Università degli Studi Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2004/2005
AL2 - Algebra 2, gruppi, anelli e campi
Prima prova di valutazione intermedia
3 novembre 2004

Soluzione

1. Sia G l'insieme delle matrici quadrate di ordine 2 a elementi in $\mathbb{Z}_8$ della forma:
$$A = \begin{pmatrix} a & 0 \\ c & d \end{pmatrix}, \text{ con } ad = 1.$$

   (a) Mostrare che G è un gruppo commutativo rispetto alla moltiplicazione righe per colonne;

   (b) Mostrare che l'applicazione
   $$\varphi : G \longrightarrow \mathcal{U}(\mathbb{Z}_8) \text{ definita da } A \to a$$
   è un omomorfismo di gruppi;

   (c) Determinare $Ker(\varphi)$ e $Im(\varphi)$ e definire l'isomorfismo canonico
   $$G/Ker(\varphi) \longrightarrow Im(\varphi);$$

   (d) Determinare $\varphi^{-1}(\bar{5})$.

Soluzione

Osserviamo che la relazione $ad = 1$ implica che
$$a \in U(\mathbb{Z}_8) = \{1, 3, 5, 7\} \cong V_4$$
Dunque $a = d$.

   (a) Verifichiamo che G è un sottogruppo di $GL_2(\mathbb{Z}_8)$. Data $A \in G$
   $$A^{-1} = \begin{pmatrix} a & 0 \\ -c & a \end{pmatrix} \in G$$
   e per ogni A e $B \in G$
   $$AB^{-1} = \begin{pmatrix} a & 0 \\ c & a \end{pmatrix} \begin{pmatrix} b & 0 \\ -c' & b \end{pmatrix} = \begin{pmatrix} ab & 0 \\ bc - ac' & ab \end{pmatrix} \in G$$
   Verifichiamo la commutatività.
   $$AB = \begin{pmatrix} a & 0 \\ c & a \end{pmatrix} \begin{pmatrix} b & 0 \\ c' & b \end{pmatrix} = \begin{pmatrix} ab & 0 \\ bc + ac' & ab \end{pmatrix}$$
   $$BA = \begin{pmatrix} b & 0 \\ c' & b \end{pmatrix} \begin{pmatrix} a & 0 \\ c & b \end{pmatrix} = \begin{pmatrix} ab & 0 \\ bc + ac' & ab \end{pmatrix}$$
   da cui G è commutativo.

(b) Siano A e $B \in G$. Verifichiamo che $\varphi(AB) = \varphi(A)\varphi(B)$.

$$\begin{aligned}
\varphi(A) &= a \\
\varphi(B) &= b \\
\varphi(AB) &= \varphi\left(\begin{pmatrix} a & 0 \\ c & a \end{pmatrix}\begin{pmatrix} b & 0 \\ c' & b \end{pmatrix}\right) \\
&= \varphi\left(\begin{pmatrix} ab & 0 \\ bc + ac' & ab \end{pmatrix}\right) \\
&= ab
\end{aligned}$$

Dunque

$$\varphi(AB) = ab = \varphi(A)\varphi(B)$$

(c)

$$\ker\varphi = \{A \in G : \varphi(A) = 1\} = \left\{\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} : c \in \mathbb{Z}_8\right\}$$

$$\mathtt{Im}\varphi = \{a \in \mathbb{Z}_8 : \exists A \in G \text{ e } \varphi(A) = a\} = \{1, 3, 5, 7\} = U(\mathbb{Z}_8)$$

Ricordiamo che $\ker\varphi$ un sottogruppo normale. Allora

$$G/\ker\varphi = \left\{\overline{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}} : a \in U(\mathbb{Z}_8)\right\}$$

Dunque l'omomorfismo canonico è definito da

$$\phi : G/\ker\varphi \longrightarrow U(\mathbb{Z}_8)$$

tale che

$$\phi\left(\overline{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}}\right) = a$$

(d)

$$\varphi^{-1}(5) = \left\{\begin{pmatrix} 5 & 0 \\ c & 5 \end{pmatrix} : c \in \mathbb{Z}_8\right\}$$

2. Sia C_{12} il gruppo delle radici complesse dodicesime dell'unità.

   (a) Determinare il gruppo $Aut(C_{12})$ degli automorfismi di C_{12}:

   (b) Stabilire se $Aut(C_{12})$ è un gruppo ciclico.

   Soluzione

   (a) Osserviamo che

   $$\begin{aligned} C_{12} &= \left\{z \in \mathbb{C} : z^{12} = 1\right\} \\ &= \left\{e^{\frac{2k\pi i}{12}} \text{ con } k = 0, \ldots, 11\right\} \end{aligned}$$

   Ricordiamo che i generatori di C_{12} sono le radici primitive dell'unità, cioé $z = e^{\frac{2k\pi i}{12}}$ con $k = 1, 5, 7, 11$. Poniamo $z_0 = e^{\frac{\pi i}{6}}$, allora

   $$C_{12} = \left\{z_0^i : i = 0 \ldots 11\right\}$$

   Dunque abbiamo quattro possibili automorfismi

   $$\varphi_i : C_{12} \longrightarrow C_{12}$$

   definiti da

   $$\varphi_i(z_0) = z_0^i$$

   per $i = 1, 5, 7, 11$. Quindi

   $$Aut(C_{12}) = \{\varphi_1 = id, \varphi_5, \varphi_7, \varphi_{11}\}.$$

   (b) Osserviamo che $\varphi_5^2 = \varphi_7^2 = \varphi_{11}^2 = \varphi_1$, quindi $Aut(C_{12}) \cong V_4$ non è ciclico.

3. Determinare le possibili strutture cicliche e gli ordini degli elementi del gruppo alterno di grado sette $\mathbf{A_7}$.

   Soluzione

   Ricordiamo che A_7 sono le permutazioni pari. Le possibili strutture cicliche sono

   - (-)
   - (- - -)
   - (- - - - -)
   - (- - - - - - -)
   - (- -)(- -)
   - (- -)(- - - -)
   - (- - -)(- - -)
   - (- - -)(- -)(- -)

   Inoltre

   - (-) ha ordine 1
   - (- - -) ha ordine 3
   - (- - - - -) ha ordine 5
   - (- - - - - - -) ha ordine 7
   - (- -)(- -) ha ordine 2
   - (- -)(- - - -) ha ordine 4
   - (- - -)(- - -) ha ordine 3
   - (- - -)(- -)(- -) ha ordine 6

4. Nel prodotto cartesiano $\mathbb{Z}_2 \times \mathbb{Z}_5$ si definisca l'operazione

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

Mostrare che rispetto a questa operazione $\mathbb{Z}_2 \times \mathbb{Z}_5$ è un gruppo ciclico e determinate tutti i suoi generatori.

Soluzione

Mostriamo che $\mathbb{Z}_2 \times \mathbb{Z}_5$ è un gruppo. Siano a, c e $e \in \mathbb{Z}_2$ e b, d e $f \in \mathbb{Z}_5$ allora

- *Chiusura*

$$(a, b) + (c, d) = (a + c, b + d) \in \mathbb{Z}_2 \times \mathbb{Z}_5$$

- *Associativià*

$$((a, b)+(c, d))+(e, f) = (a+c+e, b+d+f) = (a, b)+((c, d)+(e, f))$$

- *Esistenza dell'elemento neutro*

$$(a, b) + (0, 0) = (0, 0) + (a, b) = (a, b)$$

- *Inverso*

$$-(a, b) = (-a, -b)$$

Inoltre è facile vedere che $\mathbb{Z}_2 \times \mathbb{Z}_5$ è generato da $(1, b)$ con $b \in \mathbb{Z}_5$ non zero

5. Sia G un gruppo moltiplicativo e N un sottogruppo normale di G di indice m. Mostrare che, per ogni $g \in G$, $g^m \in N$.

   Soluzione

   Poiché $[G : N] = m$ abbiamo $\#(G/N) = m$. Per ogni $g \in G$ consideriamo la sua classe $gN \in G/N$ allora

$$g^m N = (gN)^m = eN$$

   Quidi

$$g^m \in N$$