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

Prova scritta del 19/07/2019

1. Sia A un anello e sia M un A-modulo non nullo tale che il gruppo abeliano $(M, +)$ sia finitamente generato.
   (a) Dimostrare che M è un A-modulo finitamente generato.
   (b) Dimostrare che, se il gruppo abeliano $(M, +)$ è indecomponibile, allora M è un A-modulo ciclico.
   (c) Dimostrare che, se A è un dominio e M è un A-modulo senza torsione, allora il gruppo abeliano $(A, +)$ è finitamente generato.
   (d) Dimostrare che, se A è un campo, allora A e M sono finiti.

2. Sia G un gruppo di ordine $8 \cdot 11 \cdot 19$.
   (a) Dimostrare che G ha un unico 11-Sylow e un unico 19-Sylow.
   (b) Dimostrare che G contiene un sottogruppo normale e ciclico K di ordine $11 \cdot 19$.
   (c) Indicando con H un 2-Sylow di G, dimostrare che non esiste un omomorfismo iniettivo di gruppi $H \to \mathrm{Aut}(K)$.
   (d) Dimostrare che $Z(G) \neq \{1\}$.

3. Sia $K \subseteq L$ un'estensione di campi tale che $[L : K] = p^2$ per qualche numero primo p. Siano inoltre $\alpha, \beta \in L$ tali che $\alpha \notin K$ e $\beta \notin K(\alpha)$.
   (a) Dimostrare che $[K(\alpha) : K] = p$.
   (b) Dimostrare che, se $K \subseteq L$ è di Galois e $L \neq K(\beta)$, allora il gruppo di Galois di $K \subseteq L$ è isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
   (c) Dimostrare che, se $p = 2$ e $L \neq K(\beta)$, allora $K \subseteq L$ è normale.
   (d) Fornire un esempio in cui $p = 2$, $L = K(\beta)$ e $K \subseteq L$ è normale, e un esempio in cui $p = 2$, $L = K(\beta)$ e $K \subseteq L$ non è normale.

Soluzioni

1. (a) Per ipotesi esistono $x_1, \ldots, x_n \in M$ tali che $M = \langle x_1, \ldots, x_n \rangle$, e questo chiaramente implica che $M = \langle x_1, \ldots, x_n \rangle_A$ (dato che in ogni caso $\langle x_1, \ldots, x_n \rangle \subseteq \langle x_1, \ldots, x_n \rangle_A$), per cui M è un A-modulo finitamente generato.

   (b) Essendo $\mathbb{Z}$ un dominio a ideali principali, lo $\mathbb{Z}$-modulo finitamente generato e indecomponibile M è isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}/p^n\mathbb{Z}$ per qualche numero primo p e qualche $n > 0$. In particolare M è ciclico come $\mathbb{Z}$-modulo, e pertanto anche come A-modulo (come già visto nel punto precedente, se $M = \langle x \rangle$, allora $M = \langle x \rangle_A$).

   (c) Preso $x \in M \setminus \{0\}$ e tenuto conto che $\mathrm{Ann}_A(x) = \{0\}$ perché M è senza torsione, si ha $\langle x \rangle_A \cong A/\mathrm{Ann}_A(x) \cong A$ come A-moduli, e quindi come gruppi abeliani. Ciò dimostra che il gruppo abeliano $(A, +)$ è isomorfo al sottogruppo $\langle x \rangle_A$ di M, e quest'ultimo è finitamente generato perché M è uno $\mathbb{Z}$-modulo noetheriano (dato che $\mathbb{Z}$ è un anello commutativo noetheriano e M è uno $\mathbb{Z}$-modulo finitamente generato).

   (d) Come si è già visto, M è un A-modulo finitamente generato, cioè è un A-spazio vettoriale di dimensione finita $n > 0$. Poiché $M \cong A^n$ è un A-modulo libero e dunque senza torsione, per il punto precedente il gruppo abeliano $(A, +)$ è finitamente generato. Allora il campo primo K di A non può essere isomorfo a $\mathbb{Q}$, altrimenti K sarebbe in particolare un sottogruppo di A isomorfo a $\mathbb{Q}$. Tenendo conto che $\mathbb{Q}$ non è finitamente generato come gruppo, questo contraddirebbe il fatto che $(A, +)$ è finitamente generato e perciò (analogamente a quanto visto nel punto precedente per M) noetheriano. Deve essere pertanto $K \cong \mathbb{F}_p$ per qualche numero primo p (coincidente con la caratteristica di A). Da ciò segue che $pa = 0$ per ogni $a \in A$, e quindi in una decomposizione di $(A, +)$ come somma diretta di gruppi ciclici (la cui esistenza è garantita dal teorema di struttura dei gruppi abeliani finitamente generati) non ci possono essere termini isomorfi a $\mathbb{Z}$. Se ne deduce che $(A, +)$ è un gruppo abeliano finitamente generato di torsione, e dunque finito; ovviamente poi anche $M \cong A^n$ è finito.

2. (a) Indicando con s_p (per $p = 11, 19$) il numero di p-Sylow di G, si ha $s_p \equiv 1 \mod p$, $s_{11} \mid 8 \cdot 19 = 152$ e $s_{19} \mid 8 \cdot 11 = 88$. Da ciò segue subito che $s_{11} = s_{19} = 1$.

(b) Indicando con K_p (per $p = 11, 19$) l'unico p-Sylow di G, K_p è un sottogruppo normale di G di ordine p (per cui $K_p \cong C_p$ è ciclico). Tenendo conto che $K_{11} \cap K_{19} = \{1\}$ (perché i due sottogruppi hanno ordini coprimi), si ottiene che $K := K_{11}K_{19}$ è un sottogruppo normale di G e $K \cong K_{11} \times K_{19} \cong C_{11} \times C_{19}$; inoltre quest'ultimo gruppo è isomorfo a $C_{11\cdot 19}$ per il teorema cinese del resto.

(c) Ricordando che $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}^*$ per ogni $n > 0$, per il punto precedente si ha $\mathrm{Aut}(K) \cong \mathbb{Z}/(11 \cdot 19)\mathbb{Z}^*$, e quindi

$$\#\mathrm{Aut}(K) = \varphi(11 \cdot 19) = \varphi(11)\varphi(19) = (11-1)(19-1) = 180.$$

Se esistesse un omomorfismo iniettivo $H \to \mathrm{Aut}(K)$, la sua immagine sarebbe un sottogruppo di $\mathrm{Aut}(K)$ di ordine $\#H = 8$, il che è impossibile per il teorema di Lagrange, dato che $8 \nmid 180$.

(d) Poiché $K \cap H = \{1\}$ (perché i due sottogruppi hanno ordini coprimi) e $KH = G$ (perché $\#KH = (\#K)(\#H) = \#G$), si ha $G = K \rtimes H$, e dunque $G \cong K \rtimes_\theta H$ per qualche omomorfismo $\theta\colon H \to \mathrm{Aut}(K)$. Per il punto precedente $H' := \ker(\theta) \neq \{1\}$, e mostriamo preliminarmente che anche $H' \cap Z(H) \neq \{1\}$. In effetti questo è ovvio se H è abeliano, e altrimenti (a meno di isomorfismo) si può supporre $H = Q$ o $H = D_4$. Tenendo conto che sia H' che $Z(H)$ sono sottogruppi normali $\neq \{1\}$ di H, nel primo caso $-1 \in H' \cap Z(H)$ (ogni sottogruppo $\neq \{1\}$ di Q contiene -1) e nel secondo $R^2 \in H' \cap Z(H)$ (ogni sottogruppo normale $\neq \{1\}$ di D_4 contiene R^2). Scelto allora $1 \neq h \in H' \cap Z(H)$, per ogni $(a, b) \in K \rtimes_\theta H$ si ha

$$\begin{aligned}(a,b)(1,h) &= (a\theta(b)(1), bh) = (a1, bh) = (a, hb)\\ &= (\mathrm{id}_K(a), hb) = (1\theta(h)(a), hb) = (1,h)(a,b),\end{aligned}$$

il che dimostra che $(1,1) \neq (1,h) \in Z(K \rtimes_\theta H) \cong Z(G)$.

3. (a) Si ha $[K(\alpha) : K] \mid [L : K] = p^2$, dato che

$$[L : K] = [L : K(\alpha)][K(\alpha) : K].$$

Poiché $K \subsetneq K(\alpha)$ (perché $\alpha \notin K$) e $K(\alpha) \subsetneq L$ (perché $\beta \in L \setminus K(\alpha)$), risulta $1 < [K(\alpha) : K] < p^2$, e quindi $[K(\alpha) : K] = p$.

(b) Il gruppo di Galois G dell'estensione di Galois $K \subseteq L$ soddisfa $\#G = [L : K] = p^2$. Poiché $K \subsetneq K(\beta) \subsetneq L$, lo stesso argomento del punto precedente mostra che anche $[K(\beta) : K] = p$. Per

il teorema fondamentale della teoria di Galois le due estensioni distinte $K \subseteq K(\alpha)$ e $K \subseteq K(\beta)$ di grado p corrispondono a due sottogruppi distinti di indice p di G. Ne segue che G non è ciclico (un gruppo ciclico di ordine p^2 ha un unico sottogruppo di indice p), e quindi (grazie alla classificazione dei gruppi di ordine p^2) $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

(c) Come già osservato si ha $[K(\alpha) : K] = [K(\beta) : K] = 2$; inoltre, essendo in ogni caso $K(\alpha, \beta) \subseteq L$,

$$[K(\alpha, \beta) : K(\alpha)] \leq [L : K(\alpha)] = \frac{[L : K]}{[K(\alpha) : K]} = \frac{4}{2} = 2,$$

per cui (tenendo conto che $[K(\alpha, \beta) : K(\alpha)] > 1$ perché $\beta \notin K(\alpha)$) $[K(\alpha, \beta) : K(\alpha)] = 2$ e $L = K(\alpha, \beta)$. Poiché ogni estensione $K \subseteq K'$ di grado 2 è normale ed è un campo di spezzamento su K del polinomio minimo m_γ per ogni $\gamma \in K' \setminus K$, $K(\alpha)$ (rispettivamente $K(\beta)$) è un campo di spezzamento su K di m_α (rispettivamente m_β). Se ne deduce immediatamente che $L = K(\alpha, \beta)$ è un campo di spezzamento su K di $\mathrm{m}_\alpha \mathrm{m}_\beta$, il che dimostra che $K \subseteq L$ è normale.

(d) Prendendo $K = \mathbb{F}_q$ un campo finito (con q una potenza di un numero primo) e $L = \mathbb{F}_{q^4}$, è noto che $K \subseteq L$ è un'estensione di Galois (in particolare normale) di grado 4. Prendendo inoltre come α (rispettivamente β) un generatore del gruppo ciclico $\mathbb{F}_{q^2}^*$ (rispettivamente $\mathbb{F}_{q^4}^*$) risulta chiaramente $K(\alpha) = \mathbb{F}_{q^2}$ (per cui $\alpha \notin K$) e $K(\beta) = L$ (per cui $\beta \notin K(\alpha)$).

Prendendo $K = \mathbb{Q}$, $\beta = \sqrt[4]{2} \in \mathbb{R}$ e $L = K(\beta)$, si ha $\mathrm{m}_\beta = X^4 - 2$ (tale polinomio è irriducibile in $\mathbb{Q}[X]$ per il criterio di Eisenstein), per cui $[L : K] = \deg(\mathrm{m}_\beta) = 4$. Inoltre $K \subseteq L$ non è normale perché m_β ha le radici non reali $\pm\beta i$, e quindi non si spezza su $L \subseteq \mathbb{R}$. Prendendo infine $\alpha = \beta^2 = \sqrt{2}$, risulta $\mathrm{m}_\alpha = X^2 - 2$, da cui segue $[K(\alpha) : K] = 2$, e dunque $\alpha \notin K$ e $\beta \notin K(\alpha)$.