Corso di Algebra 2 - a.a. 2018-2019
Prova scritta dell'11/02/2020

1. Siano A un dominio a ideali principali, M un A-modulo finitamente generato e M' un sottomodulo di M.
   (a) Dimostrare che M' è noetheriano.
   (b) Fornire un esempio in cui M è indecomponibile, $M' \neq M$ e M/M' non è indecomponibile.
   (c) Dimostrare che, se M è ciclico, allora M' è ciclico.
   (d) È vero che, se M è indecomponibile e $M' \neq \{0\}$, allora M' è indecomponibile?

2. In ciascuno dei seguenti casi stabilire se esiste un gruppo semplice di ordine n.
   (a) $n = 275$.
   (b) $n = 360$.
   (c) $n = 380$.
   (d) $n = 450$.

3. Siano $\alpha, \beta \in \mathbb{C}$ tali che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] = 2$ e $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$. Sia inoltre $L := \mathbb{Q}(\alpha, \beta)$.
   (a) Dimostrare che $[L : \mathbb{Q}] = 4$.
   (b) Dimostrare che $\mathbb{Q} \subseteq L$ è un'estensione di Galois e determinarne il gruppo di Galois.
   (c) Dimostrare che, se $\alpha^2, \beta^2 \in \mathbb{Q}$, allora $L = \mathbb{Q}(\alpha + \beta)$.
   (d) Sia $L \subsetneq L'$ un'estensione tale che $\mathbb{Q} \subseteq L'$ sia un campo di spezzamento di $f \in \mathbb{Q}[X]$ di quarto grado. Dimostrare che il gruppo di Galois di f su $\mathbb{Q}$ è isomorfo a D_4.

Soluzioni

1. (a) Essendo A un anello commutativo noetheriano, un A-modulo è noetheriano se e solo se è finitamente generato. Dunque M è noetheriano, e ciò implica che anche M' lo è (un sottomodulo di un modulo noetheriano è noetheriano).

   (b) Sia $A = M = \mathbb{Z}$ e $M' = 6\mathbb{Z}$: $\mathbb{Z}$ è indecomponibile (perché è un dominio), mentre $\mathbb{Z}/6\mathbb{Z} = \langle\overline{3}\rangle \oplus \langle\overline{2}\rangle \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ non lo è.

   (c) A meno di isomorfismo, si può supporre $M = A/I$ con I ideale di A. Allora esiste un unico A-sottomodulo (cioè ideale) J di A tale che $I \subseteq J$ e $M' = J/I$. D'altra parte J è un ideale principale di A, cioè è un A-modulo ciclico, e questo implica che anche il suo quoziente M' lo è.

   (d) Sì, è vero. È infatti noto, che, a meno di isomorfismo, si può supporre $M = A$ o (nel caso in cui A non sia un campo) $M = A/P^n$ con P ideale massimale di A e $n > 0$. In ogni caso M è ciclico, e dunque anche M' lo è per il punto precedente. Indicando con x un generatore di M', si ha allora $M' \cong A/\mathrm{Ann}_A(x)$; si noti che $x \neq 0$ perché $M' = \langle x\rangle_A \neq \{0\}$. Se $M = A$, allora $\mathrm{Ann}_A(x) = \{0\}$ (perché A è un dominio e $x \neq 0$), e quindi $M' \cong A$ è indecomponibile. Se invece $M = A/P^n$, allora x è di P-torsione (perché M lo è), per cui $\mathrm{Ann}_A(x) = P^{n'}$ per qualche $n' > 0$ (e $n' \leq n$, come è facile vedere). Se ne deduce che $M' \cong A/P^{n'}$ è indecomponibile anche in questo caso.

2. (a) No, non esiste. Infatti ogni gruppo di ordine $275 = 5^2 \cdot 11$ ha un unico 11-Sylow (il numero di 11-Sylow è $\equiv 1 \mod 11$ e divide 25), che è quindi normale.

   (b) Sì, esiste: A_6 è un gruppo semplice di ordine $6!/2 = 360$.

   (c) No, non esiste. Sia G un gruppo di ordine $380 = 2^2 \cdot 5 \cdot 19$, e indichiamo con s_p il numero di p-Sylow di G per $p = 5$ e $p = 19$. Da $s_{19} \equiv 1 \mod 19$ e $s_{19} \mid 20$ segue $s_{19} = 1$ o $s_{19} = 20$, mentre da $s_5 \equiv 1 \mod 5$ e $s_5 \mid 76$ segue $s_5 = 1$ o $s_5 = 76$. Non può essere $s_{19} = 20$ e $s_5 = 76$, perché in quel caso G conterrebbe $20 \cdot 18 = 360$ elementi di ordine 19 (ogni 19-Sylow contiene 18 tali elementi, e l'intersezione di due 19-Sylow distinti è $\{1\}$) e analogamente $76 \cdot 4 = 304$ elementi di ordine 5, il che è impossibile, dato che $360 + 304 > 380 = \#G$. Se ne deduce che $s_{19} = 1$ o $s_5 = 1$, per cui il 19-Sylow o il 5-Sylow è normale in G.

(d) No, non esiste. Sia G un gruppo di ordine $450 = 2 \cdot 3^2 \cdot 5^2$: usando la notazione del punto precedente, da $s_5 \equiv 1 \mod 5$ e $s_5 \mid 18$ segue $s_5 = 1$ o $s_5 = 6$. Se $s_5 = 1$, il 5-Sylow è normale in G. Se invece $s_5 = 6$, il normalizzatore H di un 5-Sylow è un sottogruppo di G di indice 6. È noto che esiste un omomorfismo di gruppi $G \to S(G/H) \cong S_6$ (indotto dalla moltiplicazione a sinistra) il cui nucleo K è un sottogruppo normale di G contenuto in H (per cui $K \neq G$). Poiché $\#G = 450 \nmid 720 = 6! = \#S_6$, deve essere anche $K \neq \{1\}$.

3. (a) Poiché $[L : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}][L : \mathbb{Q}(\alpha)] = 2[L : \mathbb{Q}(\alpha)]$, si tratta di dimostrare che $[L : \mathbb{Q}(\alpha)] = 2$. In ogni caso

$$[L : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)] \leq [\mathbb{Q}(\beta) : \mathbb{Q}] = 2,$$

per cui basta dimostrare che $[L : \mathbb{Q}(\alpha)] > 1$ cioè che $\beta \notin \mathbb{Q}(\alpha)$. Se per assurdo fosse $\beta \in \mathbb{Q}(\alpha)$, si avrebbe $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$, e quindi

$$2 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}][\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] = 2[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)],$$

da cui seguirebbe $[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] = 1$, cioè $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.

(b) Indicando con m_α e m_β i polinomi minimi di α e β su $\mathbb{Q}$, è facile vedere che $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ è un campo di spezzamento di m_α (in $\mathbb{Q}(\alpha)[X]$ si ha $\mathrm{m}_\alpha = (X-\alpha)g$ con g monico di primo grado, cioè della forma $X - \alpha'$), e analogamente $\mathbb{Q} \subseteq \mathbb{Q}(\beta)$ è un campo di spezzamento di m_β. Ne segue che $\mathbb{Q} \subseteq L$ è un campo di spezzamento di $\mathrm{m}_\alpha\mathrm{m}_\beta$: chiaramente $\mathrm{m}_\alpha\mathrm{m}_\beta$ si spezza su L, e ogni sottocampo K di L su cui si spezza deve contenere α e β, e quindi $K \supseteq \mathbb{Q}(\alpha, \beta) = L$. Essendo campo di spezzamento di un polinomio, l'estensione $\mathbb{Q} \subseteq L$ è allora normale; d'altra parte è anche finita (come visto nel punto precedente) e separabile (perché $\mathbb{Q}$ ha caratteristica 0), e dunque è di Galois. Indicando con G il gruppo di Galois di $\mathbb{Q} \subseteq L$, si ha $\#G = [L : \mathbb{Q}] = 4$, quindi a priori $G \cong C_4$ o $G \cong C_2 \times C_2$. Per il teorema fondamentale della teoria di Galois i due diversi campi intermedi non banali $\mathbb{Q}(\alpha)$ e $\mathbb{Q}(\beta)$ dell'estensione di Galois $\mathbb{Q} \subseteq L$ corrispondono a due diversi sottogruppi non banali di G. Deve essere pertanto $G \cong C_2 \times C_2$.

(c) Sia $a := \alpha^2 \in \mathbb{Q}$ e $b := \beta^2 \in \mathbb{Q}$, e si osservi che $a \neq b$ (altrimenti $\alpha = \pm\beta$, contro l'ipotesi $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$. Posto $\gamma := \alpha + \beta$, si ha $\gamma^2 = a + b + 2\alpha\beta$, per cui $\alpha\beta = (\gamma^2 - a - b)/2 \in \mathbb{Q}(\gamma)$. Da ciò segue che anche $\alpha\beta\gamma = \alpha^2\beta + \alpha\beta^2 = a\beta + b\alpha \in \mathbb{Q}(\gamma)$. Pertanto

$\alpha = (a\beta + b\alpha - a\gamma)/(b - a) \in \mathbb{Q}(\gamma)$, e analogamente $\beta \in \mathbb{Q}(\gamma)$, il che dimostra che $L = \mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\gamma)$. Poiché chiaramente vale anche $\mathbb{Q}(\gamma) \subseteq L$, si conclude che $L = \mathbb{Q}(\gamma)$.

(d) Il gruppo di Galois G' di f su $\mathbb{Q}$ (che coincide con il gruppo di Galois di $\mathbb{Q} \subseteq L'$) è isomorfo a un sottogruppo di S_4 (perché $\deg(f) = 4$), per cui, in particolare, $n := \#G' \mid \#S_4 = 24$. Tenendo conto che inoltre $4 = [L : \mathbb{Q}] \mid [L' : \mathbb{Q}] = n$ e che $[L : \mathbb{Q}] < [L' : \mathbb{Q}]$ (perché $L \subsetneq L'$), può essere solo $n = 24$, $n = 12$ o $n = 8$. D'altra parte l'estensione normale $\mathbb{Q} \subseteq L$ di grado 4 corrisponde a un sottogruppo normale H di G' di indice 4 (tale che $G'/H \cong G \cong C_2 \times C_2$). Allora non può essere $n = 24$, perché in quel caso si avrebbe $G' \cong S_4$, ma gli unici sottogruppi normali non banali di S_4 sono A_4 (di indice 2) e V_4 (di indice 6). Analogamente non può essere $n = 12$, perché in quel caso si avrebbe $G' \cong A_4$, ma l'unico sottogruppo normale non banale di A_4 è V_4 (di indice 3). Deve essere pertanto $n = 8$ e quindi $G' \cong D_4$: è infatti noto che S_4 contiene sottogruppi isomorfi a D_4, e tutti i sottogruppi di ordine 8 di S_4 (essendo 2-Sylow) sono tra loro isomorfi.