Corso di Algebra 2 - a.a. 2020-2021
Prova scritta del 07/02/2022

1. Siano A un anello e M un A-modulo.
   (a) Dimostrare che, se A è un campo e $M \neq \{0\}$, allora M contiene un sottomodulo semplice.
   (b) Dimostrare che, se A è un dominio ma non un campo e M è semplice, allora M è di torsione.
   (c) Dimostrare che, se A è un dominio a ideali principali ma non un campo e M è finitamente generato, allora M contiene un sottomodulo semplice se e solo se M non è libero.

2. Sia G un gruppo semplice di ordine 168.
   (a) Determinare il numero di 7-Sylow di G.
   (b) Dimostrare che G non contiene sottogruppi di indice n per $1 < n < 7$.
   (c) Dimostrare che G contiene un sottogruppo non abeliano di indice 8.

3. Per ogni intero a sia $f_a := X^4 - aX^3 + aX^2 + 2aX - 3$.
   (a) Trovare un numero primo p e un intero a tali che $\mathrm{G}_{\mathbb{F}_p}(f_a) \cong C_2$.
   (b) Trovare un intero a tale che $\mathrm{G}_{\mathbb{Q}}(f_a) \cong D_4$
   (c) Dimostrare che $\mathrm{G}_{\mathbb{Q}}(f_a) \cong D_3$ se e solo se $a = 1$.

1. (a) Preso $0 \neq x \in M$, $M' := \langle x \rangle_A$ è un A-sottomodulo (cioè sottospazio vettoriale) di M di dimensione 1. Dunque $M' \cong A$ è un A-modulo semplice (i soli sottomoduli, cioè ideali, di A sono quelli banali perché A è un campo).

   (b) Essendo M un A-modulo semplice, esiste un ideale (sinistro, ma in effetti bilatero, dato che A è commutativo) massimale I di A tale che $M \cong A/I$. Inoltre $\{0\}$ non è un ideale massimale di A perché A non è un campo, dunque $I \neq \{0\}$. Allora M è di torsione perché lo è A/I, dato che, preso $0 \neq b \in I$, si ha $b(a+I) = ba + I = I$ per ogni $a \in A$.

   (c) Se M contiene un sottomodulo semplice M', allora M' è di torsione per il punto precedente. Ne segue che M non è libero, perché se lo fosse sarebbe senza torsione, e quindi anche M' lo sarebbe.

   Viceversa, se M non è libero, allora $\mathrm{T}(M) \neq \{0\}$ (dato che in ogni caso esiste un A-modulo libero di rango finito L tale che $M = \mathrm{T}(M) \oplus L$). Per il teorema di struttura dei moduli finitamente generati su un dominio a ideali principali esistono allora un ideale massimale P di A e $n > 0$ tali che $\mathrm{T}(M)$ (e quindi M) contiene un sottomodulo isomorfo a A/P^n. Per concludere basta allora osservare che P^{n-1}/P^n è un sottomodulo di A/P^n isomorfo a A/P, e pertanto semplice.

2. Sia S_p il numero di p Sylow di G per ogni primo p che divide $168 = 2^3 \cdot 3 \cdot 7$.

   (a) Per il teorema di Sylow $s_7 \equiv 1 \mod 7$ e $s_7 \mid 2^3 \cdot 3 = 24$. Tenendo conto che $s_7 \neq 1$ (altrimenti il 7-Sylow sarebbe normale in G, contro l'ipotesi che G sia semplice), deve essere $s_7 = 8$.

   (b) Sia H un sottogruppo di G di indice $n > 1$. L'azione di G su G/H data dalla moltiplicazione a sinistra induce un omomorfismo $f\colon G \to S(G/H) \cong S_n$ tale che $\ker(f) \subseteq H \subsetneq G$. Essendo $\ker(f)$ normale in G e G semplice, deve essere $\ker(f) = \{1\}$, cioè f è iniettivo, e quindi S_n contiene un sottogruppo isomorfo a G. Se ne deduce (per il teorema di Lagrange) che $7 \mid 168 = \#G \mid \#S_n = n!$, il che implica (essendo 7 primo) che $7 \mid m$ per qualche $0 < m \leq n$. Si conclude allora che $n \geq m \geq 7$.

(c) Sia H il normalizzatore di un 7-Sylow di G: per il teorema di Sylow e per il primo punto si ha $[G : H] = s_7 = 8$, e resta da dimostrare che H non è abeliano. Supponendo per assurdo che H sia abeliano e osservando che $\#H = \#G/[G : H] = 168/8 = 21$, sia K un 3-Sylow di H (e quindi di G). Dato che K è normale in H, si ha $H < N(K)$, e quindi $s_3 = [G : N(K)] \mid [G : H] = 8$. Tenendo conto che $s_3 \equiv 1 \mod 3$, dovrebbe essere $s_3 = 1$ o $s_3 = 4$, ma il primo caso è impossibile perché K non è normale in G e il secondo per il punto precedente.

3. (a) Si può prendere per esempio $p = 3$ e $a = 1$: infatti in $\mathbb{F}_3[X]$ si ha $f_1 = X^4 - X^3 + X^2 - X = X(X - 1)(X^2 + 1)$ con $X^2 + 1$ irriducibile (perché di secondo grado e senza radici in $\mathbb{F}_3$).

(b) Si può prendere $a = 0$: infatti $f_0 = X^4 - 3$ è irriducibile in $\mathbb{Z}[X]$, e quindi in $\mathbb{Q}[X]$, per il criterio di Eisenstein relativo al primo 3. Inoltre le radici complesse di f_0 sono $\pm\sqrt[4]{3}, \pm\sqrt[4]{3}i$, per cui il campo di spezzamento (contenuto in $\mathbb{C}$) di f_0 su $\mathbb{Q}$ è $L := \mathbb{Q}(\pm\sqrt[4]{3}, \pm\sqrt[4]{3}i) = \mathbb{Q}(\sqrt[4]{3}, i)$. Poiché f_0 e $X^2 + 1$ sono i polinomi minimi di $\sqrt[4]{3}$ e di i su $\mathbb{Q}$, si ha $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = \deg(f_0) = 4$ e $[\mathbb{Q}(i) : \mathbb{Q}] = \deg(X^2+1) = 2$, dunque $4 = \mathrm{mcm}(4, 2) \mid [L : \mathbb{Q}] \leq 8$. Dato che $i \notin \mathbb{Q}(\sqrt[4]{3}) \subseteq \mathbb{R}$, si ottiene $[L : \mathbb{Q}] = 8$ e, tenendo conto che l'estensione $\mathbb{Q} \subseteq L$ è di Galois (è normale perché campo di spezzamento di un polinomio ed è separabile perché $\mathrm{char}(\mathbb{Q}) = 0$), $\mathrm{G}_{\mathbb{Q}}(f_0) = \mathrm{G}_{\mathbb{Q}}(L)$ ha pure ordine 8. Per concludere basta osservare che l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{3})$ non è normale (f_0 ha una radice ma non si spezza su $\mathbb{Q}(\sqrt[4]{3})$), quindi (per il teorema fondamentale della teoria di Galois) $\mathrm{G}_{\mathbb{Q}}(f_0)$ contiene un sottogruppo non normale, e D_4 è l'unico gruppo di ordine 8 (a meno di isomorfismo) che contiene un sottogruppo non normale.

(c) $f_1 = X^4 - X^3 + X^2 + 2X - 3 = (X - 1)g$ con $g := X^3 + X + 3$ irriducibile in $\mathbb{Q}[X]$ (perché di terzo grado e senza radici razionali). Poiché inoltre $\Delta(g) = -4 \cdot 1^3 - 27 \cdot 3^2 < 0$ non è un quadrato in $\mathbb{Q}$, si ottiene $\mathrm{G}_{\mathbb{Q}}(f_0) = \mathrm{G}_{\mathbb{Q}}(g) \cong S_3 \cong D_3$.

Viceversa, se $G := \mathrm{G}_{\mathbb{Q}}(f_a) \cong D_3$, allora f_a non può essere irriducibile (nel qual caso $4 = \deg(f_a) \mid \#G$) né prodotto di due fattori irriducibili di secondo grado (nel qual caso $\#G = 2$ o 4) in $\mathbb{Q}[X]$. Dunque f_a ha una radice razionale, che può essere solo $\pm 1, \pm 3$. D'altra parte $f_a(1) = 2a - 2 = 0$ se e solo se $a = 1$, mentre non esiste $a \in \mathbb{Z}$ tale che $f_a(-1) = -2$, $f_a(3) = 78 - 12a$ o $f_a(-3) = 78 + 30a$ sia 0.