

CdL in Matematica

ALGEBRA 1

prof. Fabio GAVARINI

a.a. 2020–2021

Esame scritto dell'1 Febbraio 2021 — Sessione Estiva Anticipata, I appello

Testo & Svolgimento

..... *

- [1] — Si consideri in $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$ la relazione “ $\simeq$ ” definita da
- $$z' \simeq z'' \iff \exists n', n'' \in \mathbb{N} : 2^{n'} z' = 2^{n''} z'' \quad (z', z'' \in \mathbb{Z}^*).$$

Dimostrare che:

- (a) $\simeq$ è una relazione di equivalenza in $\mathbb{Z}^*$;
- (b) $\simeq$ è compatibile con la moltiplicazione in $\mathbb{Z}^*$;
- (c) indicando con $\odot$ l'operazione in $\mathbb{Z}^*/\simeq$ canonicamente indotta dalla moltiplicazione in $\mathbb{Z}^*$, il monoide quoziente $(\mathbb{Z}^*/\simeq; \odot)$ è isomorfo a $((2\mathbb{Z}+1); \cdot)$.

[2] — Siano E, F, L tre insiemi, sia “ $\sim$ ” l'usuale relazione di equipotenza tra insiemi, e si indichino con $\mathcal{P}(X)$ e Y^X rispettivamente l'insieme delle parti di un qualunque insieme X e l'insieme delle funzioni da un insieme a X all'insieme Y .

- (a) Dimostrare che se $E \sim F$, allora $\mathcal{P}(E) \sim \mathcal{P}(F)$.
- (b) Dimostrare che $(E \times F)^L \sim E^L \times F^L$.

[3] — Determinare l'insieme di tutte le soluzioni in $\mathbb{Z}$ del sistema di congruenze lineari

$$\begin{cases} -3x \equiv 6073^{354939} \pmod{7} \\ 276x \equiv -42 \pmod{5} \end{cases}$$

[4] — Sia G un gruppo, siano $H \leq G$, $K \leq G$, e siano G/H , G/K e $G/(H \cap K)$ i corrispondenti spazi di classi laterali sinistre (modulo H , modulo K e modulo $H \cap K$).

- (a) Dimostrare che esiste una funzione iniettiva $G/(H \cap K) \hookrightarrow (G/H) \times (G/K)$.
- (b) Dimostrare che se $H \trianglelefteq G$, $K \trianglelefteq G$, allora è anche $(H \cap K) \trianglelefteq G$.
- (c) Dimostrare che se $H \trianglelefteq G$, $K \trianglelefteq G$, e i gruppi quoziente G/H e G/K sono abeliani, allora anche il gruppo quoziente $G/(H \cap K)$ è abeliano.

[5] — Siano G un gruppo e E un G -spazio. A partire dall'azione di G su E , si definisca la funzione

$$\sigma_{\times} : G \times (E \times E) \longrightarrow (E \times E) \quad , \quad (g, (e_+, e_-)) \mapsto (g.e_+, g.e_-)$$

- (a) Dimostrare che $\sigma_{\times}$ è una azione di G su $(E \times E)$.
- (b) Nel caso di $G := \mathcal{S}_n$ ($n \in \mathbb{N}_+$) e $E := \{1, 2, \dots, n\}$, determinare il numero di G -orbite in $(E \times E)$ per la suddetta azione.

[6] — Siano A un anello e E un insieme, e sia A^E l'insieme di tutte le funzioni da E ad A dotato della sua struttura naturale di anello (indotta da A). Definiamo poi

$$\begin{aligned} \text{Supp}(f) &:= \{ e \in E \mid f(e) \neq 0_A \} & \forall f \in A^E \\ A_{\mathcal{E}}^E &:= \{ f \in A^E \mid \text{Supp}(f) \subseteq \mathcal{E} \} & \forall \mathcal{E} \subseteq E \\ A_{\text{fin}}^E &:= \{ f \in A^E \mid |\text{Supp}(f)| \in \mathbb{N} \} \end{aligned}$$

- (a) Dimostrare che A_{fin}^E è ideale dell'anello A^E .
- (b) Dimostrare che $A_{\mathcal{E}}^E$ è ideale dell'anello A^E , per ogni $\mathcal{E} \subseteq E$.
- (c) Dimostrare che per ogni $\mathcal{E} \subseteq E$ esiste un isomorfismo di anelli $A^E / A_{\mathcal{E}}^E \cong A^{E \setminus \mathcal{E}}$.

— ★ —

SVOLGIMENTO

N.B.: lo svolgimento qui presentato è molto lungo... Questo non significa che lo svolgimento ordinario di tale compito (nel corso di un esame scritto) debba essere altrettanto lungo. Semplicemente, questo lo è perché si approfitta per spiegare — in diversi modi, con lunghe digressioni, ecc. ecc. — in dettaglio e con molti particolari tutti gli aspetti della teoria toccati più o meno a fondo dal testo in questione.

[1] — Dal *Teorema Fondamentale dell'Aritmetica* — cioè il risultato per cui ogni intero non nullo ammette una fattorizzazione (essenzialmente) unica in prodotto di irriducibili — ricordiamo che per ogni $z \in \mathbb{Z}^*$ esiste un unico $n(z) \in \mathbb{N}$ tale che $2^{n(z)} \mid z$ mentre $2^{n(z)+1} \nmid z$. Risulta allora definita la funzione

$$\phi : \mathbb{Z}^* \longrightarrow (2\mathbb{Z} + 1) \quad , \quad z \mapsto \phi(z) := z / 2^{n(z)} \quad \forall z \in \mathbb{Z}^* \quad (1)$$

e ogni $z \in \mathbb{Z}^*$ può essere riscritto nella forma $z = 2^{n(z)} \phi(z)$.

Procediamo ora ad affrontare i singoli quesiti.

(a) Sia ρ_ϕ la relazione in $\mathbb{Z}^*$ canonicamente associata alla funzione ϕ , cioè quella definita da

$$z' \rho_\phi z'' \iff \phi(z') = \phi(z'') \quad \forall z', z'' \in \mathbb{Z}^* \quad (2)$$

Per un risultato generale, sappiamo che

$$\rho_\phi \text{ è una relazione di equivalenza.} \quad (3)$$

Inoltre, osserviamo adesso che

$$\text{la relazione } \simeq \text{ coincide con } \rho_\phi \quad (4)$$

perché per ogni $z', z'' \in \mathbb{Z}^*$ si ha

$$\begin{aligned} (\supseteq): \quad z' \rho_\phi z'' &\implies \phi(z') = \phi(z'') \implies 2^{n(z'')} 2^{n(z')} \phi(z') = 2^{n(z')} 2^{n(z'')} \phi(z'') \implies \\ &\implies 2^{n(z'')} z' = 2^{n(z')} z'' \implies z' \simeq z'', \quad \text{cioè in breve } z' \rho_\phi z'' \implies z' \simeq z'' \\ (\subseteq): \quad z' \simeq z'' &\implies \exists n', n'' \in \mathbb{N} : 2^{n'} z' = 2^{n''} z'' \implies \\ &\implies \exists n', n'' \in \mathbb{N} : 2^{n'} 2^{n(z')} \phi(z') = 2^{n''} 2^{n(z'')} \phi(z'') \implies \phi(z') = \phi(z'') \implies z' \rho_\phi z'', \\ &\text{cioè in breve } z' \simeq z'' \implies z' \rho_\phi z'' \end{aligned}$$

Ma allora (2) e (3) insieme ci dicono che *la relazione $\simeq$ è una equivalenza*, e l'affermazione (a) è dimostrata.

(b) Per ogni $z', z'' \in \mathbb{Z}^*$ si ha $n(z' z'') = n(z') n(z'')$ — per l'unicità della fattorizzazione in irriducibili — e quindi anche $\phi(z' z'') = \phi(z') \phi(z'')$. Questo significa che ϕ è un *morfismo* dal monoide $(\mathbb{Z}^*; \cdot)$ degli interi non nulli (con l'operazione di moltiplicazione) al monoide $((2\mathbb{Z}+1); \cdot)$ degli interi dispari (ancora con l'operazione di moltiplicazione). Come conseguenza, da un risultato generale sappiamo che la relazione (di equivalenza) ρ_ϕ in $\mathbb{Z}^*$ associata al morfismo ϕ è automaticamente *compatibile* con l'operazione $\cdot$ in $\mathbb{Z}^*$; pertanto, dato che $\rho_\phi = \simeq$ grazie alla (4), possiamo concludere che la relazione (di equivalenza) $\simeq$ è *compatibile* con l'operazione $\cdot$, q.e.d.

(c) Per il *Teorema Fondamentale di Omomorfismo*, il morfismo di monoidi ϕ in (1) induce canonicamente un isomorfismo

$$\phi_* : (\mathbb{Z}^*/\rho_\phi; \odot) \xrightarrow{\cong} \text{Im}(\phi) \quad , \quad [z]_{\rho_\phi} \mapsto \phi_*([z]_{\rho_\phi}) := \phi(z)$$

che grazie alla (4) diventa

$$\phi_* : (\mathbb{Z}^*/\simeq; \odot) \xrightarrow{\cong} \text{Im}(\phi) \quad , \quad [z]_{\simeq} \mapsto \phi_*([z]_{\simeq}) := \phi(z) \quad (5)$$

D'altra parte, per definizione abbiamo che $\phi(z) = z$ per ogni $z \in (2\mathbb{Z}+1)$ — in altre parole, ϕ è l'identità sugli interi *dispari* — e quindi $\text{Im}(\phi) = (2\mathbb{Z}+1)$. Perciò in conclusione la (5) diventa

$$\phi_* : (\mathbb{Z}^*/\simeq; \odot) \xrightarrow{\cong} \text{Im}(\phi) \quad , \quad [z]_{\simeq} \mapsto \phi_*([z]_{\simeq}) := \phi(z)$$

che significa appunto che il monoide $(\mathbb{Z}^*/\simeq; \odot)$ è isomorfo a $((2\mathbb{Z}+1); \cdot)$, q.e.d.

[2] — Procediamo alla soluzione dell'esercizio punto per punto.

(a) Per cominciare osserviamo che per ogni funzione $f : A \longrightarrow B$ esiste una corrispondente funzione

$$f_{\mathcal{P}} : \mathcal{P}(A) \longrightarrow \mathcal{P}(B), \quad A' \mapsto f_{\mathcal{P}}(A') := f(A') = \{f(a') \mid a' \in A'\} \quad \forall A' \in \mathcal{P}(A)$$

In aggiunta, osserviamo che per tale costruzione si ha anche

- (1) $(id_X)_{\mathcal{P}} = id_{\mathcal{P}(X)}$ per ogni insieme X ,
- (2) $(k \circ h)_{\mathcal{P}} = k_{\mathcal{P}} \circ h_{\mathcal{P}}$ per ogni scelta di funzioni $h : X \longrightarrow Y$ e $k : Y \longrightarrow Z$.

Consideriamo ora due insiemi E ed F tali che $E \sim F$: questo significa che esiste una funzione $f : E \longrightarrow F$ che è *invertibile*, dunque esiste anche la funzione inversa $\ell := f^{-1} : F \longrightarrow E$ che ci dà

$$\ell \circ f = id_E \quad \text{e} \quad f \circ \ell = id_F \quad (6)$$

Allora (1) e (2) applicate a (6) ci dà

$$\ell_{\mathcal{P}} \circ f_{\mathcal{P}} = id_{\mathcal{P}(E)} \quad \text{e} \quad f_{\mathcal{P}} \circ \ell_{\mathcal{P}} = id_{\mathcal{P}(F)} \quad (7)$$

il che significa che le due funzioni $f_{\mathcal{P}} : \mathcal{P}(E) \longrightarrow \mathcal{P}(F)$ e $\ell_{\mathcal{P}} : \mathcal{P}(F) \longrightarrow \mathcal{P}(E)$ sono inverse l'una dell'altra, e quindi $\mathcal{P}(E) \sim \mathcal{P}(F)$, q.e.d.

(b) Dati due insiemi E ed F consideriamo le funzioni “proiezioni”

$$\begin{aligned} \pi_E : E \times F &\longrightarrow E, & (e, f) &\mapsto \pi_E(e, f) := e & \forall (e, f) \in E \times F \\ \pi_F : E \times F &\longrightarrow F, & (e, f) &\mapsto \pi_F(e, f) := f & \forall (e, f) \in E \times F \end{aligned}$$

Dato poi un terzo insieme L , consideriamo le funzioni

$$\begin{aligned} \Psi : (E \times F)^L &\longrightarrow (E^L \times F^L), & \delta &\mapsto \Psi(\delta) := (\pi_E \circ \delta, \pi_F \circ \delta) & \forall \delta \in (E \times F)^L \\ \Omega : (E^L \times F^L) &\longrightarrow (E \times F)^L, & (\eta, \phi) &\mapsto \Omega(\eta, \phi) := \eta \boxtimes \phi & \forall (\eta, \phi) \in (E^L \times F^L) \end{aligned}$$

dove $\eta \boxtimes \phi : L \longrightarrow E \times F$ è la funzione definita da $\ell \mapsto (\eta \boxtimes \phi)(\ell) := (\eta(\ell), \phi(\ell))$. Una verifica diretta mostra che $\Omega \circ \Psi = id_{(E \times F)^L}$ e $\Psi \circ \Omega = id_{(E^L \times F^L)}$, cioè Ω e Ψ sono funzioni inverse l'una dell'altra: questo dimostra che $(E \times F)^L \sim E^L \times F^L$, q.e.d.

[3] — Cominciamo col semplificare le singole equazioni congruenziali del sistema.

Per la prima equazione, osserviamo che $276 \equiv 1 \pmod{5}$ mentre $-42 \equiv 3 \pmod{5}$, perciò tale equazione è equivalente a $x \equiv 3 \pmod{5}$ che si presenta come già risulta...

Per la seconda equazione, cominciamo semplificando modulo 7 la potenza 6073^{354939} che compare come termine noto.

Per la base di tale potenza abbiamo $6073 \equiv -3 \equiv 4 \pmod{7}$, e quindi $6073^{354939} \equiv (-3)^{354939} \equiv 4^{354939} \pmod{7}$.

Per l'esponente, osserviamo che $\text{M.C.D.}(-3, 7) = 1 = \text{M.C.D.}(4, 7)$ e quindi possiamo applicare il *Teorema di Eulero-Fermat* che in questo caso ci dà $(-3)^{\phi(7)} \equiv 1 \pmod{7}$ o

equivalentemente $4^{\phi(7)} \equiv 1 \pmod{7}$, dove ϕ è la funzione di Eulero. Considerato che $\phi(7) = 7 - 1 = 6$, possiamo allora *ridurre modulo 6* l'esponente della nostra potenza, per il quale troviamo $354939 \equiv 3 \pmod{6}$. Allora da $(-3)^{\phi(7)} \equiv 1 \pmod{7}$ deduciamo che

$$6073^{354939} \equiv (-3)^{354939} \equiv (-3)^3 \equiv -27 \equiv 1 \pmod{7}$$

o equivalentemente

$$6073^{354939} \equiv 4^{354939} \equiv 4^3 \equiv 64 \equiv 1 \pmod{7}$$

In conclusione, la seconda equazione è equivalente a $-3x \equiv 1 \pmod{7}$. Facendo un passo indietro, questa la riscriviamo come $-3x \equiv (-3)^3 \pmod{7}$ che si semplifica ancora (cosa che è possibile perché $\text{M.C.D.}(-3, 7) = 1$, e quindi -3 è invertibile modulo 7) nella equazione equivalente $x \equiv (-3)^2 \pmod{7}$, cioè $x \equiv 2 \pmod{7}$.

Avendo semplificato le due equazioni — cioè avendole sostituite con equazioni congruenziali equivalenti e più semplici — il sistema di partenza viene sostituito da un sistema equivalente come segue

$$\begin{cases} -3x \equiv 6073^{354939} & \pmod{7} \\ 276x \equiv -42 & \pmod{5} \end{cases} \implies \begin{cases} x \equiv 2 & \pmod{7} \\ x \equiv 3 & \pmod{5} \end{cases}$$

Si noti che il nuovo sistema è in forma *cinese*, con moduli 7 e 5 che sono tra loro coprimi: pertanto lo si può risolvere utilizzando il *Teorema Cinese del Resto*. In alternativa, possiamo risolverlo per sostituzioni successive, come segue:

$$\begin{aligned} & \begin{cases} -3x \equiv 6073^{354939} & \pmod{7} \\ 276x \equiv -42 & \pmod{5} \end{cases} \implies \begin{cases} x \equiv 2 & \pmod{7} \\ x \equiv 3 & \pmod{5} \end{cases} \implies \\ & \implies \begin{cases} x = 2 + 7k & (\forall k \in \mathbb{Z}) \\ x \equiv 3 & \pmod{5} \end{cases} \implies \begin{cases} x = 2 + 7k & (\forall k \in \mathbb{Z}) \\ 2 + 7k \equiv 3 & \pmod{5} \end{cases} \implies \\ & \implies \begin{cases} x = 2 + 7k & (\forall k \in \mathbb{Z}) \\ 7k \equiv 1 & \pmod{5} \end{cases} \implies \begin{cases} x = 2 + 7k & (\forall k \in \mathbb{Z}) \\ 7k \equiv 21 & \pmod{5} \end{cases} \implies \\ & \implies \begin{cases} x = 2 + 7k & (\forall k \in \mathbb{Z}) \\ k \equiv 3 & \pmod{5} \end{cases} \implies \begin{cases} x = 2 + 7(3 + 5\ell) \\ k = 3 + 5\ell & (\forall \ell \in \mathbb{Z}) \end{cases} \implies \\ & \implies x = 23 + 35\ell \quad (\forall \ell \in \mathbb{Z}) \implies x \in (23 + 35\mathbb{Z}) = [23]_{\equiv 35} \end{aligned}$$

dunque in conclusione l'insieme di tutte le soluzioni del sistema assegnato è

$$(23 + 35\mathbb{Z}) = [23]_{\equiv 35} = \{23 + 35\ell \mid \ell \in \mathbb{Z}\}$$

[4] — Rispondiamo nell'ordine ai diversi quesiti.

(a) Consideriamo la funzione

$$\kappa : G \longrightarrow (G/H) \times (G/K) \quad , \quad g \mapsto \kappa(g) := (gH, gK) \quad (8)$$

Per il *Teorema Fondamentale delle Applicazioni*, tale κ induce canonicamente una funzione *iniettiva*

$$\kappa_* : G/\rho_\kappa \hookrightarrow (G/H) \times (G/K) \quad , \quad [g]_{\rho_\kappa} \mapsto \kappa_*([g]_{\rho_\kappa}) := \kappa(g) \quad (9)$$

dove ρ_κ indica la relazione di equivalenza in G associata canonicamente alla funzione κ , definita da $g_+ \rho_\kappa g_- \iff \kappa(g_+) = \kappa(g_-)$ per ogni $g_+, g_- \in G$.

Dimostriamo ora che

$$\rho_\kappa = \rho_{H \cap K}^s \quad (10)$$

dove $\rho_{H \cap K}^s$ indica la relazione (di equivalenza) *sinistra* in G associata canonicamente al sottogruppo $H \cap K$, data da $g_+ \rho_{H \cap K}^s g_- \iff g_+(H \cap K) = g_-(H \cap K)$ per ogni $g_+, g_- \in G$.

Infatti, per ogni $g_+, g_- \in G$ si ha

$$\begin{aligned} g_+ \rho_{H \cap K}^s g_- &\iff g_+(H \cap K) = g_-(H \cap K) \iff g_+^{-1}g_- \in (H \cap K) \iff \\ &\iff (g_+^{-1}g_- \in H) \ \& \ (g_+^{-1}g_- \in K) \iff (g_+ H = g_- H) \ \& \ (g_+ K = g_- K) \iff \\ &\iff (g_+ H, g_+ K) = (g_- H, g_- K) \iff \kappa(g_+) = \kappa(g_-) \end{aligned}$$

così che la (10) è dimostrata. Ma allora, grazie alla (10) e ricordando che l'insieme quoziente $G/\rho_{H \cap K}^s$ è l'insieme $G/(H \cap K)$ delle classi laterali sinistre del sottogruppo $(H \cap K)$ in G , la funzione in (9) si può leggere come

$$\kappa_* : G/(H \cap K) \hookrightarrow (G/H) \times (G/K) \quad , \quad [g]_{\rho_\kappa} \mapsto \kappa_*([g]_{\rho_\kappa}) := \kappa(g) \quad (11)$$

dunque ci dà proprio una funzione *iniettiva* del tipo richiesto in (a).

(b) Se $H \trianglelefteq G$ e $K \trianglelefteq G$, allora gli insiemi quozienti hanno una struttura canonica di *gruppo quoziente* per la quale le proiezioni canoniche

$$\pi_H : G \twoheadrightarrow G/H \quad , \quad g \mapsto gH \quad , \quad \pi_K : G \twoheadrightarrow G/K \quad , \quad g \mapsto gK$$

sono morfismi. Da questo segue subito che anche la funzione $\kappa : G \twoheadrightarrow (G/H) \times (G/K)$ in (8) è un morfismo di gruppi, dove in $(G/H) \times (G/K)$ consideriamo la struttura standard di *gruppo prodotto diretto*. Per tale morfismo, il calcolo diretto ci dà

$$\begin{aligned} \text{Ker}(\kappa) &:= \{g \in G \mid \kappa(g) = (1_G H, 1_G K)\} = \{g \in G \mid (gH, gK) = (1_G H, 1_G K)\} = \\ &= \{g \in G \mid g \in H, g \in K\} = H \cap K \end{aligned}$$

cioè

$$\text{Ker}(\kappa) = H \cap K \quad (12)$$

In particolare $H \cap K$ è il nucleo di un morfismo di gruppi, e pertanto è un sottogruppo normale, q.e.d.

(c) Come già osservato per il punto (b), la funzione $\kappa : G \twoheadrightarrow (G/H) \times (G/K)$ in (8) è un morfismo di gruppi. Pertanto, il *Teorema Fondamentale di Omomorfismo (per Gruppi)* per κ ci dice che la funzione *iniettiva*

$$\kappa_* : G/\rho_\kappa = G/(H \cap K) \hookrightarrow (G/H) \times (G/K)$$

in (11) è in effetti un *morfismo iniettivo* di gruppi; inoltre, tramite tale κ_* , il gruppo quoziente $G/(H \cap K)$ è isomorfo al sottogruppo $\text{Im}(\kappa)$ di $(G/H) \times (G/K)$. Infine, nell'ipotesi che i due quozienti (G/H) e (G/K) siano abeliani (= commutativi) anche il loro prodotto diretto $(G/H) \times (G/K)$ è automaticamente abeliano, e quindi anche ogni suo sottogruppo: in particolare, il sottogruppo $\text{Im}(\kappa)$ in $(G/H) \times (G/K)$ è abeliano, e allora anche $G/(H \cap K)$, essendo isomorfo a $\text{Im}(\kappa)$, è a sua volta abeliano, q.e.d.

[5] — Affrontiamo separatamente i due quesiti.

(a) Utilizziamo la notazione sintetica $g.(e_+, e_-) := \sigma_\times(g, (e_+, e_-))$ per ogni $g \in G$ e $(e_+, e_-) \in (E \times E)$. Per dimostrare che $\sigma_\times$ è una azione di G su $(E \times E)$, dobbiamo provare che valgono le due seguenti proprietà:

$$\begin{aligned} \text{— (a.1)} \quad g_1.(g_2.(e_+, e_-)) &= (g_1 g_2).(e_+, e_-) & \forall g \in G, (e_+, e_-) \in (E \times E); \\ \text{— (a.2)} \quad 1_G.(g_2.(e_+, e_-)) &= (e_+, e_-) & \forall g \in G, (e_+, e_-) \in (E \times E). \end{aligned}$$

Per (a.1) si ha

$$\begin{aligned} g_1.(g_2.(e_+, e_-)) &:= g_1.(g_2.e_+, g_2.e_-) := (g_1.(g_2.e_+), g_1.(g_2.e_-)) = \\ &= ((g_1 g_2).e_+, (g_1 g_2).e_-) =: (g_1 g_2).(e_+, e_-) \end{aligned}$$

così che (a.1) è provata, mentre (a.2) è provata da

$$1_G.(e_+, e_-) := (1_G.e_+, 1_G.e_-) = (e_+, e_-)$$

(b) Consideriamo ora il caso $G := \mathcal{S}_n$ ($n \in \mathbb{N}_+$) e $E := \{1, 2, \dots, n\}$, e cerchiamo il numero di $\mathcal{S}_n$ -orbite in $(E \times E)$.

Cominciamo con una osservazione: per ogni $\sigma \in \mathcal{S}_n$ e ogni $(x, y) \in (E \times E)$ si ha

$$\sigma.x = \sigma.y \iff \sigma(x) = \sigma(y) \iff x = y \quad (13)$$

Consideriamo allora i due sottoinsiemi di $(E \times E)$

$$\Delta_E := \{(x, y) \in (E \times E) \mid x = y\}, \quad \nabla_E := \{(x, y) \in (E \times E) \mid x \neq y\}$$

— quindi, in particolare, $\nabla_E = (E \times E) \setminus \Delta_E$ e $\Delta_E = (E \times E) \setminus \nabla_E$. Con questa notazione, la (13) ci dice che

$$\sigma.\Delta_E \subseteq \Delta_E, \quad \sigma.\nabla_E \subseteq \nabla_E \quad \forall \sigma \in \mathcal{S}_n \quad (14)$$

(e quindi in effetti vale la “=” in entrambi i casi): ne segue che

$$\begin{aligned} &\text{le } \mathcal{S}_n\text{-orbite degli elementi di } \Delta_E \text{ — rispettivamente, di } \nabla_E \text{ — sono} \\ &\text{sempre diverse da quelle degli elementi di } \nabla_E \text{ — rispettivamente, di } \Delta_E. \end{aligned} \quad (15)$$

Pertanto, studiamo separatamente le orbite degli elementi in Δ_E e quelle degli elementi in ∇_E . A tal fine, *distinguiamo i due casi* $n = 1$ e $n > 1$.

$n = 1$: Quando $E := \{1, \dots, n\} = \{1\}$ si ha $\nabla_E = \emptyset$ e $\Delta_E = (E \times E) = \{(1, 1)\}$ che ovviamente è composto di una unica orbita di $\mathcal{S}_n = \mathcal{S}_1 = \{id_E\}$.

$n > 1$: Per ogni $(x, y) \in (E \times E)$, studiamone la $\mathcal{S}_n$ -orbita, che indichiamo con $\mathcal{O}_{(x,y)} := \{\sigma.(x, y) \mid \sigma \in \mathcal{S}_n\}$. Come già osservato, dobbiamo distinguere due casi, secondo che sia $(x, y) \in \Delta_E$ oppure $(x, y) \in \nabla_E$: in corrispondenza, troviamo

$$\mathcal{O}_{(x,y)} = \Delta_E \quad \forall (x, y) \in \Delta_E, \quad \mathcal{O}_{(x,y)} = \nabla_E \quad \forall (x, y) \in \nabla_E \quad (16)$$

Infatti, per prima cosa la (14) significa esattamente che

$$\mathcal{O}_{(x,y)} \subseteq \Delta_E \quad \forall (x, y) \in \Delta_E, \quad \mathcal{O}_{(x,y)} \subseteq \nabla_E \quad \forall (x, y) \in \nabla_E \quad (17)$$

Per le inclusioni inverse invece andiamo a studiare separatamente i due casi possibili.

Primo caso: $(x, y) \in \Delta_E$ — Quando $(x, y) \in \Delta_E$, cioè $x = y$, per ogni altro elemento $(x', y') = (x', x') \in \Delta_E$ esiste un $\sigma \in \mathcal{S}_n$ — ad esempio, la trasposizione $\sigma := (x x')$ — tale che $\sigma.x := \sigma(x) = x'$. Ma allora è anche

$$\sigma.(x, y) = \sigma.(x, x) = (\sigma.x, \sigma.x) = (x', x') = (x', y')$$

dunque $(x', y') = \sigma.(x, y) \in \mathcal{O}_{(x,y)}$ per ogni $(x', y') \in \Delta_E$ e quindi $\mathcal{O}_{(x,y)} \supseteq \Delta_E$ per ogni $(x, y) \in \Delta_E$; insieme alla (17), questo ci permette di concludere che per ogni $(x, y) \in \Delta_E$ si ha $\mathcal{O}_{(x,y)} = \Delta_E$, q.e.d.

Secondo caso: $(x, y) \in \nabla_E$ — Quando $(x, y) \in \nabla_E$, cioè $x \neq y$, consideriamo un elemento $(x', y') \in \nabla_E$, dunque con $x' \neq y'$. Distinguiamo allora i quattro casi possibili:

(1) $\{x', y'\} \cap \{x, y\} = \{x, y\}$: In questo caso si ha $(x', y') = (x, y) = id.(x, y) \in \mathcal{O}_{(x,y)}$ oppure $(x', y') = (y, x) = \sigma_{(xy)}(x, y) \in \mathcal{O}_{(x,y)}$ dove $\sigma_{(xy)} := (xy) \in \mathcal{S}_n$ è la trasposizione in $\mathcal{S}_n$ che scambia tra loro x e y e lascia fissi tutti gli elementi di $E \setminus \{x, y\}$.

Comunque sia, in entrambi i casi si ha $(x', y') \in \mathcal{O}_{(x,y)}$.

(2) $\{x', y'\} \cap \{x, y\} = \{x\}$: In questo caso si ha $(x', y') = (x, y')$ se $x' = x$, e allora abbiamo $(x', y') = (x, y') = \sigma_{(yy')}.(x, y) \in \mathcal{O}_{(x,y)}$, oppure $(x', y') = (x', x)$ se $y' = x$, e allora abbiamo $(x', y') = (x', x) = \sigma_{(yxx')}.(x, y) \in \mathcal{O}_{(x,y)}$, dove $\sigma_{(yxx')} := (yx x')$ è la permutazione che manda la y in x , la x in x' , la x' in y .

Comunque sia, in entrambi i casi si ha $(x', y') \in \mathcal{O}_{(x,y)}$.

(3) $\{x', y'\} \cap \{x, y\} = \{y\}$: In questo caso si ha $(x', y') = (x', y)$ se $y' = y$, e allora abbiamo $(x', y') = (x', y) = \sigma_{(xx')}.(x, y) \in \mathcal{O}_{(x,y)}$, oppure $(x', y') = (y, y')$ se $x' = y$, e allora abbiamo $(x', y') = (y, y') = \sigma_{(xyy')}.(x, y) \in \mathcal{O}_{(x,y)}$, dove $\sigma_{(xyy')} := (xy y')$ è la permutazione che manda la x in y , la y in y' , la y' in x .

Comunque sia, in entrambi i casi si ha $(x', y') \in \mathcal{O}_{(x,y)}$.

(4) $\{x', y'\} \cap \{x, y\} = \emptyset$: In questo caso è $(x', y') = \sigma_{(xx')(yy')}.(x, y) \in \mathcal{O}_{(x,y)}$, dove $\sigma_{(xx')(yy')} := (xx')(yy')$ è la permutazione che manda la x in x' e la y in y' .

In particolare si ha $(x', y') \in \mathcal{O}_{(x,y)}$.

NOTA: si noti che i casi (2) e (3) si verificano se e soltanto è $n > 2$, mentre il caso (4) si verifica se e soltanto è $n > 3$.

Dall'analisi precedente dei vari casi possibili emerge che quando è $(x, y) \in \nabla_E$ allora per ogni $(x', y') \in \nabla_E$ si ha $(x', y') \in \mathcal{O}_{(x, y)}$; pertanto, è $\nabla_E \subseteq \mathcal{O}_{(x, y)}$; insieme alla (17), questo ci fa concludere che per ogni $(x, y) \in \nabla_E$ si ha $\mathcal{O}_{(x, y)} = \nabla_E$, q.e.d.

Dunque la (16) è provata, e ci dice — dato che $\Delta_E \neq \emptyset \neq \nabla_E$ se $n > 1$ — che le $\mathcal{S}_n$ -orbite in $(E \times E)$ per $n > 1$ sono esattamente due, una data da Δ_E e l'altra da ∇_E .

In conclusione, *il numero di $\mathcal{S}_n$ -orbite in $(E \times E)$ è 1 per $n = 1$ ed è 2 per $n > 1$.*

[6] — Rispondiamo separatamente ai diversi quesiti.

(a) Osserviamo che per gli insiemi $\text{Supp}(f)$ valgono le seguenti proprietà:

$$(1) \quad \text{Supp}(0) = \emptyset \text{ per la funzione costante pari a } 0 \text{ (che è lo zero dell'anello } A^E),$$

$$(2) \quad \text{Supp}(-f) = \text{Supp}(f) \quad \forall f \in A^E,$$

perché $(-f)(e) = -f(e) \neq 0 \iff f(e) \neq 0$

$$(3) \quad \text{Supp}(h + k) \subseteq \text{Supp}(h) \cup \text{Supp}(k) \quad \forall h, k \in A^E,$$

perché $e \in \text{Supp}(h + k) \implies (h + k)(e) := h(e) + k(e) \neq 0 \implies$

$$\implies (h(e) \neq 0) \vee (k(e) \neq 0) \implies (e \in \text{Supp}(h)) \vee (e \in \text{Supp}(k)) \implies$$

$$\implies e \in (\text{Supp}(h) \cup \text{Supp}(k))$$

$$(4) \quad \text{Supp}(h \cdot k) \subseteq \text{Supp}(h) \cap \text{Supp}(k) \quad \forall h, k \in A^E,$$

perché $e \in \text{Supp}(h \cdot k) \implies (h \cdot k)(e) := h(e) \cdot k(e) \neq 0 \implies$

$$\implies (h(e) \neq 0) \wedge (k(e) \neq 0) \implies (e \in \text{Supp}(h)) \wedge (e \in \text{Supp}(k)) \implies$$

$$\implies e \in (\text{Supp}(h) \cap \text{Supp}(k))$$

Ora, siccome l'insieme vuoto è finito, e l'unione di due insiemi finiti è finita, la (1), la (2) e la (3) implicano subito che A_{fn}^E è un sottogruppo di $(A^E; +)$. Inoltre, se $\text{Supp}(h)$ è finito oppure $\text{Supp}(k)$ è finito ne segue che anche $\text{Supp}(h) \cap \text{Supp}(k)$ è un insieme finito: da questo e dalla (4) segue allora che $h \cdot k \in A_{fn}^E$ e $k \cdot h \in A_{fn}^E$ per ogni $h \in A_{fn}^E$ e ogni $k \in A^E$; pertanto concludiamo che A_{fn}^E è un ideale (bilatero) dell'anello A^E , q.e.d.

(b) Per ogni $\mathcal{E} \subseteq E$, consideriamo la funzione

$$r_{E \setminus \mathcal{E}} : A^E \longrightarrow A^{E \setminus \mathcal{E}}, \quad f \mapsto r_{E \setminus \mathcal{E}}(f) := f|_{E \setminus \mathcal{E}} \quad \forall f \in A^E \quad (18)$$

che associa ad ogni funzione f da E ad A la sua restrizione al sottoinsieme $E \setminus \mathcal{E}$. È immediato osservare che questa funzione è un *morfismo* di anelli; inoltre, per esso abbiamo

$$\begin{aligned} \text{Ker}(r_{E \setminus \mathcal{E}}) &:= \{ f \in A^E \mid r_{E \setminus \mathcal{E}}(f) = f|_{E \setminus \mathcal{E}} = 0 \} = \{ f \in A^E \mid f(e) = 0 \ \forall e \in E \setminus \mathcal{E} \} = \\ &= \{ f \in A^E \mid \forall e \in E, f(e) = 0 \implies e \in \mathcal{E} \} = \{ f \in A^E \mid \text{Supp}(f) \subseteq \mathcal{E} \} =: A_{\mathcal{E}}^E \end{aligned}$$

cioè in breve

$$\text{Ker}(r_{E \setminus \mathcal{E}}) = A_{\mathcal{E}}^E \quad (19)$$

Ma allora $A_{\mathcal{E}}^E = \text{Ker}(r_{E \setminus \mathcal{E}})$, essendo il nucleo di un morfismo tra anelli, è automaticamente un ideale dell'anello A^E , q.e.d.

(c) Applicando il *Teorema Fondamentale di Omomorfismo per Anelli* al morfismo in (18) otteniamo un isomorfismo di anelli

$$\begin{aligned} r_{E \setminus \mathcal{E}}^* : A^E / \text{Ker}(r_{E \setminus \mathcal{E}}) &\xrightarrow{\cong} \text{Im}(r_{E \setminus \mathcal{E}}^*) \\ f + \text{Ker}(r_{E \setminus \mathcal{E}}) &\mapsto r_{E \setminus \mathcal{E}}^*(f + \text{Ker}(r_{E \setminus \mathcal{E}})) := r_{E \setminus \mathcal{E}}(f) = f|_{E \setminus \mathcal{E}} \end{aligned} \quad (20)$$

Ora, è chiaro che $\text{Im}(r_{E \setminus \mathcal{E}}) = A^{E \setminus \mathcal{E}}$: infatti, per ogni $f' \in A^{E \setminus \mathcal{E}}$ possiamo considerare ad esempio la funzione $f \in A^E$ definita da $f(e') := \begin{cases} f'(e), & \forall e \in E \setminus \mathcal{E} \\ 0, & \forall e \in \mathcal{E} \end{cases}$ e osservare che per essa si ha $r_{E \setminus \mathcal{E}}(f) = f'$, così che $f' \in \text{Im}(r_{E \setminus \mathcal{E}})$. Ma allora, da questo e da (19) otteniamo che l'isomorfismo in (20) è in effetti un isomorfismo di anelli

$$r_{E \setminus \mathcal{E}}^* : A^E / A_{\mathcal{E}}^E \xrightarrow{\cong} A^{E \setminus \mathcal{E}}$$

del tipo richiesto.