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

Prova scritta del 23/01/2024

1. Sia H un sottogruppo di un gruppo G. Si dice che H è *pienamente invariante* in G se $f(H) \subseteq H$ per ogni endomorfismo f di G.

   (a) Dimostrare che, se H è pienamente invariante in G, allora H è normale in G.

   (b) Dimostrare che, se G è ciclico, allora H è pienamente invariante in G.

   (c) Dimostrare che il sottogruppo dei commutatori $[G, G]$ è pienamente invariante in G.

   (d) Dimostrare che, se G è finito, H è normale in G e H e G/H hanno ordini coprimi, allora H è pienamente invariante in G.

2. Siano I e J due ideali in un anello commutativo A tali che $I \not\subseteq J$ e $J \not\subseteq I$.

   (a) Dimostrare che $I \cap J$ non è primo.

   (b) È possibile che sia $A = \mathbb{Q}[X]$ e $I \cap J = (X^5 + 3X^4 - 3)$?

   (c) È possibile che sia $A = \mathbb{Q}[X]$ e $I \cap J = (X^5 + 2X^4 - 3)$?

   (d) È possibile che sia $A = \mathbb{Z}[X]$ e $I \cap J = (2, X^5 + 3X^4 - 3)$?

Soluzioni

1. (a) Per definizione un sottogruppo H di G è normale se e solo se $aHa^{-1} \subseteq H$ per ogni $a \in G$. La tesi segue allora immediatamente dal fatto che $aHa^{-1} = \gamma_a(H)$ (dove $\gamma_a \colon G \to G$ è la funzione definita da $\gamma_a(g) := aga^{-1}$) e γ_a è un endomorfismo (in effetti anche un automorfismo) di G per ogni $a \in G$.

   (b) Indicando con g un generatore di G, per ogni endomorfismo f di G esiste $k \in \mathbb{Z}$ tale che $f(g) = g^k$. Per ogni $a \in G$, poiché esiste $i \in \mathbb{Z}$ tale che $a = g^i \in \langle g \rangle = G$, si ha allora

   $$f(a) = f(g^i) = f(g)^i = (g^k)^i = g^{ki} = (g^i)^k = a^k.$$

   In particolare, se $a \in H$, si ottiene $f(a) = a^k \in H$, cioè $f(H) \subseteq H$.

   (c) Ricordando che $[G, G] = \langle C \rangle$, dove

   $$C := \{aba^{-1}b^{-1} \,:\, a, b \in G\},$$

   va dimostrato che $f(\langle C \rangle) \subseteq \langle C \rangle$ per ogni endomorfismo f di G. Essendo f un omomorfismo, in ogni caso si ha $f(\langle C \rangle) = \langle f(C) \rangle$, per cui basta dimostrare che $f(C) \subseteq \langle C \rangle$. In effetti per ogni $a, b \in G$ si ha

   $$f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1} \in C,$$

   e dunque $f(C) \subseteq C \subseteq \langle C \rangle$.

   (d) Siano $\iota \colon H \to G$ l'inclusione e $\pi \colon G \to G/H$ la proiezione al quoziente. Per ogni endomorfismo f di G consideriamo l'omomorfismo (perché composizione di omomorfismi) $f' := \pi \circ f \circ \iota \colon H \to G/H$. Per il primo teorema di isomorfismo si ha $\operatorname{im}(f') \cong H/\ker(f')$, da cui segue (per il teorema di Lagrange) $\#(\operatorname{im}(f')) \mid \#(G/H)$ e $\#(\operatorname{im}(f')) = \#(H/\ker(f')) \mid \#H$. Se ne deduce che

   $$\#(\operatorname{im}(f')) \mid \operatorname{mcd}(\#(G/H), \#H) = 1,$$

   cioè f' è l'omomorfismo banale. D'altra parte $f' = \pi \circ f \circ \iota$ è banale se e solo se $f(H) = \operatorname{im}(f \circ \iota) \subseteq \ker(\pi) = H$.

2. (a) Per ipotesi esistono $a \in I$ e $b \in J$ tali che $a \notin J$ e $b \notin I$. Dunque $ab \in IJ \subseteq I \cap J$, ma $a, b \notin I \cap J$, il che dimostra che $I \cap J$ non è primo.

(b) No, non è possibile. Per il punto precedente è infatti sufficiente verificare che, posto $f := X^5 + 3X^4 - 3$, l'ideale (f) è primo in $\mathbb{Q}[X]$. Essendo $\mathbb{Q}[X]$ un dominio a fattorizzazione unica (è anche a ideali principali perché $\mathbb{Q}$ è un campo), (f) è primo in $\mathbb{Q}[X]$ se e solo se f è irriducibile in $\mathbb{Q}[X]$. In effetti f è irriducibile in $\mathbb{Z}[X]$ (e quindi anche in $\mathbb{Q}[X]$) per il criterio di Eisenstein relativo al numero primo 3.

(c) Sì, è possibile. Posto $g := X^5+2X^4-3$, le eventuali radici razionali di g possono essere solo ± 1 o ± 3. Si trova subito che solo 1 è radice di g, che $g = g_1 g_2$ con $g_1 := X-1$, $g_2 := X^4+3X^3+3X^2+3X+3$ e che g_2 non ha radici razionali. In particolare g_1 è irriducibile e non divide g_2 nel dominio a ideali principali $\mathbb{Q}[X]$. Pertanto $\mathrm{mcd}(g_1, g_2) = 1$ e gli ideali $I := (g_1)$ e $J := (g_2)$ sono coprimi. Per il teorema cinese del resto generalizzato si ha allora

$$I \cap J = IJ = (g_1)(g_2) = (g_1 g_2) = (g),$$

e chiaramente $I \not\subseteq J$ (perché $g_2 \nmid g_1$) e $J \not\subseteq I$ (perché $g_1 \nmid g_2$).

(d) Sì, è possibile. Posto $K := (2, f)$ (con $f := X^5 + 3X^4 - 3$) e $A := \mathbb{Z}[X]/(2)$, tenendo presente che la corrispondenza biunivoca tra ideali di $\mathbb{Z}[X]$ contenenti (2) e ideali di A (che manda K' in $K'/(2)$) chiaramente preserva le inclusioni e le intersezioni, trovare I e J come richiesto equivale a trovare due ideali $\overline{I} = I/(2)$ e $\overline{J} = J/(2)$ di A tali che $\overline{I} \not\subseteq \overline{J}$, $\overline{J} \not\subseteq \overline{I}$ e $\overline{I} \cap \overline{J} = \overline{K} := K/(2)$. Si ha $A \cong \mathbb{Z}/2\mathbb{Z}[X]$ e, attraverso questo isomorfismo, $\overline{K}$ si identifica all'ideale $(\overline{f}) \subseteq \mathbb{Z}/2\mathbb{Z}[X]$. È facile fattorizzare $\overline{f}$ in $\mathbb{Z}/2\mathbb{Z}[X]$ e si trova $\overline{f} = \overline{f_1}\,\overline{f_2}$ con $f_1 := X^2 + X + 1$ e $f_2 := X^3 + X + 1$ in $\mathbb{Z}[X]$ tali che $\overline{f_1}$ e $\overline{f_2}$ sono irriducibili in $\mathbb{Z}/2\mathbb{Z}[X]$. Ragionando in modo completamente analogo al punto precedente (con il campo $\mathbb{Z}/2\mathbb{Z}$ al posto di $\mathbb{Q}$ e con il polinomio $\overline{f} = \overline{f_1}\,\overline{f_2}$ al posto di $g = g_1 g_2$) si trova che si può prendere $\overline{I} = (\overline{f_1})$ e $\overline{J} = (\overline{f_2})$ in A, cioè $I = (2, f_1)$ e $J = (2, f_2)$ in $\mathbb{Z}[X]$.