

Algebra — 29 Luglio 2010

1. Quali dei seguenti insiemi di matrici quadrate $n \times n$ formano un anello (**non necessariamente con identità**) con l'addizione e il prodotto di matrici? (motivare le risposte)
 - Matrici simmetriche.
 - Matrici triangolari alte. ($a_{ij} = 0$ per $i > j$)
 - Matrici triangolari alte con tutti 0 sulla diagonale
 - Matrici i cui elementi sono tutti nulli eccetto, possibilmente, quelli della prima colonna.
 - Dimostrare che, in quest'ultimo caso, tutti gli elementi sono divisori di zero.
2. Considerato il campo $\mathbb{F} = \mathbb{Z}_2[\alpha]$ con $\alpha^3 + \alpha + 1 = 0$
 - Verificare che il polinomio $x^3 + x + 1$ è irriducibile in $\mathbb{Z}_2[x]$.
 - Scrivere gli elementi del campo $\mathbb{F}$.
 - Calcolare $(1 + \alpha + \alpha^2)(1 + \alpha)$
 - Trovare $(1 + \alpha)^{-1}$.
 - Mostrare che $1 + \alpha$ è un elemento primitivo. Quali sono gli altri elementi primitivi?
 - Scrivere tutti gli elementi del campo come potenze di $1 + \alpha$.
3. Sia R un anello commutativo con identità i cui unici ideali sono $\{0\}$ e R stesso.
 - Dimostrare che R è un campo.
 - E' vero il viceversa?
4. Sia A un gruppo commutativo e sia $End(A) = \{f : A \rightarrow A \text{ con } f \text{ omomorfismo}\}$ l'insieme degli endomorfismi di A .
 - Mostrare che $End(A)$ è un anello con identità.
 - Sia $I = \{f \in End(A) \text{ tali che } f(a) = e \text{ se } a \in A \text{ ha ordine finito}\}$. Mostrare che I è un ideale bilaterale di $End(A)$.
5. Trovare tutti i numeri interi positivi k per cui, in $\mathbb{Z}_{11}^*$, si ha $3^k = 4$.

TRACCIA DELLE SOLUZIONI

Esercizio n.1:

No, sì, sì, sì. Le matrici considerate nell'ultimo caso hanno tutte determinante nullo e quindi sono divisori di zero.

Esercizio n.2:

Gli 8 elementi sono:

$$1, 1 + \alpha, 1 + \alpha^2, 1 + \alpha + \alpha^2 \\ 0, \alpha, \alpha^2, \alpha + \alpha^2$$

Posto $(1 + \alpha)^{-1} = a + b\alpha + c\alpha^2$ con $a, b, c \in \mathbb{Z}_2$, si ha:

$$\begin{aligned} (1 + \alpha)(a + b\alpha + c\alpha^2) &= a + b\alpha + c\alpha^2 + a\alpha + b\alpha^2 + c\alpha^3 = \\ a + c + (a + b + c)\alpha + (b + c)\alpha^2 &= 1 \end{aligned}$$

da cui si ricava subito: $a = 0, b, c = 1$. Un elemento primitivo è un generatore del gruppo $\mathbb{F}^*$ degli elementi invertibili del campo, ovvero un elemento di ordine moltiplicativo 7; siccome l'ordine di un elemento deve dividere l'ordine del gruppo, e 7 è un numero primo, tutti gli elementi $\neq 0, 1$ sono primitivi.

Esercizio n.3:

Sia $a \neq 0 \in R$ e consideriamo l'ideale generato da a : si ha $(a) = R$. Quindi $1 \in (a)$ e quindi esiste $b \in R$ tale che $ab = ba = 1$; abbiamo quindi dimostrato che tutti gli elementi $\neq 0$ sono invertibili. Per il viceversa basta osservare che in un campo K ogni elemento $\neq 0$ è invertibile e quindi se un qualsiasi ideale contiene un elemento $\neq 0$ deve anche contenere 1 e quindi coincidere con K .

Esercizio n.4:

$End(A)$ è un anello con le operazioni:

$$\begin{aligned} (f + g)(a) &= f(a)g(a) \\ (f \cdot g)(a) &= f(g(a)) \end{aligned}$$

la commutatività del gruppo A assicura la commutatività della operazione $+$ in $End(A)$. Lo zero dell'anello è l'endomorfismo $0(a) = e \forall a \in A$ e l'elemento 1 dell'anello è l'endomorfismo $1(a) = a \forall a \in A$. L'opposto additivo è $(-f)(a) = [f(a)]^{-1}$

I è un ideale bilaterale perchè è banalmente un sottogruppo additivo: se a ha ordine finito si ha

$$(f + g)(a) = f(a)g(a) = ee = e,$$

ed inoltre se $h \in I$ e $f \in End(A)$ si ha:

$$\begin{aligned} (f \cdot h)(a) &= f(h(a)) = f(e) = e \\ (h \cdot f)(a) &= h(f(a)) = e \end{aligned}$$

Dove l'ultima uguaglianza deriva dal fatto che in un gruppo se a ha ordine finito e f è un endomorfismo, anche $f(a)$ ha ordine finito. Infatti se $a^n = e$, si ha anche:

$$[f(a)]^n = f(a^n) = f(e) = e.$$

Esercizio n.5:

Basta calcolare, modulo 11, le potenze di 3 fino ad ottenere 1 :

$$3^2 \bmod 11 = 9, 3^3 \bmod 11 = 5, 3^4 \bmod 11 = 4, 3^5 \bmod 11 = 1$$

Segue immediatamente che $k = 4 + 5N$ (con N intero non negativo), infatti:

$$3^{4+5N} \bmod 11 = 3^4 3^{5N} \bmod 11 = 4$$