Istituzioni di Algebra e Geometria — Algebra, a.a. 2024-2025

Soluzioni foglio 8

1. L'insieme A è un sottoanello commutativo dell'anello $\mathbb{R}^{2,2}$: dati due elementi $M_1 = \begin{pmatrix} a_1 & b_1 \\ b_1 & a_1 \end{pmatrix}$ e $M_2 = \begin{pmatrix} a_2 & b_2 \\ b_2 & a_2 \end{pmatrix}$ di A infatti

$$M_1 - M_2 = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ b_1 - b_2 & a_1 - a_2 \end{pmatrix} \in A, \quad \text{e} \quad M_1 M_2 = \begin{pmatrix} a_1a_2 + b_1b_2 & a_1b_2 + b_1a_2 \\ b_1a_2 + a_1b_2 & b_1b_2 + a_1a_2 \end{pmatrix} = M_2M_1 \in A.$$

Adesso consideriamo l'applicazione (suriettiva) $\varphi : A \to \mathbb{R}$ definita da

$$\varphi \begin{pmatrix} a & b \\ b & a \end{pmatrix} = a - b.$$

È immediato verificare che si tratta di un omomorfismo di anelli unitari, infatti date di nuovo due matrici $M_1, M_2 \in A$ come sopra, si ha che

$$\varphi(M_1 + M_2) = \varphi \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ b_1 + b_2 & a_1 + a_2 \end{pmatrix} = (a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) = \varphi(M_1) + \varphi(M_2)$$

$$\varphi(M_1M_2) = \varphi \begin{pmatrix} a_1a_2 + b_1b_2 & a_1b_2 + b_1a_2 \\ b_1a_2 + a_1b_2 & b_1b_2 + a_1a_2 \end{pmatrix} = (a_1a_2 + b_1b_2) - (a_1b_2 + b_1a_2) = (a_1 - b_1)(a_2 - b_2) = \varphi(M_1)\varphi(M_2)$$

$$\varphi(1_A) = \varphi \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1 - 0 = 1_{\mathbb{R}}.$$

Poiché $\mathrm{Ker}(\varphi) = I$, segue che I è un ideale. Inoltre, poiché φ è suriettivo, il teorema fondamentale di omomorfismo per anelli ci dice che abbiamo un isomorfismo $A/I \simeq \mathbb{R}$, e quindi, essendo il quoziente A/I isomorfo a un campo, l'ideale I è massimale.

2. Dati P, Q due ideali primi di A, dimostriamo che $P \cap Q$ è primo $\Leftrightarrow$ $P \subseteq Q$ oppure $P \supseteq Q$. L'implicazione ($\Leftarrow$) è ovvia, mentre per l'implicazione ($\Rightarrow$) supponiamo che $P \nsubseteq Q$ che $P \nsupseteq Q$. Allora esiste $a \in P \setminus Q$ e $b \in Q \setminus P$. Poiché P e Q sono entrambi ideali, il prodotto ab appartiene ad entrambi, e quindi $ab \in P \cap Q$, ma nessuno dei due fattori a e b appartiene all'intersezione, che quindi non può essere un ideale primo.

3. (a) Sappiamo già (dall'esercizio 10 foglio 6) che vale l'inclusione $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$. Viceversa, sia $a \in \sqrt{\sqrt{I}}$, allora esiste $n \in \mathbb{N}$ tale che $a^n \in \sqrt{I}$, e quindi esiste $m \in \mathbb{N}$ tale che $(a^n)^m = a^{nm} \in I$, e quindi $a \in \sqrt{I}$.

   (b) Di nuovo, l'inclusione $I \subseteq \sqrt{I}$ è sempre vera. Viceversa, sia $a \in \sqrt{I}$, allora esiste $n \in N$ tale che $a^n = aa^{n-1} \in I$ ideale primo, quindi o $a \in I$, oppure $a^{n-1} \in I$. Ma $a^{n-1} = aa^{n-2} \in I$ primo implica che o $a \in I$ oppure $a^{n-2} \in I$...e così via, fino ad ottenere $a \in I$.

4. Trovate la soluzione di questo esercizio nelle slide del 3 dicembre.

5.
   - $x^3 - x^2 + 5x = x(x^2 - x) + 5x$ (quoziente $q(x) = x$ e resto $r(x) = 5x$);
   - $x^3 + x^2 + x + 1 = (x + 1)x^2 + x + 1$ (quoziente $q(x) = x + 1$ e resto $r(x) = x + 1$);
   - $x^4 + x^2 = (x^3 - x^2 + 2x - 2)(x + 1) + 2$ (quoziente $q(x) = x^3 - x^2 + 2x - 2$ e resto $r(x) = 2$);
   - $x^3 + x^2 = (x + 1)(x^2 + 1) + (-x - 1)$ (quoziente $q(x) = x + 1$ e resto $r(x) = -x - 1$);
   - $x^5 - 1 = x^2(x^3 - 1) + x^2 - 1$ (quoziente $q(x) = x^2$ e resto $r(x) = x^2 - 1$).

6. (a) Il valore del polinomio $x^4 + n - 1$ in $x = 1$ è n. In particolare abbiamo

$$x^4 + n - 1 = (x^3 + x^2 + x + 1)(x - 1) + n,$$

e quindi il polinomio si fattorizza in $\mathbb{Z}_n[x]$.

(b) Assumiamo che il polinomio $x^4 + n - 1$ si fattorizzi in $\mathbb{Z}[x]$. Se $n - 1 \geq 0$, l'equazione $x^4 + n - 1 = 0$ non ha radici in $\mathbb{Z}$, quindi il polinomio $x^4 + n - 1$ è prodotto di due polinomi di grado 2 che possono essere supposti monici. L'uguaglianza

$$(x^2 + ax + b)(x^2 + cx + d) = x^4 + n - 1$$

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

$$\begin{cases} a + c = 0 \\ d + b + ac = 0 \\ ad + bc = 0 \\ bd = n - 1 \end{cases}$$

Quindi $c = -a$ e $a(d - b) = 0$. Se $a \neq 0$ allora $b = d$, dunque $n - 1 = b^2$. Invece, se $a = 0$ allora $d = -b$, dunque $n - 1 = -b^2$ che è un quadrato quando $b = 0$. Concludiamo che se $n - 1$ non è un quadrato il polinomio $x^4 + n - 1$ è irriducibile.

(c) Basta osservare che $x^4 + 9$ è indecomponibile.

7. Il polinomio $p(x) = x^4 + 2x + 4$ è monico con coefficienti $0, 0, 2$ e termine noto 4. Quindi il numero primo 2 divide tutti i coefficienti e il suo quadrato divide il termine noto: concludiamo che il polinomio considerato non soddisfa le ipotesi del teorema di Eisenstein.

Assumiamo che $p(x)$ si fattorizzi in un prodotto di due polinomi: la somma dei loro gradi deve essere 4 e possiamo assumere che essi siano monici. Se

$$p(x) = (x + a)(x^3 + bx^2 + cx + d),$$

dovremmo avere $ad = 4$. In particolare la radice $-a$ di $p(x)$ dovrebbe dividere 4: deduciamo che $a \in \{\pm 1, \pm 2, \pm 4\}$. Poiché $p(1) = 7$, $p(-1) = 3$, $p(2) = 24$, $p(-2) = 16$, $p(4) = 208$, $p(-4) = 192$, concludiamo che $p(x)$ non ha fattori di grado 1 in $\mathbb{Z}$. Se invece avessimo

$$p(x) = (x^2 + ax + b)(x^2 + cx + d),$$

questo implicherebbe il seguente sistema di equazioni in $\mathbb{Z}$:

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

Dalla prima relazione si deduce $c=-a$, e sostituendo nella seconda abbiamo $a^2=b+d$. Dall'ultima relazione deduciamo: $(b,d)\in\{(1,4),(-1,-4),(2,2),(-2,-2),(4,1),(-4,-1)\}$, e sostituendo tali valori nella seconda relazione otteniamo che $a^2\in\{5,-5,4,-4\}$. L'unico caso possibile è allora $b=d=2$, $a=\pm 2$, e quindi $c=\mp 2$. Sostituendo nella terza relazione otteniamo l'identità $0=2$, e quindi una contraddizione. Concludiamo che $p(x)$ è irriducibile in $\mathbb{Z}[x]$.

8. (a) Osserviamo che $p(1)=p'(1)=0$: questo significa che $x=1$ è una radice doppia (o di molteplicità 2) del polinomio, e quindi $p(x)=(x-1)^2q(x)$ per un certo polinomio di grado 1 $q(x)$. Facendo il conto, troviamo $p(x)=(x-1)^2(x+2)$. In $\mathbb{Q}[x]$, che è un PID, un ideale non nullo è primo se e solo se è massimale se e solo se è generato da un elemento irriducibile. Siccome $p(x)$ è riducibile, I non è né primo, né massimale.

   (b) Sia J un ideale di $\mathbb{Q}[x]$ contenente I. Siamo in un PID, dunque esiste un polinomio $q(x)$ tale che $J=(q(x))$. L'inclusione $I\subseteq J$ implica che $p(x)=r(x)q(x)$ per qualche $r(x)\in\mathbb{Q}[x]$. Deduciamo che gli ideali J' e J'' vanno necessariamente cercati fra quelli generati dai fattori di $p(x)$. Sia $J'=(x-1)$ e $J''=(x+2)$. Abbiamo che

   $$3=-(x-1)+(x+2)\in J'+J'',$$

   in particolare $J'+J''$ è un ideale contenente un elemento invertibile di $\mathbb{Q}[x]$, e quindi $J'+J''=\mathbb{Q}[x]$.

   (c) Ricordiamo che $q(x)\in\mathbb{Q}[x]$ ha classe nulla in $\mathbb{Q}[x]/I$ se e solo se $q(x)\in I$. Quindi la classe di $a(x)$ in $\mathbb{Q}[x]$ è zero–divisore in $\mathbb{Q}[x]/I$ se e solo se $a(x)\notin I$ ed esiste $b(x)\in\mathbb{Q}[x]\setminus I$ tale che $a(x)b(x)\in I$. Concludiamo che la classe di ogni elemento divisibile per $x-1$ o $x+2$ ma non per $(x-1)^2(x+2)$ è zero–divisore in $\mathbb{Q}[x]/I$.

   (d) Ricordiamo che ogni classe modulo I è rappresentata da un unico polinomio monico di grado minore di quello di $p(x)$, perché $\mathbb{Q}[x]$ è euclideo: sia esso x^2+ax+b. Ciò significa che $(x^2+ax+b)^2$ è divisibile per $p(x)=(x-1)^2(x+2)$, quindi x^2+ax+b deve essere divisibile sia per $x-1$ che per $x+2$. Necessariamente allora $q(x)\in(x^2+x-2)$.

9. (a) Come già ricordato, in $\mathbb{Q}[x]$, che è un PID, un ideale non nullo è primo se e solo se è massimale se e solo se è generato da un elemento irriducibile. Siccome $p(x)=(x+3)^2$ è riducibile (è un quadrato di un polinomio di grado 1!), segue che I non è né primo, né massimale.

   (b) Poiché $(x+3)^2\in I$ segue che $x+3\in\sqrt{I}$. Deduciamo che ogni generatore $r(x)$ di $\sqrt{I}$ divide $x+3$. Se $r(x)$ fosse costante dovrebbe essere diverso da 0 perché $(0)\neq I\subseteq\sqrt{I}$, dunque invertibile. Seguirebbe allora che $1\in\sqrt{I}$, dunque $1\in I$: ma ciò non è possibile perché il grado minimo di un polinomio non nullo in I è 2, e quindi $\deg(r(x))\geq 1$. Deduciamo che $r(x)$ deve coincidere con $x+3$ a meno di un fattore moltiplicativo, cioè $\sqrt{I}=(x+3)$.

(c) Ogni polinomio di grado 1 è irriducibile, dunque genera un ideale massimale in $\mathbb{Q}[x]$. In particolare $\sqrt{I} = (x+3)$ è un ideale massimale contenente I.

(d) È sufficiente considerare $q(x) = 1$, che soddisfa la condizione $\overline{q(x)}^2 = \overline{1}$.

(e) Risulta $\overline{q(x)}^2 = \overline{0}$ se e solo se $q(x)^2 \in I$, cioè se e solo se $q(x) \in (x+3)$. In particolare la classe di $x+3$ in $\mathbb{Q}[x]/I$ è non nulla e ha la proprietà cercata.

(f) Si noti che $\overline{x}$ è invertibile se e solo se esiste $a(x) \in \mathbb{Q}[x]$ tale che $\overline{x}\overline{a(x)} = \overline{1}$. Ciò accade se e solo se esistono $a(x), b(x) \in \mathbb{Q}[x]$ tali che

$$1 = xa(x) + (x+3)^2 b(x),$$

cioè se e solo se $\mathrm{MCD}(x, (x+3)^2) = 1$. Poiché

$$9 = x(-x-6) + 1 \cdot (x+3)^2,$$

segue che $\overline{x}$ è invertibile e il suo inverso è

$$(\overline{x})^{-1} = \frac{1}{9}(-x-6).$$

10. (a) Sia $1 = 2a(x) + xb(x)$ per opportuni $a(x), b(x) \in \mathbb{Z}[x]$: valutando entrambi i membri in 0 otteniamo l'uguaglianza $1 = 2a(0)$, che in $\mathbb{Z}$ non è mai verificata.

(b) Dimostriamo che l'ideale I definito sopra non è principale. Se esistesse $p(x) \in \mathbb{Z}[x]$ tale che $I = (p(x))$ allora

$$2 = \alpha(x)p(x), \qquad x = \beta(x)p(x)$$

per opportuni $\alpha(x), \beta(x) \in \mathbb{Z}[x]$. Poiché $\mathbb{Z}$ è un dominio di integrità, il grado di un prodotto di polinomi non nulli è la somma dei loro gradi. Deduciamo che $\deg(\alpha(x)) = \deg(p(x)) = 0$, $\deg(\beta(x)) = 1$. In particolare esistono $a, b, c \in \mathbb{Z}$ tali che $\beta(x) = ax + b$ e $p(x) = c$. L'uguaglianza $x = \beta(x)p(x)$ allora implica

$$ac = 1, \qquad bc = 0.$$

Segue che $b = 0$ e $a = c = \pm 1$: in particolare si dovrebbe avere $1 \in I$, in contraddizione con quanto verificato in precedenza.

(c) Sia $q(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ un polinomio. Osserviamo che $q(x) \notin I$ se e solo se il termine noto $a_0 = 2k+1$ è dispari, e possiamo quindi scrivere $q(x) = 1 + 2 \cdot k + x \cdot (a_1 + a_2 x + \ldots + a_n x^{n-1})$. Segue immediatamente che la classe di $q(x)$ è

$$\overline{q(x)} = \overline{1 + 2 \cdot k + x \cdot (a_1 + a_2 x + \ldots + a_n x^{n-1})} = \overline{1} \in \mathbb{Z}[x]/I.$$

(d) Sappiamo che $\mathbb{Z}[x]/I$ è un anello. Per quanto visto sopra esso ha solo due elementi, precisamente $\overline{0}$ e $\overline{1}$. Deduciamo che $\mathbb{Z}[x]/I \cong \mathbb{Z}_2$ è isomorfo a un campo, quindi è un campo esso stesso. (Si veda anche la soluzione della parte (a) dell'esercizio 12, dove viene fatto lo stesso ragionamento con $J = (3, x)$.)

11. (a) Poiché $p(x) = (x+1)^2+1$, il polinomio non ha radici in $\mathbb{Q}$: in particolare $p(x)$ è irriducibile in $\mathbb{Q}[x]$, quindi anche in $\mathbb{Z}[x]$. Inoltre $p(x) = 2 \cdot 1 + x \cdot (2+x) \in (2, x)$.

(b) Da quanto visto nella parte (a), $I \subseteq J = (2, x) \subseteq \mathbb{Z}[x]$ e tutte le inclusioni sono proprie, quindi I non è massimale.

(c) Usando la scrittura $p(x) = (x+1)^2 + 1 = q(x)^2 + 1$ è immediato verificare che il polinomio $q(x) = x + 1$ soddisfa l'uguaglianza indicata.

(d) Se $\overline{q(x)} \in \mathbb{Z}[x]/I$ è tale che $\overline{q(x)}^2 = \overline{0}$ allora in $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ vale l'uguaglianza

$$q(x)^2 = a(x)p(x)$$

per qualche $a(x) \in \mathbb{Z}[x]$. Poiché $p(x)$ è irriducibile in $\mathbb{Q}[x]$, l'ideale da esso generato è un ideale primo: in particolare se $q(x)^2 \in I$ in $\mathbb{Q}[x]$, allora $q(x) = b(x)p(x) \in I$ in $\mathbb{Q}[x]$: segue che una uguaglianza simile deve valere anche in $\mathbb{Z}[x]$, quindi $\overline{q(x)} = \overline{0}$ in $\mathbb{Z}[x]/I$.

12. (a) Osserviamo che $I \subseteq J = (3, x) \subseteq \mathbb{Z}[x]$: l'inclusione $I \subseteq J$ è propria perché, ad esempio, il polinomio costante 3 appartiene a $J \setminus I$. Se $J = \mathbb{Z}[x]$, allora $1 = 3a(x) + xb(x)$ per opportuni $a(x), b(x) \in \mathbb{Z}[x]$. Valutando ambo i membri in 0 si deduce facilmente che una tale uguaglianza non può valere in $\mathbb{Z}[x]$, quindi J è un ideale proprio e I non può essere massimale.

Mostriamo invece che J è massimale: per ogni $a(x) \in \mathbb{Z}[x]$, indichiamo con $r_a \in \{0, 1, 2\}$ il resto della divisione intera di $a_0 = a(0)$ per 3. L'applicazione

$$\begin{aligned} \varphi \colon \mathbb{Z}[x] &\longrightarrow \mathbb{Z}_3 \\ a(x) &\longrightarrow \overline{r_a}, \end{aligned}$$

è composta dall'omomorfismo $\mathbb{Z}[x] \to \mathbb{Z}$ definito da $a(x) \mapsto a_0$ seguito dalla proiezione canonica $\mathbb{Z} \to \mathbb{Z}_3$, dunque è un omomorfismo. Inoltre $\varphi(0) = \overline{0}$, $\varphi(1) = \overline{1}$, $\varphi(2) = \overline{2}$: concludiamo che φ è un epimorfismo. Risulta

$$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \operatorname{Ker}(\varphi)$$

se e solo se a_0 è multiplo di 3, cioè se e solo se $a(x) \in J$. Concludiamo che $J = \operatorname{Ker}(\varphi)$, e $\mathbb{Z}[x]/J \cong \mathbb{Z}_3$ che è un campo: deduciamo che J è massimale.

(b) Se $\overline{3} \in \mathbb{Z}[x]/I$ fosse invertibile, esisterebbero $a(x), b(x) \in \mathbb{Z}[x]$ tali che

$$3a(x) = b(x)(x^2 - 3) + 1.$$

Valutando ambo i membri in 0 avremmo una relazione del tipo $3(a(3) + b(3)) = 1$ che non è mai verificata in $\mathbb{Z}$. Quindi $\overline{3}$ non è invertibile in $\mathbb{Z}[x]/I$.

13. (a) È sufficiente ripetere passo passo il ragionamento della parte (a) dell'esercizio precedente con $I = (p(x))$ e $J = (5, x)$.

(b) L'uguaglianza $\overline{q(x)}^2 = \overline{1}$ è equivalente ad affermare l'esistenza di $a(x) \in \mathbb{Z}[x]$ tale che

$$q(x)^2 - 1 = (q(x) - 1)(q(x) + 1) = a(x)(x^2 - 5).$$

Poiché $x^2 - 5$ è irriducibile in $\mathbb{Q}[x]$, esso genera un ideale massimale (e quindi primo) in $\mathbb{Q}[x]$, quindi o si ha $q(x) - 1 \in (p(x)) \subseteq \mathbb{Q}[x]$, oppure $q(x) + 1 \in (p(x)) \subseteq \mathbb{Q}[x]$. Supponiamo che valga il primo caso, e quindi che esista $b(x) \in \mathbb{Q}[x]$ tale che

$$q(x) - 1 = b(x)(x^2 - 5) :$$

possiamo supporre $b(x) \in \mathbb{Z}[x]$, quindi deve essere $q(x) = b(x)(x^2 - 5) + 1$, cioè $\overline{q(x)} = \overline{1}$. Lo stesso tipo di argomento implica che se $q(x) \neq b(x)(x^2 - 5) + 1$ per ogni $b(x) \in \mathbb{Z}[x]$, allora esiste $c(x) \in \mathbb{Z}[x]$ tale che $q(x) = c(x)(x^2 - 5) - 1$, quindi $\overline{q(x)} = \overline{-1}$. In conclusione, gli unici $\overline{q(x)} \in \mathbb{Z}[x]/I$ tali che $\overline{q(x)}^2 = \overline{1}$ sono $\overline{q(x)} = \overline{\pm 1}$.

(c) Se $\overline{3x - 1}$ fosse invertibile, esisterebbe una classe $\overline{a(x)} \in \mathbb{Z}[x]/I$ tale che $(\overline{3x - 1})\overline{a(x)} = \overline{1}$: quindi esisterebbe un polinomio $b(x) \in \mathbb{Z}[x]$ tale che

$$(3x - 1)a(x) = 1 + b(x)(x^2 - 5).$$

Questa uguaglianza deve valere per tutti i valori di x, valutiamola quindi in $x = 3$:

$$8a(3) = 1 + 4b(3) \quad \Rightarrow \quad 1 = 4(2a(3) - b(3)),$$

che però non è mai soddisfatta da nessun possibile valore $a(3) \in \mathbb{Z}$, quindi $\overline{3x - 1}$ non è invertibile.

14. (a) Col criterio di Eisenstein si verifica che $p(x)$ è irriducibile su $\mathbb{Q}$, quindi I è massimale.

(b) Verifichiamo $char(\mathbb{Q}[x]/I) = 0$. Se $\mathbb{Q}[x]/I$ avesse caratteristica positiva, diciamo $k > 0$, avremmo

$$k\overline{1} = k(1 + I) = \overline{0} = I,$$

ovvero esisterebbe un intero positivo k tale che $k1 = k$ sia un multiplo di $p(x)$, cosa che è chiaramente impossibile.

(c) Sia $\overline{f(x)} \in \mathbb{Q}[x]/I$ una qualsiasi classe non nulla. Il resto $r(x)$ della divisione di $f(x)$ per $p(x)$ è in $\overline{f(x)}$ perché $f(x) - r(x) \in I$ per definizione. Infine se $s(x) \in \overline{f(x)}$ è un altro polinomio con $\deg(s(x)) \leq 3$, segue che $r(x) - s(x)$ è un polinomio di grado al massimo 3 in $(p(x))$, dunque $r(x) = s(x)$.

(d) Sia

$$f(x) = ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$$

polinomio tale che $\overline{f(x)}^2 = \overline{-1}$. Si ha allora

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

Poiché $\overline{x}^6 = 2\overline{x}^2$, $\overline{x}^5 = 2\overline{x}$, $\overline{x}^4 = 2$, deduciamo che

$$(2bc + 2ad)x^3 + (c^2 + 2a^2 + 2bd)x^2 + (2cd + 4ab)x + (d^2 + 2b^2 + 4ac) \in \overline{f(x)}^2.$$

Da questa uguaglianza ricaviamo il sistema:

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

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. Concludiamo che non esistono radici quadrate di -1 in $\mathbb{Q}[x]/I$.

15. (a) Osserviamo che $p_n(\overline{0}) = \overline{0}$ se e solo se $\overline{n} = \overline{0}$ in $\mathbb{Z}_3$ cioè se e solo se $n \in 3\mathbb{Z}$, ovvero se e solo se esiste $m \in \mathbb{Z}$ tale che $n = 3m$. Similmente $p_n(\overline{1}) = \overline{0}$ se e solo se $\overline{n} = \overline{0}$ in $\mathbb{Z}_3$. Infine $p_n(\overline{2}) = \overline{0}$ se e solo se $\overline{n} + \overline{2} = \overline{0}$ in $\mathbb{Z}_3$ cioè se e solo se esiste $m \in \mathbb{Z}$ tale che $n = 3m + 1$.

(b) Poiché $\mathbb{Z}_3$ è un campo, $\mathbb{Z}_3[x]$ è un PID e il quoziente $\mathbb{Z}_3[x]/(p_2(x))$ è un campo se e solo se $p_2(x)$ è irriducibile. Per quanto visto sopra, il polinomio monico $p_2(x)$ non ha radici in $\mathbb{Z}_3$, quindi se non è irriducibile, esso si spezza necessariamente in un prodotto di due polinomi monici irriducibili di grado 2 in $\mathbb{Z}_3[x]$. Potete verificare che gli unici polinomi monici irriducibili di grado 2 in $\mathbb{Z}_3[x]$ sono

$$x^2 + \overline{1}, \qquad x^2 + x + \overline{2}, \qquad x^2 + \overline{2}x + \overline{2}.$$

D'altra parte

$$(x^2 + \overline{1})^2 = x^4 + \overline{2}x^2 + \overline{1}, \qquad (x^2 + x + \overline{2})^2 = x^4 + \overline{2}x^3 + \overline{2}x^2 + x + \overline{1},$$

$$(x^2 + \overline{2}x + \overline{2})^2 = x^4 + x^3 + \overline{2}x^2 + \overline{2}x + \overline{1}, \qquad (x^2 + \overline{1})(x^2 + x + \overline{2}) = x^4 + x^3 + x + \overline{2},$$

$$(x^2 + \overline{1})(x^2 + \overline{2}x + \overline{2}) = x^4 + \overline{2}x^3 + \overline{2}x + \overline{2}, \qquad (x^2 + x + \overline{2})(x^2 + \overline{2}x + \overline{2}) = x^4 + \overline{1},$$

quindi $p_2(x)$ è irriducibile, e $\mathbb{Z}_3[x]/(p_2(x))$ è un campo.

(c) Osserviamo che

$$x(\overline{2}x^3 + x^2) = 2p_1(x) + \overline{1}$$

quindi la classe di $\overline{2}x^3 + x^2$ modulo $p_1(x)$ è l'inverso di $\overline{x}$ in $\mathbb{Z}_3[x]/(p_1(x))$.

16. (a) Se $p(x)$ fosse riducibile, si spezzerebbe nel prodotto di un polinomio di grado 1 per uno di grado 2: in particolare $p(x)$ avrebbe una radice in $\mathbb{Z}_3$, per il Teorema di Ruffini. D'altra parte possiamo calcolare che

$$p(\overline{0}) = p(\overline{1}) = p(\overline{2}) = \overline{1} \neq \overline{0},$$

segue che $p(x)$ è irriducibile. Di conseguenza, essendo $\mathbb{Z}_3$ un campo (e quindi $\mathbb{Z}_3[x]$ un PID), l'ideale I è massimale, o equivalentemente il quoziente $\mathbb{Z}_3[x]/I$ è un campo.

(b) Ricordiamo che la caratteristica di un anello è l'ordine additivo dell'unità. Si verifica facilmente quindi che $char(\mathbb{Z}_3[x]/I) = 3$.

Per quanto riguarda la cardinalità, sappiamo $\mathbb{Z}_3[x]/I$ è uno spazio vettoriale sul campo $\mathbb{Z}_3$ con le usuali operazioni di somma e prodotto per scalare: ogni elemento in tale quoziente è rappresentato da un unico polinomio monico di grado al più 2, e sappiamo che $\{\overline{1}, \overline{x}, \overline{x^2}\}$ è una base di tale spazio vettoriale, quindi $\dim_{\mathbb{Z}_3}(\mathbb{Z}_3[x]/I) = 3$ e la cardinalità di $\mathbb{Z}_3[x]/I$ è $3^3 = 27$.

(c) Abbiamo dimostrato che $\mathbb{Z}_3[x]/I$ è un campo, e un campo non ammette divisori dello zero, quindi no, un tale $\overline{q(x)}$ non esiste.

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!