Corso di Algebra 1 - a.a. 2014-2015

Prova scritta del 23.9.2015

1. Dati un intero positivo n e un numero primo p tali che $p > n/2$, sia H un sottogruppo di S_n di ordine p.
   (a) Dimostrare che ogni elemento non banale di H è un ciclo di ordine p.
   (b) Sia H' un altro sottogruppo di ordine p. Verificare che esiste $g \in S_n$ tale che $H' = gHg^{-1}$.

2. (a) Contare gli elementi di ordine 3 in $S_3 \times \mathbb{Z}/4\mathbb{Z}$.
   (b) Dimostrare che non esiste un omomorfismo iniettivo di gruppi da A_4 a $S_3 \times \mathbb{Z}/4\mathbb{Z}$.
   (c) Dimostrare che esiste un omomorfismo non banale di gruppi da A_4 a $S_3 \times \mathbb{Z}/4\mathbb{Z}$.

3. Sia A un anello commutativo. Dati $a, b \in A$, sia $\overline{b}$ l'immagine di b in $A/(a)$.
   (a) Dimostrare che $\overline{b}$ è invertibile in $A/(a)$ se e solo se $(a, b) = A$.
   (b) Se A è un dominio a fattorizzazione unica e $a \neq 0$, dimostrare che $\overline{b}$ è un divisore di zero in $A/(a)$ se e solo se $b \notin (a)$ e $\mathrm{mcd}(a, b)$ non è un'unità di A.

4. Sia $P(X) = 3X^4 - 8X^3 + 16 \in \mathbb{Q}[X]$.
   (a) Dimostrare che P ha una radice multipla.
   (b) Dimostrare che nell'anello quoziente $\mathbb{Q}[X]/(P)$ esiste un elemento $a \neq 0$ tale che $a^2 = 0$.

Soluzioni

1. (a) Sia $\sigma \in H$ con $\sigma \neq e$. Dato che H ha ordine p primo, risulta che anche l'ordine di σ è p. Ricordiamo che se $\sigma = \sigma_1\sigma_2 \dots \sigma_k$ è la decomposizione di σ in cicli disgiunti, l'ordine di σ è il minimo comune multiplo degli ordini di σ_i. Deduciamo che ciascun fattore σ_i ha ordine p, ovvero è un ciclo di lunghezza p. Dato che $p > n/2$ non è possibile costruire due p-cicli disgiunti in S_n e dunque necessariamente $k = 1$ e σ è un p-ciclo.

   (b) Siano $\sigma \in H$ e $\sigma' \in H'$ elementi non banali. Dal punto precedente sappiamo σ e σ' sono due p-cicli e dunque esiste $g \in S_n$ tale che $\sigma' = g\sigma g^{-1}$. Del resto dato che H e H' hanno ordine p primo, deduciamo che $H = \langle\sigma\rangle$ e $H' = \langle\sigma'\rangle$. Segue che

$$gHg^{-1} = g\langle\sigma\rangle g^{-1} = \langle g\sigma g^{-1}\rangle = \langle\sigma'\rangle = H' .$$

2. (a) Dato $(\sigma, a) \in S_3 \times \mathbb{Z}/4\mathbb{Z}$, si ha $\mathrm{ord}((\sigma, a)) = \mathrm{mcm}(\mathrm{ord}(\sigma), \mathrm{ord}(a))$. Ora $\mathrm{ord}(a) \in \{1, 2, 4\}$, mentre $\mathrm{ord}(\sigma) \in \{1, 2, 3, 6\}$. Dunque l'unica possibilità affinché $\mathrm{ord}(\sigma, a) = 3$ è che $\mathrm{ord}(\sigma) = 3$ e $\mathrm{ord}(a) = 1$. Ora in S_3 ci sono 2 elementi di ordine 3 (i 3-cicli), mentre chiaramente l'unico elemento di ordine 1 in $\mathbb{Z}/4\mathbb{Z}$ è l'elemento neutro. In conclusione gli elementi di ordine 3 in $S_3 \times \mathbb{Z}/4\mathbb{Z}$ sono 2: le coppie $((1, 2, 3), \overline{0})$ e $((1, 3, 2), \overline{0})$.

   (b) In A_4 ci sono 8 elementi di ordine 3 (i 3-cicli). Ora se esistesse un omomorfismo iniettivo $f : A_4 \to S_3 \times \mathbb{Z}/4\mathbb{Z}$, esso manderebbe elementi di ordine 3 in elementi di ordine 3. Ma poiché A_4 contiene 8 elementi di ordine 3 mentre $S_3 \times \mathbb{Z}/4\mathbb{Z}$ ne contiene solo 2 per il punto precedente, la funzione f non può essere iniettiva.

   (c) Ricordiamo che A_4 contiene un sottogruppo normale, V_4, di ordine 4 formato dalle doppie trasposizioni e dall'elemento neutro. Il quoziente è un gruppo di ordine 3. In particolare A_4/V_4 è isomorfo a $\mathbb{Z}/3\mathbb{Z}$. Del resto il gruppo $\mathbb{Z}/3\mathbb{Z}$ è isomorfo al gruppo A_3. Otteniamo dunque un omomorfismo suriettivo $f : A_4 \to A_3$ componendo la proiezione canonica $A_4 \to A_4/V_4$ con l'isomorfismo $A_4/V_4 \to A_3$. L'omomorfismo cercato si ottiene infine componendo f con le inclusioni $A_3 \to S_3 \to S_3 \times \mathbb{Z}/4\mathbb{Z}$.

3. (a) $\overline{b}$ è invertibile se e solo se esiste $c \in A$ tale che $\overline{b}\overline{c} = \overline{1}$, cioè $bc \in 1 + (a)$. Per definizione di (a), quest'ultima condizione è

verificata se e solo se esiste $d \in A$ tale che $bc = 1 + ad$. Dunque $\overline{b}$ è invertibile se e solo se esistono $c, d \in A$ tali che $1 = bc - ad$, se e solo se $1 \in (a, b)$, se e solo se $(a, b) = A$ (dato che A è l'unico ideale di A che contiene 1).

(b) Per definizione, $\overline{b}$ è un divisore di zero se e solo se $\overline{b} \neq \overline{0}$ ed esiste $c \in A$ tale che $\overline{c} \neq \overline{0}$ e $\overline{b}\overline{c} = \overline{0}$. Chiaramente $\overline{b} \neq \overline{0}$ vale se e solo se $b \notin (a)$, e resta da dimostrare che l'esistenza di c con le proprietà indicate equivale a $m = \mathrm{mcd}(a, b) \notin A^*$. Infatti, se $m \notin A^*$, allora esistono $c, d \in A$ tali che $a = mc$ e $b = md$ con $c \notin (a)$ (altrimenti esisterebbe $n \in A$ tale che $c = na$, quindi $a = mc = mna$, da cui, essendo $a \neq 0$, seguirebbe $mn = 1$, cioè $m \in A^*$). Dunque $\overline{c} \neq \overline{0}$ e $bc = mdc = ad \in (a)$, cioè $\overline{b}\overline{c} = \overline{0}$. Viceversa, se $m \in A^*$ e $c \in A$ verifica $\overline{b}\overline{c} = \overline{0}$, cioè $bc = aa'$ per qualche $a' \in A$, allora risulta $c \in (a)$ (questo segue subito dall'unicità delle fattorizzazioni), cioè $\overline{c} = \overline{0}$.

4. (a) $q \in \mathbb{Q}$ è una radice multipla di P se e solo se $P(q) = P'(q) = 0$. Essendo $P'(X) = 12X^3 - 24X^2 = 12X^2(X - 2)$, le sole radici di P' sono 0 e 2. Si ha $P(0) = 16 \neq 0$ e $P(2) = 0$, dunque 2 è l'unica radice multipla di P.

(b) Per il punto precedente si può scrivere $P = (X-2)^2 Q$ per qualche $Q \in \mathbb{Q}[X]$ (è anche facile vedere che $Q(X) = 3X^2 + 4X + 4$, che è irriducibile). Allora l'elemento $a = (X - 2)Q + (P)$ di $\mathbb{Q}[X]/(P)$ verifica $a \neq 0$ (perché $(X - 2)Q \notin (P)$) e $a^2 = 0$ (perché $((X - 2)Q)^2 = PQ \in (P)$).