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

Prova scritta del 23/06/2020

1. Siano A un anello, M un A-modulo e M' un sottomodulo di M.
   (a) Dimostrare che $\mathrm{Ann}(M) \subseteq \mathrm{Ann}(M') \cap \mathrm{Ann}(M/M')$, e che vale l'uguaglianza se M' è un addendo diretto di M.
   (b) Dimostrare che $\mathrm{Ann}(M')\mathrm{Ann}(M/M') \subseteq \mathrm{Ann}(M)$.
   (c) Trovare M' tale che
   $$\mathrm{Ann}(M')\mathrm{Ann}(M/M') \subsetneq \mathrm{Ann}(M) \subsetneq \mathrm{Ann}(M') \cap \mathrm{Ann}(M/M')$$
   quando $A = \mathbb{Z}$ e $M = \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

2. Sia p un numero primo e sia G un gruppo di ordine $p(2p + 5)$.
   (a) Dimostrare che, se $2p + 5$ è primo, allora G è ciclico.
   (b) Dimostrare che, se $p > 2$, allora G ha un unico p-Sylow.
   (c) Dimostrare che, se $p = 47$, allora G è abeliano.

3. Sia $\alpha := \sqrt{2}\sqrt[3]{3} \in \mathbb{R}$.
   (a) Dimostrare che $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$.
   (b) Dimostrare che il polinomio minimo di α su $\mathbb{Q}$ è $X^6 - 72$.
   (c) Esiste un'estensione di campi $\mathbb{Q} \subseteq K$ tale che il gruppo di Galois di $X^6 - 72$ su K sia non ciclico di ordine 4?

Soluzioni

1. (a) Se $a \in \operatorname{Ann}(M)$ (cioè $a \in A$ e $ax = 0$ per ogni $x \in M$), allora ovviamente $a \in \operatorname{Ann}(M')$ perché $ax = 0$ per ogni $x \in M'$. Inoltre $a \in \operatorname{Ann}(M/M')$ perché $a(x + M') = ax + M' = 0 + M' = M'$ per ogni $x \in M$. Ciò dimostra che $\operatorname{Ann}(M) \subseteq \operatorname{Ann}(M') \cap \operatorname{Ann}(M/M')$. Se M' è un addendo diretto di M e M'' è un sottomodulo di M tale che $M = M' \oplus M''$, allora $M/M' \cong M''$, per cui $\operatorname{Ann}(M/M') = \operatorname{Ann}(M'')$ e basta dimostrare che $\operatorname{Ann}(M') \cap \operatorname{Ann}(M'') \subseteq \operatorname{Ann}(M)$. Dato $a \in \operatorname{Ann}(M') \cap \operatorname{Ann}(M'')$, per ogni $x \in M$ esistono (unici) $x' \in M'$ e $x'' \in M''$ tali che $x = x' + x''$, e quindi $ax = a(x' + x'') = ax' + ax'' = 0 + 0 = 0$, cioè $a \in \operatorname{Ann}(M)$.

   (b) Dato $a \in \operatorname{Ann}(M')\operatorname{Ann}(M/M')$, per definizione di prodotto di ideali esistono $b_1, \dots, b_n \in \operatorname{Ann}(M')$ e $c_1, \dots, c_n \in \operatorname{Ann}(M/M')$ (per qualche $n \in \mathbb{N}$) tali che $a = \sum_{i=1}^n b_i c_i$. Per ogni $i = 1, \dots, n$ e per ogni $x \in M$ si ha $M' = c_i(x + M') = c_i x + M'$ (perché $c_i \in \operatorname{Ann}(M/M')$), cioè $c_i x \in M'$; allora $(b_i c_i)x = b_i(c_i x) = 0$ (perché $b_i \in \operatorname{Ann}(M')$), il che dimostra che $b_i c_i \in \operatorname{Ann}(M)$. Tenendo conto che $\operatorname{Ann}(M)$ è un ideale e in particolare un sottogruppo di A, si conclude che $a = \sum_{i=1}^n b_i c_i \in \operatorname{Ann}(M)$.

   (c) Poiché $\operatorname{Ann}(\mathbb{Z}/n\mathbb{Z}) = n\mathbb{Z}$ per ogni $n \in \mathbb{N}$, si ha (grazie al primo punto) $\operatorname{Ann}(M) = \operatorname{Ann}(Z/8\mathbb{Z}) \cap \operatorname{Ann}(Z/4\mathbb{Z}) = 8\mathbb{Z} \cap 4\mathbb{Z} = 8\mathbb{Z}$. Si può prendere $M' := \langle(\overline{2}, \overline{0})\rangle = \langle\overline{2}\rangle \oplus \langle\overline{0}\rangle \cong \mathbb{Z}/4\mathbb{Z}$, e quindi $M/M' \cong (\mathbb{Z}/8\mathbb{Z})/\langle\overline{2}\rangle \oplus (\mathbb{Z}/4\mathbb{Z})/\langle\overline{0}\rangle \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Infatti $\operatorname{Ann}(M') = 4\mathbb{Z}$ e $\operatorname{Ann}(M/M') = \operatorname{Ann}(\mathbb{Z}/2\mathbb{Z}) \cap \operatorname{Ann}(\mathbb{Z}/4\mathbb{Z}) = 2\mathbb{Z} \cap 4\mathbb{Z} = 4\mathbb{Z}$, per cui $\operatorname{Ann}(M')\operatorname{Ann}(M/M') = (4\mathbb{Z})(4\mathbb{Z}) = 16\mathbb{Z}$, $\operatorname{Ann}(M) \cap \operatorname{Ann}(M/M') = 4\mathbb{Z} \cap 4\mathbb{Z} = 4\mathbb{Z}$ e chiaramente $16\mathbb{Z} \subsetneq 8\mathbb{Z} \subsetneq 4\mathbb{Z}$.

2. (a) Poiché ogni gruppo di ordine pq con $p < q$ primi è ciclico se $q \not\equiv 1 \mod p$, basta dimostrare che $2p + 5 \not\equiv 1 \mod p$ se $2p + 5$ è primo. In effetti $5 \equiv 2p + 5 \equiv 1 \mod p$ se e solo se $p \mid (5 - 1) = 4$ se e solo se $p = 2$, e $2p + 5 = 9$ non è primo per $p = 2$.

   (b) Il numero s_p di p-Sylow di G soddisfa $s_p \equiv 1 \mod p$ e $s_p \mid (2p+5)$. Allora $s_p = (2p + 5)/d$ per qualche divisore d di $2p + 5$, e non può essere $d = 1$ perché, come si è visto nel punto precedente, $2p+5 \not\equiv 1 \mod p$ per $p > 2$. Poiché d è dispari (essendolo $2p + 5$), deve essere $d \geq 3$, e dunque per $p \geq 5$ si ha $s_p = (2p+5)/d \leq 3p/3 = p$, il che implica $s_p = 1$. D'altra parte $2p + 5 = 11$ è primo per $p = 3$, per cui $d = 11$ e $s_p = 1$ anche in questo caso.

(c) $2p+5 = 99 = 3^2 \cdot 11$ per $p = 47$, dunque $\#G = 3^2 \cdot 11 \cdot 47$. Per il punto precedente $s_{47} = 1$; inoltre da $s_{11} \equiv 1 \mod 11$ e $s_{11} \mid 3^2 \cdot 47$ segue $s_{11} = 1$ (basta osservare che $47 \equiv 3 \mod 11$ e che $3, 3^2, 3^3 \not\equiv 1 \mod 11$). Indicando con H_q (per $q = 3, 11, 47$) un q-Sylow di G, si ha allora $H_{11}, H_{47} \lhd G$, e quindi anche $H := H_{11}H_{47} \lhd G$ e $H \cong H_{11} \times H_{47} \cong C_{11} \times C_{47} \cong C_{11\cdot 47}$. Tenuto conto che $H \cap H_3 = \{1\}$ (avendo H e H_3 ordini coprimi) e $HH_3 = G$ (dato che $\#(HH_3) = (\#H)(\#H_3) = 11 \cdot 47 \cdot 3^2 = \#G$), si ha $G = H \rtimes H_3 \cong C_{11\cdot 47} \rtimes_\theta H_3$ per qualche omomorfismo $\theta\colon H_3 \to \mathrm{Aut}(C_{11\cdot 47})$. Visto che $\mathrm{Aut}(C_{11\cdot 47}) \cong \mathbb{Z}/(11\cdot 47)\mathbb{Z}^*$ ha ordine $\varphi(11\cdot 47) = \varphi(11)\varphi(47) = 10 \cdot 46$ coprimo con $\#H_3 = 9$, θ è banale e $G \cong C_{11\cdot 47} \times H_3$ è abeliano ($H_3 \cong C_9$ o C_3^2).

3. (a) Ovviamente $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$, per cui $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$. D'altra parte $\alpha^3 = 6\sqrt{2}, \alpha^4 = 12\sqrt[3]{3} \in \mathbb{Q}(\alpha)$, e quindi $\sqrt{2}, \sqrt[3]{3} \in \mathbb{Q}(\alpha)$, da cui segue $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) \subseteq \mathbb{Q}(\alpha)$.

(b) Chiaramente α è radice di $f := X^6 - 72$, per cui $\mathrm{m}_{\alpha,\mathbb{Q}} \mid f$, e per concludere che $\mathrm{m}_{\alpha,\mathbb{Q}} = f$ basta dimostrare che $\deg(\mathrm{m}_{\alpha,\mathbb{Q}}) = \deg(f) = 6$ (dato che entrambi i polinomi sono monici). Poiché $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ (essendo $\mathrm{m}_{\sqrt{2},\mathbb{Q}} = X^2 - 2$ e $\mathrm{m}_{\sqrt[3]{3},\mathbb{Q}} = X^3 - 3$) e $\mathrm{mcd}(2,3) = 1$, si ha $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) : \mathbb{Q}] = 2\cdot 3 = 6$. Ricordando che $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ per il punto precedente, si ottiene allora $\deg(\mathrm{m}_{\alpha,\mathbb{Q}}) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) : \mathbb{Q}] = 6$.

(c) Sì, per esempio $K = \mathbb{Q}(\sqrt[3]{3})$. Infatti le radici complesse di f sono $\alpha\omega^j$ per $j = 0, \dots, 5$ con $\omega := e^{(2\pi i)/6} = (1 + \sqrt{3}i)/2$, e dunque $L := \mathbb{Q}(\alpha, \omega)$ è un campo di spezzamento di f su $\mathbb{Q}$. Poiché $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, \omega)$ per il primo punto, L è anche un campo di spezzamento di f su K, e $G := \mathrm{G}_K(f) = \mathrm{G}_K(L)$. L'estensione $K \subseteq L$ è di Galois (è normale e finita perché campo di spezzamento di un polinomio, e è separabile perché $\mathrm{char}(K) = \mathrm{char}(\mathbb{Q}) = 0$), per cui $\#G = [L : K]$. Dato che $L = K(\sqrt{2}, \omega)$, si ha

$$[L : K] = [L : K(\sqrt{2})][K(\sqrt{2}) : K].$$

$[K(\sqrt{2}) : K] = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{3})] = 2$ (per quanto visto nel punto precedente). Inoltre $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\mathrm{m}_{\omega,\mathbb{Q}}) = 2$ (è facile vedere che $\mathrm{m}_{\omega,\mathbb{Q}} = X^2 - X + 1$), da cui segue (visto che $K(\sqrt{2}) \subset \mathbb{R}$ e $\omega \notin \mathbb{R}$) che anche $[L : K(\sqrt{2})] = [K(\sqrt{2}, \omega) : K(\sqrt{2})] = 2$. Si ottiene allora $\#G = [L : K] = 2 \cdot 2 = 4$, e G non è ciclico perché contiene due sottogruppi non banali distinti (per il teorema fondamentale della teoria di Galois) $\mathrm{G}_{K(\sqrt{2})}(L)$ e $\mathrm{G}_{K(\omega)}(L)$.