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

Prova scritta del 17/06/2025

1. Dati due gruppi G e H, siano $a \in G$ e $b \in H$.

   (a) Dimostrare che, se $\langle (a,b) \rangle$ è normale in $G \times H$, allora $\langle a \rangle$ è normale in G.

   Nel seguito si supponga $\langle a \rangle$ normale in G, $\mathrm{ord}(a) = 4$ e $a \notin Z(G)$.

   (b) Dimostrare che esiste $g \in G$ tale che $gag^{-1} = a^{-1}$.

   (c) Dimostrare che, se $\mathrm{ord}(b) = 4$, allora $\langle (a,b) \rangle$ non è normale in $G \times H$.

   (d) Dimostrare che, se $\mathrm{ord}(b) = 2$, allora $\langle (a,b) \rangle$ è normale in $G \times H$ se e solo se $b \in Z(H)$.

2. Dati un anello commutativo A, un ideale I di A e $a \in A$, sia

$$J := \{b \in A \,:\, ab \in I\}.$$

   (a) Dimostrare che J è un ideale di A.

   (b) Dimostrare che $I \subseteq J$ e che $J = A$ se e solo se $a \in I$. Dimostrare inoltre che, se I è primo e $a \notin I$, allora $I = J$.

   Sia f il polinomio $X^4 + 12X^3 - 15X^2 + 18X - 21$.

   (c) Stabilire se $I = J$ nel caso in cui $A = \mathbb{Q}[X]$, $I = (f)$ e $a = X^5 - 1$.

   (d) Trovare a tale che $I \subsetneq J \subsetneq A$ nel caso in cui $A = \mathbb{Z}[X]$ e $I = (2, f)$.

Soluzioni

1. (a) Dati $g \in G$ e $a' \in \langle a \rangle$ (cioè $a' = a^n$ per qualche $n \in \mathbb{Z}$), va dimostrato che $ga'g^{-1} \in \langle a \rangle$. Poiché $(a^n, b^n) = (a, b)^n \in \langle (a, b) \rangle$ e $\langle (a, b) \rangle$ è normale in $G \times H$, anche

$$(g, 1)(a^n, b^n)(g, 1)^{-1} = (ga^n g^{-1}, 1b^n 1^{-1}) = (ga'g^{-1}, b^n) \in \langle (a, b) \rangle.$$

Dunque $(ga'g^{-1}, b^n) = (a, b)^m = (a^m, b^m)$ per qualche $m \in \mathbb{Z}$, e in particolare $ga'g^{-1} = a^m \in \langle a \rangle$.

(b) Poiché $a \notin Z(G)$, esiste $g \in G$ tale che $ga \neq ag$, cioè $gag^{-1} \neq a$. D'altra parte $gag^{-1} \in \langle a \rangle$ (perché $a \in \langle a \rangle$ e $\langle a \rangle$ è normale in G) e $\mathrm{ord}(gag^{-1}) = \mathrm{ord}(a) = 4$ (perché il coniugio con g, essendo un automorfismo di G, preserva l'ordine degli elementi). Considerando che gli unici elementi di ordine 4 di $\langle a \rangle$ sono a e $a^{-1} = a^3$ (infatti $\mathrm{ord}(1) = 1$ e $\mathrm{ord}(a^2) = 2$), deve allora essere $gag^{-1} = a^{-1}$.

(c) Per il punto precedente esiste $g \in G$ tale che $gag^{-1} = a^{-1}$. Dato che $(a, b) \in \langle (a, b) \rangle$ e

$$(g, 1)(a, b)(g, 1)^{-1} = (gag^{-1}, 1b1^{-1}) = (a^{-1}, b),$$

per concludere che $\langle (a, b) \rangle$ non è normale in $G \times H$ basta dimostrare che $(a^{-1}, b) \notin \langle (a, b) \rangle$. Se per assurdo $(a^{-1}, b) \in \langle (a, b) \rangle$, esisterebbe $n \in \mathbb{Z}$ tale che $(a^{-1}, b) = (a, b)^n = (a^n, b^n)$, cioè $a^{-1} = a^n$ e $b = b^n$. Questo non è possibile perché (essendo $\mathrm{ord}(a) = \mathrm{ord}(b) = 4$) si ha $a^n = a^{-1}$ se e solo se $n \equiv -1 \mod 4$ e $b^n = b$ se e solo se $n \equiv 1 \mod 4$.

(d) Se $\langle (a, b) \rangle$ è normale in $G \times H$, allora lo stesso argomento del primo punto ovviamente dimostra che $\langle b \rangle$ è normale in H. Dunque $hbh^{-1} \in \langle b \rangle$ per ogni $h \in H$. Inoltre (essendo $\mathrm{ord}(b) = 2$) si ha $\langle b \rangle = \{1, b\}$ e $hbh^{-1} \neq 1$, per cui $hbh^{-1} = b$ (cioè $hb = bh$) per ogni $h \in H$. Questo dimostra che $b \in Z(H)$.

Viceversa, se $b \in Z(H)$, allora $hbh^{-1} = b$ per ogni $h \in G$. Tenendo conto che, come visto nel secondo punto, per ogni $g \in G$ si ha $gag^{-1} = a$ o $gag^{-1} = a^{-1}$, si ottiene che per ogni $(g, h) \in G \times H$ il coniugato $(g, h)(a, b)(g, h)^{-1} = (gag^{-1}, hbh^{-1})$ può essere solo (a, b) o (a^{-1}, b). Poiché $(a^{-1}, b) = (a^{-1}, b^{-1}) = (a, b)^{-1}$ (dato che $\mathrm{ord}(b) = 2$), se ne deduce che $(g, h)(a, b)(g, h)^{-1} \in \langle (a, b) \rangle$ per ogni $(g, h) \in G \times H$. Usando il fatto che il coniugio con (g, h) è un automorfismo di $G \times H$, questo chiaramente implica che $(g, h)\langle (a, b) \rangle (g, h)^{-1} \subseteq \langle (a, b) \rangle$ per ogni $(g, h) \in G \times H$, cioè $\langle (a, b) \rangle$ è normale in $G \times H$.

2. (a) $0 \in J$ perché $a0 = 0 \in I$. Dati $b, b' \in J$ (cioè $ab, ab' \in I$), si ha $b + b' \in J$ perché $a(b + b') = ab + ab' \in I$. Infine $bc \in J$ per ogni $b \in J$ (cioè $ab \in I$) e per ogni $c \in A$ perché $a(bc) = (ab)c \in I$.

   (b) Per ogni $b \in I$ si ha $b \in J$ perché $ab \in I$.

   Se $J = A$, allora $1 \in J$, cioè $a = a1 \in I$. Viceversa, se $a \in I$, allora $ab \in I$ per ogni $b \in A$, il che dimostra che $b \in J$ per ogni $b \in A$, cioè $J = A$.

   Se I è primo e $a \notin I$, allora $J \subseteq I$ (e quindi $J = I$, avendo già dimostrato che in ogni caso $I \subseteq J$) perché per ogni $b \in J$ (cioè $ab \in I$) si ha $b \in I$ per definizione di ideale primo.

   (c) f è irriducibile sia in $\mathbb{Z}[X]$ che in $\mathbb{Q}[X]$ per il criterio di Eisenstein relativo al numero primo 3. Poiché $\mathbb{Q}[X]$ è un dominio a fattorizzazione unica (essendo $\mathbb{Q}$ un campo), questo implica che l'ideale $I = (f)$ è primo. È anche facile verificare che $X^5 - 1 \notin (f)$, cioè che $f \nmid (X^5 - 1)$ (per questo basta osservare che $X^5 - 1 = (X - 1)g$ con $g = X^4 + X^3 + X^2 + X + 1$ tale che $f \nmid (X - 1)$, $f \nmid g$). Segue allora dal punto precedente che $I = J$.

   (d) Basta dimostrare che esistono $a, b \in A \setminus I$ tali che $ab \in I$: infatti, per quanto visto nel secondo punto, $I \subsetneq J$ (perché $b \in J \setminus I$ e in ogni caso $I \subseteq J$) e $J \subsetneq A$ (perché $a \notin I$). Si osservi che tali a, b esistono se e solo se I non è primo e $I \neq \mathbb{Z}[X]$, se e solo se $\mathbb{Z}[X]/I$ non è un dominio e non è banale. Ciò è vero perché, per il terzo teorema di isomorfismo per anelli, si ha

$$\mathbb{Z}[X]/I \cong (\mathbb{Z}[X]/(2))/(f + (2)) \cong \mathbb{Z}/2\mathbb{Z}[X]/(\overline{f}),$$

   con $\overline{f} = X^4 + X^2 + \overline{1} = (X^2 + X + \overline{1})^2$ non 0, non invertibile e non irriducibile nel dominio a fattorizzazione unica $\mathbb{Z}/2\mathbb{Z}[X]$ (essendo $\mathbb{Z}/2\mathbb{Z}$ un campo). Questo suggerisce anche che si può prendere $a = b = X^2 + X + 1$. In effetti con tali scelte si ha $a = b \notin I$ (perché $X^2 + X + \overline{1} \notin (\overline{f})$ in $\mathbb{Z}/2\mathbb{Z}[X]$) e

$$ab = X^4 + 2X^3 + 3X^2 + 2X + 1 = f + 2(-5X^3 + 9X^2 - 8X + 11) \in I.$$