Corso di Algebra 1 - a.a. 2024-2025

Prova scritta del 02/09/2025

1. Dato un gruppo G, sia

$$K := \{f \in \mathrm{Aut}(G) \,:\, f(H) = H \text{ per ogni sottogruppo } H \text{ di } G\}.$$

   (a) Dimostrare che K è un sottogruppo di $\mathrm{Aut}(G)$.

   (b) Dimostrare che K è normale in $\mathrm{Aut}(G)$.

   (c) Dimostrare che $K = \mathrm{Aut}(G)$ se $G = \mathbb{Z}/n\mathbb{Z}$ per qualche intero positivo n.

   (d) Dimostrare che $\{\mathrm{id}_G\} \subsetneq K \subsetneq \mathrm{Aut}(G)$ se $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

2. Dati due omomorfismi di anelli $f, g\colon A \to B$, siano

$$A' := \{a \in A \,:\, f(a) = g(a)\}, \qquad D := \{f(a) - g(a) \,:\, a \in A\}.$$

   (a) Dimostrare che A' è un sottoanello di A.

   (b) Dimostrare che D è un ideale di B se $f(A') = B$.

   (c) Nel caso in cui B è commutativo, $A = B[X]$ ed esiste $b \in B$ tale che $f(p) = p(b)$ e $g(p) = p(0)$ per ogni $p \in B[X]$, dimostrare che $D = (b)$.

   (d) Fornire un esempio in cui $A = \mathbb{Z}[X]$, $B = \mathbb{Q}$ e D non è un ideale di B.

Soluzioni

1. (a) Chiaramente $\mathrm{id}_G \in K$, dato che $\mathrm{id}_G(H) = H$ per ogni sottogruppo H di G. Se $f, g \in K$, anche $f \circ g^{-1} \in K$ perché

$$f \circ g^{-1}(H) = f(g^{-1}(H)) = f(g^{-1}(g(H))) = f(H) = H$$

per ogni sottogruppo H di G.

(b) Per ogni $f \in K$ e per ogni $g \in \mathrm{Aut}(G)$ si ha $g \circ f \circ g^{-1} \in K$ perché per ogni sottogruppo H di G si ha (tenendo conto che, essendo g^{-1} un omomorfismo, $g^{-1}(H)$ è un sottogruppo di G, e dunque $f(g^{-1}(H)) = g^{-1}(H)$)

$$g \circ f \circ g^{-1}(H) = g(f(g^{-1}(H))) = g(g^{-1}(H)) = H.$$

(c) Va dimostrato che $f(H) = H$ per ogni $f \in \mathrm{Aut}(G)$ e per ogni sottogruppo H di $G = \mathbb{Z}/n\mathbb{Z}$. Posto $d := \#H$ (che è un divisore di n per il teorema di Lagrange), è noto che $H = \langle \frac{n}{d} + n\mathbb{Z} \rangle$ è l'unico sottogruppo di G di ordine d. Poiché $f(H)$ è pure un sottogruppo di G di ordine d (essendo f un isomorfismo), si conclude che $f(H) = H$.

(d) La funzione $f\colon G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \to G$ definita da $(x, y) \mapsto (y, x)$ è chiaramente un automorfismo di G. Dato che $H := \mathbb{Z}/3\mathbb{Z} \times \{\bar{0}\}$ è un sottogruppo di G tale che $f(H) = \{\bar{0}\} \times \mathbb{Z}/3\mathbb{Z} \neq H$, si ottiene $f \in \mathrm{Aut}(G) \setminus K$, per cui $K \subsetneq \mathrm{Aut}(G)$.

Più in generale è molto facile vedere che, se G è un gruppo abeliano additivo, la funzione $g\colon G \to G$ definita da $a \mapsto -a$ è un automorfismo di G tale che $g(H) = H$ per ogni sottogruppo H di G (cioè $g \in K$). Inoltre, se $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, si ha per esempio $g((\bar{1}, \bar{0})) = (\overline{-1}, \bar{0}) \neq (\bar{1}, \bar{0})$. Questo dimostra $g \in K \setminus \{\mathrm{id}_G\}$, e pertanto $\{\mathrm{id}_G\} \subsetneq K$.

2. (a) $1_A \in A'$ perché $f(1_A) = 1_B = g(1_A)$. Dati $a, a' \in A'$, anche $a - a', aa' \in A'$ perché

$$f(a - a') = f(a) - f(a') = g(a) - g(a') = g(a - a'),$$
$$f(aa') = f(a)f(a') = g(a)g(a') = g(aa').$$

(b) Chiaramente $0_B = 0_B - 0_B = f(0_A) - g(0_A) \in D$. Dati $d, \tilde{d} \in D$ e $b \in B$, esistono $a, \tilde{a} \in A$ e $a' \in A'$ tali che $d = f(a) - g(a)$,

$\tilde{d} = f(\tilde{a}) - g(\tilde{a})$ e $b = f(a') = g(a')$. Si ottiene allora

$$\begin{aligned} d + \tilde{d} &= f(a) - g(a) + f(\tilde{a}) - g(\tilde{a}) = f(a + \tilde{a}) - g(a + \tilde{a}), \\ bd &= b(f(a) - g(a)) = f(a')f(a) - g(a')g(a) = f(a'a) - g(a'a), \\ db &= (f(a) - g(a))b = f(a)f(a') - g(a)g(a') = f(aa') - g(aa'), \end{aligned}$$

il che dimostra che $d + \tilde{d}, bd, db \in D$.

(c) Per definizione gli elementi di D sono tutti e soli quelli della forma $p(b) - p(0)$ con $p \in B[X]$. Se $p = \sum_{i=0}^{n} b_i X^i$ (con $b_i \in B$), si ha

$$p(b) - p(0) = \sum_{i=0}^{n} b_i b^i - b_0 = \sum_{i=1}^{n} b_i b^i = b \sum_{i=1}^{n} b_i b^{i-1} \in (b),$$

e dunque $D \subseteq (b)$. D'altra parte vale anche $(b) \subseteq D$ perché per ogni $b' \in B$ si ha $b'b = p(b) - p(0) \in D$ prendendo $p = b'X$.

(d) Si può prendere per esempio $f(p) := p(1)$ e $g(p) := p(0)$ per ogni $p \in \mathbb{Z}[X]$. In effetti $f = i \circ f'$ e $g = i \circ g'$, dove i indica l'inclusione di $\mathbb{Z}$ in $\mathbb{Q}$ e f' e g' sono definiti come f e g, ma considerandoli come omomorfismi $\mathbb{Z}[X] \to \mathbb{Z}$. Indicando con D' il sottoinsieme di $\mathbb{Z}$ definito come D, ma relativo a f' e g', per il punto precedente di ha $D' = (1) = \mathbb{Z}$. Poiché chiaramente $D = i(D')$, si conclude che $D = \mathbb{Z}$ non è un ideale di $\mathbb{Q}$ (essendo $\mathbb{Q}$ un campo, i suoi unici ideali sono $\{0\}$ e $\mathbb{Q}$).