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

Prova scritta del 26/06/2019

1. Sia A un anello e, dati $x, y \in A$, sia $M := \{(a, b) \in A^2 : ax = by\}$.
   (a) Dimostrare che M è un A-sottomodulo di A^2.
   (b) Dimostrare che, se A è un dominio, allora M e A^2/M sono A-moduli senza torsione.
   (c) Dimostrare che, se A è un dominio a ideali principali e $(x, y) \neq (0, 0)$, allora M e A^2/M sono A-moduli liberi di rango 1.
   (d) Stabilire se A^2/M è un A-modulo libero nel caso in cui $A = K[X, Y]$ (con K un campo), $x = X$ e $y = Y$.

2. Sia n un intero positivo e sia G un gruppo di ordine $35n$.
   (a) Dimostrare che, se $n = 5$ o $n = 7$, allora G è abeliano.
   (b) Fornire un esempio in cui G non è abeliano per $n = 2$ e per $n = 3$.
   (c) Dimostrare che, se $n = 4$, allora G è risolubile.
   (d) Fornire un esempio in cui G non è risolubile per $n = 12$.

3. Sia p un numero primo e siano $\alpha_p, \beta_p \in \mathbb{C}$ radici, rispettivamente, di $X^2 + p$ e di $X^3 - p$; sia inoltre $f_p = (X^2 + p)(X^3 - p)$.
   (a) Dimostrare che l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\beta_p)$ non è normale.
   (b) Dimostrare che il gruppo di Galois di f_3 su $\mathbb{Q}$ è isomorfo a D_3.
   (c) Dimostrare che l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_p, \beta_p)$ è un campo di spezzamento di f_p su $\mathbb{Q}$ se e solo se $p = 3$.
   (d) Dimostrare che per $p \neq 3$ il gruppo di Galois di f_p su $\mathbb{Q}$ è isomorfo a D_6.

Soluzioni

1. (a) Chiaramente $(0,0) \in M$. Se $(a,b),(a',b') \in M$ (cioè $ax = by$ e $a'x = b'y$), allora $(a,b)+(a',b') = (a+a', b+b') \in M$ perché

$$(a+a')x = ax + a'x = by + b'y = (b+b')y.$$

Se poi $(a,b) \in M$ e $c \in A$, allora $c(a,b) = (ca, cb) \in M$ perché

$$(ca)x = c(ax) = c(by) = (cb)y.$$

   (b) M è senza torsione perché sottomodulo di A^2, che è libero e quindi senza torsione. Inoltre $M = \ker(f)$, dove $f\colon A^2 \to A$ indica la funzione A-lineare definita da $(a,b) \mapsto ax - by$. Se ne deduce che $A^2/M \cong \mathrm{im}(f)$ (per il primo teorema di isomorfismo per moduli) è senza torsione, dato che $\mathrm{im}(f)$ è un sottomodulo del modulo libero e quindi senza torsione A.

   (c) Tenendo conto che su un dominio a ideali principali un sottomodulo di un modulo libero di rango n è libero di rango $\leq n$, per quanto visto nel punto precedente M (essendo un sottomodulo di A^2) è libero di rango $i \leq 2$ e A^2/M (essendo isomorfo a un sottomodulo di A) è libero di rango $j \leq 1$. Inoltre M è un addendo diretto di A^2 (perché A^2/M è libero), e da ciò segue che

$$A^2 \cong M \oplus A^2/M \cong A^i \oplus A^j \cong A^{i+j},$$

per cui $i+j = 2$. D'altra parte $A^2/M \cong \mathrm{im}(f) = Ax + Ay \neq \{0\}$ perché $(x,y) \neq (0,0)$; pertanto $j > 0$, e quindi $i = j = 1$.

   (d) $A^2/M \cong \mathrm{im}(f)$ non è libero perché $\mathrm{im}(f) = (X,Y)$ è un ideale non principale del dominio $K[X,Y]$, e un ideale in un dominio è un modulo libero se e solo se è un ideale principale.

2. Per ogni numero primo p (che divida $35n$) indichiamo con s_p il numero di p-Sylow di G; ricordiamo che per il teorema di Sylow, se l'ordine di un p-Sylow è p^k, allora $s_p \mid \frac{35n}{p^k}$ e $s_p \equiv 1 \mod p$.

   (a) In entrambi i casi $s_5 = 1$ (perché $s_5 \mid 49$ e $s_5 \equiv 1 \mod 5$) e $s_7 = 1$ (perché $s_7 \mid 25$ e $s_7 \equiv 1 \mod 7$). Dunque G ha un unico 5-Sylow H e un unico 7-Sylow K, e pertanto $G \cong H \times K$. Per concludere basta osservare che sia H che K sono abeliani, perché hanno ordine 25 e 7 (se $n = 5$) o 5 e 49 (se $n = 7$), cioè un numero primo o il quadrato di un numero primo.

(b) Se $n = 2$ si può prendere $G = D_{35}$. Se $n = 3$ esiste G' non abeliano di ordine 21 (perché $21 = 3 \cdot 7$ con 3 e 7 numeri primi tali che $7 \not\equiv 1 \mod 3$) e si può prendere $G = C_5 \times G'$.

(c) $s_7 = 1$ (perché $s_7 \mid 20$ e $s_7 \equiv 1 \mod 7$), per cui l'unico 7-Sylow K di G è normale in G. Poiché $K \cong C_7$ è risolubile, per dimostrare che G è risolubile basta verificare che $\bar{G} := G/K$ lo è. Si ha $\#\bar{G} = \frac{\#G}{\#K} = \frac{35 \cdot 4}{7} = 20$, e (sempre per il teorema di Sylow) $\bar{G}$ ha un unico 5-Sylow K', che quindi è normale in $\bar{G}$. Dato che $\#(\bar{G}/K') = \frac{\#\bar{G}}{\#K'} = \frac{20}{5} = 4$, sia $K' \cong C_5$ che $\bar{G}/K' \cong C_4$ o $C_2 \times C_2$ sono risolubili; da ciò segue che anche $\bar{G}$ è risolubile.

(d) Si può prendere $G = A_5 \times C_7$, che non è risolubile perché contiene il sottogruppo $A_5 \times \{1\} \cong A_5$, che non è risolubile (perché semplice e non abeliano).

3. (a) $X^3 - p$ è irriducibile in $\mathbb{Q}[X]$ (per il criterio di Eisenstein relativo al primo p) e monico, dunque coincide con il polinomio minimo m_{β_p} di β_p su $\mathbb{Q}$. Le radici in $\mathbb{C}$ di m_{β_p} sono β_p, $\beta_p\omega$ e $\beta_p\omega^2$, dove

$$\omega := e^{\frac{2\pi i}{3}} = \cos\frac{2\pi}{3} + \sin\frac{2\pi}{3}i = -\frac{1}{2} + \frac{\sqrt{3}}{2}i,$$

mentre ω e $\omega^2 = \omega^{-1}$ sono le radici di $\mathrm{m}_\omega = X^2 + X + 1$ (che è irriducibile in $\mathbb{Q}[X]$ perché di grado 2 e senza radici in $\mathbb{Q}$). Se per assurdo $\mathbb{Q} \subseteq \mathbb{Q}(\beta_p)$ fosse normale, per definizione $\mathbb{Q}(\beta_p)$ conterrebbe $\beta_p\omega$ e quindi anche $\omega = \frac{\beta_p\omega}{\beta_p}$. Dalle estensioni $\mathbb{Q} \subseteq \mathbb{Q}(\omega) \subseteq \mathbb{Q}(\beta_p)$ si otterrebbe allora

$$[\mathbb{Q}(\beta_p) : \mathbb{Q}] = [\mathbb{Q}(\beta_p) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}],$$

ma questo non è possibile perché $[\mathbb{Q}(\beta_p) : \mathbb{Q}] = \deg(\mathrm{m}_{\beta_p}) = 3$ e $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\mathrm{m}_\omega) = 2$.

(b) In generale le radici di f_p in $\mathbb{C}$ sono $\pm\alpha_p, \beta_p, \beta_p\omega, \beta_p\omega^2$, per cui l'unico campo di spezzamento in $\mathbb{C}$ di f_p su $\mathbb{Q}$ è

$$L_p = \mathbb{Q}(\pm\alpha_p, \beta_p, \beta_p\omega, \beta_p\omega^2) = \mathbb{Q}(\alpha_p, \beta_p, \omega).$$

Indichiamo con G_p il gruppo di Galois di f_p su $\mathbb{Q}$, cioè il gruppo di Galois dell'estensione $\mathbb{Q} \subseteq L_p$ (che è di Galois, in quanto campo di spezzamento di un polinomio su un campo di caratteristica 0). Poiché $\alpha_p = \pm\sqrt{p}i$ e $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, è chiaro che $\alpha_3 \in \mathbb{Q}(\omega)$, per cui $L_3 = \mathbb{Q}(\beta_3, \omega)$ coincide con il campo di spezzamento di

$\mathrm{m}_{\beta_3} = X^3 - 3$ su $\mathbb{Q}$. Ne segue che G_3 è isomorfo a un sottogruppo di $S_{\deg(\mathrm{m}_{\beta_3})} = S_3$, per cui $\#G_3 \mid \#S_3 = 6$. D'altra parte, poiché (come si è visto nel punto precedente) $\mathbb{Q}(\beta_3) \subsetneq \mathbb{Q}(\beta_3, \omega)$, si ha

$$\#G_3 = [\mathbb{Q}(\beta_3, \omega) : \mathbb{Q}] > [\mathbb{Q}(\beta_3) : \mathbb{Q}] = 3,$$

da cui si conclude che $\#G_3 = 6$ e $G \cong S_3 \cong D_3$.

(c) Analogamente a prima è chiaro che $\omega \in \mathbb{Q}(\alpha_3)$, per cui $L_3 = \mathbb{Q}(\alpha_3, \beta_3)$. Supponiamo viceversa $\mathbb{Q}(\alpha_p, \beta_p) = L_p$. Tenendo conto che $[\mathbb{Q}(\alpha_p) : \mathbb{Q}] = \deg(\mathrm{m}_{\alpha_p}) = 2$ (ovviamente $\mathrm{m}_{\alpha_p} = X^2 + p$) si trova facilmente $[\mathbb{Q}(\alpha_p, \beta_p) : \mathbb{Q}] = [\mathbb{Q}(\beta_p, \omega) : \mathbb{Q}] = 6$. Risulta quindi $L_p = \mathbb{Q}(\beta_p, \omega)$, che è il campo di spezzamento di $X^3 - p$ su $\mathbb{Q}$, e ragionando come nel punto precedente (in cui $p = 3$) si trova ancora $G_p \cong S_3$. Per il teorema fondamentale della teoria di Galois esiste un'unica estensione $\mathbb{Q} \subseteq K \subseteq L_p$ tale che $[K : \mathbb{Q}] = 2$, corrispondente all'unico sottogruppo A_3 di indice 2 in S_3. Deve essere allora $\mathbb{Q}(\alpha_p) = K = \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{3}i)$. Poiché $\{1, \sqrt{3}i\}$ è una base di K su $\mathbb{Q}$, esistono unici $a, b \in \mathbb{Q}$ tali che $\alpha_p = a + b\sqrt{3}i$, da cui si deduce

$$-p = \alpha_p^2 = (a + b\sqrt{3}i)^2 = a^2 - 3b^2 + 2ab\sqrt{3}i,$$

cioè $-p = a^2 - 3b^2$ e $2ab = 0$. Non può essere $b = 0$, perché la prima equazione diventerebbe $-p = a^2$, che non ha soluzione $a \in \mathbb{Q}$; la seconda equzione implica allora $a = 0$, per cui la prima diventa $p = 3b^2$, che ha soluzione $b \in \mathbb{Q}$ se e solo se $p = 3$.

(d) Sia $p \neq 3$: per il punto precedente $\omega \notin \mathbb{Q}(\alpha_p, \beta_p)$, per cui

$$1 < [L_p = \mathbb{Q}(\alpha_p, \beta_p, \omega) : \mathbb{Q}(\alpha_p, \beta_p)] \leq [\mathbb{Q}(\omega) : \mathbb{Q}] = 2,$$

cioè $[L_p : \mathbb{Q}(\alpha_p, \beta_p)] = 2$. Essendo poi $[\mathbb{Q}(\alpha_p, \beta_p) : \mathbb{Q}] = 6$, si ha

$$\#G_p = [L_p : \mathbb{Q}] = [L_p : \mathbb{Q}(\alpha_p, \beta_p)][\mathbb{Q}(\alpha_p, \beta_p) : \mathbb{Q}] = 2 \cdot 6 = 12.$$

Conoscendo la classificazione dei gruppi di ordine 12, per concludere che $G_p \cong D_6$ basta dimostrare che G_p ha un sottogruppo H di ordine 4 non normale e non ciclico. In effetti basta prendere come H il gruppo di Galois di $\mathbb{Q}(\beta_p) \subseteq L_p$: per il teorema fondamentale della teoria di Galois H ha indice $[\mathbb{Q}(\beta_p) : \mathbb{Q}] = 3$ (quindi ha ordine 4), non è normale perché $\mathbb{Q} \subseteq \mathbb{Q}(\beta_p)$ non è normale e non è ciclico perché $\sigma^2 = \mathrm{id}_{L_p}$ per ogni $\sigma \in G_p$. Per verificare quest'ultimo fatto basta osservare che $\sigma^2(\alpha_p) = \alpha_p$ (perché $\sigma(\alpha_p) = \pm\alpha_p$) e $\sigma^2(\omega) = \omega$ (perché $\sigma(\omega) = \omega$ o ω^{-1}), tenendo conto che $L_p = \mathbb{Q}(\beta_p)(\alpha_p, \omega)$.