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

Prova scritta del 09/09/2021

1. Siano B un dominio e A un sottoanello di B tali che A sia un dominio a ideali principali e B sia un A-modulo finitamente generato.

   (a) Dimostrare che esiste un intero positivo k tale che $B \cong A^k$ come A-modulo.

   (b) Dati due A-sottomoduli M e N di B tali che $M \cap N = \{0\}$, dimostrare che esistono $m, n \in \mathbb{N}$ tali che $M \cong A^m$, $N \cong A^n$ e $m + n \leq k$.

   (c) Dimostrare che, se I è un ideale non nullo di B, allora $I \cap A \neq \{0\}$.

2. Sia G un gruppo di ordine $25p^2$ con p numero primo.

   (a) Dimostrare che, se $p > 5$, allora G ha un unico p-Sylow.

   (b) Dimostrare che, se $p > 5$ e $p \equiv 3 \mod 5$, allora G è abeliano.

   (c) Dimostrare che, se $p = 3$, allora G è abeliano se e solo se contiene un sottogruppo normale di indice 5.

3. Sia $K \subseteq L$ un'estensione di Galois e sia G il suo gruppo di Galois.

   (a) Dimostrare che per ogni $\alpha \in L$ esiste un unico campo di spezzamento $K \subseteq K_\alpha$ del polinomio minimo di α su K tale che $K_\alpha \subseteq L$.

   (b) Dimostrare che, se G è semplice, allora $\{\alpha \in L : K_\alpha \neq L\} = K$.

   (c) Dimostrare che, se $G \cong S_n$ con $n > 1$, allora $\{\alpha \in L : K_\alpha \neq L\}$ è un sottocampo di L.

Soluzioni

1. (a) B è un A-modulo senza torsione perché $ab = 0$ con $a \in A$ e $b \in B$ implica $a = 0$ o $b = 0$ (essendo B un dominio). Poiché B è anche un A-modulo finitamente generato e A è un dominio a ideali principali, ne segue che B è un A-modulo libero di rango finito, cioè esiste (unico) $k \in \mathbb{N}$ tale che $B \cong A^k$. Inoltre deve essere $k > 0$ perché $B \neq \{0\}$.

   (b) Essendo A un dominio a ideali principali, ogni A-sottomodulo di A^k è isomorfo a A^l con $0 \leq l \leq k$. Dunque esistono (unici) $m, n \in \mathbb{N}$ tali che $M \cong A^m$ e $N \cong A^n$ con $m, n \leq k$. Dal fatto che $M \cap N = \{0\}$ si ottiene anche $M + N = M \oplus N \cong A^m \oplus A^n \cong A^{m+n}$ con $m + n \leq k$, dato che anche $M + N$ è un A-sottomodulo di $B \cong A^k$.

   (c) Per assurdo sia $I \cap A = \{0\}$. Sia I (che è un B-sottomodulo di B) che A sono A-sottomoduli di B, quindi per il punto precedente esistono $m, n \in \mathbb{N}$ tali che $I \cong A^m$ e $A \cong A^n$ (come A-moduli) e $m+n \leq k$; chiaramente $n = 1$, per cui $m < k$. D'altra parte, preso $x \in I \setminus \{0\}$, l'ideale principale $J := Bx$ di B è tale che $J \cong B$ come B-modulo (la funzione $B \to J$, $b \mapsto bx$ è un isomorfismo di B-moduli), e quindi $J \cong B \cong A^k$ come A-modulo. Questo contraddice il fatto che J è un A-sottomodulo (essendo anche un B-sottomodulo) di $I \cong A^m$, dato che $m < k$.

2. Per $q = 5$ o p indichiamo con s_q il numero di q-Sylow e con H_q un q-Sylow di G.

   (a) Per il teorema di Sylow $s_p \equiv 1 \mod p$ e $s_p \mid 25$. Dunque $s_p = 1$, perché se fosse $s_p = 5$ o $s_p = 25$ si avrebbe $5 \equiv 1 \mod p$ (cioè $p \mid 4$) o $25 \equiv 1 \mod p$ (cioè $p \mid 24$), da cui seguirebbe $p = 2$ o 3.

   (b) Per il teorema di Sylow $s_5 \equiv 1 \mod 5$ e $s_5 \mid p^2$. Non potendo essere $s_5 = p$ (perché $p \equiv 3 \not\equiv 1 \mod 5$) o $s_5 = p^2$ (perché $p^2 \equiv 3^2 \equiv 4 \not\equiv 1 \mod 5$), si ha $s_5 = 1$, per cui $H_5 \lhd G$. Tenendo conto che anche $H_p \lhd G$ per il punto precedente, risulta $G = H_p \times H_5$. Si conclude allora che G è abeliano perché lo sono sia H_p che H_5 (avendo entrambi come ordine il quadrato di un numero primo).

   (c) Se G è abeliano, indicando con H un sottogruppo di H_5 di ordine 5 (che esiste per il teorema di Cauchy), $H_3 \times H$ è un sottogruppo (necessariamente normale) di $G = H_3 \times H_5$ di ordine $9 \cdot 5 = 45$, e quindi di indice 5.

Viceversa, se $K \triangleleft G$ e $[G : K] = 5$ (cioè $\#K = 45$), ogni 3-Sylow di K è anche 3-Sylow di G; si può quindi supporre $H_3 \subseteq K$. Poiché il numero di 3-Sylow di K è $\equiv 1 \mod 3$ e divide 5, H_3 è l'unico 3-Sylow di K. Per ogni $g \in G$ si ha allora $gH_3g^{-1} \subseteq gKg^{-1} = K$, da cui segue (essendo gH_3g^{-1} un 3-Sylow di K) $gH_3g^{-1} = H_3$, cioè $H_3 \triangleleft G$. A questo punto, esattamente come nel punto precedente, si conclude che anche $H_5 \triangleleft G$ e $G = H_3 \times H_5$ è abeliano.

3. Sia $U := \{\alpha \in L : K_\alpha \neq L\}$.

   (a) $\mathrm{m}_{\alpha,K}$ si spezza su L (perché l'estensione $K \subseteq L$ è normale), dunque esiste un unico campo di spezzamento $K \subseteq K_\alpha$ di $\mathrm{m}_{\alpha,K}$ tale che $K_\alpha \subseteq L$. Esplicitamente, indicando con $\alpha_1 = \alpha, \dots, \alpha_n$ le radici di $\mathrm{m}_{\alpha,K}$ in L, si ha $K_\alpha = K(\alpha_1, \dots, \alpha_n)$.

   (b) $K \neq L$ (perché $G \neq \{1\}$) e le uniche estensioni $K \subseteq L' \subseteq L$ con $K \subseteq L'$ normale sono $L' = K$ e $L' = L$ (perché, per il teorema fondamentale della teoria di Galois, sono in corrispondenza biunivoca con i sottogruppi normali di G). Tenendo conto che per ogni $\alpha \in L$ l'estensione $K \subseteq K_\alpha$ è normale (essendo campo di spezzamento di un polinomio), se ne deduce che $K_\alpha = K \neq L$ se $\alpha \in K$, mentre $K_\alpha = L$ se $\alpha \in L \setminus K$. Pertanto $U = K$.

   (c) Esiste $\{1\} \neq H \triangleleft G$ tale che $H \subseteq H'$ per ogni H' tale che $\{1\} \neq H' \triangleleft G$: attraverso l'isomorfismo tra G e S_n, H corrisponde a A_n se $n \neq 4$ e a V_4 se $n = 4$. Vogliamo dimostrare $U = L^H$ (che è un sottocampo di L). Se $\alpha \in L^H$, tenendo conto che $K \subseteq L^H$ è un'estensione normale (sempre per il teorema fondamentale della teoria di Galois), lo stesso argomento del primo punto mostra che $K_\alpha \subseteq L^H$. Poiché $L^H \subsetneq L$ (dato che $H \neq \{1\}$), si ottiene $K_\alpha \neq L$, cioè $\alpha \in U$. Viceversa, se $\alpha \in U$, l'estensione $K \subseteq K_\alpha$ è normale e $K_\alpha \neq L$, per cui $H' := \mathrm{G}_{K_\alpha}(L) \triangleleft G$ e $H' \neq \{1\}$. Per definizione di H si ha allora $H \subseteq H'$, e quindi $\alpha \in K_\alpha = L^{H'} \subseteq L^H$.