

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

Nota preliminare. *Nell'esercizio S.1.5. non vi è alcuna ragione per restringersi ai campi finiti \mathbb{F}_q con q primo. Esiste un campo finito per ogni numero naturale $q \in \mathbb{N}$, tuttavia questo vi è ignoto al momento e dunque è sembrata cosa naturale restringersi al caso dei campi finiti di vostra conoscenza ovvero $\mathbb{F}_q = \mathbb{Z}_q$ con q numero primo.*

Esercizio S.1. 1. Siano G e G' due gruppi finiti. Sia $\varphi : G \rightarrow G'$ un omomorfismo suriettivo e sia $H' < G'$. Dimostrare che:

$$[G' : H'] = [G : \varphi^{-1}(H')]$$

[Suggerimento. Mostrare che $\varphi^{-1}(H')$ è un sottogruppo di G . Ragionare sulle preimmagini tramite φ delle classi laterali di G modulo H']

Soluzione. Cominciamo osservando che $\varphi^{-1}(H')$ è un sottogruppo di G , infatti se $h_1, h_2 \in \varphi^{-1}(H')$ allora $\varphi(h_1 h_2) = \varphi(h_1) \varphi(h_2) \in H'$ poiché H' è un sottogruppo e $\varphi(h_1), \varphi(h_2) \in H'$.

Vogliamo ora mostrare che le preimmagini tramite φ delle classi laterali sinistre di G' modulo H' sono esattamente le classi laterali sinistre di G modulo $\varphi^{-1}(H')$. A tal scopo scegliamo un rappresentante g'_1, \dots, g'_m per ciascuna classe laterale sinistra di G' modulo H' . Siano g_1, \dots, g_m elementi di G tali che $\varphi(g_i) = g'_i$; tali elementi esistono perché stiamo assumendo che l'omomorfismo φ sia suriettivo.

Vogliamo vedere che $\{\varphi^{-1}(H')g_1, \dots, \varphi^{-1}(H')g_m\}$ è una partizione di G in classi laterali sinistre di G modulo $\varphi^{-1}(H')$.

Verifichiamo che se $i \neq j$ allora $\varphi^{-1}(H')g_i \cap \varphi^{-1}(H')g_j = \emptyset$. Osserviamo che

$$\varphi(\varphi^{-1}(H')g_j) \cap \varphi(\varphi^{-1}(H')g_i) = H'g'_j \cap H'g'_i = \emptyset$$

e pertanto $\varphi^{-1}(H')g_i \cap \varphi^{-1}(H')g_j = \emptyset$ perché contenuti nelle rispettive preimmagini di due sottoinsiemi disgiunti di G' .

Supponiamo ora che esista $g \in G$ che non appartiene ad alcun $\varphi^{-1}(H')g_i$. Essendo $\{H'g'_i\}_{i=1}^m$ una partizione di G' deve accadere necessariamente $\varphi(g) \in H'g'_j$ per un opportuno indice j . Non ci resta che osservare che $\varphi^{-1}(H'g'_j) = \varphi^{-1}(H')g_j$. L'inclusione \supseteq è banale. L'altra inclusione invece può essere ottenuta come segue: supponiamo che $g \in \varphi^{-1}(H'g'_j)$ in particolare $\varphi(gg_j^{-1}) = h'g'_j \cdot (g'_j)^{-1} = h' \in H'$ e dunque $gg_j^{-1} \in \varphi^{-1}(H')$, ovvero $g \in \varphi^{-1}(H')g_j$. \square

Esercizio S.1.2. Sia S_n il gruppo simmetrico su n elementi (ovvero l'insieme delle applicazioni biettive da $\{1, \dots, n\}$ in sé). Sia $\text{Stab}_{S_n}(1) = \{\gamma \in S_n \mid \gamma(1) = 1\}$.

(A) Mostrare che $\text{Stab}_{S_n}(1)$ è un sottogruppo di S_n .

(B) Mostrare che $[S_n : \text{Stab}_{S_n}(1)] = n$. [Suggerimento. Stabilire un isomorfismo tra S_{n-1} e $\text{Stab}_{S_n}(1)$]

Soluzione. Rispondiamo al punto (A). Supponiamo che $\gamma, \gamma_1, \gamma_2 \in \text{Stab}_{S_n}(1)$; vogliamo far vedere che $\gamma^{-1} \in \text{Stab}_{S_n}(1)$ e che $\gamma_1 \cdot \gamma_2 \in \text{Stab}_{S_n}(1)$.

Supponiamo che $\gamma^{-1}(1) = j \neq 1$ allora si avrebbe $(\gamma^{-1} \cdot \gamma)(1) = \gamma^{-1}(\gamma(1)) = \gamma^{-1}(1) = j \neq 1$ ma questo è assurdo perché $\gamma^{-1} \cdot \gamma = 1_{S_n}$ che agisce sull'insieme $\{1, \dots, n\}$ come l'identità.

Osserviamo infine che $(\gamma_1 \cdot \gamma_2)(1) = \gamma_1(\gamma_2(1)) = \gamma_1(1) = 1$ e dunque $\gamma_1 \cdot \gamma_2 \in \text{Stab}_{S_n}(1)$.

Rispondiamo ora al punto (B). Osserviamo che esiste un omomorfismo iniettivo da S_{n-1} in S_n la cui immagine è $\text{Stab}_{S_n}(1)$. Scriviamo tale omomorfismo esplicitandone il valore sul generico k -ciclo di S_{n-1} :

$$\varphi : S_{n-1} \rightarrow S_n, \quad (i_1 \cdots i_k) \mapsto (i_1 + 1 \cdots i_k + 1)$$

Chiamiamo φ questo omomorfismo (ovvero lo shift di 1). Bisogna dimostrare che si tratta di un omomorfismo iniettivo la cui immagine è $\text{Stab}_{S_n}(1)$. L'injectività segue dall'injectività sui cicli, che è di facile verifica. Consideriamo ora $\gamma \in \text{Stab}_{S_n}(1)$, scriviamo $\gamma = \sigma_1^\gamma \cdots \sigma_\ell^\gamma$ come prodotto di cicli disgiunti. Nessuno di tali cicli contiene 1, altrimenti non potrebbe essere $\gamma(1) = 1$ (infatti 1 sarebbe contenuto in un unico ciclo e dunque verrebbe inviato in un numero differente) e dunque è ben definito l'unico elemento di S_{n-1} che viene inviato da φ in γ : se $\sigma_j^\gamma = (i_{j,1}^\gamma \cdots i_{j,m_j}^\gamma)$ allora

$$(i_{1,1}^\gamma - 1 \cdots i_{1,m_1}^\gamma - 1) \cdots (i_{\ell,1}^\gamma - 1 \cdots i_{\ell,m_\ell}^\gamma - 1) \in S_{n-1}$$

e $\varphi((i_{1,1}^\gamma - 1 \cdots i_{1,m_1}^\gamma - 1) \cdots (i_{\ell,1}^\gamma - 1 \cdots i_{\ell,m_\ell}^\gamma - 1)) = \gamma$.

Per mostrare che è un omomorfismo ci basta osservare che se $f : \{1, \dots, n-1\} \rightarrow \{2, \dots, n\} \subset \{1, \dots, n\}$ con $f(\{1, \dots, n-1\}) = \{2, \dots, n\}$, $f(i)=i+1$, allora $\varphi(\gamma) = f \circ \gamma \circ f^{-1}$. La condizione di omomorfismo allora è banalmente verificata dato che $\varphi(\gamma_1 \gamma_2) = f \circ (\gamma_1 \cdot \gamma_2) \circ f^{-1} = (f \circ \gamma_1 \circ f^{-1}) \cdot (f \circ \gamma_2 \circ f^{-1}) = \varphi(\gamma_1) \cdot \varphi(\gamma_2)$. \square

Esercizio S.1. 3. Sia H un sottogruppo di S_n con la seguente proprietà: per ogni coppia $(i, j) \in \{1, \dots, n\}^2$ esiste $\gamma \in H$ tale che $\gamma(i) = j$. Sia $\text{Stab}_H(1) = \{\gamma \in H \mid \gamma(1) = 1\}$.

(A) Mostrare che $\text{Stab}_H(1)$ di un sottogruppo di H .

(B) Mostrare che $[H : \text{Stab}_H(1)] = n$. [Suggerimento. Utilizzare la proprietà verificata da H per caratterizzare i laterali di $\text{Stab}_H(1)$.]

Soluzione. Cominciamo rispondendo al punto (A). Ci viene chiesto di dimostrare che il sottoinsieme $\text{Stab}_H(1) = \{\gamma \in H \mid \gamma(1) = 1\}$ è un sottogruppo di H . Osserviamo che se $\gamma_1, \gamma_2 \in \text{Stab}_H(1)$ allora risulta: $\gamma_1, \gamma_2 \in H$ e dunque $\gamma_1 \cdot \gamma_2 \in H$ ed inoltre $(\gamma_1 \cdot \gamma_2)(1) = \gamma_1(\gamma_2(1)) = \gamma_1(1) = 1$; pertanto $\gamma_1 \cdot \gamma_2 \in \text{Stab}_H(1)$. Supponiamo ora che $\gamma \in \text{Stab}_H(1)$, mostriamo che $\gamma^{-1} \in \text{Stab}_H(1)$. Innanzitutto essendo H un sottogruppo ed essendo $\gamma \in H$ deve risultare $\gamma^{-1} \in H$. D'altra parte supponiamo che $\gamma^{-1}(1) = j \neq 1$, allora avremmo $j = (\gamma^{-1} \circ \gamma)(1) = 1_{S_n}(1) = 1$, che è assurdo e dunque deve risultare $\gamma^{-1}(1) = 1$ e $\gamma^{-1} \in \text{Stab}_H(1)$.

Passiamo alla dimostrazione del punto (B). Ricordiamo che H è tale che per ogni coppia (i, j) esiste $h \in H$ tale che $\gamma(i) = j$. Scriviamo le classi laterali di H modulo $\text{Stab}_H(1)$.

Siano esse $\text{Stab}_H(1)\gamma_1, \dots, \text{Stab}_H(1)\gamma_m$.

Osserviamo che tutti gli elementi di una classe laterale di H modulo $\text{Stab}_H(1)$ devono mandare 1 nello stesso elemento. Viceversa supponiamo che γ' sia tale che $\gamma'(1) = \gamma_j(1)$, allora $(\gamma' \cdot \gamma_j^{-1})(1) = 1$ e dunque $\gamma' \in \text{Stab}_H(1)$. Risulta quindi che $m = n$ (osserviamo che questo discende dalla proprietà verificata da H : da essa infatti segue per ogni coppia $(1, j)$ esiste un elemento γ_j tale che $\gamma_j(1) = j$) e supporremo quindi di aver numerato i $\{\gamma_i\}$ in modo tale che ciascun γ_j sia tale che $\gamma_j(1) = j$. Abbiamo quindi che $H = \text{Stab}_H(1) \cup \text{Stab}_H(1)\gamma_2 \cdots \text{Stab}_H(1)\gamma_n$. Tali classi laterali sono a due a due disgiunte per definizione e coprono tutto H (infatti se $\gamma \in H < S_n$ deve risultare $\gamma(1) = j$ per un opportuno j e dunque $\gamma \in \text{Stab}_H(1)\gamma_j$). Abbiamo quindi $[H : \text{Stab}_H(1)] = n$. \square

Esercizio S.1. 4. Sia X un insieme finito, denotiamo con $S(X)$ l'insieme delle mappe biettive da X in X (ovvero l'insieme delle permutazioni sugli elementi di X). Sia $\varphi : G \rightarrow S(X)$ un omomorfismo e supponiamo che $\text{Im}(\varphi)$ sia tale che per ogni coppia $(x, y) \in X \times X$ esista $\sigma \in \text{Im}(\varphi)$ tale che $\sigma(x) = y$. Sia $x_0 \in X$ fissato. Dimostrare che $[G : \varphi^{-1}(\text{Stab}_{\text{Im}(\varphi)}(x_0))] = |X|$.

Soluzione. Sia $|X| = n$. Possiamo identificare $S(X)$ con S_n ; in tal caso la proprietà richiesta su $H = \text{Im}(\varphi) < S_n$ è che per ogni coppia $(i, j) \in \{1, \dots, n\}^2$ esista $\gamma \in H = \text{Im}(\varphi)$ tale che $\gamma(i) = j$. Nell'identificazione scelta tra X e $\{1, \dots, n\}$ possiamo supporre di avere $x_0 \leftrightarrow 1$. La tesi allora diventa dimostrare che $[G : \varphi^{-1}(\text{Stab}_H(1))] = n$. Ma noi sappiamo che, vista la proprietà soddisfatta da H risulta $[H : \text{Stab}_H(1)] = n$ mentre grazie all'esercizio S.1.1. considerando $\varphi : G \rightarrow \text{Im}(\varphi)$ abbiamo che:

$$[G : \varphi^{-1}(\text{Stab}_H(1))] = [H : \text{Stab}_H(1)] = n$$

che è ciò che volevamo dimostrare. \square

Richiami e notazioni. Ricordiamo che, in generale, l'anello degli interi modulo n , $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$ è un anello commutativo unitario. Dalla teoria sappiamo che \mathbb{Z}_n è un campo se e soltanto se n è un numero primo. Denoteremo il campo finito di cardinalità prima q con \mathbb{F}_q invece di \mathbb{Z}_q , per coerenza con l'usuale notazione per i campi finiti. Denoteremo infine con \mathbb{F}_q^* il gruppo moltiplicativo del campo finito \mathbb{F}_q (ovvero gli invertibili di \mathbb{Z}_q).

Esercizio S.1.5. Sia $q \in \mathbb{N}$ un numero primo. Sia \mathbb{F}_q il campo finito di ordine q .

(A) Verificare che $\mathbb{F}_q \times \mathbb{F}_q$ è un \mathbb{F}_q -spazio vettoriale rispetto alla somma coordinata per coordinata e al prodotto per scalari in \mathbb{F}_q .

(B) Determinare per elencazione l'insieme $\mathcal{R}_{\mathbb{F}_q \times \mathbb{F}_q}$ delle rette¹ in $\mathbb{F}_q \times \mathbb{F}_q$.

(C) Sia $GL_2(\mathbb{F}_q)$ il gruppo delle trasformazioni lineari invertibili da $\mathbb{F}_q \times \mathbb{F}_q$ in sé (in altre parole $GL_2(\mathbb{F}_q)$ è il gruppo delle matrici 2×2 a coefficienti in \mathbb{F}_q e determinante diverso da $\bar{0}$). Verificare che

la formula per determinare l'inversa della matrice $\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$ è la seguente:

$$\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}^{-1} = \det \left(\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \right)^{-1} \cdot \begin{pmatrix} \bar{d} & -\bar{b} \\ -\bar{c} & \bar{a} \end{pmatrix}$$

(D) Mostrare che

$$SL_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \mid \bar{a}\bar{d} - \bar{b}\bar{c} = \bar{1}, \bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{F}_q \right\}$$

è un sottogruppo normale di $GL_2(\mathbb{F}_q)$.

(E) Mostrare che $\det : GL_2(\mathbb{F}_q) \rightarrow \mathbb{F}_q^*$ è un omomorfismo di gruppi il cui nucleo coincide con $SL_2(\mathbb{F}_q)$.

(F) Mostrare che il seguente sottoinsieme di $SL_2(\mathbb{F}_q)$ è un sottogruppo:

$$B = \left\{ \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{0} & \bar{a}^{-1} \end{pmatrix} \mid \bar{b} \in \mathbb{F}_q, \bar{a} \in \mathbb{F}_q^* \right\}$$

(G) Sia $\varphi : SL_2(\mathbb{F}_q) \rightarrow S(\mathcal{R}_{\mathbb{F}_q \times \mathbb{F}_q})$ definita da $\varphi : A \mapsto \sigma_A$ dove $\sigma_A : \mathcal{R}_{\mathbb{F}_q \times \mathbb{F}_q} \rightarrow \mathcal{R}_{\mathbb{F}_q \times \mathbb{F}_q}$ è data da $r \mapsto A \cdot r$. Mostrare che si tratta di un omomorfismo. Osservare che $Im(\varphi)$ ha la proprietà che per ogni coppia $(r_1, r_2) \in \mathcal{R}_{\mathbb{F}_q \times \mathbb{F}_q}^2$ esiste $\sigma \in Im(\varphi)$ tale che $\sigma(r_1) = r_2$.

(H) Mostrare che $B = \varphi^{-1}(\text{Stab}_{Im(\varphi)}(\mathbb{F}_q \cdot (\bar{1}, \bar{0})))$. Dedurre che $[SL_2(\mathbb{F}_q) : B] = q + 1$ e che $|SL_2(\mathbb{F}_q)| = q(q^2 - 1)$. [Suggerimento. Sfruttare l'esercizio S.1.4]

Soluzione punto (A). Per verificare che $\mathbb{F}_q \times \mathbb{F}_q$ è uno spazio vettoriale sul campo \mathbb{F}_q bisogna verificare che esso è un gruppo additivo rispetto alla somma coordinata per coordinata, e che è ben definita la moltiplicazione per scalari in \mathbb{F}_q , la quale deve essere distributiva rispetto alla somma. Che $\mathbb{F}_q \times \mathbb{F}_q$ sia un gruppo additivo rispetto alla somma coordinata per coordinata segue dal fatto che è il prodotto diretto di due copie del gruppo additivo \mathbb{F}_q degli interi modulo q . Possiamo quindi risparmiarci le verifiche delle varie proprietà. Osserviamo solamente che l'elemento neutro è dato dall'elemento $(\bar{0}, \bar{0})$. Per quanto riguarda la moltiplicazione per scalare essa è definita come segue:

$$\mathbb{F}_q \times (\mathbb{F}_q \times \mathbb{F}_q) \rightarrow \mathbb{F}_q \times \mathbb{F}_q, \quad (\bar{k}, (\bar{k}_1, \bar{k}_2)) \mapsto (\bar{k} \cdot \bar{k}_1, \bar{k} \cdot \bar{k}_2)$$

Data tale definizione è chiaro che tale moltiplicazione possiede un elemento neutro, ovvero $\bar{1} \in \mathbb{F}_q$, così come è chiaro che verifica le proprietà di distributività:

$$\begin{aligned} \bar{k} \cdot [(\bar{k}_1, \bar{k}_2) + (\bar{h}_1, \bar{h}_2)] &= \bar{k} \cdot (\bar{k}_1, \bar{k}_2) + \bar{k} \cdot (\bar{h}_1, \bar{h}_2) \\ (\bar{k}_1 + \bar{k}_2) \cdot (\bar{h}_1, \bar{h}_2) &= \bar{k}_1 \cdot (\bar{h}_1, \bar{h}_2) + \bar{k}_2 \cdot (\bar{h}_1, \bar{h}_2) \end{aligned}$$

che vengono entrambe ereditate dalla distributività della moltiplicazione rispetto alla somma in \mathbb{F}_q . \square

Soluzione punto (B). Gli \mathbb{F}_q -sottospazi vettoriali di dimensione 1 in $\mathbb{F}_q \times \mathbb{F}_q$ possono essere facilmente determinati nel modo seguente: innanzitutto ciascuno di essi deve necessariamente contenere $(\bar{0}, \bar{0})$ dato che $\bar{0} \cdot (\bar{k}_1, \bar{k}_2) = (\bar{0}, \bar{0})$, e dunque $(\bar{0}, \bar{0}) \in \mathbb{F}_q \cdot (\bar{k}_1, \bar{k}_2)$. Consideriamo quindi gli \mathbb{F}_q -sottospazi di dimensione 1 passanti per $(\bar{1}, \bar{k})$ al variare di $\bar{k} \in \mathcal{F}_q$ e quello passante per $(\bar{0}, \bar{1})$; mostriamo che

¹L'insieme degli \mathbb{F}_q -sottospazi vettoriali di dimensione 1.

tali rette si intersecano esclusivamente nell'origine e che ciascun punto di $\mathbb{F}_q \times \mathbb{F}_q$ è contenuto in almeno una di queste rette. Partiamo dalla seconda affermazione: consideriamo $(\bar{k}_1, \bar{k}_2) \in \mathbb{F}_q \times \mathbb{F}_q$; possiamo supporre che $(\bar{k}_1, \bar{k}_2) \neq (\bar{0}, \bar{0})$, e dunque almeno una delle due coordinate è diversa da $\bar{0}$. Supponiamo ad esempio che $\bar{k}_1 \neq \bar{0}$, allora \bar{k}_1 è invertibile; sia \bar{k}_1^{-1} l'inverso di \bar{k}_1 in \mathbb{F}_q , ne segue che $\mathbb{F}_q \cdot (\bar{k}_1, \bar{k}_2) = \mathbb{F}_q \cdot (\bar{1}, \bar{k}_1^{-1}\bar{k}_2)$. Se invece $\bar{k}_1 = \bar{0}$ ne segue che $\mathbb{F}_q \cdot (\bar{k}_1, \bar{k}_2) = \mathbb{F}_q \cdot (\bar{0}, \bar{k}_2) = \mathbb{F}_q \cdot (\bar{0}, \bar{1})$.

Dimostriamo ora la prima affermazione: supponiamo che $(\bar{k}_1, \bar{k}_2) \in \mathbb{F}_q \cdot (\bar{1}, \bar{k}) \cap \mathbb{F}_q \cdot (\bar{1}, \bar{h})$ con $\bar{k} \neq \bar{h}$. Osserviamo preliminarmente che $(\bar{1}, \bar{h}) \notin \mathbb{F}_q \cdot (\bar{1}, \bar{k})$, infatti $(\bar{1}, \bar{k})$ è l'unico elemento in $\mathbb{F}_q \cdot (\bar{1}, \bar{k})$ ad avere $\bar{1}$ in prima coordinata. Poiché $\bar{h} \neq \bar{k}$ almeno uno dei due deve essere diverso da $\bar{0}$, supponiamo sia \bar{h} . Ne segue che (\bar{k}_1, \bar{k}_2) ha entrambe le coordinate diverse da $\bar{0}$ o entrambe uguali a $\bar{0}$ (perché $\bar{0} \in \mathbb{F}_q$ e perché in \mathbb{F}_q non ci sono divisori di $\bar{0}$ non banali). Supponiamo per assurdo di essere nel primo caso; osserviamo che $(\bar{k}_1, \bar{k}_2) = \bar{k}_1 \cdot (\bar{1}, \bar{k}_1^{-1}\bar{k}_2)$ dunque $(\bar{k}_1, \bar{k}_2) \in \mathbb{F}_q \cdot (\bar{1}, \bar{k})$ o $(\bar{k}_1, \bar{k}_2) \in \mathbb{F}_q \cdot (\bar{1}, \bar{h})$ a seconda che $\bar{k}_1^{-1}\bar{k}_2$ sia uguale a \bar{k} o \bar{h} , ma questo è assurdo poiché avevamo supposto che appartenesse ad entrambe le rette. Deve pertanto valere $(\bar{k}_1, \bar{k}_2) = (\bar{0}, \bar{0})$. Per dimostrare che $\mathbb{F}_q \cdot (\bar{0}, \bar{1}) \cap \mathbb{F}_q \cdot (\bar{1}, \bar{k}) = \{(\bar{0}, \bar{0})\}$ si procede in modo del tutto analogo.

Osserviamo quindi che l'insieme delle rette $\mathcal{R}_{\mathbb{F}_q \times \mathbb{F}_q}$ è un insieme di cardinalità $q + 1$:

$$\mathcal{R}_{\mathbb{F}_q \times \mathbb{F}_q} = \{\mathbb{F}_q \cdot (\bar{1}, \bar{0}), \dots, \mathbb{F}_q \cdot (\bar{1}, q - \bar{1}), \mathbb{F}_q \cdot (\bar{0}, \bar{1})\}$$

Soluzione punto (C). Verifichiamo la formula:

$$\begin{aligned} \det \left(\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \right)^{-1} \cdot \begin{pmatrix} \bar{d} & -\bar{b} \\ -\bar{c} & \bar{a} \end{pmatrix} \cdot \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} &= (\bar{a}\bar{d} - \bar{b}\bar{c})^{-1} \cdot \begin{pmatrix} \bar{a}\bar{d} - \bar{b}\bar{c} & \bar{0} \\ \bar{0} & \bar{a}\bar{d} - \bar{b}\bar{c} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} \\ \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \cdot \det \left(\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \right)^{-1} \cdot \begin{pmatrix} \bar{d} & -\bar{b} \\ -\bar{c} & \bar{a} \end{pmatrix} &= (\bar{a}\bar{d} - \bar{b}\bar{c})^{-1} \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \cdot \begin{pmatrix} \bar{d} & -\bar{b} \\ -\bar{c} & \bar{a} \end{pmatrix} = \\ &= (\bar{a}\bar{d} - \bar{b}\bar{c})^{-1} \cdot \begin{pmatrix} \bar{a}\bar{d} - \bar{b}\bar{c} & \bar{0} \\ \bar{0} & \bar{a}\bar{d} - \bar{b}\bar{c} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} \end{aligned}$$

dove gli inversi delle espressioni $(\bar{a}\bar{d} - \bar{b}\bar{c})$ sono naturalmente da intendersi in \mathbb{F}_q .

Soluzione punto (D). Osserviamo che, grazie al punto (C) sappiamo che se $A \in \text{SL}_2(\mathbb{F}_q)$ allora $A^{-1} \in \text{SL}_2(\mathbb{F}_q)$. Per quanto riguarda il prodotto di due matrici $A_1, A_2 \in \text{SL}_2(\mathbb{F}_q)$ osserviamo che:

$$A_1 \cdot A_2 = \begin{pmatrix} \bar{a}_1 & \bar{b}_1 \\ \bar{c}_1 & \bar{d}_1 \end{pmatrix} \cdot \begin{pmatrix} \bar{a}_2 & \bar{b}_2 \\ \bar{c}_2 & \bar{d}_2 \end{pmatrix} = \begin{pmatrix} \bar{a}_1\bar{a}_2 + \bar{b}_1\bar{c}_2 & \bar{a}_1\bar{b}_2 + \bar{b}_1\bar{d}_2 \\ \bar{c}_1\bar{a}_2 + \bar{d}_1\bar{c}_2 & \bar{c}_1\bar{b}_2 + \bar{d}_1\bar{d}_2 \end{pmatrix}$$

e dunque:

$$\begin{aligned} (\dagger) \quad \det(A_1 \cdot A_2) &= (\bar{a}_1\bar{a}_2 + \bar{b}_1\bar{c}_2) \cdot (\bar{c}_1\bar{b}_2 + \bar{d}_1\bar{d}_2) - (\bar{a}_1\bar{b}_2 + \bar{b}_1\bar{d}_2) \cdot (\bar{c}_1\bar{a}_2 + \bar{d}_1\bar{c}_2) = \\ &= (\bar{a}_1\bar{d}_1 - \bar{b}_1\bar{c}_1) \cdot (\bar{a}_2\bar{d}_2 - \bar{b}_2\bar{c}_2) = \bar{1} \end{aligned}$$

dove i raggruppamenti sono da fare in analogia con quanto fatto per $\text{SL}_2(\mathbb{Z})$ in un foglio precedente. Siccome $\text{Id}_{\text{GL}_2(\mathbb{F}_q)}$ ha chiaramente determinante $\bar{1}$ possiamo concludere che $\text{SL}_2(\mathbb{F}_q)$ è un sottogruppo di $\text{GL}_2(\mathbb{F}_q)$ (per la proprietà associativa si osservi che essa è valida perché l'operazione in $\text{SL}_2(\mathbb{F}_q)$ è restrizione di una operazione associativa).

Dobbiamo dimostrare che tale sottogruppo è un sottogruppo normale. Si osservi che il calcolo fatto in (\dagger) fino alla penultima uguaglianza è valido per $A_1, A_2 \in \text{GL}_2(\mathbb{F}_q)$, dunque vale $\det(A_1 \cdot A_2) = \det(A_1) \cdot \det(A_2)$. Dunque per ogni elemento $A \in \text{GL}_2(\mathbb{F}_q)$ ed ogni $B \in \text{SL}_2(\mathbb{F}_q)$ vale

$$\det(A \cdot B \cdot A^{-1}) = \det(A) \cdot \det(B) \cdot \det(A^{-1})$$

Osserviamo che $\bar{1} = \det(\text{Id}_{\text{GL}_2(\mathbb{F}_q)}) \det(A \cdot A^{-1}) = \det(A) \cdot \det(A^{-1})$ e dunque:

$$\det(A \cdot B \cdot A^{-1}) = \det(B) = \bar{1}$$

ne segue che $A \cdot B \cdot A^{-1} \in \text{SL}_2(\mathbb{F}_q)$. Quindi $\text{SL}_2(\mathbb{F}_q)$ è normale in $\text{GL}_2(\mathbb{F}_q)$. \square

Soluzione punto (E). Questo punto dell'esercizio è pressoché risolto: \det è infatti una applicazione da $\text{GL}_2(\mathbb{F}_q)$ in \mathbb{F}_q^* (infatti le matrici di $\text{GL}_2(\mathbb{F}_q)$ hanno determinante diverso da $\bar{0}$).

Se consideriamo \mathbb{F}_q^* come gruppo moltiplicativo, la condizione $\det(A \cdot B) = \det(A) \cdot \det(B)$ ci dice precisamente che

$$\det : GL_2(\mathbb{F}_q) \rightarrow \mathbb{F}_q^*$$

è un omomorfismo di gruppi. In particolare $SL_2(\mathbb{F}_q) = \{A \in GL_2(\mathbb{F}_q) \mid \det(A) = \bar{1}\} = \ker(\det)$. \square

Soluzione punto (F). Verifichiamo che B è un sottogruppo di $SL_2(\mathbb{F}_q)$. Innanzitutto osserviamo che $\text{Id}_{GL_2(\mathbb{F}_q)} = \text{Id}_{SL_2(\mathbb{F}_q)}$ appartiene all'insieme B (si prenda $\bar{a} = \bar{1} \in \mathbb{F}_q^*$ e $\bar{b} = \bar{0} \in \mathbb{F}_q$). Verifichiamo che la moltiplicazione di elementi in B è ancora in B :

$$\begin{pmatrix} \bar{a}_1 & \bar{b}_1 \\ \bar{0} & \bar{a}_1^{-1} \end{pmatrix} \cdot \begin{pmatrix} \bar{a}_2 & \bar{b}_2 \\ \bar{0} & \bar{a}_2^{-1} \end{pmatrix} = \begin{pmatrix} \bar{a}_1\bar{a}_2 & \bar{a}_1\bar{b}_2 + \bar{a}_2^{-1}\bar{b}_1 \\ \bar{0} & (\bar{a}_1\bar{a}_2)^{-1} \end{pmatrix} \in B$$

Osserviamo infine che l'inversa di un elemento $\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{0} & \bar{a}^{-1} \end{pmatrix}$ è ancora in B , grazie alla formula dimostrata nel punto (C) (verificate). \square

Soluzione punto (G). Osserviamo innanzitutto che essendo gli elementi di $SL_2(\mathbb{F}_q)$ matrici esse sono \mathbb{F}_q -lineari; consideriamo $A, B \in SL_2(\mathbb{F}_q)$, mostriamo che $\sigma_{A \cdot B} = \sigma_A \circ \sigma_B$. A tal scopo è sufficiente osservare che per sapere dove viene inviata una retta da una trasformazione $A \in SL_2(\mathbb{F}_q)$ è sufficiente sapere dove viene mandato un vettore non nullo appartenente a tale retta (per linearità). Osservato questo fatto la proprietà precedente è di banale verifica: basta osservare che su ogni spazio vettoriale V e per ogni coppia di trasformazioni lineari A, B , vale $(A \cdot B) \cdot v = A \cdot (B \cdot v)$. Inoltre osserviamo che $\text{Id}_{SL_2(\mathbb{F}_q)} \cdot (\bar{k}, \bar{h}) = (\bar{k}, \bar{h})$ e dunque fissa ogni retta in $\mathcal{R}_{\mathbb{F}_q \times \mathbb{F}_q}$, pertanto $\sigma_{\text{Id}_{SL_2(\mathbb{F}_q)}} = \text{id}_{S(\mathcal{R}_{\mathbb{F}_q \times \mathbb{F}_q})}$.

Questo dimostra che $\varphi : SL_2(\mathbb{F}_q) \rightarrow S(\mathcal{R}_{\mathbb{F}_q \times \mathbb{F}_q})$ è un omomorfismo di gruppi.

Per mostrare che $\text{Im}(\varphi)$ ha la proprietà richiesta nel punto (G) osserviamo che se $\bar{k} \neq \bar{0}$ e $\bar{h} \in \mathbb{F}_q$ allora

$$\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{h} - \bar{k} & \bar{1} \end{pmatrix} \cdot (\bar{1}, \bar{k}) = (\bar{1}, \bar{h})$$

Infine osserviamo che

$$\begin{pmatrix} \bar{0} & \bar{1} \\ \bar{q} - \bar{1} & \bar{0} \end{pmatrix} \cdot (\bar{0}, \bar{1}) = (\bar{1}, \bar{0})$$

e questo conclude la dimostrazione del fatto che $\text{Im}(\varphi)$ agisce in modo transitivo sulle rette. \square

Soluzione punto (H). Supponiamo che $A \in \varphi^{-1}(\text{Stab}_{\text{Im}(\varphi)}(\mathbb{F}_q \cdot (\bar{1}, \bar{0})))$; questo significa che $A \cdot (\bar{1}, \bar{0}) = (\bar{a}, \bar{0})$, dunque significa che A^1 , la prima colonna di A è il vettore $(\bar{a}, \bar{0})$. Poiché il determinante di $A \in SL_2(\mathbb{F}_q)$ è uguale ad $\bar{1}$ ne segue che A^2 deve avere la forma (\bar{b}, \bar{a}^{-1}) e dunque $A \in B$. Viceversa supponiamo che $A \in B$ allora $A \in \varphi^{-1}(\text{Stab}_{\text{Im}(\varphi)}(\mathbb{F}_q \cdot (\bar{1}, \bar{0})))$ come si verifica facilmente applicando a $(\bar{1}, \bar{0})$ la matrice A .

A questo punto si osservi che $[\text{Im}(\varphi) : \text{Stab}_{\text{Im}(\varphi)}(\mathbb{F}_q \cdot (\bar{1}, \bar{0}))] = |\mathcal{R}_{\mathbb{F}_q \times \mathbb{F}_q}|$. D'altra parte, per quanto dimostrato nell'esercizio S. 1. 4., ne segue che $[SL_2(\mathbb{F}_q) : B] = q + 1$. D'altra parte le matrici in B sono $q \cdot (q - 1)$ (dipendono infatti dai due parametri \bar{a} e \bar{b} , il primo che varia in \mathbb{F}_q^* mentre il secondo in \mathbb{F}_q), ne deduciamo quindi che la cardinalità di $SL_2(\mathbb{F}_q)$ è: $|SL_2(\mathbb{F}_q)| = |B| \cdot [SL_2(\mathbb{F}_q) : B] = q \cdot (q - 1) \cdot (q + 1) = q \cdot (q^2 - 1)$.² \square

²Notare che a questo punto, sfruttando il punto (E) è automatico il calcolo della cardinalità di $GL_2(\mathbb{F}_q)$:

$$|GL_2(\mathbb{F}_q)| = (q^2 - q) \cdot (q^2 - 1)$$