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

Prova scritta del 14/02/2023

1. Siano $f\colon G \to G'$ e $g\colon G' \to G$ due omomorfismi di gruppi tali che $\ker(f) = \mathrm{im}(g)$ e $\mathrm{im}(f) = \ker(g)$.

   (a) Dimostare che, se f è iniettivo o suriettivo, allora f è un isomorfismo e g è banale.

   (b) Dimostrare che, se G e G' sono finiti, allora hanno lo stesso ordine.

   (c) Determinare $\ker(f)$ e $\mathrm{im}(f)$ nel caso in cui $G = \mathbb{Z}/6\mathbb{Z}$ e $G' = S_3$.

   (d) Dimostrare che non può essere $G = \mathbb{Z}/12\mathbb{Z}$ e $G' = A_4$.

2. Dati due ideali I e J in un anello commutativo A, sia

$$L := \left\{ \sum_{i \geq 0} a_i X^i \in A[X] \,:\, a_0 \in I,\, a_1 \in J \right\}.$$

   (a) Dimostrare che L è un sottoanello di $A[X]$ se e solo se $I = A$.

   (b) Dimostrare che L è un ideale di $A[X]$ se e solo se $I \subseteq J$.

   (c) Dimostrare che L è un ideale primo di $A[X]$ se e solo se I è un ideale primo di A e $J = A$.

   (d) Assumendo $A = \mathbb{Z}$ e $I = \{0\}$, dimostrare che $\mathbb{Z}[X]/L$ ha infiniti ideali primi.

Soluzioni

1. (a) Prima di tutto notiamo che g è banale se e solo se $\mathrm{im}(g) = \{1\}$ se e solo se $\ker(g) = G'$. Se f è iniettivo, allora $\mathrm{im}(g) = \ker(f) = \{1\}$, per cui g è l'omomorfismo banale. Dunque in questo caso si ha anche $\mathrm{im}(f) = \ker(g) = G'$, cioè f è pure suriettivo. Analogamente, se f è suriettivo, allora $\ker(g) = \mathrm{im}(f) = G'$, per cui di nuovo g è l'omomorfismo banale. Dunque in questo caso si ha anche $\ker(f) = \mathrm{im}(g) = \{1\}$, e pertanto f è pure iniettivo.

   (b) Per il primo teorema di isomorfismo per gruppi $\mathrm{im}(f) \cong G/\ker(f)$ e $\mathrm{im}(g) \cong G'/\ker(g)$, e quindi (grazie al teorema di Lagrange) $\#G = (\#\ker(f))(\#\mathrm{im}(f))$ e $\#G' = (\#\ker(g))(\#\mathrm{im}(g))$. Per concludere basta osservare che dall'ipotesi su f e g segue ovviamente $\#\ker(f) = \#\mathrm{im}(g)$ e $\#\mathrm{im}(f) = \#\ker(g)$.

   (c) Poiché $\mathbb{Z}/6\mathbb{Z} \ncong S_3$, segue dal primo punto che f (e analogamente g) non è né iniettivo né suriettivo. In particolare $\mathrm{im}(f) = \ker(g)$ è un sottogruppo normale di G' non banale, cioè diverso sia da $\{1\}$ (altrimenti g sarebbe iniettivo) che da G' (altrimenti f sarebbe suriettivo). Se ne deduce che $\mathrm{im}(f) = A_3$, essendo A_3 l'unico sottogruppo normale non banale di S_3. Inoltre per quanto visto nel punto precedente si ha

$$\#\ker(f) = \frac{\#G}{\#\mathrm{im}(f)} = \frac{\#\mathbb{Z}/6\mathbb{Z}}{\#A_3} = \frac{6}{3} = 2,$$

   e dunque necessariamente $\ker(f) = \langle\bar{3}\rangle = \{\bar{0}, \bar{3}\}$, dato che quest'ultimo è l'unico sottogruppo di ordine 2 di $\mathbb{Z}/6\mathbb{Z}$.

   (d) Supponendo per assurdo $G = \mathbb{Z}/12\mathbb{Z}$ e $G' = A_4$, osserviamo che sia $\ker(f) < \mathbb{Z}/12\mathbb{Z}$ che $\mathrm{im}(f) \cong (\mathbb{Z}/12\mathbb{Z})/\ker(f)$ sono ciclici, dato che sottogruppi e quozienti di un gruppo ciclico (quale è $\mathbb{Z}/12\mathbb{Z}$) sono ciclici. D'altra parte, se $\sigma \in A_4$ è tale che $\mathrm{im}(f) = \langle\sigma\rangle$, si ha $\#\mathrm{im}(f) = \mathrm{ord}(\sigma)$; inoltre $\ker(f) = \mathrm{im}(g) \cong A_4/\ker(g)$, e se $\tau \in A_4$ è tale che $A_4/\ker(g) = \langle\bar{\tau}\rangle$, si ottiene $\#\ker(f) = \#(A_4/\ker(g)) = \mathrm{ord}(\bar{\tau}) \mid \mathrm{ord}(\tau)$. Tenendo conto che il massimo ordine di un lemento in A_4 è 3, questo dimostra $\#\mathrm{im}(f), \#\ker(f) \leq 3$, il che porta all'assurdo

$$12 = \#\mathbb{Z}/12\mathbb{Z} = (\#\ker(f))(\#\mathrm{im}(f)) \leq 3 \cdot 3 = 9.$$

2. In ogni caso L è un sottogruppo di $A[X]$. Infatti chiaramente $0 \in L$ e, se $f = \sum_{i\geq 0} a_i X^i, g = \sum_{i\geq 0} b_i X^i \in L$ (cioè $a_0, b_0 \in I$ e $a_1, b_1 \in J$), allora anche $f - g = \sum_{i\geq 0}(a_i - b_i)X^i \in L$, dato che $a_0 - b_0 \in I$ e $a_1 - b_1 \in J$ (essendo I e J sottogruppi di A).

   (a) Poiché $1 \in L$ se e solo se $1 \in I$ se e solo se $I = A$, è chiaro che $I = A$ se L è un sottoanello di $A[X]$. Viceversa, se $I = A$, resta da dimostrare che $fg \in L$ per ogni $f = \sum_{i\geq 0} a_i X^i, g = \sum_{i\geq 0} b_i X^i \in L$ (cioè $a_1, b_1 \in J$). Questo è vero perché $fg = \sum_{i\geq 0} c_i X^i$ con $c_0 = a_0 b_0 \in A = I$ e $c_1 = a_0 b_1 + a_1 b_0 \in J$ (essendo $a_1, b_1 \in J$ e J ideale di A).

   (b) Se $I \subseteq J$, allora L è un ideale di $A[X]$ perché $fg \in L$ per ogni $f = \sum_{i\geq 0} a_i X^i \in L$ (cioè $a_0 \in I \subseteq J$ e $a_1 \in J$) e per ogni $g = \sum_{i\geq 0} b_i X^i \in A[X]$. Infatti $fg = \sum_{i\geq 0} c_i X^i$ con $c_0 = a_0 b_0 \in I$ (essendo $a_0 \in I$ e I ideale di A) e $c_1 = a_0 b_1 + a_1 b_0 \in J$ (essendo $a_0, a_1 \in J$ e J ideale di A). Viceversa, se L è un ideale di $A[X]$, allora per ogni $a \in I$ si ha $a \in L$, da cui segue $aX \in L$, e quindi $a \in J$. Ciò dimostra che $I \subseteq J$.

   (c) Se I è primo in A e $J = A$, allora $L \neq A[X]$ perché $1 \notin I$, quindi $1 \notin L$. Va inoltre dimostrato che, dati $f = \sum_{i\geq 0} a_i X^i, g = \sum_{i\geq 0} b_i X^i \in A[X]$ tali che $fg \in L$, si ha $f \in L$ o $g \in L$. In effetti $fg = \sum_{i\geq 0} c_i X^i$ con $c_0 = a_0 b_0 \in I$, da cui segue $a_0 \in I$ o $b_0 \in I$ perché I è primo in A; poiché in ogni caso $a_1, b_1 \in J = A$, questo dimostra che $f \in L$ o $g \in L$. Viceversa, se L è primo in $A[X]$, allora I è primo in A: infatti $I \neq A$ perché $1 \notin L$, quindi $1 \notin I$; inoltre, dati $a, b \in A$ tali che $ab \in I$, si ha $ab \in L$, da cui si ottiene (essendo L primo in $A[X]$) $a \in L$ o $b \in L$, cioè $a \in I$ o $b \in I$. Infine $J = A$ perché $XX = X^2 \in L$, quindi (essendo L primo in $A[X]$) $X \in L$, cioè $1 \in J$.

   (d) Per ogni numero primo p l'ideale

$$L_p := \left\{ \sum_{i\geq 0} a_i X^i \in \mathbb{Z}[X] \,:\, a_0 \in p\mathbb{Z} \right\}$$

   (che chiaramente contiene L) è primo in $\mathbb{Z}[X]$ grazie al punto precedente (essendo $p\mathbb{Z}$ primo in $\mathbb{Z}$). Poiché i numeri primi sono infiniti, grazie alla corrispondenza biunivoca tra gli ideali di $\mathbb{Z}[X]$ contenenti L e gli ideali di $\mathbb{Z}[X]/L$, otteniamo infiniti ideali di $\mathbb{Z}[X]/L$ della forma L_p/L, che sono primi perché $(\mathbb{Z}[X]/L)/(L_p/L) \cong \mathbb{Z}[X]/L_p$ per il terzo teorema di isomorfismo per anelli, e $\mathbb{Z}[X]/L_p$ è un dominio (dato che L_p è primo in $\mathbb{Z}[X]$).