e commutativi. Infatti, sia l'addizione che la moltiplicazione, godono della proprieta' associativa, e la somma o il prodotto di due numeri non dipende dall'ordine degli addendi ovvero dei fattori.

ESEMPIO 2.- Nell'insieme delle parti di un insieme Ω le operazioni di unione e di intersezione sono associative e commutative. Si hanno dunque i semigruppi unitari e commutativi:

$$\left(P(A),\cup\right) \quad , \quad \left(P(A),\cap\right)$$

essendo rispettivamente $\varnothing$, Ω (parte vuota e parte piena) gli elementi neutri. Il lettore si convinca che in queste strutture soltanto gli elementi neutri sono invertibili. (Le equazioni $A \cup X = \varnothing$ oppure $A \cap X = \Omega$ hanno soluzione solo se $A = \varnothing$ ovvero Ω).

2. ELEMENTI DI TEORIA DEI GRUPPI

Una importante classe di strutture algebriche e' quella dei gruppi. Dicesi <u>gruppo</u> un semigruppo G per cui sono soddisfatte le seguenti proprieta' :

1) Esiste un elemento e di G, detto <u>elemento neutro</u>, tale che si abbia, quale che sia $a \in G$:
$a \circ e = e \circ a = a$.
2) Per ogni elemento a di G esiste un elemento a' di G, detto <u>simmetrico</u> di a, tale che:
$a \circ a' = a' \circ a = e$.

La nozione di gruppo puo' essere anche caratterizzata da

assiomatiche differenti, magari piu' deboli, come provano i due teoremi seguenti:

TEOREMA 5. Un semigruppo $(G, \circ)$ e' un gruppo se e soltanto se:

1') In G esiste un elemento e_s tale che $\forall\, a \in G$ si ha

$$e_s \circ a = a \text{ (neutro sinistro)}$$

2') Per ogni $a \in G$, $\exists$ in G un elemento a'_s, tale che

$$a'_s \circ a = e_s \text{ (inverso sinistro).}$$

DIMOSTRAZIONE. Un gruppo e' intanto un semigruppo che gode delle 1') e 2'). Proviamo il viceversa. Si tratta di mostrare che ammesse in un semigruppo $(G, \circ)$ le proprieta' 1') e 2'), da queste seguono :

(i) $\quad \forall\, a \in G, \Rightarrow a \circ e_s = a$

(ii) $\quad \forall\, a \in G, \Rightarrow a \circ a'_s = e_s$.

Posto $b = a'_s$ ed $u = e_s$ si ha :

$$(b \circ a) \circ b = u \circ b = b,$$

cioe' per l'associativa

$$b \circ (a \circ b) = b,$$

da qui, moltiplicando a sinistra ambo i membri per un simmetrico b'sinistro di b si ottiene sempre per la proprieta' associativa:

$$u \circ (a \circ b) = u$$

e quindi $\quad a \circ b = u$ cioe' la (i).

Dalla 2'), dalla associativa e dalla (ii) si ha:

$$a \circ u = a \circ (b \circ a) = (a \circ b) \circ a = u \circ a = a,$$

e quindi la (i). Si e' cosi' provato l'asserto.

Proviamo ora che:

TEOREMA 6. Un semigruppo $(G, \circ)$ e' un gruppo se e soltanto se le due equazioni $a \circ x = b$ ed $y \circ a = b$, $\forall\ a,b \in G$, ammettono ciascuna una ed una sola soluzione in G.

DIMOSTRAZIONE. Se $(G, \circ)$ e' un gruppo, $\forall\ a,b \in G$, l'equazione $a \circ x = b$ ammette l'evidente soluzione $x = a' \circ b$. Essa e' unica, poiche' da $a \circ x = b = a \circ x'$ si deduce , moltiplicando ambo i membri della relazione per a', l'eguaglianza $x = x'$. Prova analoga si ha per l'equazione $y \circ a = b$ che ha l'unica soluzione $x = b \circ a'$. Inversamente, si abbia un semigruppo $(G, \circ)$, per il quale le due suddette equazioni hanno una unica soluzione, proviamo che e' un gruppo.

PASSO 1. Proviamo che esiste un unico elemento neutro destro e . Notiamo intanto che $\forall\ a \in G$ esiste, per le ipotesi sulle equazioni, un unico elemento x di G, ed un unico y di G, tali che:

$$a \circ x = a\ ,\ b \circ y = b.$$

Esiste anche un elemento z tale che $z \circ b = a$, ed allora si ha :

$$z \circ (b \circ y) = z \circ b = a \quad \text{cioe'} \quad (z \circ b) \circ y = a \quad \text{cioe'} \quad a \circ y = a$$

e quindi

$$x = y := e_d.$$

PASSO 2 (osservazione). Esiste un unico neutro sinistro e_s. La Dal teorema dell'unicita dell'elemento neutro segue che l'elemento $e = x = y$ e' l'elemento neutro.

Analogamente hanno una unica soluzione, $\forall\ a \in G$, le due equazioni $a \circ u = e$, $v \circ a = e$. L'unico elemento di un

semigruppo, che soddisfa le due equazioni verifica le condizioni di essere l'inverso di a.

prova e' analoga a quella del PASSO 1..

PASSO 3 (osservazione). Esiste un unico elemento neutro $e:=e_s=e_d$, per il teorema di unicita'.

PASSO 4. Proviamo che ogni elemento di A e' invertibile. Per ogni $a \in G$ esistono $x,y \in G$ tali che $ax=e$, $ya=e$. Proviamo che $x=y$. Si ha infatti $y(ax)= ye = y$, cioe' $(ya)x = y$, cioe' $ex=y$, $x= y$.

In particolare un semigruppo abeliano per il quale valgano le proprieta' 1) e 2) si dice gruppo abeliano.
Un gruppo si dice finito o infinito, secondo che esso e' costituito da un numero finito o infinito di elementi.
Se il gruppo e' finito, si definisce ordine del gruppo il numero dei suoi elementi.
Trattiamo ora alcuni esempi di gruppi.
ESEMPIO 1 .- Il gruppo $(\mathbb{Z},+)$. L'insieme $\mathbb{Z}$ degli interi relativi con l'operazione di addizione e' un gruppo. Infatti la somma di due interi relativi qualsiasi e' un intero relativo, l'addizione e' associativa, l'elemento neutro e' lo zero, esiste l'elemento simmetrico che per un qualsiasi elemento a di $\mathbb{Z}$ e' l'opposto -a. Questo gruppo e' inoltre commutativo.

ESEMPIO 2.- L'insieme $\mathbb{Z}$ con l'operazione di moltiplicazione non e' un gruppo, infatti il simmetrico (inverso) di un

intero relativo non e' un elemento di $\mathbb{Z}$. Fissato, ad esempio, l'elemento 2 in $\mathbb{Z}$, non esiste in $\mathbb{Z}$ alcun elemento a' tale che 2 a' = 1.

ESEMPIO 3 .- $(\mathbb{Q}\setminus\{0\}, \times)$. L'insieme $\mathbb{Q}$, dei razionali non nulli e' un gruppo rispetto all'operazione di moltiplicazione. Notiamo che lo zero va escluso perche' e' privo di elemento inverso.

ESEMPIO 4.- $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{R}\setminus\{0\},\times)$, $(\mathbb{C}\setminus\{0\},\times)$.
Gli insiemi dei numeri razionali, reali ovvero complessi con l'operazione di addizione formano un gruppo commutativo.
L'insieme dei numeri reali o complessi non nulli con l'operazione di moltiplicazione formano un gruppo commutativo.

ESEMPIO 5.- Lo spazio dei vettori ordinari $(\mathbb{V},+)$.
L'insieme $\mathbb{V}$ dei vettori dello spazio con l'operazione di addizione di vettori e' un gruppo commutativo denotato con $(\mathbb{V},+)$.
Infatti l'addizione tra vettori e' associativa e commutativa, il vettore nullo O e' l'elemento neutro e per ogni vettore $\mathbf{v} \in V$ il vettore $-\mathbf{v}$ e' il simmetrico, (cfr. per dettagli il Cap III).

Rappresentazione a tabella di gruppi finiti. Un modo suggestivo per rappresentare la struttura di un gruppo finito e' il seguente. Si dispongono gli elementi del gruppo

in un certo ordine, partendo dall'unita', in uno schema quadrato avente tante righe (e colonne) quanto e' l'ordine del gruppo. All'incrocio della r-ma riga con la s-ma colonna, si scrive l'elemento che e' il risultato della operazione applicata agli elementi che contrassegnano rispettivamente l'r-ma riga e l's-ma colonna. Lo schema prende il nome di tabella operativa del gruppo. Si noti che, in questo contesto, un gruppo finito e' commutativo se e solo se la tabella risulta simmetrica rispetto alla diagonale principale.

ESEMPIO 6.- Il gruppo moltiplicativo dei segni. Il gruppo finito G = {1,-1} con l'operazione di moltiplicazione puo' rappresentare con la prima tabella in figura.

*	1	-1
1	1	-1
-1	-1	1

*	+	−
+	+	−
−	−	+

La seconda tabella, che e' una lettura in termini astratti della prima, costituisce la ben nota regola moltiplicativa dei segni.

ESEMPIO 7. Il gruppo delle unita' complesse. Diamo un esempio di gruppo finito commutativo contenente, diciamo come "sottoinsieme", il precedente. Consideriamo l'insieme G = {1,-1,i,-i}, essendo i l'unita' immaginaria; come operazione consideriamo l'ordinaria moltiplicazione di numeri complessi. Da notare che i quattro elementi di G

sono gli unici numeri complessi a coefficienti interi i cui inversi sono ancora numeri complessi a coefficienti interi. Infatti dato un numero complesso $a+ib$ con $a,b \in \mathbb{Z}$ perche' i coefficienti dell'inverso in $\mathbb{C}$, e cioe' i razionali $a/(a^2+b^2)$, $-b/(a^2+b^2)$, siano ancora interi, occorre e basta che sia $a^2+b^2 = 1$. Tale gruppodi ordine quattro si puo' rappresentare con la seguente tabella:

x	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

ESEMPIO 8. Le *n* radici *n-esime* complesse dell'unita' formano un gruppo moltiplicativo (finito e commutativo).

Infatti se $x_h = \exp [2\pi ih/n]$, $x_k = \exp [2\pi ik/n]$, $h,k<n$, sono due radici n-me risulta :

$$x_h\, x_k = \exp [2\pi ih/n] \exp [2\pi ik/n] = \exp [2\pi i(h+k)/n]$$

che e' ancora una radice n-ma dell'unita' sia se $h+k < n$ sia se $i+j = q\,n + r$ $(0 \leq r< n)$, per essere

$$\exp [2\pi ir] = \cos 2\pi r + i \operatorname{sen} 2\pi r = 1.$$

Per n=4 tale gruppo coincide con quello dell' ESEMPIO 7.

ESEMPIO 9.- Semigruppo delle applicazioni suriettive e

gruppo delle applicazioni biettive.

Sia A un'insieme. Sia F l'insieme delle applicazioni suriettive di A in se stesso. Se:

$$f : A \longrightarrow A , \qquad g : A \longrightarrow A$$

sono due applicazioni, si puo' definire la composizione $F = f \circ g$, come l'applicazione $F : A \longrightarrow A$, che $\forall\, x \in A$ e' definita da:

$$F(x) = f\,[g(x)] .$$

Si prova facilmente che quali che siano le tre applicazioni suriettive $f, g, h : A \longrightarrow A$ allora:

$$f \circ (g \circ h) = (f \circ g) \circ h.$$

Infatti $\forall\, x \in A$ si ha :

$$[f \circ (g \circ h)](x) = f \circ [(g \circ h)(x)] = f\Big[g[h(x)]\Big] =$$

$$= (f \circ g)[h(x)] = [(f \circ g) \circ h](x).$$

Segue allora che $(F, \circ)$ e' un semigruppo non commutativo con elemento neutro, tale essendo la funzione identica su A cioe' l'applicazione $I_A : A \longrightarrow A$ definita ponendo $I_A(x) = x$, $\forall\, x \in A$. Gli elementi invertibili del semigruppo sono ovviamente tutte e sole le applicazioni biettive di A. Poiche' la composizione di due biettive e' biettiva e I_A e' biettiva segue che le applicazioni biettive di A in A formano un gruppo G(A). Tale gruppo G(A) si chiama il gruppo totale delle trasformazioni di A. Se A e' finito, formato da n oggetti, allora esso e' il gruppo delle permutazioni su n elementi. Proviamo ora che

TEOREMA 7.- Il gruppo G(A) delle applicazioni di A in se risulta non commutativo se la cardinalita' di A e' almeno

3. Dimostrazione. Siano a, b, c tre elementi distinti di A. Siano

$$f, g : A \dashrightarrow A$$

due biezioni tali che :

1) $f(a) = b, \quad f(b) = a, \quad f(c) = c$,

2) $g(a) = c, \quad g(b) = a, \quad g(c) = b.$

e che lascino fissi gli elementi di A diversi da a_1, a_2, a_3. Risulta: $f \circ g\,(a) = f(c) = c$, mentre $g \circ f(a) = g(b) = a$.

Esempio 9(Permutazioni su 4 elementi)

Le permutazioni su 4 elementi, ad esempio, si possono vedere anche in altro modo. Supponiamo che una applicazione di un insieme di 4 elementi in se sia rappresentata, a meno dell'ordine delle colonne, col simbolo

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & d \end{pmatrix}$$

dove la quaterna ordinata a,b,c,d e' una permutazione di 1,2,3,4. Ogni colonna fornisce i corrispondenti degli elementi. Date due applicazioni biunivoche del tipo

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & d \end{pmatrix} \qquad y = \begin{pmatrix} a & b & c & d \\ \alpha_1 & \beta_1 & \gamma_1 & \delta_1 \end{pmatrix},$$

si definisce l'applicazione prodotto:

$$x \circ y = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \alpha_1 & \beta_1 & \gamma_1 & \delta_1 \end{pmatrix}$$

che nasce dalle successive applicazioni delle due funzioni: $1 \longrightarrow a \longrightarrow \alpha_1$ quindi $1 \longrightarrow \alpha_1$ etc.

Si ha, ad esempio

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ * & \$ & \# & \& \end{pmatrix} \circ \begin{pmatrix} \& & * & \$ & \# \\ 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} * & \$ & \# & \& \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

[infatti 1—>2—>1, 2 —>3 —>2, 3 —>4 —>3, 4 —>1 —>4];

Sia S_4 l'insieme delle sostituzioni su 4 elementi (sono esattamente 4!=24) e sia ($\circ$) la composizione definita sopra. Allora se consideriamo

$$I = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \qquad \text{e} \quad X^{-1} = \begin{pmatrix} a & b & c & d \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

e' semplice verificare che $(S_4, \circ)$ e' un gruppo non commutativo nel quale I e' l'elemento neutro e X^{-1} e' il simmetrico di una generica sostituzione X su 4 elementi. La proprieta' associativa discende dall'esempio 8 essendo una sostituzione una applicazione biettiva di M in se.

Se indichiamo con A l'insieme delle 4 permutazioni :

$$I = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad II = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad III = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad IV = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

la struttura $(A, \circ)$ si ottiene dalla seguente tabella operativa:

$\circ$	I	II	III	IV
I	I	II	III	IV
II	II	III	IV	I
III	III	IV	I	II
IV	IV	I	II	III

Il simmetrico di II e' IV, il simmetrico di III e' III stesso, il simmetrico di IV e' II e quello di I e' I stesso.

Esempio 10. (Permutazioni su n elementi)
Sia S_n l'insieme delle permutazioni (o sostituzioni) del tipo

$$\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

essendo $(a_1, a_2, \dots, a_n)$ una permutazione di $(1, 2, \dots, n)$.
Posto:

$$x \circ y := \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \dots & n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b'_1 & b'_2 & \dots & b'_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ b'_1 & b'_2 & \dots & b'_n \end{pmatrix}$$

Viene definita una struttura algebrica che verifica gli assiomi di definizione di gruppo: tale gruppo e' detto gruppo generale delle sostituzioni.

Proviamo che :

TEOREMA 8.- Il gruppo G_n delle permutazioni su n elementi ha cardinalita' n! .

DIMOSTRAZIONE: Sia $S = \{a_1, a_2, \ldots, a_n\}$. Al variare di tutte le possibili applicazioni biettive di S in su se stesso, l'elemento a_1 puo' avere come corrispondente uno qualsiasi degli n elementi di S, pertanto ad a_1 si possono associare n possibili applicazioni. Fissato ora il corrispondente di a_1, notiamo che per il corrispondente di a_2 vi sono invece n-1 possibilita', perche' a_2 ha come corrispondente uno qualsiasi degli elementi $a_1, \ldots, a_n$ purche' diverso (essendo le applicazioni biettive) dal corrispondente di a_1. Continuando in tal modo, si ha che il numero totale delle permutazioni e':

$$n(n-1)(n-2) \ldots 1 = n!$$

Esempio 11. Strutture di matrici.

Un altro esempio di gruppo e' dato dall'insieme delle matrici aventi un finito numero m di righe e n di colonne, ovvero di tipo $m \times n$, con l'operazione di addizione di matrice. Date due matrici quadrate di tipo $m \times n$:

$$A = \begin{pmatrix} a_{11} \ldots . a_{1n} \\ \ldots\ldots\ldots\ldots \\ a_{m1} \ldots . a_{mn} \end{pmatrix}, \qquad B = \begin{pmatrix} b_{11} \ldots . b_{1n} \\ \ldots\ldots\ldots\ldots \\ b_{m1} \ldots . b_{mn} \end{pmatrix}$$

si definisce loro somma e si denota col simbolo A + B, la matrice quadrata C di ugual tipo:

$$C = \begin{pmatrix} c_{11} \ldots . c_{1n} \\ \ldots\ldots\ldots\ldots \\ c_{m1} \ldots . c_{mn} \end{pmatrix}$$

dove $c_{ij} = a_{ij} + b_{ij}$. Tale operazione gode (come sara'

provato nel paragrafo delle matrici) delle proprieta' associativa e commutativa.

$$(A+B) + C = A + (B+C) \qquad \text{(associativa)}$$

$$A + B = B + A. \qquad \text{(commutativa)}$$

Esiste una matrice, detta matrice nulla, del tipo fissato, data dalla matrice avente gli elementi tutti uguali a zero, che funziona come elemento neutro rispetto alla addizione. Inoltre, data una matrice quadrata di tipo mxn, se si considera la matrice ottenuta da quella data cambiando di segno ciascuno dei suoi termini, questa, sommata(come matrice) a quella data, fornisca la matrice nulla; tale matrice ha quindi tutto il diritto di essere chiamata opposta (inversa addittiva) di quella data.
Dunque l'insieme delle matrici quadrate di fissato tipo con l' addizione di matrici risulta essere un gruppo abeliano.

Un altro esempio di gruppo e' dato dalle matrici quadrate di un ordine n fissato a determinante diverso da zero con l'operazione di moltiplicazione di matrici. Date due matrici siffatte

$$A = \begin{pmatrix} a_{11} & \dots a_{1n} \\ \dots\dots & \\ a_{n1} & \dots a_{nn} \end{pmatrix}, \qquad B = \begin{pmatrix} b_{11} & \dots b_{1n} \\ \dots\dots & \\ b_{n1} & \dots b_{nn} \end{pmatrix}$$

si definisce loro prodotto righe per colonne e si denota col simbolo A x B, la matrice quadrata C di ordine n:

$$C = A \times B = \begin{pmatrix} c_{11} & \dots c_{1n} \\ \dots\dots & \\ c_{n1} & \dots c_{nn} \end{pmatrix}$$

i cui elementi $c_{ij} = a_{i1}\, b_{1j} + a_{i2}\, b_{2j} + \dots + a_{in}\, b_{nj}$.
Si puo' facilmente dimostrare che tale operazione gode della

proprieta' associativa:

$$(A \times B) \times C = A \times (B \times C).$$

Chiamiamo matrice unitaria I_n la matrice di ordine n aventi gli elementi della diagonale principale tutti uguali ad 1 e gli altri elementi tutti ugualia zero. Tale matrice e' ovviamente l'elemento neutro rispetto alle moltiplicazioni tra matrici.

Data una qualsiasi matrice quadrata A di ordine n a determinante diverso da zero, esiste una matrice di ordine n, che si indica con A', che moltiplicata per A da' la matrice unitaria I_n .

Tale matrice prende il nome di matrice inversa di quella data.

La matrice A' inversa della matrice data A si costruisce col seguente procedimento:

1) Si costruisce la matrice i cui elementi sono ordinatamente i complementi algebrici degli elementi della matrice A. Tale matrice prende il nome di matrice aggiunta;

2) Si costruisce la matrice trasposta della matrice aggiunta. (Ricordiamo che la trasposta di una matrice e' la matrice che si ottiene scambiando ordinatamente le righe con le colonne);

3) Si divide ogni elemento della matrice ottenuta per il determinente di A. Dunque l'insieme delle matrici quadrate a determinante diverso da zero, con l'operazione di moltiplicazione (righe per colonne) di matrici e' un gruppo non commutativo.

Tratteremo ampiamente su queste operazioni per generalizzarle, nel paragrafo dedicato alle matrici

DEFINIZIONE.-Il gruppo GL(n,R) delle matrici quadrate non degeneri d'ordine n sui reali, detto anche il gruppo lineare d'ordine n sul campo R(o su un campo qualsiasi).

3. GRUPPI E SOTTOGRUPPI

Dato un gruppo G, si dice sottogruppo di G ogni sottoinsieme S di G i cui elementi formano gruppo rispetto alla operazione definita in G. Pertanto una condizione necessaria ma non sufficiente perche' S sia un sottogruppo del gruppo G e' che S contenga l'elemento neutro di G. Il lettore puo' riprendere i 12 esempi di gruppo illustrati sopra per cogliere esempi di sottogruppi. Ad esempio $(\mathbb{Z},+)$ e' sottogruppo di $(\mathbb{Q},+)$ il quale lo e' di $(\mathbb{R},+)$ etc.
L'insieme dei vettori 1-dimensionali oppure 2-dimensionali sono sottogruppi dell' insieme dei vettori 3-dimensionali. Il gruppo delle unita' intere e' sottogruppo di quello delle unita complesse. L'insieme delle sostituzioni e' sottogruppo di quello delle applicazioni biettive e cosi $(A,\circ)$ e' sottogruppo di $(M,\circ)$ (esempi 9 e 11).

Proviamo che:

TEOREMA 9.- Un sottoinsieme $S \neq \emptyset$ di un gruppo G e' un sottogruppo di G se e solo se:

(i) $\forall\, x,y, \in S \Rightarrow x \circ y \in S$.

(ii) $\forall\, x \in S \Rightarrow$ l'inverso $x' \in S$

DIMOSTRAZIONE. Se S e' un sottogruppo valendo le (i),... sono banalmente verificate.

Sia ora S un sottoinsieme di G verificante le due proprieta'. Proviamo che S l' elemento neutro e di G, ne seguira' che S e' un gruppo e quindi un sottogruppo di G. Sia $x \in S \neq \emptyset$, sia x' l'inverso di x. Per (ii) si ha $x' \in S$ e per (i) si ha $e = x \circ x' \in S$.

TEOREMA 10. Un sottoinsieme $S \neq \emptyset$ di G e' un sottogruppo di G se e solo se :

(i) $\forall\, x,y \in S \Rightarrow x \circ y' \in S$.

Dimostrazione Se S e' un sottogruppo di G, la verifica delle proprieta' e' banale. Supponiamo, viceversa, che S soddisfi alle due proprieta' enunciate. Sia $x \in S \neq \emptyset$, allora da (i) segue:

$x = y$ implica $e = y \circ y' \in S$

$x = e$ implica $y' = e \circ y' \in S$

cioe' l'asserto.

4. OMOMORFISMI TRA SEMIGRUPPI E GRUPPI

Nel capitolo dedicato alla teoria degli Insiemi abbiamo parlato di applicazioni tra insiemi. E' chiaro che se gli

insiemi tra i quali e' definita una applicazione sono "algebricamente strutturati" e si fanno interagire tra loro i due concetti nasce una problematica del tutto nuova. Lo studio di tali problematiche e' l'obiettivo di questo paragrafo.

Siano date due strutture algebriche (anche coincidenti) denotate con $(G, \circ)$ e $(G', *)$. Un omomorfismo di G in G' e' una applicazione $f : G \longrightarrow G'$ tale che

$$f(a \circ b) = f(a) * f(b) , \quad \forall\, a,b \in G.$$

In altre parole: "un omomorfismo *conserva* l'operazione". Se esiste un omomorfismo di G in G', si dice che G e' omomorfo a G'. Un omomorfismo di G in G', suriettivo come applicazione, si chiama epimorfismo; un omomorfismo, iniettivo come applicazione, si dice un monomorfismo. Dicesi, infine, isomorfismo , un omomorfismo biettivo come applicazione.

Se esiste un isomorfismo tra due strutture algebriche $(G, \circ)$ e $(G', *)$, si dice che G e' isomorfo a G' e si scrive

$$G \cong G'.$$

Dal punto di vista delle proprieta' strutturali, due strutture isomorfe sono riguardati come una stessa struttura. In particolare e come e' ovvio l'applicazione identica di una struttura algebrica in se e' un isomorfismo.

ESEMPIO Sia $\mathbb{R}$ il campo reale. Considero i due gruppi $(\mathbb{R}, +)$ ed $(\mathbb{R}^+, *)$ e l'applicazione biettiva $f : \mathbb{R} \longrightarrow \mathbb{R}^+$ definita ponendo

$$\forall\, x \in \mathbb{R} \qquad f(x) = a^x , \quad a \in \mathbb{R},\ a > 1.$$

Risulta come ben noto

$$f(x+y) = f(x) * f(y)$$

Dunque tale applicazione e' un isomorfismo, tra la struttura addittiva e quella moltiplicativa dei reali. L'isomorfismo inverso e' il logaritmo in base a. L'elemento neutro di $(\mathbb{R},+)$ ha come corrispondente l'elemento neutro di $(\mathbb{R}^+,*)$. Infatti

$$f(0) = a^0 = 1.$$

Il corrispondente dell'elemento $-x$ opposto di x in $(\mathbb{R},+)$ e'

$$a^{-x} = 1/a^x$$

inverso dell'elemento a^x in $(\mathbb{R}^+,*)$.

A volte un isomorfismo permette di fare delle identificazioni, nel senso che ora preciseremo . Si consideri, ad esempio, il semigruppo dei numeri naturalie quello degli interi positivi, entrambi con l'operazione di addizione e completati dallo zero. L'applicazione $f : N \cup \{0\} \longrightarrow \mathbb{Z}^+ \cup \{0\}$ definita, per ogni naturale n, ponendo $f(n) = +n$ e' un isomorfismo. E' usuale, come di fatto "si fa", scrivere n in luogo di $f(n) = + n$, cioe' "forzando l'eguaglianza-isomorfismo: $+n = n$ ", che si puo' chiamare una "identificazione per isomorfismo". Analogamente tra razionali apparenti e interi relativi, si ha una ulteriore identificazione per isomorfismo (di semigruppi).

ESEMPIO 2. Il lettore osservi le seguenti strutture algebriche ove la prima tabella e' la "regola dei segni" e nelle altre P significa "pari" e D "dispari".

*	+	−
+	+	−
−	−	+

+	P	D
P	P	D
D	D	P

*	P	D
P	P	P
D	P	D

La tabella "regola dei segni" , pensata quale struttura algebrica, forma gruppo. Per questo e' sufficiente prendere l'insieme dei due interi relativi -1 e +1 e notare che questo insieme con la ordinaria moltiplicazione e' chiuso, eredita le proprietaa' associativa, esistenza di elemento neutor +1, e commutativa. Inoltre ciascun elemento ha come inverso se stesso. Per confronto dei quadri allora, la regola dei segni e' un gruppo moltiplicativo isomorfo al gruppo additivo del pari e dispari. Cio' segue dal confronto delle tabelle. La terza tabella, del prodotto tra pari e dispari e' isomorfa alla tabella della ordinaria moltiplicazione sui numeri 0 ed 1.

Cominciamo ora a provare che

TEOREMA 11. Se f : G --> G' e' un isomorfismo tra le strutture algebriche $(G,\circ)$ e $(G',*)$ allora f^{-1}: G' --> G e' un isosmorfismo tra $(G',*)$ e $(G,\circ)$.

DIMOSTRAZIONE. Quali che siano $a',b' \in G'$ sappiamo che esistono un solo elemento a di G ed un solo elemento b di G, tali che :

$$a' = f(a), \quad b' = f(b), \qquad \text{da cui}$$
$$a = f^{-1}(a'), \quad b = f^{-1}(b').$$

Si ha allora:

$$f(a \circ b) = f\,[f^{-1}(a') \circ f^{-1}(b')] = a' * b' .$$

Applicando f^{-1} ad ogni membro della relazione, si ha:

$$f^{-1}(a' * b') = [f^{-1}(a') \circ f^{-1}(b')] = a \circ b.$$

Cioe' f^{-1} e' un isomorfismo di G' in G.

Si prova subito che:

TEOREMA 12. Il prodotto di due isomorfismi e' un isomorfismo.

DIMOSTRAZIONE. Se $(G, \circ)$, $(G', *)$, $(G'', \square)$ sono strutture algebri- che e $\varphi : G \longrightarrow G'$ e $\psi : G' \longrightarrow G''$ due isomorfismi, allora :

(1) $\forall\, a,b \in G : \quad \varphi\,(a \circ b) = \varphi(a) * \varphi(b)$

(2) $\forall\, a',b' \in G' : \quad \psi\,(a' * b') = \psi\,(a')\ \omega\ \psi\,(b')$.

Si ha allora, per la biezione $\psi \circ \varphi$, e $\forall\, a,b \in G$:

$$(\psi \circ \varphi)\,(a \circ b) = \psi\,[\varphi\,(a \circ b)] = \psi\,[\varphi\,(a) * \varphi\,(b)] =$$
$$= [(\psi \circ \varphi)\,(a)] \square [(\psi \circ \varphi)\,(b)]$$

onde $(\psi \circ \varphi)$ e' un isomorfismo; il teorema e' provato.

La relazione di isomorfismo nella classe delle strutture

algebriche $(G, \circ)$ e' manifestamente una relazione d'equivalenza. (Essa e' riflessiva: ogni struttura e' isomorfa a se stessa; simmetrica : l'inverso di un isomorfismo e' un isomorfismo; transitiva : per il Terorema 12 appena provato). Ogni classe di equivalenza di strutture in relazione si dira' struttura astratta.

Proviamo ancora che:

TEOREMA 13. Sia $(G, \circ)$ un gruppo e $(G', *)$ una struttura algebrica. Se esiste un isomorfismo $\varphi : G \dashrightarrow G'$ allora anche $(G', *)$ e' un gruppo. In esso l'elemento neutro e' l'elemento $\varphi(e)$, essendo e l'elemento neutro di $(G. \circ)$. Inoltre $\forall\ a \in G$, l'elemento $\varphi(a) \in G'$ ha come simmetrico l'elemento $\varphi(a')$ essendo a' il simmetrico di a in $(G, \circ)$.

DIMOSTRAZIONE. Proviamo che in $(G', *)$ vale la proprieta' associativa. Siano a', b', c' tre qualsiasi elementi di G'. Esistono allora tre elementi di G, diciamo a, b, c tali che:

$$a' = \varphi(a),\ b' = \varphi(b), c' = \varphi(c).$$

In $(G, \circ)$ si ha:

$$(a \circ b) \circ c = a \circ (b \circ c) .$$

Calcoliamo φ in ambo i membri, si ha:

$$\varphi[(a \circ b) \circ c] = [\varphi(a \circ b)] * \varphi(c) = [\varphi(a) * \varphi(b)] * \varphi(c)$$

$$\varphi[a \circ (b \circ c)] = \varphi(a) * [\varphi(b \circ c) = \varphi(a) * [\varphi(b) * \varphi(c)]$$

l'eguaglianza dei primi membri implicando quella degli ultimi.

Per $\varphi(e)$ e $\varphi(a')$ sono sufficienti banali verifiche.

5. LA STRUTTURA DI ANELLO, CORPI E CAMPI

Accanto alla struttura di gruppo, in cui e' definita una sola operazione binaria interna, esistono altre strutture nelle quali sono definite due operazioni interne. La piu' importante tra tali strutture, anche per i legami con questioni di carattere applicativo, e' quella di anello.

E' convenzione universale indicare le due operazioni dell'anello con i simboli + , - ; ma ovviamente si tratta di operazioni astratte, che nulla hanno in comune con l'addizione e la moltiplicazione ordinarie.

DEFINIZIONE. Dicesi anello, una struttura algebrica $(A, +, -)$ che verifichi le seguenti proprieta':

1) La struttura $(A, +)$ e' un gruppo abeliano; il suo elemento neutro e' denotato con "0" (zero), l'opposto di $a \in A$ con $-a$

2) La struttura $(A, -)$ e' un semigruppo; l'elemento $a - b$ verra' denotato anche con ab.

3) Valgono le due seguenti proprieta' distributive. (Si noti che esse costituiscono un legame tra le due operazioni):

$$a(b + c) = ab + ac \tag{5.1}$$

$$(b + c)a = ba + ca \tag{5.2}$$

quali che siano $a, b, c \in A$.
Naturalmente se la moltiplicazione e' commutativa, cosa che in generale non accade, le due proprieta' (3.1) e (3.2), coincidono.

OSSERVAZIONE. In genere si suppone che un anello sia costituito almeno da due elementi distinti; tuttavia possiamo considerare un anello speciale fatto da un solo elemento (che identifichiamo con lo zero, che certamente ci deve essere). Indicheremo allora l'insieme con $A = \{0\}$ e definiamo le operazioni con le posizioni:

$$0 + 0 := 0 \cdot 0 := 0 .$$

E' immediato verificare che tutte le proprieta' di anello sono verificate. E' facile anche verificare che anche la parte moltiplicativa e' un gruppo e che 0 e' anche l'elemento neutro moltiplicativo e che quindi ha come inverso se stesso. Questo anello si chiama anello nullo.

Elenchiamo ora alcune proprieta' che danno luogo ad importanti classi di anelli.

a) Se $(A, \cdot)$ e' un semigruppo commutativo, l'anello si dice commutativo.

b) Se esiste un elemento e, detto elemento unitario, per il quale:

$$a \cdot e = e \cdot a = a \qquad \forall \ a \in A.$$

l'anello si dice unitario.

c) Se un anello e' unitario e vale la legge di annullamento del prodotto , cioe' se risulta che:

$a \cdot b = 0 \quad \Longrightarrow \quad a = 0$ oppure $b = 0$ oppure $a = b = 0$

allora l'anello si dice un anello di integrita'.

OSSERVAZIONE. In ogni gruppo e quindi anche in $(A,+)$, le equazioni di primo grado ($a+x = b$) hanno una unica soluzione. Cio' implica:

TEOREMA 15. Il prodotto di due elementi di un anello e' sempre nullo se uno dei due fattori e' nullo; cioe' per ogni elemento di A sussiste l'uguaglianza:

$$a \cdot 0 = 0 \cdot a = 0.$$

DIMOSTRAZIONE. Osservato che l'equazione $c + x = c$ ha $x = 0$ come unica soluzione e che quindi sussiste l'eguaglianza $b = b + 0$, si ha dalle proprieta' associative:

$$a \cdot b = a \cdot (b + 0) = a \cdot b + a \circ 0$$

Tale eguaglianza implica che $a \cdot 0$ e' l'unica soluzione della equazione $a \circ b = a \circ b + a \circ 0$ e quindi $a \circ 0 = 0$.
Analogamente si ha $0 \cdot a = 0$. Il teorema e' cosi' provato.

OSSERVAZIONE. Il teorema non e' invertibile. Infatti puo' accadere che il prodotto di due elementi di un anello sia nullo, essendo i due elementi diversi da zero. In tale caso, se risulta:

$$a \cdot b = 0 \quad \text{con} \quad a \neq 0 \,, \; b \neq 0$$

gli elementi a e b prendono il nome di divisori dello zero.

ESEMPIO 1. Tra gli insiemi numerici considerati in precedenza, sono strutturabili come anelli commutativi

unitari ed integri, l'anello degli interi relativi $(\mathbb{Z},+,x)$; dei numeri razionali $(\mathbb{Q},+,x)$; dei numeri reali $(\mathbb{R},+,x)$ e dei numeri complessi $(\mathbb{C},+,x)$.

ESEMPIO 2. L'insieme (n), o anche n $\mathbb{Z}$, degli interi relativi multipli di un fissato intero $n \geq 2$, con le operazioni di addizione e moltiplicazione ordinarie, costituisce un anello commutativo, non unitario. (Infatti il numero 1 non e' ottenibile come multiplo di n, e quindi non e' nell'insieme (n) = n $\mathbb{Z}$).

ESEMPIO 3. L'insieme dei polinomi a coefficienti interi in una indeterminata con le operazioni di addizione e moltiplicazione tra polinomi e strutturabile come un anello.

DEFINIZIONE. Un elemento di un anello unitario A si dice <u>invertibile</u>, o <u>regolare</u>, o che e' <u>una unita'</u> di A, se esso ammette un simmetrico (nel senso dei semigruppi) cioe', se esiste un $a' \in A$ (che sappiamo essere necessariamente unico) tale che :

$$aa' = a'a = e.$$

OSSERVAZIONE. In un anello A, unitario e non nullo, esiste almeno un elemento non invertibile : lo zero. Infatti non esiste x con $0x=x0=1$ a meno che non sia $0=1$!

Sussiste il seguente:

TEOREMA 15. L'insieme degli elementi invertibili di un anello unitario non nullo e', rispetto alla moltiplicazione dell'anello, un gruppo contenuto nel semigruppo moltiplicativo (senza lo zero).

Dimostrazione. Sia U l'insieme degli elementi invertibili di A. Intanto U non e' vuoto contenendo almeno l'elemento neutro e. Proviamo che il prodotto di due elementi di U e' in U, cioe' che se $a,b \in U$ allora ab e' invertibile. Infatti si ha:

$$(ab)^{-1} = b^{-1}a^{-1} .$$

Banalmente in $(U, \circ)$ si eredita la proprieta' associativa ed ogni elementodi di U e' invertibile con inverso ancora in U. Infatti, come provato per i semigruppi, l'inverso di un elemento invertibile e' invertibile essendo l'elemento di partenza.

ESEMPI. Nell'anello $\mathbb{Z}$ il gruppo delle unita' e' costituito da $\{-1, +1\}$ strutturato con la moltiplicazione. L'anello degli interi complessi $a + i\,b$, con $a,b \in \mathbb{Z}$, chiamato anche anello di Gauss, ha come gruppo delle unita' l'insieme $\{-1,-i,+1,+i\}$ strutturato con la moltiplicazione.. Ancora l'anello dei polinomi a coefficienti reali in una indeterminata ha come gruppo delle unita' l'insieme delle costanti, con la moltiplicazione.

DEFINIZIONE (di ideale). Un insieme I, non vuoto, di elementi di un anello A, si dice un ideale di A se:

1) Quali che siano $a,b \in I$ si ha: $a-b = a+(-b) \in I$.
2) Per ogni $a \in I$ e per ogni $b \in A$ si ha sia $ab \in I$ che $ba \in I$.

Si chiama corpo un anello A nel quale la struttura $(A\setminus(0),\circ)$ e' un gruppo. Proviamo che:

TEOREMA 16. In un corpo non ci sono divisori dello zero.

DIMOSTRAZIONE . Supponiamo, per assurdo, di prendere due elementi $a\neq0$ e $b\neq0$ tali che sia $a\cdot b=0$. Siccome siamo in un corpo, ogni elemento $a\neq0$ possiede inverso; sia a' l'inverso di a. Segue $a'(ab)=a'\cdot0=0$, poiche' la moltiplicazione e' associativa si ha, contro l'ipotesi $b\neq0$:

$$0 = a'(ab) = (a'a)b = eb = b .$$

Si chiama campo un corpo commutativo. Dunque un campo e' un anello A unitario tale che $(A-\{0\},\circ)$ e' un gruppo abeliano.

Si noti bene che mentre in un anello unitario "proprio" (per i non unitari il problema non si pone) vi sono elementi che hanno inverso ed elementi che non hanno inverso, in un corpo e quindi in un campo sono invertibili tutti gli elementi non nulli.

6. L'ANELLO DELLE CLASSI RESTO

Nell'anello degli interi relativi $\mathbb{Z}$ fissiamo un numero intero positivo $m > 2$ e introduciamo la seguente relazione:
Se a,b sono interi relativi, si dice che "a e' congruo b modulo m " ed in simboli si scrive:

$$a \equiv b \bmod m \quad \text{oppure} \quad a \equiv b \ (m)$$

se e solo se la differenza a-b e' divisibile per m.
La relazione di congruenza e' una relazione di equivalenza; infatti e' facilmente verificabile che gode delle proprieta' riflessiva, simmetrica e transitiva.
Le classi di equivalenza nelle quali gli interi relativi vengono suddivise dalla relazione di equivalenza considerata prendono il nome di classi resto modulo m e si indicano col simbolo $[a]_m$ o solo con [a] se la scrittura non da' luogo ad equivoci.
Il nome di classe resto viene dal fatto che due elementi a e b appartengono ad una medesima classe di equivalenza modulo m se e solo se divisi per m danno lo stesso resto.
Poiche' i resti distinti possibili sono dati da tutti gli interi minori di m, si hanno m classi:

$$[0], [1], [2], \ldots, [m-1].$$

Indichiamo con $\mathbb{Z}_{(m)}$ l'insieme di queste classi.
Cosi' ad esempio, se costruiamo le classi resto mod 2, otteniamo le due classi [0], [1] e ogni relativo appartiene alla classe [0] oppure alla classe [1] a seconda che sia rispettivamente pari o dispari.
In generale nel caso m, le classi possono pensarsi costruite

con le colonne della seguente tabella:

-m	-m+1	-m+2	...	-1
0	1	2	...	m-1
m	m+1	m+2	...	2m-1
hm	hm+1	hm+2	...	(h+1)m-1

Gli elementi della stessa colonna sono congrui modulo m, due elementi posti in colonne diverse non sono congrui e ogni colonna costituisce appunto una classe di equivalenza. La classe $[0]_m$ e' costituita da tutti i numeri interi che divisi per m danno come resto il numero zero. La classe $[1]_m$ e' costituita da tutti gli interi che divisi per m danno resto 1. Cosi' si ha, ad esempio:

$\mathbb{Z}_2$

-4	-3
-2	-1
0	1
2	3
4	5
....	.....
2h	2h+1
....	.....
[0]	[1]

$\mathbb{Z}_3$

-6	-5	-4
-3	-2	-1
0	1	2
3	4	5
6	7	8
....	.....	.....
3h	3h+1	3h+2
....	.....	.....
[0]	[1]	[2]

Definiamo in $\mathbb{Z}_m$ due operazioni (+) e (x). Quali che siano le classi [a], [b] di $\mathbb{Z}_m$, porremo:

$$[a] + [b] = [a + b]$$

in $\mathbb{Z}_m$

$$[a] \times [b] = [a \times b]$$

OSSERVAZIONE. Occorre ora provare che se:

$a' \in [a]$, $b' \in [b] \Rightarrow a'+b' \in [a+b]$, $a'b' \in [ab]$.

Si esprime questa circostanza dicendo che le "definizioni sono ben poste". La prova e' facile. Notiamo per questo che le ipotesi $a' \in [a]$ e $b' \in [b]$ si traducono in:

$$a' = a + km \,, \qquad b' = b + hm$$

e quindi

$$a' + b' = a + b + (h + k)m$$

$$a' \times b' = ab + (ah + bh + hkm)m$$

da cui l'asserto.

La struttura algebrica $(\mathbb{Z}_m, +, \times)$ e', come facilmente si verifica, un anello commutativo unitario avente (indipendentemente da $m>2$) come elemento neutro moltiplicativo la classe [1], come zero di $(\mathbb{Z}_m, +)$ la classe [0] e come elemento opposto della classe [a], la classe [m-a]. La validita' delle proprieta' associativa e commutativa e' banale. Costruiamo, come esempio delle operazioni su definite, le tabelle operative delle classi resto modulo 3 e modulo 4. Per m=3, si ha:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Per m = 4 , si ha:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Dal punto di vista dei divisori dello zero e degli elementi invertibili, si presenta una notevole differenza a seconda che m sia un numero composto o primo. Sussistono le seguenti due notevoli proposizioni:

PROPOSIZIONE I. Se m e' un numero composto allora $\mathbb{Z}m$ e' un anello non integro. Infatti le classi individuate dai divisori di m diversi da 1 e da m sono divisori dello zero mentre le classi individuate da numeri primi con m sono elementi invertibili.

PROPOSIZIONE II L'anello $\mathbb{Z}m$ e' un campo se e solo se m e' un primo p.

Per provare quanto asserito occorre qualche complemento e

sviluppo di Teoria dei Numeri. Iniziamo con il definire per ogni numero naturale n (≥ 1) il numero $\phi(n)$ detto indicatore (o totalizzatore) di Eulero. Il numero $\phi(n)$ e', per definizione, il numero dei numeri interi $m \geq 1$, non superiori ad n e primi con n, cioe':

$$\phi(n) = \left|\left\{x : x \in \mathbb{N},\ 1 \leq x \leq n, (x;n)=1\right\}\right|.$$

Si vede subito che:
$\phi(1)=\phi(2) = 1$, $\phi(p) = p-1$, $\phi(4) = 2$, $\phi(6) = 2$, $\phi(8) = 4$ etc.
Per ogni numero primo $p > 1$ sara' $\phi(p)=p-1$, giacche' i numeri naturali primi con p e minori di p saranno tutti i primi p-1 numeri naturali. Piu' generalmente si ha che:

I. Qualunque siano i numeri naturali p e n, se p e' primo e >1, risultera' $\phi(p^n) = p^{n-1}(p-1)$.

Infatti, i numeri naturali primi con p^n e minori di p^n si otterranno, se e' $p > 1$, scartando dal sistema di tutti i p^n numeri naturali $1, 2, \ldots, p^n$ quelli che risultano multipli di p (i quali soltanto non saranno primi con p^n, avendo in comune con p^n il divisore $p > 1$), e cioe' i p^{n-1} numeri $p, 2p, \ldots, p^n$, che si ottengono, moltiplicando i p numeri naturali $1, 2, \ldots, p^{n-1}$ per p.

II. Qualunque siano i numeri naturali a, b primi fra loro, si ha $\phi(ab)=\phi(a)\cdot\phi(b)$ (proprieta' moltiplicativa).

Infatti, escluso il caso banale a=1, o b=1, posto, per

brevita' di scrittura $\phi(a)=s$, $\phi(b)=t$, indichiamo con $\alpha_1, \alpha_2, \ldots, \alpha_s$ i numeri naturali primi con a e minori di a e con $\beta_1, \beta_2, \ldots, \beta_t$ i numeri naturali primi con b e minori di b, e consideriamo, per ogni coppia di numeri naturali h,k non superiori rispettivamente a s e a t, il numero $a\beta_k+b\alpha_h$, il quale sara' primo con ab, perche', se p e' un numero primo divisore comune di ab ed $a\beta_k+b\alpha_h$, se cioe' riesce:

$$ab \equiv 0 , \qquad a\beta_k+b\alpha_h \equiv 0, (\mathrm{mod.}\, p)$$

allora, per la prima di queste, o sara' $a \equiv 0$ (mod.p), onde, per la seconda, $a\beta_k \equiv 0$, $b\alpha_h \equiv 0$ (mod.p), onde analogamente $b\alpha_h \equiv 0$, $a\beta_k \equiv 0$ (mod.p), e quindi varra' l'una o l'altra delle $a \equiv 0$, $\beta_k \equiv 0$ (mod.p), e pertanto in ogni caso p riuscira' un divisore comune di a e b , cioe' necessariamente uguale ad uno, dato che a e b si sono supposti primi fra loro. D'altra parte, per ogni altra coppia di numeri naturali i, j non superiori rispettivamente ad s e a t, si avra' certamente $a\beta_j+b\alpha_i \not\equiv a\beta_k+b\alpha_h$ (mod.ab), perche' in caso contrario risulterebbe $a(\beta_j-\beta_k) \equiv b(\alpha_k+\alpha_i)$ (mod.ab), onde si trae $b(\alpha_h-\alpha_i) \equiv 0$ (mod.a) , $a(\beta_j-\beta_k) \equiv 0$ (mod.b) , il che implica $\alpha_h-\alpha_i \equiv 0$ (mod.a), $\beta_j-\beta_k \equiv 0$ (mod.b) (che' a e b sono stati supposti primi fra loro), cioe' $\alpha_h=\alpha_i$, $\beta_j=\beta_k$ (che' α_k, α_i sono non negativi e minori di a e β_j, β_k sono non negativi e minori di b).

Da queste considerazioni appare come i resti rispetto al modulo ab degli st numeri rappresentati da $a\beta_k + b\alpha_h$, per h = 1,2, ...,s e k=1,2, ...,t, riescano tutti primi con

ab e diversi uno dall'altro. Inversamente, mostriamo che ogni numero naturale γ primo con ab e minore di ab sara' necessariamente uno degli st resti ora detti. Infatti gli ab numeri rappresentati da $a\beta+b\alpha$, per $\alpha=0,1,2,\ldots,a-1$ e $\beta=0,1,2,\ldots,b-1$ riescono due a due incongrui fra loro rispetto al modulo ab (come si vede, applicando il ragionamento di poco fa, nel caso che α_h, α_i siano due qualsivoglia numeri interi non negativi e minori di b), sicche' i loro resti rispetto al modulo ab sono necessariamente tutti gli ab numeri $0,1,2,\ldots,ab-1$; ma γ e' uno di questi, onde vi saranno due ben determinati interi non negativi α, β, il primo minore di a e il secondo minore di b, per cui risultera' $\gamma=a\beta+b\alpha$ (mod.ab), e dovranno essere α primo con a (cioe' uno degli $\alpha_1,\alpha_2,\ldots,\alpha_s$) e β primo con b (cioe' uno dei $\beta_1,\beta_2,\ldots,\beta_t$), perche' altrimenti γ o non sarebbe primo con a, o non sarebbe primo con b, contro l'ipotesi che esso sia primo con ab.

III. (Teorema di Eulero sulle congruenze.)
Siano $a,m \in \mathbb{N}$ tali che $(a;m)=1$, allora

$$a^{\phi(m)} \equiv 1 \bmod m$$

DIMOSTRAZIONE. I numeri r_i sono ciascuno tra 1 ed m e sono tutti distinti, segue :

$$a_1 \ldots a_\phi = r_1 \ldots r_\phi .$$

Proviamo cio'. Sia $i \neq j$. Risulta:

$$a(a_i - a_j) = r_i - r_j + (\rho_i - \rho_j)m.$$

Se per assurdo fosse $r_i = r_j$ avremo che m primo con a, deve necessariamente dividere l'altro fattore (come afferma il

primo teorema di Euclide). Questo e' assurdo perche' m e' piu' piccolo di $a_i - a_j$. Segue allora:

$$(aa_1) \ldots (aa_\phi) = r_1 r_2 \ldots r_\phi + tm$$

che prova l'asserto. □

DIMOSTRAZIONI delle Proposizioni I e II. Iniziamo con il provare che se m e' composto allora $\mathbb{Z}_m$ non e' un campo. Se m e' composto sia d un divisore proprio di m; dunque esiste d_1 tale che $dd_1=m$. Allora esistono due classi individuate da d e d_1 tali che:

$$[d][d_1] = [dd_1] = [m] = [0]$$

con $[d] \neq [0]$ e $[d_1] \neq [0]$. Dunque se m e' composto $\mathbb{Z}_m$ ha divisori dello zero e non puo' essere un campo.

Proviamo ora che se m=p e' un primo allora ogni elemento non nullo di $\mathbb{Z}_p$ e' invertibile.

Per provare questo proviamo piu' in generale che ogni classe [a] con $[a] \neq [0]$ e a primo con m (primo o no) e' invertibile. Dal teorema di Eulero segue che se (a;m)=1 allora

$$a^{\phi(m)} \equiv 1 \text{ (modulo m)}$$

dunque

$$[a][a^{\phi(m)-1}] = [1].$$

□

A completamento di quanto visto sopra proviamo in particolare che:

TEOREMA. Siano a ed m due interi con $m \geq 2$. Sia $1 < a < m$ e sia $(a;m) > 1$. Allora in $\mathbb{Z}_m$ la classe [a] e' un divisore dello zero.

DIMOSTRAZIONE. Sia $(a;m) = d > 1$. Allora il massimo comun divisore d e', in particolare, un comune divisore e quindi risulta:

$$a = hd, \quad m = kd \qquad \text{con} \qquad 1 < h,k < m.$$

Come ovvio, da cio' risulta :

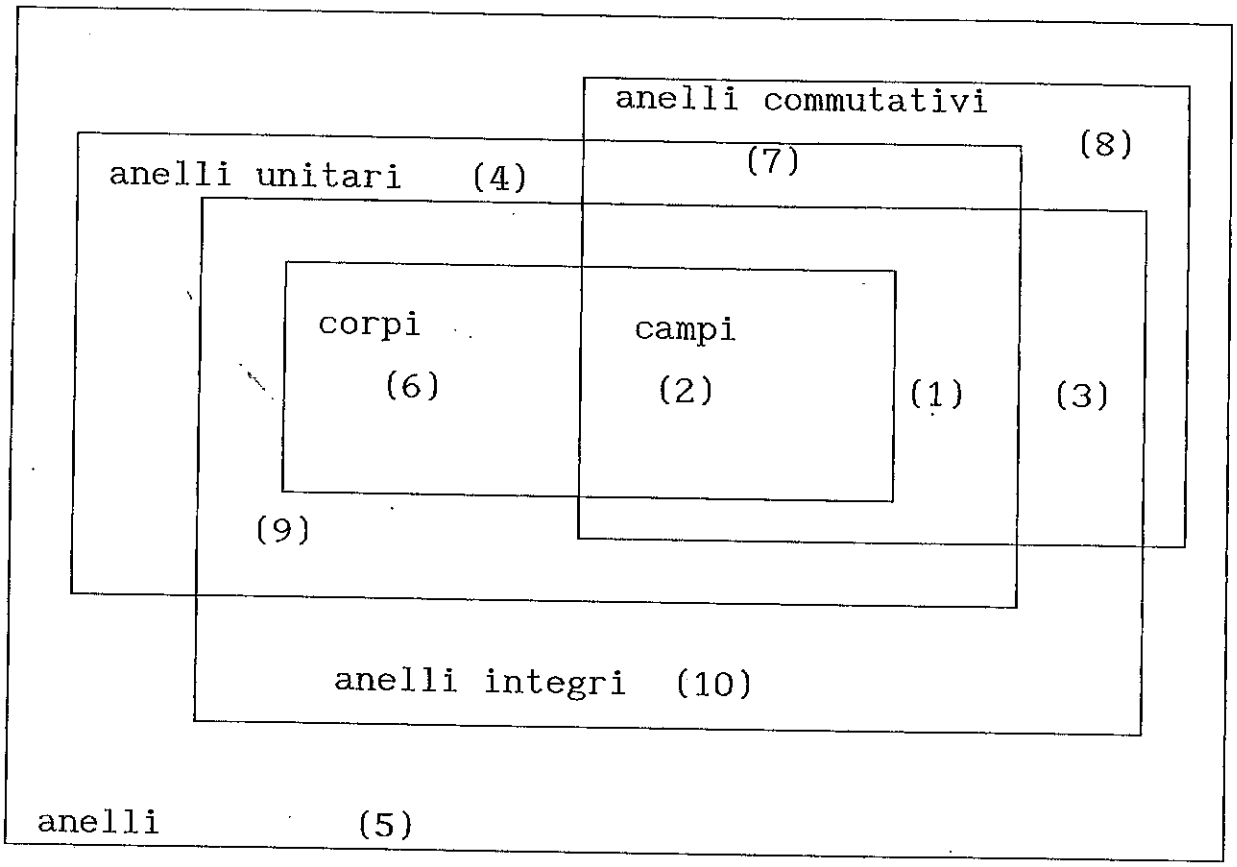
$$[a][k] = [ak] = [hdk] = [hm] = [0].$$

essendo sia [a] che [k] classi non nulle, per essere $a,k < m$.

7. CONSIDERAZIONI RIASSUNTIVE E FINALI

Concludiamo il capitolo con alcune osservazioni:

La figura seguente esprime in termini di diagrammi di Eulero-Venn le mutue intersezioni e contenenze tra le varie classi di anelli introdotte sopra. Ciascun punto del rettangolo rappresenta un anello. Il nostro problema e' quello di costruire un esempio per ciascuna delle zone possibili.



Caso generale

(1) $(\mathbb{Z},+,x)$ e' un anello commutativo, unitario, integro che non e' un campo (vale la legge di annullamento, ma non e' un campo perche' non e' vero che ogni elemento non nullo e' invertibile).

(2) Gli anelli $(\mathbb{Q},+,x)$, $(\mathbb{R},+,x)$, $(\mathbb{C},+,x)$ e $(\mathbb{Z}_p,+,x)$ con p primo, formano campi.

(3) Per costruire un anello commutativo ed integro ma non unitario si puo' prendere in un anello commutativo, integro ed unitario l'insieme dei multipli di un elemento diverso da 1. Ad esempio gli numeri interi pari con le operazioni

classiche.

(4) Le matrici quadrate di ordine n formano una struttura $(Mn, +, \times)$ che e' un anello unitario, non integro e non commutativo.

(5) Un anello neanche unitario e sempre non integro e non commutativo, si ottiene come sotto-anello del precedente prendendo come elementi i multipli di una qualsiasi matrice $A \neq I_n$. Considero cioe' l'insieme $\{ HA$ tale che $H \in Mn\}$; questa struttura forma un anello essendo :

$$H \times A + H' \times A = (H+H') \times A$$

$$(H \times A) \times (H' \times A) = (H \times A \times H') \times A$$

La proprieta'associativa e distributiva sono ereditate; non vale la proprieta' commutativa e l'elemento neutro non esiste.

(6) Un esempio di corpo e' dato dalla struttura dei quaternioni (somma dei numeri con i vettori tridimensionali) di cui ci occuperemo nel seguito.

(7) Un esempio di anello commutativo, unitario e non integro. L'insieme delle funzioni reali (non necessariamente continue) di variabile reale, definite su un medesimo intervallo, formano un anello non integro, commutativo ed unitario. Due funzioni non nulle il cui prodotto e' nullo (definite ad esempio su tutto $\mathbb{R}$) sono date da:
$f(x) = 0$ se $x = 1$ con $f(x) = 1$ se $x \neq 1$

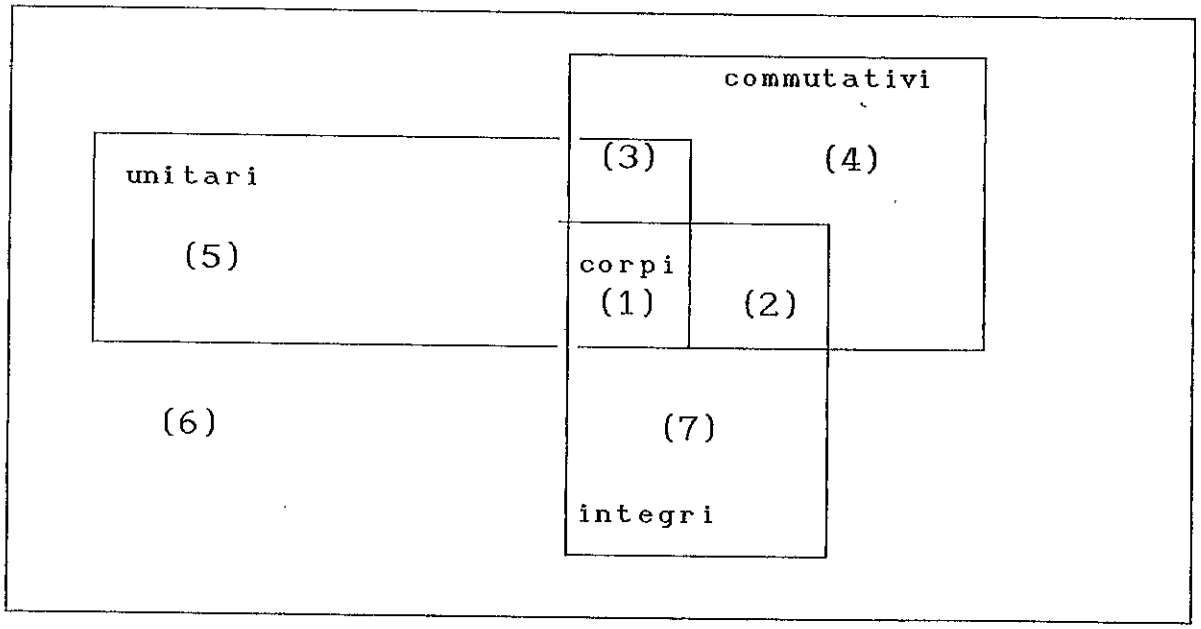
$g(x) = 1$ se $x = 1$ con $g(x) = 0$ se $x \neq 1$.

(8) Un esempio di anello commutativo, non unitario e non integro si ottiene dal precedente prendendo i multipli funzionali di un elemento non unitario.

(9) Un esempio di anello unitario, integro, non commutativo e non corpo è dato dall'insieme dei quaternioni a coefficienti interi (o anche razionali)

(10) Un esempio di anello non unitario, integro, non commutativo si ottiene dal precedente considerando i multipli di un fissato elemento non unitario.

Trattiamo, per cfompletezza il caso finito.



Caso finito

Nel caso che gli anelli in esame abbiano un numero finito di elementi alcune delle parti in esame sono vuote.

Si dimostra, e la dimostrazione complessa esula dai

nostri scopi, il seguente:

TEOREMA DI VEDDEBURN. Ogni corpo finito e' un campo.

Un facile teorema e' invece il seguente:

TEOREMA D'INVERSIONE . In ogni anello finito ed unitario un elemento non nullo e non divisore dello zero e' invertibile. Cio' significa in particolare che se un anello e' unitario ed integro esso e' un corpo e quindi per il teorma di Veddeburn e' un campo.

DIMOSTRAZIONE. Sia $a \in A$ un elemento non divisore dello zero (e non nullo). L'applicazione $x \longrightarrow ax$ e' manifestamente iniettiva (infatti $ax = ax'$ implica $a(x - x') = 0$ e quindi $x = x'$). Detta f tale applicazione, sia $f(A)$ la sua immagine; essendo A finito ed equicardinale ad $f(A)$ segue $f(A) = A$. Dunque per ogni $b \in A$ esiste un x tale che $f(x) = ax = b$, in particolare se b e' l'elemento neutro. Analogamente usando l'applicazione $a \longrightarrow xa$ si prova l'esistenza di un inverso destro, e quindi dell'unico inverso bilatero. La parte restante del teorema e' banale.

Diamo ora degli esempi per mostrare che le parti indicate in figura non sono vuote.

(1) Consideriamo $\mathbb{Z}_p$ con p primo.

(2) Un esempio di anello finito commutativo, integro , non unitario si ottiene, ad esempio, definendo su $(\mathbb{Z}_3, +)$ la moltiplicazione $(\times)$ definita ponendo:

$$a \times 0 = 0 \times a = 0 \quad , \quad \forall\, a \in \mathbb{Z}_3$$

$$a \times b = 2 \quad , \quad (a \neq 0 \quad , \quad b \neq 0) \quad \forall\, a, b \in \mathbb{Z}_3.$$

(Si puo' anche prendere $a \times b = 1$)

(3) Considero i binomi formali a coefficienti in $\mathbb{Z}_p$, p primo, del tipo $a + ib$ con somma e prodotto definiti alla maniera dei numeri complessi, ma con $i^2 = 0$. Ho un esempio di anello finito unitario e commutativo ma non integro. (Altri tipi possono ottenersi ponendo $i^2 = 1$ ovvero $\alpha i + \beta$, ove l'equazione $i^2 = \alpha i + \beta$ ha soluzioni in $\mathbb{Z}_p$).
In questo anello, in forza del teorema d'inversione sopra provato, gli elementi che non sono divisori dello zero sono invertibili. Si vede subito che, essendo :

$$(a + ib)\,(x + iy) = ax + i\,(bx + ay)$$

i divisori dello zero sono i numeri del tipo ib. I numeri del tipo $a + ib$, con $a \neq 0$, sono invertibili ed hanno l'inverso dato da :

$$x = 1/a \quad , \quad y = -b/a^2.$$

(4) Un esempio di anello finito commutativo, non unitario e non integro si ottiene dal precedente prendendo i multipli secondo gli elementi dell'anello di un divisore dello zero, ad esempio i multipli di i .

(5) Un esempio di anello finito unitario, non commutativo e non integro si costruisce prendendo l'insieme delle matrici, ad esempio quadrate su $\mathbb{Z}_p$ (p primo). Piu' in generale prendo le matrici quadrate d'ordine n.

(6) Un esempio di anello finito non unitario, non commutativo e non integro si costruisce prendendo l'insieme delle matrici, ad esempio quadrate su $\mathbb{Z}_p$, multiple di una fissata matrice divisore dello zero, ad esempio:

$$\begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix}.$$

(7) Un esempio di anello finito non commutativo, integro e non unitario si ottiene, ad esempio, considerando su $(\mathbb{Z}_3, +)$ la moltiplicazione $(\times)$ definita ponendo:

$$a \times 0 = 0 \times a = 0 \quad , \quad \forall\, a \in \mathbb{Z}_3$$

$$1\times1 = 1\times2 = 1 \ , \quad 2\times1 = 2\times2 = 2.$$

La verifica e' immediata.