

Corso di Algebra 1 - a.a. 2025-2026

Prova scritta del 03/09/2026

1. Dato un gruppo finito G , sia $O(G)$ il sottoinsieme di $\mathbb{N}$ costituito dagli interi k tali che G contiene un elemento di ordine k .
 - (a) Dimostrare che, se $k \in O(G)$ e d è un divisore positivo di k , allora $d \in O(G)$.
 - (b) Dimostrare che, se H è un sottogruppo normale di G , allora $O(G/H) \subseteq O(G)$.
 - (c) Dimostrare che, se G è abeliano, allora $O(G) \neq O(S_3)$.
 - (d) Trovare un intero $n > 1$ tale che $O(A_n) = \{k \in \mathbb{N} : 1 \leq k \leq n\}$.
2. Sia A un anello commutativo con un solo ideale I diverso sia da $\{0\}$ che da A .
 - (a) Dimostrare che ogni elemento di $A \setminus I$ è invertibile.
 - (b) Dimostrare che, se esiste un omomorfismo suriettivo e non iniettivo di anelli $A \rightarrow B$ con $B \neq \{0\}$, allora B è un campo.
 - (c) Dimostrare che, se $A = K[X]/(f)$ con K campo e $f \in K[X]$ polinomio di grado $d > 0$, allora d è pari.
 - (d) Dimostrare che, se $A = \mathbb{Z}[X]/(p, 2X^4 - X^2 - 1)$ con p numero primo, allora $p = 2$.

Soluzioni

1. (a) Poiché $k \in O(G)$, per definizione esiste $a \in G$ tale che $\text{ord}(a) = k$. Per ipotesi esiste un intero positivo m tale che $k = dm$, e dunque

$$\text{ord}(a^m) = \frac{\text{ord}(a)}{\text{mcd}(\text{ord}(a), m)} = \frac{k}{\text{mcd}(k, m)} = \frac{dm}{m} = d,$$

il che dimostra che $d \in O(G)$.

- (b) Per ogni $d \in O(G/H)$ per definizione esiste $a \in G$ tale che $\text{ord}(aH) = d$. D'altra parte $\text{ord}(aH)$ è un divisore positivo di $\text{ord}(a)$ perché $aH = \pi(a)$, con $\pi: G \rightarrow G/H$ omomorfismo di proiezione al quoziente, e $\text{ord}(a) < \infty$ (essendo G finito). Dato che $\text{ord}(a) \in O(G)$, segue allora dal punto precedente che $d \in O(G)$.
- (c) Si osservi intanto che $O(S_3) = \{1, 2, 3\}$: infatti, a parte l'elemento neutro (di ordine 1), gli unici elementi di S_3 sono i 2-cicli (di ordine 2) e i 3-cicli (di ordine 3). Per assurdo sia G abeliano tale che $O(G) = \{1, 2, 3\}$. In particolare, esistono $a, b \in G$ tali che $\text{ord}(a) = 2$ e $\text{ord}(b) = 3$. Poiché $ab \neq 1$ (altrimenti si avrebbe $b = a^{-1} = a$), $(ab)^2 = a^2b^2 = b^2 \neq 1$ e $(ab)^3 = a^3b^3 = a \neq 1$, si ottiene la contraddizione $3 < \text{ord}(ab) \in O(G)$. In effetti è facile vedere che $\text{ord}(ab) = 6$ (più in generale è vero che, se $ab = ba$, $\text{ord}(a) = m$, $\text{ord}(b) = n$ e $\text{mcd}(m, n) = 1$, allora $\text{ord}(ab) = mn$).
- (d) Si può prendere $n = 7$. Infatti, ricordando che l'ordine di una permutazione è il minimo comune multiplo delle lunghezze dei cicli disgiunti che la costituiscono e che la permutazione è pari se e solo se un numero pari di tali lunghezze è pari, a parte l'elemento neutro (di ordine 1), gli elementi di A_7 hanno tutti e soli i seguenti tipi di decomposizione in cicli disgiunti:
- 2-ciclo + 2-ciclo (di ordine 2);
 - 3-ciclo e 3-ciclo + 3-ciclo (di ordine 3);
 - 4-ciclo + 2-ciclo (di ordine 4);
 - 5-ciclo (di ordine 5);
 - 3-ciclo + 2-ciclo + 2-ciclo (di ordine 6);
 - 7-ciclo (di ordine 7).

Inoltre è facile vedere che 7 è il minimo (in realtà anche l'unico) valore possibile di n : analogamente per $1 < n < 7$ si trova

$$\begin{aligned} O(A_2) &= \{1\}, & O(A_3) &= \{1, 3\}, & O(A_4) &= \{1, 2, 3\}, \\ O(A_5) &= \{1, 2, 3, 5\}, & O(A_6) &= \{1, 2, 3, 4, 5\}. \end{aligned}$$

2. (a) Dato $a \in A \setminus I$, l'ideale (a) di A è tale che $(a) \neq I$ (perché $a \in (a)$ e $a \notin I$) e ovviamente $(a) \neq \{0\}$. Per ipotesi si ha allora $(a) = A$, e quindi esiste $a' \in A$ tale che $1 = aa' = a'a$, cioè $a \in A^*$.
- (b) Sia $\alpha: A \rightarrow B$ un omomorfismo suriettivo e non iniettivo di anelli con $B \neq \{0\}$. Allora B è commutativo perché A lo è e α è un omomorfismo suriettivo. Per dimostrare che B è un campo resta da verificare che $b \in B^*$ per ogni $b \in B \setminus \{0\}$. Per la suriettività di α esiste $a \in A$ tale che $b = \alpha(a)$; inoltre $a \notin \ker(\alpha)$ perché $\alpha(a) = b \neq 0$. D'altra parte $\ker(\alpha)$ è un ideale di A diverso sia da $\{0\}$ (perché α non è iniettivo) che da A (perché $\alpha(1_A) = 1_B \neq 0_B$). Pertanto deve essere $\ker(\alpha) = I$, e dunque $a \in A \setminus I$. Per il punto precedente questo implica $a \in A^*$, da cui segue $b = \alpha(a) \in B^*$.
- (c) Gli ideali di $A = K[X]/(f)$ sono tutti e soli della forma $J/(f)$ con J ideale di $K[X]$ contenente f . Poiché $K[X]$ è un dominio a ideali principali (essendo K un campo), deve essere $J = (g)$ per qualche $g \in K[X]$, e la condizione $(f) \subseteq (g)$ equivale a $g \mid f$. Perciò gli ideali di A sono in corrispondenza biunivoca con i divisori monici di f in $K[X]$. Se $f = c \prod_{i=1}^n p_i^{e_i}$ con $c \in K \setminus \{0\}$, i p_i irriducibili monici distinti di $K[X]$ e gli e_i interi positivi, i divisori monici di f sono tutti e soli della forma $\prod_{i=1}^n p_i^{e'_i}$ con $0 \leq e'_i \leq e_i$ per ogni $i = 1, \dots, n$. Se ne deduce che il numero degli ideali di A (che per ipotesi è 3) è $\prod_{i=1}^n (e_i + 1)$, da cui segue immediatamente $n = 1$ e $e_1 = 2$. Pertanto $d = \deg(f) = 2 \deg(f_1)$ è pari.
- (d) Posto $f := 2X^4 - X^2 - 1$, per il terzo teorema di isomorfismo per anelli si ha

$$A = \mathbb{Z}[X]/(p, f) \cong (\mathbb{Z}[X]/(p))/(\bar{f}) \cong \mathbb{Z}/p\mathbb{Z}[X]/(\bar{f}),$$

con $\bar{f} = 2X^4 - X^2 - \bar{1} \in \mathbb{Z}/p\mathbb{Z}[X]$. Poiché $\mathbb{Z}/p\mathbb{Z}$ è un campo (essendo p un numero primo), per quanto visto nel punto precedente $\bar{f}$ deve essere associato al quadrato di un irriducibile di $\mathbb{Z}/p\mathbb{Z}[X]$. Ora, questo succede per $p = 2$ (nel qual caso $\bar{f} = X^2 - \bar{1} = (X - \bar{1})^2$), ma non per $p > 2$. Infatti, osservando che $f = (X - 1)(X + 1)(2X^2 + 1)$ in $\mathbb{Z}[X]$, si ha in ogni caso $\bar{f} = (X - \bar{1})(X + \bar{1})(\bar{2}X^2 + \bar{1})$ in $\mathbb{Z}/p\mathbb{Z}[X]$, e $X - \bar{1}$ e $X + \bar{1}$ sono irriducibili monici distinti per $p > 2$.