**Corso di Algebra 1 - a.a. 2022-2023**

*Prova scritta del 05/09/2023*

1. Sia $G$ un gruppo finito. Dati un sottogruppo $H$ di $G$ e $g \in G$ sia

$$\mathrm{ord}(g, H) := \min\{k > 0 \,:\, g^k \in H\}.$$

   (a) Dimostrare che $\mathrm{ord}(g, H) \mid \mathrm{ord}(g)$.

   (b) Dimostrare che, se $H$ è normale, allora $\mathrm{ord}(g, H) \mid [G : H]$.

   (c) Fornire un esempio in cui $\mathrm{ord}(g, H) \nmid [G : H]$.

   (d) Dimostrare che in ogni caso $\mathrm{ord}(g, H) \leq [G : H]$.

2. Sia $A$ un anello commutativo. Dato $a \in A$, sia

$$\mathrm{Ann}(a) := \{b \in A \,:\, ba = 0\}.$$

   (a) Dimostrare che $\mathrm{Ann}(a)$ è un ideale di $A$.

   (b) Assumendo $A \neq \{0\}$, dimostrare che $\mathrm{Ann}(a)$ è un ideale primo per ogni $a \neq 0$ se e solo se $A$ è un dominio.

   (c) Dimostrare che, se $\mathrm{Ann}(a)$ è un ideale primo e $a^2 \neq 0$, allora $\mathrm{Ann}(a) = \mathrm{Ann}(a^2)$.

   (d) Nel caso in cui $A = K[X]/(f)$ con $K$ campo e $f \in K[X] \setminus \{0\}$, dimostrare che per ogni ideale $I$ di $A$ esiste $a \in A$ tale che $\mathrm{Ann}(a) = I$.

*Soluzioni*

1. Sia $n := \mathrm{ord}(g)$, $n' := \mathrm{ord}(g, H)$ e $m := [G : H]$.

   (a) Essendo $n' > 0$, esistono unici $q, r \in \mathbb{Z}$ tali che $n = qn' + r$ e $0 \leq r < n'$. Poiché $g^n = 1$ e $g^{n'} \in H$, anche
   $$g^r = g^{n-qn'} = g^n (g^{n'})^{-q} = (g^{n'})^{-q} \in H.$$
   Per definizione di $n'$ non può essere $0 < r < n'$, e quindi $r = 0$, cioè $n' \mid n = qn'$.

   (b) Per ogni $k \in \mathbb{Z}$ nel gruppo $G/H$ si ha $(gH)^k = g^k H = H$ se e solo se $g^k \in H$. Dunque $n'$ coincide con l'ordine di $gH$ in $G/H$, e per il teorema di Lagrange si conclude che $n' \mid \#(G/H) = m$.

   (c) Sia per esempio $G = D_3$, $H = \langle S \rangle$ e $g = RS$. Infatti in questo caso $n' = 2$ (dato che $g \notin H = \{1, S\}$ e $g^2 = 1 \in H$) e $m = (\#G)/(\#H) = 6/2 = 3$.

   (d) Nell'insieme $G/H$ di cardinalità $m$ gli $m + 1$ elementi
   $$\{g^i H \,:\, i = 0, \ldots, m\}$$
   non possono essere tutti distinti. Pertanto esistono $0 \leq i < j \leq m$ tali che $g^i H = g^j H$, da cui segue
   $$H = g^{-i} g^i H = g^{-i} g^j H = g^{j-i} H,$$
   cioè $g^{j-i} \in H$. Essendo $j - i > 0$, per definizione di $n'$ si ottiene allora $n' \leq j - i \leq m - 0 = m$.

2. (a) $0 \in \mathrm{Ann}(a)$ perché $0a = 0$. Dati $b, b' \in \mathrm{Ann}(a)$ (cioè $ba = b'a = 0$), anche $b + b' \in \mathrm{Ann}(a)$ perché
   $$(b + b')a = ba + b'a = 0 + 0 = 0.$$
   Infine $cb \in \mathrm{Ann}(a)$ per ogni $c \in A$ e per ogni $b \in \mathrm{Ann}(a)$ perché
   $$(cb)a = c(ba) = c0 = 0.$$

   (b) Se $A$ è un dominio e $a \neq 0$, per definizione $ba = 0$ se e solo se $b = 0$, cioè $\mathrm{Ann}(a) = \{0\}$. Poiché in un dominio $\{0\}$ è un ideale primo, se ne deduce che $\mathrm{Ann}(a)$ è primo. Viceversa, se $\mathrm{Ann}(a)$ è primo per ogni $a \neq 0$, in particolare $\mathrm{Ann}(1)$ è primo ($1 \neq 0$ perché $A \neq \{0\}$). Dato che
   $$\mathrm{Ann}(1) = \{b \in A \,:\, b = b1 = 0\} = \{0\},$$
   si conclude che $\{0\}$ è primo, e quindi $A$ è un dominio.

(c) In ogni caso $\mathrm{Ann}(a) \subseteq \mathrm{Ann}(a^2)$: dato $b \in \mathrm{Ann}(a)$ (cioè $ba = 0$) si ha anche $b \in \mathrm{Ann}(a^2)$ perché $ba^2 = (ba)a = 0a = 0$. Resta da dimostrare che $\mathrm{Ann}(a^2) \subseteq \mathrm{Ann}(a)$ se $\mathrm{Ann}(a)$ è primo e $a^2 \neq 0$. Dato $b \in \mathrm{Ann}(a^2)$, da $0 = ba^2 = (ba)a$ segue $ba \in \mathrm{Ann}(a)$, e quindi $b \in \mathrm{Ann}(a)$ o $a \in \mathrm{Ann}(a)$ perché $\mathrm{Ann}(a)$ è primo. D'altra parte $a \notin \mathrm{Ann}(a)$ (altrimenti si avrebbe $a^2 = 0$), e si conclude che $b \in \mathrm{Ann}(a)$.

(d) Ogni ideale $I$ di $A$ è della forma $J/(f)$ per qualche ideale $J$ di $K[X]$ tale che $(f) \subseteq J$. Essendo $K[X]$ un dominio a ideali principali (perché $K$ è un campo), esiste $g \in K[X]$ tale che $J = (g)$, e la condizione $(f) \subseteq J = (g)$ equivale a $g \mid f$, cioè esiste $h \in K[X]$ tale che $f = gh$. Vogliamo allora dimostrare che

$$a := h + (f) \in K[X]/(f) = A$$

verifica $\mathrm{Ann}(a) = I$. In effetti, dato $b = p + (f) \in A$ (con $p \in K[X]$), $b \in \mathrm{Ann}(a)$ se e solo se

$$(f) = ba = [p + (f)][h + (f)] = ph + (f)$$

se e solo se $ph \in (f)$. Poiché $f = gh$, $h \neq 0$ (essendo $f \neq 0$) e $K[X]$ è un dominio, quest'ultima condizione equivale a $p \in (g)$, e quindi a $b = p + (f) \in (g)/(f) = I$.