~~Di caratteristica di un campo si intende~~

14/10/2013 (1)

In $\mathbb{Z}_2$ definiamo un'altra operazione binaria interna: il <u>prodotto</u> " $\cdot$ "

$\cdot$	0	1
0	0	0
1	0	1

L'ELEMENTO P VIENE MANDATO NELLA SUA CLASSE DI EQUIVALENZA $\overline{p}$

$$\begin{array}{ccccc} \overline{p} & \in & \mathbb{Z}_2 & \longrightarrow & \mathbb{Z}_2\ \overline{q} \\ \uparrow & & \uparrow & & \uparrow \\ p & \in & \mathbb{Z} & \longrightarrow & \mathbb{Z}_2 \\ & & p & \longmapsto & q \end{array}$$

COSÌ COME PER ALTRE PROPRIETÀ CHE VOGLIAMO VERIFICARE IN UNO SPAZIO QUOZIENTE, ANCHE IL PRODOTTO DI DUE CLASSI $\overline{p}\cdot\overline{q}$ SI OTTIENE IN QUESTO MODO: SI PRENDONO UN RAPPRESENTANTE PER LA CLASSE $\overline{p}$, P, ED UNO PER LA CLASSE $\overline{q}$, q: SI MOLTIPLICANO $p\cdot q$ IN $\mathbb{Z}$ E SI CONSIDERA LA CLASSE $\overline{p\cdot q}$: SE PRESI p_1 E q_1 TALI CHE $\overline{p}=\overline{p_1}$ E $\overline{q}=\overline{q_1}$, SI HA $\overline{p_1\cdot q_1}=\overline{p\cdot q} \Rightarrow$ SI PONE $\overline{p}\cdot\overline{q}=\overline{p\cdot q}$.

Quindi $(\mathbb{Z}_2,+,\cdot)$ è un campo (<u>finito</u> PERCHÈ HA UN NUMERO FINITO DI ELEMENTI)

Il numero di elementi in un campo K finito è sempre del tipo p^n, $n\in\mathbb{N}$ e p <u>numero primo</u>.

Dato un elemento $x\in K$ si dimostra che se moltiplico $px = \underbrace{x+x+x+\dots+x}_{p \text{ VOLTE}}$ è pari a zero, $\Rightarrow$ DICIAMO CHE il campo K ha <u>caratteristica p</u>. SE

$$\forall x\in K \Rightarrow px = \underbrace{x+x+x+\dots+x}_{p} = 0 .$$

$\mathbb{Q},\mathbb{R},\mathbb{C}$ hanno caratteristica 0.

Alcune PROPRIETÀ che NON VALGONO nei campi di caratteristica p (nel quale AD ESEMPIO non si può dividere per p) si possono ~~fare~~ VALERE nei campi di caratteristica 0.

Un sottoinsieme contenuto in un insieme che ha UNA STRUTTURA ALGEBRICA DI GRUPPO, CAMPO O ANELLO, ... viene chiamato <u>sottogruppo</u>, <u>sottocampo</u> o <u>sottoanello</u>.

SE TALE sottoinsieme è chiuso rispetto ALLE OPERAZIONI CHE DEFINISCONO LA STRUTTURA ALGEBRICA: AD ESEMPIO: $U\subset G$, $(G,+)$ gruppo additivo, È SOTTOGRUPPO SE 0, ELEMENTO NEUTRO DI G, APPARTIENE AD U, E $\forall\, u_1,u_2\in U$, $u_1+u_2\in U$.

<u>ULTERIORI</u> <u>OPERAZIONI TRA MATRICI</u>:

CERCHIAMO un'operazione di "<u>prodotto</u>" tra matrici: UN PRODOTTO RIGA x COLONNA: SE LA CERCHIAMO SU $\mathcal{M}(\mathbb{R})$ COME operazione binaria INTERNA DEL TIPO:

$$\begin{array}{ccc} \mathcal{M}(\mathbb{R})\times\mathcal{M}(\mathbb{R}) & \longrightarrow & \mathcal{M}(\mathbb{R}) \\ (A;B) & \longmapsto & AB \end{array}$$

NON RIUSCIAMO A DARLA:

Non è possibile per ogni coppia!! DI MATRICI QUALUNQUE:

Definiamo l'operazione:

$$A = (a_{i,j})_{\substack{i=1,\dots,r\\ j=1,\dots,s}} \quad e \quad B = (b_{h,k})_{\substack{h=1,\dots,n\\ k=1,\dots,s}} \Rightarrow \text{definiamo } AB = C = (c_{\ell,m})_{\substack{\ell=1,\dots,\\ m=1,\dots}}$$

in questo modo $c_{\ell,m} = \sum_{r=1}^{n} a_{\ell,r} \cdot b_{r,m}$

PERCHÉ SI POSSA DETERMINARE LA MATRICE PRODOTTO, È CHIARO CHE il numero di colonne della prima matrice A deve essere uguale al numero di righe della seconda matrice B.

ESEMPIO:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}_{2\times\boxed{3}} \quad e \quad B = \begin{pmatrix} 1 & 0 & 1 \\ -1 & -1 & -1 \\ 2 & 1 & 0 \end{pmatrix}_{\boxed{3}\times 3}$$

$$\Rightarrow AB = \begin{pmatrix} c_{11} = \sum_{r=1}^{3} a_{1r} b_{r1} = a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31} = 1 + (-2) + 6 = 5 \dots \\ c_{21} \end{pmatrix} = \begin{pmatrix} 5 & c_{12} = 1 & c_{13} = -1 \\ c_{21} = 11 & c_{22} = 1 & c_{23} = -1 \end{pmatrix}$$

$$AB = \begin{pmatrix} 5 & 1 & -1 \\ 11 & 1 & -1 \end{pmatrix}_{2\times 3}$$

Quindi abbiamo come risultato una matrice che ha tante colonne quante ne ha la seconda matrice e tante righe quante ne ha la prima matrice.

$$\text{"}\circ\text{"}: \mathcal{M}_{p\times n} \times \mathcal{M}_{n\times q} \longrightarrow \mathcal{M}_{p\times q}$$
$$(A, B) \longmapsto A\cdot B$$

Se prendo: LE MATRICI QUADRATE DI ORDINE n:

$$\mathcal{M}_{n\times m} \times \mathcal{M}_{m\times m} \longrightarrow \mathcal{M}_{m\times m}$$
$$(A, B) \longmapsto A\circ B$$

IL PRODOTTO È ORA SEMPRE POSSIBILE E TALE OPERAZIONE È BINARIA INTERNA

Quando si può fare, il prodotto tra matrici è <u>ASSOCIATIVO</u>; (DIMOSTRARLO)

cioè $A\cdot(B\cdot C) = (A\cdot B)\cdot C$: SI DIMOSTRA CONSIDERANDO $A = (a_{ij})$ $B = (b_{\ell m})$ e $C = (c_{kn})$ ED ESEGUENDO IL PRODOTTO NEL MEMBRO A DESTRA E NEL MEMBRO A SINISTRA E FACENDO VEDERE CHE OTTENIAMO LA STESSA MATRICE.

VEDIAMO GLI ORDINI DELLE MATRICI:

$$\underbrace{A_{p\times n}\cdot \underbrace{(B_{n\times k}\cdot C_{k\times s})}_{P_{n\times s}}}_{p\times s} = \underbrace{\underbrace{(A\cdot B)}_{D_{p\times k}}\cdot C_{k\times s}}_{p\times s}$$

Esiste l'elemento neutro, dato la matrice $A=(a_{i,j})_{i,j=1,\dots,n}$, cerco una matrice $B=(b_{i,j})_{i,j=1,\dots,n}$ tale che $A\cdot B = A$:

IMPONGO L'UGUAGLIANZA TRA LE ENTRATE DELLE MATRICI

DIMOSTRAZIONE: $\Longrightarrow$ $AB = C = (c_{i,j}) \rightarrow c_{ij} = \sum_{r=1}^{n} a_{ir} b_{rj} = a_{ij} \quad \forall\, ij$

$$c_{ij} = a_{i,j}$$

Per ottenere questo ~~posso~~ MI BASTA, porre $b_{rj} = \begin{cases} 0 & r \neq j \\ 1 & r = j \end{cases}$

allora la nostra matrice B è una matrice diagonale:

$$B = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \dots & 1 \end{pmatrix} = I_n \quad : \quad \text{matrice identità}$$

ESISTE ELEMENTO NEUTRO ANCHE SE IL PRODOTTO È DEFINITO PER MATRICI NON QUADRATE: DEFINIAMO IL PRODOTTO PER LE MATRICI

$$\mathcal{M}_{p\times n} \times \mathcal{M}_{n\times n} \longrightarrow \mathcal{M}_{p\times n}$$

$\Rightarrow$ L'ELEMENTO NEUTRO È ANCORA LA MATRICE $I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & 0 \dots & 0 \\ \vdots & & \ddots & 0 \\ 0 & \dots & & 1 \end{pmatrix}$

Esercizio:

$$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$\nexists \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tale che sia vera l'uguaglianza: INFATTI ESEGUITO IL PRODOTTO A SINISTRA, L'UGUAGLIANZA TRA MATRICI, PORTA AD UN SISTEMA SCALARE

$$\begin{pmatrix} a+2c & b+2d \\ 2a+4c & 2b+4d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{cases} a+2c = 1 \\ b+2d = 0 \\ 2a+4c = 0 \\ 2b+4d = 1 \end{cases}$$

OTTENUTO UGUAGLIANDO LE ENTRATE CORRISPONDENTI

Non esiste nessun a,b,c,d tale che sia vera l'uguaglianza!

Date un esempio del fatto che il prodotto non è commutativo.

ESERCIZIO · ↑

INTRODUCIAMO UN'ALTRA OPERAZIONE:

MOLTIPLICAZIONE PER UNO SCALARE

La moltiplicazione per uno scalare $\alpha \in \mathbb{R}$ si definisce come:

$$\cdot \; \mathbb{R} \times \mathcal{M}_{p \times n}(\mathbb{R}) \longrightarrow \mathcal{M}_{p \times n}(\mathbb{R})$$

$$(\alpha, A) \longmapsto \alpha A$$

DOVE αA È LA MATRICE COSÌ DEFINITA:

Se $A = (a_{i,j})_{\substack{i=1,\dots,p \\ j=1,\dots,n}} \Rightarrow \alpha A = (\alpha \cdot a_{ij})_{\substack{i=1,\dots,p \\ j=1,\dots,n}}$.

ESEMPIO:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \quad e \quad \alpha = 2 \Rightarrow 2A = \begin{pmatrix} 2 & 4 & 6 \\ 8 & 10 & 12 \end{pmatrix}$$

L'elemento neutro è $1 \in \mathbb{R}$

ESERCIZIO: provare la proprietà distributiva: $\alpha(A+B) = \alpha A + \alpha B$