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 $\varphi : G \to G'$ 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 $g'_1, ...g'_m$ per ciascuna classe laterale sinistra di G' modulo H'. Siano $g_1, ..., g_m$ 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 $\{\varphi^{-1}(H')g_1, .., \varphi^{-1}(H')g_m\}$ è una partizione di G in classi laterali sinistre di G modulo $\varphi^{-1}(H')$.
Verifichiamo che se $i \neq j$ allora $\varphi^{-1}(H')\, g_i \cap \varphi^{-1}(H')\, g_j = \varnothing$. Osserviamo che

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

e pertanto $\varphi^{-1}(H')\, g_i \cap \varphi^{-1}(H')\, g_j = \varnothing$ 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 $\varphi(g\, g_j^{-1}) = h'\, g'_j \cdot (g'_j)^{-1} = h' \in H'$ e dunque $g\, g_j^{-1} \in \varphi^{-1}(H')$, 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 $\mathrm{Stab}_{S_n}(1) = \{\gamma \in S_n \mid \gamma(1) = 1\}$.
(A) Mostrare che $\mathrm{Stab}_{S_n}(1)$ è un sottogruppo di S_n.
(B) Mostrare che $[S_n : \mathrm{Stab}_{S_n}(1)] = n$. [*Suggerimento. Stabilire un isomorfismo tra* S_{n-1} *e* $\mathrm{Stab}_{S_n}(1)$]

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

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 $\{1, .., n\}$ come l'identità.

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

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

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

Chiamiamo φ questo omomorfismo (ovverlo lo shift di 1). Bisogna dimostrare che si tratta di un omomorfismo iniettivo la cui immagine è $\mathrm{Stab}_{S_n}(1)$. L'iniettività segue dall'iniettività sui cicli, che è di facile verifica. Consideriamo ora $\gamma \in \mathrm{Stab}_{S_n}(1)$, 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 $f : \{1, .., n-1\} \to \{2, ...n\} \subset \{1, .., n\}$ con $f(\{1, .., n-1\}) = \{2, ..., n\}$, $f(i)$=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 $\mathrm{Stab}_H(1) = \{\gamma \in H \mid \gamma(1) = 1\}$.
(A) Mostrare che $\mathrm{Stab}_H(1)$ di un sottogruppo di H.
(B) Mostrare che $[H : \mathrm{Stab}_H(1)] = n$. [*Suggerimento. Utilizzare la proprietà verificata da H per caratterizzare i laterali di* $\mathrm{Stab}_H(1)$.]

Soluzione. Cominciamo rispondendo al punto (A). Ci viene chiesto di dimostrare che il sottoinsieme $\mathrm{Stab}_H(1) = \{\gamma \in H \mid \gamma(1) = 1\}$ è un sottogruppo di H. Osserviamo che se $\gamma_1, \gamma_2 \in \mathrm{Stab}_H(1)$ 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 $\gamma_1 \cdot \gamma_2 \in \mathrm{Stab}_H(1)$. Supponiamo ora che $\gamma \in \mathrm{Stab}_H(1)$, mostriamo che $\gamma^{-1} \in \mathrm{Stab}_H(1)$. 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 $\gamma^{-1} \in \mathrm{Stab}_H(1)$.
Passiamo alla dismotrazione 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 $\mathrm{Stab}_H(1)$.
Siano esse $\mathrm{Stab}_H(1)\, \gamma_1, \dots \mathrm{Stab}_H(1)\, \gamma_m$.
Osserviamo che tutti gli elementi di una classe laterale di H modulo $\mathrm{Stab}_H(1)$ 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 $\gamma' \in \mathrm{Stab}_H(1)$. 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 $H = \mathrm{Stab}_H(1) \cup \mathrm{Stab}_H(1)\gamma_2 \cdots \mathrm{Stab}_H(1)\gamma_n$. 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 $\gamma \in \mathrm{Stab}_H(1)\, \gamma_j$). Abbiamo quindi $[H : \mathrm{Stab}_H(1)] = n$. $\square$

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 $\varphi : G \to S(X)$ un omomorfismo e supponiamo che $Im(\varphi)$ sia tale che per ogni coppia $(x, y) \in X \times X$ esista $\sigma \in Im(\varphi)$ tale che $\sigma(x) = y$. Sia $x_0 \in X$ fissato. Dimostrare che $[G : \varphi^{-1}(\mathrm{Stab}_{Im(\varphi)}(x_0))] = |\, X\, |$.

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

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

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 rette[1] 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 $\overline{0}$). Verificare che la formula per determinare l'inversa della matrice $\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$ è la seguente:

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

(D) Mostrare che

$$\mathrm{SL}_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \;\middle|\; \overline{a}\overline{d} - \overline{b}\overline{c} = \overline{1},\ \overline{a}, \overline{b}, \overline{c}, \overline{d} \in \mathbb{F}_q \right\}$$

è un sottogruppo normale di $GL_2(\mathbb{F}_q)$.
(E) Mostrare che $\det : GL_2(\mathbb{F}_q) \to \mathbb{F}_q^*$ è un omomorfismo di gruppi il cui nucleo coincide con $\mathrm{SL}_2(\mathbb{F}_q)$.
(F) Mostrare che il seguente sottoinsieme di $\mathrm{SL}_2(\mathbb{F}_q)$ è un sottogruppo:

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

(G) Sia $\varphi : \mathrm{SL}_2(\mathbb{F}_q) \to S(\mathcal{R}_{\mathbb{F}_q\times\mathbb{F}_q})$ definita da $\varphi : A \mapsto \sigma_A$ dove $\sigma_A : \mathcal{R}_{\mathbb{F}_q\times\mathbb{F}_q} \to \mathcal{R}_{\mathbb{F}_q\times\mathbb{F}_q}$ 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 $(r_1, r_2) \in \mathcal{R}^2_{\mathbb{F}_q\times\mathbb{F}_q}$ esiste $\sigma \in Im(\varphi)$ tale che $\sigma(r_1) = r_2$.
(H) Mostrare che $B = \varphi^{-1}\left(\mathrm{Stab}_{Im(\varphi)}(\mathbb{F}_q \cdot (\overline{1}, \overline{0}))\right)$. Dedurne che $[\mathrm{SL}_2(\mathbb{F}_q) : B] = q + 1$ e che $|\,\mathrm{SL}_2(\mathbb{F}_q)\,| = q\,(q^2 - 1)$. [*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 lélemento neutro è dato dall'elemento $(\overline{0}, \overline{0})$. Per quanto riguarda la moltiplicazione per scalare essa è definita come segue:

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

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

$$\overline{k} \cdot [(\overline{k}_1, \overline{k}_2) + (\overline{h}_1, \overline{h}_2)] = \overline{k} \cdot (\overline{k}_1, \overline{k}_2) + \overline{k}(\overline{h}_1, \overline{h}_2)$$
$$(\overline{k}_1 + \overline{k}_2) \cdot (\overline{h}_1, \overline{h}_2) = \overline{k}_1 \cdot (\overline{h}_1, \overline{h}_2) + \overline{k}_2(\overline{h}_1, \overline{h}_2)$$

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

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 $(\overline{0}, \overline{0})$ dato che $\overline{0} \cdot (\overline{k}_1, \overline{k}_2) = (\overline{0}, \overline{0})$, e dunque $(\overline{0}, \overline{0}) \in \mathbb{F}_q \cdot (\overline{k}_1, \overline{k}_2)$. Consideriamo quindi gli $\mathbb{F}_q$-sottospazi di dimensione 1 passanti per $(\overline{1}, \overline{k})$ al variare di $\overline{k} \in \mathcal{F}_q$ e quello passante per $(\overline{0}, \overline{1})$; mostriamo che

[1] L'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 $(\overline{k}_1, \overline{k}_2) \in \mathbb{F}_q \times \mathbb{F}_q$; possiamo supporre che $(\overline{k}_1, \overline{k}_2) \neq (\overline{0}, \overline{0})$, e dunque almeno una delle due coordinate è diversa da $\overline{0}$. Supponiamo ad esempio che $\overline{k}_1 \neq \overline{0}$, allora $\overline{k}_1$ è invertibile; sia $\overline{k}_1^{-1}$ l'inverso di $\overline{k}_1$ in $\mathbb{F}_q$, ne segue che $\mathbb{F}_q \cdot (\overline{k}_1, \overline{k}_2) = \mathbb{F}_q \cdot (\overline{1}, \overline{k}_1^{-1}\overline{k}_2)$. Se invece $\overline{k}_1 = \overline{0}$ ne segue che $\mathbb{F}_q \cdot (\overline{k}_1, \overline{k}_2) = \mathbb{F}_q \cdot (\overline{0}, \overline{k}_2) = \mathbb{F}_q \cdot (\overline{0}, \overline{1})$.
Dimostriamo ora la prima affermazione: supponiamo che $(\overline{k}_1, \overline{k}_2) \in \mathbb{F}_q \cdot (\overline{1}, \overline{k}) \cap \mathbb{F}_q \cdot (\overline{1}, \overline{h})$ con $\overline{k} \neq \overline{h}$. Osserviamo preliminarmente che $(\overline{1}, \overline{h}) \notin \mathbb{F}_q \cdot (\overline{1}, \overline{k})$, infatti $(\overline{1}, \overline{k})$ è l'unico elemento in $\mathbb{F}_q \cdot (\overline{1}, \overline{k})$ ad avere $\overline{1}$ in prima coordinata. Poiché $\overline{h} \neq \overline{k}$ almeno uno dei due deve essere diverso da $\overline{0}$, supponiamo sia $\overline{h}$. Ne segue che $(\overline{k}_1, \overline{k}_2)$ ha entrambe le coordinate diverse da $\overline{0}$ o entrambe uguali a $\overline{0}$ (perché $\overline{0} \in \mathbb{F}_q$ e perché in $\mathbb{F}_q$ non ci sono divisori di $\overline{0}$ non banali). Supponiamo per assurdo di essere nel primo caso; osserviamo che $(\overline{k}_1, \overline{k}_2) = \overline{k}_1 \cdot (\overline{1}, \overline{k}_1^{-1}\overline{k}_2)$ dunque $(\overline{k}_1, \overline{k}_2) \in \mathbb{F}_q \cdot (\overline{1}, \overline{k})$ o $(\overline{k}_1, \overline{k}_2) \in \mathbb{F}_q \cdot (\overline{1}, \overline{h})$ a seconda che $\overline{k}_1^{-1}\overline{k}_2$ sia uguale a $\overline{k}$ o $\overline{h}$, ma questo è assurdo poiché avevamo supposto che appartenesse ad entrambe le rette. Deve pertanto valere $(\overline{k}_1, \overline{k}_2) = (\overline{0}, \overline{0})$. Per dimostrare che $\mathbb{F}_q \cdot (\overline{0}, \overline{1}) \cap \mathbb{F}_q \cdot (\overline{1}, \overline{k}) = \{(\overline{0}, \overline{0})\}$ 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 $q+1$:

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

Soluzione punto (C). Verifichiamo la formula:

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

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

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

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

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

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

e dunque:

$$(\dagger) \qquad \det(A_1 \cdot A_2) = (\overline{a}_1\overline{a}_2 + \overline{b}_1\overline{c}_2) \cdot (\overline{c}_1\overline{b}_2 + \overline{d}_1\overline{d}_2) - (\overline{a}_1\overline{b}_2 + \overline{b}_1\overline{d}_2) \cdot (\overline{c}_1\overline{a}_2 + \overline{d}_1\overline{c}_2) =$$

$$= (\overline{a}_1\overline{d}_1 - \overline{b}_1\overline{c}_1) \cdot (\overline{a}_2\overline{d}_2 - \overline{b}_2\overline{c}_2) = \overline{1}$$

dove i raggruppamenti sono da fare in analogia con quanto fatto per $\mathrm{SL}_2(\mathbb{Z})$ in un foglio precedente. Siccome $\mathrm{Id}_{GL_2(\mathbb{F}_q)}$ ha chiaramente determinante $\overline{1}$ possiamo concludere che $\mathrm{SL}_2(\mathbb{F}_q)$ è un sottogruppo di $GL_2(\mathbb{F}_q)$ (per la proprietà associativa si osservi che essa è valida perché l'operazione in $\mathrm{SL}_2(\mathbb{F}_q)$ 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 $A_1, A_2 \in GL_2(\mathbb{F}_q)$, dunque vale $\det(A_1 \cdot A_2) = \det(A_1) \cdot \det(A_2)$. Dunque per ogni elemento $A \in GL_2(\mathbb{F}_q)$ ed ogni $B \in \mathrm{SL}_2(\mathbb{F}_q)$ vale

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

Osserviamo che $\overline{1} = \det(\mathrm{Id}_{GL_2(\mathbb{F}_q)}) \det(A \cdot A^{-1}) = \det(A) \cdot \det(A^{-1}$ e dunque:

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

ne segue che $A \cdot B \cdot A^{-1} \in \mathrm{SL}_2(\mathbb{F}_q)$. Quindi $\mathrm{SL}_2(\mathbb{F}_q)$ è normale in $GL_2(\mathbb{F}_q)$. $\square$

Soluzione punto (E). Questo punto dell'esercizio è pressoché risolto: det è infatti una applicazione da $GL_2(\mathbb{F}_q)$ in $\mathbb{F}_q^*$ (infatti le matrici di $GL_2(\mathbb{F}_q)$ hanno determinante diverso da $\overline{0}$).

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

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

è un omomorfismo di gruppi. In particolare $\mathrm{SL}_2(\mathbb{F}_q) = \{A \in GL_2(\mathbb{F}_q) \mid \det(A) = \overline{1}\} = \ker(\det)$. $\square$

Soluzione punto (F). Verifichiamo che B è un sottogruppo di $\mathrm{SL}_2(\mathbb{F}_q)$. Innanzitutto osserviamo che $\mathrm{Id}_{GL_2(\mathbb{F}_q)} = \mathrm{Id}_{\mathrm{SL}_2(\mathbb{F}_q)}$ appartiene all'insieme B (si prenda $\overline{a} = \overline{1} \in \mathbb{F}_q^*$ e $\overline{b} = \overline{0} \in \mathbb{F}_q$). Verifichiamo che la moltiplicazione di elementi in B è ancora in B:

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

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

Soluzione punto (G). Osserviamo innanzitutto che essendo gli elementi di $\mathrm{SL}_2(\mathbb{F}_q)$ matrici esse sono $\mathbb{F}_q$-lineari; consideriamo $A, B \in \mathrm{SL}_2(\mathbb{F}_q)$, 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 $A \in \mathrm{SL}_2(\mathbb{F}_q)$ 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 $\mathrm{Id}_{\mathrm{SL}_2(\mathbb{F}_q)} \cdot (\overline{k}, \overline{h}) = (\overline{k}, \overline{h})$ e dunque fissa ogni retta in $\mathcal{R}_{\mathbb{F}_q \times \mathbb{F}_q}$, pertanto $\sigma_{\mathrm{Id}_{\mathrm{SL}_2(\mathbb{F}_q)}} = \mathrm{id}_{S(\mathcal{R}_{\mathbb{F}_q \times \mathbb{F}_q})}$.
Questo dimostra che $\varphi : \mathrm{SL}_2(\mathbb{F}_q) \to S(\mathcal{R}_{\mathbb{F}_q \times \mathbb{F}_q})$ è un omomorfismo di gruppi.
Per mostrare che $Im(\varphi)$ ha la proprietà richiesta nel punto (G) osserviamo che se $\overline{k} \neq \overline{0}$ e $\overline{h} \in \mathbb{F}_q$ allora

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

Infine osserviamo che

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

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

Soluzione punto (H). Supponiamo che $A \in \varphi^{-1}(\mathrm{Stab}_{Im(\varphi)}(\mathbb{F}_q \cdot (\overline{1}, \overline{0})))$; questo significa che $A \cdot (\overline{1}, \overline{0}) = (\overline{a}, \overline{0})$, dunque significa che A^1, la prima colonna di A è il vettore $(\overline{a}, \overline{0})$. Poiché il determinante di $A \in \mathrm{SL}_2(\mathbb{F}_q)$ è uguale ad $\overline{1}$ ne segue che A^2 deve avere la forma $(\overline{b}, \overline{a}^{-1})$ e dunque $A \in B$. Viceversa supponiamo che $A \in B$ allora $A \in \varphi^{-1}(\mathrm{Stab}_{Im(\varphi)}(\mathbb{F}_q \cdot (\overline{1}, \overline{0})))$ come si verifica facilmente applicando a $(\overline{1}, \overline{0})$ la matrice A.
A questo punto si osservi che $[Im(\varphi) : \mathrm{Stab}_{Im(\varphi)}(\mathbb{F}_q \cdot (\overline{1}, \overline{0})) = |\mathcal{R}_{\mathbb{F}_q \times \mathbb{F}_q}|$. D'altra parte, per quanto dimostrato nell'esercizio S. 1. 4., ne segue che $[\mathrm{SL}_2(\mathbb{F}_q) : B] = q+1$. D'altra parte le matrici in B sono $q \cdot (q-1)$ (dipendono infatti dai due parametri $\overline{a}$ e $\overline{b}$, il primo che varia in $\mathbb{F}_q^*$ mentre il secondo in $\mathbb{F}_q$), ne deduciamo quindi che la cardinalità di $\mathrm{SL}_2(\mathbb{F}_q)$ è: $|\mathrm{SL}_2(\mathbb{F}_q)| = |B| \cdot [\mathrm{SL}_2(\mathbb{F}_q) : B] = q \cdot (q-1) \cdot (q+1) = q \cdot (q^2 - 1)$.[2] $\square$

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

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