Corso di Algebra 1 - a.a. 2021-2022

Prova scritta del 05/07/2022

1. Sia G un gruppo abeliano e, per ogni intero k, sia $G_k := \{g^k \,:\, g \in G\}$.
   (a) Dimostrare che G_k è un sottogruppo di G per ogni $k \in \mathbb{Z}$.
   (b) Dimostrare che, se G è ciclico infinito, allora $G_k \neq G$ per ogni $k > 1$.
   (c) Dimostrare che, se G è ciclico di ordine n (intero positivo), allora $G_k = G$ se e solo se $\mathrm{mcd}(k, n) = 1$.
   (d) Fornire un esempio in cui G non è banale e $G_k = G$ per ogni $k > 0$.

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

$$I' := \{f \in A[X] \,:\, f(a) \in I\}.$$

   (a) Dimostrare che I' è un ideale di $A[X]$.
   (b) Dimostrare che I è primo in A se e solo se I' è primo in $A[X]$.
   (c) È vero che I è massimale in A se e solo se I' è massimale in $A[X]$?
   (d) Se A è un dominio, dimostrare che non esiste $f \in A[X]$ tale che $\deg(f) \geq 2$ e $I' = (f)$.

Soluzioni

1. (a) Chiaramente $1 = 1^k \in G_k$. Dati poi $a, b \in G_k$, per definizione esistono $g, h \in G$ tali che $a = g^k$ e $b = h^k$. Si ha allora
$$ab^{-1} = g^k(h^k)^{-1} = g^k(h^{-1})^k = (gh^{-1})^k \in G_k$$
(l'ultima uguaglianza vale per la commutatività).

   (b) Osserviamo preliminarmente che, se c è un generatore di G, allora c^k è un generatore di G_k: infatti $\langle c^k \rangle \subseteq G_k$ perché $c^k \in G_k$; viceversa $G_k \subseteq \langle c^k \rangle$ perché per ogni $g \in G$ esiste $m \in \mathbb{Z}$ tale che $g = c^m$, quindi $g^k = (c^m)^k = (c^k)^m \in \langle c^k \rangle$. Se ne deduce che $c \notin G_k = \langle c^k \rangle$ (quindi $G \neq G_k$) per $k > 1$, perché altrimenti esisterebbe $l \in \mathbb{Z}$ tale che $c = (c^k)^l = c^{kl}$, il che è impossibile, dato che $\mathrm{ord}(c) = \infty$ e $kl \neq 1$.

   (c) Come nel punto precedente, indicando con c un generatore di G, si ha $G_k = \langle c^k \rangle$. Poiché G è finito, $G_k = G$ se e solo se $\#G_k = \#G = n$. D'altra parte
$$\#G_k = \mathrm{ord}(c^k) = \frac{\mathrm{ord}(c)}{\mathrm{mcd}(k, \mathrm{ord}(c))} = \frac{n}{\mathrm{mcd}(k, n)},$$
per cui $G = G_k$ se e solo se $\mathrm{mcd}(k, n) = 1$.

   (d) Si può prendere $G = \mathbb{Q}$. Si noti che, essendo $\mathbb{Q}$ un gruppo additivo, risulta $\mathbb{Q}_k = \{kq : q \in \mathbb{Q}\}$. Allora $\mathbb{Q}_k = \mathbb{Q}$ per ogni $k > 0$ perché, dato $a \in \mathbb{Q}$, esiste $q = a/k \in \mathbb{Q}$ tale che $a = kq$.

2. Siano $\pi\colon A \to A/I$ la proiezione al quoziente e $\psi\colon A[X] \to A$, $f \mapsto f(a)$ la valutazione in a. Poiché sia π che ψ sono omomorfismi suriettivi di anelli, anche la loro composizione $\phi := \pi \circ \psi\colon A[X] \to A/I$ lo è.

   (a) I' è un ideale di $A[X]$ perché $I' = \ker(\phi)$: per ogni $f \in A[X]$ si ha infatti
$$\phi(f) = \pi(\psi(f)) = \pi(f(a)) = f(a) + I \in A/I,$$
per cui $f \in \ker(\phi)$ se e solo se $f(a) + I = I$ se e solo se $f(a) \in I$ se e solo se $f \in I'$.

   (b) I è primo in A se e solo se A/I è un dominio e I' è primo in $A[X]$ se e solo se $A[X]/I'$ è un dominio. Per concludere basta allora osservare che per il primo teorema di isomorfismo per anelli (e tenendo conto che $\ker(\phi) = I'$, come visto nel punto precedente)
$$A/I = \mathrm{im}(\phi) \cong A[X]/\ker(\phi) = A[X]/I'.$$

(c) Sì, è vero, e la dimostrazione è simile a quella del punto precedente, questa volta usando il fatto che I è massimale in A se e solo se A/I è un campo e I' è massimale in $A[X]$ se e solo se $A[X]/I'$ è un campo.

(d) Supponiamo per assurdo che sia $I' = (f)$ con $\deg(f) \geq 2$.

Se $I = \{0\}$, allora π è un isomorfismo, e perciò $I' = \ker(\phi) = \ker(\psi)$. D'altra parte $\ker(\psi) = (X-a)$, per cui $(f) = I' = (X-a)$. Essendo A (e quindi anche $A[X]$) un dominio, se ne deduce che f e $X - a$ sono associati, cioè esiste $c \in A[X]^* = A^*$ tale che $f = c(X - a)$. Questo è però impossibile, dato che $\deg(f) \geq 2$, mentre $\deg(c(X - a)) = 1$.

Se invece $I \neq \{0\}$, allora esiste $0 \neq b \in I$, e quindi $b = \psi(b) \in I' = (f)$. Pertanto esiste $0 \neq g \in A[X]$ tale che $b = fg$, e dunque

$$0 = \deg(b) = \deg(fg) = \deg(f) + \deg(g)$$

(dove l'ultima uguaglianza vale perché A è un dominio), il che porta all'assurdo $\deg(g) = -\deg(f) \leq -2$.