Algebra - 30 settembre 2011

Linee guida: *ogni affermazione che scrivete o utilizzate deve essere giustificata, o da un calcolo diretto, o da una dimostrazione, oppure dall'applicazione di un risultato trattato nel corso e adeguatamente citato. Il voto dipende anche dalla qualità delle spiegazioni, non solo dall'esattezza dei calcoli.*

1. Sia G l'insieme:
$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \text{ con } 1, a, b, c \in \mathbb{Z}_2 \right\}$$
   - Mostrare che G è un gruppo con l'usuale prodotto tra matrici con elementi in un campo.
   - Quanti elementi ha?
   - Trovare un sottogruppo H di ordine 4.
   - A che gruppo noto G è isomorfo?

2. Sia F_{81} il campo con 81 elementi.
   - Mostrare che l'applicazione $f : F_{81} \to F_{81}$ definita da $f(a) = a^3$ con $a \in F_{81}$ è un omomorfismo.
   - E' un isomorfismo?
   - Trovare l'insieme dei punti fissi[1] di f e mostrare che è un sottocampo di F_{81}.

3. Sia R un anello con unità. Dati $a, b \in R$ tali che $(1 - ab)$ sia invertibile, sia c l'inverso di $(1 - ab)$:
   - Dimostrare che $d = (1 + bca)$ è l'inverso di $(1 - ba)$.
   - Calcolare $(1 + adb)$.

4. Trovare tutti gli interi positivi k per cui vale:
$$3^k \bmod 11 = 4$$

[1] Ovvero l'insieme degli $a \in F_{81}$ per cui $f(a) = a$

Soluzioni

Esercizio n.1

$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \text{ con } 1, a, b, c \in \mathbb{Z}_2 \right\}$ è un gruppo perchè il prodotto è associativo, interno, e contiene l'identità e gli inversi. L'inverso è:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a & b+ac \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \tag{1}$$

Il gruppo G ha 8 elementi:

$$G = \left\{ \begin{array}{cccc} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, & \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, & \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, & \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, & \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, & \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, & \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \end{array} \right\} \tag{2}$$

Un sottogruppo di ordine 4 è quello generato da un elemento di ordine 4:

$$H = \left\{ \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\} \tag{3}$$

Posto, ad esempio,

$$c = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{4}$$

Si ottiene:

$$b^2 = c^4 = 1 \text{ con la relazione } cb = bc^{-1} \tag{5}$$

Per cui $G = D_4$.

Esercizio n.2

E'evidente che $f(1) = 1$ e che $f(ab) = f(a)f(b)$ l'unico punto da verificare è:

$$f(a+b) = f(a) + f(b) \tag{6}$$

Si ha, ricordando che la caratteristica di F_{81} è 3 (infatti $81 = 3^4$):

$$(a+b)^3 = a^3 + b^3 + 3ab^2 + 3a^2b = a^3 + b^3 \tag{7}$$

Calcoliamo ora il nucleo: $a^3 = 1$ se e solo se $a = 1$ perchè 3 non divide 80 (l'ordine di F_{81}^*) e quindi f è un isomorfismo.
L'insieme dei punti fissi è l'insieme $a^3 - a = 0$. Questa equazione ha esattamente 3 radici: $0, 1, 1+1$ (infatti ne abbiamo trovate 3 e non possono, in un campo, essercene di più del grado). Il loro insieme forma un campo (ovviamente isomorfo al sottocampo primo $\mathbb{Z}_3$), infatti le tavole delle operazioni sono (ricordando che la caratteristica è 3):

$$\begin{array}{cccc} + & \mathbf{0} & \mathbf{1} & \mathbf{1+1} \\ \mathbf{0} & 0 & 1 & 1+1 \\ \mathbf{1} & 1 & 1+1 & 0 \\ \mathbf{1+1} & 1+1 & 0 & 1 \end{array} \qquad \begin{array}{cccc} \cdot & \mathbf{0} & \mathbf{1} & \mathbf{1+1} \\ \mathbf{0} & 0 & 0 & 0 \\ \mathbf{1} & 0 & 1 & 1+1 \\ \mathbf{1+1} & 0 & 1+1 & 1 \end{array} \tag{8}$$

Esercizio n.3

Se c è l'inverso di $(1 - ab)$, si ha che:

$$(1-ab)\,c = 1 \Rightarrow c - abc = 1 \tag{9}$$
$$c\,(1-ab) = 1 \Rightarrow c - cab = 1 \tag{10}$$

ovvero, moltiplicando la prima a destra per a e la seconda a sinistra per b:

$$ca - abca = a \tag{11}$$
$$bc - bcab = b \tag{12}$$

Possiamo ora calcolare:

$$(1-ba)\,(1+bca) = 1 + bca - ba - babca = 1 + bca - ba - b\,(ca - a) = 1 \tag{13}$$
$$(1+bca)\,(1-ba) = 1 + bca - ba - bcaba = 1 + bca - ba - (bc - b)\,a = 1 \tag{14}$$

Cioè $(1 - ba)$ è invertibile con inversa d.
Calcoliamo ora $(1 + adb)$:

$$1 + adb = 1 + a(1 + bca)b = 1 + ab + abcab = 1 + ab + cab - ab = 1 + cab = c$$

Esercizio n.4

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:

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