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

Prova scritta del 26/01/2021

1. Siano A un anello e M un A-modulo. In ciascuno dei seguenti casi stabilire se esiste un omomorfismo di A-moduli $f\colon M \to M$ tale che $\ker(f) = \operatorname{im}(f)$.
   (a) M è un A-modulo semplice.
   (b) $M = A^2$.
   (c) A è un dominio a ideali principali e $M = A^3$.

2. In ciascuno dei seguenti casi stabilire se esiste un gruppo non abeliano di ordine n, e, nel caso esista, se è anche unico a meno di isomorfismo.
   (a) $n = 39$.
   (b) $n = 52$.
   (c) $n = 9 \cdot 11 \cdot 17$.

3. Sia $f := X^4 - 3X^2 - 3$.
   (a) Dimostrare che, se f è il polinomio minimo di una sua radice su un campo di caratteristica $p > 0$, allora $p > 5$.
   (b) Dimostrare che $\mathrm{G}_{\mathbb{R}}(f) \cong \mathrm{G}_{\mathbb{F}_2}(f)$.
   (c) Determinare $\mathrm{G}_{\mathbb{Q}}(f)$.

1. (a) Non esiste. Infatti, se f è l'omomorfismo nullo, allora $\ker(f) = M \neq \operatorname{im}(f) = \{0\}$. Altrimenti deve essere $\ker(f) \neq M$ e $\operatorname{im}(f) \neq \{0\}$, e quindi (dato che M è semplice e $\ker(f)$ e $\operatorname{im}(f)$ sono sottomoduli di M) $\ker(f) = \{0\} \neq \operatorname{im}(f) = M$.

   (b) Esiste. Per esempio $f\colon A^2 \to A^2$ definito da $(a,b) \mapsto (b,0)$ è chiaramente A-lineare e $\ker(f) = \operatorname{im}(f) = \{(a,0) : a \in A\}$.

   (c) Non esiste. Infatti, supponiamo per assurdo che $f\colon A^3 \to A^3$ sia un omomorfismo tale che $\ker(f) = \operatorname{im}(f)$. Essendo A un dominio a ideali principali, il sottomodulo $\operatorname{im}(f)$ di A^3 è ancora libero di rango $n \leq 3$. Per il primo teorema di isomorfismo per moduli $A^3/\ker(f) \cong \operatorname{im}(f)$ è dunque libero, e questo implica che $\ker(f)$ è un addendo diretto di A^3. Indicando con $N \cong \operatorname{im}(f)$ un complementare di $\ker(f)$ in A^3, si ha allora $A^3 = \ker(f) \oplus N \cong A^n \oplus A^n \cong A^{2n}$, il che è assurdo perché $2n \neq 3$.

2. (a) Esiste ed è unico a meno di isomorfismo. Questo segue immediatamente dalla classificazione dei gruppi di ordine pq con $p < q$ primi tali che $q \equiv 1 \mod p$ (in questo caso $p = 3$ e $q = 13$). Esplicitamente un gruppo non abeliano di ordine 39 è $C_{13} \rtimes_\theta C_3$ con $\theta\colon C_3 \to \operatorname{Aut}(C_{13}) \cong \mathbb{Z}/13\mathbb{Z}^* \cong C_{12}$ omomorfismo non banale.

   (b) Esiste ma non è unico a meno di isomorfismo. Infatti i gruppi $G_1 := C_{13} \rtimes_{\theta_1} C_4$ e $G_2 := C_{13} \rtimes_{\theta_2} (C_2 \times C_2)$ con $\theta_1\colon C_4 \to \operatorname{Aut}(C_{13}) \cong C_{12}$ e $\theta_2\colon C_2 \times C_2 \to \operatorname{Aut}(C_{13}) \cong C_{12}$ omomorfismi non banali (per esempio $\theta_1(\overline{a}) := g^{3a}$ e $\theta_2((\overline{a},\overline{b})) := g^{6a}$ con g generatore di $\operatorname{Aut}(C_{13})$) non sono abeliani. Inoltre $G_1 \not\cong G_2$ perché i 2-Sylow di G_1 sono isomorfi a C_4 e i 2-Sylow di G_2 sono isomorfi a $C_2 \times C_2$.

   (c) Non esiste. In effetti, indicando con H_p (per $p = 3, 11, 17$) un p-Sylow di un gruppo G di ordine $3^2 \cdot 11 \cdot 17$ e con s_p il numero dei suoi p-Sylow, per il teorema di Sylow $s_{17} = 1$ (perché $s_{17} \equiv 1 \mod 17$ e $s_{17} \mid 3^2 \cdot 11$) e $s_{11} = 1$ (perché $s_{11} \equiv 1 \mod 11$ e $s_{11} \mid 3^2 \cdot 17$). Dunque H_{17} e H_{11} sono normali in G, e pertanto anche $H := H_{17}H_{11} \cong H_{17} \times H_{11} \cong C_{17} \times C_{11} \cong C_{17\cdot 11}$ lo è. Avendo H e H_3 ordini coprimi, si ha $H \cap H_3 = \{1\}$, da cui segue $G = HH_3$, e dunque $G = H \rtimes H_3 \cong C_{17\cdot 11} \rtimes_\theta H_3$ per qualche omomorfismo $\theta\colon H_3 \to \operatorname{Aut}(C_{17\cdot 11})$. Poiché $\operatorname{Aut}(C_{17\cdot 11}) \cong \mathbb{Z}/(17 \cdot 11)\mathbb{Z}^*$ ha ordine $\varphi(17 \cdot 11) = \varphi(17)\varphi(11) = 16 \cdot 10$ coprimo con $\#H_3 = 3^2$, θ è necessariamente banale. Ciò dimostra che $G \cong C_{17 \cdot 11} \times H_3$ è abeliano (dato che H_3 è isomorfo a C_9 o a $C_3 \times C_3$).

3. (a) Se f è il polinomio minimo di una sua radice su un campo K di caratteristica $p > 0$, allora f è irriducibile in $K[X]$, e quindi anche in $\mathbb{F}_p[X]$ (dato che K è un'estensione di $\mathbb{F}_p$). Basta allora osservare che f non è irriducibile in $\mathbb{F}_p[X]$ per $p = 2$ (perché $f = (X^2 + X + 1)^2$), $p = 3$ (perché $\overline{0}$ è radice di f) e $p = 5$ (perché $\overline{1}$ è radice di f).

   (b) Come visto nel punto precedente, $f = (X^2 + X + 1)^2$ in $\mathbb{F}_2[X]$, da cui segue $\mathrm{G}_{\mathbb{F}_2}(f) \cong C_2$. D'altra parte $f(X) = g(X^2)$, dove $g(Y) := Y^2 - 3Y - 3$. Poiché g ha radici (reali) $(3 + \sqrt{21})/2 > 0$ e $(3 - \sqrt{21})/2 < 0$, le radici complesse di f sono $\pm\alpha$ e $\pm\beta i$ con $\alpha := \sqrt{(\sqrt{21} + 3)/2}$ e $\beta := \sqrt{(\sqrt{21} - 3)/2}$. Un campo di spezzamento di f su $\mathbb{R}$ è pertanto $\mathbb{R}(\alpha, \beta i) = \mathbb{R}(i) = \mathbb{C}$, e quindi $\mathrm{G}_{\mathbb{R}}(f) \cong \mathrm{G}_{\mathbb{R}}(\mathbb{C}) \cong C_2$.

   (c) Per quanto visto nel punto precedente, un campo di spezzamento di f su $\mathbb{Q}$ è $K := \mathbb{Q}(\alpha, \beta i)$. Osservando che $\alpha\beta = \sqrt{3}$, si ha $\beta i = \sqrt{3}i/\alpha$, da cui segue $K = \mathbb{Q}(\alpha, \sqrt{3}i)$. Poiché f è irriducibile in $\mathbb{Q}[X]$ (per il criterio di Eisenstein relativo al primo 3), f è il polinomio minimo di α su $\mathbb{Q}$, e dunque $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 4$; d'altra parte $[\mathbb{Q}(\sqrt{3}i) : \mathbb{Q}] = \deg(X^2 + 3) = 2$. Se ne deduce che $4 = \mathrm{mcm}(4, 2) \mid [K : \mathbb{Q}] \leq 4 \cdot 2 = 8$. Non potendo essere $[K : \mathbb{Q}] = 4$ (altrimenti $\sqrt{3}i \in K = \mathbb{Q}(\alpha) \subset \mathbb{R}$), si ottiene che $\mathrm{G}_{\mathbb{Q}}(f) \cong \mathrm{G}_{\mathbb{Q}}(K)$ è un gruppo di ordine $[K : \mathbb{Q}] = 8$. Inoltre $\mathrm{G}_{\mathbb{Q}}(f)$ è isomorfo a un sottogruppo di $S_{\deg(f)} = S_4$, e si conclude che $\mathrm{G}_{\mathbb{Q}}(f) \cong D_4$ perché ogni sottogruppo di ordine 8 (cioè ogni 2-Sylow) di S_4 è isomorfo a D_4.