A.A. 2015-2016. CORSO DI ALGEBRA 1.
PROFF. P. PIAZZA, E. SPINELLI.
SOLUZIONE ESERCIZI FOGLIO 3.

Esercizio 2.1. Sia $(A, +, \cdot)$ un anello (associativo) unitario.
(A) Mostrare che se $a \in A$ è invertibile allora l'inverso sinistro e l'inverso destro coincidono.
(B) Dimostrare che se $a \in A$ è un divisore dello zero non banale allora a non è invertibile.
(C) Assumiamo che $(A, +, \cdot)$ sia anche commutativo. Mostrare che l'insieme dei divisori dello zero è chiuso rispetto al prodotto.

Soluzione. Per quanto riguarda il punto (A). Supponiamo che $a \in A$ sia invertibile; per definizione questo significa che a possiede sia un inverso sinistro che un inverso destro. Li denoteremo rispettivamente ℓ_a, r_a. Allora:

$$r_a = 1_A \cdot r_a = (\ell_a \cdot a) \cdot r_a = \ell_a \cdot (a \cdot r_a) = \ell_a \cdot 1_A = \ell_a$$

Questo dimostra il punto (A) dell'esercizio.

Per quanto riguarda il punto (B). Ragioniamo per assurdo: supponiamo che a sia un divisore dello zero non banale, e supponiamo che esso sia invertibile. Questo significa che esiste $b \neq 0_A$ tale che $a \cdot b = 0_A$ oppure $b \cdot a = 0_A$ (assumeremo che valga la prima, l'altro caso è analogo), ed esiste un elemento, $a^{-1} \in A \setminus \{0_A\}$, tale che $a^{-1} \cdot a = a \cdot a^{-1} = 1_A$. Allora risulta

$$0_A = a^{-1} \cdot 0_A = a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = 1_A \cdot b = b$$

Ma per ipotesi $b \neq 0_A$. Questo conclude la dimostrazione.

Passiamo al punto (C); vogliamo dimostrare che, sotto l'addizionale ipotesi di commutatività dell'anello $(A, +, \cdot)$, l'insieme dei divisori dello zero è chiuso rispetto al prodotto. Siano quindi $a, c \in A$ due divisori dello zero. Possiamo assumere che $a \cdot c \neq 0_A$ dato che, se così non fosse, l'asserzione seguirebbe banalmente. Essendo a un divisore dello zero non banale ed utilizzando la commutatività di $(A, +, \cdot)$ deduciamo che esiste b tale che $a \cdot b = b \cdot a = 0_A$. Ne segue che $b \cdot (a \cdot c) = (b \cdot a) \cdot c = 0_A \cdot c = 0_A$, e dunque l'elemento $a \cdot c$ è un divisore dello zero non banale. □

Esercizio 2. 2. [1] Sia G un gruppo nel quale sia verificata per ogni coppia di elementi $a, b \in G$ l'uguaglianza: $(ab)^2 = a^2b^2$. Mostrare che il gruppo G è abeliano.

Soluzione. Sappiamo che per ogni coppia di elementi $a, b \in G$ risulta $(ab)^2 = a^2b^2$; scrivendo esplicitamente $(ab)^2 = abab$ la precedente uguaglianza può essere scritta come $abab = a^2b^2$. Moltiplicando a sinistra per a^{-1} e a destra per b^{-1} entrambi i lati dell'uguaglianza troviamo:

$$ab = (a^{-1} \cdot a) \cdot ab \cdot (b \cdot b^{-1}) = a^{-1} \cdot a^2b^2 \cdot b^{-1} = a^{-1} \cdot abab \cdot b^{-1} = (a^{-1} \cdot a) \cdot ba \cdot (b \cdot b^{-1}) = ba$$

Poiché tale relazione è verificata per ogni coppia di elementi $a, b \in G$ ne segue che il gruppo G è abeliano. □

Esercizio 2. 3. [2] Siano $a, b, x \in \mathbb{Z}$. Supponiamo che $a \,|\, x$, $b \,|\, x$ e $\mathrm{MCD}(a, b) = 1$. Mostrare che $ab \,|\, x$.

Soluzione. Poiché $a \,|\, x$ per definizione di divisibilità ne segue che $x = y \cdot a$; ora $b \,|\, x$ e dunque b divide il prodotto $y \cdot a$: $b \,|\, y \cdot a$. Poiché $\mathrm{MCD}(a, b) = 1$, segue dal Lemma di Euclide che $b \,|\, y$; pertanto $y = z \cdot b$. Andando a sostituire nell'equazione $x = y \cdot a$ l'equazione $y = z \cdot b$ ne ricaviamo l'uguaglianza $x = z \cdot (a \cdot b)$ che è equivalente a dire $ab \,|\, x$. □

[1] Tratto dal libro Algebra di I.N. Herstein, Esercizio 3, Sezione 2.3
[2] Tratto dal libro Algebra di I.N. Herstein, Esercizio 4, Sezione 1.3

Esercizio 2. 4. Utilizzando l'algoritmo delle divisioni successive determinare l' MCD e una Identità di Bézout per la seguente coppia di numeri interi: 334 e 219. (*Invito. Allenatevi a casa a fare questo stesso tipo di esercizio con altre coppie di numeri*)

Soluzione. Applichiamo l'algoritmo delle divisioni successive:

$$334 = 1 \cdot 219 + 115$$
$$219 = 1 \cdot 115 + 104$$
$$115 = 1 \cdot 104 + 11$$
$$104 = 9 \cdot 11 + 5$$
$$11 = 2 \cdot 5 + 1$$
$$5 = 5 \cdot 1 + 0$$

Il primo resto non nullo è 1, pertanto $\mathrm{MCD}(334, 219) = 1$. Per scrivere una identità di Bézout (seguendo il capitolo 2 del vostro libro di testo) procediamo come segue:

$$115 = 334 - 1 \cdot 219$$
$$104 = 219 - 1 \cdot 115 = 2 \cdot 219 - 1 \cdot 334$$
$$11 = 115 - 104 = -3 \cdot 219 + 2 \cdot 334$$
$$5 = 104 - 9 \cdot 11 = 2 \cdot 219 - 1 \cdot 334 - 18 \cdot 334 + 27 \cdot 219 = 29 \cdot 219 - 19 \cdot 334$$
$$1 = 11 - 2 \cdot 5 = 40 \cdot 334 - 61 \cdot 219$$

L'ultima uguaglianza è l'identità di Bézout che stavamo cercando. □

Esercizio 2. 5. Siano p e q due numeri primi distinti. Mostrare che $\{k\,p \mid k \in \mathbb{Z}\} \setminus \{k\,q \mid k \in \mathbb{Z}\}$ e $\{k\,q \mid k \in \mathbb{Z}\} \setminus \{k\,p \mid k \in \mathbb{Z}\}$ sono sottoinsiemi di $\mathbb{Z}$ di cardinalità numerabile.

Soluzione. Mostriamo che il primo insieme contiene un numero infinito di elementi. Trattandosi di un sottoinsieme di $\mathbb{Z}$ esso sarà dunque numerabile (per il secondo insieme si può ragionare in totale analogia). La strategia è mostrare che $p^k = p^{k-1} \cdot p$ sono contenuti nell'insieme $\{k\,p \mid k \in \mathbb{Z}\} \setminus \{k\,q \mid k \in \mathbb{Z}\}$. Sia allora $k_0 = \min\{k \in \mathbb{N} \mid p^k = m \cdot q\}$; poiché p, $q > 1$ e $\mathrm{MCD}(p, q) = 1$ (si tratta infatti di numeri primi distinti) deve risultare $k_0 > 1$ (diversamente avremmo $q \mid p$). Per la stessa ragione, utilizzando il lemma di Euclide dalla condizione $q \mid p^{k_0-1} \cdot p$ ricaviamo che $q \mid p^{k_0-1}$, questo contraddice la minimalità di k_0. Pertanto nessuno dei p^k è multiplo di q. Poiché $\{p^k \mid k \in \mathbb{N}\} \subset \{k\,p \mid k \in \mathbb{Z}\} \setminus \{k\,q \mid k \in \mathbb{Z}\} \subset \mathbb{Z}$ ne segue che l'insieme $\{k\,p \mid k \in \mathbb{Z}\} \setminus \{k\,q \mid k \in \mathbb{Z}\}$ ha cardinalità numerabile. □

Esercizio 2. 6. Sia G un gruppo ed a un elemento di $G \setminus \{1\}$ tale che $a^k = 1$ per qualche $k \in \mathbb{N}$. Sia m il più piccolo intero positivo per cui $a^m = 1$. Mostrare che se $a^k = 1$ allora $m \mid k$. (*Suggerimento. Usare la minimalità di $m \in \mathbb{N}$ e la divisione con resto*)
Sia G un gruppo abeliano e siano $a, b \in G$ due elementi il cui prodotto in G è non banale e tali che $a^p = 1$ e $b^q = 1$ per $p, q \in \mathbb{N}$ due numeri primi distinti. Mostrare che il più piccolo $k \in \mathbb{N}$ per cui $(ab)^k = 1$ è $k = p\,q$. (*Suggerimento. Usare il Lemma di Euclide*)

Soluzione Cominciamo dalla prima parte dell'esercizio. Sia G un gruppo e supponiamo che $a^k = 1$ per un qualche $k \in \mathbb{N} \setminus \{0\}$. Sia $m = \min\{n \in \mathbb{N} \setminus \{0\} \mid a^n = 1\}$. Vogliamo far vedere che $m \mid k$. Supponiamo dunque che $m \not| k$. Essendo $m < k$ possiamo scrivere $k = q \cdot m + r$ con $0 < r < m$; d'altra parte $1 = a^k = a^{q \cdot m + r} = a^{q \cdot m} a^r = (a^m)^q a^r = a^r$. Questo contraddice la minimalità di m. Dunque deve risultare $m \mid k$.

Passiamo quindi al secondo punto dell'esercizio. In questa seconda parte si assume G abeliano e si considerano due elementi $a, b \in G$ tali che $a^p = b^q = 1$, per p, q due numeri primi distinti. Osserviamo che, per abelianità di G, risulta evidentemente che $(ab)^{p\,q} = a^{p\,q} b^{p\,q} = (a^p)^q (b^q)^p = 1$. Vogliamo far vedere che il più piccolo k per cui $(ab)^k = 1$ è proprio $k = p \cdot q$. Se cosí non fosse, per il punto precedente dovrebbe esistere un k_0, minimale rispetto alla proprietà $(ab)^k = 1$, tale che $k_0 \mid p\,q$ e $k_0 < p \cdot q$. Essendo $k_0 \neq 1$ (altrimenti $a \cdot b = 1$) osserviamo che, essendo p, q primi, deve risultare che:

$\{\mathrm{MCD}(k_0,p)=p \text{ e } \mathrm{MCD}(k_0,q)=q\}$ oppure uno tra $\mathrm{MCD}(k_0,p)$ e $\mathrm{MCD}(k_0,q)$ deve essere uguale ad 1. Supponiamo che valga la prima possibilità. Dalla condizione $\mathrm{MCD}(k_0,p)=p$ segue che $k_0=m\cdot p$, dalla seconda condizione $\mathrm{MCD}(k_0,q)$ segue che $q\,|\,m\cdot p$; poiché $\mathrm{MCD}(p,q)=1$ per il Lemma di Euclide deve risultare $q\,|\,m$ e dunque $m=n\cdot q$. D'altra parte avevamo supposto che fosse $n\cdot p\cdot q=k_0<p\cdot q$, e $k_0>1$ e questo è assurdo. Consideriamo quindi la seconda possibiltà; assumiamo che valga $\mathrm{MCD}(k_0,p)=1$ (l'altro caso è analogo). Vi sono due possibilità: $\mathrm{MCD}(k_0,q)=1$ oppure $\mathrm{MCD}(k_0,q)=q$. Se valessero contemporaneamente $\mathrm{MCD}(p,k_0)=\mathrm{MCD}(q,k_0)=1$ avremmo un assurdo, per il Lemma di Euclide infatti se $k_0\,|\,p\cdot q$ e $\mathrm{MCD}(k_0,p)=1$ allora $k_0\,|\,q$. Possiamo assumere $\mathrm{MCD}(k_0,q)=q$. Scriviamo quindi $k_0=m\cdot q$ ed osserviamo che $m\cdot q\,|\,p\cdot q\ \Rightarrow m\,|\,p$; essendo p un numero primo questo implica che $m=1,p$. Poiché $k_0<p\,q$ deve essere $m=1$ ma chiaramente $(a\cdot b)^q=a^q\cdot b^q=a^q$ non può essere uguale ad 1, infatti $a^p=1$ e per il punto precedente, essendo p primo, è banale osservare che p è il minimo tra i numeri $k\in\mathbb{N}\setminus\{0\}$ tali che $a^k=1$; sempre sfruttando il punto precedente quindi, se fosse $a^q=1$, dovrebbe essere verificata $p\,|\,q$, il che è assurdo perché $\mathrm{MCD}(p,q)=1$.

Abbiamo quindi dimostrato che non può essere $k_0<p\cdot q$, dunque $p\cdot q$ è il minimo intero positivo tale che $(ab)^k=1$. □

Esercizio 2. 7. Consideriamo l'insieme $\mathfrak{M}_{2,2}(\mathbb{Z})$ delle matrici 2×2 a coefficienti in $\mathbb{Z}$. Consideriamo le due operazioni seguenti:

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}+\begin{pmatrix}e&f\\g&h\end{pmatrix}=\begin{pmatrix}a+e&b+f\\c+g&d+h\end{pmatrix}$$

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}\cdot\begin{pmatrix}e&f\\g&h\end{pmatrix}=\begin{pmatrix}ae+bg&af+bh\\ce+dg&cf+dh\end{pmatrix}$$

(A) Verificare che $(\mathfrak{M}_{2,2}(\mathbb{Z}),+)$ è un gruppo abeliano.
(B) Verificare che $(\mathfrak{M}_{2,2}(\mathbb{Z}),+,\cdot)$ è un anello (associativo) unitario. E' commutativo?
(C) Esistono divisori dello zero non banali? In caso affermativo esibirne uno.
(D) Richiamiamo il seguente fatto di algebra lineare: sia $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathfrak{M}_{2,2}(\mathbb{R})$ l'inversa di A è data dalla formula seguente:

$$A^{-1}=\frac{1}{\det(A)}\cdot\begin{pmatrix}d&-b\\-c&a\end{pmatrix}=\frac{1}{ad-bc}\cdot\begin{pmatrix}d&-b\\-c&a\end{pmatrix}$$

Definiamo $\mathrm{SL}_2(\mathbb{Z})=\{A\in\mathfrak{M}_{2,2}(\mathbb{Z})\mid \det(A)=1\}$. Mostrare che tale insieme è un gruppo rispetto al prodotto. (*Suggerimento. Utilizzare la formula fornita per verificare che l'inversa di un elemento* $A\in\mathrm{SL}_2(\mathbb{Z})$ *è ancora in* $\mathrm{SL}_2(\mathbb{Z})$).
(E) Mostrare che la matrice $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$ commuta con tutte le matrici in tale insieme se e solo se $A=\pm Id=\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}$. (*Suggerimento. Utilizzare la condizione sul determinante e quella di commutazione con le matrici* $\begin{pmatrix}0&1\\-1&0\end{pmatrix}$, $\begin{pmatrix}1&1\\0&1\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$ *per ottenere equazioni per i coefficienti*).
(F) Qual è l'ordine del gruppo generato dalle potenze dalla matrice $\begin{pmatrix}0&1\\-1&0\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$?
(G) Sia $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$ e supponiamo che i coefficienti di A siano tutti non nulli. Mostrare che $\mathrm{MCD}(a,b)=1$. (*Suggerimento. Sfruttare l'identità di Bézout*)
(H) Mostrare che se $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$ allora $\begin{pmatrix}a&b\\c+ka&d+kb\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$ per ogni $k\in\mathbb{Z}$.

Soluzioni. Cominciamo da (A). Di banale verifica il fatto che l'elemento $0_{2,2}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$ è l'elemento neutro della somma. In modo altrettanto semplice si può osservare che l'elemento $\begin{pmatrix}-a&-b\\-c&-d\end{pmatrix}$ è

l'opposto dell'elemento $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Previa verifica del fatto che la somma è associativa, questo dimostra che $(\mathfrak{M}_{2,2}(\mathbb{Z}), +)$ è un gruppo. L'abelianità del gruppo $(\mathfrak{M}_{2,2}(\mathbb{Z}), +)$ segue dal fatto che l'operazione "+" è definita entrata per entrata:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} = \begin{pmatrix} e+a & f+b \\ g+c & h+d \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Questo prova il punto (A).

Passiamo alla soluzione del punto (B). Sappiamo già che $(\mathfrak{M}_{2,2}(\mathbb{Z}), +)$ è un gruppo abeliano. Dobbiamo quindi mostrare che l'operazione di prodotto è associativa, ammette un elemento neutro ed è distributiva rispetto alla somma. Verifichiamo l'associatività del prodotto:

$$\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right] \cdot \begin{pmatrix} i & l \\ m & n \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} \cdot \begin{pmatrix} i & l \\ m & n \end{pmatrix} =$$

$$= \begin{pmatrix} (ae+bg)i + (af+bh)m & (ae+bg)l + (af+bh)n \\ (ce+dg)i + (cf+dh)m & (ce+dg)l + (cf+dh)n \end{pmatrix} =$$

$$= \begin{pmatrix} (ei+fm)a + (gi+hm)b & (el+fn)a + (gl+hn)b \\ (ei+fm)c + (gi+hm)d & (el+fn)c + (gl+hn)d \end{pmatrix} =$$

$$= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} ei+fm & el+fn \\ gi+hm & gl+hn \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left[\begin{pmatrix} e & f \\ g & h \end{pmatrix} \cdot \begin{pmatrix} i & l \\ m & n \end{pmatrix}\right]$$

E' di facile verifica il fatto che l'elemento neutro della moltiplicazione esiste, ed è dato dall'elemento $1_{2,2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Verifichiamo dunque la distributività del prodotto rispetto alla somma (verificheró la distributività solamente rispetto alla moltiplicazione a sinistra, il caso in cui si moltiplica a destra è analogo):

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left[\begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} i & l \\ m & n \end{pmatrix}\right] = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e+i & f+l \\ g+m & h+n \end{pmatrix} = \begin{pmatrix} a(e+i)+b(g+m) & a(f+l)+b(h+n) \\ c(e+i)+d(g+m) & c(f+l)+d(h+n) \end{pmatrix} =$$

$$= \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} + \begin{pmatrix} ai+bm & al+bn \\ ci+dm & cl+dn \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} i & l \\ m & n \end{pmatrix}$$

La non commutatività può essere facilmente verificata moltiplicando nei due modi possibili le matrici:

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

Per quanto riguarda il punto (C) si osservi che $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = 0_{2,2}$, dunque $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ è un divisore dello zero non banale.

Nel punto (D) si introduce l'insieme $\mathrm{SL}_2(\mathbb{Z}) \subset \mathfrak{M}_{2,2}(\mathbb{Z})$ e si chiede di verificare che esso è un gruppo rispetto all'operazione di prodotto. E' di banale verifica osservare che $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ appartiene all'insieme $\mathrm{SL}_2(\mathbb{Z})$. Verifichiamo che il prodotto di due matrici in $\mathrm{SL}_2(\mathbb{Z})$ è ancora in $\mathrm{SL}_2(\mathbb{Z})$. Siano quindi $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $\begin{pmatrix} e & f \\ g & h \end{pmatrix}$ due matrici a determinante uguale ad 1. Calcoliamo il determinante del loro prodotto:

$$\det\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right) = \det\left(\begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}\right) = (ae+bg)(cf+dh) - (ce+dg)(af+bh) =$$

$$= ad(eh-fg) - bc(eh-fg) = ad - bc = 1$$

Per quanto riguarda l'esistenza dell'inversa della matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ segue direttamente dalla formula riportata nel testo dell'esercizio e dal fatto che $\det(A) = 1$ che l'inversa è determinata dalla seguente:

$$A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Tale matrice ha lo stesso determinante di A ed è a coefficienti interi. Pertanto $A^{-1} \in \mathrm{SL}_2(\mathbb{Z})$. L'associatività è già stata verificata per tutte le matrici in $\mathfrak{M}_{2,2}(\mathbb{Z})$. Questo conclude la verifica del fatto che $\mathrm{SL}_2(\mathbb{Z})$ è un gruppo.

Vogliamo fornire una condizione necessaria e sufficiente per una matrice in $\mathrm{SL}_2(\mathbb{Z})$ affinché essa commuti con tutte le altre matrici di tale insieme. Osserviamo che se $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ commuta con tutti gli elementi di $\mathrm{SL}_2(\mathbb{Z})$ essa in particolare dovrà commutare con gli elementi $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ e con l'elemento $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Dalla prima relazione segue:

$$\begin{pmatrix} -b & a \\ -d & c \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ -a & -b \end{pmatrix}$$

Deve quindi risultare $a = d$ e $b = -c$. D'altra parte la seconda condizione ci dice che

$$\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$$

dalla quale segue $c = 0$. Ora, considerato che

$$1 = \det(A) = \det\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \det\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right) = a^2$$

e che $a \in \mathbb{Z}$ ne segue che $a = \pm 1$ e dunque che $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; tale condizione oltre ad essere necessaria è anche sufficiente (verificare).

Per quanto riguarda il punto (F), calcoliamo le prime potenze dell'elemento $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$:

$$J^2 = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \; ; \quad J^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \; ; \quad J^4 = \left[\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2\right]^2 = \left[-\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right]^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Abbiamo quindi scoperto che il gruppo delle potenze della matrice J è un gruppo il cui ordine è 4. Esso infatti è costituito dagli elementi $\{Id, J, J^2, J^3\}$.

Per quanto riguarda il punto (G) l'osservazione da fare è molto semplice: si consideri una matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Dato che tale matrice ha determinante 1, ed essendo i coefficienti di A tutti diversi da 0, l'equazione $1 = \det(A) = ad - bc$ costituisce una Identità di Bézout per la coppia (a, b) (oppure (a, c), (d, b), (d, c)). Ma se esiste una coppia di numeri non nulli tali che $ar + bs = 1$ sappiamo dalla teoria che $\mathrm{MCD}(a, b) = 1$. Quindi possiamo concludere.

Il punto (H) dell'esercizio si risolve anch'esso con un semplice calcolo del determinante:

$$\det\left(\begin{pmatrix} a & b \\ c+ka & d+kb \end{pmatrix}\right) = a(d+kb) - b(c+ka) = ad - bc + kab - kab = ad - bc = \det\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = 1$$