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

Prova scritta del 24/06/2021

1. Siano A un anello, M un A-modulo e M' e M'' due sottomoduli di M tali che $M = M' + M''$.
   (a) Dimostrare che M è noetheriano se e solo se M' e M'' sono noetheriani.
   (b) Dimostrare che, se M' è semplice e $M'' \neq M$, allora $M = M' \oplus M''$.
   (c) Dimostrare che, se A è un dominio a ideali principali con un solo ideale massimale e M è finitamente generato e indecomponibile, allora $M' = M$ o $M'' = M$.

2. Sia p un numero primo e sia $n := 77p^2$.
   (a) Dimostrare che, se $p \leq 5$, allora esiste un gruppo di ordine n non abeliano.
   (b) Dimostrare che, se $p > 11$, allora ogni gruppo di ordine n ha un sottogruppo di Sylow normale.
   (c) Dimostrare che, se $p = 17$, allora ogni gruppo di ordine n è abeliano.

3. Sia $K = \mathbb{Q}(\sqrt{3}, i)$.
   (a) Dimostrare che l'estensione $\mathbb{Q} \subseteq K$ è di Galois e determinarne il gruppo di Galois.
   (b) Dimostrare che l'estensione $\mathbb{Q} \subseteq K(\sqrt[4]{3})$ è di Galois e il suo gruppo di Galois non è abeliano.
   (c) Dimostrare che, se $\alpha \in \mathbb{C} \setminus K$ e $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, allora l'estensione $\mathbb{Q} \subseteq K(\alpha)$ è di Galois e il suo gruppo di Galois è abeliano.

1. (a) Chiaramente, se M è noetheriano, anche i suoi sottomoduli M' e M'' lo sono. Viceversa, se M' e M'' sono noetheriani, anche $M' \oplus M''$ lo è. Poiché l'omomorfismo di moduli $f\colon M' \oplus M'' \to M$, $(x', x'') \mapsto x' + x''$ è tale che $\mathrm{im}(f) = M' + M'' = M$, per il primo teorema di isomorfismo per moduli si ha $M = \mathrm{im}(f) \cong (M' \oplus M'')/\ker(f)$. Dunque M è noetheriano perché isomorfo a un quoziente di un modulo noetheriano.

   (b) Basta dimostrare che $M' \cap M'' = \{0\}$. Se così non fosse, si avrebbe $M' \cap M'' = M'$ (dato che $M' \cap M''$ è un sottomodulo del modulo semplice M'), cioè $M' \subseteq M''$, e quindi $M' + M'' = M'' \neq M$.

   (c) Se A è un campo, allora (essendo M indecomponibile) posso supporre $M = A$ (a meno di isomorfismo). Poiché gli unici sottomoduli di A sono $\{0\}$ e A, se fosse $M' \neq M \neq M''$, si avrebbe la contraddizione $M = M' + M'' = \{0\} + \{0\} = \{0\}$. Se A non è un campo, e P è l'unico ideale massimale di A, allora (essendo M indecomponibile e finitamente generato) posso supporre $M = A$ o $M = A/P^n$ per qualche $n > 0$ (a meno di isomorfismo). Poiché i sottomoduli non nulli di A (rispettivamente A/P^n) sono tutti e soli della forma P^i con $i \in \mathbb{N}$ (rispettivamente P^i/P^n con $0 \leq i < n$), è chiaro che $M' \subseteq M''$ o $M'' \subseteq M'$. Dunque $M = M' + M''$ coincide con M' (se $M'' \subseteq M'$) o con M'' (se $M' \subseteq M''$).

2. Per ogni gruppo G di ordine n e per ogni primo q che divide n sia s_q il numero di q-Sylow di G. Sia inoltre H_q un q-Sylow di G.

   (a) Si può prendere $G = G' \times C_{\frac{n}{pq}}$, dove $q = 7$ se $p = 2$ o 3, $q = 11$ se $p = 5$ e G' è un gruppo non abeliano di ordine pq (che esiste perché $q \equiv 1 \mod p$).

   (b) Per il teorema di Sylow $s_p \mid 77 = 7 \cdot 11$ e $s_p \equiv 1 \mod p$. Poiché i divisori di 77 sono $1, 7, 11, 77$ e $p > 11$, può essere solo $s_p = 1$ o 77. Quest'ultimo caso si può presentare solo se $p \mid (77 - 1) = 2^2 \cdot 19$, cioè se $p = 19$. Dunque $H_p \lhd G$ per $p \neq 19$. Se $p = 19$, deve essere $s_7 \mid 11 \cdot 19^2$ e $s_7 \equiv 1 \mod 7$; poiché i divisori di $11 \cdot 19^2$ sono $1, 11, 19, 11 \cdot 19, 19^2, 11 \cdot 19^2$, e di questi 1 è l'unico $\equiv 1 \mod 7$, si conclude che in questo caso $H_7 \lhd G$.

   (c) $H_{17} \lhd G$ come visto nel punto precedente. Inoltre da $s_{11} \mid 7 \cdot 17^2$ e $s_{11} \equiv 1 \mod 11$ segue $s_{11} = 1$, cioè $H_{11} \lhd G$. D'altra parte da

$s_7 \mid 11 \cdot 17^2$ e $s_7 \equiv 1 \mod 7$ si deduce $s_7 = 1$ o $11 \cdot 17^2$. Dato che $H := H_7 H_{11}$ è un sottogruppo di G (perché $H_{11} \lhd G$) e $H_7 \lhd H$ (H è abeliano perché di ordine $7 \cdot 11$ e $11 \not\equiv 1 \mod 7$), si ha $H \subseteq N(H_7)$. Sempre per il teorema di Sylow si ottiene allora $s_7 = [G : N(H_7)] \leq [G : H] < [G : H_7] = 11 \cdot 17^2$, e quindi $s_7 = 1$, cioè anche $H_7 \lhd G$. Si conclude che $G = H_7 \times H_{11} \times H_{17}$ è abeliano, dato che lo sono $H_7 \cong C_7$, $H_{11} \cong C_{11}$ e $H_{17} \cong C_{17^2}$ o C_{17}^2.

3. In tutti i casi per dimostrare che l'estensione è di Galois basta verificare che è normale e finita (è anche separabile perché $\mathrm{char}(\mathbb{Q}) = 0$).

   (a) L'estensione $\mathbb{Q} \subseteq K$ è normale e finita perché campo di spezzamento di $(X^2 - 3)(X^2 + 1)$ (le cui radici sono $\pm\sqrt{3}, \pm i$). Per $\beta = \sqrt{3}, i$ si ha $[\mathbb{Q}(\beta) : \mathbb{Q}] = \deg(\mathrm{m}_{\beta,\mathbb{Q}}) = 2$ (essendo $\mathrm{m}_{\sqrt{3},\mathbb{Q}} = X^2 - 3$ e $\mathrm{m}_{i,\mathbb{Q}} = X^2 + 1$); inoltre $[K : \mathbb{Q}(\sqrt{3})] = 2$ perché $[K : \mathbb{Q}(\sqrt{3})] = [\mathbb{Q}(\sqrt{3})(i) : \mathbb{Q}(\sqrt{3})] \leq [\mathbb{Q}(i) : \mathbb{Q}] = 2$ e $i \notin \mathbb{Q}(\sqrt{3}) \subset \mathbb{R}$. Perciò $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$, quindi anche $\#\mathrm{G}_{\mathbb{Q}}(K) = 4$. Per ogni $\sigma \in \mathrm{G}_{\mathbb{Q}}(K)$ si ha $\sigma(\sqrt{3}) = \pm\sqrt{3}$ (perché $\sigma(\sqrt{3})$ è radice di $\mathrm{m}_{\sqrt{3},\mathbb{Q}} = X^2 - 3$) e analogamente $\sigma(i) = \pm i$, per cui $\sigma^2(\sqrt{3}) = \sqrt{3}$ e $\sigma^2(i) = i$. Da ciò segue chiaramente $\sigma^2 = \mathrm{id}_K$, e quindi $\mathrm{G}_{\mathbb{Q}}(K) \cong C_2^2$.

   (b) Dato che $\sqrt{3} = \sqrt[4]{3}^2$, si ha $K(\sqrt[4]{3}) = \mathbb{Q}(\sqrt[4]{3}, i) = \mathbb{Q}(\sqrt[4]{3}, \sqrt[4]{3}i)$. Se ne deduce che $\mathbb{Q} \subseteq K(\sqrt[4]{3})$ è normale e finita perché campo di spezzamento di $X^4 - 3$ (le cui radici sono $\pm\sqrt[4]{3}, \pm\sqrt[4]{3}i$). Tenendo conto che $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{3})$ non è normale (infatti $\mathrm{m}_{\sqrt[4]{3},\mathbb{Q}} = X^4 - 3$ non si spezza su $\mathbb{Q}(\sqrt[4]{3}) \subset \mathbb{R}$), segue dal teorema fondamentale della teoria di Galois che $\mathrm{G}_{\mathbb{Q}(\sqrt[4]{3})}(K(\sqrt[4]{3}))$ è un sottogruppo non normale di $\mathrm{G}_{\mathbb{Q}}(K(\sqrt[4]{3}))$. Pertanto $\mathrm{G}_{\mathbb{Q}}(K(\sqrt[4]{3}))$ non è abeliano.

   (c) L'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$, avendo grado 2, è normale ed è campo di spezzamento di $\mathrm{m}_{\alpha,\mathbb{Q}}$. Allora $\mathbb{Q} \subseteq K(\alpha)$ è campo di spezzamento di $(X^2 - 3)(X^2 + 1)\mathrm{m}_{\alpha,\mathbb{Q}}$, e quindi è normale e finita. Deve essere $[K(\alpha) : K] = 2$ perché $[K(\alpha) : K] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ e $\alpha \notin K$. Se ne deduce che $[K(\alpha) : \mathbb{Q}] = [K(\alpha) : K][K : \mathbb{Q}] = 2 \cdot 4 = 8$ e anche $\#G = 8$ con $G := \mathrm{G}_{\mathbb{Q}}(K(\alpha))$. Sempre per il teorema fondamentale $H := \mathrm{G}_K(K(\alpha))$ e $H' := \mathrm{G}_{\mathbb{Q}(\alpha)}(K(\alpha))$ sono sottogruppi normali di G (dato che $\mathbb{Q} \subseteq K$ e $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ sono normali). Inoltre $\#H = [K(\alpha) : K] = 2$ e $\#H' = [K(\alpha) : \mathbb{Q}(\alpha)] = \frac{[K(\alpha):\mathbb{Q}]}{[\mathbb{Q}(\alpha):\mathbb{Q}]} = \frac{8}{2} = 4$ (per cui H e H' sono abeliani). Dato che $H \cap H' = \{1\}$ (perché $\sigma \in H \cap H'$ implica $\sigma|_K = \mathrm{id}_K$ e $\sigma(\alpha) = \alpha$, per cui $\sigma = \mathrm{id}_{K(\alpha)}$) e $HH' = G$ (perché $\#(HH') = \#G$), si conclude che $G = H \times H'$ è abeliano.