ESERCIZI SU

GRUPPI E SOTTOGRUPPI

N.B.: il simbolo ☡ contrassegna gli esercizi (relativamente) più complessi.

— ∗ —

1 — Sia G un gruppo, per il quale usiamo la notazione moltiplicativa. Dimostrare che:

(a) l'elemento neutro di G è unico;

(b) per ogni $g \in G$, l'inverso g^{-1} di g in G è unico;

(c) per ogni $g \in G$ si ha $\left(g^{-1}\right)^{-1} = g$;

(d) per ogni $x, y \in G$ si ha $\left(x\,y\right)^{-1} = y^{-1}\,x^{-1}$;

(e) *(condizioni di commutatività)* per ogni $x, y \in G$ si ha
$x\,y = y\,x \iff (x\,y)^2 = x^2\,y^2$ e $x\,y = y\,x \iff \left(x\,y\right)^{-1} = x^{-1}\,y^{-1}$

(f) *(assenza di idempotenti non banali)* se $\gamma \in G$ è tale che $\gamma^2 = \gamma$, allora $\gamma = 1_G$.

2 — Sia G un gruppo, e sia $H \in \mathcal{P}(G) \setminus \{\emptyset\}$ un sottoinsieme non vuoto di G che sia *chiuso per l'operazione in* G, cioè $HH := \left\{ h'h'' \,\middle|\, h', h'' \in H \right\} \subseteq H$ e sia *finito*.

Dimostrare che H è un sottogruppo di G.

<u>Suggerimento:</u> *Si utilizzi il Teorema di Cayley applicato al gruppo G e si valuti l'"effetto" su H delle applicazioni $\lambda_g : G \longrightarrow G \left(x \mapsto \lambda_g(x) := g\,x \right)$ in esso considerate...*

Il risultato segue anche come conseguenza dell'esercizio 4 qui sotto, per $S := H$.

3 ☡ — Sia M un monoide *finito* che sia anche *cancellativo* (a sinistra e a destra), cioè

$$\forall\ a, b, c \in G\,, \quad a\,b = a\,c \implies b = c\,, \quad \text{e} \quad b\,a = c\,a \implies b = c \quad .$$

Dimostrare che M è un gruppo.

<u>Suggerimento:</u> *Si utilizzi il Teorema di Cayley applicato al monoide M , e in particolare le applicazioni $\lambda_m : M \longrightarrow M \left(x \mapsto \lambda_m(x) := m\,x \right)$ in esso considerate. L'ipotesi che M sia cancellativo comporta che tali applicazioni siano [...]; ma siccome M è anche finito, da questo deriva che esse sono anche [...]. Quindi...*

4 ☡ — Sia S un semigruppo *finito* non vuoto che sia anche *cancellativo* (a sinistra e a destra). Dimostrare che S è un gruppo.

<u>Suggerimento:</u> *Riducendosi all'esercizio 3 qui sopra, è sufficiente dimostrare che S è un monoide, dunque che ha un elemento neutro. A tal fine, si utilizzi il Teorema di Cayley per il semigruppo S, e in particolare le applicazioni* $\lambda_s : S \longrightarrow S \ \big(x \mapsto \lambda_s(x) := m\,x \big)$ *in esso considerate. Siccome S è cancellativo, tali applicazioni sono iniettive, e poiché S è anche finito, da questo deriva che esse sono anche suriettive. Quindi...*

5 — Sia S un monoide *finito* non vuoto che sia anche *cancellativo a sinistra* oppure *cancellativo a destra*. Dimostrare che S è un gruppo.

<u>Suggerimento:</u> *Si utilizzi ancora il Teorema di Cayley per il semigruppo S, e in particolare le applicazioni* $\lambda_s : S \longrightarrow S \ \big(x \mapsto \lambda_s(x) := m\,x \big)$ *in esso considerate, come per gli esercizi precedenti.*

6 — Sia $\big(G\,;\,\cdot\,\big)$ un semigruppo. Supponiamo che esista $u \in G$ tale che $g\,u = g$ per ogni $g \in G$ (cioè u è un "elemento neutro a destra") e per ogni $g \in G$ esista $g' \in G$ tale che $g\,g' = u$ (cioè g^{-1} è un "inverso a destra" di g^{-1}).

Dimostrare che allora $\big(G\,;\,\cdot\,\big)$ è un gruppo.

7 — Sia $\big(G\,;\cdot\big)$ un insieme *finito non vuoto* con un'operazione associativa tale che

$$\forall\ a, b \in G\,,\ \ \exists\ c_d, c_s \in G\ :\ a \cdot c_d = b\,,\ \ c_s \cdot a = b$$

(cioè le "equazioni lineari" sono risolvibili). Dimostrare che $\big(G\,;\,\cdot\,\big)$ è un gruppo.

8 — Dato un insieme E, per ogni sottoinsieme $F \subseteq E$ definiamo

$$G_F := \big\{\, \sigma \in \mathcal{S}(E) \,\big|\, \sigma(F) = F \,\big\} \quad , \qquad G_{(F)} := \big\{\, \nu \in \mathcal{S}(E) \,\big|\, \nu(f) = f\,,\ \ \forall\, f \in F \,\big\}$$

Dimostrare le seguenti proprietà di tali sottoinsiemi:

(a) $G_{(F)} = \bigcap\limits_{f \in F} G_{\{f\}} \subseteq G_F$;

(b) $G_{(F)} = G_F \iff \big|F\big| = 1$;

(c) $G_{E \setminus F} = G_F$;

(d) $G_{(A \cup B)} = G_{(A)} \cap G_{(B)}$, per ogni $A, B \subseteq E$;

(e) $G_{(A)} \subseteq G_{(B)} \iff A \supseteq B$, per ogni $A, B \subseteq E$;

(f) G_F è sottogruppo di $\mathcal{S}(E)$;

(g) $G_{(F)}$ è sottogruppo di $\mathcal{S}(E)$;

(h) $G_{(F)}$ è sottogruppo *normale* di G_F ;

(i) se $\big|E \setminus F\big| > 1$, allora $G_{(F)}$ *non* è *normale* come sottogruppo di $\mathcal{S}(E)$.

Suggerimento: *Tutto segue dalle definizioni e da calcoli elementari. In aggiunta, la parte (g) si può ottenere come conseguenza della parte (f) applicata ai vari* $G_{\{f\}}$ *(per ogni* $f \in F$ *) e della parte (a). Per la parte (i), ci si può ridurre al caso in cui* $\big|E\big| = 3$ *,* $\big|F\big| = 1$ *e* $\big|E \setminus F\big| = 2$ *, e in questo caso trovare un* $\nu \in G_{(F)}$ *e un* $\sigma \in \mathcal{S}(E)$ *tali che* $\sigma \circ \nu \circ \sigma^{-1} \notin G_{(F)}$ *.*

9 — Dato un insieme E e un suo sottoinsieme $F \subseteq E$, siano

$$G_F := \big\{\, \sigma \in \mathcal{S}(E) \,\big|\, \sigma(F) = F \,\big\} \quad , \qquad G_{(F)} := \big\{\, \nu \in \mathcal{S}(E) \,\big|\, \nu(f) = f \,,\ \forall\, f \in F \,\big\}$$

come nell'esercizio 8 qui sopra. Supponiamo inoltre che $\big|E\big| = n$ e $\big|F\big| = k$.

Dimostrare che:

(a) $\big|\, G_F \big| \;=\; k\,!\,(n-k)!$;

(b) $\big|\, G_{(F)} \big| \;=\; (n-k)!$.

10 — Dato un insieme E e una relazione (binaria) ρ in E si definisca

$$\mathcal{S}(E)_{[\rho]} \;:=\; \big\{\, \sigma \in \mathcal{S}(E) \,\big|\, e' \rho\, e'' \Longleftrightarrow \sigma\big(e'\big)\, \rho\, \sigma\big(e''\big) \,,\ \forall\, e', e'' \in E \,\big\}$$

Dimostrare che:

(a) $\mathcal{S}(E)_{[\rho]}$ è un sottogruppo di $\big(\mathcal{S}(E)\,;\,\circ\big)$;

(b) con la notazione dell'Esercizio 8 qui sopra, considerato che $\rho \in \mathcal{P}(E \times E)$, si ha

$$\mathcal{S}(E)_{[\rho]} \;=\; \Big\{\, \sigma \in \mathcal{S}(E) \,\Big|\, (\sigma \times \sigma) \in \mathcal{S}(E \times E)_{\rho} \,\Big\}$$

dove $(\sigma \times \sigma) : E \times E \longrightarrow E \times E$ è la funzione definita da $(\sigma \times \sigma)\big(e', e''\big) := \big(\sigma\big(e'\big), \sigma\big(e''\big)\big)$.

Suggerimento: *La parte (a) si può dimostrare direttamente (per verifica diretta), oppure come conseguenza immediata della parte (b), la quale è una mera rilettura delle definizioni.*

11 — Sia $\mathbb{A} \in \big\{\, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \,\big\} \cup \big\{\, \mathbb{Z}_n \,\big\}_{n \in \mathbb{N}}$, o più in generale sia $\mathbb{A}$ un qualsiasi anello commutativo unitario. Si consideri $\mathbb{P}_{\mathbb{A}} := \mathbb{A} \cup \{\infty\}$ e sia

$$\mathcal{G}_{\mathbb{P}_{\mathbb{A}}} \;:=\; \left\{\, f \in \mathbb{P}_{\mathbb{A}}^{\mathbb{P}_{\mathbb{A}}} \;\middle|\; \exists\, a, b, c, d \in \mathbb{A} : ad - bc \in U\big(\mathbb{A}\,;\,\cdot\big) \,,\ f(x) = \frac{ax+b}{cx+d} \ \forall\, x \in \mathbb{P}_{\mathbb{A}} \,\right\} .$$

Verificare che $\mathbb{P}_{\mathbb{A}}$ è sottogruppo del gruppo $\big(\mathcal{S}\big(\mathbb{P}_{\mathbb{A}}\big)\,;\,\circ\big)$ di tutte le permutazioni di $\mathbb{P}_{\mathbb{A}}$.

12 — Dati due insiemi X e Y, ed un'applicazione $h \in Y^X$, cioè $h : X \longrightarrow Y$, sia $G_h := \big\{\, f \in \mathcal{S}(X) \,\big|\, h \circ f = h \,\big\}$. Dimostrare che G_h è un sottogruppo di $\big(\mathcal{S}(X)\,;\,\circ\big)$.

13 — Siano X, Y e Z tre insiemi, e siano $h \in Y^X$, $k \in Z^Y$. Con la notazione dell'esercizio 9 qui sopra, dimostrare che

(a) $G_h \subseteq G_{k \circ h}$;

(b) se h è suriettiva, allora $G_{k \circ h} = G_h$ se e soltanto se k è iniettiva.

14 — Sia E un insieme, sia $F \subseteq E$, e sia $\chi_F : E \longrightarrow \{0,1\}$ la funzione caratteristica di F. Con la notazione degli esercizi 9 e 5 qui sopra, dimostrare che $G_{\chi_F} = G_F$.

15 — Per un qualsiasi gruppo G, definiamo i sottoinsiemi

$$Z(G) := \{ z \in G \mid z\,g = g\,z\,,\ \forall\, g \in G \} \qquad (=: \text{“centro di } G\text{”})$$

$$C_G(g) := \{ x \in G \mid x\,g = g\,x \} \qquad (=: \text{“centralizzante di } g\text{”}) \qquad \forall\ g \in G$$

Dimostrare che:

(a) $Z(G) = \bigcap_{g \in G} C_G(g)$;

(b) $Z(G) = \{ g \in G \mid C_G(g) = G \}$;

(c) $Z(G) \leq G$;

(d) $C_G(g) \leq G$ per ogni $g \in G$.

<u>Suggerimento:</u> *Tutto segue direttamente dalle definizioni. Inoltre, la parte (c) si può ottenere anche come conseguenza immediata delle parti (d) e (a) insieme.*

16 — Per un qualsiasi gruppo G, consideriamo gli elementi $(g,h) := g\,h\,g^{-1}\,h^{-1}$ — per ogni $g,h \in G$ — e il sottogruppo da essi generato in G, cioè

$$G' := \Big\langle \{ (g,h) := g\,h\,g^{-1}\,h^{-1} \mid g,h \in G \} \Big\rangle \qquad (=: \text{“sottogruppo derivato” di } G)$$

Dimostrare che:

(a) $G' \trianglelefteq G$;

(b) G è abeliano $\iff G' = \{1_G\}$.

17 — Sia H un sottogruppo di un gruppo G. Dimostrare che l'unica classe laterale sinistra (o destra) di H in G che sia un sottogruppo è H stesso.

18 — Sia G un gruppo, e siano $x, y \in G$ tali che $xy = yx$ e $\langle x \rangle \cap \langle y \rangle = \{1\}$, dove $\langle x \rangle$ e $\langle y \rangle$ indicano rispettivamente il sottogruppo di G generato da x e da y. Verificare che l'ordine di xy è il minimo comune multiplo degli ordini di x e di y.

19 — Sia G un gruppo ciclico con m elementi, e siano H e K due sottogruppi di G di ordine rispettivamente h e k. Determinare l'ordine del sottogruppo $H \cap K$.

20 — Per ogni $n \in \mathbb{N}_+$, dimostrare che il gruppo $\mathcal{C}_n := \{ z \in \mathbb{C} \mid z^n = 1 \}$ è un sottogruppo di $(\mathbb{C} \setminus \{0\}\,;\,\cdot)$, e che (come gruppo) è ciclico di ordine n.

21 — Determinare tutti i sottogruppi di $\mathbb{Z}_6$, e la decomposizione di $\mathbb{Z}_6$ in classi laterali rispetto a ciascuno di essi.

22 — Usando la notazione $\mathcal{S}_n := \mathcal{S}\big(\{1,2,\dots,n\}\big)$ — per ogni $n \in \mathbb{N}_+$ — determinare tutti i sottogruppi di $\mathcal{S}_3$, e la decomposizione di $\mathcal{S}_3$ in classi laterali destre o in classi laterali sinistre rispetto a ciascuno di essi.

23 — Usando la notazione $\mathcal{S}_n := \mathcal{S}\big(\{1,2,\dots,n\}\big)$ — per ogni $n \in \mathbb{N}_+$ — determinare quali dei sottogruppi di $\mathcal{S}_3$ e di $\mathcal{S}_4$ siano ciclici.

24 — Siano $g = \big(1\,5\,2\,6\big)\big(3\,4\,7\big)$ e $h = \big(1\,5\big)\big(2\,3\,7\,6\big)$ due elementi del gruppo simmetrico $\mathcal{S}_7$ (cioè permutazioni di 7 elementi). Calcolare la permutazione $h \circ g^{-1}$.

25 — Siano $\alpha = \big(2\,3\big)$ e $\beta = \big(1\,3\big)\big(2\,4\,5\big)$ due elementi del gruppo simmetrico $\mathcal{S}_5$. Calcolare esplicitamente le quattro permutazioni $\alpha \circ \beta$, $\beta \circ \alpha$, α^{-1} e β^{-1}.

26 — Siano $\alpha = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 5&3&4&2&1 \end{smallmatrix}\right)$ e $\beta = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 4&1&3&5&2 \end{smallmatrix}\right)$ e $\gamma = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 1&3&2&5&4 \end{smallmatrix}\right)$ tre elementi del gruppo simmetrico $\mathcal{S}_5$. Calcolare esplicitamente le tre permutazioni $(\gamma \circ \beta) \circ \alpha$, $\alpha^2 \circ \gamma$ e $\gamma \circ \alpha^{-1}$.

27 — Siano $\alpha = \left(\begin{smallmatrix} 1&2&3&4 \\ 2&3&4&1 \end{smallmatrix}\right)$ e $\beta = \left(\begin{smallmatrix} 1&2&3&4 \\ 1&3&2&4 \end{smallmatrix}\right)$ due elementi del gruppo simmetrico $\mathcal{S}_4$. Determinare l'ordine di α, di β, di $\alpha \circ \beta$, di $\beta \circ \alpha$ e di $\alpha^3 \circ \beta \circ \alpha$.

28 — Siano $\alpha = (1\,3\,2\,5)$, $\beta = (1\,3)(4\,5)$ e $\gamma = (2\,3)(4\,5)$ tre elementi del gruppo simmetrico $\mathcal{S}_5$. Determinare l'ordine di α, di α^3, di β, di $\gamma \circ \alpha$, di $\alpha \circ \beta \circ \gamma$ e di $\beta \circ \gamma \circ \beta \circ \alpha$.

29 — Sia $\mathbb{A} \in \big\{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\big\} \cup \big\{\mathbb{Z}_n\big\}_{n \in \mathbb{N}_+}$, oppure (più in generale) sia $\mathbb{A}$ un qualsiasi *anello*. Dati $h, k \in \mathbb{N}_+$, sia

$$Mat_{h\times k}(\mathbb{A}) := \left\{ (a_{i,j})_{i=1,\dots,h;}^{j=1,\dots,k;} \,\middle|\, a_{i,j} \in \mathbb{A}\ \forall\, i,j \right\}$$

l'insieme delle matrici $h \times k$ a coefficienti in $\mathbb{A}$. Per tale insieme consideriamo le operazioni "$\oplus$" e "$\odot$" definite da

$$\big(a'_{i,j}\big)_{i,j} \oplus \big(a''_{i,j}\big)_{i,j} := \big(a'_{i,j} + a''_{i,j}\big)_{i,j} \quad , \qquad \big(a'_{i,j}\big)_{i,j} \odot \big(a''_{i,j}\big)_{i,j} := \big(a'_{i,j} \cdot a''_{i,j}\big)_{i,j}$$

Inoltre, nel caso di $h = k =: n$ (cioè per matrici quadrate di taglia n) si consideri anche l'operazione di "prodotto righe per colonne" — indicato con "$\bullet$" — definito da

$$\big(a'_{i,j}\big)_{i,j} \bullet \big(a''_{i,j}\big)_{i,j} := \big(\textstyle\sum_{\ell=1}^{n} a'_{i,\ell} \cdot a''_{\ell,j}\big)_{i,j}$$

Dimostrare che:

(a) il gruppoide $\big(Mat_{h\times k}(\mathbb{A})\,;\,\oplus\big)$ è un gruppo abeliano;

(b) il gruppoide $\big(Mat_{h\times k}(\mathbb{A})\,;\,\odot \big)$ è un semigruppo abeliano, ed è un monoide se l'anello $\mathbb{A}$ è unitario — come nel caso $\mathbb{A} \in \big\{ \mathbb{N}\,,\mathbb{Z}\,,\mathbb{Q}\,,\mathbb{R}\,,\mathbb{C} \big\} \cup \big\{ \mathbb{Z}_n \big\}_{n\in\mathbb{N}_+}$ — ma *non* è un gruppo se $\mathbb{A} \neq \{0\}$ — come nel caso $\mathbb{A} \in \big\{ \mathbb{N}\,,\mathbb{Z}\,,\mathbb{Q}\,,\mathbb{R}\,,\mathbb{C} \big\} \cup \big\{ \mathbb{Z}_n \big\}_{n\in\mathbb{N}_+}$;

(c) il gruppoide $\big(Mat_{n\times n}(\mathbb{A})\,;\,\bullet \big)$ è un semigruppo, ed è un monoide se l'anello $\mathbb{A}$ è unitario — come nel caso $\mathbb{A} \in \big\{ \mathbb{N}\,,\mathbb{Z}\,,\mathbb{Q}\,,\mathbb{R}\,,\mathbb{C} \big\} \cup \big\{ \mathbb{Z}_n \big\}_{n\in\mathbb{N}_+}$ — ma *non* è un gruppo se $\mathbb{A} \neq \{0\}$, ed è commutativo se e soltanto se $\mathbb{A}\cdot\mathbb{A} = \{0\}$ oppure $n = 1$ e l'anello $\mathbb{A}$ è commutativo;

(d) quando l'anello $\mathbb{A}$ — come accade nel caso $\mathbb{A} \in \big\{ \mathbb{N}\,,\mathbb{Z}\,,\mathbb{Q}\,,\mathbb{R}\,,\mathbb{C} \big\} \cup \big\{ \mathbb{Z}_n \big\}_{n\in\mathbb{N}_+}$ — è unitario e commutativo, descrivere il gruppo $GL_n(\mathbb{A}) := U\big(Mat_{n\times n}(\mathbb{A})\,;\,\bullet \big)$ degli elementi invertibili nel monoide $\big(Mat_{n\times n}(\mathbb{A})\,;\,\bullet \big)$, cioè il gruppo delle matrici (quadrate) invertibili rispetto al prodotto righe per colonne.

<u>Suggerimento</u>: *Le parti (a), (b) e (c) sono verifiche dirette, elementari; per l'ultima parte dell'enunciato (c) basta trovare matrici* 2×2 *che non commutino tra loro (si cerchino matrici del genere fatte soltanto di qualche 1 e di qualche 0...). Per (d) occorre conoscere la formula esplicita per l'inversa di una matrice — rispetto al prodotto* $\bullet$ *— e osservare che essa richiede soltanto una certa condizione sul determinante della matrice data.*

30 — Sia $\mathbb{A} \in \big\{ \mathbb{Z}\,,\mathbb{Q}\,,\mathbb{R}\,,\mathbb{C} \big\} \cup \big\{ \mathbb{Z}_n \big\}_{n\in\mathbb{N}_+}$, oppure (più in generale) sia $\mathbb{A}$ un qualsiasi *anello unitario*. Dati $h,k \in \mathbb{N}_+$, siano $Mat_{n\times n}(\mathbb{A})$ il monoide delle matrici $n\times n$ a coefficienti in $\mathbb{A}$ (rispetto al prodotto righe per colonne) e $GL_n(\mathbb{A})$ il corrispondente gruppo delle matrici $n\times n$ invertibili, come nell'esercizio 29 qui sopra.

Si considerino i sottoinsiemi di matrici

$$d_n(\mathbb{A}) := \big\{ (m_{i,j})_{i=1,\dots,n;}^{j=1,\dots,n;} \in Mat_{n\times n}(\mathbb{A}) \;\big|\; m_{i,j} = 0\,,\ \forall\, i \neq j \big\}$$
$$t_n^+(\mathbb{A}) := \big\{ (m_{i,j})_{i=1,\dots,n;}^{j=1,\dots,n;} \in Mat_{n\times n}(\mathbb{A}) \;\big|\; m_{i,j} = 0\,,\ \forall\, i > j \big\}$$
$$t_n^-(\mathbb{A}) := \big\{ (m_{i,j})_{i=1,\dots,n;}^{j=1,\dots,n;} \in Mat_{n\times n}(\mathbb{A}) \;\big|\; m_{i,j} = 0\,,\ \forall\, i < j \big\}$$
$$D_n(\mathbb{A}) := d_n(\mathbb{A}) \cap GL_n(\mathbb{A}) \quad , \quad T_n^+(\mathbb{A}) := t_n^+(\mathbb{A}) \cap GL_n(\mathbb{A}) \quad , \quad T_n^-(\mathbb{A}) := t_n^-(\mathbb{A}) \cap GL_n(\mathbb{A})$$
$$U_n^+(\mathbb{A}) := \big\{ (u_{i,j})_{i=1,\dots,n;}^{j=1,\dots,n;} \in t_n^+(\mathbb{A}) \;\big|\; u_{k,k} = 1\,,\ \forall\, k \big\}$$
$$U_n^-(\mathbb{A}) := \big\{ (u_{i,j})_{i=1,\dots,n;}^{j=1,\dots,n;} \in t_n^-(\mathbb{A}) \;\big|\; u_{k,k} = 1\,,\ \forall\, k \big\}$$

Dimostrare che, rispetto al prodotto righe per colonne, si ha:

(a) $d_n(\mathbb{A})$, $t_n^+(\mathbb{A})$, $t_n^+(\mathbb{A})$ sono monoidi (dunque sono *sottomonoidi* di $Mat_{n\times n}(\mathbb{A})$);

(b) $D_n(\mathbb{A})$, $T_n^+(\mathbb{A})$, $T_n^-(\mathbb{A})$, $U_n^+(\mathbb{A})$, $U_n^-(\mathbb{A})$ sono sottogruppi di $GL_n(\mathbb{A})$.

<u>Suggerimento</u>: *La parte (a) si dimostra con verifica diretta. La (b) è analoga per quanto riguarda il fatto che i sottoinsiemi considerati siano chiusi rispetto al prodotto righe per colonne e contengano la matrice identità, mentre per verificare che contengano l'inverso di ogni loro elemento bisogna guardare la forma esplicita dell'inversa di una matrice.*

31 — Sia $GL_2(\mathbb{Z}_5)$ il gruppo generale lineare di ordine 2 a coefficienti in $\mathbb{Z}_5$.

(a) Determinare l'ordine del gruppo $GL_2(\mathbb{Z}_5)$;

(b) Determinare l'ordine dell'elemento $\begin{pmatrix} 2 & 0 \\ 4 & 3 \end{pmatrix}$ nel gruppo $GL_2(\mathbb{Z}_5)$.

32 — Sia $GL_n(\mathbb{Z}_p)$ il gruppo generale lineare di ordine p a coefficienti in $\mathbb{Z}_p$, con p primo. Determinare l'ordine del gruppo $GL_n(\mathbb{Z}_p)$.

Suggerimento: Consideriamo una matrice quadrata $p\times p$ a coefficienti in $\mathbb{Z}_p$ come fatta di p colonne, ciascuna scelta in $(\mathbb{Z}_p)^p$. La condizione perché tale matrice sia invertibile è che tali colonne siano tra loro linearmente indipendenti su $\mathbb{Z}_p$. Guardandole nell'ordine dalla prima all'ultima, questa condizione equivale a chiedere che:

— la prima colonna sia una qualunque $p-$pla in $(\mathbb{Z}_p)^p$, tranne l'unica fatta di tutti zeri (quindi il numero di possibilità è...);

— la seconda colonna sia una qualunque $p-$pla in $(\mathbb{Z}_p)^p$, escludendo tutti i possibili multipli (per uno scalare in $\mathbb{Z}_p$) della prima colonna (quindi il numero di possibilità è...);

— la terza colonna sia una qualunque $p-$pla in $(\mathbb{Z}_p)^p$, escludendo tutte le possibili combinazioni lineari (a coefficienti in $\mathbb{Z}_p$) delle prime due colonne (quindi il numero di possibilità è...);

— [...] in generale, per ogni $i = 2, \dots, p$ la $i-$esima colonna sia una qualunque $p-$pla in $(\mathbb{Z}_p)^p$, escludendo tutte le possibili combinazioni lineari (a coefficienti in $\mathbb{Z}_p$) delle prime $(i-1)$ colonne (quindi il numero di possibilità è...).

Questo ci dà il numero di scelte per tutte le colonne, e dunque l'ordine di $GL_n(\mathbb{Z}_p)$.

33 — Sia V uno spazio vettoriale su un campo $\mathbb{K}$ (arbitrario), e siano

$$End\,(V) := \big\{\text{trasformazioni } \mathbb{K}\text{–lineari di } V \text{ in sé stesso}\big\} \ , \quad Aut\,(V) := End\,(V) \bigcap \mathcal{S}(V)$$

Dimostrare che, rispetto al prodotto di composizione $\circ$, si ha:

(a) $\big(End\,(V)\,;\circ\big)$ è un monoide (dunque è un *sottomonoide* di $\big(V^V;\circ\big)$ ...);

(b) $\big(Aut\,(V)\,;\circ\big)$ è un sottogruppo di $\big(\mathcal{S}(V)\,;\circ\big)$.

Suggerimento: Si tratta di dimostrare che la composizione di trasformazioni lineari è lineare, che se una trasformazione lineare è invertibile, allora la sua inversa è lineare, ecc.

34 — Sia V uno spazio vettoriale (su un campo $\mathbb{K}$), e sia $\underline{B} : V_1 \subseteq V_2 \subseteq \cdots \subseteq V_k$ una catena di sottospazi vettoriali di V ciascuno incluso nel successivo (detta "bandiera" di sottospazi). Definiamo allora

$$End_{\underline{B}}(V) := \big\{\, \phi \in End_{\underline{B}}(V) \;\big|\; \phi(V_i) \subseteq V_i \,,\ \forall\, i = 1, \dots, k \,\big\}$$
$$Aut_{\underline{B}}(V) := End_{\underline{B}}(V) \bigcap Aut\,(V)$$

Dimostrare che:

(a) $Aut_{\underline{B}}(V) \;=\; End_{\underline{B}}(V) \bigcap \mathcal{S}(V)$;

(b) $Aut_{\underline{B}}(V) \;=\; End\,(V) \bigcap \Big(\bigcap_{i=1}^{k} \mathcal{S}_{V_i}(V) \Big)$, dove adottiamo la notazione $\mathcal{S}_{V_i}(V) := \big\{ \sigma \in \mathcal{S}(V) \;\big|\; \sigma(V_i) = V_i \big\}$ come nell'esercizio 8 qui sopra;

(c) $\big(End_{\underline{B}}(V)\,;\circ \big)$ è un monoide (che è *sottomonoide* di $\big(End\,(V);\circ \big)$ ...);

(d) $\big(Aut_{\underline{B}}(V)\,;\circ \big)$ è un sottogruppo di $\big(Aut\,(V)\,;\circ \big)$.

<u>Suggerimento</u>: *Si cominci dimostrando i risultati richiesti nel caso in cui sia* $k = 1$ *, cioè per un solo sottospazio vettoriale* V_1 *. Poi si può ottenere il risultato generale con una facile estensione del ragionamento, oppure osservando che, indicando con* $\underline{B}_i : V_i$ *la "bandiera elementare" fatta dal solo sottospazio* i*–esimo, si ha* $End_{\underline{B}}(V) \;=\; \bigcap_{i=1}^{k} End_{\underline{B}_i}(V)$ *e analogamente* $Aut_{\underline{B}}(V) = \bigcap_{i=1}^{k} Aut_{\underline{B}_i}(V)$.

35 — Sia G un gruppo, e sia $\Gamma \subseteq G$ un sottoinsieme in G. Definiamo in G le due relazioni ρ_d^{Γ} e ρ_s^{Γ} date da

$$a\,\rho_d^{\Gamma}\,b \;\overset{\triangle}{\Longleftrightarrow}\; a\,b^{-1} \in \Gamma \quad , \qquad a\,\rho_s^{\Gamma}\,b \;\overset{\triangle}{\Longleftrightarrow}\; b^{-1}a \in \Gamma \qquad\qquad \forall \quad a,b \in G \;.$$

Dimostrare che ρ_d^{Γ} è equivalenza $\Longleftrightarrow$ Γ è sottogruppo $\Longleftrightarrow$ ρ_s^{Γ} è equivalenza.

36 — Sia G un gruppo, sia $H \leq G$ un sottogruppo in G, e siano ρ_d^H e ρ_s^H le due relazioni di equivalenza in G definite come nell'esercizio 35 qui sopra. Dimostrare che:

(a) la relazione ρ_d^H è *compatibile a destra* (con l'operazione del gruppo), cioè

$$a\,\rho_d^H\,b \quad\Longrightarrow\quad (a\,c)\,\rho_d^H\,(b\,c) \qquad\qquad \forall\;\; a,b,c \in G$$

e inoltre $[1_G]_{\rho_d^H} = H$;

(b) la relazione ρ_s^H è *compatibile a sinistra* (con l'operazione del gruppo), cioè

$$a\,\rho_s^H\,b \quad\Longrightarrow\quad (d\,a)\,\rho_s^H\,(d\,b) \qquad\qquad \forall\;\; a,b,d \in G$$

e inoltre $[1_G]_{\rho_s^H} = H$.

37 — Sia G un gruppo, sia ρ una relazione di equivalenza in G, e sia $H := [1_G]_{\rho}$ la classe di $\rho-$equivalenza dell'elemento neutro $1_G \in G$. Con la terminologia e la notazione introdotte nell'esercizio 36 qui sopra, dimostrare che:

(a) se ρ è *compatibile a destra* (con l'operazione di G), allora $H \leq G$ e $\rho_d^H = \rho$;

(b) se ρ è *compatibile a sinistra* (con l'operazione di G), allora $H \leq G$ e $\rho_s^H = \rho$.