Traccia delle Soluzioni della Prova di Algebra per Informatica del 9-1-2006

<u>Esercizio 1</u> a) Poiché $4725 = 3^3 \cdot 5^2 \cdot 7$, si ha che il numero di elementi invertibili in $\mathbb{Z}_{4725}$ è

$$\varphi(4725) = \varphi(3^3)\varphi(5^2)\varphi(7) = (27-9)(25-5)\,6 =$$
$$= 18 \cdot 20 \cdot 6 = 2160.$$

$\bar{a}$ è invertibile in $\mathbb{Z}_{4725}$ se $(a, 4725) = 1$ dunque $\overline{1555}$ non è invertibile mentre $4096 = 2^{12}$ lo è. Per calcolare l'inverso di $\overline{4096}$ scriviamo l'identità di Bezout relativa a $4096, 4725$. Si ha

$4725 = 4096 \cdot 1 + 629$
$4096 = 629 \cdot 6 + 322$
$629 = 322 \cdot 1 + 307$
$322 = 307 \cdot 1 + 15$
$307 = 15 \cdot 20 + 7$
$15 = 7 \cdot 2 + 1$
$7 = 7 \cdot 1 + 0$

da cui

$$4096 \cdot 631 - 4725 \cdot 547 = 1$$

e

$$\overline{4096} \cdot \overline{631} = \bar{1}$$

b) Risulta $U_{27} = \{\bar{a} \mid 1 \le a < 27,\ (a, 27) = 1\}$
$= \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}, \overline{10}, \overline{11}, \overline{13}, \overline{14}, \overline{16}, \overline{17}, \overline{19}, \overline{20}, \overline{22}, \overline{23}, \overline{25}, \overline{26}\}$

un gruppo di ordine $18 = \varphi(3^3)$. Si vede subito che $\langle \bar{2} \rangle = U_{27}$. Dunque U_{27} ha uno e un solo sottogruppo (ciclico) per ogni divisore dell'ordine. Poiché $18 = 2 \cdot 3^2$, gli ordini possibili sono $1, 2, 3, 6, 9, 18$

Il reticolo dei sottogruppi è

$$\begin{tikzcd}[column sep=small]
 & U_{27} \arrow[dl, no head] \arrow[dr, no head] & \\
\langle \bar{4} \rangle \arrow[d, no head] & & \langle \bar{8} \rangle \arrow[dll, no head] \arrow[d, no head] \\
\langle \overline{10} \rangle \arrow[dr, no head] & & \langle \overline{26} \rangle \arrow[dl, no head] \\
 & \{\bar{1}\} &
\end{tikzcd}$$

(Si ricordi che se $G = \langle g \rangle$ e $|G| = n$, $H \leq G$, $|H| = m$, allora $H = \langle g^{\frac{n}{m}} \rangle$.)

c) Risulta $\gamma = \alpha^{-2}\beta = (\alpha^{-1})^2 \beta =$
$= (1,2,6,3,7,4,8,5)$ (infatti $\alpha = (1,4,6,8,3,5,7)$, $\beta = (1,2,3,4,5,6,7,8)$). Dunque γ ha ordine 8 ed è una permutazione dispari.

Esercizio 2 a) Detti v_1, v_2, v_3 i vettori che generano V, si vede immediatamente che $v_3 = v_1 + v_2$, dunque v_1, v_2, v_3 sono linearmente dipendenti. Poiché v_1, v_2 non sono proporzionali, essi sono indipendenti e generatori per V, dunque sono una base. W è l'insieme delle soluzioni del sistema associato alla matrice $\begin{pmatrix} 1 & 0 & 1 & -2 \\ 1 & 0 & -1 & 0 \end{pmatrix}$. Poiché

$$\begin{pmatrix} 1 & 0 & 1 & -2 \\ 1 & 0 & -1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 & -2 \\ 0 & 0 & -2 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

il sistema è equivalente a $\begin{cases} x_1 = x_4 \\ x_3 = x_4 \end{cases}$ che ha per soluzioni

$$\mathbb{R}\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \oplus \mathbb{R}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

b) Una base per $W+V$ è data dalle righe non nulle di una forma a gradini della matrice

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

Essendo tale matrice equivalente per righe a $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$, dunque una base per $W+V$ è

$\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \right\}$. Dalla formula di Grassmann segue che $\dim V \cap W = 2+2-3 = 1$. Poiché $v_3 \in V \cap W$,

$$V \cap W = \mathbb{R} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}.$$

<u>Esercizio 3</u> a) Risulta $F\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$, $F\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 6 & -10 \\ -10 & 3 \end{pmatrix}$, $F\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 18 & -36 \\ -36 & 11 \end{pmatrix}$. Dunque

$$A = \begin{pmatrix} 2 & 6 & 18 \\ 0 & -10 & -36 \\ 0 & 3 & 11 \end{pmatrix}.$$

b) Il polinomio caratteristico di A è $\begin{vmatrix} 2-t & 6 & 18 \\ 0 & -10-t & -36 \\ 0 & 3 & 11-t \end{vmatrix} = 0$,

cioè $(t-2)(t^2-t-2) = (t-2)^2(t+1)$.

Pertanto gli autovalori sono $2, -1$ con molteplicità algebriche $2, 1$ rispettivamente. Dall'analisi degli autospazi deduciamo che

$$m_g(2) = 3 - rg\begin{pmatrix} 0 & 6 & 18 \\ 0 & -12 & -36 \\ 0 & 3 & 9 \end{pmatrix} = 3 - 1 = 2,$$

pertanto F è diagonalizzabile.

Esercizio 4   a, b, c, e) Si vedano testi o dispense

d) $1001 = 7 \cdot 11 \cdot 13$. I sottogruppi propri di $\mathbb{Z}_{1001}$ sono tanti quanti i divisori non banali dell'ordine, dunque $7, 11, 13, 7 \cdot 11, 7 \cdot 13, 11 \cdot 13$. In totale abbiamo 6 sottogruppi propri

e) Dobbiamo trovare una partizione $(m_1, \ldots, m_k)$ di 9 tale che $m.c.m(m_1, \ldots, m_k) = 12$ e $\sum (m_i - 1)$ sia pari. Le partizioni con la prima proprietà sono $(4, 3, 2)$ e $(4, 3, 1, 1)$. Solo la prima ha la seconda proprietà richiesta. Dunque un possibile esempio è $\sigma = (1, 2, 3, 4)(5, 6, 7)(8, 9)$