Corso di Algebra 1 - a.a. 2018-2019

Prova scritta del 23/09/2019

1. Sia n un intero positivo e siano $\sigma, \tau \in S_n$ due cicli disgiunti di lunghezza, rispettivamente, s e t.
   (a) Dimostrare che $\langle \sigma \rangle \cap \langle \tau \rangle = \{1\}$.
   (b) Dimostrare che $\langle \sigma, \tau \rangle = \langle \sigma\tau \rangle$ se e solo se $\mathrm{mcd}(s,t) = 1$.

2. Per ogni $a \in \mathbb{R}$ indichiamo con $\overline{a}$ la classe laterale $a + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$.
   (a) Dimostrare che $\mathrm{ord}(\overline{a}) < \infty$ se e solo se $a \in \mathbb{Q}$.
   (b) Dati $b, c \in \mathbb{Q}$, dimostrare che $\langle \overline{b} \rangle = \langle \overline{c} \rangle$ se e solo se $\mathrm{ord}(\overline{b}) = \mathrm{ord}(\overline{c})$.
   (c) Dimostrare che ogni sottogruppo finito di $\mathbb{R}/\mathbb{Z}$ è ciclico.

3. Sia K un campo. Per ogni sottoinsieme S di $\mathbb{N}$ sia
$$E_S := \left\{ \sum_{i \geq 0} a_i X^i \in K[X] \,:\, a_i = 0 \ \forall i \in \mathbb{N} \setminus S \right\}.$$
   (a) Dimostrare che E_S è un sottoanello di $K[X]$ se e solo se S è un sottomonoide di $\mathbb{N}$ (cioè $0 \in S$ e $n + m \in S$ per ogni $n, m \in S$).
   (b) Sia S un sottomonoide di $\mathbb{N}$ e sia T un sottoinsieme di S. Dimostrare che E_T è un ideale di E_S se e solo se $n + m \in T$ per ogni $n \in T$ e per ogni $m \in S$.
   (c) Siano S e T come nel punto precedente. Dimostrare che E_T è un ideale massimale di E_S se e solo se $T = S \setminus \{0\}$.

4. Si consideri il polinomio $f = 6X^4 + 5X^3 + 4X^2 + 4X + 1$.
   (a) Fattorizzare f in $\mathbb{Z}[X]$.
   (b) Per quali valori di p primo f è irriducibile in $\mathbb{Z}/p\mathbb{Z}[X]$?

Soluzioni

1. (a) Supponiamo $\sigma = (i_1, \ldots, i_s)$, $\tau = (j_1, \ldots, j_t)$ e poniamo $A = \{i_1, \ldots, i_s\}$ e $B = \{j_1, \ldots, j_t\}$. Per ipotesi $A \cap B = \varnothing$. Inoltre $\sigma(x) = x$ per ogni $x \notin A$ e $\tau(x) = x$ per ogni $x \notin B$. Se $g \in \langle\sigma\rangle \cap \langle\tau\rangle$, allora $g = \sigma^p = \tau^q$ per opportuni interi p, q. Se $x \notin A$ si ha $g(x) = \sigma^p(x) = x$. Se invece $x \in A$, allora $x \notin B$, dunque $g(x) = \tau^q(x) = x$. Quindi $g = 1 \in S_n$.

   (b) L'inclusione $\langle\sigma, \tau\rangle \supset \langle\sigma\tau\rangle$ è sempre valida. L'inclusione opposta $\langle\sigma, \tau\rangle \subset \langle\sigma\tau\rangle$ è equivalente al fatto che

   $$\sigma, \tau \in \langle\sigma\tau\rangle. \tag{1}$$

   Basta dimostrare che vale (1) $\Leftrightarrow \mathrm{mcd}(s, t) = 1$. Se $\mathrm{mcd}(s, t) = 1$, esistono $h, k \in \mathbb{Z}$ tali che $hs + kt = 1$, dunque – ricordando che $\sigma\tau = \tau\sigma$ perché cicli disgiunti commutano – si ha $(\sigma\tau)^{hs} = \sigma^{hs}\tau^{1-kt} = \tau$ e $(\sigma\tau)^{kt} = \sigma^{1-hs}\tau^{kt} = \sigma$. Dunque vale (1). Viceversa, se (1) vale, esiste $N \in \mathbb{Z}$ tale che $\sigma = (\sigma\tau)^N$. Dunque $\sigma^{1-N} = \tau^N \in \langle\sigma\rangle \cap \langle\tau\rangle$. Per il punto (a) $\sigma^{1-N} = \tau^N = 1$. Dunque $s|(1-N)$ e $t|N$, quindi $1 - N = hs$, $N = kt$ e $1 = hs + kt$, dunque $\mathrm{mcd}(s, t) = 1$.

2. (a) Per definizione $\mathrm{ord}(\overline{a}) < \infty$ se e solo se esiste un intero positivo n tale che $n\overline{a} = \overline{0}$. Poiché $n\overline{a} = \overline{na}$, questa condizione è verificata se e solo se $na \in \mathbb{Z}$. Dunque $\mathrm{ord}(\overline{a}) < \infty$ se e solo se esistono $m, n \in \mathbb{Z}$ con $n > 0$ tali che $a = mn^{-1}$, cioè se e solo se $a \in \mathbb{Q}$.

   (b) Se $\langle\overline{b}\rangle = \langle\overline{c}\rangle$, allora chiaramente

   $$\mathrm{ord}(\overline{b}) = \#\langle\overline{b}\rangle = \#\langle\overline{c}\rangle = \mathrm{ord}(\overline{c}).$$

   Viceversa, se $\mathrm{ord}(\overline{b}) = \mathrm{ord}(\overline{c}) = n > 0$ (si noti che $n < \infty$ per il punto precedente), allora $n\overline{b} = \overline{0}$ e, come prima, esiste $m \in \mathbb{Z}$ tale che $b = mn^{-1}$. Passando al quoziente si ottiene $\overline{b} = m\overline{n^{-1}} \in \langle\overline{n^{-1}}\rangle$, e quindi $\langle\overline{b}\rangle \subseteq \langle\overline{n^{-1}}\rangle$. D'altra parte $\mathrm{ord}(\overline{n^{-1}}) = n$ (perché $nn^{-1} = 1 \in \mathbb{Z}$, mentre $n'n^{-1} \notin \mathbb{Z}$ per $0 < n' < n$), per cui

   $$\#\langle\overline{b}\rangle = \mathrm{ord}(\overline{b}) = n = \mathrm{ord}(\overline{n^{-1}}) = \#\langle\overline{n^{-1}}\rangle.$$

   Se ne deduce che $\langle\overline{b}\rangle = \langle\overline{n^{-1}}\rangle$, e analogamente $\langle\overline{c}\rangle = \langle\overline{n^{-1}}\rangle$; pertanto $\langle\overline{b}\rangle = \langle\overline{c}\rangle$.

(c) Sia $H = \{\overline{a_1}, \ldots, \overline{a_k}\}$ un sottogruppo finito di $\mathbb{R}/\mathbb{Z}$. Ogni elemento di H ha ordine finito (per il teorema di Lagrange), dunque (grazie al primo punto) $a_i \in \mathbb{Q}$ per ogni $i = 1, \ldots, k$, cioè esistono $m_i, n_i \in \mathbb{Z}$ con $n_i > 0$ tali che $a_i = m_i n_i^{-1}$. Posto $n := \mathrm{mcm}(n_1, \ldots, n_k)$, per ogni $i = 1, \ldots, k$ esiste $l_i = m_i n_i^{-1} n \in \mathbb{Z}$ tale che $a_i = l_i n^{-1}$, e quindi $\overline{a_i} = l_i \overline{n^{-1}} \in \langle \overline{n^{-1}} \rangle$. Ciò implica che $H \subseteq \langle \overline{n^{-1}} \rangle$ è ciclico perché sottogruppo di un gruppo ciclico.

3. (a) Osserviamo per prima cosa che E_S è sempre un sottogruppo di $K[X]$: infatti ovviamente $0 \in E_S$ e, se $f = \sum_{i \geq 0} a_i X^i$ e $g = \sum_{i \geq 0} b_i X^i$ sono due elementi di E_S (cioè $a_i = b_i = 0$ per ogni $i \in \mathbb{N} \setminus S$), allora anche $f - g = \sum_{i \geq 0} (a_i - b_i) X^i \in E_S$ (perché $a_i - b_i = 0 - 0 = 0$ per ogni $i \in \mathbb{N} \setminus S$). È inoltre chiaro che $1 \in E_S$ se e solo se $0 \in S$. Resta allora da dimostrare che E_S è chiuso rispetto al prodotto se e solo se S è chiuso rispetto alla somma. Supponiamo che S sia chiuso rispetto alla somma e siano $f, g \in E_S$ come sopra. Si ha $fg = \sum_{i \geq 0} c_i X^i$ con $c_i = \sum_{j=0}^{i} a_j b_{i-j}$, e va dimostrato che $fg \in E_S$, cioè che $c_i = 0$ per ogni $i \in \mathbb{N} \setminus S$. Fissato dunque $i \in \mathbb{N} \setminus S$, è sufficiente dimostrare che $a_j b_{i-j} = 0$ per ogni $j = 0, \ldots, i$: se così non fosse, si avrebbe $j, i - j \in S$ e $i = j + (i - j) \notin S$, contro l'ipotesi. Viceversa, se S non è chiuso rispetto alla somma, allora esistono $n, m \in S$ tali che $n + m \notin S$: questo implica che $X^n, X^m \in E_S$ e $X^{n+m} = X^n X^m \notin E_S$, per cui E_S non è chiuso rispetto al prodotto.

(b) Come visto nel punto precedente, E_T è sempre un sottogruppo di $K[X]$ e quindi di E_S (dato che $E_T \subseteq E_S$ perché $T \subseteq S$). Resta allora da dimostrare che E_T assorbe il prodotto in E_S se e solo se T assorbe la somma in S. Supponiamo che T assorba la somma in S e siano $f \in E_T$ e $g \in E_S$ come sopra. Va dimostrato che $fg \in E_T$, cioè (sempre usando la notazione di prima) $c_i = 0$ per ogni $i \in \mathbb{N} \setminus T$. Fissato dunque $i \in \mathbb{N} \setminus T$, è sufficiente dimostrare che $a_j b_{i-j} = 0$ per ogni $j = 0, \ldots, i$: se così non fosse, si avrebbe $j \in T$, $i - j \in S$ e $i = j + (i - j) \notin T$, contro l'ipotesi. Viceversa, se T non assorbe la somma in S, allora esistono $n \in T$ e $m \in S$ tali che $n + m \notin T$: questo implica che $X^n \in E_T$, $X^m \in E_S$ e $X^{n+m} = X^n X^m \notin E_T$, per cui E_T non assorbe il prodotto in E_S.

(c) Se $T = S \setminus \{0\}$, allora per ogni $n \in T$ e per ogni $m \in S$ si ha $n + m \in S$ (perché S è chiuso rispetto alla somma) e $n + m > 0$ (perché $n > 0$), cioè $n + m \in T$: per il punto precedente questo dimostra che E_T è un ideale di E_S. Inoltre la funzione

$\alpha\colon E_S \to K$, $\sum_{i\geq 0} a_i X^i \mapsto a_0$ è chiaramente un omomorfismo di anelli tale che $\ker(\psi) = E_T$. Poiché ψ è suriettiva (perché $0 \in S$), per il primo teorema di isomorfismo per anelli si ottiene $K = \mathrm{im}(\psi) \cong E_S/\ker(\psi) = E_S/E_T$. Dunque E_T è massimale in E_S perché E_S/E_T è un campo. Viceversa, se E_T è un ideale massimale di E_S, allora $0 \notin T$ (se no $1 \in E_T$), cioè $T \subseteq S \setminus \{0\}$, e quindi $E_T \subseteq E_{S\setminus\{0\}}$. Essendo entrambi ideali massimali, deve essere $E_T = E_{S\setminus\{0\}}$ e perciò $T = S \setminus \{0\}$.

4. (a) Se $x = p/q \in \mathbb{Q}$ è una radice, allora $p|1$ e $q|6$. Fra le varie possibilità si verifica che $x = -1/3$ è una radice. Dunque $h := 3X + 1$ divide f in $\mathbb{Q}[X]$. Siccome f è primitivo, h divide f anche in $\mathbb{Z}[X]$. Infatti $f = hq$ con $q = 2X^3 + X^2 + X + 1$. Le possibili radici razionali di q sono ± 1 e $\pm 1/2$, ma nessuna di loro è radice. Dunque q non ha radici su $\mathbb{Q}$, quindi – essendo un polinomio cubico – è irriducibile in $\mathbb{Q}[X]$ e in $\mathbb{Z}[X]$.

   (b) Sia p un primo e supponiamo che $\overline{f}$ sia irriducibile in $\mathbb{Z}/p\mathbb{Z}[X]$. La fattorizzazione $f = hq$ in $\mathbb{Z}[X]$, dà luogo a una fattorizzazione $\overline{f} = \overline{h}\overline{q}$ in $\mathbb{Z}/p\mathbb{Z}[X]$. Siccome $\overline{f}$ è irriducibile, questa fattorizzazione deve essere banale, dunque $\overline{h} = \overline{1}$ o $\overline{q} = \overline{1}$. Ma $\overline{q} \neq \overline{1}$ perché $\overline{1} \neq \overline{0}$ in $\mathbb{Z}/p\mathbb{Z}$. Quindi $\overline{h} = \overline{1}$ ossia $3 \equiv 0 \mod p$, cioè $p = 3$. Dunque l'unica possibilità è $p = 3$ e in $\mathbb{Z}/3\mathbb{Z}[X]$ $\overline{f} = \overline{q}$. Siccome $\overline{q}$ non ha radici in $\mathbb{Z}/3\mathbb{Z}$, è irriducibile. Pertanto $p = 3$ è l'unico primo tale che f sia irriducibile in $\mathbb{Z}/p\mathbb{Z}[X]$.