Corso di Algebra 2 - a.a. 2019-2020

Prova scritta del 07/09/2020

1. Siano A un anello e M e N due A-moduli non nulli. Dimostrare che esiste un omomorfismo non nullo di A-moduli $M \to N$ in ciascuno dei seguenti casi.

   (a) M è un A-modulo libero.

   (b) $M = A/I$ con I ideale sinistro di A e esiste $x \in N \setminus \{0\}$ tale che $I \subseteq \mathrm{Ann}_A(x)$.

   (c) A è un dominio a ideali principali ma non un campo e M e N sono finitamente generati e di P-torsione per qualche ideale massimale P di A.

2. Sia G un gruppo di ordine $12p$ con $p > 3$ primo e sia K un p-Sylow di G. Si supponga inoltre che G contenga un sottogruppo $H \cong A_4$.

   (a) Dimostrare che, se $p \neq 5, 11$, allora K è normale in G.

   (b) Per $p = 5$ fornire un esempio in cui K non è normale in G.

   (c) Dimostrare che, se $p > 11$ e $p \not\equiv 1 \mod 3$, allora $G \cong C_p \times A_4$.

3. Siano K un campo, $f := X^6 - 5X^3 + 6 \in K[X]$ e G il gruppo di Galois di f su K.

   (a) Dimostrare che, se $K \subseteq L$ è un'estensione di campi e $\alpha \in L$ è una radice di f, allora $[K(\alpha) : K] \leq 3$.

   (b) Trovare, per ogni $n = 1, 2, 3$, un numero primo p tale che $G \cong C_n$ se $K = \mathbb{F}_p$.

   (c) Dimostrare che esiste K tale che $G \cong S_3$.

Soluzioni

1. (a) Sia $\{x_\lambda : \lambda \in \Lambda\}$ una base di M (con $x_\lambda \neq x_\mu$ se $\lambda \neq \mu$). Allora, scelti arbitrariamente elementi $y_\lambda \in N$ per ogni $\lambda \in \Lambda$, esiste (unico) un omomorfismo di A-moduli $f\colon M \to N$ tale che $f(x_\lambda) = y_\lambda$ per ogni $\lambda \in \Lambda$. Il fatto che $M \neq \{0\}$ implica $\Lambda \neq \emptyset$, quindi, dato che anche $N \neq \{0\}$, gli elementi y_λ possono essere scelti non tutti nulli, ottenendo allora f non nullo.

   (b) La funzione $f_x\colon A \to N$, $a \mapsto ax$ è un omomorfismo di A-moduli tale che $\ker(f_x) = \{a \in A : ax = 0\} = \mathrm{Ann}_A(x) \supseteq I$. Per il teorema di omomorfismo per moduli esiste (unico) un omomorfismo di A-moduli $f\colon A/I \to N$ tale che $f(\overline{a}) = f_x(a)$ per ogni $a \in A$ (dove $\overline{a} := a + I \in A/I$). Chiaramente f non è nullo perché $f(\overline{1}) = f_x(1) = x \neq 0$.

   (c) Osserviamo preliminarmente che, se $M = M' \oplus M''$, $N = N' \oplus N''$ e $f\colon M' \to N'$ è un omomorfismo non nullo di A-moduli, allora anche la composizione $M \xrightarrow{\mathrm{pr}} M' \xrightarrow{f} N' \xrightarrow{\mathrm{in}} N$ lo è (dove pr indica la proiezione e in l'inclusione). Ora, per il teorema di struttura dei moduli finitamente generati su un dominio a ideali principali, M e N sono somme dirette finite (non vuote, essendo M e N non nulli) di A-moduli indecomponibili di P-torsione, cioè della forma A/P^l per qualche $l > 0$. Possiamo pertanto supporre $M = A/P^m$ e $N = A/P^n$ con $m, n > 0$. In questo caso, indicando con $p \in A$ un generatore dell'ideale (principale) P, la tesi segue dal punto precedente con $I = P^m$ e $x = p^{n-1} + P^n \in A/P^n = N$: infatti $x \neq 0$ (perché $p^{n-1} \notin P^n = (p^n)$) e $I = P^m \subseteq \mathrm{Ann}_A(x) = P$ (si noti che $P \subseteq \mathrm{Ann}_A(x)$ perché chiaramente $p \in \mathrm{Ann}_A(x)$ e $\mathrm{Ann}_A(x) \subsetneq A$ perché $x \neq 0$).

2. (a) Il numero s_p di p-Sylow soddisfa $s_p \equiv 1 \mod p$ e $s_p \mid 12$. In particolare $s_p \leq 12$ e, se fosse $s_p > 1$, si avrebbe anche $s_p > p$, per cui $p < 12$. Dato che $p > 3$ e $p \neq 5, 11$, l'unica possibilità sarebbe dunque $p = 7$, ma da $s_7 \equiv 1 \mod 7$ e $s_7 \mid 12$ segue chiaramente $s_7 = 1$. Questo dimostra che in ogni caso $s_p = 1$, e quindi K è normale.

   (b) Si può prendere $G = A_5$. Infatti $\#A_5 = 60 = 12 \cdot 5$ e sicuramente un 5-Sylow K non è normale, dato che A_5 è semplice. Inoltre $H := \{\sigma \in A_5 : \sigma(5) = 5\}$ è un sottogruppo di A_5 tale che $H \cong A_4$.

(c) Essendo $p > 11$, per il primo punto K è normale in G. Poiché $\#K = p$, $\#H = \#A_4 = 12$ e $\mathrm{mcd}(p, 12) = 1$, si ha $H \cap K = \{1\}$ e $HK = G$ (dato che $\#(HK) = (\#H)(\#K) = 12p = \#G$). Ne segue che $G = K \rtimes H$, e pertanto $G \cong C_p \rtimes_\theta A_4$ per qualche omomorfismo $\theta\colon A_4 \to \mathrm{Aut}(C_p) \cong \mathbb{Z}/p\mathbb{Z}^*$. Per il primo teorema di isomorfismo $\mathrm{im}(\theta) \cong A_4/\ker(\theta)$, dove $\ker(\theta)$ è un sottogruppo normale di A_4 e dunque può essere solo $\{1\}$, V_4 o A_4. Se $\ker(\theta)$ fosse $\{1\}$ o V_4, $\mathrm{im}(\theta)$ avrebbe ordine $12/1 = 12$ o $12/4 = 3$, e in particolare multiplo di 3. Questo però non è possibile, perché per il teorema di Lagrange anche $\#\mathrm{Aut}(C_p) = p - 1$ sarebbe multiplo di 3, contro l'ipotesi $p \not\equiv 1 \mod 3$. Si conclude allora che $\ker(\theta) = A_4$, cioè θ è l'omomorfismo banale, e pertanto $G \cong C_p \times A_4$.

3. (a) $f = gh$ in $K[X]$ con $g := X^3 - 2$ e $h := X^3 - 3$. Dunque α, essendo radice di f, deve essere radice di g o di h, e ciò implica che $\mathrm{m}_{\alpha,K}$ divide g o h. Allora $[K(\alpha) : K] = \deg(\mathrm{m}_{\alpha,K}) \leq \deg(g) = \deg(h) = 3$.

   (b) Ricordiamo che, se $\#K < \infty$ e $f = f_1 \cdots f_r$ con f_i irriducibile di grado d_i per $i = 1, \ldots, r$, allora $G \cong C_{\mathrm{mcm}(d_1,\ldots,d_r)}$.
   Se $n = 1$ si può prendere $p = 3$ perché $g = (X - 2)^3$ e $h = X^3$.
   Se $n = 2$ si può prendere $p = 2$ perché $g = X^3$ e $h = X^3 - 1 = (X - 1)(X^2 + X + 1)$ con $X^2 + X + 1$ irriducibile in $\mathbb{F}_2[X]$.
   Se $n = 3$ si può prendere $p = 7$ perché g e h sono irriducibili (essendo di grado 3 e senza radici in $\mathbb{F}_7$).

   (c) Le radici complesse di g (rispettivamente h) sono $\sqrt[3]{2}\omega^i$ (rispettivamente $\sqrt[3]{3}\omega^i$) per $i = 0, 1, 2$ con $\omega := e^{2\pi i/3}$. Quindi un campo di spezzamento di $f = gh$ su $\mathbb{Q}$ è $L := \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}, \omega)$, e basta dimostrare che esiste un campo intermedio $\mathbb{Q} \subseteq K \subseteq L$ tale che $\mathrm{G}_K(L) \cong S_3$ (perché L è campo di spezzamento di f anche su K). A priori ci sono due possibilità: g può essere o non essere irriducibile in $\mathbb{Q}(\sqrt[3]{3})[X]$ (in effetti non sarebbe difficile dimostrare che è vera la prima alternativa). Se g è irriducibile in $\mathbb{Q}(\sqrt[3]{3})[X]$, allora si può prendere $K = \mathbb{Q}(\sqrt[3]{3})$: infatti $K \subseteq L = K(\sqrt[2]{3}, \omega)$ è campo di spezzamento di g irriducibile di terzo grado con $\Delta(g) < 0$ che non è un quadrato in $K \subseteq \mathbb{R}$, per cui $G = \mathrm{G}_K(g) \cong S_3$. Se invece g non è irriducibile in $\mathbb{Q}(\sqrt[3]{3})[X]$, allora si può prendere $K = \mathbb{Q}$: infatti g (avendo grado 3) deve avere una radice in $\mathbb{Q}(\sqrt[3]{3}) \subseteq \mathbb{R}$ (necessariamente $\sqrt[3]{2}$); ne segue che $K \subseteq L = K(\sqrt[3]{3}, \omega)$ è campo di spezzamento di h irriducibile di terzo grado con $\Delta(h) < 0$ che non è un quadrato in $K = \mathbb{Q}$, per cui $G = \mathrm{G}_K(h) \cong S_3$.