Corso di Algebra 1 - a.a. 2023-2024

Prova scritta del 14/02/2024

1. Dati un gruppo G e un intero positivo k, sia $Z_k(G)$ il sottoinsieme di G costituito dagli elementi il cui ordine divide k.

   (a) Dimostrare che, se G è abeliano, allora $Z_k(G)$ è un sottogruppo di G per ogni k.

   (b) Dimostrare che $Z_2(S_n)$ non è un sottogruppo di S_n per $n \geq 3$.

   (c) Trovare k tale $Z_k(S_3)$ è un sottogruppo non banale di S_3.

   (d) Esiste k tale $Z_k(S_4)$ è un sottogruppo non banale di S_4?

2. Sia K un campo e sia $A := \{f \in K[X] : f(0) = f(1)\}$.

   (a) Dimostrare che A è un sottoanello di $K[X]$.

   (b) Dimostrare che per ogni $f \in A$ esistono unici $g \in K[X]$ e $a \in K$ tali che $f = (X^2 - X)g + a$.

   (c) Dato $f \in A$ tale che $f(0) \neq 0$, dimostrare che $fA = A \cap fK[X]$.

   (d) Dato $f \in A \setminus \{0\}$ tale che $f(0) = 0$, dimostrare che $fK[X]$ è un ideale non principale di A.

Soluzioni

1. Osserviamo preliminarmente che, dato $a \in G$, si ha (per le proprietà dell'ordine di un elemento) $a \in Z_k(G)$ se e solo se $a^k = 1$.

   (a) $1 \in Z_k(G)$ perché $1^k = 1$. Se $a, b \in Z_k(G)$, cioè $a^k = b^k = 1$, allora $ab, a^{-1} \in Z_k(G)$ perché $(ab)^k = a^k b^k = 1 \cdot 1 = 1$ (essendo $ab = ba$) e $(a^{-1})^k = (a^k)^{-1} = 1^{-1} = 1$.

   (b) Ogni trasposizione (avendo ordine 2) appartiene a $Z_2(S_n)$. In particolare $(1,2), (2,3) \in Z_2(S_n)$, ma $(1,2)(2,3) = (1,2,3) \notin Z_2(S_n)$ (i 3-cicli hanno ordine 3).

   (c) Per esempio $Z_3(S_3) = A_3$ è un sottogruppo non banale di S_3. Infatti A_3 è costituito dall'elemento neutro (1) (di ordine 1) e dai 3-cicli (di ordine 3), mentre gli altri elementi di S_3 sono trasposizioni (di ordine 2).

   (d) No, non esiste. Sia infatti k tale che $Z_k(S_4)$ è un sottogruppo di S_4; va dimostrato che allora $Z_4(S_4)$ è S_4 o $\{(1)\}$. Se k è pari, allora $Z_k(S_4)$ contiene tutti gli elementi di ordine 2, e in particolare tutte le trasposizioni. Poiché le trasposizioni generano S_4 e $Z_k(S_4)$ è un sottogruppo di S_4, ne segue che in questo caso $Z_k(S_4) = S_4$. Se invece k (e quindi ogni suo divisore) è dispari, allora $Z_k(S_4)$ contiene solo elementi di ordine dispari. Poiché gli unici elementi di ordine dispari in S_4 sono (1) (di ordine 1) e i 3-cicli (di ordine 3), se ne deduce che $Z_k(S_4) = \{(1)\}$ se $3 \nmid k$. D'altra parte non può essere $3 \mid k$ perché in quel caso $Z_k(S_4)$ sarebbe costituito precisamente dall'elemento neutro e dagli 8 3-cicli. Si avrebbe allora $\#(Z_k(S_4)) = 9 \nmid 24 = \#S_4$, impossibile per il teorema di Lagrange.

2. (a) Chiaramente $1 \in A$, e più in generale $a \in A$ per ogni $a \in K$, dato che $a(0) = a(1) = a$. Inoltre per ogni $f, g \in A$ si ha

$$(f-g)(0) = f(0) - g(0) = f(1) - g(1) = (f-g)(1),$$
$$(fg)(0) = f(0)g(0) = f(1)g(1) = (fg)(1),$$

   il che dimostra che $f - g, fg \in A$.

   (b) Facendo la divisione con resto in $K[X]$ di f per $X^2 - X$ si trova che esistono unici $g, r \in K[X]$ tali che $f = (X^2 - X)g + r$ con

$r = 0$ o $\deg(r) < \deg(X^2 - X) = 2$. La condizione su r equivale al fatto che esistono unici $a, b \in K$ tali che $r = a + bX$. Poiché

$$f(0) = (0^2 - 0)g(0) + r(0) = a,$$
$$f(1) = (1^2 - 1)g(1) + r(1) = a + b,$$

l'ipotesi $f(0) = f(1)$ equivale a $b = 0$, cioè a $r = a$, come richiesto.

(c) Poiché $f \in A \subseteq K[X]$ e A è un sottoanello di $K[X]$ per il punto precedente, è ovvio che $fA \subseteq A$ e $fA \subseteq fK[X]$, per cui vale l'inclusione $fA \subseteq A \cap fK[X]$. Per dimostrare l'inclusione opposta, sia $h \in A \cap fK[X]$. Esiste allora $g \in K[X]$ tale che $h = fg$ e $h(0) = h(1)$. Dall'uguaglianza $h(i) = f(i)g(i)$ per $i = 0, 1$ e dall'ipotesi $f(0) = f(1) \neq 0$ si ottiene $g(i) = f(i)^{-1}h(i)$ per $i = 0, 1$, e quindi $g(0) = g(1)$. Ciò dimostra $g \in A$, e dunque $h = fg \in fA$.

(d) Poiché $f(0) = f(1) = 0$, per ogni $g \in K[X]$ si ha $(fg)(i) = f(i)g(i) = 0$ per $i = 0, 1$, e in particolare $(fg)(0) = (fg)(1)$, cioè $fg \in A$. Pertanto $I := fK[X] \subseteq A$ e I è un ideale di A (essendo un ideale di $K[X]$ contenuto nel suo sottoanello A). Supponiamo ora per assurdo che I sia principale in A, cioè che esista $p \in I$ tale che $I = pA$. Per definizione di I esiste $g \in K[X]$ tale che $p = fg$; inoltre $f \in I = pA$, per cui esiste $h \in A$ tale che $f = ph$. Pertanto $f = ph = fgh$, da cui si deduce (essendo $K[X]$ un dominio e $f \neq 0$) $gh = 1$. In particolare $g \in K[X]^* = K^* = K \setminus \{0\}$, e poiché chiaramente $K^* \subseteq A^*$ (in effetti $K^* = A^*$), si ottiene che f e $p = fg$ sono associati in A. Dunque $I = pA = fA$, e per ottenere un assurdo basta osservare che per ogni $k \in K[X] \setminus A$ (per esempio $k = X$) si ha $fk \in I$ ma $fk \notin fA$ (si noti che non esiste $\tilde{k} \in A$ tale che $fk = f\tilde{k}$ perché, sempre grazie al fatto che $K[X]$ è un dominio e $f \neq 0$, si avrebbe $\tilde{k} = k \notin A$).