

Istituzioni di Algebra e Geometria — Algebra, a.a. 2025-2026
Soluzioni foglio 10

1. Se $\alpha = \sqrt{3} + \sqrt{7}$ allora

$$\alpha^2 = 10 + 2\sqrt{21} \Rightarrow \alpha^4 - 20\alpha^2 + 100 = 84.$$

Deduciamo che $p(x) = x^4 - 20x^2 + 16$ ha α come radice. Inoltre tale polinomio si scomponga su \mathbb{R} come

$$p(x) = (x - \sqrt{10 - 2\sqrt{21}})(x - \sqrt{10 + 2\sqrt{21}})(x + \sqrt{10 - 2\sqrt{21}})(x + \sqrt{10 + 2\sqrt{21}}),$$

quindi ha $\pm\sqrt{10 \pm 2\sqrt{21}}$ come sue radici in \mathbb{R} .

Si noti che $x^2 - 21$ ha $\sqrt{21}$ come radice; per il criterio di Eisenstein è irriducibile in \mathbb{Z} , dunque in \mathbb{Q} , essendo primitivo. Concludiamo che il polinomio minimo di $\sqrt{21}$ su \mathbb{Q} è $x^2 - 21$, quindi $\sqrt{21} \notin \mathbb{Q}$. Allora $10 \pm 2\sqrt{21} \notin \mathbb{Q}$, dunque $\pm\sqrt{10 \pm 2\sqrt{21}} \notin \mathbb{Q}$. Quindi se $p(x)$ fosse riducibile su \mathbb{Q} , si dovrebbe scomporre in un prodotto di due polinomi di grado 2 a coefficienti in \mathbb{Q} : si verifica con un conto diretto che questo non è possibile. Concludiamo che $p(x) = x^4 - 20x^2 + 16$ è il polinomio minimo di α su \mathbb{Q} .

Se $\beta = \sqrt{1 + \sqrt{3}}$ allora

$$\beta^2 = 1 + \sqrt{3} \Rightarrow \beta^4 - 2\beta^2 + 1 = 3,$$

da cui deduciamo che il polinomio $q(x) = x^4 - 2x^2 - 2$ ha β come radice. Se mostriamo che è irriducibile su \mathbb{Q} , esso è il polinomio minimo cercato. Di nuovo, avendo a che fare con un polinomio primitivo, possiamo guardare la sua irriducibilità su \mathbb{Z} , e in particolare usare il primo criterio con $p = 5$. Mostriamo quindi che la riduzione di $q(x)$ modulo 5 è irriducibile su \mathbb{Z}_5 , e quindi $q(x)$ è irriducibile su \mathbb{Z} , e quindi su \mathbb{Q} . Osserviamo che $\overline{q(x)} = x^4 - \bar{2}x^2 - \bar{2}$ non ha radici in \mathbb{Z}_5 , quindi l'unico modo possibile di spezzarsi è quello di essere il prodotto di due polinomi di grado 2, che possono essere supposti monici. L'uguaglianza

$$(x^2 + \bar{a}x + \bar{b})(x^2 + \bar{c}x + \bar{d}) = x^4 - \bar{2}x^2 - \bar{2}$$

implica il seguente sistema di equazioni in \mathbb{Z}_5 :

$$\begin{cases} \bar{a} + \bar{c} = \bar{0} \\ \bar{d} + \bar{b} + \bar{a}\bar{c} = -\bar{2} \\ \bar{a}\bar{d} + \bar{b}\bar{c} = \bar{0} \\ \bar{b}\bar{d} = -\bar{2} \end{cases}$$

Quindi $\bar{c} = -\bar{a}$ e $\bar{a}(\bar{d} - \bar{b}) = \bar{0}$. Siamo in un dominio di integrità, quindi o $\bar{a} = \bar{0}$, e allora $\bar{c} = \bar{0}$ e $\bar{d} + \bar{b} = -\bar{2}$, e quindi $\bar{d}(\bar{d} + \bar{2}) = \bar{2}$, che però non ha soluzioni in \mathbb{Z}_5 , oppure $\bar{d} - \bar{b} = \bar{0}$ e $\bar{d}^2 = -\bar{2}$, che di nuovo non ha soluzioni in \mathbb{Z}_5 . Concludiamo che $q(x) = x^4 - 2x^2 - 2$ è il polinomio minimo di β su \mathbb{Q} .

Infine, se $\gamma = 1 - \sqrt[3]{5}$ allora

$$\gamma - 1 = -\sqrt[3]{5} \Rightarrow \gamma^3 - 3\gamma^2 + 3\gamma - 1 = -5,$$

da cui deduciamo che il polinomio $r(x) = x^3 - 3x^2 + 3x + 4$ ha γ come radice. Possiamo applicare il criterio 1 con primo $p = 7$ a $r(x)$: la sua riduzione $\bar{r}(x) \in \mathbb{Z}_7[x]$ è irriducibile perché non ha radici, e quindi $r(x)$ è un polinomio irriducibile su \mathbb{Z} , ed essendo primitivo, è irriducibile anche su \mathbb{Q} . Concludiamo che $r(x) = x^3 - 3x^2 + 3x + 4$ è il polinomio minimo di γ su \mathbb{Q} .

2. (a) Poiché per ipotesi $\alpha \in \mathbb{C}$ è algebrico su \mathbb{Q} , $K_\alpha = \mathbb{Q}[\alpha] \subseteq \mathbb{C}$ è un campo. Inoltre $[K_\alpha : \mathbb{Q}]$ coincide con il grado del polinomio minimo di α su \mathbb{Q} , che è 2 per ipotesi.
- (b) L'elemento β è algebrico su \mathbb{Q} : poiché il suo polinomio minimo ha coefficienti in $\mathbb{Q} \subseteq K_\alpha$, segue che β è anche algebrico su K_α con polinomio minimo di grado al più 2: come prima, deduciamo allora che $K_{\alpha,\beta} = K_\alpha[\beta] \subseteq \mathbb{C}$ è un sottocampo.

Abbiamo che $[K_\alpha : \mathbb{Q}] = 2$ e $[K_{\alpha,\beta} : K_\alpha] \leq 2$. Allora

$$[K_{\alpha,\beta} : \mathbb{Q}] = [K_{\alpha,\beta} : K_\alpha][K_\alpha : \mathbb{Q}]$$

può essere 0 o 2 o 4.

- (c) Sappiamo che $K_{\alpha,\beta} = K_\alpha[\beta]$ è un campo tale che $[K_{\alpha,\beta} : \mathbb{Q}] \leq 4$. Dal contenimento

$$\mathbb{Q} \subseteq K_{\alpha+\beta}, K_{\alpha\beta} \subseteq K_{\alpha,\beta}$$

$K_{\alpha+\beta}$ e $K_{\alpha\beta}$ sono estensioni finite di \mathbb{Q} , quindi $\alpha + \beta$ e $\alpha\beta$ sono algebrici su \mathbb{Q} . Osserviamo che $K_{\alpha+\beta}$ e $K_{\alpha\beta}$ sono sottospazi di $K_{\alpha,\beta}$. Inoltre

$$[K_{\alpha,\beta} : \mathbb{Q}] = [K_{\alpha,\beta} : K_{\alpha+\beta}][K_{\alpha+\beta} : \mathbb{Q}] = [K_{\alpha,\beta} : K_{\alpha\beta}][K_{\alpha\beta} : \mathbb{Q}],$$

quindi $[K_{\alpha+\beta} : \mathbb{Q}]$ e $[K_{\alpha\beta} : \mathbb{Q}]$ devono dividere $[K_{\alpha,\beta} : \mathbb{Q}]$.

3. (a) Cominciamo a dimostrare che $\alpha \in \mathbb{A}$, $\alpha \neq 0$, implica $\alpha^{-1} \in \mathbb{A}$. Supponiamo che α sia radice del polinomio

$$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Q}[x];$$

è immediato verificare che allora α^{-1} è radice di

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n \in \mathbb{Q}[x],$$

dunque $\alpha^{-1} \in \mathbb{A}$. Sia ora $\beta \in \mathbb{A}$ un altro elemento algebrico; per dimostrare che la somma $\alpha + \beta$ e il prodotto $\alpha\beta$ sono algebrici, osserviamo che la catena di inclusioni

$$\mathbb{Q} \subseteq K_{\alpha+\beta}, K_{\alpha\beta} \subseteq K_{\alpha,\beta}$$

che appare nella soluzione della parte (c) dell'esercizio 2 è vera a prescindere dal grado dei polinomi minimi di α e β . Quindi $K_{\alpha+\beta}$ e $K_{\alpha\beta}$ sono estensioni finite, e quindi algebriche.

Esistono anche costruzioni esplicite che, a partire dai due polinomi che hanno come radici α e β , forniscono polinomi che hanno come radice la somma $\alpha + \beta$ e il prodotto $\alpha\beta$, ma vanno oltre le cose che impariamo in questo corso.

- (b) Si noti che $\alpha \in \mathbb{A}$ se e solo se esiste $f(x) \in \mathbb{Z}[x]$ tale che $f(\alpha) = 0$. Infatti sappiamo che α è radice di un $g(x) \in \mathbb{Q}[x]$: moltiplicando $g(x)$ per un comune multiplo dei denominatori dei suoi coefficienti otteniamo il polinomio $f(x)$.

Per ogni $N \in \mathbb{N}$ si consideri l'insieme finito di polinomi

$$X_N = \left\{ \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x] \mid n + \sum_{i=0}^n |a_i| = N \right\},$$

e sia Y_N l'insieme di tutti gli $\alpha \in \mathbb{A}$ che sono radici di un qualche elemento di X_N : anche l'insieme Y_N è finito perché nessun polinomio in X_N è identicamente nullo. Poniamo infine

$$\mathbb{A}_N = Y_N \setminus \bigcup_{i=1}^{N-1} Y_i.$$

Gli insiemi \mathbb{A}_N sono finiti, disgiunti a coppie e $\bigcup_{N \in \mathbb{N}} \mathbb{A}_N = \mathbb{A}$. Poiché dunque l'insieme \mathbb{A} è un'unione numerabile di insiemi finiti, esso è numerabile.

4. (a) Osserviamo che $x^2 - 2 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ è monico, irriducibile su \mathbb{Z} per il criterio di Eisenstein, dunque su \mathbb{Q} , e ha $\sqrt{2}$ come radice: quindi coincide con il polinomio minimo di $\sqrt{2}$ su \mathbb{Q} . In particolare questo implica che $\sqrt{2} \notin \mathbb{Q}$.
- (b) Usiamo la notazione dell'esercizio 2 e chiamiamo $\mathbb{Q}[\sqrt{2}] = K_{\sqrt{2}}$; poiché $\sqrt{2}$ è un elemento algebrico su \mathbb{Q} , $K_{\sqrt{2}}$ è un campo i cui elementi si scrivono in modo unico nella forma $a + b\sqrt{2}$ con $a, b \in \mathbb{Q}$. Osserviamo che $(\sqrt{2})^{-1} = a + b\sqrt{2}$, se e solo se $1 = a\sqrt{2} + 2b$: concludiamo che deve essere $a = 0$, $b = 1/2$.
- (c) Se $\sqrt{3}$ fosse un elemento di $K_{\sqrt{2}}$, esisterebbero $a, b \in \mathbb{Q}$ tali che $\sqrt{3} = a + b\sqrt{2}$, dunque

$$3 - a^2 - 2b^2 = 2ab\sqrt{2}.$$

Ora, se $ab \neq 0$ allora

$$\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q},$$

in contraddizione con il fatto che $\sqrt{2} \notin \mathbb{Q}$. Quindi necessariamente $ab = 0$. Poiché il polinomio minimo di $\sqrt{3}$ su \mathbb{Q} è $x^2 - 3$, di grado 2, $\sqrt{3} \notin \mathbb{Q}$. Quindi $b \neq 0$, e quindi $ab = 0$ implica $a = 0$, cioè $\sqrt{3} = b\sqrt{2}$ per qualche $b \in \mathbb{Q}$. Il polinomio primitivo $2x^2 - 3 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ è irriducibile su \mathbb{Z} per il criterio di Eisenstein, dunque su \mathbb{Q} , e ha $b = \sqrt{3}/\sqrt{2}$ come radice: quindi coincide con il polinomio minimo di b su \mathbb{Q} , che implica che $b \notin \mathbb{Q}$, assurdo.

- (d) Nell'esercizio 2 abbiamo verificato che la somma di elementi algebrici con polinomio minimo di grado 2 su \mathbb{Q} è ancora un elemento algebrico: inoltre, nelle parti (a) e (c) di questo esercizio abbiamo visto che sia $\sqrt{2}$ che $\sqrt{3}$ sono di questo tipo, dunque $\sqrt{2} + \sqrt{3}$ è algebrico su \mathbb{Q} . Sempre dall'esercizio 2 sappiamo che $[K_{\sqrt{2}+\sqrt{3}} : \mathbb{Q}]$ deve dividere $[K_{\sqrt{2},\sqrt{3}} : \mathbb{Q}]$, e che quest'ultimo può essere 2 o 4 a seconda che $[K_{\sqrt{2},\sqrt{3}} : K_{\sqrt{2}}]$ sia 1 o 2. Avendo dimostrato che $\sqrt{3} \notin K_{\sqrt{2}}$, segue che $[K_{\sqrt{2},\sqrt{3}} : K_{\sqrt{2}}] = 2$ e $[K_{\sqrt{2},\sqrt{3}} : \mathbb{Q}] = 4$. Quindi anche $[K_{\sqrt{2}+\sqrt{3}} : \mathbb{Q}]$ può essere 2 o 4. Se dimostriamo che il polinomio monico $f(x) = x^4 - 6x^2 + 1 \in$

$\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ è irriducibile, avendo $\sqrt{2} + \sqrt{3}$ come radice esso coinciderà con il suo polinomio minimo, e quindi $[K_{\sqrt{2}+\sqrt{3}} : \mathbb{Q}] = \deg f(x) = 4$. Per dimostrare l'irriducibilità osserviamo che è sufficiente dimostrarla su \mathbb{Z} , in quanto $f(x)$ è primitivo. Usiamo il primo criterio e consideriamo la riduzione modulo 5 $f(x) = x^4 - x^2 + \bar{1} \in \mathbb{Z}_5[x]$. Intanto, poiché $\overline{f(x)}$ non si annulla in nessuno dei 5 elementi di \mathbb{Z}_5 , segue che $\overline{f}(x)$ non ha fattori lineari in $\mathbb{Z}_5[x]$. Se $\overline{f(x)}$ fosse riducibile, dovrebbe fattorizzarsi come

$$(x^2 + \bar{a}x + \bar{c})(x^2 + \bar{b}x + \bar{d}), \quad \bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{Z}_5,$$

con $\overline{cd} = \bar{1}$, quindi $\bar{c} = \bar{d} = \pm \bar{1}$. Sviluppando e confrontando i coefficienti con $x^4 - x^2 + \bar{1}$, si ottiene il sistema

$$\begin{cases} \bar{a} + \bar{b} = \bar{0}, \\ \bar{ab} + \bar{2c} = -\bar{1}. \end{cases}$$

Da $\bar{b} = -\bar{a}$ segue

$$-\bar{a}^2 + \bar{2c} = -\bar{1} \Rightarrow \bar{a}^2 = \bar{2c} + \bar{1},$$

che però non è mai verificata. Infatti se $\bar{c} = \bar{1}$, allora $\bar{a}^2 = \bar{3}$, che non è un quadrato in \mathbb{Z}_5 , quindi non può accadere. Se invece $\bar{c} = -\bar{1}$, allora $\bar{a}^2 = \bar{4}$, ma ciò porta a coefficienti incompatibili con il termine in x^2 . Concludiamo che $\overline{f(x)}$ è irriducibile su \mathbb{Z}_5 , e quindi $f(x)$ lo è su \mathbb{Q} .

5. Abbiamo che $\gamma = 1 + \alpha^2 = 1 + \sqrt{2} \notin \mathbb{Q}$ (abbiamo dimostrato che $\sqrt{2} \notin \mathbb{Q}$ nell'esercizio 4 qui sopra), quindi il suo polinomio minimo su \mathbb{Q} ha grado almeno 2. Poiché

$$\gamma - 1 = \sqrt{2},$$

elevando al quadrato entrambi i membri dell'equazione segue che

$$\gamma^2 - 2\gamma + 1 = 2,$$

e quindi il polinomio $p(x) = x^2 - 2x - 1 \in \mathbb{Q}[x]$ e si annulla in $1 + \alpha^2$. L'altra radice (in \mathbb{R}) di $p(x)$ è $1 - \sqrt{2}$, e nemmeno questa radice appartiene a \mathbb{Q} . Quindi $p(x)$ è un polinomio di grado 2 che non ha radici in \mathbb{Q} , e quindi irriducibile su \mathbb{Q} : in conclusione, è il polinomio minimo cercato.

6. (a) Chiaramente $1 + i\sqrt{5} \notin \mathbb{Q}$, quindi il suo polinomio minimo ha grado ≥ 2 . Osserviamo che

$$(x - 1 - i\sqrt{5})(x - 1 + i\sqrt{5}) = x^2 - 2x + 6 \in \mathbb{Q}[x] :$$

concludiamo che α è algebrico su \mathbb{Q} , con polinomio minimo $x^2 - 2x + 6$ di grado 2 ($x^2 - 2x + 6$ è irriducibile per il criterio di Eisenstein con primo $p = 2$), quindi $K = \mathbb{Q}[\alpha]$ è un campo, estensione algebrica di \mathbb{Q} di grado 2.

- (b) Poiché K è contenuto nell'insieme degli elementi algebrici su \mathbb{Q} , che abbiamo dimostrato nell'esercizio 3 essere numerabile, è numerabile esso stesso e quindi non può contenere \mathbb{R} che è più che numerabile.

7. (a) Si noti che -1 è radice di $p(x)$, quindi per Ruffini $x+1$ divide $p(x)$ e il quoziente è $x^2 - x + 2$ che è irriducibile in \mathbb{R} , dunque anche in \mathbb{Q} .
- (b) L'elemento $\alpha \notin \mathbb{Q}$ è una radice di $p(x)$ se e solo se α è radice di $x^2 - x + 2$ che è monico e irriducibile su \mathbb{Q} . In particolare $x^2 - x + 2$ è il polinomio minimo di α su \mathbb{Q} , dunque $[K_\alpha : \mathbb{Q}] = 2$.
- (c) Poiché $[K_\alpha : \mathbb{Q}] = 2$, segue che una base di K_α come spazio vettoriale su K è $\{1, \alpha\}$. Se $u = a + b\alpha \in K_\alpha$ con $a, b \in \mathbb{Q}$ è tale che $u^2 + 1 = 0$ allora

$$a^2 + 2ab\alpha + b^2\alpha^2 + 1 = 0.$$

Tenendo conto che $\alpha^2 = \alpha - 2$ in K_α segue che

$$a^2 - 2b^2 + 1 + (2a + b)b\alpha = 0$$

Se fosse $(2a + b)b \neq 0$ si dedurrebbe che

$$\alpha = -\frac{a^2 - 2b^2 + 1}{(2a + b)b} \in \mathbb{Q}.$$

Dalla contraddizione deduciamo che o $b = 0$ o $b = -2a$. Nel primo caso avremmo $a^2 + 1 = 0$, in contraddizione con la condizione $a \in \mathbb{Q}$. Nel secondo caso $7b^2 = 1$, in contraddizione con la condizione $b \in \mathbb{Q}$. Concludiamo che un elemento u con le proprietà indicate non esiste.

8. (a) Il criterio di Eisenstein garantisce che il polinomio $p(x)$ è irriducibile, dunque in $\mathbb{Q}[x]$ l'ideale I è massimale e K è un campo.
- (b) Sappiamo che ogni elemento di K ha un unico rappresentante della forma di un polinomio di grado al più 3 in x . Se $u = ax^3 + bx^2 + cx + d + I$ con $a, b, c, d \in \mathbb{Q}$, allora

$$u^2 = a^2x^6 + 2abx^5 + (b^2 + 2ac)x^4 + (2bc + 2ad)x^3 + (c^2 + 2bd)x^2 + 2cdx + d^2 + I.$$

In K vale la relazione $x^4 + I = 2 + I$ (perché la classe di $x^4 - 2$ è zero), quindi la relazione $u^2 + 1 = 0$ diviene

$$(2bc + 2ad)x^3 + (c^2 + 2a^2 + 2bd)x^2 + (2cd + 4ab)x + d^2 + 2b^2 + 4ac + 1 + I = 0,$$

e quindi deve valere

$$\begin{cases} bc + ad = 0 \\ c^2 + 2a^2 + 2bd = 0 \\ 2cd + 4ab = 0 \\ d^2 + 2b^2 + 4ac + 1 = 0, \end{cases}$$

perché $(1, \bar{x}, \bar{x}^2, \bar{x}^3)$ è una base di K come spazio vettoriale su \mathbb{Q} (dove con la barra sopra denoto la classe laterale nel quoziente K). Dall'ultima equazione deduciamo che necessariamente $ac < 0$, cioè a e c hanno segno opposto. Poiché dalla prima equazione ricaviamo che $d = -bc/a$, deduciamo che $bd \geq 0$. La seconda equazione implica allora $a = c = 0$, in contraddizione con quanto osservato. Quindi non esiste $u \in K$ tale che $u^2 + 1 = 0$.

9. (a) Consideriamo il polinomio

$$p(x) = \prod_{i=1}^N (x - a_i) :$$

per costruzione $p(a_i) = 0_K$ per $i = 1, \dots, N$ e $\deg(p) = N$ (il coefficiente di x^N è 1), dunque $p(x) \neq 0_K$.

- (b) Chiaramente se $a_i = 0_K$ si ha $p_i(a_j) = p(a_j) + 0_K = 0_K$: quindi se $a_i = 0_K$ le radici di $p_i(x)$ sono tutti gli elementi di K . Se, invece, $a_i \neq 0_K$, si ha $p_i(a_j) = p(a_j) + a_i \neq 0_K$ per ogni $j = 1, \dots, N$: quindi se $a_i \neq 0_K$ il polinomio $p_i(x)$ non ha radici in K .
 - (c) Poiché $1_K \neq 0_K$, segue che il polinomio $q(x) = p(x) + 1_K$ non ha radici in K che, quindi, non è algebricamente chiuso.
10. (a) Poiché $p(x)$ ha grado 3, per Ruffini esso è irriducibile se e solo se non ha radici in \mathbb{Z}_3 , e si calcola facilmente che

$$p(\bar{0}) = p(\bar{1}) = p(\bar{2}) = \bar{2} \neq \bar{0}.$$

Essendo \mathbb{Z}_3 un campo, gli ideali principali in $\mathbb{Z}_3[x]$ generati dai polinomi irriducibili sono massimali.

- (b) Poiché $\deg(p(x)) = [K : \mathbb{Z}_3] = 3$, il campo $\mathbb{Z}_3[x]/I$ si può identificare con uno spazio vettoriale di dimensione 3 su \mathbb{Z}_3 ; la sua cardinalità quindi è $3^3 = 27$. Segue che $|K^*| = 26$.
- (c) Osserviamo preliminarmente che l'ordine di un qualsiasi elemento in $K \setminus \{0, 1\}$ divide 26, dunque è o 2, o 13. Chiamiamo s la classe di x in K (evitiamo la notazione \bar{x} per non far confusione con le classi di resto in \mathbb{Z}_3): ogni elemento in K si scrive in maniera unica come polinomio in s di grado al più 2, a coefficienti in \mathbb{Z}_3 . In particolare s^2 è diverso da $\bar{1} \in \mathbb{Z}_3$, e l'ordine di s non è 2. Invece si ha $s^3 + \bar{2}s + \bar{2}$, cioè $s^3 = s + \bar{1}$. In particolare $s^4 = s^2 + s$ e $s^5 = s^3 + s^2 = s^2 + s + \bar{1}$. Calcoliamo allora che

$$s^{13} = (s^3)^4 \cdot s = (s+1)^4 s = s^5 + s^4 + s^2 + s = s^2 + s + \bar{1} + s^2 + s + s^2 + s = \bar{1},$$

quindi l'ordine di s è 13. A voi verificare che anche $s+1$ e $s+2$ hanno ordine 13.

- (d) Abbiamo già trovato ben 3 elementi di ordine 13. Per trovare un elemento di ordine 2 invece basta considerare $\bar{2} \in \mathbb{Z}_3 \subseteq K$.

N.B. Ricordate che in generale il metodo per risolvere un esercizio non è unico. Se qualche cosa non vi è chiara, e/o se pensate di aver trovato un errore di stampa, fatemi sapere!