Soluzione Prima Prova Parziale di Algebra
Compito B

Esercizio 1

a) Si ha $\rho = (19)(25347)$ e $\sigma = (192)(3547)$.
L' ordine di una permutazione è il minimo comune multiplo delle lunghezze dei suoi cicli disgiunti. Quindi l' ordine di ρ è 10 e l' ordine di σ è 12.
Ogni ciclo di lunghezza l è prodotto di $l-1$ scambi. Quindi $sgn(\rho) = -1$ e $sgn(\sigma) = -1$ in quanto ρ e σ sono prodotto di 5 scambi.

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

c) $A\rho$ e $A\sigma$ coincidono se e solo se $\rho\sigma^{-1} \in A$. Ora $\sigma^{-1} = (129)(3745)$ e $\rho\sigma^{-1} = (15432)$. Perciò $\rho\sigma^{-1} \notin A$.

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

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 $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$ elementi di A. Allora

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

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

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 $NM \in I$.

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

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

poichè $a, a' \in n\mathbb{Z}$ implica $a - a' \in n\mathbb{Z}$.
2. Siano $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in A$, $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in I$. Allora

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

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

poichè, se $a \in n\mathbb{Z}$ anche $ax \in n\mathbb{Z}$.

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

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

ϕ è omomorfismo d'anelli in quanto:

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

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

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

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

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

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 $J = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in A \mid a \in m\mathbb{Z}\}$, 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 irriducubile.
Si ha $4 + 2i = 2(2+i) = (1+i)(1-i)(2+i)$ 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 $4 + 2i$ è riducibile.

b) Come visto sopra, $4 + 2i$ 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 fattorizzazione di $1 + i$ almeno uno dei fattori deve avere norma 1 e quindi è 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.