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

Prova scritta del 09/07/2019

1. Sia G un gruppo e sia H un sottogruppo di G. Diciamo che un sottoinsieme E di G è *invariante* per H se per ogni $x \in E$ e per ogni $h \in H$ si ha $hx \in E$. Dimostrare le affermazioni seguenti.
   (a) Ogni laterale destro di H è invariante per H.
   (b) E è invariante per H se e solo se è unione di laterali destri di H.

2. Sia G un gruppo abeliano tale che $g^2 = 1$ per ogni $g \in G$.
   (a) Dimostrare che dati $g_1, g_2, g_3 \in G$ esiste un unico omomorfismo di gruppi $\phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to G$ tale che $\phi(\overline{1}, \overline{0}, \overline{0}) = g_1$, $\phi(\overline{0}, \overline{1}, \overline{0}) = g_2$ e $\phi(\overline{0}, \overline{0}, \overline{1}) = g_3$.
   (b) Dimostrare che ϕ è iniettivo se e solo se $g_1 \neq 1$, $g_2 \notin \{1, g_1\}$ e $g_3 \notin \{1, g_1, g_2, g_1g_2\}$.
   (c) Calcolare l'ordine di $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

3. Sia I un ideale di un anello commutativo A. Per ogni $n \in \mathbb{N}$ sia inoltre
$$I_n := \left\{ \sum_{i \geq 0} a_i X^i \in A[X] \,:\, a_i = 0 \ \forall i < n,\ a_i \in I \ \forall i \geq n \right\}.$$
   (a) Dimostrare che I_n è un ideale di $A[X]$.
   (b) Dimostrare che, se $I = A$, allora I_n è primo se e solo se $n = 1$ e A è un dominio.
   (c) Dimostrare che, se $I \neq A$ e $I \neq \{0\}$, allora I_n è primo se e solo se $n = 0$ e I è primo.

4. Dati $a, b, c \in \mathbb{Z}$, si consideri il polinomio $f = X^4 + aX^3 + bX^2 + cX + 15$.
   (a) Supponendo che b sia pari e che uno solo tra a e c sia dispari, dimostrare che f è irriducibile in $\mathbb{Z}[X]$.
   (b) Supponendo che b sia dispari e che a e c siano pari, fornire un esempio in cui f è irriducibile in $\mathbb{Z}[X]$ e un esempio in cui non lo è.

Soluzioni

1. (a) Un laterale destro di H è un sottoinsieme di G della forma Hg per qualche $g \in G$. Per ogni $x \in Hg$, per definizione esiste $a \in H$ tale che $x = ag$. Quindi per ogni $h \in H$ si ha (tenendo presente che $ha \in H$, dato che H è un sottogruppo di G)

$$hx = h(ag) = (ha)g \in Hg.$$

Questo dimostra che Hg è invariante per H.

(b) Se $E = \bigcup_{i \in I} E_i$ con $E_i = Hg_i$ laterale destro di H per ogni $i \in I$, allora per ogni $x \in E$ esiste $i \in I$ tale che $x \in E_i$. Poiché E_i è invariante per H (grazie al punto precedente), si ha $hx \in E_i \subseteq E$ per ogni $h \in H$, cioè E è invariante per H.
Viceversa, se E è invariante per H, allora per definizione

$$Hx = \{hx \,:\, h \in H\} \subseteq E$$

per ogni $x \in E$, e da ciò segue che $\bigcup_{x \in E} Hx \subseteq E$. D'altra parte $x = 1x \in Hx$ (dato che $1 \in H$) per ogni $x \in G$, per cui si ha anche $E \subseteq \bigcup_{x \in E} Hx$. In conclusione $E = \bigcup_{x \in E} Hx$ è unione di laterali destri di H.

2. (a) Se ϕ esiste, siccome G è abeliano, si ha

$$\phi(\overline{m}, \overline{n}, \overline{k}) = g_1^m g_2^n g_3^k. \tag{1}$$

In particolare, se ϕ esiste, ϕ è unico. Inoltre possiamo usare la formula (1) per definire ϕ. La definizione è ben posta, perché $g_i^2 = 1$. Dal fatto che G è abeliano, segue che

$$\begin{aligned}&\phi(\overline{m} + \overline{m'}, \overline{n} + \overline{n'}, \overline{k} + \overline{k'}) = \phi(\overline{m+m'}, \overline{n+n'}, \overline{k+k'})\\ &= g_1^{m+m'} g_2^{n+n'} g_3^{k+k'} = g_1^m g_2^n g_3^k g_1^{m'} g_2^{n'} g_3^{k'} = \phi(\overline{m}, \overline{n}, \overline{k})\phi(\overline{m'}, \overline{n'}, \overline{k'}).\end{aligned}$$

Dunque ϕ è un omomorfismo che soddisfa le condizioni richieste.

(b) Se ϕ è iniettivo, allora $g_1 = \phi(\overline{1}, \overline{0}, \overline{0}) \neq 1$ e $g_2 = \phi(\overline{1}, \overline{0}, \overline{0}) \notin \{1, g_1\}$. Infine $(\overline{0}, \overline{0}, \overline{1}) \notin \{(\overline{0}, \overline{0}, \overline{0}), (\overline{1}, \overline{0}, \overline{0}), \overline{0}, \overline{1}, \overline{0}), (\overline{1}, \overline{1}, \overline{0})\}$, quindi $g_3 \notin \{1, g_1, g_2,\ g_1 g_2\}$. Viceversa, supponiamo $g_1 \neq 1$, $g_2 \notin \{1, g_1\}$ e $g_3 \notin \{1, g_1, g_2, g_1 g_2\}$. Se $(\overline{m}, \overline{n}, \overline{k}) \in \ker \phi$, allora $g_1^m g_2^n g_3^k = 1$, dunque $g_3^k = g_1^{-m} g_2^{-n}$. Se k è dispari, segue $g_3 = g_3^k \in \langle g_1, g_2 \rangle = \{1, g_1, g_2, g_1 g_2\}$, contro l'ipotesi. Dunque k è pari. Ma allora

$g_1^m g_2^n = 1$. Se n è dispari, $g_2 \in \langle g_1 \rangle = \{1, g_1\}$, contro l'ipotesi. Dunque anche n è pari e $g_1^m = 1$. Ma $g_1 \neq 1$, quindi anche m è pari. Quindi $(\overline{m}, \overline{n}, \overline{k}) = (\overline{0}, \overline{0}, \overline{0})$ e $\ker \phi = \{(\overline{0}, \overline{0}, \overline{0})\}$. Quindi ϕ è iniettiva.

(c) Gli automofismi di $G := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sono esattamente gli omomorfismi iniettivi $\phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to G$. Assegnare un automorfismo di G è dunque equivalente a scegliere $g_1, g_2, g_3 \in G$ che soddisfino le condizioni in (b). Possiamo scegliere $g_1 \in G - \{1\}$, $g_2 \in G - \{1, g_1\}$ e $g_3 \in G - \{1, g_1, g_2, g_1 g_2\}$. Quindi nel complesso abbiamo

$$|G - \{1\}| \cdot |G - \{1, g_1\}| \cdot |G - \{1, g_1, g_2, g_1 g_2\}| = 7 \cdot 6 \cdot 4 = 168$$

scelte. Quindi $|\mathrm{Aut}(G)| = 168$.

3. (a) Chiaramente $0 \in I_n$. Se $f = \sum_{i \geq 0} a_i X^i, g = \sum_{i \geq 0} b_i X^i \in I_n$ (cioè $a_i = b_i = 0$ per ogni $i < n$ e $a_i, b_i \in I$ per ogni $i \geq n$), allora $f + g = \sum_{i \geq 0} (a_i + b_i) X^i \in I_n$ perché $a_i + b_i = 0$ per ogni $i < n$ e $a_i + b_i \in I$ (essendo I un sottogruppo additivo di A) per ogni $i \geq n$. Se poi $h = \sum_{i \geq 0} c_i X^i \in A[X]$, allora $fh = \sum_{i \geq 0} d_i X^i$ con $d_i = \sum_{j=0}^{i} a_j c_{i-j}$. Se $i < n$, in tale espressione di d_i risulta sempre $a_j = 0$, e quindi $d_i = 0$; d'altra parte, in ogni caso $a_j \in I$, per cui (essendo I un ideale di A) $d_i \in I$ per ogni $i \geq 0$. Pertanto $fh \in I_n$.

(b) Poiché $I = A$, si ha $\sum_{i \geq 0} a_i X^i \in I_n$ se e solo se $a_i = 0$ per ogni $i < n$, e da ciò si deduce immediatamente che $I_n = (X^n)$. In particolare $I_0 = (1) = A[X]$ non è primo. I_n non è primo nemmeno per $n > 1$: si può supporre $A \neq \{0\}$ (altrimenti $I_n = A[X] = \{0\}$), e allora $X, X^{n-1} \notin I_n$, mentre $X^n = X X^{n-1} \in I_n$. Dunque I_n può essere primo solo per $n = 1$, e $I_1 = (X)$ è primo se e solo se $A[X]/(X) \cong A$ è un dominio.

(c) Si ha $I_0 = I[X]$, che è primo se e solo se $A[X]/I[X] \cong (A/I)[X]$ è un dominio, se e solo se A/I è un dominio, se e solo se I è primo. Invece I_n non è mai primo se $n > 0$: esiste $a \in I \setminus \{0\}$ e $aX^n \in I_n$, mentre $a \notin I_n$ (perché $n > 0$ e $a \neq 0$) e $X^n \notin I_n$ (perché $1 \notin I$).

4. (a) Se a è dispari e b e c sono pari, la riduzione di f su $\mathbb{Z}/2\mathbb{Z}$ è $\bar{f} = X^4 + X^3 + 1$. Questo polinomio non ha radici in $\mathbb{Z}/2\mathbb{Z}$, dunque f non ha radici in $\mathbb{Z}$. In particolare $\bar{f}$ e f non hanno fattori lineari. Se $\bar{f}$ fosse riducibile in $\mathbb{Z}/2\mathbb{Z}[X]$, allora sarebbe prodotto di due polinomi quadratici senza radici. L'unico polinomio quadratico

senza radici in $\mathbb{Z}/2\mathbb{Z}[X]$ è $g = X^2 + X + 1$. Ma $g^2 \neq \bar{f}$. Quindi $\bar{f}$ ed f non hanno fattori quadratici. Quindi $\bar{f}$ ed f sono irriducibili. Se invece c è dispari e a e b sono pari, la riduzione di f su $\mathbb{Z}/2\mathbb{Z}$ è $\bar{f} = X^4 + X + 1$. Anche in questo caso $\bar{f}$ non ha radici e $\bar{f} \neq g^2$. Dunque $\bar{f}$ ed f sono irriducibili.

(b) Scegliendo $a = c = 10$ e $b = 5$, il polinomio è irriducibile per il criterio di Eisenstein. Invece $f = X^4 + 2X^3 + 9X^2 + 8X + 15 = (X^2 + X + 3)(X^2 + X + 5)$ è riducibile.