Corso di Algebra 1 - a.a. 2017-2018

Prova scritta del 06/09/2018

1. Sia G un gruppo. Trovare un sottogruppo normale K di G tale che $K \cong G/K$ in ciascuno dei seguenti casi.

   (a) Esiste un omomorfismo $f\colon G \to G$ tale che $\mathrm{im}(f) \cong \ker(f)$.

   (b) $G = \mathbb{Z}/n^2\mathbb{Z}$ per qualche intero positivo n.

   (c) $G = G' \times G'$ per qualche gruppo G'.

2. Indicando con $\varepsilon(\sigma) \in \{\pm 1\}$ il segno di una permutazione σ, sia

$$G := \{(\sigma, \overline{a}) \in S_3 \times \mathbb{Z}/4\mathbb{Z} \,:\, \varepsilon(\sigma) = (-1)^a\}.$$

   (a) Dimostrare che G è un sottogruppo di $S_3 \times \mathbb{Z}/4\mathbb{Z}$.

   (b) Dimostrare che G ha ordine 12 e che contiene un sottogruppo di indice 2.

   (c) Esiste un sottogruppo non normale di G?

3. Sia A un anello. Una funzione $d\colon A \to A$ è una *derivazione* se è un omomorfismo di gruppi additivi e $d(ab) = d(a)b + ad(b)$ per ogni $a, b \in A$.

   (a) Dimostrare che, per ogni $x \in A$, la funzione $d_x\colon A \to A$ definita da $d_x(a) := xa - ax$ è una derivazione di A.

   (b) Se $d\colon A \to A$ è una derivazione, dimostrare che $\ker(d)$ è un sottoanello di A.

   (c) Se $d\colon \mathbb{Q} \to \mathbb{Q}$ è una derivazione, dimostrare che d è identicamente nulla.

4. Per ogni $a \in \mathbb{Z}$ sia $f_a := X^5 + 3X^2 - 6X + a \in \mathbb{Z}[X]$.

   (a) Fattorizzare f_0.

   (b) Trovare $a < 0$ tale che f_a sia riducibile.

   (c) Dimostrare che f_a è irriducibile se a è dispari.

Soluzioni

1. (a) Basta prendere $K = \ker(f)$ (che è un sottogruppo normale di G). Infatti $G/K = G/\ker(f) \cong \operatorname{im}(f)$ per il primo teorema di isomorfismo e $\operatorname{im}(f) \cong \ker(f) = K$ per ipotesi.

   (b) Per ogni sottogruppo (necessariamente normale) H di $G = \mathbb{Z}/n^2\mathbb{Z}$, sia H che G/H sono ciclici (perché sottogruppi e quozienti di gruppi ciclici sono ciclici). Dunque $H \cong G/H$ se e solo se

   $$\#H = \#(G/H) = \frac{\#G}{\#H} = \frac{n^2}{\#H}$$

   se e solo $\#H = n$. Il sottogruppo cercato è allora $K := \langle \overline{n} \rangle$, dato che

   $$\#K = \operatorname{ord}(\overline{n}) = \frac{n^2}{\operatorname{mcd}(n, n^2)} = \frac{n^2}{n} = n.$$

   (c) Si può prendere $K = G' \times \{1\}$. Infatti la proiezione sul secondo fattore

   $$\begin{aligned} p\colon G = G' \times G' &\to G' \\ (a, b) &\mapsto b \end{aligned}$$

   è un omomorfismo suriettivo con $\ker(p) = K$ (che quindi è un sottogruppo normale di G). Inoltre, sempre per il primo teorema di isomorfismo,

   $$G/K = G/\ker(p) \cong \operatorname{im}(p) = G',$$

   e chiaramente anche $K \cong G'$.

2. (a) Chiaramente $((1), \overline{0}) \in G$. Essendo G finito, per concludere che è un sottogruppo basta dimostrare che, se $(\sigma, \overline{a}), (\tau, \overline{b}) \in G$ (cioè $\varepsilon(\sigma) = (-1)^a$ e $\varepsilon(\tau) = (-1)^b$), anche

   $$(\sigma, \overline{a})(\tau, \overline{b}) = (\sigma\tau, \overline{a} + \overline{b}) = (\sigma\tau, \overline{a + b}) \in G.$$

   Questo in effetti è vero perché

   $$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau) = (-1)^a(-1)^b = (-1)^{a+b}.$$

(b) Per ogni $\sigma \in S_3$ ci sono esattamente due elementi $\overline{a} \in \mathbb{Z}/4\mathbb{Z}$ tali che $(\sigma, \overline{a}) \in G$ ($\overline{a} = \overline{0}, \overline{2}$ se $\varepsilon(\sigma) = 1$ e $\overline{a} = \overline{1}, \overline{3}$ se $\varepsilon(\sigma) = -1$). Ne segue che che $\#G = 2 \cdot \#S_3 = 2 \cdot 6 = 12$.

L'elemento $g := ((1,2,3), \overline{2}) \in G$ (perché $\varepsilon((1,2,3)) = 1 = (-1)^2$) verifica

$$\operatorname{ord}(g) = \operatorname{mcm}(\operatorname{ord}((1,2,3)), \operatorname{ord}(\overline{2})) = \operatorname{mcm}(3,2) = 6.$$

Allora $\langle g \rangle$ è un sottogruppo di G di ordine 6, e quindi di indice 2.

(c) Sì: per esempio, $H := \langle h \rangle$ con $h := ((1,2), \overline{1})$. Infatti $h \in G$ perché $\varepsilon((1,2)) = -1 = (-1)^1$, e analogamente $k := ((1,3), \overline{1}) \in G$. Dunque H è un sottogruppo di G, e non è normale perché

$$\begin{aligned} khk^{-1} &= ((1,3), \overline{1})((1,2), \overline{1})((1,3), \overline{1})^{-1} \\ &= ((1,3)(1,2)(1,3)^{-1}, \overline{1} + \overline{1} - \overline{1}) = ((2,3), \overline{1}) \notin H. \end{aligned}$$

Per verificare quest'ultimo fatto basta osservare che $h^i = ((1,2)^i, \overline{i})$ e $(2,3) \neq (1,2)^i$ per ogni $i \in \mathbb{Z}$ ($(1,2)^i = (1)$ se i è pari e $(1,2)^i = (1,2)$ se i è dispari).

3. (a) Per ogni $a, b \in A$ si ha

$$d_x(a+b) = x(a+b) - (a+b)x = xa + xb - ax - bx = d_x(a) + d_x(b)$$

(dunque d_x è un omomorfismo di gruppi additivi) e

$$d_x(ab) = xab - abx = xab - axb + axb - abx = d_x(a)b + ad_x(b).$$

(b) $\ker(d)$ è un sottogruppo di A perché d è un omomorfismo di gruppi. Se inoltre $a, b \in \ker(d)$ (cioè $d(a) = d(b) = 0$), allora

$$d(ab) = d(a)b + ad(b) = 0b + a0 = 0,$$

cioè $ab \in \ker(d)$. Infine, dall'uguaglianza

$$d(1) = d(1 \cdot 1) = d(1)1 + 1d(1) = d(1) + d(1)$$

segue $d(1) = 0$ (per la legge di cancellazione nel gruppo $(A, +)$), cioè $1 \in \ker(d)$.

(c) Per il punto precedente $\ker(d)$ è un sottoanello di $\mathbb{Q}$, dunque contiene 1 e il sottogruppo generato da 1, cioè $\mathbb{Z}$. Dato $q = \frac{a}{b} \in \mathbb{Q}$ (con $a, b \in \mathbb{Z}$ e $b \neq 0$), si ha allora

$$0 = d(a) = d(bq) = d(b)q + bd(q) = 0q + bd(q) = bd(q),$$

da cui segue $d(q) = 0$, essendo $\mathbb{Q}$ un dominio e $b \neq 0$.

4. (a) La fattorizzazione completa è $f_0 = X(X^4 + 3X - 6)$: il secondo fattore è irriducibile per il criterio di Eisenstein relativo al primo 3.

   (b) È sufficiente trovare $n \in \mathbb{Z}$ tale che $f_0(n) > 0$, perché poi n sarà radice di f_a con $a = -f_0(n)$. Per esempio $f_0(-1) = 8$, dunque $f_{-8}(-1) = 0$, il che dimostra che f_{-8} è divisibile per $X+1$ e quindi è riducibile.

   (c) Se a è dispari f_a è irriducibile perché è monico e la sua riduzione modulo 2 è $X^5 + X^2 + \overline{1}$, che è irriducibile in $\mathbb{Z}/2Z[X]$. È infatti immediato verificare che $X^5 + X^2 + \overline{1}$ non ha radici in $\mathbb{Z}/2\mathbb{Z}$ e non è divisibile per l'unico polinomio irriducibile di secondo grado in $\mathbb{Z}/2Z[X]$, cioè $X^2 + X + \overline{1}$.