**Corso di Algebra 2 - a.a. 2018-2019**

*Prova scritta del 14/01/2020*

1. Siano $A$ un anello e $M$ un $A$-modulo. Per ogni $a \in A$ sia inoltre

$$M_a := \{x \in M \,:\, ax = 0\}.$$

   (a) Dimostrare che $M_a$ è un sottogruppo di $M$, e che è anche un $A$-sottomodulo se $A$ è commutativo.

   (b) Dimostrare che, se $I$ è un ideale sinistro ma non destro di $A$ e $M = A/I$, allora esiste $a \in A$ tale che $M_a$ non è un $A$-sottomodulo di $M$.

   (c) Dimostrare che, se $A$ è un dominio e $M$ è di torsione e finitamente generato, allora esiste $a \in A \setminus \{0\}$ tale che $M_a = M$.

   (d) Dimostrare che, se $A = \mathbb{Z}$ e $M$ è finitamente generato, allora esiste un intero $a > 1$ tale che $M_a = \{0\}$.

2. Sia $n$ un intero positivo. In ciascuno dei seguenti casi stabilire se è vero che ogni gruppo di ordine $n$ contiene un sottogruppo di ordine $d$ per ogni divisore positivo $d$ di $n$.

   (a) $n < 12$.

   (b) $n = 60$.

   (c) $n = 63$.

   (d) $n = 66$.

3. Per ogni intero $a$ si consideri il polinomio $f_a = X^4 + X^3 + X^2 + aX + 1$ e per ogni campo $K$ sia $\mathrm{Gal}_K(f_a)$ il gruppo di Galois di $f_a$ su $K$.

   (a) Trovare un numero primo $p$ tale che $\mathrm{Gal}_{\mathbb{F}_p}(f_1) = \{1\}$.

   (b) Dimostrare che $\mathrm{Gal}_{\mathbb{Q}}(f_1) \cong \mathrm{Gal}_{\mathbb{F}_2}(f_1)$.

   (c) Dimostrare che non esiste un numero primo $p$ tale che $\mathrm{Gal}_{\mathbb{Q}}(f_2) \cong \mathrm{Gal}_{\mathbb{F}_p}(f_2)$.

   (d) Esiste un numero primo $p$ tale che $\mathrm{Gal}_{\mathbb{Q}}(f_3) \cong \mathrm{Gal}_{\mathbb{F}_p}(f_3)$?

*Soluzioni*

1. (a) $0 \in M_a$ perché $a0 = 0$. Se $x, y \in M_a$ (cioè $ax = ay = 0$), allora anche $x - y \in M_a$, dato che $a(x - y) = ax - ay = 0 - 0 = 0$. Ciò dimostra che $M_a$ è un sottogruppo di $M$. Se $A$ è commutativo, $x \in M_a$ e $b \in A$, allora anche $bx \in M_a$ perché $abx = bax = b0 = 0$. Dunque $M_a$ è anche un $A$-sottomodulo di $M$ se $A$ è commutativo.

   (b) Per ipotesi esitono $a \in I$ e $b \in A$ tali che $ab \notin I$. Ponendo $\overline{c} := c + I \in M = A/I$ per ogni $c \in A$, si ha $\overline{1} \in M_a$ perché $a\overline{1} = \overline{a} = \overline{0}$ (l'ultima uguaglianza segue dal fatto che $a \in I$). D'altra parte $b\overline{1} = \overline{b} \notin M_a$ (il che dimostra che $M_a$ non è un $A$-sottomodulo di $M$) perché $a\overline{b} = \overline{ab} \neq \overline{0}$ (la disuguaglianza segue dal fatto che $ab \notin I$).

   (c) Per ipotesi esiste un insieme finito $\{x_1, \ldots, x_n\}$ di generatori di $M$ come $A$-modulo; inoltre per ogni $i = 1, \ldots, n$ esiste $a_i \in A \setminus \{0\}$ tale che $a_i x_i = 0$. Allora $a := a_1 \cdots a_n \in A \setminus \{0\}$ (perché $A$ è un dominio) soddisfa $x_1, \ldots, x_n \in M_a$. Infatti per ogni $i = 1, \ldots, n$ si ha (tenendo conto che $A$ è commutativo) $a = a_i' a_i$ con $a_i' := a_1 \cdots a_{i-1} a_{i+1} \cdots a_n$, per cui $ax_i = a_i' a_i x_i = a_i' 0 = 0$. Essendo $M_a$ un $A$-sottomodulo di $M$ per il primo punto, si conclude che $M_a \supseteq \langle x_1 \cdots x_n \rangle_A = M$, cioè $M_a = M$.

   (d) Per ogni numero primo $p$ si ha chiaramente

   $$M_p \subseteq \mathrm{T}_p(M) := \{x \in M \,:\, p^m x = 0 \text{ per qualche } m \in \mathbb{N}\}.$$

   Poiché $M$ è finitamente generato, l'insieme dei numeri primi $p$ tali che $\mathrm{T}_p(M) \neq \{0\}$ è finito; perciò (tenendo conto che i numeri primi sono infiniti) esiste un numero primo $a$ tale che $\mathrm{T}_a(M) = 0$, e quindi $M_a = \{0\}$.

2. Osserviamo preliminarmente che, dato un divisore positivo $d$ di $n$, un gruppo di ordine $n$ contiene sicuramente un sottogruppo di ordine $d$ se $d = n$ (il gruppo stesso è un tale sottogruppo) o se $d$ è una potenza di un numero primo (per il teorema di Sylow).

   (a) È vero. Infatti $n$ è della forma $pq$ con $p$ e $q$ primi distinti (se $n = 6$ o $n = 10$) o $p^k$ con $p$ primo e $k \in \mathbb{N}$ (per tutti gli altri valori di $n$). Tenendo conto che i divisori positivi di $n$ sono 1, $p$, $q$ e $pq = n$ nel primo caso e $p^h$ con $0 \leq h \leq k$ nel secondo, l'affermazione segue allora da quanto detto all'inizio.

(b) Non è vero. Per esempio $A_5$ ha ordine 60 e non contiene un sottogruppo di ordine 30: se esistesse, un tale sottogruppo sarebbe normale (in quanto di indice 2), il che è impossibile perché $A_5$ è semplice.

(c) È vero. Sia infatti $G$ un gruppo di ordine $63 = 3^2 \cdot 7$: per quanto detto all'inizio basta dimostrare che $G$ contiene un sottogruppo di ordine $3 \cdot 7 = 21$. Per il teorema di Sylow $G$ ha un unico 7-Sylow $K$ (dato che il numero di 7-Sylow è $\equiv 1 \mod 7$ e divide $3^2 = 9$), che è quindi normale in $G$ e di ordine 7. Indicando con $H$ un sottogruppo di $G$ di ordine 3 (che esiste sempre per il teorema di Sylow), si ha $H \cap K = \{1\}$ (perché $H$ e $K$ hanno ordini coprimi), quindi $HK = KH$ è un sottogruppo di $G$ di ordine $(\#H)(\#K) = 3 \cdot 7 = 21$.

(d) È vero. Dato un gruppo $G$ di ordine $66 = 2 \cdot 3 \cdot 11$, sempre per quanto detto all'inizio basta dimostrare che $G$ contiene sottogruppi di ordini $2 \cdot 3 = 6$, $2 \cdot 11 = 22$ e $3 \cdot 11 = 33$. Indicando con $H_p$ un $p$-Sylow e con $s_p$ il numero di $p$-Sylow di $G$ (per $p = 2, 3, 11$), per il teorema di Sylow $s_{11} = 1$ (perché $s_{11} \equiv 1 \mod 11$ e $s_{11} \mid 6$), per cui $H_{11}$ è normale in $G$. Ragionando come nel punto precedente, $H_2H_{11}$ e $H_3H_{11}$ sono sottogruppi di $G$ di ordini $2 \cdot 11 = 22$ e $3 \cdot 11 = 33$; se inoltre $H_2$ o $H_3$ è normale in $G$, $H_2H_3$ è un sottogruppo di $G$ di ordine $2 \cdot 3 = 6$. Resta dunque da dimostrare che $G$ contiene un sottogruppo di ordine 6 quando né $H_2$ né $H_3$ è normale in $G$, cioè quando $s_2, s_3 > 1$. In questo caso, poiché $s_3 \equiv 1 \mod 3$ e $s_3 \mid 22$, deve essere $s_3 = 22$. Indicando con $S$ l'insieme degli elementi di ordine 3 di $G$ (cioè gli elementi non banali dei 3-Sylow), ne segue che $\#S = 22 \cdot 2 = 44$ (perché ogni 3-Sylow contiene 2 elementi di ordine 3 e l'intersezione di due 3-Sylow distinti è $\{1\}$). Poiché $G' := H_2H_{11} \subseteq G \setminus S$ (per il teorema di Lagrange $G'$ non contiene elementi di ordine 3) e $\#G' = \#(G \setminus S) = 22$, si ha $G' = G \setminus S$. D'altra parte ogni 2-Sylow di $G$ (non contenendo elementi di ordine 3) è anche un 2-Sylow di $G' = G \setminus S$, per cui $s_2$ coincide con il numero $s_2'$ di 2-Sylow di $G'$. Da $s_2' \mid 11$ si ottiene allora $s_2 = s_2' = 11$, e pertanto il normalizzatore di $H_2$ in $G$ è un sottogruppo di $G$ di indice 11, cioè di ordine 6.

3. (a) Si può prendere $p = 5$. Infatti $f_1 = (X^5 - 1)/(X - 1)$ in $K[X]$ per ogni campo $K$ e $X^5 - 1 = (X - 1)^5$ in $\mathbb{F}_5[X]$, per cui $f_1 = (X - 1)^4$ si spezza su $\mathbb{F}_5$, e pertanto $\mathrm{Gal}_{\mathbb{F}_5}(f_1) = \{1\}$.

(b) $f_1$ è un polinomio di quarto grado 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 irriducibile di secondo grado in $\mathbb{F}_2[X]$. Ne segue che $\mathbb{F}_2 \subset \mathbb{F}_{2^4}$ è un campo di spezzamento di $f_1$ su $\mathbb{F}_2$ e che $\mathrm{Gal}_{\mathbb{F}_2}(f_1) \cong C_4$. D'altra parte $f_1 = \phi_5$ è il quinto polinomio ciclotomico, ed è noto che $\mathrm{Gal}_{\mathbb{Q}}(\phi_5) \cong \mathbb{Z}/5\mathbb{Z}^* \cong C_4$.

(c) $f_2 = (X + 1)g$ con $g = X^3 + X + 1$, per cui $\mathrm{Gal}_K(f_2) \cong \mathrm{Gal}_K(g)$ per ogni campo $K$. Poiché $g$ è un polinomio di terzo grado senza radici razionali (una tale eventuale radice dovrebbe valere 1 o $-1$, ma $g(1) = 3 \neq 0 \neq -1 = g(-1)$), $g$ è irriducibile in $\mathbb{Q}[X]$. A priori il gruppo di Galois di un tale polinomio su $\mathbb{Q}$ può essere isomorfo solo a $A_3$ o a $S_3$, e per concludere basta dimostrare che $\mathrm{Gal}_{\mathbb{Q}}(g) \cong S_3$, dato che $S_3$ non è ciclico, mentre $\mathrm{Gal}_{\mathbb{F}_p}(g)$ è ciclico (di ordine $\leq 3$) per ogni primo $p$. Il fatto che il discriminante di $g$ sia $-4 \cdot 1^3 - 27 \cdot 1^2 = -31$, che non è un quadrato in $\mathbb{Q}$, implica che $\mathrm{Gal}_{\mathbb{Q}}(g) \cong S_3$. In alternativa alla stessa conclusione si può arrivare facilmente osservando che $g$ ha una sola radice reale $\alpha$ (perché $g$ ha grado dispari e, come funzione $\mathbb{R} \to \mathbb{R}$, è strettamente crescente, dato che $g' = 3X^2 + 1 \geq 1$). Indicando con $\mathbb{Q} \subset L$ il campo di spezzamento di $g$ su $\mathbb{Q}$ contenuto in $\mathbb{C}$, da questo segue che $\mathbb{Q}(\alpha) \subsetneq L$, per cui $\#\mathrm{Gal}_{\mathbb{Q}}(g) = [L : \mathbb{Q}] > [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(g) = 3$.

(d) No, non esiste. Infatti $\mathrm{Gal}_{\mathbb{F}_p}(f_3)$ è ciclico (di ordine $\leq 4$) per ogni primo $p$, per cui basta dimostrare che $\mathrm{Gal}_{\mathbb{Q}}(f_3)$ non è ciclico. In effetti $f_3$ è irriducibile in $\mathbb{Z}[X]$ e quindi in $\mathbb{Q}[X]$, dato che lo è in $\mathbb{F}_2[X]$, come si è visto nel secondo punto ($f_3$ coincide con $f_1$ in $\mathbb{F}_2[X]$). È inoltre facile vedere che $f_3$ ha esattamente due radici reali, dato che $f_3' = 4X^3 + 3X^2 + 2X + 3 = (X + 1)(4X^2 - X + 3)$ ha come unica radice reale $-1$ e $f_3(-1) = -1 < 0$. Indicando con $\mathbb{Q} \subset L$ il campo di spezzamento di $f_3$ su $\mathbb{Q}$ contenuto in $\mathbb{C}$ e con $\alpha$ una radice reale di $f_3$, si ha dunque $\mathbb{Q}(\alpha) \subsetneq L$, per cui $\#\mathrm{Gal}_{\mathbb{Q}}(f_3) = [L : \mathbb{Q}] > [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f_3) = 4$. Da questo si deduce che $\mathrm{Gal}_{\mathbb{Q}}(f_3)$ non è cicliclo, dato che è isomorfo a un sottogruppo di $S_4$, e $S_4$ non contiene sottogruppi ciclici di ordine $> 4$.