Algebra I - Soluzioni 6

3 Maggio

1 Esercizi

Esercizio 1. Per prima cosa si calcolano

1) $3943 = 13 \cdot 303 + 4$,
2) $7134 = 12 \cdot 594 + 6$,
3) $126 = 44 \cdot 2 + 38$.

Il sistema dunque è

$$\begin{cases} 4^6 x \equiv 5 \pmod{13} \\ 38x \equiv 6 \pmod{44} \end{cases} \implies \begin{cases} x \equiv 5 \pmod{13} \\ 19x \equiv 3 \pmod{22} \end{cases} \implies \begin{cases} x \equiv 5 \pmod{13} \\ -3x \equiv 3 \pmod{22} \end{cases} \implies \begin{cases} x \equiv 5 \pmod{13} \\ x \equiv -1 \pmod{22} \end{cases}$$

Le soluzioni quindi sono $x = 109 + 286k$ per $k \in \mathbb{Z}$.

Esercizio 2.

- $\diamond$ $2x^2 - 5x + 2 = 2\left(x^2 - \dfrac{5}{2}x + 1\right)$. Dunque cerchiamo due numeri la cui somma sia $5/2$ e il cui prodotto sia 1. Segue che

$$2x^2 - 5x + 2 = 2(x-2)\left(x - \frac{1}{2}\right).$$

- $\diamond$ Una radice razionale di questo polinomio deve essere del tipo

$$x = \frac{p}{q}$$

con $p \mid 2$ e $q \mid 2$. Il polinomio in questi valori non si annulla mai, pertanto non ha soluzioni razionali.

- $\diamond$ Siccome il polinomio è monico si ha che le radici razionali possibili sono $\pm 1, \pm 2, \pm 4$. Valutando il polinomio in questi numeri segue che

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

Per il discriminante, o per Eisenstein, se vogliamo, il secondo polinomio non è più scomponibile in $\mathbb{Q}$.

- $\diamond$ La scomposizione segue dai prodotti notevoli

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

- $\diamond$ Bisogna trovare due numeri la cui somma sia -1 e il cui prodotto sia -2.

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

Esercizio 3. Il gruppo degli invertibili di $\mathbb{Z}/44\mathbb{Z}$ ha ordine 20. Gli elementi di ordine 5 sono tutti contenuti nei 5 Sylow, dunque si può procedere calcolando questi gruppi. Per il terzo teorema di Sylow $n_5 \mid 4$ e $n_5 \equiv 1 \pmod 5$, da cui segue che $n_5 = 1$. C'è quindi solo un 5 Sylow e dunque gli elementi di ordine 5 sono $5 - 1$.

Esercizio 4. $\mathbb{Z}[i]$ è un dominio euclideo, e dunque a ideali principali, quindi un ideale massimale $\mathfrak{m} = (m)$ contiene $(12 + 6i)$ se $m \mid 12 + 6i$. Scomponiamo quindi il numero

$$12 + 6i = 6 \cdot (2 + i) = (1 + i)(1 - i)3(2 + i).$$

Gli ideali massimali coincidono con i fattori irriducibili di $12 + 6i$, dunque sono

1) $\mathfrak{m}_1 = (2 + 1)$,
2) $\mathfrak{m}_2 = (3)$,
3) $\mathfrak{m}_3 = (1 + i) = (1 - i)$.

Esercizio 5. Prendiamo $x \in Z(G)$ e mostriamo che $\varphi(x) \in Z(G)$. Prendiamo $y \in G$ qualsiasi, e sia $z = \varphi^{-1}(y)$. z esiste ed è unico perché φ è un automorfismo.

Allora

$$\varphi(x)y = \varphi(x)\varphi(z) = \varphi(xz) = \varphi(zx) = \varphi(z)\varphi(x) = y\varphi(x),$$

da cui $\varphi(x) \in Z(G)$.

Abbiamo quindi appena dimostrato che

$$\varphi(Z(G)) \subseteq Z(G).$$

Siccome φ è un automorfismo generico, vale anche per φ^{-1}, dunque

$$\varphi^{-1}(Z(G)) = Z(G) \implies Z(G) \subseteq \varphi(Z(G)).$$

Da ciò segue l'uguaglianza.

Esercizio 6. Per equipaggiare $\mathfrak{m}/\mathfrak{m}^2$ di una struttura di spazio vettoriale serve un campo che vi agisca. Poiché la costruzione deve essere valida per ogni ideale massimale $\mathfrak{m}$, la scelta del campo deve dipendere da quest'ultimo. Il campo più naturale da scegliere è $k = A/\mathfrak{m}$.

Preso un elemento $x + \mathfrak{m} \in A/\mathfrak{m}$, e un elemento $y + \mathfrak{m}^2 \in \mathfrak{m}/\mathfrak{m}^2$, con $y \in \mathfrak{m}$, vogliamo mostrare che il prodotto rimane in $\mathfrak{m}/\mathfrak{m}^2$.

$$(x + \mathfrak{m})(y + \mathfrak{m}^2) = xy + x\mathfrak{m}^2 + y\mathfrak{m} + \mathfrak{m}^3$$

Poiché $y \in \mathfrak{m}$, allora $xy \in \mathfrak{m}$ e $y\mathfrak{m} \in \mathfrak{m}^2$. Dunque equivale a

$$xy + \mathfrak{m}^2, \qquad xy \in \mathfrak{m},$$

che è in $\mathfrak{m}/\mathfrak{m}^2$.

Ora osserviamo che le proprietà delle operazioni sono rispettate: *somma*: $\mathfrak{m}$ è un ideale di A, dunque è un anello. $\mathfrak{m}^2$ è un ideale di $\mathfrak{m}$, segue quindi che $\mathfrak{m}/\mathfrak{m}^2$ è un anello quoziente. Questo ci basta per dire che è un gruppo additivo con la somma. *prodotto esterno*: Il prodotto di sopra è una restrizione del prodotto su A, da ciò segue che è distributivo.

Le proprietà vengono rispettate, dunque è uno spazio vettoriale.

Esercizio 7. Tutti questi insiemi sono gruppi abeliani, dunque bisogna verificare solo che il prodotto esterno sia chiuso e distributivo.

◇ Se consideriamo come prodotto il classico, il prodotto in $\mathbb{C}[x, y]$, l'ideale è un $\mathbb{R}$-modulo. Infatti, essendo un ideale è chiuso rispetto a questo prodotto, ed essendo la restrizione del prodotto globale, è distributivo rispetto alla somma.

- $\diamond$ Questo insieme è il nucleo della mappa di valutazione

$$ev_{(x,y)=(0,0)} : \mathbb{C}[x,y] \to \mathbb{C}.$$

Dunque, essendo un ideale, è un R-modulo per le stesse motivazioni del punto precedente.

- $\diamond$ Se consideriamo come prodotto il classico

$$\begin{aligned} \mathbb{C}[x,y] \times \mathbb{C}[x^2,y^2] &\to \mathbb{C}[x^2,y^2] \\ (p(x,y), v(x,y)) &\mapsto p(x,y)v(x,y) \end{aligned}$$

non è un R modulo perché manca la chiusura. Ad esempio $x \cdot x^2 = x^3 \notin \mathbb{C}[x^2,y^2]$

Se consideriamo invece come prodotto

$$\begin{aligned} \mathbb{C}[x,y] \times \mathbb{C}[x^2,y^2] &\to \mathbb{C}[x^2,y^2] \\ (p(x,y), v(x,y)) &\mapsto p(x^2,y^2)v(x,y) \end{aligned}$$

allora l'insieme diventa uno spazio vettoriale, infatti

1) $p(x,y) \cdot v(x,y) = p(x^2,y^2)v(x,y) \in \mathbb{C}[x^2,y^2]$,
2) $p(x,y) \cdot (v(x,y)+u(x,y)) = p(x^2,y^2)(v(x,y)+u(x,y)) = p(x^2,y^2)v(x,y)+p(x^2,y^2)u(x,y)$,
3) $(p(x,y)q(x,y)) \cdot v(x,y) = p(x^2,y^2)q(x^2,y^2)v(x,y) = p(x,y) \cdot (q(x,y) \cdot v(x,y))$.

- $\diamond$ Anche questo è un R modulo considerando il prodotto

$$\begin{aligned} \mathbb{C}[x,y] \times \mathbb{C}[x,y]/(x-2y) &\to \mathbb{C}[x,y]/(x-2y) \\ \big(p(x,y), a(x,y) + (x-2y)_{\mathbb{C}[x,y]}\big) &\mapsto p(x,y)a(x,y) + (x-2y)_{\mathbb{C}[x,y]} \end{aligned}$$

Questo prodotto, per come è definito, è chiuso. Essendo inoltre costruito sul prodotto standard tra polinomi è ancora distributivo. Segue dunque che questo insieme con questo prodotto è un R-modulo.

Esercizio 8. $\diamond$ È libero con base $\mathcal{B} = \{1\}$,

- $\diamond$ È libero con base $\mathcal{B} = \{2\}$,
- $\diamond$ Non è libero e non ammette neanche una base infinita. Osserviamo però che se prendiamo l'elemento formale $\frac{1}{2}$ che moltiplicato per 2 dà 1, si ottiene una sorta di base,
- $\diamond$ Ammette una base, ma è infinita ed è $\mathcal{B} = \{1, x, x^2, \dots, x^n, \dots\}$,
- $\diamond$ È libero con base $\mathcal{B} = \{1, i\}$.