Corso di Algebra 2 - a.a. 2020-2021

Prova scritta del 17/01/2022

1. Siano A un anello commutativo, M un A-modulo e $a \in A$.
   (a) Dimostrare che $aM := \{ax : x \in M\}$ è un sottomodulo di M.
   (b) Dimostrare che, se A è un dominio, M è senza torsione e $a \neq 0$, allora $aM \cong M$.
   (c) Dimostrare che, se A è un dominio a ideali principali, M è finitamente generato e indecomponibile e $aM \ncong M$, allora esiste $n > 0$ tale che $a^n M = \{0\}$.

2. Sia G un gruppo di ordine p^3q con p e q numeri primi distinti. Siano inoltre s_p e s_q il numero, rispettivamente, di p-Sylow e di q-Sylow di G.
   (a) Dimostrare che, se $s_q = p$, allora $s_p = 1$.
   (b) Dimostrare che, se $s_q = p^3$, allora $s_p = 1$.
   (c) Dimostrare che G non è semplice.

3. Sia $f := X^3 - 4X + 2$.
   (a) Determinare la più piccola potenza q di un numero primo tale che $\mathrm{G}_{\mathbb{F}_q}(f) \cong C_2$.
   (b) Trovare un campo K tale che $\mathrm{G}_K(f) \cong S_3$.
   (c) Esiste un numero primo p tale che $\mathrm{G}_{\mathbb{Q}(\sqrt{p})}(f) \cong \mathrm{G}_{\mathbb{F}_p}(f)$?

Soluzioni

1. (a) Dato che $aM = \mathrm{im}(f)$, dove $f\colon M \to M$ indica la funzione definita da $f(x) := ax$, basta dimostrare che f è A-lineare. In effetti per ogni $x, x' \in M$ e per ogni $b \in A$ si ha $f(x + x') = a(x + x') = ax + ax' = f(x) + f(x')$ e $f(bx) = a(bx) = b(ax) = bf(x)$.

   (b) Con la notazione del punto precedente, si ha $\ker(f) = \{0\}$ perché $a \neq 0$ e M è senza torsione. Dunque f induce un isomorfismo di A-moduli tra M e $\mathrm{im}(f) = aM$.

   (c) Chiaramente si può supporre $a \neq 0$, quindi per il punto precedente M non può essere senza torsione, e in particolare $M \ncong A$. Dalla classificazione dei moduli finitamente generati e indecomponibili su un dominio a ideali principali segue che A non è un campo ed esistono un ideale massimale $P = (p)$ di A e $n > 0$ tali che $M \cong A/P^n$. Per concludere basta dimostrare che $a \in P$, perché allora $a^n \in P^n = \mathrm{Ann}(M)$, cioè $a^n M = \{0\}$. Per assurdo sia $a \notin P$, cioè $p \nmid a$ in A. Poiché p è irriducibile, si ha $\mathrm{mcd}(a, p^n) = 1$, per cui esistono $b, c \in A$ tali che $1 = ba + cp^n$. Tenendo conto che $cp^n \in P^n = \mathrm{Ann}(M)$, si ottiene

   $$x = (ba + cp^n)x = bax + cp^n x = abx \in aM$$

   per ogni $x \in M$, il che dimostra $aM = M$, contraddicendo l'ipotesi $aM \ncong M$.

2. Per il teorema di Sylow $s_p \mid q$ e $s_p \equiv 1 \mod p$, quindi $s_p = 1$ o $s_p = q$, e quest'ultimo caso è possibile solo se $q \equiv 1 \mod p$. Analogamente $s_q \mid p^3$ e $s_q \equiv 1 \mod q$, quindi $s_q = p^i$ con $0 \leq i \leq 3$ tale che $p^i \equiv 1 \mod q$.

   (a) Per quanto detto sopra si ha $s_q = p \equiv 1 \mod q$. Pertanto $p > q$, il che chiaramente implica $q \not\equiv 1 \mod p$, e allora $s_p = 1$.

   (b) Avendo ordine q primo, ogni q-Sylow contiene $q - 1$ elementi di ordine q, e due q-Sylow distinti si intersecano solo nell'elemento neutro. Ne segue che l'insieme T degli elementi di ordine q è tale che $\#T = s_q(q - 1) = p^3(q - 1)$, e dunque $\#(G \setminus T) = \#G - \#T = p^3 q - p^3(q - 1) = p^3$. Poiché ogni p-Sylow ha ordine p^3 ed è contenuto in $G \setminus T$, si conclude che $G \setminus T$ è l'unico p-Sylow, e in particolare $s_p = 1$.

(c) Naturalmente G non è semplice se $s_p = 1$ o $s_q = 1$, perché in tal caso il p-Sylow o il q-Sylow è normale. Per quanto già dimostrato si può quindi supporre $s_p = q$ e $s_q = p^2$; inoltre deve essere $q \equiv 1 \mod p$ e $p^2 \equiv 1 \mod q$. Se ne deduce che $q > p$ e $q \mid (p^2 - 1) = (p-1)(p+1)$, il che implica $q \mid (p-1)$ o $q \mid (p+1)$ (perché q è primo). Non può essere $q \mid (p-1)$ (altrimenti si avrebbe $p < q \leq p-1$), quindi $q \mid (p+1)$, da cui si ottiene $p < q \leq p+1$, e dunque $q = p+1$. Pertanto $p = 2$ e $q = 3$, cioè $\#G = 24$. In tal caso G non è semplice perché, indicando con H un 2-Sylow, esiste un omomorfismo $f\colon G \to S(G/H)$ tale che $\ker(f) \subseteq H$. Avendo $S(G/H) \cong S_3$ ordine $6 < 24$, f non è iniettivo, e allora $\ker(f)$ è un sottogruppo normale non banale di G.

3. (a) Il valore cercato è $q = 5$. Infatti $f = X^3$ in $\mathbb{F}_2[X]$, per cui f si spezza su $\mathbb{F}_2$ e $\mathrm{G}_{\mathbb{F}_2}(f) \cong C_1$; naturalmente lo stesso vale per l'estensione $\mathbb{F}_4$ di $\mathbb{F}_2$. Inoltre $f = X^3 - X + 2$ in $\mathbb{F}_3[X]$, e si verifica subito che f non ha radici in $\mathbb{F}_3$; dunque f è irriducibile (avendo grado 3) e $\mathrm{G}_{\mathbb{F}_3}(f) \cong C_3$. D'altra parte $f = X^3 + X + 2$ in $\mathbb{F}_5[X]$; si trova che -1 è l'unica radice di f in $\mathbb{F}_5$ e che $f = (X+1)(X^2 - X + 2)$ con $X^2 - X + 2$ irriducibile (perché senza radici in $\mathbb{F}_5$ e di grado 2). Ciò implica $\mathrm{G}_{\mathbb{F}_5}(f) \cong C_2$.

(b) Si può prendere $K = \mathbb{Q}$. Infatti f è irriducibile in $\mathbb{Z}[X]$ e quindi in $\mathbb{Q}[X]$, per esempio perché monico e irriducibile in $\mathbb{F}_3[X]$, come già visto. Inoltre $\Delta(f) = -4(-4)^3 - 27 \cdot 2^2 = 148 = 2^2 \cdot 37$ non è un quadrato in $\mathbb{Q}$, per cui $\mathrm{G}_{\mathbb{Q}}(f) \cong S_3$.

(c) No, non esiste. Infatti per ogni radice complessa α di f si ha $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 3$ (dato che f è irriducibile in $\mathbb{Q}[X]$). Allora per ogni primo p si ha $\alpha \notin \mathbb{Q}(\sqrt{p})$ (altrimenti si otterrebbe $3 = [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$), e dunque f è irriducibile in $\mathbb{Q}(\sqrt{p})[X]$ (perché di terzo grado e senza radici). Inoltre $\mathrm{G}_{\mathbb{Q}(\sqrt{p})}(f) \cong C_3$ se $\Delta(f) = 2^2 \cdot 37$ è un quadrato (se e solo se 37 lo è) in $\mathbb{Q}(\sqrt{p})$, e $\mathrm{G}_{\mathbb{Q}(\sqrt{p})}(f) \cong S_3$ altrimenti. Ora, 37 è un quadrato in $\mathbb{Q}(\sqrt{p})$ se e solo se $p = 37$: l'altra implicazione essendo ovvia, sia p primo tale che $37 = \gamma^2$ per qualche $\gamma = a + b\sqrt{p} \in \mathbb{Q}(\sqrt{p})$ (con $a, b \in \mathbb{Q}$); da $37 = a^2 + 2ab\sqrt{p} + b^2 p$ segue $a^2 + b^2 p = 37$ e $2ab = 0$, e si deduce facilmente che deve essere $a = 0$, $b = \pm 1$ e $p = 37$. Tenendo conto che S_3 non è ciclico, mentre $\mathrm{G}_{\mathbb{F}_p}(f)$ è ciclico e ha ordine 3 se e solo se f è irriducibile in $\mathbb{F}_p[X]$, per concludere basta allora dimostrare che f non è irriducibile in $\mathbb{F}_{37}[X]$. In effetti, se lo fosse, sarebbe anche separabile (essendo $\mathbb{F}_{37}$ perfetto), contraddicendo il fatto che $\Delta(f) = 0$ in $\mathbb{F}_{37}$.