Algebra 1

Proff. A. D'Andrea, A. De Sole

Primo appello, 26 giugno 2023

Nome: ____________________________________

Cognome: ____________________________________

Numero di matricola: __________________________

Docente: **D'Andrea** $\setminus$ **De Sole** (cerchiare il/i docente/i).

Esercizio	Punti totali	Punteggio
1	6	
2	6	
3	6	
4	6	
5	6	
Totale	30	

Esercizio 1. Si consideri l'insieme $S = \{\theta \in \mathbb{R} \mid \sin(\theta) \in \mathbb{Q}\}$. Determinare se l'insieme S ha cardinalità finita, numerabile o se ha la cardinalità del continuo, giustificando la risposta.

Soluzione: Se $\sin\theta = q$, allora $S_q = \sin^{-1}(q) = \{\theta + 2k\pi, k \in \mathbb{Z}\} \cup \{(2k+1)\pi - \theta, k \in \mathbb{Z}\}$ è un insieme numerabile. Di conseguenza,

$$S = \bigcup_{q \in [-1,1] \cap \mathbb{Q}} S_q$$

è unione numerabile di insiemi numerabili, ed è pertanto numerabile.

Risposta: $|S| =$ **finita** / **numerabile** / **card. del continuo** (cerchiare la risposta corretta).

Esercizio 2. (a) Determinare il numero n_7 di 7-Sylow nel gruppo S_7.

(b) Dato un 7-Sylow $H \subset S_7$, sia $K = N_G(H)$ il normalizzatore di H (ovvero il più grande sottogruppo di G in cui H è normale). Determinare l'ordine di K.

Soluzione:

(a) Il gruppo simmetrico S_7 ha ordine $7! = 5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$ e quindi i suoi 7-Sylow sono tutti e soli i sottogruppi di ordine 7. Un sottogruppo di ordine 7 in S_7 è ciclico, generato da un elemento di ordine 7 che è necessariamente un 7-ciclo.

Ogni 7-Sylow contiene sei elementi di ordine 7, ciascuno dei quali ne é un generatore ciclico. Inoltre, se $P \neq Q$ sono sottogruppi di ordine 7, allora $P \cap Q$ ha ordine che divide 7 per il Teorema di Lagrange, e contiene quindi soltanto l'identità. Per contare i 7-Sylow di S_7 è allora sufficiente contare i 7-cicli in S_7 e dividere tale numero per 6. Si ottiene facilmente $6!/6 = 5! = 120$.

(b) Il numero dei 7-Sylow in S_7 coincide con l'indice del normalizzatore di ciascun 7-Sylow. Di conseguenza, il normalizzatore di ciascun 7-Sylow ha indice 120, e quindi ordine $7!/120 = 42$.

Risposta: (a) $n_7 = \boxed{}$ (b) $|K| = \boxed{}$

Esercizio 3. Ci interessiamo all'anello quoziente $A = \mathbb{Z}[i]/(7+5i)$.

(a) Dire se A sia un dominio d'integrità.

(b) Calcolare il nucleo dell'omomorfismo $\phi : \mathbb{Z} \to A$ definito da $\phi(n) = [n]$.

(c) Quanti elementi contiene A?

Soluzione:

(a) A è un dominio d'integrità se e solo se $(7+5i)$ è un ideale primo in $\mathbb{Z}[i]$, cioè quando $7+5i$ è primo/irriducibile in $\mathbb{Z}[i]$. Ad ogni modo, $7+5i = (1+i)(6-i)$ non è irriducibile e quindi A non è un dominio d'integrità.

(b) $n \in \mathbb{Z}$ appartiene a $\ker\phi$ se e solo se $[n] = [0]$ in $\mathbb{Z}[i]/(7+5i)$ e cioè esattamente quando $7+5i$ divide n in $\mathbb{Z}[i]$.

Pertanto, $n \in \ker\phi \iff n/(7+5i) \in \mathbb{Z}[i]$ e abbiamo

$$\frac{n}{7+5i} = \frac{n(7-5i)}{(7+5i)(7-5i)} = \frac{7n}{74} - \frac{5n}{74}i.$$

La parte reale e quella immaginaria sono entrambe intere esattamente quando n è un multiplo di 74. In conclusione, $\ker\phi = (74)$.

(c) Come gruppo abeliano, $\mathbb{Z}[i] \simeq \mathbb{Z}^2$ e l'ideale generato da $7+5i$ corrisponde, attraverso l'isomorfismo, al sottogruppo generato da $(7,5)$ e $(-5,7)$. L'anello quoziente A è quindi isomorfo, come gruppo abeliano, al quoziente $\mathbb{Z}^2/\langle(7,5),(-5,7)\rangle$. Mettendo la matrice

$$\begin{pmatrix} 7 & -5 \\ 5 & 7 \end{pmatrix}$$

in forma canonica di Smith, si ottiene, dopo qualche passaggio,

$$\begin{pmatrix} 1 & 0 \\ 0 & 74 \end{pmatrix}.$$

Si conclude subito che A, come gruppo abeliano, è isomorfo a $\mathbb{Z}/(74)$ e possiede pertanto 74 elementi.

Risposta: (a) A dominio? **SI** / **NO**. (a) $\ker(\phi) =$ $\boxed{}$. (c) $|A| =$ $\boxed{}$

Esercizio 4. Sia $A \neq \mathrm{Id}$ una matrice 3×3 a coefficienti razionali che soddisfa l'identità $(A^4 + 5\mathrm{Id})(A^2 - 2A + \mathrm{Id}) = 0$. Determinare le possibili forme di Jordan (complesse) J di A.

[Sugg.: che si può dire del polinomio minimo di A?]

Soluzione: Il polinomio minimo $\mu(x)$ di A, che divide il corrispondente polinomio caratteristico, ha grado ≤ 3, coefficienti in $\mathbb{Q}$, e divide $(x^4 + 5)(x - 1)^2$. Poiché sia $x^4 + 5$, per il Criterio di Eisenstein, che $x - 1$, avendo grado 1, sono irriducibili in $\mathbb{Q}[x]$, solo tali due polinomi possono comparire nella fattorizzazione di $\mu(x)$ in primi di $\mathbb{Q}[x]$.

Ricordando che $\mu(x)$ ha grado ≤ 3, concludiamo che $x^4 + 5$ non compare nella fattorizzazione di $\mu(x)$, e quindi che $\mu(x)$ divide $(x - 1)^2$; accettando senza perdere di generalità che il polinomio minimo sia monico, le uniche possibilità sono $\mu(x) = x - 1$ oppure $\mu(x) = (x - 1)^2$.

Tuttavia, l'unica matrice ad avere polinomio minimo $x - 1$ è l'identità, e questo è escluso dal testo dell'esercizio. Pertanto $\mu(x) = (x - 1)^2$ e di conseguenza la forma di Smith della matrice $A - x\mathrm{Id}$, ricordando che il polinomio caratteristico ha grado 3 e che i divisori elementari si dividono l'un l'altro, è

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & x-1 & 0 \\ 0 & 0 & (x-1)^2 \end{pmatrix}.$$

La forma canonica di Jordan cercata è allora

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Risposta: $J = \boxed{}$

Esercizio 5. Calcolare il polinomio minimo $f(x)$ di $\alpha = \sqrt{\sqrt{2}+\sqrt{3}}$ su $\mathbb{Q}$.

Soluzione: Si calcola facilmente $\alpha^2 = \sqrt{2}+\sqrt{3} \implies \alpha^4 = 5+2\sqrt{6}$ da cui $(\alpha^4-5)^2 = 24 \implies \alpha^8 - 10\alpha^4 + 1 = 0$. Pertanto α annulla il polinomio $x^8 - 10x^4 + 1$, del quale è però difficile verificare direttamente l'irriducibilità: non ha radici razionali, ma questo mostra soltanto che non possiede fattori di grado 1 in $\mathbb{Q}[x]$.

Calcoliamo allora il grado $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Nel caso in cui sia 8, il polinomio $x^8 - 10x^4 + 1$ sarà irriducibile e sarà quindi il polinomio minimo di α su $\mathbb{Q}$. Consideriamo le estensioni

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2},\sqrt{3}) \subset \mathbb{Q}(\alpha).$$

Vogliamo mostrare che ciascun campo è un'estensione di grado 2 del precedente: questo ci permetterà di concludere che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2\cdot 2\cdot 2 = 8$.

L'estensione $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ ha grado 2, in quando $\sqrt{2}$ soddisfa il polinomio x^2-2, irriducibile per il Criterio di Eisenstein. Otteniamo, in particolare, che $1, \sqrt{2}$ è una $\mathbb{Q}$-base di $\mathbb{Q}(\sqrt{2})$.

Allo stesso modo, l'estensione $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2},\sqrt{3})$ ha grado 2. In effetti, $\sqrt{3}$ soddisfa il polinomio x^2-3 a coefficienti in $\mathbb{Q}(\sqrt{2})$ e l'estensione ha quindi grado al più 2. Inoltre, $\sqrt{3}$ non appartiene a $\mathbb{Q}(\sqrt{2})$.

Per convincercene, osserviamo che se $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, allora $\sqrt{3} = a + b\sqrt{2}$, con $a, b \in \mathbb{Q}$. Quadrando, si ottiene $3 = (a^2+2b^2) + 2ab\sqrt{2}$ e quindi $a^2 + 2b^2 = 3, 2ab = 0$, che si vedono facilmente non avere soluzioni razionali. Di nuovo otteniamo, come conseguenza, che $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ è una $\mathbb{Q}$-base di $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

Passiamo all'ultima estensione $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subset \mathbb{Q}(\alpha)$. Sappiamo che α soddisfa il polinomio $x^2 - (\sqrt{2}+\sqrt{3})$ a coefficienti in $\mathbb{Q}(\sqrt{2},\sqrt{3})$ e quindi $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2},\sqrt{3})] \leq 2$. Inoltre il grado dell'estensione è proprio 2 nel caso in cui α non appartenga a $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

Procediamo come fatto in precedenza: se $\alpha \in \mathbb{Q}(\sqrt{2},\sqrt{3})$, allora deve essere della forma

$$\alpha = c + d\sqrt{2} + e\sqrt{3} + f\sqrt{6},$$

con $c, d, e, f \in \mathbb{Q}$. Quadrando, si ottiene

$$0\cdot 1 + 1\cdot\sqrt{2} + 1\cdot\sqrt{3} + 0\cdot\sqrt{6} = \alpha^2 = (c^2+2d^2+3e^2+6f^2) + 2(cd+3ef)\sqrt{2} + 2(ce+2df)\sqrt{3} + 2(cf+de)\sqrt{6}.$$

Confrontando i coefficienti che moltiplicano 1, si ottiene $c^2+2d^2+3e^2+6f^2 = 0$, da cui $c = d = e = f = 0$, il che è assurdo.

Risposta: $f(x) = \boxed{}$

Foglio per la brutta copia

Foglio per la brutta copia

Foglio per la brutta copia