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

Prova scritta del 03/09/2019

1. Sia A un anello e sia $f\colon M \to N$ un omomorfismo di A-moduli. Per ogni A-modulo P si consideri la funzione

$$\begin{aligned} f_P\colon \mathrm{Hom}_A(N,P) &\to \mathrm{Hom}_A(M,P) \\ g &\mapsto g \circ f. \end{aligned}$$

   (a) Dimostrare che f_P è un omomorfismo di gruppi, e anche di A-moduli se A è commutativo.

   (b) Dimostrare che, se f è suriettivo, allora f_P è iniettivo per ogni A-modulo P.

   (c) Dimostrare che, se f_P è iniettivo per ogni A-modulo P, allora f è suriettivo.

   (d) Fornire un esempio in cui f è iniettivo e f_P non è suriettivo.

2. Sia $n \geq 3$ un intero.

   (a) Dimostrare che, se $n-1$ e $n+1$ sono numeri primi, allora ogni gruppo di ordine n^2-1 è ciclico.

   (b) Determinare il più piccolo valore pari di n tale che esiste un gruppo non abeliano di ordine n^2-1.

   (c) Determinare il più piccolo valore di n tale che ogni gruppo di ordine n^2-1 è abeliano, ma $n-1$ e $n+1$ non sono entrambi primi.

   (d) Determinare il più piccolo valore di n tale che ogni gruppo di ordine n^2-1 è ciclico, ma $n-1$ e $n+1$ non sono entrambi primi.

3. Sia K un campo perfetto e sia $f \in K[X]$. Indichiamo con $K \subseteq L$ un campo di spezzamento e con G il gruppo di Galois di f su K. Sia inoltre $\alpha \in L$ una radice di f.

   (a) Assumendo che f sia irriducibile in $K[X]$, dimostrare che l'estensione $K \subseteq K(\alpha)$ è normale se e solo se $L = K(\alpha)$.

   (b) Dimostrare che, se f è irriducibile e G è abeliano, allora $L = K(\alpha)$.

   (c) Determinare G nel caso in cui $K = \mathbb{F}_2$ e $f = X^5 + X^3 + 1$.

   (d) Dimostrare che G non è abeliano se $K = \mathbb{Q}$ e $f = X^5 + X^3 + 1$.

Soluzioni

1. (a) f_P è un omomorfismo di gruppi perché

$$f_P(g+h) = (g+h) \circ f = g \circ f + h \circ f = f_P(g) + f_P(h)$$

per ogni $g, h \in \mathrm{Hom}_A(N, P)$: l'uguaglianza centrale segue dal fatto che per ogni $x \in M$ si ha

$$\begin{aligned}((g+h) \circ f)(x) &= (g+h)(f(x)) = g(f(x)) + h(f(x)) \\ &= (g \circ f)(x) + (h \circ f)(x) = (g \circ f + h \circ f)(x).\end{aligned}$$

Se inoltre A è commutativo, allora f_P è un omomorfismo di A-moduli perché

$$f_P(ag) = (ag) \circ f = a(g \circ f) = a f_P(g)$$

per ogni $a \in A$ e per ogni $g \in \mathrm{Hom}_A(N, P)$: l'uguaglianza centrale segue dal fatto che per ogni $x \in M$ si ha

$$((ag) \circ f)(x) = (ag)(f(x)) = ag(f(x)) = (a(g \circ f))(x).$$

(b) Dato $g \in \mathrm{Hom}_A(N, P)$ tale che $f_P(g) = g \circ f = 0 \in \mathrm{Hom}_A(M, N)$, per definizione $g(f(x)) = 0_P$ per ogni $x \in M$. Essendo f suriettivo, per ogni $y \in N$ esiste $x \in M$ tale che $y = f(x)$, per cui $g(y) = g(f(x)) = 0_P$, cioè $g = 0 \in \mathrm{Hom}_A(N, P)$. Questo dimostra che $\ker(f_P) = \{0\}$, e quindi f_P è iniettivo.

(c) Prendendo $P = N/\operatorname{im}(f)$ e indicando con $\pi \colon N \to P$ l'omomorfismo di proiezione al quoziente, si ha $f_P(\pi) = \pi \circ f = 0 \in \mathrm{Hom}_A(M, P)$, perché $(\pi \circ f)(x) = \pi(f(x)) = 0_P$ (dato che $f(x) \in \operatorname{im}(f)$) per ogni $x \in M$. Per l'iniettività di f_P questo implica $\pi = 0 \in \mathrm{Hom}_A(N, P)$, cioè $\pi(y) = 0_P$ per ogni $y \in N$. Quest'ultima condizione equivale a $y \in \operatorname{im}(f)$ per ogni $y \in N$, e dunque f è suriettivo.

(d) Basta prendere come f l'inclusione di un sottomodulo M in un modulo N tale che M non sia addendo diretto di N (per esempio, $A = \mathbb{Z}$, $N = \mathbb{Z}$ e $M = 2\mathbb{Z}$). Prendendo infatti $P = M$, si ha $\mathrm{id}_M \in \mathrm{Hom}_A(M, P)$, ma non esiste $g \in \mathrm{Hom}_A(N, P)$ tale che $f_P(g) = g \circ f = g|_M = \mathrm{id}_M$, per cui f_P non è suriettivo.

2. (a) Se $p := n - 1$ e $q := n + 1$ sono primi, ogni gruppo di ordine $n^2 - 1 = pq$ è ciclico perché $p < q$ e $q \equiv 2 \not\equiv 1 \mod p$.

(b) Il valore cercato è $n = 8$. Infatti per $n = 4$ e per $n = 6$ sia $n - 1$ (rispettivamente 3 e 5) che $n + 1$ (rispettivamente 5 e 7) sono primi, per cui ogni gruppo di ordine $n^2 - 1$ è ciclico, e quindi abeliano, per il punto precedente. D'altra parte, esiste un gruppo non abeliano di ordine $8^2 - 1 = 63 = 3^2 \cdot 7$, per esempio $C_3 \times G_0$ con G_0 gruppo non abeliano di ordine $21 = 3 \cdot 7$ (tale G_0 esiste perché $7 \equiv 1 \mod 3$).

(c) Il valore cercato è $n = 10$. Infatti per $n \geq 3$ dispari $n^2 - 1 \geq 3^2 - 1 = 8$ è pari, ed esiste un gruppo non abeliano di ordine $n^2 - 1$ (per esempio $D_{\frac{n^2-1}{2}}$). Inoltre, come visto nel punto precedente, $n - 1$ e $n + 1$ sono primi per $n = 4$ e per $n = 6$, mentre esiste un gruppo non abeliano di ordine $n^2 - 1$ per $n = 8$. D'altra parte, $10 - 1 = 9$ non è primo, e ogni gruppo G di ordine $10^2 - 1 = 99 = 3^2 \cdot 11$ è abeliano. Per dimostrare quest'ultimo fatto basta osservare che (indicando con H_p un p-Sylow e con s_p il numero di p-Sylow di G per ogni primo p) per il teorema di Sylow si ha $s_{11} = 1$ (perché $s_{11} \equiv 1 \mod 11$ e $s_{11} \mid 9$) e $s_3 = 1$ (perché $s_3 \equiv 1 \mod 3$ e $s_3 \mid 11$). Ne segue che G è isomorfo a $H_{11} \times H_3$, e dunque è abeliano, dato che sia $H_{11} \cong C_{11}$ che $H_3 \cong C_9$ o $C_3 \times C_3$ lo sono.

(d) Il valore cercato è $n = 16$. Infatti, per quanto visto nel punto precedente, deve essere n pari e $n > 10$. Inoltre non può essere $n = 12$ perché $12-1 = 11$ e $12+1 = 13$ sono primi o $n = 14$ perchè esiste un gruppo non abeliano di ordine $14^2 - 1 = 3 \cdot 5 \cdot 13$, per esempio $C_5 \times G_1$ con G_1 gruppo non abeliano di ordine $39 = 3 \cdot 13$ (tale G_1 esiste perché $13 \equiv 1 \mod 3$). Infine per un gruppo G di ordine $16^2 - 1 = 255 = 3 \cdot 5 \cdot 17$ si ha $s_{17} = 1$ (perché $s_{17} \equiv 1 \mod 17$ e $s_{17} \mid 15$), per cui H_{17} è normale in G. Ne segue che $K := H_{17}H_5$ è un sottogruppo di G; poiché $\#K = 5 \cdot 17 = 85$ e $17 \not\equiv 1 \mod 5$, risulta $K \cong C_{85}$. In particolare H_5 è normale in K, per cui, indicando con G' il normalizzatore di H_5 in G, si ha $K \subseteq G'$. Per il teorema di Sylow questo implica che $s_5 = [G : G'] \leq [G : K] = 3$ e $s_5 \equiv 1 \mod 5$, per cui $s_5 = 1$ e H_5 è normale in G. Allora anche K è normale in G; tenendo conto che $H_3 \cap K = \{1\}$ e $H_3K = G$, si ottiene $G = K \rtimes H_3$. Dunque $G \cong C_{85} \rtimes_\theta C_3$ per qualche omomorfismo $\theta \colon C_3 \to \mathrm{Aut}(C_{85}) \cong \mathbb{Z}/85\mathbb{Z}^*$. Poiché $\#C_3 = 3$ e $\#\mathrm{Aut}(C_{85}) = \varphi(85) = \varphi(5)\varphi(17) = 4 \cdot 16$ sono coprimi, θ è banale, per cui $G \cong C_{85} \times C_3 \cong C_{255}$ per il teorema cinese del resto.

3. (a) Se $L = K(\alpha)$, allora $K \subseteq K(\alpha) = L$ è normale perché campo di spezzamento di f. Viceversa, se $K \subseteq K(\alpha)$ è normale, allora il

polinomio minimo m_α di α su K si spezza in $K(\alpha)$. Poiché α è radice di f e f è irriducibile, f è associato a m_α, e dunque f si spezza in $K(\alpha)$. Essendo $K \subseteq L$ un campo di spezzamento di f, l'inclusione $K(\alpha) \subseteq L$ implica allora $L = K(\alpha)$.

(b) Osserviamo intanto che l'estensione $K \subseteq L$ è di Galois: è normale e finita perché campo di spezzamento di un polinomio, ed è separabile perché K è perfetto. Se G è abeliano, tutti i suoi sottogruppi sono normali, e per il teorema fondamentale della teoria di Galois questo implica che $K \subseteq K'$ è normale per ogni estensione $K \subseteq K' \subseteq L$. In particolare $K \subseteq K(\alpha)$ è normale, e questo implica $L = K(\alpha)$ per il punto precedente.

(c) È molto facile verificare che f è irriducibile in $\mathbb{F}_2[X]$, dato che non ha radici in $\mathbb{F}_2$, non è divisibile per X^2+X+1 (che è l'unico polinomio irriducibile di secondo grado in $\mathbb{F}_2[X]$) e $\deg(f) = 5$. Essendo $\mathbb{F}_2$ un campo finito, segue allora che un campo di spezzamento di f è $\mathbb{F}_2 \subseteq \mathbb{F}_{2^5} = \mathbb{F}_{32}$ e $G \cong C_5$.

(d) Poiché f è monico a coefficienti interi, dal fatto (visto nel punto precedente) che f è irriducibile in $\mathbb{F}_2[X]$ segue che f è irriducibile anche in $\mathbb{Z}[X]$ e in $\mathbb{Q}[X]$. È anche facile vedere che delle radici complesse di f (che sono $\deg(f) = 5$ distinte perché f è separabile) una sola è reale: ce n'è almeno una perché $f \in \mathbb{R}[X]$ e $\deg(f)$ è dispari, e non ce n'è più di una perché f (vista come funzione $\mathbb{R} \to \mathbb{R}$) è strettamente crescente (infatti $f' = 5X^4+3X^2$ soddisfa $f'(x) \geq 0$ per ogni $x \in \mathbb{R}$ e $f'(x) = 0$ se e solo se $x = 0$). Si può prendere allora come L il sottocampo di $\mathbb{C}$ generato su $\mathbb{Q}$ dalle radici complesse di f e come α la radice reale di f. Allora $K(\alpha) \subseteq \mathbb{R}$ mentre $L \not\subseteq \mathbb{R}$, per cui $L \neq K(\alpha)$, e quindi G non è abeliano per il punto (b).