Corso di Algebra 1 - a.a. 2016-2017

Prova scritta del 22.9.2017

1. Sia G il gruppo $S_4 \times \mathbb{Z}/4\mathbb{Z}$.
   (a) Quanti sono gli elementi di G di ordine 2?
   (b) Esistono elementi di G di ordine 8?
   (c) Sia $\varphi : G \to \mathbb{Z}/4\mathbb{Z}$ la proiezione sul secondo fattore. Definire un omomorfismo non banale da G a $\mathbb{Z}/4\mathbb{Z}$ diverso da φ.

2. Sia $f\colon G \to G'$ un omomorfismo suriettivo di gruppi. Diciamo che f è *invertibile a destra* se esiste un omomorfismo $h\colon G' \to G$ tale che $f \circ h = \mathrm{id}_{G'}$.
   (a) Dimostrare che, se $G' = \mathbb{Z}$, allora f è invertibile a destra.
   (b) Fornire un esempio in cui $G = \mathbb{Z}$ e f non è invertibile a destra.
   (c) Dimostrare che, se $G = S_3$, allora f è invertibile a destra.

3. Sia A un anello commutativo. Dato un ideale $J \subseteq A[X]$, definiamo $t(J)$ l'insieme composto dallo 0 e dagli elementi di A che compaiono come coefficienti dei monomi di grado massimo di elementi di J.
   (a) Dimostrare che $t(J)$ è un ideale di A.
   (b) Dimostrare che per ogni ideale I di A esiste un ideale J di $A[X]$ tale che $t(J) = I$.
   (c) Esiste un ideale $J \subsetneq A[X]$ tale che $t(J) = A$?

4. Siano p un polinomio a coefficienti interi e n un intero positivo tali che esiste un omomorfismo di anelli $f\colon \mathbb{Z}[X]/(p) \to \mathbb{Z}/n\mathbb{Z}$.
   (a) Dimostrare che f è suriettivo.
   (b) Dimostrare che esiste $a \in \mathbb{Z}$ tale che $p(a) \equiv 0 \mod n$.
   (c) È possibile che sia $p = X^2 + X + 1$ e $n = 11$?

Soluzioni

1. (a) In un prodotto diretto di gruppi $A \times B$ l'ordine di un elemento (a, b) è il minimo comune multiplo tra l'ordine di a in A e l'ordine di b in B. Perciò, perché questo sia 2 ambedue gli ordini devono essere divisori di 2 e almeno uno dei due deve essere esattamente 2.

   Gli elementi di S_4 che hanno ordine 2 sono le trasposizioni, che sono 6, e le doppie trasposizioni, che sono 3; in $\mathbb{Z}/4\mathbb{Z}$ invece di ordine 2 c'è solo 2. Perciò gli elementi di ordine 2 di G sono 19: 9 di essi hanno come primo elemento della coppia un elemento di ordine 2 di S_4 e come secondo elemento l'identità di $\mathbb{Z}/4\mathbb{Z}$, 1 ha l'identità di S_4 come primo elemento e 2 come secondo, e 9 hanno un elemento di ordine 2 di S_4 come primo elemento e 2 come secondo.

   (b) Per quanto già detto, perché un elemento di G abbia ordine 8 il minimo comune multiplo degli ordini dei due componenti della coppia deve essere 8. Ma in S_4 ci sono elementi di ordine $1, 2, 3$ e 4, mentre in $\mathbb{Z}/4\mathbb{Z}$ ci sono elementi di ordine $1, 2$ e 4; il minimo comune multiplo di questi numeri non è mai 8, quindi non ci sono elementi di ordine 8 in G.

   (c) Esistono molti omomorfismi che rispondono alle caratteristiche richieste. Ad esempio, si può considerare la proiezione al quoziente $\pi : S_4 \to S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$ composta con l'inclusione $i : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ che manda 0 in 0 e 1 in 2; questo omomorfismo $\psi = i \circ \pi$ non è banale (ad esempio perchè π è suriettivo e quindi l'immagine di ψ contiene 2) e non è la proiezione sul secondo fattore (ad esempio perché non è suriettivo).

2. (a) Poiché f è suriettivo, esiste $g \in G$ tale che $f(g) = 1 \in \mathbb{Z}$. Allora $h\colon \mathbb{Z} \to G$ definito da $h(n) = g^n$ è un omomorfismo tale che $f \circ h(n) = f(g^n) = nf(g) = n \cdot 1 = n$, cioè $f \circ h = \mathrm{id}_{\mathbb{Z}}$.

   (b) Sia $G' = \mathbb{Z}/n\mathbb{Z}$ con $n > 1$ e $f\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la proiezione naturale. Allora $h\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ è necessariamente l'omomorfismo banale: h è della forma $h(\overline{a}) = ax$ con $x \in \mathbb{Z}$ di ordine un divisore di n, e $x = 0$ perché 0 è l'unico elemento di $\mathbb{Z}$ di ordine finito. Ne segue che anche $f \circ h\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ è l'omomorfismo banale, dunque diverso da $\mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$, dato che $n > 1$.

(c) $\ker(f)$ è un sottogruppo normale di S_3, dunque può essere solo $\{1\}$, A_3 o S_3. Se $\ker(f) = \{1\}$, f è iniettivo (oltre che suriettivo per ipotesi), dunque è un isomorfismo. Pertanto f è invertibile (sia a destra che a sinistra), cioè $h = f^{-1}$ soddisfa la proprietà richiesta. Se invece $\ker(f) = S_3$, $G' = \mathrm{im}(f) = \{1\}$ è il gruppo banale e l'unico omomorfismo $h\colon G' \to S_3$ (quello banale) è tale che $f \circ h\colon G' \to G'$ è l'unico omomorfismo (di nuovo quello banale), che ovviamente coincide con $\mathrm{id}_{G'}$. Se infine $\ker(f) = A_3$, per il primo teorema di isomorfismo

$$G' = \mathrm{im}(f) \cong S_3/\ker(f) = S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}.$$

Chiaramente f manda gli elementi di A_3 in 1 e gli elementi di $S_3 \setminus A_3$ (cioè le trasposizioni) nell'unico elemento $g \neq 1$ di G'. Scelta una trasposizione $\tau \in S_3$, la funzione $h\colon G' \to S_3$ definita da $h(1) = 1$ e $h(g) = \tau$ è un omomorfismo (dato che $G' \cong \mathbb{Z}/2\mathbb{Z}$ e τ ha ordine 2) tale che $f \circ h = \mathrm{id}_{G'}$.

3. (a) Per dimostrare che $t(J)$ è un ideale verifichiamo le tre proprietà che deve soddisfare.

   i. $0 \in t(J)$: questo viene direttamente dalla definizione.

   ii. chiusura per somma: se $a_1, a_2 \in t(J)$ esistono due polinomi $p_1, p_2 \in J$ che li hanno (rispettivamente) come coefficienti del monomio di grado massimo. Siano d_1, d_2 i gradi di p_1 e p_2 e supponiamo, senza perdita di generalità, che $d_1 \geq d_2$: allora anche $q = x^{d_1 - d_2} p_1 + p_2 \in J$, perché J è un ideale, e il coefficiente del monomio di grado massimo di q è proprio $a_1 + a_2$, che quindi è in $t(J)$.

   iii. chiusura per prodotto con elementi di A: se $a_1 \in t(J)$, esso è il coefficiente del monomio di grado massimo di un polinomio $p_1 \in J$. Sia ora $a_2 \in A$ un elemento qualunque: essendo J un ideale, $a_2 p_1 \in J$ e il coefficiente del suo monomio di grado massimo è proprio $a_2 a_1$, che quindi appartiene a $t(J)$.

   (b) Ad esempio l'ideale $I[X]$, cioè quello generato da I e da X in $A[X]$, soddisfa $t(I[X]) = I$. Infatti per definizione tutti i coefficienti dei suoi elementi sono in I, quindi anche quelli del monomio di grado massimo di ciascun suo elemento.

   (c) Ci sono in generale molti ideali $J \subsetneq A[X]$ per cui $t(J) = A$. Ad esempio l'ideale (principale) generato da X, come quello generato da ogni polinomio monico in $A[X]$ che non sia 1, ha questa proprietà.

4. (a) Più in generale, per ogni anello A, un omomorfismo di anelli $f\colon A \to \mathbb{Z}/n\mathbb{Z}$ è sempre suriettivo. Infatti l'immagine di f è un sottoanello B di $\mathbb{Z}/n\mathbb{Z}$, per cui, in particolare, $\overline{1} \in B$ e B è un sottogruppo di $\mathbb{Z}/n\mathbb{Z}$. Se ne deduce che B contiene il sottogruppo di $\mathbb{Z}/n\mathbb{Z}$ generato da $\overline{1}$, che è tutto $\mathbb{Z}/n\mathbb{Z}$. Questo dimostra che $B = \mathbb{Z}/n\mathbb{Z}$, cioè f è suriettivo.

   (b) Indicando con $\pi\colon \mathbb{Z}[X] \to \mathbb{Z}[X]/(p)$ la proiezione naturale, sia $f' := f \circ \pi\colon \mathbb{Z}[X] \to \mathbb{Z}/n\mathbb{Z}$, e si noti che anche f' è un omomorfismo di anelli (in quanto composizione di omomorfismi di anelli). Inoltre $f'(m) = \overline{m} \in \mathbb{Z}/n\mathbb{Z}$ per ogni $m \in \mathbb{Z}$ (perché $f'(1) = \overline{1}$ e f' è un omomorfismo di gruppi additivi). Scelto allora $a \in \mathbb{Z}$ tale che $\overline{a} = f'(X)$, il fatto che f' sia un omomorfismo di anelli implica che $f'(q) = \overline{q(a)}$ per ogni $q \in \mathbb{Z}[X]$. In particolare $\overline{f'(p)} = \overline{p(a)}$, ma $f'(p) = \overline{0}$ perché $p \in \ker(\pi) \subseteq \ker(f')$. Dunque $\overline{p(a)} = \overline{0}$, cioè $p(a) \equiv 0 \mod n$.

   (c) No, non è possibile. Se infatti lo fosse, per il punto precedente esisterebbe $a \in \mathbb{Z}$ tale che $p(a) = a^2 + a + 1 \equiv 0 \mod 11$, mentre è facile vedere che questo non è vero. Per dimostrare quest'ultimo fatto si può semplicemente verificare che nessuno dei valori di a da 0 a 10 soddisfa la congruenza. In alternativa si può osservare che $(X-1)p = X^3 - 1$, per cui un'eventuale soluzione a della congruenza soddisfa anche $a^3 \equiv 1 \mod 11$ e $a \not\equiv 1 \mod 11$. Questo implica che $\overline{a} \in \mathbb{Z}/11\mathbb{Z}^*$ e che in tale gruppo $\overline{a}$ ha ordine 3, ma ciò contraddice il teorema di Lagrange, dato che (essendo 11 un numero primo) $\#(\mathbb{Z}/11\mathbb{Z}^*) = 11 - 1 = 10$ e 3 non divide 10.