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

$$M_1 - M_2 = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ b_1 - b_2 & a_1 - a_2 \end{pmatrix} \in A, \quad \text{e} \quad M_1M_2 = \begin{pmatrix} a_1a_2 + b_1b_2 & a_1b_2 + b_1a_2 \\ b_1a_2 + a_1b_2 & b_1b_2 + a_1a_2 \end{pmatrix} = M_2M_1 \in A.$$

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 $P \nsubseteq Q$. 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 $a^n = aa^{n-1} \in I$ che è un ideale primo, quindi o $a \in I$, oppure $a^{n-1} \in I$. Ma $a^{n-1} = aa^{n-2} \in I$ ideale primo implica che o $a \in I$ oppure $a^{n-2} \in I$...e così via, fino ad ottenere $a \in I$.

4. Sia I ideale primo di A PID, quindi esiste un elemento $a \in A$ tale che l'ideale $I = (a)$ è l'ideale principale generato da a. Sia poi $J \subseteq A$ un altro ideale tale che $I \subseteq J \subseteq A$; di nuovo, poiché A è un PID, esiste un altro elemento $b \in A$ tale che $J = (b)$. L'inclusione $(a) \subseteq (b)$ implica in particolare che $a \in (b)$, e quindi che esiste un terzo elemento $c \in A$ tale che $a = bc \in I$. Per ipotesi l'ideale I è primo, quindi almeno uno di questi due fattori deve appartenere ad I.

   - Se $b \in I$ allora $J = (b) \subseteq I$, e quindi per la doppia inclusione $I = J$;
   - se invece $c \in I = (a)$, allora esiste un elemento $d \in A$ tale che $c = ad$. Ne deduciamo la catena di uguaglianze $a = bc = b(ad) = a(b)$, e siccome siamo in un dominio di integrità e vale la legge di cancellazione per il prodotto: $a = a(bd) \Rightarrow 1_A = bd \in (b) = J$, quindi J contiene l'unità, cioè $J = A$.

   In conclusione quindi se J è un ideale tale che $I \subseteq J \subseteq A$, o $I = J$, oppure $J = A$, cioè I è massimale.

5. (a) Date $\varphi, \psi \in \mathcal{C}^0[0,1]$, abbiamo che:

$$v_0(\varphi + \psi) = (\varphi + \psi)(0) = \varphi(0) + \psi(0) = v_0(\varphi) + v_0(\psi),$$

$$v_0(\varphi\psi) = (\varphi\psi)(0) = \varphi(0)\psi(0) = v_0(\varphi)v_0(\psi).$$

   Denotiamo con $\mathbb{1}$ la funzione costante 1, che è l'unità dell'anello $\mathcal{C}^0[0,1]$. Abbiamo che $v_0(\mathbb{1}) = \mathbb{1}(0) = 1 = 1_{\mathbb{R}}$. In totale quindi v_0 è un omomorfismo di anelli unitari.

   (b) Osserviamo che I coincide con il nucleo dell'omomorfismo v_0, infatti:

$$\mathrm{Ker}(v_0) = \{\varphi \in \mathcal{C}^0[0,1] \mid v_0(\varphi) = \varphi(0) = 0\} = I,$$

   e quindi è un ideale.

   (c) Osserviamo che l'omomorfismo v_0 è suriettivo: $\forall\, k \in \mathbb{R}$, l'applicazione costante $\varphi(x) = k$ è tale che $v_0(\varphi) = k$. Se quindi applichiamo a v_0 il teorema fondamentale di omomorfismo di anelli l'isomorfismo

$$\mathcal{C}^0[0,1]/I = \mathcal{C}^0[0,1]/\mathrm{Ker}(v_0) \simeq \mathrm{Im}(v_0) = \mathbb{R}.$$

   Poiché dunque il quoziente $\mathcal{C}^0[0,1]/I$ è isomorfo ad un campo, è un campo esso stesso, e quindi l'ideale I è massimale.

6. - $x^3 - x^2 + 5x = x(x^2 - x) + 5x$ (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 $r(x) = x^2 - 1$).

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

8. (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 $q(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ 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 $q(x) = 1 + 2 \cdot k + x \cdot (a_1 + a_2x + \ldots + a_nx^{n-1})$. Segue immediatamente che la classe di $q(x)$ è

$$\overline{q(x)} = \overline{1 + 2 \cdot k + x \cdot (a_1 + a_2x + \ldots + a_nx^{n-1})} = \overline{1} \in \mathbb{Z}[x]/I.$$

(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 7 qui sopra, dove viene fatto lo stesso ragionamento con $J = (3, x)$.)

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!