CdL in Matematica

ALGEBRA 1

prof. Fabio GAVARINI

a.a. 2018–2019

Esame scritto del 24 Settembre 2019 — Sessione Autunnale, II appello

Testo & Svolgimento

. . . . . * . . . . . .

[1] — Nell'insieme $\mathbb{Z}^\times := \mathbb{Z} \setminus \{0\}$ si consideri la relazione η definita da

$$a \,\eta\, b \iff \exists\, n \in \mathbb{N} \;:\; a\,b = n^2 \qquad \forall\; a\,,b \in \mathbb{Z}^\times$$

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

(b) Descrivere esplicitamente le classi di η–equivalenza $[1]_\eta$, $[5]_\eta$, $[-6]_\eta$, $[6]_\eta$, $[45]_\eta$, in funzione della fattorizzazione di ciascun intero non nullo in potenze di primi distinti.

[2] — Determinare tutti i possibili valori di $x \in \mathbb{Z}$ che soddisfino simultaneamente le seguenti tre condizioni:

$$137\,x \,\equiv\, -54 \pmod{11}\;, \qquad -\overline{103}\,\overline{x} \,=\, \overline{47} \text{ in } \mathbb{Z}_9\;, \qquad \exists\; y \in \mathbb{Z} \;:\; 83\,x + 15\,y \,=\, 503$$

[3] — Sia A un anello commutativo unitario, e $U(A)$ il gruppo dei suoi elementi invertibili (rispetto alla moltiplicazione). Consideriamo il sottoinsieme

$$Aff(A) \;:=\; \left\{ Y_{a,b} \,\middle|\, a \in U(A)\,, b \in A \right\} \qquad \left(\subseteq A^A \right)$$

di applicazioni da A in sé stesso definite da $Y_{a,b}(x) := a\,x + b$ (per ogni $x \in A$) per ogni $(a,b) \in U(A) \times A$. Indichiamo poi con $\mathcal{S}(A)$ l'insieme di tutte le permutazioni di A in sé stesso. Dimostrare che:

(a) $Aff(A) \subseteq \mathcal{S}(A)$ — cioè ogni $Y_{a,b}$ è una permutazione;

(b) $Aff(A)$ è un sottogruppo del gruppo $\big(\mathcal{S}(A)\,;\circ\big)$;

(c) il sottoinsieme $O(A) := \left\{ Y_{a,0} \,\middle|\, a \in U(A) \right\}$ è un sottogruppo di $\big(Aff(A)\,;\circ\big)$;

(d) il sottoinsieme $T(A) := \left\{ Y_{1,b} \,\middle|\, b \in A \right\}$ è un sottogruppo normale di $\big(Aff(A)\,;\circ\big)$;

(e) la funzione $O(A) \times T(A) \longrightarrow Aff(A)$ data da $\big(Y_{a,0}\,, Y_{1,b}\big) \mapsto Y_{a,0} \circ Y_{1,b}$ è biiettiva.

[4] — Sia A un anello commutativo unitario, e sia $M_2(A)$ l'anello delle matrici quadrate 2×2 a coefficienti in A. Per ogni $\alpha \in A$, consideriamo il sottoinsieme

$$M_2^{(\alpha)}(A) \;:=\; \left\{ \begin{pmatrix} u+v & u \\ \alpha\, u & v \end{pmatrix} \in M_2(A) \;\middle|\; u\,,v \in A \right\} \qquad \Big(\subseteq M_2(A) \Big)$$

Dimostrare che:

(a) $M_2^{(\alpha)}(A)$ è un sottoanello dell'anello $M_2(A)$;

(b) il (sotto)anello $M_2^{(\alpha)}(A)$ è commutativo;

(c) in generale — cioè tranne che per casi banali — il (sotto)anello $M_2^{(\alpha)}(A)$ non è un ideale (bilatero) dell'anello $M_2(A)$.

[5] — Si considerino in $\mathbb{Q}[x]$ i due polinomi

$$p(x) \;:=\; x^4 - 1 \quad , \qquad q(x) \;:=\; x^4 - 3\,x^3 + 3\,x - 1$$

(a) Determinare il $\text{M.C.D.}\big(\,p(x)\,,q(x)\big)$.

(b) Determinare il $\text{m.c.m.}\big(\,p(x)\,,q(x)\big)$.

(c) Determinare una identità di Bézout esplicita per $\text{M.C.D.}\big(\,p(x)\,,q(x)\big)$.

— $\star$ —

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] — Ricordando che la relazione η in $\mathbb{Z}^\times$ è definita da

$$a\,\eta\,b \iff \exists\, n \in \mathbb{N} \;:\; a\,b = n^2 \qquad\qquad \forall \quad a\,,b \in \mathbb{Z}^\times$$

procediamo alla soluzione dell'esercizio punto per punto.

(a) Dobbiamo dimostrare che η è una equivalenza in $\mathbb{Z}$. A tal fine, dobbiamo verificare che η gode delle tre proprietà che caratterizzano ogni equivalenza, cioè la *riflessività*, la *transitività*, la *simmetricità*. Ne dimostriamo una alla volta.

Riflessività: I calcoli diretti ci danno $a\,a \,=\, a^2 \,=\, n^2$ con $n := a \in \mathbb{N}$, per ogni $a \in \mathbb{Z}^\times$: quindi η è *riflessiva*, q.e.d.

Transitività: Per ogni $a\,,b\,,c \in \mathbb{Z}^\times$, i calcoli diretti ci danno

$$a\,\eta\,b\,,\;\; b\,\eta\,c \quad\Longrightarrow\quad \exists\;\, n\,,m \in \mathbb{N} \;:\; a\,b \,=\, n^2\,,\; b\,c \,=\, m^2 \quad\Longrightarrow\quad a\,b \,=\, \left(\frac{n\,m}{|b|}\right)^2 \qquad (1)$$

dove abbiamo $\dfrac{n\,m}{|b|} \in \mathbb{Q}_{\geq}$, cioè $\dfrac{n\,m}{|b|}$ è un razionale positivo, per costruzione. Osserviamo ora che in effetti è $\frac{n\,m}{|b|} \in \mathbb{N}$. Infatti, se così non fosse, prendendo la fattorizzazione in primi del numeratore e del denominatore potremmo semplificare la frazione $\dfrac{n\,m}{|b|}$ nella forma più semplice $\dfrac{n\,m}{|b|} = \dfrac{\nu\,\mu}{p_1\,p_2\cdots p_k}$ dove $k \geq 1$ e $p_1\,,\,p_2\,,\,\ldots\,,\,p_k$ sono numeri primi che dividono $|b|$ ma *non* dividono $n\,m$, mentre ν e μ sono opportuni divisori di n e di m rispettivamente. Ma allora otteniamo anche

$$a\,b \,=\, \left(\frac{n\,m}{|b|}\right)^2 \,=\, \left(\frac{\nu\,\mu}{p_1\,p_2\cdots p_k}\right)^2 \qquad\Longrightarrow\qquad p_1^2\,p_2^2\cdots p_k^2\,a\,b \;=\; \nu^2\,\mu^2$$

Ora, l'ultima identità è impossibile, per via dell'esistenza e unicità di fattorizzazioni in irriducibili per gli interi. Infatti, il membro di sinistra è divisibile per ciascuno dei suoi fattori primi p_i (con $i = 1,\ldots,k$); d'altra parte, ciascuno di questi fattori p_i *non* divide il prodotto $\nu\,\mu$ e quindi — dato che p_i è primo! — non divide nemmeno il prodotto $\nu^2\,\mu^2 = (\nu\,\mu)^2$, ce è il membro di destra della (presunta) identità.

Questo dimostra che $n\,m \,\in \mathbb{N}$, come affermato. Pertanto dalla (1) otteniamo che $a\,\eta\,c$, il che dimostra che η è transitiva, q.e.d.

Simmetricità: Per ogni $a\,,b \in \mathbb{Z}^\times$, poiché il prodotto in $\mathbb{Z}^\times$ è commutativo, si ha

$$a\,\eta\,b \quad\Longleftrightarrow\quad \exists\, n \in \mathbb{N} \;:\; a\,b = n^2 \quad\Longleftrightarrow\quad \exists\, n \in \mathbb{N} \;:\; b\,a = n^2 \quad\Longleftrightarrow\quad b\,\eta\,a$$

e quindi η è *simmetrica*, q.e.d.

(b) Dovendo descrivere esplicitamente la classe di η–equivalenza $[z]_\rho$ di un elemento $1, z \in \mathbb{Z}^\times$, ricordiamo che essa è definita da

$$[z]_\eta \;:=\; \left\{\, x \in \mathbb{Z}^\times \,\middle|\, x\,\eta\,z \,\right\} \qquad (2)$$

Ora osserviamo che

$$x\,\eta\,z \;\overset{\triangle}{\Longleftrightarrow}\; \exists\, n \in \mathbb{N} \;:\; x\,z = n^2 \qquad (3)$$

In prima battuta, da questo segue subito che

$$x\,\eta\,z \;\overset{\triangle}{\Longleftrightarrow}\; (-x)\,\eta\,(-z)$$

semplicemente perché $(-a)\,(-b) = a\,b$; in particolare questo significa che

$$x \in [z]_\eta \;\overset{\triangle}{\Longleftrightarrow}\; (-x) \in [-z]_\eta \quad, \qquad \text{e quindi} \qquad [-z]_\eta \,=\, -[z]_\eta \qquad (4)$$

In aggiunta, se $x \in [z]_\eta$ allora — siccome $x \,\eta\, z$, applicando (3) e osservando che n^2 è sempre positivo — troviamo che x è *concorde* con z — cioè x è positivo, rispettivamente negativo, se e soltanto se z è positivo, rispettivamente negativo. Pertanto, scrivendo x e z nella forma $x = \epsilon_x\,|x|$ e $z = \epsilon_z\,|z|$ con $\epsilon_x, \epsilon_z \in \{+, -\}$, abbiamo

$$x \in [z]_\eta \quad \Longrightarrow \quad \Big(\epsilon_x = \epsilon_z \;\; \& \;\; |x|\,\eta\,|z| \Big) \tag{5}$$

In conclusione, dalla (5) abbiamo che basta descrivere le classi di η–equivalenza degli interi z *positivi*, e poi applicare la (4) per descrivere quelle degli interi negativi.

Sia ora dunque $z \in \mathbb{Z}_+$, e passiamo a descrivere la sua classe $[z]_\eta$. Se $x \in [z]_\eta$, dall'analisi precedente sappiamo che x è concorde con z, quindi $x \in \mathbb{Z}_+$; inoltre, da (2) e da (3) otteniamo che esiste un $n \in \mathbb{N}$ tale che $x\,z = n^2$. Ora, in quest'ultima identità fattorizziamo in numeri primi (positivi) entrambi i membri, e otteniamo

$$p_1^{\chi_1+\zeta_1}\, p_2^{\chi_2+\zeta_2} \cdots p_k^{\chi_k+\zeta_k} \;=\; p_1^{2\,\nu_1}\, p_2^{2\,\nu_2} \cdots p_k^{2\,\nu_k} \tag{6}$$

dove $x = p_1^{\chi_1}\, p_2^{\chi_2} \cdots p_k^{\chi_k}$, $z = p_1^{\zeta_1}\, p_2^{\zeta_2} \cdots p_k^{\zeta_k}$ e $n = p_1^{\nu_1}\, p_2^{\nu_2} \cdots p_k^{\nu_k}$ sono le fattorizzazioni in primi di x, di z e di n — in cui prendiamo gli esponenti χ_i, ζ_i e ν_i positivi *o nulli*, così da facilitare il confronto delle diverse fattorizzazioni in gioco. Ora, dalla (6) l'unicità della fattorizzazione in primi implica che $\chi_i + \zeta_i = 2\,\nu_i$ per ogni $1 = 1, 2, \ldots, k$, quindi $\overline{\chi_i} + \overline{\zeta_i} = \overline{0} \pmod 2$ e quindi $\overline{\chi_i} = \overline{\zeta_i} \pmod 2$ per ogni $1 = 1, 2, \ldots, k$. In conclusione,

$$x \in [z]_\eta \quad \Longleftrightarrow \quad x\,\eta\,z \quad \Longrightarrow \quad \left\{ \begin{array}{l} x = p_1^{\chi_1}\, p_2^{\chi_2} \cdots p_k^{\chi_k} \\ z = p_1^{\zeta_1}\, p_2^{\zeta_2} \cdots p_k^{\zeta_k} \\ \overline{\chi_i} = \overline{\zeta_i} \pmod 2\,, \quad \forall\;\; 1 = 1, 2, \ldots, k \end{array} \right. \tag{7}$$

che ci dà condizioni *necessarie* perché sia $x \in [z]_\eta$. D'altra parte, le condizioni in (7) ovviamente sono anche *sufficienti*, cioè si ha

$$\left\{ \begin{array}{l} x = p_1^{\chi_1}\, p_2^{\chi_2} \cdots p_k^{\chi_k} \\ z = p_1^{\zeta_1}\, p_2^{\zeta_2} \cdots p_k^{\zeta_k} \\ \overline{\chi_i} = \overline{\zeta_i} \pmod 2\,, \quad \forall\;\; i = 1, 2, \ldots, k \end{array} \right. \quad \Longrightarrow \quad x\,\eta\,z \quad \Longleftrightarrow \quad x \in [z]_\eta \tag{8}$$

perché l'implicazione "$\Longrightarrow$" di sinistra segue subito dal fatto che

$$\left\{ \begin{array}{l} x = p_1^{\chi_1}\, p_2^{\chi_2} \cdots p_k^{\chi_k} \\ z = p_1^{\zeta_1}\, p_2^{\zeta_2} \cdots p_k^{\zeta_k} \\ \overline{\chi_i} = \overline{\zeta_i} \pmod 2\,, \quad \forall\;\; i \end{array} \right. \quad \Longrightarrow \quad x\,z \;=\; p_1^{\chi_1+\zeta_1}\, p_2^{\alpha_2+\zeta_2} \cdots p_k^{\chi_k+\zeta_k} \;=\; n^2$$

con $n := p_1^{(\chi_1+\zeta_1)/2}\, p_2^{(\chi_2+\zeta_2)/2} \cdots p_k^{(\chi_k+\zeta_k)/2}$ — dove $(\chi_i + \zeta_i)/2 \in \mathbb{N}$ per ogni i, grazie all'ipotesi $\overline{\chi_i} = \overline{\zeta_i} \pmod 2$ — da cui segue per definizione $x\,\eta\,z$.

Dunque (7) e (8) insieme caratterizzano gli elementi x della classe $[z]_\eta$ con $z \in \mathbb{Z}_+$: tenendo in conto anche la (4), in definitiva concludiamo che, se $z = \epsilon\, p_1^{\zeta_1}\, p_2^{\zeta_2} \cdots p_k^{\zeta_k}$ è la fattorizzazione in primi di z (con $\epsilon = \pm$), allora

$$[z]_\eta \;=\; \left\{ x \in \mathbb{Z}^\times \;\middle|\; \begin{array}{l} x \;=\; \epsilon\, p_1^{\chi_1} \cdots p_k^{\chi_k}\, p_{k+1}^{2\,\chi_{k+1}} \cdots p_t^{2\,\chi_t} \\ \overline{\chi_i} = \overline{\zeta_i} \pmod 2 \quad \forall\; 1 \le i \le k \end{array} \right\} \tag{9}$$

Applichiamo ora la descrizione in (9) ai vari casi $z \in \{1\,,5\,,-6\,,6\,,45\}$. Otteniamo

$$[1]_\eta \;=\; \left\{ x \in \mathbb{Z}^\times \,\middle|\, x \,=\, +p_{k+1}^{2\,\chi_{k+1}} \cdots p_t^{2\,\chi_t} \right\} \;=\; \left\{ n^2 \,\middle|\, n \in \mathbb{N}_+ \right\}$$

$$[5]_\eta \;=\; \left\{ x \in \mathbb{Z}^\times \,\middle|\, x \,=\, 5^{\chi_1} p_{k+1}^{2\,\chi_{k+1}} \cdots p_t^{2\,\chi_t}\,,\; \overline{\chi_1} = \overline{1} \right\} \;=\; \left\{ 5\,n^2 \,\middle|\, n \in \mathbb{N}_+ \right\}$$

$$[-6]_\eta = \left\{ x \in \mathbb{Z}^\times \,\middle|\, x = -2^{\chi_1}\, 3^{\chi_2}\, p_{k+1}^{2\,\chi_3} \cdots p_t^{2\,\chi_t}\,,\; \overline{\chi_1} = \overline{1}\,,\; \overline{\chi_2} = \overline{1} \right\} = \left\{ -6\,n^2 \,\middle|\, n \in \mathbb{N}_+ \right\}$$

$$[6]_\eta \;=\; \left\{ x \in \mathbb{Z}^\times \,\middle|\, x = 2^{\chi_1}\, 3^{\chi_2}\, p_{k+1}^{2\,\chi_3} \cdots p_t^{2\,\chi_t}\,,\; \overline{\chi_1} = \overline{1}\,,\; \overline{\chi_2} = \overline{1} \right\} \;=\; \left\{ 6\,n^2 \,\middle|\, n \in \mathbb{N}_+ \right\}$$

$$[45]_\eta \;=\; \left\{ x \in \mathbb{Z}^\times \,\middle|\, x \,=\, +3^{\chi_1}\, 5^{\chi_2}\, p_{k+1}^{2\,\chi_3} \cdots p_t^{2\,\chi_t}\,,\; \overline{\chi_1} = \overline{2}\,,\; \overline{\chi_2} = \overline{1} \right\} \;=\; \left\{ 5\,n^2 \,\middle|\, n \in \mathbb{N}_+ \right\}$$

Si noti tra l'altro che queste descrizioni esplicite danno anche $[6]_\eta = -[-6]_\eta$ — come già prescritto da (4) — e $[5]_\eta = [45]_\eta$ — che possiamo dedurre a priori dal fatto che $5\,\eta\,45$ in quanto $5 \cdot 45 = 5 \cdot \left(5 \cdot 3^2\right) = 5^2\,3^2 = (5 \cdot 3)^2$, cioè $5 \cdot 45 = n^2$ con $n = 5 \cdot 3 = 15$.

[2] — Dobbiamo determinare tutti i possibili valori di $x \in \mathbb{Z}$ che soddisfino simultaneamente le seguenti tre condizioni:

$$137\,x \;\equiv\; -54 \pmod{11}\;,\qquad -\overline{103}\,\overline{x} \;=\; \overline{47} \text{ in } \mathbb{Z}_9\;,\qquad \exists\; y \in \mathbb{Z} \;:\; 83\,x + 15\,y \;=\; 503$$

A tal fine, osserviamo che la prima è che x sia soluzione di una certa equazione congruenziale. La seconda condizione è che la classe di x in $\mathbb{Z}_9$ sia soluzione di una certa equazione modulare, che equivale ad una equazione congruenziale, precisamente $-103\,x \;\equiv\; 47 \pmod{9}$. La terza condizione infine è che x sia parte di una coppia di interi $(x\,,y) \in \mathbb{Z}\times Z$ che sia soluzione dell'equazione diofantea $83\,x + 15\,y \;=\; 503$, e questo a sua volta equivale a che x sia soluzione dell'equazione congruenziale $83\,x \;\equiv\; 503 \pmod{15}$. Pertanto, in definitiva risolvere il problema assegnato equivale a risolvere il sistema di equazioni congruenziali

$$\circledast \;:\; \begin{cases} 137\,x \;\equiv\; -54 \pmod{11} \\ -103\,x \;\equiv\; 47 \pmod{9} \\ 83\,x \;\equiv\; 503 \pmod{15} \end{cases} \tag{10}$$

Per risolvere il sistema (10), per prima cosa, in ciascuna equazione congruenziale ogni numero può essere sostituito con un altro ad esso congruente (modulo il numero che fa da modulo — scusate la ripetizione! — nella specifica equazione in esame). Procedendo in questo modo, e osservando che

$$\begin{array}{rcl} 137 \equiv 5 \pmod{11}\;, & \qquad & -54 \equiv 1 \equiv 45 \pmod{11} \\ -103 \equiv 5 \pmod{9}\;, & & 47 \equiv 2 \equiv 20 \pmod{9} \\ 83 \equiv 8 \pmod{15}\;, & & 503 \equiv 8 \pmod{15} \end{array}$$

il nostro sistema si trasforma in

$$\circledast' \;:\; \begin{cases} 5\,x \;\equiv\; 45 \pmod{11} \\ 5\,x \;\equiv\; 20 \pmod{9} \\ 8\,x \;\equiv\; 8 \pmod{15} \end{cases}$$

che è un sistema in cui ciascuna singola equazione ha una soluzione ovvia, così che in definitiva troviamo

$$\circledast'' \; : \; \begin{cases} x \equiv 9 \pmod{11} \\ x \equiv 4 \pmod{9} \\ x \equiv 1 \pmod{15} \end{cases} \tag{11}$$

si noti ora che il sistema $\circledast''$, che è *in forma cinese* — cioè le singole equazioni sono già risolte — *ma* i moduli *non* sono a due a due doprimi perché abbiamo $\mathrm{MCD}(9\,,15) = 3 \neq 1\,$, quindi *non si può applicare il Teorema Cinese del Resto*. Procediamo allora, invece, a risolvere il sistema $\circledast''$ per sostituzioni successive.

Cominciamo risolvendo la prima equazione congruenziale in (11) — che in effetti è già risolta... — e sostituiamo i valori trovati nella seconda e nella terza: questo dà un nuovo sottosistema di due equazioni congruenziali, che risolviamo a sua volta; iterando il procedimento, dopo un numero finito di passi troviamo il risultato finale. In dettaglio, abbiamo:

$$\circledast'' \; : \; \begin{cases} x \equiv 9 \pmod{11} \\ x \equiv 4 \pmod{9} \\ x \equiv 1 \pmod{15} \end{cases} \implies \begin{cases} x = 9 + 11\,h \;\; \big(h \in \mathbb{Z}\big) \\ 9 + 11\,h \equiv 4 \pmod{9} \\ 9 + 11\,h \equiv 1 \pmod{15} \end{cases} \implies$$

$$\implies \begin{cases} x = 9 + 11\,h \;\; \big(h \in \mathbb{Z}\big) \\ 2\,h \equiv 4 \pmod{9} \\ -4\,h \equiv -8 \pmod{15} \end{cases} \implies \begin{cases} x = 9 + 11\,h \;\; \big(h \in \mathbb{Z}\big) \\ h \equiv 2 \pmod{9} \\ h \equiv 2 \pmod{15} \end{cases} \implies$$

$$\implies \begin{cases} x = 9 + 11\,h \;\; \big(h \in \mathbb{Z}\big) \\ h = 2 + 9\,k \;\; \big(k \in \mathbb{Z}\big) \\ 2 + 9\,k \equiv 2 \pmod{15} \end{cases} \implies \begin{cases} x = 9 + 11\,h \;\; \big(h \in \mathbb{Z}\big) \\ h = 2 + 9\,k \;\; \big(k \in \mathbb{Z}\big) \\ 9\,k \equiv 0 \pmod{15} \end{cases} \implies$$

$$\implies \begin{cases} x = 9 + 11\,h \;\; \big(h \in \mathbb{Z}\big) \\ h = 2 + 9\,k \;\; \big(k \in \mathbb{Z}\big) \\ 3\,k \equiv 0 \pmod{5} \end{cases} \implies \begin{cases} x = 9 + 11\,h \;\; \big(h \in \mathbb{Z}\big) \\ h = 2 + 9\,k \;\; \big(k \in \mathbb{Z}\big) \\ k \equiv 0 \pmod{5} \end{cases} \implies$$

$$\implies \begin{cases} x = 9 + 11\,h \;\; \big(h \in \mathbb{Z}\big) \\ h = 2 + 9\,k \;\; \big(k \in \mathbb{Z}\big) \\ k = 5\,\ell \;\; \big(\ell \in \mathbb{Z}\big) \end{cases} \implies$$

$$\implies \qquad x \;=\; 9 + 11\,h \;=\; 9 + 11\,(2 + 9\,k) = \; 9 + 11\,(2 + 9 \cdot 5\,\ell\,) = 31 + 495\,\ell \quad \big(\ell \in \mathbb{Z}\big)$$

dunque la conclusione è

$$x \;=\; 31 + 495\,\ell \quad \big(\,\forall\, \ell \in \mathbb{Z}\,\big)$$

oppure, descrivendo lo stesso insieme di soluzioni in modalità differente,

$$x \;\equiv\; 31 \pmod{495}$$

In altri termini, l'insieme di tutte le soluzioni del sistema $\circledast''$ in (11), e quindi del sistema (10) equivalente al problema in esame, è il sottoinsieme di $\mathbb{Z}$ dato dalla classe di congruenza — che scriviamo anche come "classe laterale" per la somma — $[31]_{\equiv_{495}} = 31 + 495\,\mathbb{Z}\,$.

[3] — Ricordiamo la notazione: A è un anello commutativo unitario, $U(A)$ il gruppo dei suoi elementi invertibili, $Aff(A) := \left\{ Y_{a,b} \,\middle|\, a \in U(A)\,, b \in A \right\}$ è il sottoinsieme di applicazioni da A in sé stesso definite da $Y_{a,b}(x) := a\,x + b$ (per ogni $x \in A$) per ogni $(a,b) \in U(A) \times A$. Affrontiamo i vari quesiti uno alla volta.

(a) Dobbiamo dimostrare che $Aff(A) \subseteq \mathcal{S}(A)$, cioè che ciascuna funzione $Y_{a,b}$ è biiettiva, oppure (equivalentemente) è invertibile; vediamo sia l'una che l'altra dimostrazione.

$Y_{a,b}$ è biiettiva: Infatti, l'iniettività si prova come segue: se per $x_1, x_2 \in A$ abbiamo $Y_{a,b}(x_1) = Y_{a,b}(x_2)$, allora

$$\begin{aligned} a\,x_1 + b =: Y_{a,b}(x_1) \,=\, Y_{a,b}(x_2) := a\,x_2 + b \;\;&\Longrightarrow\;\; a\,x_1 + b = a\,x_2 + b \;\;\Longrightarrow \\ &\Longrightarrow\;\; a\,x_1 = a\,x_2 \;\;\Longrightarrow\;\; a^{-1}\,a\,x_1 = a^{-1}\,a\,x_2 \;\;\Longrightarrow\;\; x_1 \,=\, x_2 \end{aligned}$$

dunque $Y_{a,b}(x_1) = Y_{a,b}(x_2) \implies x_1 = x_2$, che significa esattamente che $Y_{a,b}$ è iniettiva.

D'altra parte, la suriettività di $Y_{a,b}$ si prova così: per ogni $\alpha \in A$, esiste effettivamente un (unico!) $x \in A$ tale che $Y_{a,b}(x) = \alpha$, precisamente $x = a^{-1}\,(\alpha - b)$, in quanto

$$Y_{a,b} = \alpha \iff a\,x + b = \alpha \iff x = a^{-1}\,(\alpha - b) \tag{12}$$

$Y_{a,b}$ è invertibile: Infatti, la formula (12) ci dice in altri termini che la funzione $Y'_{a,b} : A \longrightarrow A$ definita da $Y'_{a,b}(y) := a^{-1}\,(y - b) = a^{-1}\,y - a^{-1}\,b$ è proprio la funzione inversa di $Y_{a,b}$, perché

$$\big(Y'_{a,b} \circ Y_{a,b}\big)(x) = x \quad \forall\, x \in A \qquad \Longrightarrow \qquad Y'_{a,b} \circ Y_{a,b} = id_A$$

e analogamente

$$\big(Y_{a,b} \circ Y'_{a,b}\big)(y) = y \quad \forall\, y \in A \qquad \Longrightarrow \qquad Y_{a,b} \circ Y'_{a,b} = id_A$$

Si noti anche che $Y'_{a,b} = Y_{a^{-1},-a^{-1}b}$, quindi in particolare abbiamo anche

$$Y_{a,b}^{-1} \,=\, Y'_{a,b} \,=\, Y_{a^{-1},-a^{-1}b} \,\in\, Aff(A) \tag{13}$$

(b) Dobbiamo dimostrare che $Aff(A)$ è un sottogruppo del gruppo $\big(\mathcal{S}(A)\,;\circ\big)$, il che equivale a provare che tale sottoinsieme di $\mathcal{S}(A)$ è non vuoto, chiuso rispetto al prodotto (a composizione di funzioni), e chiuso per l'inverso.

In prima istanza, $Aff(A)$ è non vuoto, perché ad esempio $Aff(A) \ni Y_{1,0} = id_A$.

Come secondo punto, $Aff(A)$ è chiuso rispetto al prodotto perché il seguente calcolo

$$\begin{aligned} \big(Y_{a',b'} \circ Y_{a'',b''}\big)(x) \,&=\, Y_{a',b'}\big(Y_{a'',b''}(x)\big) \,=\, a'\,\big(a''\,x + b''\big) + b' \,= \\ &=\, \big(a'\,a''\big)\,x + \big(a'\,b'' + b'\big) \,=\, Y_{a'\,a'',\,a'\,b''+b'}(x)\;, \qquad \forall\, x \in A \end{aligned}$$

ci dice che

$$Y_{a',b'} \circ Y_{a'',b''} \,=\, Y_{a'\,a'',\,a'\,b''+b'} \,\in\, Aff(A) \tag{14}$$

per ogni $\big(a',b'\big), \big(a'',b''\big) \in U(A) \times A$.

In terza battuta, $Aff(A)$ è chiuso rispetto all'inverso, perché la (13) ci dice proprio che la funzione inversa di una in $Aff(A)$, dunque di una della forma $Y_{a,b}$, è a sua volta della forma $Y_{a',b'} \in Aff(A)$, precisamente con $a' = a^{-1}$ e $b' = -a^{-1}\,b$.

(c) Per dimostrare che $O(A) := \left\{ Y_{a,0} \,\middle|\, a \in U(A) \right\}$ è un sottogruppo di $\big(Aff(A)\,;\circ\big)$, procediamo come al punto *(b)*, dimostrando che è non vuoto, chiuso rispetto al prodotto e chiuso rispetto all'inverso.

Per costruzione abbiamo $O(A) \ni Y_{1,0} = id_A$, quindi $O(A)$ non è vuoto, q.e.d.

Applicando la (14) a due elementi di $O(A)$ otteniamo

$$Y_{a',0} \circ Y_{a'',0} \;=\; Y_{a'\,a'',\,0} \;\in\; O(A)$$

per ogni $a', a'' \in U(A)$, perciò $O(A)$ è chiuso rispetto al prodotto, q.e.d.

Infine, applicando la (13) a un qualsiasi elemento di $O(A)$ otteniamo

$$Y_{a,0}^{-1} \;=\; Y_{a^{-1},\,0} \;\in\; O(A)$$

per ogni $a \in U(A)$, dunque $O(A)$ è chiuso rispetto all'inverso, q.e.d.

(d) Dovendo dimostrare che $T(A) := \left\{ Y_{1,b} \,\middle|\, b \in A \right\}$ è un sottogruppo normale di $\big(Aff(A)\,;\circ\big)$, possiamo seguire due metodi diversi:

<u>*Primo metodo*</u>: Possiamo procedere come ai punti *(b)* e *(c)* per dimostrare che $T(A)$ è un sottogruppo, e poi in aggiunta verificare che esso soddisfa anche la condizione di normalità, considerata nella forma $g\,n\,g^{-1} \in T(A)$ per ogni $n \in T(A)$ e $g \in Aff(A)$.

Per prima cosa, per costruzione si ha $T(A) \ni Y_{1,0} = id_A$, quindi $T(A)$ non è vuoto, q.e.d. A seguire, applicando la (14) a due elementi di $T(A)$ otteniamo

$$Y_{1,b'} \circ Y_{1,b''} \;=\; Y_{1,\,b'+b''} \;\in\; T(A)$$

per ogni $b', b'' \in A$, perciò $T(A)$ è chiuso rispetto al prodotto, q.e.d. Infine, applicando la (13) a un qualsiasi elemento di $T(A)$ si ottiene

$$Y_{1,b}^{-1} \;=\; Y_{1,-b} \;\in\; T(A)$$

per ogni $b \in A$, dunque $T(A)$ è anche chiuso rispetto all'inverso, q.e.d. Questi tre fatti complessivamente dimostrano che $T(A)$ è sottogruppo di $Aff(A)$.

Dimostriamo ora che il sottogruppo $T(A)$ soddisfa anche la condizione di normalità

$$g\,n\,g^{-1} \;\in\; T(A) \qquad \forall \;\; n \in T(A)\,,\;\; g \in Aff(A) \tag{15}$$

Ora, un generico elemento $n \in T(A)$ è della forma $n = Y_{1,\beta}$ — con $\beta \in A$ — mentre un generico elemento $g \in Aff(A)$ ha forma $g = Y_{a,b}$ — con $(a,b) \in U(A) \times A$. Per tali elementi, sfruttando la (13) e la (14) il calcolo diretto ci dà

$$\begin{aligned} Y_{a,b} \circ Y_{1,\beta} \circ Y_{a,b}^{-1} \;&=\; Y_{a,b} \circ Y_{1,\beta} \circ Y_{a^{-1},\,-a^{-1}b} \;=\; Y_{a\cdot 1,\,a\,\beta+b} \circ Y_{a^{-1},\,-a^{-1}b} \;= \\ &=\; Y_{a\cdot 1\cdot a^{-1},\,(a\cdot 1)(-a^{-1}b)+(a\,\beta+b)} \;=\; Y_{1,\,-b+a\,\beta+b} \;=\; Y_{1,\,a\,\beta} \end{aligned}$$

quindi in sintesi $Y_{a,b} \circ Y_{1,\beta} \circ Y_{a,b}^{-1} \;=\; Y_{1,\,a\,\beta} \;\in\; T(A)$, così che la (15) è soddisfatta, q.e.d.

Secondo metodo: Ricordando che i sottogruppi normali di un gruppo G sono tutti e soli i nuclei dei morfismi che hanno G come dominio, cerchiamo di trovare un morfismo di gruppi avente per dominio $Aff(A)$, dunque del tipo $\phi : Aff(A) \longrightarrow \Gamma$ dove Γ sia un gruppo opportuno, tale che $Ker(\phi) = T(A)$. Se ci riusciremo, potremo concludere che $T(A)$, essendo il nucleo di un morfismo tra gruppi, è senz'altro un sottogruppo normale, senza bisogno di ulteriori verifiche.

Ora, consideriamo la funzione

$$\phi : Aff(A) \longrightarrow U(A) \ , \quad Y_{a,b} \mapsto \phi(Y_{a,b}) := a \qquad \forall \ Y_{a,b} \in Aff(A)$$

Dalla definizione segue subito che

$$Ker(\phi) \ := \ \phi^{-1}(1) \ = \ \big\{ Y_{a,b} \in Aff(A) \,\big|\, \phi\big(Y_{a,b}\big) = 1 \big\} \ = \\ = \ \big\{ Y_{a,b} \in Aff(A) \,\big|\, a = 1 \big\} \ = \ \big\{ Y_{1,b} \,\big|\, b \in A \big\} \ =: \ T(A)$$

cioè in sintesi $Ker(\phi) = T(A)$. Inoltre, la funzione ϕ è un morfismo di gruppi: infatti dalla definizione e dalla (14) otteniamo

$$\phi\big(Y_{a',b'} \circ Y_{a'',b''}\big) \ = \ \phi\big(Y_{a'\,a'',\,a'\,b''+b'}\big) \ = \ a'\,a'' \ = \ \phi\big(Y_{a',b'}\big) \cdot \phi\big(Y_{a'',b''}\big)$$

per ogni $Y_{a',b'}, Y_{a'',b''} \in Aff(A)$, il che significa esattamente che ϕ è un morfismo. Ma allora ϕ è un morfismo di gruppi con nucleo $Ker(\phi) = T(A)$, e quindi come già spiegato possiamo concludere che $T(A)$ è sottogruppo normale di $Aff(A)$, q.e.d.

(e) Dobbiamo dimostrare che la funzione $h : O(A) \times T(A) \longrightarrow Aff(A)$ definita da $\big(Y_{a,0}\,, Y_{1,b}\big) \mapsto Y_{a,0} \circ Y_{1,b}$ è biiettiva. Questa è una mera verifica, che segue da calcoli diretti che sfruttano la forma esplicita del prodotto in $Aff(A)$ data dalla formula in (14).

In dettaglio, sfruttando la (14) la suddetta funzione si riscrive nella forma

$$h : O(A) \times T(A) \longrightarrow Aff(A) \ , \quad \big(Y_{a,0}\,, Y_{1,b}\big) \ \mapsto \ Y_{a,0} \circ Y_{1,b} \ = \ Y_{a\,\cdot 1\,,\,ab+0} \ = \ Y_{a\,,\,ab} \quad (16)$$

Possiamo ora dimostrare che tale funzione è biiettiva seguendo due approcci diversi:

Primo Approccio: Dimostriamo che la funzione h in (16) è biettiva in modo *diretto*, cioè provando che è iniettiva e suriettiva:

Iniettività: Consideriamo due coppie $\big(Y_{a',0}\,, Y_{1,b'}\big)$ e $\big(Y_{a'',0}\,, Y_{1,b''}\big)$ in $O(A) \times T(A)$ che abbiano la stessa immagine per la nostra funzione, dunque $Y_{a',\,a'b'} = Y_{a'',\,a''b''}$: vogliamo dimostrare che allora è $Y_{a',\,b'} = Y_{a'',\,b''}$. Ora, da $Y_{a',\,a'b'} = Y_{a'',\,a''b''}$ otteniamo in particolare

$$a'b' \ = \ a' \cdot 0 + a'b' \ = \ Y_{a',\,a'b'}(0) \ = \ Y_{a'',\,a''b''}(0) \ = \ a'' \cdot 0 + a''b'' \ = \ a''b''$$

cioè $a'b' = a''b''$, e anche

$$a' + a'b' \ = \ a' \cdot 1 + a'b' \ = \ Y_{a',\,a'b'}(1) \ = \ Y_{a'',\,a''b''}(1) \ = \ a'' \cdot 1 + a''b'' \ = \ a'' + a''b''$$

cioè $a' + a'b' = a'' + a''b''$. Ma allora

$$\begin{cases} a'b' \ = \ a''b'' \\ a' + a'b' \ = \ a'' + a''b'' \end{cases} \implies \begin{cases} a'b' \ = \ a''b'' \\ a' \ = \ a'' \end{cases} \implies \begin{cases} b' \ = \ b'' \\ a' \ = \ a'' \end{cases} \implies Y_{a',\,b'} \ = \ Y_{a'',\,b''}$$

— dove nel penultimo passaggio si sfrutta il fatto che a' e a'' sono invertibili.

Suriettività: Per ogni $Y_{a,b} \in Aff(A)$, vogliamo dimostrare che esiste una coppia $\big(Y_{\alpha,0}\,,Y_{1,\beta}\big) \in O(A) \times T(A)$ tale che $\big(Y_{\alpha,0}\,,Y_{1,\beta}\big) \mapsto Y_{a,b}$, cioè tale che $Y_{\alpha\,,\,\alpha\beta} = Y_{a,b}$.

Ora, procedendo come prima si ha che $Y_{\alpha\,,\,\alpha\beta} = Y_{a,b}$ implicherebbe in particolare

$$\alpha\beta \;=\; \alpha\cdot 0 + \alpha\beta \;=\; Y_{\alpha,\,\alpha\beta}(0) \;=\; Y_{a,\,b}(0) \;=\; a\cdot 0 + b \;=\; b$$

cioè $\alpha\beta = b$, e anche

$$\alpha + \alpha\beta \;=\; \alpha\cdot 1 + \alpha\beta \;=\; Y_{\alpha,\,\alpha\beta}(1) \;=\; Y_{a,\,b}(1) \;=\; a\cdot 1 + b \;=\; a + b$$

cioè $\alpha + \alpha\beta = a + b$. Ma allora

$$\begin{cases} \alpha\beta = b \\ \alpha + \alpha\beta = a + b \end{cases} \Longrightarrow \begin{cases} \alpha\beta = b \\ \alpha = a \end{cases} \Longrightarrow \begin{cases} \beta = a^{-1}b \\ \alpha = a \end{cases} \Longrightarrow \big(Y_{\alpha\,,\,0}\,,Y_{1\,,\,\beta}\big) \;=\; \big(Y_{a,\,0}\,,Y_{1\,,\,a^{-1}b}\big)$$

— dove nel penultimo passaggio si sfrutta il fatto che $a = \alpha$ sia invertibile, per definizione. L'ultima formula ci dice che una coppia $Y_{\alpha,\beta} \in O(A) \times T(A)$ che soddisfi la nostra richiesta dev'essere necessariamente della forma $\big(Y_{\alpha,\,0}\,,Y_{1\,,\,\beta}\big) = \big(Y_{a,\,0}\,,Y_{1\,,\,a^{-1}b}\big)$. D'altra parte, il procedimento si inverte, e la coppia $\big(Y_{a,\,0}\,,Y_{1\,,\,a^{-1}b}\big)$ effettivamente soddisfa la condizione $\big(Y_{a,\,0}\,,Y_{1\,,\,a^{-1}b}\big) \mapsto Y_{a,b}$, come si verifica immediatamente. Pertanto, la funzione considerata è suriettiva, q.e.d.

Secondo Approccio: Dimostriamo che la funzione h in (16) è biettiva in modo *indiretto*, cioè provando che è invertibile, perché ne esibiamo esplicitamente la funzione inversa. A tal fine, consideriamo la funzione

$$k : Aff(A) \longrightarrow O(A) \times T(A) \quad , \qquad Y_{a\,,\,b} \;\mapsto\; \big(Y_{a,0}\,,Y_{1,a^{-1}b}\big) \tag{17}$$

e dimostriamo che tale funzione è l'inversa della funzione h in (16) provando che

$$h \circ k = id_{Aff(A)} \qquad \text{e} \qquad k \circ h = id_{O(A)\times T(A)} \tag{18}$$

Infatti, il calcolo diretto ci dà

$$(h\circ k)\big(Y_{a\,,\,b}\big) \;=\; h\big(k\big(Y_{a\,,\,b}\big)\big) \;=\; h\big(\big(Y_{a,0}\,,Y_{1,a^{-1}b}\big)\big) \;=\; Y_{a\cdot 1\,,\,a\,a^{-1}\,b} \;=\; Y_{a\,,\,b} \;=\; id_{Aff(A)}\big(Y_{a\,,\,b}\big)$$

per ogni $Y_{a\,,\,b} \in Aff(A)$, il che dimostra l'identità di sinistra in (18). Analogamente

$$\begin{aligned}(k\circ h)\big(Y_{a,0}\,,Y_{1,b}\big) \;&=\; k\big(h\big(Y_{a,0}\,,Y_{1,b}\big)\big) \;=\; k\big(Y_{a,ab}\big) \;= \\ &=\; \big(Y_{a,0}\,,Y_{1,a^{-1}(ab)}\big) \;=\; \big(Y_{a,0}\,,Y_{1,b}\big) \;=\; id_{O(A)\times T(A)}\big(Y_{a,0}\,,Y_{1,b}\big)\end{aligned}$$

per ogni $\big(Y_{a,0}\,,Y_{1,b}\big) \in O(A) \times T(A)$, e questo dimostra l'identità di destra in (18).

[4] — Rispondiamo ai diversi quesiti uno alla volta

(a) Ricordiamo che un sottoinsieme S di un anello R è un sottoanello se e soltanto se *(1)* S è non vuoto, *(2)* S è chiuso per alla differenza, *(3)* S è chiuso per il prodotto.

Andiamo dunque a verificare queste tre proprietà nel caso del sottoinsieme

$$S \;:=\; M_2^{(\alpha)}(A) \;:=\; \left\{ \left(\begin{array}{cc} u+v & u \\ \alpha\, u & v \end{array} \right) \in M_2(A) \;\middle|\; u\,,v \in A \right\}$$

nell'anello $R := M_2(A)$.

La *(1)* è soddisfatta perché certamente abbiamo $M_2^{(\alpha)}(A) \ni \left(\begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array} \right)$ — corrispondente alla scelta $u := 0$ e $v := 0$.

La *(2)* è soddisfatta perché per la differenza di due elementi in $M_2^{(\alpha)}(A)$ abbiamo

$$\left(\begin{array}{cc} u'+v' & u' \\ \alpha\, u' & v' \end{array} \right) - \left(\begin{array}{cc} u''+v'' & u'' \\ \alpha\, u'' & v'' \end{array} \right) \;=\; \left(\begin{array}{cc} \big(u'+v'\big) - \big(u''-v''\big) & u'-u'' \\ \alpha\, u' - \alpha\, u'' & v'-v'' \end{array} \right) \;=$$

$$= \left(\begin{array}{cc} \big(u'-u''\big) + \big(v'-v''\big) & u'-u'' \\ \alpha\,\big(u'-u''\big) & v'-v'' \end{array} \right)$$

e l'ultima è chiaramente una matrice appartenente a $M_2^{(\alpha)}(A)$, q.e.d.

Infine la *(3)* è soddisfatta perché per il prodotto (righe per colonne) di due generici elementi in $M_2^{(\alpha)}(A)$ abbiamo

$$\left(\begin{array}{cc} u'+v' & u' \\ \alpha\, u' & v' \end{array} \right) \cdot \left(\begin{array}{cc} u''+v'' & u'' \\ \alpha\, u'' & v'' \end{array} \right) \;=\; \left(\begin{array}{cc} \big(u'+v'\big)\big(u''+v''\big) + u'\,\alpha\, u'' & \big(u'+v'\big)u'' + u'\,v'' \\ \alpha\, u'\,\big(u''+v''\big) + v'\,\alpha\, u'' & \alpha\, u'\, u'' + v'\, v'' \end{array} \right) =$$

$$= \left(\begin{array}{cc} \Big(\big(u'+v'\big)u'' + u'\,v'' \Big) + \big(\alpha\, u'\, u'' + v'\, v''\big) & \big(u'+v'\big)u'' + u'\,v'' \\ \alpha\,\Big(\big(u'+v'\big)u'' + u'\,v'' \Big) & \alpha\, u'\, u'' + v'\, v'' \end{array} \right)$$

e di nuovo vediamo che l'ultima matrice è effettivamente appartenente a $M_2^{(\alpha)}(A)$, q.e.d.

(b) Il calcolo diretto — già svolto in precedenza trattando il punto *(a)* — ci mostra che per due generici elementi di $M_2^{(\alpha)}(A)$ si ha

$$\left(\begin{array}{cc} u'+v' & u' \\ \alpha\, u' & v' \end{array} \right) \cdot \left(\begin{array}{cc} u''+v'' & u'' \\ \alpha\, u'' & v'' \end{array} \right) \;=$$

$$= \left(\begin{array}{cc} \Big(\big(u'+v'\big)u'' + u'\,v'' \Big) + \big(\alpha\, u'\, u'' + v'\, v''\big) & \big(u'+v'\big)u'' + u'\,v'' \\ \alpha\,\Big(\big(u'+v'\big)u'' + u'\,v'' \Big) & \alpha\, u'\, u'' + v'\, v'' \end{array} \right)$$

e quindi poi invertendo l'ordine dei fattori

$$\left(\begin{array}{cc} u''+v'' & u'' \\ \alpha\, u'' & v'' \end{array} \right) \cdot \left(\begin{array}{cc} u'+v' & u' \\ \alpha\, u' & v' \end{array} \right) \;=$$

$$= \left(\begin{array}{cc} \Big(\big(u''+v''\big)u' + u''\,v' \Big) + \big(\alpha\, u''\, u' + v''\, v'\big) & \big(u''+v''\big)u' + u''\,v' \\ \alpha\,\Big(\big(u''+v''\big)u' + u''\,v' \Big) & \alpha\, u''\, u' + v''\, v' \end{array} \right)$$

A questo punto il confronto diretto — ricordando che il prodotto in A è commutativo — ci mostra che

$$\left(\begin{array}{cc} u'+v' & u' \\ \alpha\, u' & v' \end{array} \right) \cdot \left(\begin{array}{cc} u''+v'' & u'' \\ \alpha\, u'' & v'' \end{array} \right) \;=\; \left(\begin{array}{cc} u''+v'' & u'' \\ \alpha\, u'' & v'' \end{array} \right) \cdot \left(\begin{array}{cc} u'+v' & u' \\ \alpha\, u' & v' \end{array} \right)$$

e quindi concludiamo che il sottoanello $M_2^{(\alpha)}(A)$ è commutativo, q.e.d.

(c) Ricordiamo che un sottoanello R' di un anello R è un ideale (bilatero) se si ha che $R'\,R \subseteq R'$ e $R\,R' \subseteq R'$. Nel caso di $R' := M_2^{(\alpha)}(A)$ e $R := M_2(A)$, consideriamo ad esempio il prodotto

$$\begin{pmatrix} 1+0 & 1 \\ \alpha\cdot 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \;=\; \begin{pmatrix} 0 & 1 \\ 0 & \alpha\,1 \end{pmatrix}$$

dove il prodotto di sinistra appartiene a $M_2^{(\alpha)}(A)\cdot M_2(A)$, perché ha il primo fattore in: dal risultato ottenuto osserviamo che la matrice ottenuta appartiene a sua volta a $M_2^{(\alpha)}(A)$ se e soltanto se $0 = \alpha\cdot 1$ e $0 = 1+\alpha\cdot 1$, cioè se e soltanto se $\alpha = 0$ e $0 = 1$. Pertanto, a meno di essere nel caso banale (cioè quando $0 = 1$) si ha sempre $\begin{pmatrix} 1+0 & 1 \\ \alpha\cdot 1 & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \notin M_2^{(\alpha)}(A)$: perciò concludiamo che $M_2^{(\alpha)}(A)\cdot M_2(A) \not\subseteq M_2^{(\alpha)}(A)$, quindi $M_2^{(\alpha)}(A)$ *non* è ideale dell'anello $M_2(A)$, q.e.d.

[5] — Ricordiamo i due polinomi in $\mathbb{Q}[x]$ sotto esame

$$p(x) \;:=\; x^4 - 1 \quad , \qquad q(x) \;:=\; x^4 - 3\,x^3 + 3\,x - 1$$

e affrontiamo separatamente i diversi quesiti.

(a) Per determinare il M.C.D.$\big(p(x)\,,q(x)\big)$ possiamo seguire due metodi.

Primo Metodo (tramite metodo euclideo): Ricordiamo che l'anello $\mathbb{Q}[\,x\,]$ dei polinomi a coefficienti in $\mathbb{Q}$ è *euclideo*, con valutazione data dal grado, indicato con ∂; in particolare, tale valutazione è *additiva*, cioè si ha $\partial\big(\alpha(x)\,\beta\big) = \partial\big(\alpha(x)\big)\,\partial\big(\beta(x)\big)$ per ogni $\alpha(x)\,,\beta(x) \in \mathbb{Q}[\,x\,]$. Possiamo allora utilizzare il *metodo euclideo delle divisioni successive* per determinare il M.C.D.$\big(p(x)\,,q(x)\big)$; inoltre, i calcoli effettuati per questo procedimento saranno utili più avanti per rispondere al quesito in *(c)*.

I calcoli espliciti — per l'algoritmo euclideo delle divisioni successive — sono

$$\begin{aligned} x^4 - 1 \;&=\; \big(x^4 - 3\,x^3 + 3\,x - 1\big)\,1 \;+\; \big(3\,x^3 - 3\,x\,\big) \\ x^4 - 3\,x^3 + 3\,x - 1 \;&=\; \big(3\,x^3 - 3\,x\,\big)\,\big(3^{-1}x - 1\big) \;+\; \big(x^2 - 1\big) \\ 3\,x^3 - 3\,x \;&=\; \big(x^2 - 1\big)\,3\,x \end{aligned}$$

da cui otteniamo che M.C.D.$\big(x^2 - 1\big)$.

Secondo Metodo (tramite fattorizzazione): Essendo un dominio euclideo, l'anello $\mathbb{Q}[\,x\,]$ è anche un dominio a fattorizzazione unica: pertanto, il M.C.D.$\big(p(x)\,,q(x)\big)$ può essere caratterizzato come il prodotto dei fattori irriducibili comuni a entrambi $p(x)$ e $q(x)$ — in fattorizzazioni di entrambi in irriducibili — elevati all'esponente più basso che figuri nelle due fattorizzazioni di tali polinomi. Perciò per determinare tale M.C.D.$\big(p(x)\,,q(x)\big)$ abbiamo bisogno di fattorizzare in irriducibili i due polinomi $p(x)$ e $q(x)$. Per $p(x)$ abbiamo

$$p(x) \;:=\; x^4 - 1 \;=\; \big(x^2 - 1\big)\big(x^2 + 1\big) \;=\; (x+1)(x-1)\big(x^2 + 1\big)$$

dove i fattori $(x+1)$, $(x-1)$ e $\big(x^2+1\big)$ sono irriducibili — i primi due perché hanno grado 1, il terzo perché se fosse riducibile avrebbe una radice, ma invece in $\mathbb{Q}$ una tale

radice non esiste perché $\kappa^2 \neq -1$ per ogni $\kappa \in \mathbb{Q}$. Per $q(x)$ abbiamo

$$q(x) := x^4 - 3\,x^3 + 3\,x - 1 = \big(x^4 - 1\big) - \big(3\,x^3 - 3\,x\big) =$$
$$= \big(x^2 - 1\big)\big(x^2 + 1\big) - \big(x^2 - 1\big)\,3\,x = \big(x^2 - 1\big)\big(x^2 - 3\,x + 1\big) = (x+1)(x-1)\big(x^2 - 3\,x + 1\big)$$

dove i fattori $(x + 1)$, $(x - 1)$ e $\big(x^2 - 3\,x + 1\big)$ sono irriducibili — i primi due perché hanno grado 1, il terzo perché se fosse riducibile avrebbe una radice, ma invece in $\mathbb{Q}$ una tale radice non esiste perché sarebbe $x = \dfrac{3 \pm \sqrt{5}}{2}$ e invece $\not\exists\, \sqrt{5} \in \mathbb{Q}$. In definitiva

$$p(x) = (x + 1)(x - 1)\big(x^2 + 1\big) \;, \qquad q(x) = (x + 1)(x - 1)\big(x^2 - 3\,x + 1\big)$$

sono le fattorizzazioni in irriducibili di $p(x)$ e $q(x)$ cercate: dal confronto tra queste troviamo allora

$$\text{M.C.D.}\big(\,p(x)\,,q(x)\big) = (x + 1)(x - 1) = x^2 - 1$$

come già trovato in precedenza col primo metodo.

(b) Per determinare il $\text{m.c.m.}\big(\,p(x)\,,q(x)\big)$ possiamo seguire due metodi diversi.

<u>*Primo Metodo:*</u> Dato che l'anello $\mathbb{Q}[\,x\,]$ è un dominio a fattorizzazione unica, sappiamo che il $\text{m.c.m.}\big(\,p(x)\,,q(x)\big)$ esiste ed è collegato al $\text{M.C.D.}\big(\,p(x)\,,q(x)\big)$ dalla relazione $\text{m.c.m.}\big(\,p(x)\,,q(x)\big)\,\text{M.C.D.}\big(\,p(x)\,,q(x)\big) = p(x)\,q(x)\,,$ da cui ricaviamo che

$$\text{m.c.m.}\big(\,p(x)\,,q(x)\big) = \frac{p(x)\,q(x)}{\text{M.C.D.}\big(\,p(x)\,,q(x)\big)}$$

siccome abbiamo già calcolato in precedenza il $\text{M.C.D.}\big(\,p(x)\,,q(x)\big)$, possiamo sfruttare tale identità per ottenere

$$\text{m.c.m.}\big(\,p(x)\,,q(x)\big) = \frac{p(x)\,q(x)}{\text{M.C.D.}\big(\,p(x)\,,q(x)\big)} = \frac{\big(x^4 - 1\big)\,\big(x^4 - 3\,x^3 + 3\,x - 1\big)}{x^2 - 1} =$$
$$= \frac{\big(x^4 - 1\big)}{x^2 - 1}\,\big(x^4 - 3\,x^3 + 3\,x - 1\big) = \big(x^2 + 1\big)\big(x^4 - 3\,x^3 + 3\,x - 1\big) = x^6 - 3\,x^5 + x^4 - x^2 + 3\,x - 1$$

dunque in conclusione troviamo

$$\text{m.c.m.}\big(\,p(x)\,,q(x)\big) = x^6 - 3\,x^5 + x^4 - x^2 + 3\,x - 1$$

<u>*Secondo Metodo (tramite fattorizzazione):*</u> Siccome l'anello $\mathbb{Q}[\,x\,]$ è un dominio euclideo, è anche un dominio a fattorizzazione unica: perciò il $\text{m.c.m.}\big(\,p(x)\,,q(x)\big)$ può essere caratterizzato come il prodotto di tutti i fattori irriducibili di $p(x)$ o di $q(x)$ — in fattorizzazioni di entrambi in irriducibili — elevati all'esponente più alto che figuri nelle due fattorizzazioni suddette. Ora, nel rispondere al quesito *(a)* tramite il primo metodo abbiamo gà trovato per $p(x)$ e $q(x)$ le seguenti fattorizzazioni in irriducibili

$$p(x) = (x + 1)(x - 1)\big(x^2 + 1\big) \;, \qquad q(x) = (x + 1)(x - 1)\big(x^2 - 3\,x + 1\big)$$

quindi in base all'analisi precedente otteniamo

$$\begin{aligned}\text{m.c.m.}\big(p(x)\,,q(x)\big) \;&=\; (x+1)(x-1)\big(x^2+1\big)\big(x^2-3\,x+1\big) \;= \\ &\big(x^4-1\big)\big(x^2-3\,x+1\big) \;=\; x^6-3\,x^5+x^4-x^2+3\,x-1\end{aligned}$$

dunque in conclusione abbiamo

$$\text{m.c.m.}\big(p(x)\,,q(x)\big) \;=\; x^6-3\,x^5+x^4-x^2+3\,x-1$$

che è lo stesso risultato già ottenuto col primo metodo.

(c) Dobbiamo determinare una identità di Bézout esplicita per $\text{M.C.D.}\big(p(x)\,,q(x)\big)$, cioè un'espressione della forma

$$\text{M.C.D.}\big(p(x)\,,q(x)\big) \;=\; r(x)\,p(x) \,+\, s(x)\,q(x) \tag{19}$$

per opportuni polinomi $r(x)\,,s(x) \in \mathbb{Q}[\,x\,]$. A tal fine possiamo seguire la procedura standard, riprendendo le formule per le divisioni trovate al punto *(a)* nel calcolo del $\text{M.C.D.}\big(p(x)\,,q(x)\big)$ con il primo metodo (cioè tramite l'algoritmo euclideo delle divisioni successive), che sono

$$\begin{aligned} x^4-1 \;&=\; \big(x^4-3\,x^3+3\,x-1\big)\cdot 1 \,+\, \big(3\,x^3-3\,x\big) \\ x^4-3\,x^3+3\,x-1 \;&=\; \big(3\,x^3-3\,x\big)\big(3^{-1}x-1\big) \,+\, \big(x^2-1\big) \\ 3\,x^3-3\,x \;&=\; \big(x^2-1\big)\,3\,x \end{aligned}$$

L'ultima identità la scartiamo, e dalla penultima in sù ricaviamo (rovesciando l'ordine)

$$\begin{aligned} x^4-3\,x^3+3\,x-1 \;&=\; \big(3\,x^3-3\,x\big)\big(3^{-1}x-1\big) \,+\, \big(x^2-1\big) \\ x^4-1 \;&=\; \big(x^4-3\,x^3+3\,x-1\big)\cdot 1 \,+\, \big(3\,x^3-3\,x\big) \end{aligned} \;\Longrightarrow$$

$$\Longrightarrow\; \begin{cases} x^2-1 \;=\; \big(x^4-3\,x^3+3\,x-1\big) \,-\, \big(3^{-1}x-1\big)\big(3\,x^3-3\,x\big) \\ 3\,x^3-3\,x \;=\; \big(x^4-1\big) \,-\, 1\cdot\big(x^4-3\,x^3+3\,x-1\big) \end{cases} \;\Longrightarrow$$

$$\begin{aligned}\Longrightarrow\quad x^2-1 \;&=\; \big(x^4-3\,x^3+3\,x-1\big) - \big(3^{-1}x-1\big)\Big(\big(x^4-1\big)-1\cdot\big(x^4-3\,x^3+3\,x-1\big)\Big) \;= \\ &=\; \big(-\,3^{-1}x+1\big)\big(x^4-1\big) \,+\, 3^{-1}x\,\big(x^4-3\,x^3+3\,x-1\big)\end{aligned}$$

dove l'ultimo passaggio ci dà

$$x^2-1 \;=\; \big(-\,3^{-1}x+1\big)\big(x^4-1\big) \,+\, 3^{-1}x\,\big(x^4-3\,x^3+3\,x-1\big)$$

che è proprio un'espressione di $\text{M.C.D.}\big(p(x)\,,q(x)\big)$ nella forma (19), come richiesto, con $r(x)=\big(-\,3^{-1}x+1\big)$ e $s(x)=3^{-1}x$.