

Istituzioni di Algebra e Geometria — Algebra, a.a. 2023-2024
Soluzioni foglio 7

1. Si ha che

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

e

$$x^5 + x^2 - 16x - 4 = x(x^4 - 16) + x^2 - 4.$$

I casi rimanenti li lascio a voi.

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

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

segue che 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 sistema di equazioni in \mathbb{Z} :

$$a + c = 0, \quad d + b + ac = 0, \quad ad + bc = 0, \quad bd = n - 1.$$

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.

3. (a) Il polinomio $p(x) = x^4 + 2x + 4$ considerato 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.

(b) 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

$$a + c = 0, \quad b + d + ac = 0, \quad ad + bc = 2, \quad bd = 4.$$

Dalla prima relazione si deduce $c = -a$: sostituendo nella seconda si ha allora $a^2 = b + d$. Dall'ultima relazione deduciamo: $(b, d) \in \{(1, 4), (-1, -4), (2, 2), (-2, -2), (4, 1), (-4, -1)\}$. 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 $0 = 2$. Concludiamo che $p(x)$ è irriducibile in $\mathbb{Z}[x]$.

4. (a) Osserviamo che $p(1) = p'(1) = 0$: risulta $p(x) = (x - 1)^2(x + 2)$.
- (b) Poiché $\mathbb{Q}[x]$ è un dominio ad ideali principali, un ideale non nullo in $\mathbb{Q}[x]$ è primo se e solo se è massimale se e solo se è generato da un elemento irriducibile. Da quanto visto sopra $p(x)$ è riducibile, quindi I non è né un ideale primo, né un ideale massimale.
- (c) Sia $(p(x)) = I \subseteq J$. Di nuovo, $\mathbb{Q}[x]$ è 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 vanno cercati fra quelli generati dai fattori di $p(x)$. Sia $J' = (x - 1)$ e $J'' = (x + 2)$. Chiaramente

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

Poiché $J' + J''$ è un ideale contenente un elemento invertibile di $\mathbb{Q}[x]$ segue che $J' + J'' = \mathbb{Q}[x]$.

- (d) 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 $\mathbb{Q}[x]/I$.
- (e) 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 $x + 2$. Concludiamo che deve essere

$$q(x) \in (x^2 + x - 2).$$

5. (a) Questa parte la lascio a voi.
- (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 particolare $\sqrt{I} = (x + 3)$ è un ideale massimale contenente I .
- (d) Chiaramente $q(x) = 1$ soddisfa la condizione $\overline{q(x)^2} = \bar{1}$: esistono altre classi in $\mathbb{Q}[x]/I$ con la stessa proprietà?

(e) Risulta $\overline{q(x)^2} = \bar{0}$ 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 \bar{x} è invertibile se e solo se esiste $a(x) \in \mathbb{Q}[x]$ tale che $\overline{xa(x)} = \bar{1}$. Ciò accade se e solo se esistono $a(x), b(x) \in \mathbb{Q}[x]$ tali che

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

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

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

segue che \bar{x} è invertibile e

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

6. (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

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

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

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

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) Se $q(0) = q_0$, allora $q(x) - q_0$ si annulla per $x = 0$, dunque il teorema di Ruffini implica che

$$q(x) = q_0 + x\hat{q}(x).$$

deduciamo che $\overline{q(x)} = \bar{q}_0$ in $\mathbb{Z}[x]/I$. Inoltre $q_0 \in 2\mathbb{Z}$ se e solo se $q(x) \in I$. Quindi se $q(x) \notin I$ allora $q_0 = 2n+1$, dunque $\overline{q(x)} = \bar{q}_0 = \bar{1}$ 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 $\bar{0}$ e $\bar{1}$. Deduciamo che $\mathbb{Z}[x]/I \cong \mathbb{Z}_2$.

7. (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 $\mathbb{Z}[x]$.

(b)-(c) Lascio a voi queste 2 parti dell'esercizio.

(d) Si noti che $q(x) = x+1$ soddisfa l'uguaglianza indicata.

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

(f) Se $\overline{4x}$ fosse invertibile in $\mathbb{Z}[x]/I$, esisterebbero $a(x), b(x) \in \mathbb{Z}[x]$ tali che

$$4xa(x) = b(x)p(x) + 1.$$

Valutando tale uguaglianza in 0 avremmo $0 = 2b_0 + 1$ che non è possibile in \mathbb{Z} . Quindi $\overline{4x}$ non è invertibile in $\mathbb{Z}[x]/I$.

8. (a) Osserviamo che $I \subseteq J = (3, x)$: provate a verificare che l'inclusione è propria. Inoltre 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 proprio.
- (b) 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

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

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

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

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

- (c) 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 possibile in \mathbb{Z} . Quindi $\overline{3}$ non è invertibile in $\mathbb{Z}[x]/I$.

9a)-(b) Lascio a voi le prime 2 parti dell'esercizio.

- (c) 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 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 $\overline{q(x)} = \pm \overline{1}$.

- (d) 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 $x = 3$:

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

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

10. (a) Col criterio di Eisenstein si verifica che $p(x)$ è irriducibile su \mathbb{Q} , quindi I è massimale.
 (b) Verifichiamo $\text{char}(\mathbb{Q}[x]/I) = 0$. Infatti se $\mathbb{Q}[x]/I$ avesse caratteristica positiva, diciamo k , avremmo

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

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

- (c) Si consideri $\overline{f(x)} \in \mathbb{Q}[x]/I$. Allora 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

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

Pertanto deve valere

$$bc + ad = 0, \quad c^2 + 2a^2 + 2bd = 0, \quad 2cd + 4ab = 0, \quad d^2 + 2b^2 + 4ac + 1 = 0.$$

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 $\mathbb{Q}[x]/I$.

11. (a) Osserviamo che $p_n(\bar{0}) = \bar{0}$ se e solo se $\bar{n} = \bar{0}$ 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 $p_n(\bar{1}) = \bar{0}$ se e solo se $\bar{n} = \bar{0}$ in \mathbb{Z}_3 . Infine $p_n(\bar{2}) = \bar{0}$ se e solo se $\bar{n} + \bar{2} = \bar{0}$ 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 dominio a ideali principali 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

$$x^2 + \bar{1}, \quad x^2 + x + \bar{2}, \quad x^2 + \bar{2}x + \bar{2}.$$

D'altra parte

$$(x^2 + \bar{1})^2 = x^4 + \bar{2}x^2 + \bar{1}, \quad (x^2 + x + \bar{2})^2 = x^4 + \bar{2}x^3 + \bar{2}x^2 + x + \bar{1},$$

$$(x^2 + \bar{2}x + \bar{2})^2 = x^4 + x^3 + \bar{2}x^2 + \bar{2}x + \bar{1}, \quad (x^2 + \bar{1})(x^2 + x + \bar{2}) = x^4 + x^3 + x + \bar{2},$$

$$(x^2 + \bar{1})(x^2 + \bar{2}x + \bar{2}) = x^4 + \bar{2}x^3 + \bar{2}x + \bar{2}, \quad (x^2 + x + \bar{2})(x^2 + \bar{2}x + \bar{2}) = x^4 + \bar{1},$$

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

- (c) Osserviamo che

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

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

12. (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. Poiché

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

segue che $p(x)$ è irriducibile.

- (b) $\mathbb{Z}_3[x]/I$ è un campo perché $p(x)$ è irriducibile, quindi I è massimale.

- (c) Lascio a voi verificare che $\text{char}(\mathbb{Z}_3[x]/I) = 3$.

Per la cardinalità, sappiamo $\mathbb{Z}_3[x]/I$ è uno spazio vettoriale sul campo \mathbb{Z}_3 con l'usuale somma e il prodotto per scalari in \mathbb{Z}_3 : ogni elemento in tale quoziente è rappresentato da un unico polinomio monico di grado al più 2, e sappiamo che $\{\bar{1}, \bar{x}, \bar{x}^2\}$ 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 $3^3 = 27$.

- (d) Visto che $\mathbb{Z}_3[x]/I$ è un campo, lascio a voi la risposta.

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!