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

Prova scritta del 08/07/2025

1. Sia G un gruppo e sia p un numero primo.

- (a) Dimostrare che esiste un omomorfismo non banale $\mathbb{Z}/p\mathbb{Z} \rightarrow G$ se e solo se G contiene un sottogruppo di ordine p .
- (b) Dimostrare che esiste un omomorfismo non banale $G \rightarrow \mathbb{Z}/p\mathbb{Z}$ se e solo se G contiene un sottogruppo normale di indice p .
- (c) Dimostrare che esiste un omomorfismo non banale $D_3 \rightarrow G$ se e solo se G contiene un sottogruppo di ordine 2.
- (d) Dimostrare che esiste un omomorfismo non banale $G \rightarrow D_3$ se e solo se G contiene un sottogruppo normale di indice 2 o 3.

2. Sia

$$I := \left\{ \sum_{i \geq 0} a_i X^i \in \mathbb{Z}[X] : 4 \mid a_0, 2 \mid a_1 \right\}.$$

- (a) Dimostrare che I è un ideale di $\mathbb{Z}[X]$.
- (b) Dimostrare che, se J è un ideale primo di $\mathbb{Z}[X]$ contenente I , allora $I \subseteq (2, X) \subseteq J$.
- (c) Dimostrare che $\mathbb{Z}[X]/I$ è isomorfo a $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ come gruppo additivo.
- (d) Dimostrare che $\mathbb{Z}[X]/I$ non è isomorfo a $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ come anello.

Soluzioni

1. (a) Se $f: \mathbb{Z}/p\mathbb{Z} \rightarrow G$ è un omomorfismo non banale, deve essere $\ker(f) = \{[0]\}$ (dato che $\{[0]\}$ e $\mathbb{Z}/p\mathbb{Z}$ sono gli unici sottogruppi di $\mathbb{Z}/p\mathbb{Z}$), cioè f è iniettivo. Dunque il sottogruppo $\text{im}(f)$ di G è isomorfo a $\mathbb{Z}/p\mathbb{Z}$, e in particolare ha ordine $\#(\mathbb{Z}/p\mathbb{Z}) = p$.

Viceversa, se esiste un sottogruppo H di G di ordine p , deve essere $H \cong \mathbb{Z}/p\mathbb{Z}$ (dato che ogni gruppo di ordine p è ciclico). La composizione di un isomorfismo $\mathbb{Z}/p\mathbb{Z} \rightarrow H$ con l'inclusione di H in G è allora un omomorfismo iniettivo (quindi non banale) $\mathbb{Z}/p\mathbb{Z} \rightarrow G$.

- (b) Se $f: G \rightarrow \mathbb{Z}/p\mathbb{Z}$ è un omomorfismo non banale, deve essere $\text{im}(f) = \mathbb{Z}/p\mathbb{Z}$ (dato che $\{[0]\}$ e $\mathbb{Z}/p\mathbb{Z}$ sono gli unici sottogruppi di $\mathbb{Z}/p\mathbb{Z}$). Dunque $\mathbb{Z}/p\mathbb{Z} = \text{im}(f) \cong G/\ker(f)$ per il primo teorema di isomorfismo, e pertanto l'indice del sottogruppo normale $\ker(f)$ di G è $\#(G/\ker(f)) = \#(\mathbb{Z}/p\mathbb{Z}) = p$.

Viceversa, se esiste un sottogruppo normale H di G di indice p , deve essere $G/H \cong \mathbb{Z}/p\mathbb{Z}$ (dato che ogni gruppo di ordine p è ciclico). La composizione della proiezione al quoziente $G \rightarrow G/H$ con un isomorfismo $G/H \rightarrow \mathbb{Z}/p\mathbb{Z}$ è allora un omomorfismo suriettivo (quindi non banale) $G \rightarrow \mathbb{Z}/p\mathbb{Z}$.

Si osservi che, grazie al primo punto, esistono omomorfismi iniettivi $i: \mathbb{Z}/2\mathbb{Z} \rightarrow D_3$ e $j: \mathbb{Z}/3\mathbb{Z} \rightarrow D_3$, considerato che D_3 contiene i sottogruppi $\langle S \rangle$ di ordine 2 e $\langle R \rangle$ di ordine 3. Analogamente, grazie al secondo punto, esiste un omomorfismo suriettivo $s: D_3 \rightarrow \mathbb{Z}/2\mathbb{Z}$, considerato che D_3 contiene il sottogruppo normale $\langle R \rangle$ di indice 2.

- (c) Per il primo punto basta dimostrare che esiste un omomorfismo non banale $D_3 \rightarrow G$ se e solo se ne esiste uno $\mathbb{Z}/2\mathbb{Z} \rightarrow G$.

Se $f: \mathbb{Z}/2\mathbb{Z} \rightarrow G$ è un omomorfismo non banale, chiaramente anche $f \circ s: D_3 \rightarrow G$ lo è.

Viceversa, se $g: D_3 \rightarrow G$ è un omomorfismo non banale, $\ker(g)$ è un sottogruppo normale di D_3 tale che $\ker(g) \neq D_3$. Quindi $\ker(g)$ può essere solo $\{1\}$ o $\langle R \rangle \cong \mathbb{Z}/3\mathbb{Z}$, e in entrambi i casi $\ker(g)$ non può contenere il sottogruppo $\text{im}(i)$ di G di ordine 2. Questo dimostra che l'omomorfismo $g \circ i: \mathbb{Z}/2\mathbb{Z} \rightarrow G$ non è banale.

- (d) Per il secondo punto basta dimostrare che esiste un omomorfismo non banale $G \rightarrow D_3$ se e solo se ne esiste uno $G \rightarrow \mathbb{Z}/p\mathbb{Z}$ con $p = 2$ o 3 .

Se $f: G \rightarrow \mathbb{Z}/p\mathbb{Z}$ è un omomorfismo non banale con $p = 2$ o 3 , in ogni caso esiste un omomorfismo iniettivo $h: \mathbb{Z}/p\mathbb{Z} \rightarrow D_3$ ($h = i$ se $p = 2$ e $h = j$ se $p = 3$). Dunque $h \circ f: G \rightarrow D_3$ è un omomorfismo non banale.

Viceversa, se $g: G \rightarrow D_3$ è un omomorfismo non banale, si può supporre che l'omomorfismo $s \circ g: G \rightarrow \mathbb{Z}/2\mathbb{Z}$ sia banale. In tal caso $\text{im}(g) \subseteq \ker(s) = \langle R \rangle \cong \mathbb{Z}/3\mathbb{Z}$, e quindi g induce un omomorfismo non banale $G \rightarrow \mathbb{Z}/3\mathbb{Z}$.

2. (a) Ovviamente $0 \in I$. Se $f = \sum_{i \geq 0} a_i X^i, g = \sum_{i \geq 0} b_i X^i \in I$ (cioè $4 \mid a_0, b_0$ e $2 \mid a_1, b_1$) e $h = \sum_{i \geq 0} c_i X^i \in \mathbb{Z}[X]$, allora anche $f + g = \sum_{i \geq 0} (a_i + b_i) X^i \in I$ (perché $4 \mid (a_0 + b_0)$ e $2 \mid (a_1 + b_1)$) e $fh = \sum_{i \geq 0} d_i X^i \in I$ (perché $4 \mid d_0 = a_0 c_0$ e $2 \mid d_1 = a_0 c_1 + a_1 c_0$).
- (b) Dato $f = \sum_{i \geq 0} a_i X^i \in I$, si ha $f = 2 \frac{a_0}{2} + X \sum_{i \geq 0} a_{i+1} X^i \in (2, X)$ perché $\frac{a_0}{2} \in \mathbb{Z} \subseteq \mathbb{Z}[X]$, il che dimostra $I \subseteq (2, X)$.
 $2 \in J$ perché $2^2 = 4 \in I \subseteq J$ e J è primo; analogamente $X \in J$ perché $X^2 \in I$. Essendo J un ideale, questo implica $(2, X) \subseteq J$.
- (c) La funzione

$$\alpha: \mathbb{Z}[X] \rightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\sum_{i \geq 0} a_i X^i \mapsto ([a_0]_4, [a_1]_2)$$

è un omomorfismo di gruppi additivi, perché

$$\alpha \left(\sum_{i \geq 0} a_i X^i + \sum_{i \geq 0} b_i X^i \right) = \alpha \left(\sum_{i \geq 0} (a_i + b_i) X^i \right) = ([a_0 + b_0]_4, [a_1 + b_1]_2)$$

$$= ([a_0]_4, [a_1]_2) + ([b_0]_4, [b_1]_2) = \alpha \left(\sum_{i \geq 0} a_i X^i \right) + \alpha \left(\sum_{i \geq 0} b_i X^i \right).$$

Chiaramente α è suriettivo e $\sum_{i \geq 0} a_i X^i \in \ker(\alpha)$ se e solo se $[a_0]_4 = [0]_4$ e $[a_1]_2 = [0]_2$, cioè $\ker(\alpha) = I$. Per il primo teorema di isomorfismo per gruppi si conclude allora che

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \text{im}(\alpha) \cong \mathbb{Z}[X]/\ker(\alpha) = \mathbb{Z}[X]/I$$

come gruppi additivi.

- (d) Basta osservare per esempio che in $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ c'è un solo elemento non nullo il cui quadrato è nullo (cioè $([2]_4, [0]_2)$), mentre in $\mathbb{Z}[X]/I$ ce ne sono almeno due (in particolare $2 + I$ e $X + I$, dato che $2, X \notin I$, mentre $2^2 = 4, X^2 \in I$).