Padova, 4 novembre 2005

Soluzione Prima Prova Parziale di Algebra
Compito A

Esercizio 1

a) Si ha $\alpha = (25347)(89)$ e $\beta = (12)(3547)(89)$.
L' ordine di una permutazione è il minimo comune multiplo delle lunghezze dei suoi cicli disgiunti. Quindi l' ordine di α è 10 e l' ordine di β è 4.
Ogni ciclo di lunghezza l è prodotto di $l-1$ scambi. Quindi $sgn(\alpha) = -1$ e $sgn(\beta) = -1$ in quanto α e β sono prodotto di 5 scambi.

b) H è evidentemente non vuoto (contiene l'identità). Siano $\sigma, \tau \in H$. Allora $\sigma(i) \le 5$ e $\tau(i) \le 5$ per ogni $i \le 5$. Pertanto anche $\tau^{-1}(i) \le 5$ per ogni $i \le 5$ e dunque $\sigma\tau^{-1} \in H$. Cioè H è sottogruppo di Σ_9

c) $H\alpha$ e $H\beta$ coincidono se e solo se $\alpha\beta^{-1} \in H$. Ora $\beta^{-1} = (12)(3745)(89)$ e $\alpha\beta^{-1} = (15432)$. Perciò $\alpha\beta^{-1} \in H$.

d) Sia $\tau \in \Sigma_9$. Non può essere $\tau(i) > 5$ per ogni $i \le 5$, quindi esiste $j \le 5$ tale che $\tau(j) \le 5$. Sia ora $\tau \notin H$. Allora esiste $i \le 5$ tale che $\tau(i) > 5$. Sia $\alpha = \tau\sigma\tau^{-1}$. Si ha $\alpha(\tau(j)) = \tau\sigma(j)$. Sia $\sigma \in H$ tale che $\sigma(j) = i$ (per esempio lo scambio (ij)), allora $\alpha(\tau(j)) = \tau(i)$ e pertanto $\alpha \notin H$ poiché $\tau(j) \le 5$ mentre $\tau(i) > 5$. Si conclude che $\tau H \tau^{-1} \neq H$.

Esercizio 2

a) A è sottoanello dell' anello delle matrici 2×2 a coefficienti interi se e solo se la differenza e il prodotto di due elementi di A è ancora un elemento di A.
Siano $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}, \begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix}$ elementi di A. Allora

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} - \begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix} = \begin{pmatrix} a-a' & 0 \\ b-b' & c-c' \end{pmatrix} \in A,$$

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \cdot \begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ ba'+cb' & cc' \end{pmatrix} \in A$$

b) I è ideale bilatero di A se e solo se:
1. I è sottogruppo additivo di A;
2. Per ogni $M \in A$ e $N \in I$, $MN \in I$ e $NM \in I$.

1. Siano $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}, \begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix} \in I$. Allora

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} - \begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix} = \begin{pmatrix} a-a' & 0 \\ b-b' & c-c' \end{pmatrix} \in I$$

poichè $c, c' \in n\mathbb{Z}$ implica $c - c' \in n\mathbb{Z}$.

2. Siano $\begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \in A$, $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in I$. Allora

$$\begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} = \begin{pmatrix} xa & 0 \\ ya+zb & zc \end{pmatrix} \in I,$$

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \cdot \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} = \begin{pmatrix} ax & 0 \\ bx+cy & cz \end{pmatrix} \in I$$

poichè, se $c \in n\mathbb{Z}$ anche $cz \in n\mathbb{Z}$.

Sia $\phi\colon A \to \mathbb{Z}/n\mathbb{Z}$ definito da

$$\phi(\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}) = c + n\mathbb{Z}.$$

ϕ è omomorfismo d'anelli in quanto:

1. $$\phi(\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} + \begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix}) = \phi(\begin{pmatrix} a+a' & 0 \\ b+b' & c+c' \end{pmatrix}) = (c+c') + n\mathbb{Z} =$$
$$= (c+n\mathbb{Z}) + (c'+n\mathbb{Z}) = \phi(\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}) + \phi(\begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix}).$$

2. $$\phi(\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \cdot \begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix}) = \phi(\begin{pmatrix} aa' & 0 \\ ba'+cb' & cc' \end{pmatrix}) = (cc') + n\mathbb{Z} =$$
$$= (c+n\mathbb{Z}) \cdot (c'+n\mathbb{Z}) = \phi(\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}) \cdot \phi(\begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix}).$$

$\operatorname{Ker}\phi = \{\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in A \mid c+n\mathbb{Z} = 0+n\mathbb{Z}\} = \{\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \mid c \in n\mathbb{Z}\} = I.$

c) ϕ è epimorfismo, quindi dal teorema fondamentale di omomorfismo d'anelli $A/I \cong \mathbb{Z}/n\mathbb{Z}$.
Se ne deduce che gli ideali di A/I sono in corrispondenza biunivoca con gli ideali di $\mathbb{Z}/n\mathbb{Z}$, cioè con gli ideali della forma $m\mathbb{Z}/n\mathbb{Z}$ dove m è un divisore di n. Pertanto gli ideali di A/I sono della forma J/I dove $J = \{\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in A \mid c \in m\mathbb{Z}\}$, con m divisore di n.

Esercizio 3

Si veda il libro.

Esercizio 4

a) $\mathbb{Z}[i]$ è dominio a ideali principali, quindi I è primo se e solo se il suo generatore è irriducibile.
Si ha $2-4i = 2(1-2i) = (1+i)(1-i)(1-2i)$ e nessuno tra questi fattori è invertibile, in quanto gli elementi invertibili di $\mathbb{Z}[i]$ sono solo quelli di norma 1, cioè $1, -1, i, -i$. Quindi $2-4i$ è riducibile.

b) Come visto sopra, $2-4i$ è un multiplo di $(1+i)$; quindi $I \subseteq J$. Inoltre $1+i$ è un elemento irriducibile. Infatti, la sua norma è 2 e quindi in ogni fattorrizzazione di $1+i$ almeno uno dei fattori deve avere norma 1, cioè deve essere invertibile. Percio' J è ideale primo e in un dominio a ideali principali un ideale primo non nullo è massimale.

c) Si ha $1+i = i(1-i)$. Quindi $1+i$ e $1-i$ sono associati e pertanto generano lo stesso ideale.