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

Prova scritta del 16/06/2026

1. Dato un sottogruppo H di un gruppo G e un intero k sia

$$H_k := \{a \in G \,:\, a^k \in H\}.$$

   (a) Dimostrare che, se G è abeliano, allora H_k è un sottogruppo di G.

   (b) Dimostrare che, se $[G : H] = 2$, allora $H_k = G$ per k pari e $H_k = H$ per k dispari.

   (c) Nel caso in cui $G = D_n$ con $n > 2$ e $H = \langle S \rangle$, dimostrare che H_2 non è un sottogruppo di G.

   (d) Nel caso in cui $G = S_4$ e $H = V_4$, dimostrare che H_k non è un sottogruppo di G se e solo se k è divisibile per 2 ma non per 3.

2. Sia $I := \{f \in \mathbb{Z}[X] \,:\, f(n) \in 2\mathbb{Z}\ \forall n \in \mathbb{Z}\}$.

   (a) Dimostrare che I è un ideale di $\mathbb{Z}[X]$.

   (b) Trovare $g \in I$ monico e di secondo grado.

   (c) Dimostrare che, se g è come nel punto precedente, allora $I = (2, g)$.

   (d) Dimostrare che $\mathbb{Z}[X]/I$ è isomorfo al prodotto di due campi.

Soluzioni

1. (a) $1 \in H_k$ perché $1^k = 1 \in H$. Dati $a, b \in H_k$ (cioè $a^k, b^k \in H$) si ha $ab^{-1} \in H_k$ perché $(ab^{-1})^k = a^k(b^{-1})^k = a^k(b^k)^{-1} \in H$.

   (b) Posto $\bar{a} := aH \in G/H$ per ogni $a \in G$, si ha $a \in H_k$ (cioè $a^k \in H$) se e solo se $\overline{a^k} = \bar{1}$. Poiché H è normale in G (avendo indice 2), G/H è un gruppo e $\overline{a^k} = \bar{a}^k$. Se ne deduce che $a \in H_k$ se e solo se $\mathrm{ord}_{G/H}(\bar{a}) \mid k$. D'altra parte $\#(G/H) = [G : H] = 2$, e quindi $\mathrm{ord}_{G/H}(\bar{a}) = 1$ se $\bar{a} = \bar{1}$ (cioè se $a \in H$) e $\mathrm{ord}_{G/H}(\bar{a}) = 2$ se $\bar{a} \neq \bar{1}$ (cioè se $a \notin H$). Si conclude allora che per k pari $\mathrm{ord}_{G/H}(\bar{a}) \mid k$ per ogni $a \in G$ (dunque $H_k = G$) e per k dispari $\mathrm{ord}_{G/H}(\bar{a}) \mid k$ se e solo se $a \in H$ (dunque $H_k = H$).

   (c) $R^i S \in H_2$ per ogni $i \in \mathbb{Z}$ perché $(R^i S)^2 = 1 \in H$. In particolare $RS, S \in H_2$, ma $RSS = R \notin H_2$, dato che $R^2 \notin H = \{1, S\}$. Pertanto H_2 non è un sottogruppo di D_n.

   (d) In ogni caso $H = V_4 \subseteq H_k$. Gli elementi di $S_4 \setminus V_4$ sono solo gli l-cicli, per $l = 2, 3, 4$. Tenendo conto che un l-ciclo ha ordine l, per ogni l-ciclo $(i_1, ..., i_l)$ (con $i_1, \ldots, i_l \in \{1, 2, 3, 4\}$ distinti) si ha

$$(i_1, i_2)^k = \begin{cases} (1) \in V_4 & \text{se } k \equiv 0 \mod 2, \\ (i_1, i_2) \notin V_4 & \text{se } k \equiv 1 \mod 2, \end{cases}$$

$$(i_1, i_2, i_3)^k = \begin{cases} (1) \in V_4 & \text{se } k \equiv 0 \mod 3, \\ (i_1, i_2, i_3) \notin V_4 & \text{se } k \equiv 1 \mod 3, \\ (i_1, i_3, i_2) \notin V_4 & \text{se } k \equiv 2 \mod 3, \end{cases}$$

$$(i_1, i_2, i_3, i_4)^k = \begin{cases} (1) \in V_4 & \text{se } k \equiv 0 \mod 4, \\ (i_1, i_2, i_3, i_4) \notin V_4 & \text{se } k \equiv 1 \mod 4, \\ (i_1, i_3)(i_2, i_4) \in V_4 & \text{se } k \equiv 2 \mod 4, \\ (i_1, i_4, i_3, i_2) \notin V_4 & \text{se } k \equiv 3 \mod 4. \end{cases}$$

   Indicando con Z_l l'insieme degli l-cicli in S_4, si ha dunque

$$H_k = \begin{cases} V_4 & \text{se } 2 \nmid k,\ 3 \nmid k, \\ V_4 \cup Z_2 \cup Z_4 & \text{se } 2 \mid k,\ 3 \nmid k, \\ V_4 \cup Z_3 = A_4 & \text{se } 2 \nmid k,\ 3 \mid k, \\ V_4 \cup Z_2 \cup Z_3 \cup Z_4 = S_4 & \text{se } 2 \mid k,\ 3 \mid k. \end{cases}$$

   Per concludere basta osservare che V_4, A_4 e S_4 sono sottogruppi di S_4, mentre $V_4 \cup Z_2 \cup Z_4$ non lo è (per esempio perché contiene $(1, 2)$ e $(1, 3)$ ma non $(1, 2)(1, 3) = (1, 3, 2)$).

2. (a) $0 \in I$ perché $0(n) = 0 \in 2\mathbb{Z}$ per ogni $n \in \mathbb{Z}$. Dati $f, f' \in I$ (cioè $f(n), f'(n) \in 2\mathbb{Z}$ per ogni $n \in \mathbb{Z}$) e $h \in \mathbb{Z}[X]$ si ha $f + f', fh \in I$ perché

$$(f + f')(n) = f(n) + f'(n) \in 2\mathbb{Z}, \qquad (fh)(n) = f(n)h(n) \in 2\mathbb{Z}$$

per ogni $n \in \mathbb{Z}$, dato che $2\mathbb{Z}$ è un ideale di Z.

(b) Si può prendere per esempio $g = X^2 + X$. Infatti in tal caso $g(n) = n^2 + n = n(n + 1) \in 2\mathbb{Z}$ per ogni $n \in \mathbb{Z}$ (essendo uno tra n e $n + 1$ sempre pari).

(c) L'inclusione $(2, g) \subseteq I$ segue dal fatto che $2, g \in I$ e che I è un ideale per il primo punto. Per dimostrare che anche $I \subseteq (2, g)$, sia $f \in I$. Poiché g è monico, esistono (unici) $q, r \in \mathbb{Z}[X]$ tali che $f = qg + r$ con $r = 0$ o $\deg(r) < \deg(g) = 2$. Esistono allora $a, b \in \mathbb{Z}$ tali che $r = aX + b$. D'altra parte $r \in I$ (perché $r = f - qg$ con $f, g \in I$ e I è un ideale), e quindi $r(n) = an + b \in 2\mathbb{Z}$ per ogni $n \in \mathbb{Z}$. In particolare $r(0) = b$ e $r(1) = a + b$ sono pari, e pertanto lo è anche $a = a + b - b$. Ciò implica che $r = 2r'$ con $r' := (a/2)X + b/2 \in \mathbb{Z}[X]$, e dunque $f = qg + r = qg + 2r' \in (2, g)$.

(d) Per il punto precedente $I = (2, g) = (2, X^2 + X)$. Usando il terzo teorema di isomorfismo per anelli si ottiene allora

$$\mathbb{Z}[X]/I = \mathbb{Z}[X]/(2, g) \cong \big(\mathbb{Z}[X]/(2)\big)/(\bar{g}) \cong \mathbb{Z}/2\mathbb{Z}[X]/(X^2 + X).$$

In $\mathbb{Z}/2\mathbb{Z}[X]$ l'ideale $J := (X^2 + X)$ è tale che $J = J_0 J_1$ con $J_0 := (X)$ e $J_1 := (X + \bar{1})$. Poiché J_0 e J_1 sono coprimi (dato che $\bar{1} = X + X + \bar{1} \in J_0 + J_1$), per il teorema cinese generalizzato si ha $\mathbb{Z}/2\mathbb{Z}[X]/J \cong \mathbb{Z}/2\mathbb{Z}[X]/J_0 \times \mathbb{Z}/2\mathbb{Z}[X]/J_1$. Ricordando che se A è un anello commutativo e $a \in A$ allora $A[X]/(X - a) \cong A$, si conclude che

$$\mathbb{Z}[X]/I \cong \mathbb{Z}/2\mathbb{Z}[X]/(X) \times \mathbb{Z}/2\mathbb{Z}[X]/(X + \bar{1}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

e $\mathbb{Z}/2\mathbb{Z}$ è un campo (perché 2 è un numero primo).