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

Prova scritta del 25/09/2020

1. Siano A un dominio e M un A-modulo.
   (a) Dimostrare che, se M è di torsione, allora l'unico omomorfismo di A-moduli $M \to A$ è quello nullo.
   (b) Dimostrare che, se A è a ideali principali e esiste un omomorfismo non nullo di A-moduli $M \to A$, allora ne esiste anche uno suriettivo.
   (c) Dimostrare che, se I è un ideale non principale di A, allora non esiste un omomorfismo suriettivo di A-moduli $I \to A$.
2. In ciascuno dei seguenti casi stabilire se esiste un gruppo G di ordine n tale che $\{1\} \neq Z(G) \neq G$.
   (a) $n = 22$.
   (b) $n = 35^2$.
   (c) $n = 55^2$.
3. Sia $f := X^5 + X^2 + 1$.
   (a) Determinare $\mathrm{G}_{\mathbb{F}_2}(f)$.
   (b) Dimostrare che esiste un campo K di caratteristica 0 tale che $\mathrm{G}_K(f) \cong C_5$.
   (c) Dimostrare che $\mathrm{G}_{\mathbb{Q}}(f)$ non è abeliano.

Soluzioni

1. (a) Sia $f\colon M \to A$ un omomorfismo di A-moduli. Essendo M di torsione, per ogni $x \in M$ esiste $a \in A \setminus \{0\}$ tale che $ax = 0$. Allora $af(x) = f(ax) = f(0) = 0$ in A, da cui segue $f(x) = 0$ perché A è un dominio e $a \neq 0$.

   (b) Se $f\colon M \to A$ è A-lineare e non nulla, allora $\mathrm{im}(f)$ è un sottomodulo (cioè un ideale) non nullo di A, e posso considerare f come una funzione A-lineare e suriettiva $M \to \mathrm{im}(f)$. Per ipotesi $\mathrm{im}(f)$ è principale, quindi esiste un isomorfismo di A-moduli $g\colon A \to \mathrm{im}(f)$: se b è un generatore di $\mathrm{im}(f)$, si può prendere come g la funzione $a \mapsto ab$, che è chiaramente A-lineare e suriettiva, ed è iniettiva perché A è un dominio e $b \neq 0$. Si conclude che $g^{-1} \circ f\colon M \to A$ è A-lineare e suriettiva (perché composizione di funzioni che lo sono).

   (c) Supponiamo per assurdo che esista un omomorfismo suriettivo di A-moduli $f\colon I \to A$. Per il primo teorema di isomorfismo per moduli $I/\ker(f) \cong \mathrm{im}(f) = A$, da cui si deduce (essendo A un A-modulo libero) che $\ker(f)$ è un addendo diretto di I. D'altra parte I è un A-modulo indecomponibile (in quanto ideale non nullo di un dominio), per cui $\ker(f) = I$ o $\ker(f) = \{0\}$. In entrambi i casi questo porta a un assurdo: se $\ker(f) = I$, allora f sarebbe l'omomorfismo nullo, contro l'ipotesi che sia suriettivo; se $\ker(f) = \{0\}$, allora f sarebbe un isomorfismo, per cui $I \cong A$ sarebbe un A-modulo ciclico, e quindi un ideale principale.

2. (a) Non esiste. Infatti $22 = 2 \cdot 11$ è della forma pq con $p < q$ primi distinti tali che $q \equiv 1 \mod p$, per cui, a meno di isomorfismo, G può essere solo C_{22} (nel qual caso $Z(G) = G$) o un prodotto semidiretto non diretto $C_{11} \rtimes C_2 \cong D_{11}$ (nel qual caso $Z(G) = \{1\}$). In alternativa si può osservare che, se $Z(G) \neq \{1\}$, allora $G/Z(G)$ è un gruppo il cui ordine è un divisore proprio di 22 (cioè 1, 2 o 11), e dunque $G/Z(G)$ è ciclico; questo implica che G è abeliano, e pertanto $Z(G) = G$.

   (b) Non esiste. Infatti, dato che $n = 5^2 \times 7^2$, per il teorema di Sylow $s_7 \equiv 1 \mod 7$ e $s_7 \mid 5^2$, per cui $s_7 = 1$; analogamente $s_5 \equiv 1 \mod 5$ e $s_5 \mid 7^2$, per cui $s_5 = 1$. Allora $G \cong H_7 \times H_5$, dove (per $p = 5, 7$) H_p indica un p-Sylow di G. Poiché H_p (avendo ordine p^2) è abeliano, anche G lo è, e dunque $G = Z(G)$.

(c) Esiste. Si può prendere per esempio $G = G_1 \times G_2$ con G_1 e G_2 gruppi di ordine 55 tali che $G_1 = C_{55}$ è abeliano e G_2 no (un tale G_2 esiste perché $55 = 5 \cdot 11$ è della forma pq con $p < q$ primi distinti tali che $q \equiv 1 \mod p$). Allora $Z(G) = Z(G_1) \times Z(G_2)$ soddisfa $Z(G) \neq \{1\}$ (perché $Z(G_1) = G_1 \neq \{1\}$) e $Z(G) \neq G$ (perché $Z(G_2) \neq G_2$).

3. (a) f è irriducibile in $\mathbb{F}_2[X]$ perché non ha radici in $\mathbb{F}_2$ e non è divisibile per $X^2 + X + 1$ (che è l'unico polinomio di secondo grado irriducibile in $\mathbb{F}_2[X]$). Ne segue che $\mathrm{G}_{\mathbb{F}_2}(f) \cong C_{\deg(f)} = C_5$.

(b) Sia $\mathbb{Q} \subseteq L$ un campo di spezzamento di f. Poiché f è irriducibile in $\mathbb{Q}[X]$ (grazie al fatto che lo è in $\mathbb{F}_2[X]$, come si è visto nel punto precedente), indicando con $\alpha \in L$ una radice di f, si ha $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 5$. D'altra parte $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ è un divisore di $[L : \mathbb{Q}] = \#\mathrm{G}_{\mathbb{Q}}(L)$, quindi per il teorema di Sylow (o di Cauchy) esiste un sottogruppo H di $\mathrm{G}_{\mathbb{Q}}(L)$ tale che $\#H = 5$. Allora per il teorema fondamentale della teoria di Galois $K := L^H$ soddisfa $\mathrm{G}_K(L) = H \cong C_5$. Per concludere basta osservare che K è un campo di caratteristica 0 (essendo un'estensione di $\mathbb{Q}$) e che $\mathrm{G}_K(L) = \mathrm{G}_K(f)$ (perché $K \subseteq L$ è un campo di spezzamento di f, dato che $\mathbb{Q} \subseteq L$ lo è).

(c) Mantenendo la notazione del punto precedente, possiamo supporre inoltre $L \subseteq \mathbb{C}$ e $\alpha \in \mathbb{R}$ (f ha una radice reale perché di grado dispari e a coefficienti reali). Se per assurdo $\mathrm{G}_{\mathbb{Q}}(f) = \mathrm{G}_{\mathbb{Q}}(L)$ fosse abeliano, il suo sottogruppo $\mathrm{G}_{\mathbb{Q}(\alpha)}(L)$ sarebbe normale, e dunque (sempre per il teorema fondamentale), l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ sarebbe normale. Pertanto $\mathrm{m}_{\alpha,\mathbb{Q}} = f$ si spezzerebbe su $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, il che è assurdo perché non tutte le radici di f sono reali. Infatti $f' = 5X^4 + 2X$ ha solo due radici reali (0 e $-\sqrt[3]{2/5}$), per cui f può avere al massimo 3 radici reali (si vede facilmente che in effetti ne ha una sola), mentre f ha 5 radici complesse distinte (essendo separabile su $\mathbb{Q}$).