SOLUZIONI DELLA PROVA SCRITTA
DI MATEMATICA DISCRETA I
1-6-2000 CANALE A-L

Esercizio 1 (a). Occorre verificare l'associatività del prodotto, l'esistenza dello elemento neutro e dell'inverso di ogni elemento. Usando il fatto che le operazioni $\bullet$, $*$ sono associative, si ha, per $g_i \in G,\ h_i \in H,\ 1 \leq i \leq 3$:

$$\begin{aligned}
&((g_1,h_1)\cdot(g_2,h_2))\cdot(g_3,h_3) = (g_1 \bullet g_2, h_1 * h_2)\cdot(g_3,h_3) = \\
&((g_1 \bullet g_2)\bullet g_3, (h_1 * h_2) * h_3) = (g_1 \bullet (g_2 \bullet g_3), h_1 * (h_2 * h_3)) = \\
&(g_1,h_1)\cdot(g_2 \bullet g_3, h_2 * h_3) = (g_1,h_1)\cdot((g_2,h_2)\cdot(g_3,h_3)).
\end{aligned}$$

e l'operazione $\cdot$ è associativa. È facile verificare che se e, e' sono gli elementi neutri di G, H, (e,e') è l'elemento neutro per $\cdot$; infine l'inverso di (g,h) è (g^{-1},h^{-1}).

(b) Ricordiamo che se una permutazione è espressa come prodotto di cicli disgiunti, il suo ordine è il m.c.m. della lunghezza di cicli. Pertanto una permutazione di S_4 ha ordine 2 se e solo se è una trasposizione o è il prodotto di due trasposizioni disgiunte, ed ha ordine 4 se e solo se è un 4-ciclo. Pertanto si ha:

$$\begin{aligned}
&(1,2),(1,3),(1,4),(2,3),(2,4),(3,4),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\\
&(1,2,3,4),(1,2,4,3),(1,3,2,4),(1,3,4,2),(1,4,2,3),(1,4,3,2).
\end{aligned}$$

Esercizio 2 (a). Denotiamo con $\sim$ l'equivalenza per righe. Poichè

$$\begin{pmatrix} 1 & k & 0 & -1 \\ i & 1 & 0 & h \end{pmatrix} \sim \begin{pmatrix} 1 & k & 0 & -1 \\ 0 & 1-ik & 0 & h+i \end{pmatrix}$$

si ha

$$dim(W) = 1 \quad \Longleftrightarrow \quad \begin{cases} 1-ik=0 \\ h+i=0 \end{cases} \quad \Longleftrightarrow h = k = -i$$

e $dim(W) = 2$ negli altri casi.
(b). Si verifica facilmente che il vettore $(i,0,1,0)$ non è mai combinazione lineare delle righe della matrice precedente. Pertanto

$$dim(V+W) = \begin{cases} 2 & \text{se } h = k = -i \\ 3 & \text{altrimenti.} \end{cases}$$

Esercizio 3 (a). Risulta $\det(A) = 2(k-2)$, pertanto per $k \neq 2$ F è un isomorfismo e dunque $Ker(F) = \{0\}$, $Im(F) = W$. Per $k = 2$ coordinate rispetto a $\mathcal{B}$ dei vettori di $Ker(F)$ si ottengono risolvendo il sistema $AX = 0$; una possibile base di $Ker(F)$ è costituita dalla matrice $\begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$. Coordinate rispetto a $\mathcal{C}$ dei vettori di $Im(F)$ si ottengono riducendo per righe ${}^tA$; una possibile base di $Im(F)$ è

$\{1+t+2t^2, -1+t\}$.
(b). Se $k \neq 2$, F è suriettiva e dunque ogni vettore di W appartiene a $Im(F)$; se $k = 2$ si verifica direttamente che $1+2t^2$ non è combinazione lineare di $1+t+2t^2, -1+t$, pertanto tale vettore non appartiene a $Im(F)$.
(c). Occorre risolvere il sistema $AX = b$ ove $b = {}^t(0,2,2)$ è il vettore delle coordinate di $2t(1+t)$ rispetto a $\mathcal{C}$. Si ha

$$F^{-1}(2t(1+t)) = \left\{ \begin{pmatrix} 1+a & 1 \\ -a & -1-a \end{pmatrix} \mid a \in \mathbb{R} \right\}.$$

Esercizio 4 Per le parti a, b, c si vedano i testi consigliati. Per il primo quesito della parte d basta dimostrare che i vettori $av_1, \ldots, av_n$ sono linearmente indipendenti, ovvero che $x_1av_1 + \ldots + x_nav_n = 0$ implica $x_1 = \ldots = x_n = 0$. Ma $x_1av_1 + \ldots + x_nav_n = 0$ se e solo se $x_1v_1 + \ldots + x_nv_n = 0$ (dato che $a \neq 0$), dunque l'asserto segue dall'indipendenza lineare di $v_1, \ldots, v_n$.

Sia $A = (a_{ij}) = {}_{\mathcal{B}}[F]_{\mathcal{B}}$. Allora $F(v_i) = \sum_{j=1}^n a_{ji}v_j$; per la linerità di F, tale relazione è equivalente a $F(av_i) = \sum_{j=1}^n a_{ji}av_j$, dunque $A = {}_{\mathcal{C}}[F]_{\mathcal{C}}$.

Esercizio 5 (a) È noto che un gruppo ciclico finito ha uno e un solo sottogruppo (anch'esso ciclico) per ogni divisore dell'ordine. Dunque l'unico sottogruppo non banale è $\{\overline{0}, \overline{3}, \overline{6}\}$.
(b) È noto che gli elementi invertibili di $\mathbb{Z}_n$ sono le classi $\overline{m}$ con $0 < m < n$, m primo con n. Pertanto $U(\mathbb{Z}_9) = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$. Costruendo la tabella moltiplicativa si può vedere che tale gruppo è generato da $\overline{2}$ o da $\overline{5}$.
(c). Supponiamo che G sia generato da g; proviamo che G' è generato da $\varphi(g)$; dato infatti $g' \in G'$, la suriettività di φ garantisce l'esistenza di $x \in G$ tale che $\varphi(x) = g'$. D'altra parte, poichè G è ciclico, è $x = g^k$ per qualche k, dunque $g' = \varphi(x) = \varphi(g^k) = \varphi(g)^k$.
(d). Dal punto precedente segue che un isomorfismo è univocamente determinato dall'immagine di un generatore e che l'immagine di un generatore è un generatore. Poichè $(U(\mathbb{Z}_9), \cdot)$ è generato da $\overline{2}$ o da $\overline{5}$ mentre $(\mathbb{Z}_6, +)$ è generato da $\overline{1}$ o da $\overline{5}$ si hanno due possibili distinti isomorfismi $\alpha, \beta : (U(\mathbb{Z}_9), \cdot) \to (\mathbb{Z}_6, +)$. Esplicitamente:

$$\alpha : \qquad \overline{2} \mapsto \overline{1} \quad \overline{4} \mapsto \overline{2} \quad \overline{8} \mapsto \overline{3} \quad \overline{7} \mapsto \overline{4} \quad \overline{5} \mapsto \overline{5} \quad \overline{1} \mapsto \overline{0}$$

$$\beta : \qquad \overline{2} \mapsto \overline{5} \quad \overline{4} \mapsto \overline{4} \quad \overline{8} \mapsto \overline{3} \quad \overline{7} \mapsto \overline{2} \quad \overline{5} \mapsto \overline{1} \quad \overline{1} \mapsto \overline{0}.$$