Algebra 1

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

Secondo esonero del 9 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. Elencare tutti gli ideali dell'anello quoziente $\mathbb{Z}[i]/(4+3i)$. Quali sono massimali? Quali primi?

Soluzione: Gli ideali di un anello quoziente A/I sono in corrispondenza biunivoca con gli ideali di A che contengono I; più precisamente, la corrispondenza si ottiene applicazione la proiezione canonica $\pi : A \to A/I$ agli ideali che contengono I o, nella direzione opposta, calcolando la controimmagine di un ideale di A/I attraverso π.

Nel nostro caso, $A = \mathbb{Z}[i]$ e $I = (4+3i)$. L'anello A è un dominio a ideali principali, e $J = (\alpha)$ contiene I se e solo se α divide $4+3i$. Inoltre, due elementi di $\mathbb{Z}[i]$ generano lo stesso ideale principale se e solo se sono associati. In conclusione, dobbiamo individuare tutti i divisori di $4+3i$ a meno di associati.

In $\mathbb{Z}[i]$ vale la fattorizzazione

$$4+3i = i(2-i)^2,$$

e quindi i divisori di $4+3i$, a meno di associati, sono $1, 2-i, (2-i)^2$, che generano gli ideali $(1) = \mathbb{Z}[i], (2-i), ((2-i)^2) = (4+3i)$. I corrispondenti ideali di $\mathbb{Z}[i]/(4+3i)$ sono tutto l'anello, $\pi((2-i))$ e (0).

La corrispondenza indicata sopra conserva le inclusioni e quindi la massimalità. Poiché la controimmagine di un ideale primo attraverso un omorfismo è ancora un ideale primo, viene conservata anche la primalità. Poiché un ideale non nullo in un dominio a ideali principali è massimale se e solo se è primo se e solo se è generato da un elemento irriducibile/primo, otteniamo che l'ideale $\pi((2-i))$ è sia primo che massimale, mentre gli altri due non sono né primi, né massimali.

Risposta:

(a) Ideali: $\boxed{}$ (b) Id. primi: $\boxed{}$ (c) Id. massimali: $\boxed{}$

Esercizio 2. Dire se $[x^2+1]$ sia invertibile in $\mathbb{Q}[x]/(x^3+2)$ ed eventualmente trovarne l'inverso.

Soluzione:

Se D è un dominio a ideali principali, $[a]$ è invertibile in $D/(b)$ esattamente quando $MCD(a,b)=1$. In questo caso x^3+2 è irriducibile — ad esempio, non ha radici razionali — e quindi x^2+1 e x^3+2 sono inevitabilmente coprimi.

Per determinare l'inverso di $[x^2+1]$ dobbiamo calcolare, ad esempio attraverso l'algoritmo euclideo, l'identità di Bézout tra x^2+1 e x^3+2. Si ha

$$\begin{aligned} x^3+2 &= x(x^2+1)-(x-2) \\ x^2+1 &= (x+2)(x-2)+5, \end{aligned}$$

da cui

$$5 = x^2+1-(x+2)(x-2) = (x^2+1)-(x+2)\left(x(x^2+1)-(x^3+2)\right) = (x+2)(x^3+2)-(x^2+2x-1)(x^2+1).$$

Pertanto $[x^2+2x-1][x^2+1]=[-5]$ in $\mathbb{Q}[x]/(x^3+2)$ e l'inverso di $[x^2+1]$ è quindi

$$\left[-\frac{x^2+2x-1}{5}\right].$$

Risposta: (a) $\exists[x^2+1]^{-1}$? **SI** / **NO**. (b) $[x^2+1]^{-1} = \boxed{}$

Esercizio 3. Sia $\Gamma \subset \mathbb{Z}^3$ il sottogruppo generato da $(18,12,6),(18,15,12),(20,15,16),(20,16,12)$. Determinare l'ordine del gruppo quoziente $G=\mathbb{Z}^3/\Gamma$ ed esprimerlo come prodotto di gruppi ciclici.

Soluzione: è sufficiente mettere in forma canonica di Smith la matrice che ha per colonne i quattro generatori dati. Per evitare di spiegare le manipolazioni che vado ad eseguire, seguirò passo per passo la procedura illustrata a lezione. Tenete presente che sono possibili molte scorciatoie per arrivare alla forma diagonale più in fretta.

$$\begin{pmatrix}18&18&20&20\\12&15&15&16\\6&12&16&12\end{pmatrix} \rightsquigarrow \begin{pmatrix}6&12&16&12\\18&18&20&20\\12&15&15&16\end{pmatrix} \rightsquigarrow \begin{pmatrix}6&0&4&0\\18&-18&-16&-16\\12&-9&-9&-8\end{pmatrix} \rightsquigarrow \begin{pmatrix}4&0&6&0\\-16&-18&18&-16\\-9&-9&12&-8\end{pmatrix} \rightsquigarrow$$

$$\begin{pmatrix}4&0&2&0\\-16&-18&34&-16\\-9&-9&21&-8\end{pmatrix} \rightsquigarrow \begin{pmatrix}2&0&4&0\\34&-18&-16&-16\\21&-9&-9&-8\end{pmatrix} \rightsquigarrow \begin{pmatrix}2&0&0&0\\34&-18&-84&-16\\21&-9&-51&-8\end{pmatrix} \rightsquigarrow \begin{pmatrix}2&0&0&0\\0&-18&-84&-16\\1&-9&-51&-8\end{pmatrix} \rightsquigarrow$$

$$\begin{pmatrix}1&-9&-51&-8\\0&-18&-84&-16\\2&0&0&0\end{pmatrix} \rightsquigarrow \begin{pmatrix}1&0&0&0\\0&-18&-84&-16\\2&18&102&16\end{pmatrix} \rightsquigarrow \begin{pmatrix}1&0&0&0\\0&-18&-84&-16\\0&18&102&16\end{pmatrix} \rightsquigarrow \begin{pmatrix}1&0&0&0\\0&-16&-84&-18\\0&16&102&18\end{pmatrix} \rightsquigarrow$$

$$\begin{pmatrix}1&0&0&0\\0&-16&-4&-2\\0&16&22&2\end{pmatrix} \rightsquigarrow \begin{pmatrix}1&0&0&0\\0&-2&-4&-16\\0&2&22&16\end{pmatrix} \rightsquigarrow \begin{pmatrix}1&0&0&0\\0&-2&0&0\\0&2&18&0\end{pmatrix} \rightsquigarrow \begin{pmatrix}1&0&0&0\\0&-2&0&0\\0&0&18&0\end{pmatrix}.$$

Il gruppo $\mathbb{Z}^3/\Gamma$ è allora isomorfo a $\mathbb{Z}/(1)\times\mathbb{Z}/(2)\times\mathbb{Z}/(18)\simeq\mathbb{Z}/(2)\times\mathbb{Z}/(18)$ e possiede $2\cdot 18=36$ elementi.

Risposta: (a) $|G| =$ $\boxed{}$ (b) $G \simeq$ $\boxed{}$

Esercizio 4. Individuare la forma canonica di Jordan J dell'endomorfismo lineare $T : \mathbb{C}^3 \to \mathbb{C}^3$ di matrice
$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & -2 \\ 0 & 1 & 3 \end{pmatrix}$$
e determinare una base $\mathcal{B}$ in cui la matrice di T è in forma di Jordan.

Soluzione: Anche in questo caso bisogna prima individuare i cosiddetti fattori invarianti dell'endomorfismo dato, mettendo in forma canonica di Smith la matrice $A - x\mathrm{Id}$. Procediamo subito:
$$\begin{pmatrix} 1-x & 0 & 1 \\ 0 & -x & -2 \\ 0 & 1 & 3-x \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 1-x & 0 \\ -2 & 0 & -x \\ 3-x & 0 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ -2 & -2(x-1) & -x \\ 3-x & -(x-3)(x-1) & 1 \end{pmatrix} \rightsquigarrow$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -2(x-1) & -x \\ 0 & -(x-3)(x-1) & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -(x-3)(x-1) & 1 \\ 0 & -2(x-1) & -x \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -(x-3)(x-1) \\ 0 & -x & -2(x-1) \end{pmatrix} \rightsquigarrow$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -x & -2(x-1) - x(x-3)(x-1) \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -(x-1)^2(x-2) \end{pmatrix}.$$

Tenendo traccia delle sole manipolazioni per righe, si vede che il $\mathbb{C}[x]$-sottomodulo di $\mathbb{C}[x]^3$ generato dalle tre colonne iniziali rimane diagonalizzato nella base
$$\begin{pmatrix} 1 \\ -2 \\ 3-x \end{pmatrix}, \begin{pmatrix} 0 \\ -x \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

In altre parole, $\mathbb{C}^3$, dotato della struttura di $\mathbb{C}[x]$-modulo nella quale la moltiplicazione per x coincide con la moltiplicazione a sinistra per A, è isomorfo a $\mathbb{C}[x]/((x-1)^2(x-2))$, e l'isomorfismo si ottiene moltiplicando tali elementi per il vettore $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$.

L'esercizio ci chiede di individuare la forma canonica di Jordan dell'endomorfismo, e poiché per il Teorema cinese dei resti il quoziente $\mathbb{C}[x]/((x-1)^2(x-2))$ è isomorfo a $\mathbb{C}[x]/((x-1)^2) \oplus \mathbb{C}[x]/(x-2)$, avremo un blocco 2×2 di autovalore 1 e uno 1×1 di autovalore 2. In altre parole, la forma di Jordan dell'endomorfismo sarà
$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Ci viene richiesta anche una base esplicita di $\mathbb{C}^3$ in cui tale forma matriciale venga ottenuta. A tale scopo, dobbiamo innanzitutto esplicitare l'isomorfismo
$$\mathbb{C}[x]/((x-1)^2) \oplus \mathbb{C}[x]/(x-2) \simeq \mathbb{C}[x]/((x-1)^2(x-2))$$
dato dal Teorema cinese dei resti. Questo si ottiene calcolando l'identità di Bézout per $(x-1)^2$ e $x-2$, che si può fare con l'algoritmo euclideo, ma si vede in realtà anche ad occhio:
$$1 = (x-1)^2 - x(x-2).$$
Il generatore del primo addendo all'interno di $\mathbb{C}[x]/((x-1)^2(x-2))$ è allora $[-x(x-2)]$, mentre il generatore del secondo addendo è $[(x-1)^2]$. Il primo blocco di Jordan (quello relativo all'autovalore 1) è allora generato come $\mathbb{C}[x]$-modulo da
$$-x(x-2)\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = 2x\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} - x^2\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = 2\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} - x\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix} - \begin{pmatrix} 1 \\ -2 \\ 3 \end{pmatrix} = \begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix},$$

mentre il secondo (dopo qualche conto) da

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

Potete verificare rapidamente che in effetti questo vettore è autovettore dell'endomorfismo dato di autovalore 2.

All'interno del blocco $\mathbb{C}[x]/((x-1)^2)$, una base di Jordan è data da $[x-1], [1]$; pertanto la $\mathbb{C}$-base di Jordan del primo blocco è ad esempio

$$(x-1)\cdot \begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & -2 \\ 0 & 1 & 3 \end{pmatrix} \begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix} - \begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix} = \begin{pmatrix} -2 \\ 2 \\ -1 \end{pmatrix} - \begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}, \qquad 1\cdot \begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix} = \begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix}.$$

In conclusione, nella base

$$\begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$$

la matrice ha la forma di Jordan indicata.

Risposta: (a) $J = \boxed{}$, $\mathcal{B} = \boxed{}$

Esercizio 5. (a) Determinare $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}]$. (b) Determinare $[\mathbb{Q}(\sqrt{2} - \sqrt[3]{2}) : \mathbb{Q}]$. (c) Dire se $\mathbb{Q}(\sqrt[6]{2})$ e $\mathbb{Q}(\sqrt{2} - \sqrt[3]{2})$ coincidono.

Soluzione: L'algebrico $\sqrt[6]{2}$ soddisfa il polinomio $x^6 - 2 \in \mathbb{Q}[x]$, che è irriducibile per il Criterio di Eisenstein unito al Lemma di Gauss. Pertanto il grado $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}]$ dell'estensione è 6. Se poniamo $\alpha = \sqrt[6]{2}$, una $\mathbb{Q}$-base di $\mathbb{Q}(\sqrt[6]{2})$ è, ad esempio, $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$.

Abbiamo allora che $\sqrt{2} - \sqrt[3]{2} = \alpha^3 - \alpha^2$ e pertanto $\sqrt{2} - \sqrt[3]{2} \in \mathbb{Q}(\sqrt[6]{2})$, da cui $\mathbb{Q}(\sqrt{2} - \sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[6]{2})$. Le prime potenze, espresse nella base appena indicata, sono

$$\begin{aligned}
1 &= 1 \cdot 1 + 0 \cdot \alpha + 0 \cdot \alpha^2 + 0 \cdot \alpha^3 + 0 \cdot \alpha^4 + 0 \cdot \alpha^5 \\
\alpha^3 - \alpha^2 &= 0 \cdot 1 + 0 \cdot \alpha - 1 \cdot \alpha^2 + 1 \cdot \alpha^3 + 0 \cdot \alpha^4 + 0 \cdot \alpha^5 \\
(\alpha^3 - \alpha^2)^2 &= 2 \cdot 1 + 0 \cdot \alpha + 0 \cdot \alpha^2 + 0 \cdot \alpha^3 + 1 \cdot \alpha^4 - 2 \cdot \alpha^5 \\
(\alpha^3 - \alpha^2)^3 &= -2 \cdot 1 + 6 \cdot \alpha - 6 \cdot \alpha^2 + 2 \cdot \alpha^3 + 0 \cdot \alpha^4 + 0 \cdot \alpha^5,
\end{aligned}$$

che sono linearmente indipendenti a vista. Pertanto $[\mathbb{Q}(\sqrt{2} - \sqrt[3]{2}) : \mathbb{Q}] \geq 4$ e sappiamo che deve dividere $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$. In conclusione $[\mathbb{Q}(\sqrt{2} - \sqrt[3]{2}) : \mathbb{Q}] = 6$.

L'ultima affermazione è a questo punto immediata: poiché $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} - \sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[6]{2})$, dall'uguaglianza dei gradi segue l'uguaglianza delle estensioni.

Risposta:

(a) $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = \boxed{}$; (b) $[\mathbb{Q}(\sqrt{2} - \sqrt[3]{2}) : \mathbb{Q}] = \boxed{}$; (c) $\mathbb{Q}(\sqrt[6]{2}) = \mathbb{Q}(\sqrt{2} - \sqrt[3]{2})$? **SI** / **NO**.