Algebra B - 27 marzo 2007

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.

1. Denotiamo con $\mathbb{Z}_n^*$ il gruppo **moltiplicativo** degli elementi invertibili di $\mathbb{Z}_n$.
   - Trovare due sottogruppi H e K di $\mathbb{Z}_{11}^*$ di ordine 2 e 5 rispettivamente.
2. Sia G un gruppo **abeliano finito** di ordine n e sia m un intero **primo** con n.
   - Dimostrare che l'applicazione $\varphi : G \to G$ definita da $\varphi(g) = g^m$ è un isomorfismo.
   - Dimostrare che $\forall g \in G$, l'equazione $x^m = g$ ha una e una sola soluzione in G (tale soluzione si dice radice $m-$ esima "discreta" di g)
   - Trovare in $\mathbb{Z}_{22}^*$ la radice cubica discreta di 5.
3. Si consideri l'anello $\mathbb{Z}\left[\sqrt{-3}\right] = \left\{a + ib\sqrt{3} \text{ con } a, b \in \mathbb{Z}\right\}$.
   - Si mostri che non ha divisori dello zero.
   - Trovare le unità di $\mathbb{Z}\left[\sqrt{-3}\right]$ e mostrare che formano un gruppo ciclico.
4. Si consideri l'insieme K :

$$K = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \text{ con } a, b, d \in \mathbb{Z}_4 \right\}$$

   K è un anello finito con le usuali operazioni tra matrici.
   - Trovare, se esistono, i divisori dello zero, quanti sono?
   - Descrivere esplicitamente K^* (il gruppo delle unità di K) e trovarne l'ordine.
   - Verificare esplicitamente nel caso dell'anello K il seguente risultato noto: *in ogni anello finito tutti gli elementi $\neq 0$ sono unità o divisori dello zero.*
   - Trovare il centro di K^*.

Soluzioni

1. Basta trovare un elemento di ordine 2 e un elemento di ordine 5. Un breve calcolo mostra che $\#10 = 2$ e che $3^5 \bmod 11 = 1$ per cui $\#3 = 5$. Ne segue subito che $H = \{1, 10\}$, mentre $K = \{\text{le potenze di } 3\} = \{1, 3, 9, 5, 4\}$

2. φ è un omomorfismo perchè il gruppo è abeliano:

$$\varphi(xy) = (xy)^m = x^m y^m = \varphi(x)\varphi(y)$$

Il nucleo di φ è dato dagli elementi g tali che $\varphi(g) = g^m = e$. Ma questo è vero per $g \neq e$ se e solo se m è multiplo di n e questo è escluso per ipotesi. Ne segue che il nucleo è ridotto al solo elemento neutro. L'applicazione è quindi iniettiva e perciò anche suriettiva (perchè iniettiva tra insiemi della stessa cardinalità finita). L'equazione data ha una soluzione perchè φ è suriettiva, e quindi $\forall g \; \exists x$ tale che $g = \varphi(x) = x^n$; la soluzione è unica perchè φ è iniettiva. In $\mathbb{Z}_{22}$, $[5] = [27] = [3^3]$, per cui la radice cubica cercata è 3.

3. Un elemento $a + ib\sqrt{3} \neq 0$ dell'anello dato è divisore dello zero se $\exists \; x + iy\sqrt{3} \neq 0$ tale che:

$$\left(a + ib\sqrt{3}\right)\left(x + iy\sqrt{3}\right) = ax - 3by + iay\sqrt{3} + ibx\sqrt{3} = 0.$$

Ne segue:

$$\begin{cases} ax - 3by = 0 \\ bx + ay = 0 \end{cases}$$

Il sistema omogeneo ha solo la soluzione nulla perchè il determinante della matrice dei coefficienti è $a^2 + 3b^2 \neq 0$. Un elemento $a + ib\sqrt{3} \neq 0$ dell'anello dato è una unità se $\exists$ $x + iy\sqrt{3} \neq 0$ tale che:

$$\left(a + ib\sqrt{3}\right)\left(x + iy\sqrt{3}\right) = ax - 3by + iay\sqrt{3} + ibx\sqrt{3} = 1.$$

Ne segue:

$$\begin{cases} ax - 3by = 1 \\ bx + ay = 0 \end{cases}$$

La cui soluzione "formale" è $\left[x = \frac{a}{a^2+3b^2}, y = -\frac{b}{a^2+3b^2}\right]$. Se imponiamo le condizioni $a, b, x, y \in \mathbb{Z}$, otteniamo che deve essere $a^2 + 3b^2 = 1$, cioè $a = \pm 1$, $b = 0$. Le uniche unità sono quindi ± 1, e quindi $\left(\mathbb{Z}\left[\sqrt{-3}\right]\right)^*$ è isomorfo a $\mathbb{Z}_2$.

4. I divisori dello zero sono le matrici $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ con $\det \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = ad = [0]_4$

oppure $=[2]_4$. Ovvero le $3+12+12+4+4+4+4+4=47$ matrici:

$$\begin{aligned}
\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \text{ con } b &= 1,2,3 \\
\begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \text{ con } d &= 1,2,3 \text{ e } b=0,1,2,3 \\
\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \text{ con } a &= 1,2,3 \text{ e } b=0,1,2,3 \\
\begin{pmatrix} 2 & b \\ 0 & 2 \end{pmatrix} \text{ con } b &= 0,1,2,3 \\
\begin{pmatrix} 1 & b \\ 0 & 2 \end{pmatrix} \text{ con } b &= 0,1,2,3 \\
\begin{pmatrix} 2 & b \\ 0 & 1 \end{pmatrix} \text{ con } b &= 0,1,2,3 \\
\begin{pmatrix} 2 & b \\ 0 & 3 \end{pmatrix} \text{ con } b &= 0,1,2,3 \\
\begin{pmatrix} 3 & b \\ 0 & 2 \end{pmatrix} \text{ con } b &= 0,1,2,3
\end{aligned}$$

E' facile infatti trovare esplicitamente per ognuno dei tipi di matrici descritte sopra una matrice diversa da zero tale che il prodotto dia la matrice nulla. Le unità sono le matrici invertibili, cioè quelle con $\det \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = ad = 1,3$.Ovvero le $8+8=16$ matrici:

$$\begin{aligned}
\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \text{ con } b &= 0,1,2,3 \text{ e } d=1,3 \\
\begin{pmatrix} 3 & b \\ 0 & d \end{pmatrix} \text{ con } b &= 0,1,2,3 \text{ e } d=1,3
\end{aligned}$$

Le matrici che costituiscono K sono in tutto $4\times 4\times 4=64=1+47+16$. Il centro di K^* sono le unità che commutano con tutte le altre unità:

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay+bz \\ 0 & dz \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} ax & bx+dy \\ 0 & dz \end{pmatrix}$$

da cui, $\forall a,b,d$ deve essere $ay+bz=bx+dy$, ovvero $x=z$ e $y=0$; inoltre la matrice ottenuta deve essere una unità, per cui $x=1,3$.