ALGEBRA I: ESERCIZI SU MODULI E ESTENSIONI DI CAMPI

(1) Esprimere il gruppo abeliano $\mathbb{Z}/(12) \times \mathbb{Z}/(15) \times \mathbb{Z}/(18)$ come prodotto diretto di gruppi ciclici $Z/(d_i)$ dove d_i divide d_j quando $i \leq j$. Esprimere inoltre lo stesso gruppo come prodotto diretto di gruppi ciclici i cui ordini siano potenze di un numero primo.

(2) Considerare l'applicazione lineare $L_M : \mathbb{C}^3 \to \mathbb{C}^3$ associata alla seguente matrice complessa

$$M = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 4 & 1 \end{pmatrix}.$$

Determinare la forma canonica di Smith della matrice $M - xI$ e la forma canonica di Jordan, nonché una base di $\mathbb{C}^3$ in cui viene raggiunta, dell'applicazione L_M.

(3) Sia$T : \mathbb{Q}^3 \to \mathbb{Q}^3$ un'applicazione $\mathbb{Q}$-lineare tale che $(T^7 + 2I)(T^2 + 3T + 2I)^2 = 0$. Determinare le possibili forme di Jordan di T e il relativo poliomio caratteristico.

(4) Se $R = \mathbb{C}[x, y]$, sia $I \subset R$ l'ideale generato da x e y. Dire se I possieda una R-base come R-modulo.

(5) Sia R un anello (non necessariamente commutativo) con unità. Descrivere tutti gli omomorfismi di R-moduli $R \to R$.

(6) Un R-modulo si dire *semplice* se gli unici suoi sottomoduli sono quelli banali. Mostrare che se S, S' sono R-moduli semplici, allora un R-omomorfismo $S \to S'$ è un isomorfismo oppure manda ogni elemento in 0. Quali sono gli $\mathbb{Z}$-moduli semplici? E gli $\mathbb{R}$-moduli semplici?

(7) Sia $U \subset \mathbb{Z}^3$ il sottogruppo generato (additivamente!) dagli elementi $(3, 1, 2), (1, 1, 3), (2, 1, 6)$. Esibire una $\mathbb{Z}$-base v_1, v_2, v_3 di $\mathbb{Z}^3$ e interi positivi $d_1|d_2|d_2$ tali che U sia generato da d_1v_1, d_2v_2, d_3v_3.

(8) Dire quanti siano, a meno di isomorfismo, i gruppi abeliani di ordine 400.

(9) Mostrare che se $\mathbb{Q}$ è prodotto diretto di due suoi sottogruppi H, K, allora uno di essi coincide col sottogruppo banale (0).

(10) Se R è un anello commutativo con unità, descrivere gli ideali $I \subset R$ tali che l'R-modulo R/I sia *libero*: possieda cioè una R-base.

(11) Sia R un anello commutativo con unità e V un R-modulo libero finitamente generato. Dimostrare o confutare le seguenti affermazioni
- Ogni insieme di generatori contiene una base;
- Ogni insieme linearmente indipendente può essere completato ad una base.

(12) Sia $\varphi : \mathbb{Z}^k \to \mathbb{Z}^k$ un omomorfismo di $\mathbb{Z}$-moduli dato dalla moltiplicazione a sinistra per la matrice A a coefficienti interi. Mostrare che l'immagine di φ è di indice finito in $\mathbb{Z}^k$ se e solo se A ha determinante non nullo e che, in tal caso, l'indice dell'immagine Im (φ) in $\mathbb{Z}^k$ coincide con $|\det(A)|$.

(13) Sia K un campo e $f(x) \in K[x]$ un polinomio monico di grado n. Esibire una matrice quadrata M tale che il polinomio caratteristico $\det(M - xI)$ sia $(-1)^n f(x)$.

(14) L'annullatore di un R-modulo M è l'insieme

$$I = \{r \in R \,|\, rm = 0 \text{ per ogni } m \in M\}.$$

Mostrare che I è un ideale di R e calcolare l'annullatore dei seguenti $\mathbb{Z}$-moduli:
- $\mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(4)$;
- $\mathbb{Z}$;
- $\mathbb{Z}/(d_1) \times \mathbb{Z}/(d_2) \times \cdots \times \mathbb{Z}/(d_n)$ se $d_1|d_2| \ldots |d_n$.

(15) Calcolare il polinomio minimo di $\sqrt{3} + \sqrt{5}$ sul campo K, quando K è
- $\mathbb{Q}$;
- $\mathbb{Q}(\sqrt{5})$;
- $\mathbb{Q}(\sqrt{10})$;
- $\mathbb{Q}(\sqrt{15})$.

(16) Sia α una radice complessa del polinomio (irriducibile) $x^3 - 3x + 4 \in \mathbb{Q}[x]$. Scrivere esplicitamente l'inverso di $\alpha^2 + \alpha + 1$ nella forma $a + b\alpha + c\alpha^2$ con $a, b, c \in \mathbb{Q}$.

(17) Siano $K \subset L$ campi e $\alpha \in L$ un elemento algebrico su K tale che $[K(\alpha) : K] = 5$. Mostrare che $K(\alpha^2) = K(\alpha)$.

(18) Mostrare che $\zeta_5 \notin \mathbb{Q}(\zeta_7)$, se $\zeta_n = e^{2\pi i/n}$.

(19) Se $\zeta_n = e^{2\pi i/n}$, calcolare il polinomio minimo su $\mathbb{Q}$ di $\zeta_4, \zeta_6, \zeta_8, \zeta_9, \zeta_{10}, \zeta_{12}$.

(20) Sia p un numero primo e $q(x) \in \mathbb{F}_p[x]$. Mostrare che se α è una radice di $q(x)$ in un'estensione K di $\mathbb{F}_p$, allora anche α^p è radice di $q(x)$.

(21) Utilizzare l'esercizio precedente per mostrare che se $q(x) \in \mathbb{F}_p[x]$ divide $x^p - x - 1$, allora $q(x)$ ha grado p. Concludere che $x^p - x - 1$ è irriducibile in $\mathbb{F}_p[x]$.

(22) Sia p un numero primo e $f(x) \in \mathbb{F}_p[x]$ un polinomio non costante con derivata nulla. Mostrare che $f(x)$ non è irriducibile.

(23) I due campi $\mathbb{F}_2[x]/(x^3+x+1)$ e $\mathbb{F}_2[x]/(x^3+x^2+1)$ hanno entrambi otto elementi e sono quindi isomorfi. Costruire tutti gli isomorfismi tra tali due campi.
(24) Quanti sono i polinomi irriducibili monici di grado 3 a coefficienti in $\mathbb{F}_3$ e $\mathbb{F}_5$?
(25) Sia K un campo con p^n elementi, $\alpha \in K$ un generatore ciclico del gruppo moltiplicativo $K^\times$. Mostrare che il polinomio minimo di α su $\mathbb{F}_p$ ha grado n. E' vero il viceversa?
(26) Sia $\alpha \in \mathbb{C}$ una radice del polinomio x^3+x+1. Calcolare il polinomio minimo di α^2+1 su $\mathbb{Q}$.
(27) Siano $\alpha, \beta \in \mathbb{C}$ radici, rispettivamente, dei polinomi $f(x), g(x) \in \mathbb{Q}[x]$. Se $K = \mathbb{Q}(\alpha), L = \mathbb{Q}(\beta)$, mostrare che $f(x)$ è irriducibile in $L[x]$ se e solo se $g(x)$ è irriducibile in $K[x]$.
(28) Sia $q(x) \in K[x]$ un polinomio irriducibile a coefficienti nel campo K di caratteristica 0. Mostrare che $q(x)$ divide $MCD(f(x), f'(x)$ se e solo se $q(x)^2$ divide $f(x)$.
(29) Se P è un poligono regolare con n lati, è possibile costruire con riga e compasso un quadrato Q con area uguale all'area di P?
(30) Sia K un campo e $\varphi : K(x) \to K(x)$ un automorfismo tale che $\varphi(c) = c$ per ogni $c \in K$. Mostrare che esistono $a, b, c, d \in K$ tali che $\varphi(x) = (ax+b)/(cx+d)$.
(31) Fattorizzare esplicitamente in $\mathbb{F}_3[x]$ i polinomi $x^9 - x$ e $x^{27} - x$.
(32) Se $K = \mathbb{F}_p(t)$, consideriamo il polinomio $f(x) = x^p - t \in K[x]$. Mostrare che $f(x)$ è irriducibile in $K[x]$; mostrare inoltre che se $f(x)$ possiede una radice α in un'estensione di K, allora α non è una radice semplice.
(33) Sia K un campo e $\overline{K}$ la sua chiusura algebrica. Mostrare che se K è finito, allora $\overline{K}$ è infinito numerabile, mentre se K è infinito, allora $\overline{K}$ ha la stessa cardinalità di K.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI ROMA – "LA SAPIENZA"
E-mail address: dandrea@mat.uniroma1.it