

ALGEBRA 1 — 2008/2009

Prof. Fabio Gavarini

Sessione estiva anticipata — prova scritta del 23 Febbraio 2009

Svolgimento completo

N.B.: lo svolgimento qui presentato è molto lungo... Questo non vuol dire che lo svolgimento ordinario di tale compito (nel corso di un esame scritto) debba esserlo altrettanto. Semplicemente, questo lo è perché si è colta l'occasione per spiegare in dettaglio i vari esercizi, anche prospettando diversi modi possibili di svolgerli.

..... *

[1] — Sia $(U(\mathbb{Z}_{40}); \cdot)$ il gruppo degli elementi invertibili dell'anello unitario $(\mathbb{Z}_{40}; +, \cdot)$.

- (a) Calcolare esplicitamente il sottoinsieme $(U(\mathbb{Z}_{40}); \cdot)$;
- (b) determinare se esistano in $(U(\mathbb{Z}_{40}); \cdot)$ elementi di ordine 2, 3, 4, 5 oppure 6;
- (c) stabilire, giustificando la conclusione, se il gruppo $(U(\mathbb{Z}_{40}); \cdot)$ sia ciclico oppure no.

Soluzione: (a) Dallo studio generale dei gruppi del tipo $(\mathbb{Z}_n; +)$, con $n \in \mathbb{N}_+$, sappiamo che gli elementi di $(U(\mathbb{Z}_n); \cdot)$ sono esattamente gli elementi dell'insieme

$$U(\mathbb{Z}_n) = \{ \bar{z} := (z \bmod n) \mid M.C.D.(z, n) = 1 \} \quad (1)$$

delle classi resto modulo n rappresentate da numeri interi *coprime* con n . Sappiamo anche che — indicando con φ la funzione di Eulero — tale insieme ha cardinalità $\varphi(n)$.

Nel nostro caso, con $n = 40$ abbiamo

$$|U(\mathbb{Z}_{40})| = \varphi(40) = \varphi(2^3 \cdot 5) = \varphi(2^3) \cdot \varphi(5) = (2-1)2^{3-1} \cdot (5-1) = 1 \cdot 4 \cdot 4 = 16$$

cioè i generatori cercati sono in tutto esattamente 16. Inoltre, il calcolo diretto dell'insieme in (1) ci dà

$$U(\mathbb{Z}_{40}) = \{ \bar{1}, \bar{3}, \bar{7}, \bar{9}, \bar{11}, \bar{13}, \bar{17}, \bar{19}, \bar{21}, \bar{23}, \bar{27}, \bar{29}, \bar{31}, \bar{33}, \bar{37}, \bar{39} \}$$

NOTA: nel fare il calcolo teniamo conto del fatto che

$$M.C.D.(z, 40) = 1 \implies M.C.D.(-z, 40) = 1$$

e quindi $\bar{z} \in U(\mathbb{Z}_{40}) \implies -\bar{z} = \overline{-z} \in U(\mathbb{Z}_{40})$; perciò, ad esempio, da $\bar{1} \in U(\mathbb{Z}_{40})$ deduciamo che $\bar{39} = -\bar{1} = \overline{-1} \in U(\mathbb{Z}_{40})$, oppure da $\bar{7} \in U(\mathbb{Z}_{40})$ deduciamo che $\bar{33} = -\bar{7} = \overline{-7} \in U(\mathbb{Z}_{40})$, o da $\bar{13} \in U(\mathbb{Z}_{40})$ che $\bar{27} = -\bar{13} = \overline{-13} \in U(\mathbb{Z}_{40})$, e così via.

Perciò, di fatto, sapendo che gli elementi sono 16, ci basta calcolarne 8, e gli altri 8 li troviamo prendendo l'opposto — in $(\mathbb{Z}_{40}; +)$ — dei primi 8.

(b) Per il Teorema di Lagrange, l'ordine di un elemento in un gruppo finito è un divisore dell'ordine del gruppo: nel caso in esame, l'ordine di un elemento di $(\mathbb{Z}_n; +)$ dev'essere divisore di 16, dunque appartiene all'insieme $\{1, 2, 4, 8, 16\}$. Quindi *possono esistere* (ma non sappiamo ancora se esistano effettivamente...) elementi di ordine 2 oppure di ordine 4, ma certamente *non esistono* elementi di ordine 3, oppure 5, oppure 6.

Un elemento di ordine 2 è facile da trovare: è l'elemento $-\bar{1} = \overline{-1} = \overline{39}$.

(N.B.: questo è vero in generale! Per ogni $n \in (\mathbb{N}_+ \setminus \{1\})$, in $(\mathbb{Z}_n; +)$, l'elemento $-\bar{1} = \overline{-1} = \overline{n-1}$ ha sempre ordine 2).

Un elemento di ordine 4 lo trovo facilmente per tentativi (al secondo colpo...). Calcolando le potenze di $\bar{7}$, si trova

$$\bar{7}^1 = \bar{7} \neq \bar{1}, \quad \bar{7}^2 = \overline{49} = \bar{9} \neq \bar{1}, \quad \bar{7}^3 = \bar{7}^2 \cdot \bar{7} = \bar{9} \cdot \bar{7} = \overline{63} = \overline{23} \neq \bar{1}, \quad \bar{7}^4 = \bar{7}^2 \cdot \bar{7}^2 = \bar{9} \cdot \bar{9} = \overline{81} = \bar{1}$$

per cui l'ordine di $\bar{7}$ è proprio 4.

(c) Il gruppo $(U(\mathbb{Z}_{40}); \cdot)$ ha 16 elementi, quindi è ciclico se e soltanto se contiene almeno un elemento di ordine 16. Perciò dobbiamo appurare se esiste o no in $U(\mathbb{Z}_{40})$ un tale elemento. A tal scopo, possiamo subito escludere gli elementi $\bar{1}$, $\overline{39}$ e $\bar{7}$, che sappiamo avere rispettivamente ordine 1, 2 e 4. Inoltre, osserviamo che essi generano rispettivamente i sottogruppi (ciclici)

$$\langle \bar{1} \rangle = \{ \bar{1} \}, \quad \langle \overline{39} \rangle = \{ \bar{1}, \overline{39} \}, \quad \langle \bar{7} \rangle = \{ \bar{1}, \bar{7}, \bar{9}, \overline{23} \}$$

perciò complessivamente possiamo escludere dai possibili “candidati” tutti gli elementi del sottoinsieme $\{ \bar{1}, \bar{7}, \bar{9}, \overline{23}, \overline{39} \}$ — ché certamente questi hanno ordine 1, oppure 2, oppure 4, ma sicuramente non 16. Prima di calcolare altre potenze, facciamo “fruttare al meglio” questi risultati! Osserviamo che, per ogni n, m , si ha

$$\text{ord}(\overline{n \cdot m}) = \text{ord}(\overline{n} \cdot \overline{m}) = m.c.m.(\text{ord}(\overline{n}), \text{ord}(\overline{m})) \quad , \quad \text{dove} \quad \text{ord}(\overline{x}) := \text{ordine di } \overline{x}$$

perchè $\text{ord}(\overline{n})$ e $\text{ord}(\overline{m})$ commutano l'uno con l'altro (stanno in un gruppo abeliano!).

Applichiamo questa osservazione nel modo seguente: da $\overline{(-1)} \cdot \bar{7} = \overline{-7} = \overline{33}$ ricaviamo

$$\text{ord}(\overline{33}) = \text{ord}(\overline{(-1)} \cdot \bar{7}) = m.c.m.(\text{ord}(\overline{-1}), \text{ord}(\bar{7})) = m.c.m.(2, 4) = 4$$

quindi $\overline{33}$ ha ordine 4 come $\bar{7}$. Inoltre, le sue potenze si ricavano facilmente da quelle del suo opposto $\bar{7}$, precisamente

$$\overline{33}^2 = \overline{-7}^2 = \bar{7}^2 = \bar{9}, \quad \overline{33}^3 = \overline{-7}^3 = -\bar{7}^3 = -\overline{23} = \overline{17}, \quad \overline{33}^4 = \overline{-7}^4 = \bar{7}^4 = \bar{1}$$

per cui $\overline{33}$ genera il sottogruppo $\langle \overline{33} \rangle = \{ \bar{1}, \overline{33}, \bar{9}, \overline{17} \}$. Con lo stesso ragionamento, troviamo che l'elemento $\overline{31} = -\bar{9}$ ha ordine 2 e genera il sottogruppo $\langle \overline{31} \rangle = \{ \bar{1}, \overline{31} \}$,

dato che $\overline{31}^2 = (-\overline{9})^2 = \overline{9}^2 = \overline{1}$. Dunque ora possiamo escludere dal novero dei “candidati” tutti gli elementi del sottoinsieme $\{\overline{1}, \overline{7}, \overline{9}, \overline{17}, \overline{23}, \overline{33}, \overline{39}\}$.

Cercando oltre, un po’ di calcoli ci danno

$$\overline{3}^1 = \overline{2}, \quad \overline{3}^2 = \overline{9}, \quad \overline{3}^3 = \overline{27}, \quad \overline{3}^4 = \overline{81} = \overline{1}$$

quindi $\overline{3}$ ha ordine 4 e genera il sottogruppo $\langle \overline{3} \rangle = \{\overline{1}, \overline{3}, \overline{9}, \overline{27}\}$: e così ora possiamo escludere tutti gli elementi del sottoinsieme $\{\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{17}, \overline{23}, \overline{27}, \overline{33}, \overline{39}\}$. Cercando ancora tra gli *altri* elementi, calcoliamo le potenze di $\overline{11}$, e troviamo

$$\overline{11}^1 = \overline{11}, \quad \overline{11}^2 = \overline{121} = \overline{1}, \quad \text{quindi} \quad \langle \overline{11} \rangle = \{\overline{1}, \overline{11}\}$$

e l’insieme da scartare diventa $\{\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{17}, \overline{23}, \overline{27}, \overline{33}, \overline{39}\}$.

Continuiamo calcolando le potenze di $\overline{37} = \overline{-3}$. Operando come prima, troviamo

$$\overline{37}^2 = \overline{-3}^2 = \overline{-9} = \overline{9}, \quad \overline{37}^3 = \overline{-3}^3 = \overline{-27} = \overline{13}, \quad \overline{37}^4 = \overline{-3}^4 = \overline{81} = \overline{1}$$

quindi $\overline{37}$ ha ordine 4, genera il sottogruppo $\langle \overline{13} \rangle = \{\overline{1}, \overline{37}, \overline{9}, \overline{13}\}$. Dunque l’insieme da scartare risulta essere $\{\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{23}, \overline{27}, \overline{33}, \overline{37}, \overline{39}\}$.

Osserviamo ancora che $\overline{29} = \overline{-11}$ ha ordine 2 come $\overline{11}$, e quindi possiamo scartare anche $\overline{29}$. Restano ancora da considerare $\overline{19}$ e $\overline{21}$, che sono l’uno l’opposto dell’altro.

Siccome $\overline{21} = \overline{37}$, possiamo calcolare le potenze di $\overline{21}$ rifacendoci a quelle (già note, e comunque più facili da calcolare!) di $\overline{3}$ e di $\overline{7}$. In particolare, troviamo subito che

$$\overline{21}^2 = \overline{3}^2 \cdot \overline{7}^2 = \overline{9} \cdot \overline{9} = \overline{81} = \overline{1}$$

per cui $\overline{21}$ ha ordine 2. Ne deduciamo allora che anche $\overline{19} = \overline{-21}$ ha a sua volta ordine 2.

In conclusione, nessun elemento di $U(\mathbb{Z}_{40})$ ha ordine 16, e questo significa che tale gruppo *non* è ciclico. $\square$

..... *

[2] — Siano A e B due insiemi non vuoti, sia B^A l’insieme di tutte le applicazioni da A a B , e sia $\mathcal{S}(B)$ il gruppo simmetrico di tutte le permutazioni di B . Si consideri in B^A la relazione ρ definita da

$$f \rho f' \iff \exists \sigma \in \mathcal{S}(B) : \sigma \circ f = f'$$

dove il simbolo $\circ$ denota il prodotto di composizione.

(a) Dimostrare che ρ è una relazione di equivalenza.

(b) Per ogni $f \in B^A$, dimostrare che $St_f := \{\sigma \in \mathcal{S}(B) \mid \sigma \circ f = f\}$ è un sottogruppo di $\mathcal{S}(B)$.

(c) Per ogni $f \in B^A$, dimostrare che per la classe di ρ -equivalenza di f vale l'inclusione $[f]_\rho \subseteq \{f' \in B^A \mid \text{Im}(f) \sim \text{Im}(f')\}$, dove il simbolo $\sim$ significa "è equipotente a".

Soluzione: (a) Dimostriamo che ρ gode delle tre proprietà che caratterizzano una relazione di equivalenza: riflessività, simmetria, transitività.

Per ogni $f \in B^A$, abbiamo che $\text{id}_B \circ f = f$, con $\text{id}_B \in \mathcal{S}(B)$: quindi $f \rho f$, e dunque ρ è riflessiva.

Per ogni $f, f' \in B^A$ tali che $f \rho f'$, esiste $\sigma \in \mathcal{S}(B)$ tale che $\sigma \circ f = f'$. Ma allora si ha anche $\sigma^{-1} \circ f' = f$, con $\sigma^{-1} \in \mathcal{S}(B)$ — ch  $\mathcal{S}(B)$   un gruppo, perci  contiene l'inverso di ogni suo elemento! — e dunque ρ   simmetrica.

Per ogni $f, f', f'' \in B^A$ tali che $f \rho f'$ e $f' \rho f''$, esistono $\sigma, \sigma' \in \mathcal{S}(B)$ tali che $\sigma \circ f = f'$ e $\sigma' \circ f' = f''$. Ma allora si ha anche $(\sigma' \circ \sigma) \circ f = \sigma' \circ (\sigma \circ f) = \sigma' \circ f' = f''$, con $(\sigma' \circ \sigma) \in \mathcal{S}(B)$ — ch  $\mathcal{S}(B)$   un gruppo, perci    chiuso! — dunque $(\sigma' \circ \sigma) \circ f = f''$ significa che ρ   transitiva.

Concludiamo che ρ , essendo riflessiva, simmetrica e transitiva,   un'equivalenza, q.e.d.

(b) Per ogni $f \in B^A$, sia $St_f := \{\sigma \in \mathcal{S}(B) \mid \sigma \circ f = f\}$; per dimostrare che questo sottoinsieme di $\mathcal{S}(B)$   un sottogruppo, dobbiamo provare che   non vuoto, che   chiuso, e che contiene l'inverso di ogni suo elemento.

  chiaro che $\text{id}_B \in St_f$, quindi St_f   non vuoto. Per ogni $\sigma, \sigma' \in St_f$ abbiamo $\sigma \circ f = f$ e $\sigma' \circ f = f$; ma allora $(\sigma \circ \sigma') \circ f = \sigma \circ (\sigma' \circ f) = \sigma \circ f = f$, cio  $\sigma \circ \sigma' \in St_f$, e possiamo concludere che St_f   chiuso. Infine, per ogni $\sigma \in St_f$ abbiamo $\sigma \circ f = f$, da cui moltiplicando ambo i membri per σ^{-1} segue che $f = \sigma^{-1} \circ f = f$; ma allora $\sigma^{-1} \in St_f$, e dunque St_f contiene l'inverso di ogni suo elemento.

(c) Sia dato un elemento $f \in B^A$. Per ogni $h \in [f]_\rho$, abbiamo $h \rho f$, quindi esiste $\sigma \in \mathcal{S}(B)$ tale che $\sigma \circ h = f$. Allora

$$\sigma(h(a)) = (\sigma \circ h)(a) = f(a) \quad \text{per ogni } a \in A \quad (2)$$

quindi

$$\begin{aligned} \sigma_* : \text{Im}(h) &:= \{h(a) \mid a \in A\} \longrightarrow \text{Im}(f) := \{f(a) \mid a \in A\} \\ h(a) &\mapsto \sigma_*(h(a)) := f(a) \end{aligned}$$

  un'applicazione *ben definita* da $\text{Im}(h)$ a $\text{Im}(f)$. Sottolineiamo che σ_*   ben definita, nel senso che se un elemento di $\text{Im}(h)$   descritto in due modi diversi, diciamo $h(a_1) = h(a_2)$, allora si ha anche $\sigma_*(h(a_1)) := f(a_1) = f(a_2) =: \sigma_*(h(a_2))$, grazie alla (2).

Poich  σ   biunivoca, in particolare   iniettiva, e quindi   iniettiva anche σ_* ; inoltre, per la (2)   chiaro che σ_*   anche suriettiva. Quindi σ_*   biunivoca, perci  $\text{Im}(h) \sim \text{Im}(f)$, e viceversa abbiamo $\text{Im}(f) \sim \text{Im}(h)$, dunque $h \in \{f' \in B^A \mid \text{Im}(f) \sim \text{Im}(f')\}$, q.e.d. $\square$

[3] — Sia $\mathbb{K}$ un campo, sia $\mathbb{K}^* := \mathbb{K} \setminus \{0\}$, e siano

$$T_2(\mathbb{K}) := \left\{ \begin{pmatrix} \alpha & c \\ 0 & \beta \end{pmatrix} \mid \alpha, \beta \in \mathbb{K}^*, c \in \mathbb{K} \right\}$$

$$U_2(\mathbb{K}) := \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \mid c \in \mathbb{K} \right\}, \quad D_2(\mathbb{K}) := \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \mid \alpha, \beta \in \mathbb{K}^* \right\}$$

sottoinsiemi dell'insieme delle matrici 2×2 a coefficienti in $\mathbb{K}$.

(a) Dimostrare che $T_2(\mathbb{K})$ è un sottogruppo del gruppo $GL_2(\mathbb{K})$ (rispetto al prodotto righe per colonne).

(b) Dimostrare che $D_2(\mathbb{K})$ è un sottogruppo di $T_2(\mathbb{K})$.

(c) Dimostrare che $U_2(\mathbb{K})$ è un sottogruppo normale di $T_2(\mathbb{K})$.

(d) Determinare esplicitamente un isomorfismo (di gruppi) dal gruppo quoziente $T_2(\mathbb{K})/U_2(\mathbb{K})$ al gruppo $D_2(\mathbb{K})$.

Soluzione: (a) Per dimostrare $T_2(\mathbb{K})$ è un sottogruppo di $GL_2(\mathbb{K})$ dobbiamo provare che è non vuoto, che è chiuso, e che contiene l'inverso di ogni suo elemento.

Per cominciare, è chiaro che $I_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in T_2(\mathbb{K})$, quindi $T_2(\mathbb{K})$ è non vuoto.

Per la chiusura, dobbiamo provare che per ogni $x, x' \in T_2(\mathbb{K})$ abbiamo $x \cdot x' \in T_2(\mathbb{K})$. Siano dunque $x = \begin{pmatrix} \alpha & c \\ 0 & \beta \end{pmatrix}$, $x' = \begin{pmatrix} \alpha' & c' \\ 0 & \beta' \end{pmatrix}$; allora, visto che $\alpha, \alpha', \beta, \beta' \in \mathbb{K}^*$, abbiamo

$$x \cdot x' = \begin{pmatrix} \alpha & c \\ 0 & \beta \end{pmatrix} \cdot \begin{pmatrix} \alpha' & c' \\ 0 & \beta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' & \alpha c' + c\beta' \\ 0 & \beta\beta' \end{pmatrix} \in T_2(\mathbb{K})$$

Infine, per ogni $x = \begin{pmatrix} \alpha & c \\ 0 & \beta \end{pmatrix} \in T_2(\mathbb{K})$ calcoliamo x^{-1} e verifichiamo che si ha $x^{-1} \in T_2(\mathbb{K})$. Poniamo $x^{-1} = \begin{pmatrix} \alpha' & c' \\ 0 & \beta' \end{pmatrix}$, e scriviamo la condizione perché tale matrice sia l'inversa di x , cioè

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 = x \cdot x' = \begin{pmatrix} \alpha & c \\ 0 & \beta \end{pmatrix} \cdot \begin{pmatrix} \alpha' & c' \\ 0 & \beta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' & \alpha c' + c\beta' \\ 0 & \beta\beta' \end{pmatrix}$$

il che ci dà le quattro condizioni espresse dal seguente sistema di equazioni lineari (nelle tre incognite α', c', β'):

$$\begin{cases} \alpha\alpha' = 1 \\ 0 = 0 \\ \alpha c' + c\beta' = 0 \\ \beta\beta' = 1 \end{cases}$$

Risolvendo tale sistema si trova (facilmente...) che $x^{-1} = \begin{pmatrix} \alpha^{-1} & -\alpha^{-1}c\beta^{-1} \\ 0 & \beta^{-1} \end{pmatrix}$, e quindi — dato che $\alpha^{-1}, \beta^{-1} \in \mathbb{K}^*$ — abbiamo $x^{-1} \in T_2(\mathbb{K})$, q.e.d.

(b) Analogamente a quanto fatto al punto (a), per dimostrare $D_2(\mathbb{K})$ è un sottogruppo di $T_2(\mathbb{K})$ dobbiamo osservare che $D_2(\mathbb{K}) \subseteq T_2(\mathbb{K})$, il che è ovvio, e poi provare che $D_2(\mathbb{K})$ è non vuoto, che è chiuso, e che contiene l'inverso di ogni suo elemento.

Di nuovo, è chiaro che $I_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in D_2(\mathbb{K})$, quindi $D_2(\mathbb{K})$ è non vuoto.

Per la chiusura, dobbiamo provare che $x \cdot x' \in D_2(\mathbb{K})$ per ogni $x, x' \in D_2(\mathbb{K})$. Siano dunque $x = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$, $x' = \begin{pmatrix} \alpha' & 0 \\ 0 & \beta' \end{pmatrix}$; allora, dato che $\alpha, \alpha', \beta, \beta' \in \mathbb{K}^*$, abbiamo

$$x \cdot x' = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \cdot \begin{pmatrix} \alpha' & 0 \\ 0 & \beta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' & 0 \\ 0 & \beta\beta' \end{pmatrix} \in D_2(\mathbb{K})$$

Infine, per ogni $x = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \in D_2(\mathbb{K})$ verifichiamo che $x^{-1} \in D_2(\mathbb{K})$. Il calcolo fatto in precedenza per $T_2(\mathbb{K})$ — tenendo conto che $D_2(\mathbb{K}) \subseteq T_2(\mathbb{K})$, e nel caso presente è $c := 0$ — ci dà $x^{-1} = \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \beta^{-1} \end{pmatrix}$, e quindi $x^{-1} \in D_2(\mathbb{K})$, q.e.d.

(c) Per dimostrare $U_2(\mathbb{K})$ è un sottogruppo di $T_2(\mathbb{K})$ si procede come prima. Intanto, $U_2(\mathbb{K}) \subseteq T_2(\mathbb{K})$, per definizione, e inoltre $I_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in U_2(\mathbb{K})$, per cui $U_2(\mathbb{K})$ è non vuoto. Poi abbiamo

$$u \cdot u' = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & c' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & c+c' \\ 0 & 1 \end{pmatrix} \in U_2(\mathbb{K})$$

per ogni $u = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$, $u' = \begin{pmatrix} 1 & c' \\ 0 & 1 \end{pmatrix} \in U_2(\mathbb{K})$; quindi $U_2(\mathbb{K})$ è chiuso. Infine, per ogni $u = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \in U_2(\mathbb{K})$, il calcolo fatto in precedenza per $T_2(\mathbb{K})$ — tenendo conto che $U_2(\mathbb{K}) \subseteq T_2(\mathbb{K})$, e nel caso presente è $\alpha := 0 =: \beta$ — ci dà $u^{-1} = \begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix}$, così che $u^{-1} \in U_2(\mathbb{K})$, q.e.d.

Resta da dimostrare che il sottogruppo $U_2(\mathbb{K})$ è *normale*, il che può essere espresso con la condizione che $x \cdot u \cdot x^{-1} \in U_2(\mathbb{K})$ per ogni $u = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \in U_2(\mathbb{K})$, $x = \begin{pmatrix} \alpha & c \\ 0 & \beta \end{pmatrix} \in T_2(\mathbb{K})$. Ora, la formule già trovata per $x^{-1} = \begin{pmatrix} \alpha^{-1} & -\alpha^{-1}c\beta^{-1} \\ 0 & \beta^{-1} \end{pmatrix}$ ci permette di calcolare

$$x \cdot u \cdot x^{-1} = \begin{pmatrix} \alpha & c \\ 0 & \beta \end{pmatrix} \cdot \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha^{-1} & -\alpha^{-1}c\beta^{-1} \\ 0 & \beta^{-1} \end{pmatrix} = \begin{pmatrix} 1 & \alpha k \beta^{-1} \\ 0 & 1 \end{pmatrix} \in U_2(\mathbb{K})$$

cioè $x \cdot u \cdot x^{-1} \in U_2(\mathbb{K})$, q.e.d.

(d) Per trovare un isomorfismo esplicito $\Phi : T_2(\mathbb{K})/U_2(\mathbb{K}) \xrightarrow{\cong} D_2(\mathbb{K})$, cominciamo col costruire un epimorfismo $\phi : T_2(\mathbb{K}) \xrightarrow{\cong} D_2(\mathbb{K})$. Per definizione, esso è dato dall'applicazione

$$\phi : T_2(\mathbb{K}) \longrightarrow D_2(\mathbb{K}) \quad , \quad \begin{pmatrix} \alpha & c \\ 0 & \beta \end{pmatrix} \mapsto \phi \begin{pmatrix} \alpha & c \\ 0 & \beta \end{pmatrix} := \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$$

e la formula ottenuta in precedenza per il prodotto di due matrici in $T_2(\mathbb{K})$ ci mostra che tale applicazione conserva il prodotto, cioè è effettivamente un morfismo. D'altra parte esso è chiaramente suriettivo, dunque si tratta di un epimorfismo.

A questo punto, il *Teorema Fondamentale di Omomorfismo* ci garantisce che l'epimorfismo $\phi : T_2(\mathbb{K}) \longrightarrow D_2(\mathbb{K})$ induce un isomorfismo $\phi_* : T_2(\mathbb{K})/Ker(\phi) \xrightarrow{\cong} D_2(\mathbb{K})$ dato da $\phi_*(t Ker(\phi)) := \phi(t)$ per ogni classe laterale $t Ker(\phi) \in T_2(\mathbb{K})/Ker(\phi)$ — dove $t \in T_2(\mathbb{K})$. Andiamo dunque a vedere chi sia il nucleo $Ker(\phi)$ dell'epimorfismo ϕ .

Per definizione, $Ker(\phi) := \{ t \in T_2(\mathbb{K}) \mid \phi(t) = I_2 \}$. Quindi, se $t = \begin{pmatrix} \alpha & c \\ 0 & \beta \end{pmatrix} \in T_2(\mathbb{K})$ abbiamo

$$t = \begin{pmatrix} \alpha & c \\ 0 & \beta \end{pmatrix} \in Ker(\phi) \iff \iff \phi(t) = \phi \begin{pmatrix} \alpha & c \\ 0 & \beta \end{pmatrix} := \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} = I_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \iff \alpha = 0 = \beta$$

e dunque $t \in Ker(\phi) \iff t \in U_2(\mathbb{K})$, per la definizione stessa di $U_2(\mathbb{K})$. Ma allora $T_2(\mathbb{K})/Ker(\phi) = T_2(\mathbb{K})/U_2(\mathbb{K})$, e l'isomorfismo $\phi_* : T_2(\mathbb{K})/Ker(\phi) \xrightarrow{\cong} D_2(\mathbb{K})$ considerato in precedenza è proprio un isomorfismo $\Phi : T_2(\mathbb{K})/U_2(\mathbb{K}) \xrightarrow{\cong} D_2(\mathbb{K})$ del tipo richiesto. $\square$

..... *

[4] — Nell'anello di polinomi $\mathbb{K}[x]$, dove $\mathbb{K}$ è un campo, si considerino i due polinomi $f(x) := x^4 - 1$, $g(x) := x^4 - 3x^3 + 3x - 1$.

Calcolare il m.c.m. tra $f(x)$ e $g(x)$, nei due casi

$$(a) \quad \mathbb{K} := \mathbb{Q} \quad , \quad (b) \quad \mathbb{K} := \mathbb{Z}_5 \quad .$$

Soluzione: Il problema si può risolvere con un approccio comune ai due casi — (a) e (b) — in esame, cioè $\mathbb{K} := \mathbb{Q}$ e $\mathbb{K} := \mathbb{Z}_5$. Per prima cosa, osserviamo che, per calcolare il m.c.m. tra $f(x)$ e $g(x)$, possiamo far uso della formula

$$m.c.m.(f(x), g(x)) = \frac{f(x)g(x)}{M.C.D.(f(x), g(x))} \quad (3)$$

che vale in generale — cioè per due qualsiasi polinomi $f(x)$ e $g(x)$ a coefficienti in un campo $\mathbb{K}$ — dove $M.C.D.(f(x), g(x))$ indica il M.C.D. (=massimo comun divisore) tra $f(x)$ e $g(x)$. Il senso di questa strategia sta nel fatto che per calcolare $M.C.D.(f(x), g(x))$ possiamo utilizzare l'algoritmo euclideo delle divisioni successive!...

Passiamo dunque a calcolare 'sto $M.C.D.(f(x), g(x))$. L'algoritmo delle divisioni successive ci dà

$$x^4 - 1 = (x^4 - 3x^3 + 3x - 1) \cdot 1 + (3x^3 - 3x)$$

$$x^4 - 3x^3 + 3x - 1 = (3x^3 - 3x) \cdot (3^{-1}x - 1) + (x^2 - 1)$$

$$3x^3 - 3x = (x^2 - 1) \cdot (3x) + 0$$

Si noti che in questi calcoli i numeri che abbiamo scritto possono rappresentare sia elementi di $\mathbb{Q}$ che elementi di $\mathbb{Z}_5$. Ad ogni modo, in entrambi i casi — (a) e (b) — l'ultimo resto non nullo nel procedimento è $x^2 - 1$, e quindi concludiamo che

$$M.C.D.(f(x), g(x)) = x^2 - 1 \quad (4)$$

Adesso calcoliamo il $m.c.m.(f(x), g(x))$ utilizzando la (4) e la (3). Vale la pena di osservare che quest'ultima formula va usata con intelligenza. Infatti, si potrebbe procedere così:

— (1) prima si calcola il prodotto $P(x) := f(x)g(x)$;

— (2) poi si calcola il rapporto $\frac{P(x)}{M.C.D.(f(x), g(x))}$, che è giusto il $m.c.m.(f(x), g(x))$

cercato.

Dal punto di vista teorico, questo modo di procedere non fa una grinza. Però dal punto di vista pratico è pericoloso. Infatti, col passo (1) si introduce un polinomio “più grosso” (cioè, di grado più alto), che è $P(x)$, che poi al passo (2) viene coinvolto in una divisione. E lavorando con polinomi “più grossi” il rischio di commettere errori di calcolo è maggiore...

In alternativa si può procedere come segue:

— (1') prima si calcola il rapporto $f_*(x) := \frac{f(x)}{M.C.D.(f(x), g(x))}$;

— (2') poi si calcola il prodotto $f_*(x)g(x)$, che è il $m.c.m.(f(x), g(x))$ cercato.

Questo secondo modo di procedere è altrettanto valido dal punto di vista teorico (è perfettamente equivalente!), ma in più coinvolge polinomi “più piccoli” — cioè di grado uguale o minore di quelli di partenza — quindi riduce il rischio di commettere errori di calcolo (e magari rende anche i calcoli più semplici...).

Naturalmente, un altro procedimento *del tutto equivalente* a (1')+(2') è il seguente:

— (1'') prima si calcola il rapporto $g_*(x) := \frac{g(x)}{M.C.D.(f(x), g(x))}$;

— (2'') poi si calcola il prodotto $f(x)g_*(x)$, che è il $m.c.m.(f(x), g(x))$ cercato.

Osservato tutto ciò, operiamo dunque il passo (1'), calcolando

$$f_*(x) := \frac{f(x)}{M.C.D.(f(x), g(x))} = \frac{x^4 - 1}{x^2 - 1} = \frac{(x^2 + 1)(x^2 - 1)}{x^2 - 1} = x^2 + 1$$

dove il calcolo è particolarmente semplice se sappiamo riconoscere il prodotto notevole $x^4 - 1 = (x^2 + 1)(x^2 - 1)$ del tipo $a^2 - b^2 = (a + b)(a - b)$.

Fatto questo, il passo (2') sarà

$$\begin{aligned} m.c.m.(f(x), g(x)) &= f_*(x)g(x) = (x^2 + 1) \cdot (x^4 - 3x^3 + 3x - 1) = \\ &= x^6 - 3x^5 + 3x^3 - x^2 + x^4 - 3x^3 + 3x - 1 = x^6 - 3x^5 + x^4 - x^2 + 3x - 1 \end{aligned}$$

cioè, in definitiva,

$$m.c.m.(f(x), g(x)) = x^6 - 3x^5 + x^4 - x^2 + 3x - 1 \quad (5)$$

Come *controprova*, procediamo ora a calcolare $m.c.m.(f(x), g(x))$ con i passi (1'')+(2'') — *N.B.*: ma in un compito d'esame *non* è necessario (nel senso che non è richiesto). Si ha

$$g_*(x) := \frac{g(x)}{M.C.D.(f(x), g(x))} = \frac{x^4 - 3x^3 + 3x - 1}{x^2 - 1} = x^2 - 3x + 1$$

per il passo (1''), e poi il passo (2'') ci dà

$$\begin{aligned} m.c.m.(f(x), g(x)) &= f(x)g_*(x) = (x^4 - 1) \cdot (x^2 - 3x + 1) = \\ &= x^6 - 3x^5 + x^4 - (x^2 - 3x + 1) = x^6 - 3x^5 + x^4 - x^2 + 3x - 1 \end{aligned}$$

e quindi ritroviamo di nuovo

$$m.c.m.(f(x), g(x)) = x^6 - 3x^5 + x^4 - x^2 + 3x - 1$$

Infine, osserviamo anche che, volendo, nel caso (b) — cioè per $\mathbb{K} = \mathbb{Z}_5$ — la soluzione espressa in (5) si può riscrivere come

$$m.c.m.(f(x), g(x)) = x^6 + 2x^5 + x^4 + 4x^2 + 3x + 4$$

perché in $\mathbb{Z}_5$ si ha $-3 = 2$ e $-1 = 4$ (intendendo $-3 = [-3]_5$, $2 = [2]_5$, e così via). $\square$