Corso di Algebra 2 - a.a. 2018-2019
Prova scritta del 19/09/2019

1. Dato un anello A e due omomorfismi di A-moduli $f_i\colon M_i \to N$ (per $i = 1, 2$), sia $M := \{(x_1, x_2) \in M_1 \oplus M_2 \,:\, f_1(x_1) = f_2(x_2)\}$.
   (a) Dimostrare che M è un A-sottomodulo di $M_1 \oplus M_2$.
   (b) Dimostrare che $M = \{(0, 0)\}$ se e solo se f_1 e f_2 sono iniettivi e $\mathrm{im}(f_1) \cap \mathrm{im}(f_2) = \{0\}$.
   (c) Dimostrare che, se f_1 e f_2 sono non nulli e M_1 e M_2 sono semplici e non isomorfi, allora $M = \{(0, 0)\}$.
   (d) Dimostrare che, se f_1 e f_2 sono iniettivi, A è un dominio a ideali principali e M_1 è ciclico, allora anche M è ciclico.

2. Si dice che un sottogruppo H di un gruppo G è *autonormalizzante* se H coincide con il normalizzatore di H in G. Sia $n = p^k r$ con k e r interi positivi e p un numero primo che non divide r.
   (a) Dimostrare che, se esiste un gruppo di ordine n con un p-Sylow autonormalizzante, allora $r \equiv 1 \mod p$.
   (b) Dimostrare che, se r è un numero primo, allora ogni gruppo di ordine n con un r-Sylow autonormalizzante ha un unico p-Sylow.
   (c) Dimostrare che, se $r \equiv 1 \mod p$ è un numero primo, allora esiste un gruppo di ordine n con un p-Sylow autonormalizzante.
   (d) Esiste un gruppo di ordine n con un p-Sylow autonormalizzante se $p = 5$, $k = 2$ e $r = 91$?

3. Sia $K \subseteq L$ un'estensione di Galois con gruppo di Galois G e sia $\alpha \in L$. Siano inoltre $n = [K(\alpha) : K]$ e m_α il polinomio minimo di α su K.
   (a) Dato $\beta \in K(\alpha)$, dimostrare che esiste unico $p \in K[X]$ tale che $\beta = p(\alpha)$ e $p = 0$ o $\deg(p) < n$.
   (b) Con la notazione del punto precedente, dimostrare che, se $\beta \notin K$, allora $[K(\alpha) : K(\beta)] \leq \deg(p)$.
   (c) Dimostrare che, se G è semplice e $n > 1$, allora $K \subseteq L$ è un campo di spezzamento di m_α.
   (d) È vero che, se G è isomorfo a S_n, allora $K \subseteq L$ è un campo di spezzamento di m_α?

Soluzioni

1. (a) $(0,0) \in M$ perché $f_1(0) = 0 = f_2(0)$. Se $(x_1, x_2), (y_1, y_2) \in M$ (cioè $f_1(x_1) = f_2(x_2)$ e $f_1(y_1) = f_2(y_2)$), allora anche $(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2) \in M$ perché

$$f_1(x_1 + y_1) = f_1(x_1) + f_1(y_1) = f_2(x_2) + f_2(y_2) = f_2(x_2 + y_2).$$

Analogamente $a(x_1, x_2) = (ax_1, ax_2) \in M$ per ogni $a \in M$ perché

$$f_1(ax_1) = af_1(x_1) = af_2(x_2) = f_2(ax_2).$$

(b) Poniamo per brevità $N' := \mathrm{im}(f_1) \cap \mathrm{im}(f_2)$ e osserviamo che N' è un sottomodulo di N perché intersezione di sottomoduli. Supponiamo che $M = \{(0,0)\}$. Allora per ogni $x_1 \in M_1 \setminus \{0\}$ si ha $(x_1, 0) \notin M$, per cui $f_1(x_1) \neq f_2(0) = 0$, cioè $x_1 \notin \ker(f_1)$. Ciò dimostra che $\ker(f_1) = \{0\}$, quindi f_1 è iniettivo, e analogamente si dimostra che anche f_2 è iniettivo. Inoltre, dato $y \in N'$, esistono $x_i \in M_i$ (per $i = 1, 2$) tali che $y = f_i(x_i)$. In particolare $f_1(x_1) = f_2(x_2)$, cioè $(x_1, x_2) \in M = \{(0,0)\}$. Ne segue che $y = f_i(x_i) = f_i(0) = 0$, il che dimostra che $N' = \{0\}$. Viceversa, supponiamo che f_1 e f_2 siano iniettivi e che $N' = \{0\}$. Per ogni $(x_1, x_2) \in M$ si ha $f_1(x_1) = f_2(x_2) \in N' = \{0\}$, per cui $f_i(x_i) = 0$ (per $i = 1, 2$). Pertanto $x_i \in \ker(f_i) = \{0\}$, cioè $(x_1, x_2) = (0, 0)$.

(c) Per il lemma di Schur $f_i \colon M_i \to N$ è iniettivo perché $f_i \neq 0$ e M_i è semplice (per $i = 1, 2$). Dunque $\mathrm{im}(f_i) \cong M_i$ è pure semplice e $\mathrm{im}(f_1) \ncong \mathrm{im}(f_2)$ perché $M_1 \ncong M_2$. Tenendo conto che N' è un sottomodulo del modulo semplice $\mathrm{im}(f_i)$ deve essere allora $N' = \{0\}$, perché altrimenti $N' = \mathrm{im}(f_i)$ (per $i = 1, 2$), e quindi $\mathrm{im}(f_1) = \mathrm{im}(f_2)$, in contraddizione con $\mathrm{im}(f_1) \ncong \mathrm{im}(f_2)$. Per il punto precedente questo dimostra che $M = \{(0,0)\}$.

(d) È chiaro che in ogni caso la funzione $f \colon M \to N$, $(x_1, x_2) \mapsto f_1(x_1) = f_2(x_2)$ è A-lineare, $\mathrm{im}(f) = N'$ e $\ker(f) = \ker(f_1) \oplus \ker(f_2)$. In particolare f è iniettiva se lo sono f_1 e f_2, e dunque nel nostro caso $M \cong \mathrm{im}(f) = N'$. Poiché N' è un sottomodulo di $\mathrm{im}(f_1) \cong M_1$, per concludere che N' (e quindi $M \cong N'$) è ciclico basta osservare che (essendo A un dominio a ideali principali) un sottomodulo di un A-modulo ciclico è ciclico. In effetti, a meno di isomorfismo, ogni A-modulo ciclico è della forma A/I con I ideale di A e i sottomoduli di A/I sono tutti e soli della forma J/I con J ideale di A contenente I. Se a è un generatore di J, l'A-modulo J/I è ciclico, generato da $a + I$.

2. (a) Se G è un gruppo di ordine n con un p-Sylow autonormalizzante H, allora per il teorema di Sylow si ha (indicando con $N(H)$ il normalizzatore di H in G e con s_p il numero di p-Sylow di G)

$$s_p = [G : N(H)] = [G : H] = \frac{\#G}{\#H} = \frac{n}{p^k} = r$$

e $s_p \equiv 1 \mod p$, per cui $r \equiv 1 \mod p$.

(b) Se G è un gruppo di ordine n con un r-Sylow autonormalizzante, allora, analogamente al punto precedente, gli r-Sylow di G sono $\frac{n}{r} = p^k$. Poiché ogni r-Sylow ha ordine r primo (e quindi contiene $r-1$ elementi di ordine r), due r-Sylow distinti si interescano solo nell'elemento neutro. Ne segue che il sottoinsieme R degli elementi di ordine r di G verifica $\#R = p^k(r-1)$, e quindi $\#(G \setminus R) = \#G - \#R = n - p^k(r-1) = p^k$. Dato che ogni p-Sylow è contenuto in $G \setminus R$ (perché non contiene elementi di ordine r), G ha un solo p-Sylow, cioè proprio $G \setminus R$.

(c) Basta trovare un gruppo G di ordine n che non abbia un unico p-Sylow: in questo caso, infatti, si ha $s_p > 1$ e $s_p \mid r$ con r primo, per cui $s_p = r$; d'altra parte, se H è un p-Sylow di G, $[G : H] = r$ e $s_p = [G : N(H)]$, da cui si conclude (essendo in ogni caso $H \subseteq N(H)$) che $H = N(H)$. Ora, è noto che esiste un gruppo G' non abeliano di ordine pr (perché $r \equiv 1 \mod p$) e che G' non ha un unico p-Sylow. Indicando con H_1 e H_2 due p-Sylow distinti di G', è chiaro che $H_i \times C_{p^{k-1}}$ (per $i = 1, 2$) sono due p-Sylow distinti di $G := G' \times C_{p^{k-1}}$.

(d) No, non esiste. Per vederlo basta dimostrare che ogni gruppo G di ordine $n = 5^2 \cdot 7 \cdot 13$ è abeliano (e quindi l'unico suo sottogruppo autonormalizzante è G stesso). In effetti si ha $s_7 = 1$ (perché $s_7 \mid 5^2 \cdot 13$ e $s_7 \equiv 1 \mod 7$) e $s_{13} = 1$ (perché $s_{13} \mid 5^2 \cdot 7$ e $s_{13} \equiv 1 \mod 13$), per cui G ha un unico 7-Sylow H_7 e un unico 13-Sylow H_{13}. Essendo H_7 e H_{13} normali, anche $K := H_7 H_{13}$ è un sottogruppo normale di G; inoltre (poiché $H_7 \cap H_{13} = \{1\}$) $K \cong H_7 \times H_{13} \cong C_7 \times C_{13} \cong C_{91}$ per il teorema cinese del resto. Indicando con H_5 un 5-Sylow di G e tenendo conto che $K \cap H_5 = \{1\}$ (perché hanno ordini coprimi) e $KH_5 = G$ (perché $\#(KH_5) = \#G$), si ottiene $G = K \rtimes H_5$. Dunque $G \cong C_{91} \rtimes_\theta H_5$ per qualche omomorfismo $\theta \colon H_5 \to \mathrm{Aut}(C_{91}) \cong \mathbb{Z}/91\mathbb{Z}^*$. D'altra parte θ è banale perché $\#H_5 = 25$ e $\#\mathrm{Aut}(C_{91}) = \varphi(91) = \varphi(7)\varphi(13) = 6 \cdot 12 = 72$ sono coprimi. Se ne deduce che $G \cong C_{91} \times H_5$ è abeliano perché lo sono sia C_{91} che H_5 (quest'ultimo perché di ordine p^2).

3. (a) La funzione $\psi\colon K[X] \to L$, $f \mapsto f(\alpha)$ è un omomorfismo di anelli con immagine $K[\alpha]$. Poiché α è algebrico su K, si ha anche $K[\alpha] = K(\alpha)$ e $\ker(\psi) = (\mathrm{m}_\alpha)$. Dato $\beta \in K(\alpha)$, esiste dunque $f \in K[X]$ tale che $\beta = \psi(f) = f(\alpha)$; inoltre un altro $g \in K[X]$ soddisfa $\beta = g(\alpha)$ se e solo se $f - g \in \ker(\psi) = (\mathrm{m}_\alpha)$. Se ne deduce che $p \in K[X]$ ha le proprietà richieste se e solo se esiste $q \in K[X]$ tale che $f = q\mathrm{m}_\alpha + p$ e $p = 0$ o $\deg(p) < \deg(\mathrm{m}_\alpha) = n$, cioè se e solo se p è un resto della divisione di f per m_α. La tesi segue allora dall'esistenza e unicità della divisione con resto in $K[X]$.

(b) L'ipotesi $\beta \notin K$ implica che p non è costante, cioè $\deg(p) > 0$. Perciò $\tilde{p} := p - \beta \in K(\beta)[X]$ soddisfa $\deg(\tilde{p}) = \deg(p)$ e $\tilde{p}(\alpha) = p(\alpha) - \beta = 0$. Indicando con m'_α il polinomio minimo di α su $K(\beta)$, si conclude che

$$[K(\alpha) : K(\beta)] = [K(\beta)(\alpha) : K(\beta)] = \deg(\mathrm{m}'_\alpha) \leq \deg(\tilde{p}) = \deg(p).$$

(c) Poiché $K \subseteq L$ è un'estensione normale, m_α si spezza su L, e quindi esiste un campo di spezzamento $K \subseteq L'$ di m_α tale che $L' \subseteq L$. Inoltre $K \subseteq L'$ è un'estensione normale, per cui (per il teorema fondamentale della teoria di Galois) esiste un sottogruppo normale H di G tale che $L' = L^H$ (dove L^H indica il sottocampo di L lasciato fisso da tutti gli elementi di H). Tenendo conto che $K(\alpha) \subseteq L'$, si ha $[L' : K] \geq [K(\alpha) : K] = n > 1$, e pertanto $L^H = L' \neq K = L^G$. Questo implica $H \neq G$, e allora (essendo G semplice) deve essere $H = \{1\}$. Si conclude perciò che $L' = L^{\{1\}} = L$, cioè $K \subseteq L' = L$ è un campo di spezzamento di m_α.

(d) Sì, è vero. Infatti, ragionando come nel punto precedente, si trova che esiste un campo di spezzamento di m_α della forma $K \subseteq L^H$ per qualche sottogruppo normale H di G. Si può inoltre supporre $n > 1$ (se no $K = L$ e la tesi diventa ovvia), e allora, come prima, deve essere $H \neq G$ e per concludere basta dimostrare $H = \{1\}$. Va cioè escluso che H sia un sottogruppo normale non banale di G. Dato che S_2 non ha sottogruppi (normali) non banali, si può anche supporre $n > 2$. Allora H non può essere il sottogruppo di G corrispondente (attraverso l'isomorfismo $G \cong S_n$) a A_n, perché altrimenti si avrebbe $[L^H : K] = [G : H] = [S_n : A_n] = 2$, mentre (come si è visto in precedenza) $[L^H : K] \geq n > 2$. L'unica altra possibilità è $n = 4$ e H corrispondente al sottogruppo V_4 di S_4, ma in questo caso si avrebbe $[L^H : K] = [G : H] = [S_4 : V_4] = 6$, il che è impossibile perché (ricordando che $K(\alpha) \subseteq L^H$) si ha $4 = [K(\alpha) : K] \mid [L^H : K]$.