Corso di Algebra 1 – a.a. 2012-2013

Prova scritta del 17.6.2013

1. Sia $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ e sia H il sottogruppo di G generato da $(\bar{1}, \bar{1}, \bar{1})$.
   (a) Si mostri che tutti gli elementi non nulli di G/H hanno ordine 2.
   (b) Si determini l'ordine massimo n_{max} degli elementi di G e si determini il numero di elementi di G di ordine n_{max}.
   (c) Si contino i sottogruppi ciclici di G di ordine n_{max}.

2. Sia G un gruppo finito, sia H un sottogruppo normale di G di ordine 5 e sia K un sottogruppo di G di ordine 7.
   (a) Si contino gli elementi di HK.
   (b) Si verifichi che $g^4 h g^{-4} = h$ per ogni $g \in G$.
   (c) Si verifichi che HK è isomorfo a $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

3. (a) Determinare gli interi m per i quali esiste un omomorfismo di anelli $\mathbb{Z}[\sqrt{m}] \to \mathbb{Z}[\sqrt{3}]$.
   (b) Per ognuno di questi valori determinare il numero dei possibili omomorfismi.

4. Sia p un numero primo e sia $L = \mathbb{F}_p$ il campo con p elementi. Sia $P \in L[X]$ un polinomio e sia n il suo grado. Sia ξ una radice di P in una estensione di L. Mostrare che:
   (a) ξ^p è una radice di P;
   (b) P è irriducibile se e solo se $\xi, \xi^p, \xi^{p^2}, \ldots, \xi^{p^{n-1}}$ sono distinti;
   (c) se P è irriducibile $L[\xi]$ è un campo di spezzamento di P su L e ha cardinalità p^n.

Soluzioni

1. (a) $\mathbb{Z}/6\mathbb{Z}$ e $\mathbb{Z}/10\mathbb{Z}$ sono isomorfi, rispettivamente, a $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ e a $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ e si può fare in modo che, nell'isomorfismo, il generatore $\bar{1}$ corrisponda a $(\bar{1}, \bar{1})$. Quindi

$$G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

   e in questo isomorfismo $(\bar{1}, \bar{1}, \bar{1})$ corrisponde a $(\bar{1}, \bar{1}, \bar{1}, \bar{1}, \bar{1})$. Inoltre, dato che 4, 3 e 5 sono a due a due primi fra loro, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ è isomorfo a $\mathbb{Z}/60\mathbb{Z}$. Quindi

$$G \cong \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \tag{1}$$

   e l'immagine di H in questo isomorfismo è generata da $(\bar{1}, \bar{1}, \bar{1})$. Questo elemento ha ordine 60 e la sua immagine per proiezione sul fattore $\mathbb{Z}/60\mathbb{Z}$ è il generatore $\bar{1}$. Quindi G/H è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; in particolare ogni suo elemento non nullo ha ordine 2.
   (b) L'isomorfismo (1) mostra che il massimo ordine di un elemento di G è 60.
   (c) Gli elementi di ordine 60 sono quelli che, nell'isomorfismo (1), corrispondono a elementi del tipo (a, b, c), dove a genera $\mathbb{Z}/60\mathbb{Z}$ e b, c sono arbitrari. Il numero dei generatori di $\mathbb{Z}/60\mathbb{Z}$ è $\varphi(60) = \varphi(4)\varphi(3)\varphi(5) = 2 \cdot 2 \cdot 4 = 16$, dove φ indica la funzione di Eulero. Il numero cercato è dunque $4 \cdot 16 = 64$.

2. (a) $\#(HK) = (\#H \cdot \#K)/\#(H \cap K) = \#H \cdot \#K = 5 \cdot 7$ perché l'ordine di $H \cap K$ divide sia $\#H = 5$ che $\#K = 7$ e quindi vale 1.

   (b) Se $h = 1$ non c'è niente da verificare. Se $h \neq 1$, è un generatore di H perché H ha ordine primo. Dato che H è normale $ghg^{-1} \in H$, quindi $ghg^{-1} = h^i$ per qualche $i \not\equiv 0 \mod 5$, e quindi $g^4hg^{-4} = h^{i^4}$. Ma $i^4 \equiv 1 \mod 5$ per il piccolo teorema di Fermat, quindi $g^4hg^{-4} = h$.

   (c) Se $1 \neq g \in K$, allora g^4 è un generatore di K perché 4 è primo con $7 = \#K$. Segue allora da (b) che $khk^{-1} = h$ per ogni $h \in H$ e ogni $k \in K$. Quindi l'applicazione $H \times K \to HK$, $(h, k) \mapsto hk$ è un omomorfismo; visto che il suo nucleo è $H \cap K$, è un isomorfismo. Ma $H \times K \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

3. (a) Ricordiamo che ogni elemento di $\mathbb{Z}[\sqrt{3}]$ si scrive in uno e un solo modo sotto la forma $a + b\sqrt{3}$ con a e b interi. Sia $\alpha : \mathbb{Z}[\sqrt{m}] \to \mathbb{Z}[\sqrt{3}]$ un omomorfismo. Se $n \in \mathbb{Z}$, $\alpha(n) = \alpha(n \cdot 1) = n\alpha(1) = n \cdot 1 = n$. Poi $\alpha(\sqrt{m})^2 = \alpha((\sqrt{m})^2) = \alpha(m) = m$. Dunque se scriviamo $\alpha(\sqrt{m}) = a + b\sqrt{3}$, con a e b interi, allora

$$m = a^2 + 3b^2 + 2ab\sqrt{3}$$

   Questo implica che $ab = 0$. Ci sono dunque due possibilità: o $b = 0$, m è un quadrato, $\mathbb{Z}[\sqrt{m}] = \mathbb{Z}$ e α è l'inclusione naturale, oppure $a = 0$ e m è il triplo di un quadrato. Supponiamo ora che $m = 3h^2$ con h intero, e mostriamo che esiste un unico omomorfismo α tale che $\alpha(\sqrt{m}) = h\sqrt{3}$. Sicuramente esiste un unico omomorfismo $\beta : \mathbb{Z}[X] \to \mathbb{Z}[\sqrt{3}]$ che manda X in $h\sqrt{3}$. D'altra parte $\mathbb{Z}[\sqrt{m}] \cong \mathbb{Z}[X]/(X^2 - m)$ e $\beta(X^2 - m) = \beta(X)^2 - m = (h\sqrt{3})^2 - m = 0$. L'esistenza e unicità di α segue dunque dal teorema di omomorfismo per anelli.

   (b) Con riferimento ai due casi considerati in (a), nel primo l'omomorfismo è unico, mentre nel secondo vi sono due scelte possibili, quella che manda $\sqrt{m}$ in $\sqrt{m}$ e quella che manda $\sqrt{m}$ in $-\sqrt{m}$.

4. (a) Scriviamo $P(X) = \sum a_i X^i$ dove $a_i \in L$; quindi $a_i^p = a_i$ per ogni i. Allora

$$0 = (P(\xi))^p = \sum a_i^p (\xi^p)^i = \sum a_i (\xi^p)^i = P(\xi^p)$$

   (b) Se $P = ST$, dove S e T sono polinomi in $L[X]$ di grado minore di n, ξ è radice di uno dei fattori, diciamo di S. Per il punto (a), $\xi, \xi^p, \xi^{p^2}, \ldots, \xi^{p^{n-1}}$ sono radici di S. Dato che $\deg(S) < n$, non possono essere distinte.
   Supponiamo viceversa che $\xi, \xi^p, \xi^{p^2}, \ldots, \xi^{p^{n-1}}$ non siano distinte, cioè che $\xi^{p^i} = \xi^{p^j}$ per qualche i e qualche j con $0 \leq i < j \leq n - 1$; poniamo $h = j - i$. Allora $\xi^{p^{i+h}} = \xi^{p^i}$, cioè

$$(\xi^{p^{j-i}})^{p^i} = \xi^{p^i}$$

   Dato che l'elevamento a p-esima potenza è una applicazione iniettiva, ne segue che $\xi = \xi^{p^{j-i}}$. Sia h il minimo intero con $0 < h < n$ tale che

$$\xi = \xi^{p^h} \tag{2}$$

   Scriviamo $E = L[\xi]$ e poniamo

$$Q(X) = \prod_{i=1}^{h} (X - \xi^{p^i}) \in E[X]$$

Per costruzione, Q divide P in $E[X]$ e ha grado $h < n = \deg(P)$. Basterà mostrare che $Q \in L[X]$. Sia $\beta : E \to E$ l'omomorfismo di Frobenius $x \mapsto x^p$. Indichiamo con la stessa lettera β la sua estensione $E[X] \to E[X]$ data da $\sum a_i X^i \mapsto \sum \beta(a_i) X^i$. L'omomorfismo β permuta ciclicamente fra loro le radici di Q. Quindi $\beta(Q) = Q$, il che significa che $\beta(a) = a$ per ogni coefficiente a di Q. Ma allora tutti i coefficienti di Q appartengono a L, come si voleva dimostrare.

Soluzione alternativa. Basta mostrare che P non è il polinomio minimo di ξ su L. La formula (2) dice che ξ è radice del polinomio $X^{p^h} - X$. Ma l'insieme delle radici di questo polinomio è il campo con p^h elementi, che ha grado h su L. Quindi il grado del polinomio minimo di ξ su L non supera $h < n$. Il polinomio minimo in questione non può dunque essere P.

(c) Se P è irriducibile (b) mostra che tutte le sue radici sono potenze di ξ e quindi appartengono a $L[\xi]$. Ne segue che questo è il campo di spezzamento di P su L. Il grado $[L[\xi] : L]$ è il grado del polinomio minimo di ξ, cioè di P, che vale n. Dunque $L[\xi]$ ha $(\#L)^n = p^n$ elementi.