Corso di Algebra 2 - a.a. 2020-2021

Prova scritta del 23/09/2021

1. Siano A un anello commutativo, I un ideale di A e M un A-modulo non nullo.
   (a) Se M è libero, dimostrare che $IM = M$ se e solo se $I = A$.
   (b) Se A è un sottoanello di un campo K, dimostrare che $IK = K$ se e solo se $I \neq \{0\}$.
   (c) Se A è un dominio a ideali principali ma non un campo e M è finitamente generato e di P-torsione (per qualche ideale massimale P di A), dimostrare che $IM = M$ se e solo se $I \not\subseteq P$.

2. In ciascuno dei seguenti casi stabilire se esiste un gruppo di ordine n che sia unione dei suoi sottogruppi di Sylow.
   (a) $n = 21$.
   (b) $n = 375$.
   (c) $n = 63$.

3. Siano K un campo perfetto, $f \in K[X]$ irriducibile di quarto grado e G il gruppo di Galois di f su K. Siano inoltre α una radice di f (in un campo di spezzamento) e c il numero di estensioni non banali $K \subsetneq K' \subsetneq K(\alpha)$.
   (a) Dimostrare che f si spezza su $K(\alpha)$ se e solo se G ha ordine 4.
   (b) Dimostrare che, se G è ciclico, allora $c = 1$.
   (c) Dimostrare che, se $G \cong A_4$ o S_4, allora $c = 0$.

Soluzioni

1. (a) Chiaramente $AM = M$, dato che $x = 1x \in AM$ per ogni $x \in M$. Viceversa, se $IM = M$, allora per ogni $x \in M$ esistono $b_1, \ldots, b_n \in I$ e $x_1, \ldots, x_n \in M$ tali che $x = \sum_{i=1}^{n} b_i x_i$. In particolare, prendendo come x un elemento di una base di M, e indicando (per ogni $i = 1, \ldots, n$) con $a_i \in A$ il coefficiente di x nell'espressione di x_i come combinazione lineare degli elementi della base, risulta $1 = \sum_{i=1}^{n} b_i a_i \in I$, per cui $I = A$.

   (b) Ovviamente $\{0\}K = \{0\} \neq K$. Se invece $I \neq \{0\}$, sia $0 \neq b \in I$. Per ogni $x \in K$ si ha (tenendo conto che b è invertibile nel campo K) $x = (bb^{-1})x = b(b^{-1}x) \in IK$. Ciò dimostra $IK = K$.

   (c) Siano $p, b \in A$ tali che $P = (p)$ e $I = (b)$. Essendo M finitamente generato e di P-torsione, esiste $n \in \mathbb{N}$ tale che $\mathrm{Ann}(M) = P^n = (p^n)$; inoltre $n > 0$ perché $M \neq \{0\}$. Se $IM = M$, segue facilmente per induzione $I^i M = M$ per ogni $i > 0$; in particolare $I^n M = M$. Da questo si ottiene $I \not\subseteq P$, perché se invece fosse $I \subseteq P$, si avrebbe anche $I^n \subseteq P^n = \mathrm{Ann}(M)$, e quindi $I^n M = \{0\}$, contraddicendo $I^n M = M \neq \{0\}$. Viceversa, se $I \not\subseteq P$, si ha $p \nmid b$ in A. Essendo p irriducibile in A, questo implica $\mathrm{mcd}(b, p^n) = 1$, quindi esistono $a, a' \in A$ tali che $1 = ab + a'p^n$. Osservando che $ab \in I$ e $a'p^n \in P^n = \mathrm{Ann}(M)$, si ottiene allora

$$x = (ab + a'p^n)x = (ab)x + (a'p^n)x = (ab)x \in IM,$$

   per ogni $x \in M$, il che dimostra $IM = M$.

2. Sia G un gruppo di ordine n e sia s_p il numero dei p-Sylow di G per ogni divisore primo p di n.

   (a) Sì, esiste. Sia infatti G un gruppo non abeliano di ordine $21 = 3 \cdot 7$ (che esiste perché $7 \equiv 1 \mod 3$; esplicitamente $G := C_7 \rtimes_\theta C_3$ con $\theta \colon C_3 \to \mathrm{Aut}(C_7) \cong \mathbb{Z}/7\mathbb{Z}^* \cong C_6$ omomorfismo non banale). Poiché G non è ciclico, per il teorema di Lagrange ogni elemento non banale g di G ha ordine 3 o 7, e dunque appartiene al sottogruppo di Sylow $\langle g \rangle$.

   (b) No, non esiste. Infatti, notando che $375 = 3 \cdot 5^3$, per il teorema di Sylow $s_5 = 1$ (perché $s_5 \equiv 1 \mod 5$ e $s_5 \mid 3$) e $s_3 = 1$ o 25 (perché $s_3 \equiv 1 \mod 3$ e $s_3 \mid 5^3$). Perciò ci sono $5^3 = 125$ elementi nell'unico 5-Sylow e al massimo $25(3-1) = 50$ elementi non banali nei 3-Sylow. Si conclude che la cardinalità dell'unione di tutti i sottogruppi di Sylow è al massimo $125 + 50 = 175 < 375$.

(c) No, non esiste. Infatti, notando che $63 = 3^2 \cdot 7$, per il teorema di Sylow $s_7 = 1$ (perché $s_7 \equiv 1 \mod 7$ e $s_7 \mid 3^2$) e $s_3 = 1$ o 7 (perché $s_3 \equiv 1 \mod 3$ e $s_3 \mid 7$). Perciò ci sono 7 elementi nell'unico 7-Sylow e al massimo $7(9-1) = 56$ elementi non banali nei 3-Sylow. Quindi la cardinalità dell'unione di tutti i sottogruppi di Sylow è al massimo $7 + 56 = 63$, ma l'uguaglianza vale se e solo se $s_3 = 7$ e $H \cap K = \{1\}$ per ogni coppia di 3 Sylow distinti H e K. Tuttavia quest'ultima condizione non può essere soddisfatta, perché altrimenti si avrebbe l'assurdo $\#(HK) = (\#H)(\#K) = 9 \cdot 9 = 81 > 63$.

3. Sia $K \subseteq L$ un campo di spezzamento di f (per cui $G = \mathrm{G}_K(L)$) tale che $\alpha \in L$. Poiché $K \subseteq L$ è di Galois (è normale e finita perché campo di spezzamento di un polinomio, è separabile perché K è perfetto), $\#G = [L : K]$.

   (a) Dato che $K(\alpha) \subseteq L$, f si spezza su $K(\alpha)$ se e solo se $L = K(\alpha)$ se e solo se $\#G = [L : K] = [K(\alpha) : K]$. Basta allora osservare che $[K(\alpha) : K] = \deg(f) = 4$ perché f è irriducibile.

   (b) Poiché $4 = [K(\alpha) : K] \mid [L : K] = \#G$ e G è isomorfo a un sottogruppo di S_4 (che non contiene elementi di ordine > 4), necessariamente $G \cong C_4$. Dal punto precedente segue $K(\alpha) = L$, dunque c coincide (per il teorema fondamentale della teoria di Galois) con il numero di sottogruppi non banali di $G \cong C_4$, cioè 1.

   (c) Sempre per il teorema fondamentale della teoria di Galois, $H := \mathrm{G}_{K(\alpha)}(L)$ è un sottogruppo di G di indice $[K(\alpha) : K] = 4$. Supponendo per assurdo $c > 0$, sia $K \subsetneq K' \subsetneq K(\alpha)$ un'estensione non banale. Essendo $[K' : K]$ un divisore non banale di $[K(\alpha) : K] = 4$, si ha $[K' : K] = 2$, per cui $H' := \mathrm{G}_{K'}(L)$ è un sottogruppo di G di indice $[K' : K] = 2$ e tale che $H \subseteq H'$; inoltre $[H' : H] = [G : H]/[G : H'] = 4/2 = 2$. Per ottenere un assurdo basta osservare che A_4 non ha sottogruppi di indice 2, mentre l'unico sottogruppo di indice 2 di S_4 è proprio A_4, che però (come appena detto) non ha sottogruppi di indice 2.