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

Prova scritta del 16/07/2021

1. Sia A un anello e sia $f\colon M \to N$ un omomorfismo di A-moduli. Il *conucleo* di f è il modulo quoziente $\operatorname{coker}(f) := N/\operatorname{im}(f)$.

   (a) Dimostrare che M e N sono noetheriani se e solo se $\ker(f)$, $\operatorname{coker}(f)$ e $\operatorname{im}(f)$ sono noetheriani.

   (b) Dimostrare che, se $\ker(f)$ è un addendo diretto di M e $\operatorname{im}(f)$ è un addendo diretto di N, allora $M \oplus \operatorname{coker}(f) \cong N \oplus \ker(f)$.

   (c) Dimostrare che, se A è un dominio a ideali principali ma non un campo e $M = N = A/P^n$ con P ideale massimale di A e $n > 0$, allora $\operatorname{coker}(f) \cong \ker(f)$.

2. Sia G un gruppo finito e sia K un sottogruppo normale non banale di G tale che K e G/K abbiano ordini coprimi.

   (a) Dimostrare che, se G/K è un p-gruppo, allora esiste un sottogruppo H di G tale che $G = K \rtimes H$.

   (b) Dimostrare che, se $\#K = 15$ e $\#(G/K) = 7$, allora G è ciclico.

   (c) Dimostrare che, se G è non abeliano di ordine 225, allora K è non ciclico di ordine 25.

3. Sia $f := (X^2 + X + 2)(X^3 - 3X - 1)$.

   (a) Determinare $\mathrm{G}_{\mathbb{R}}(f)$.

   (b) Determinare $\mathrm{G}_{\mathbb{F}_q}(f)$ per $q = 2, 3, 4$.

   (c) Esiste una potenza di un primo q tale che $\mathrm{G}_{\mathbb{F}_q}(f) \cong \mathrm{G}_{\mathbb{Q}}(f)$?

Soluzioni

1. (a) Se M e N sono noetheriani, lo sono anche $\ker(f)$ (perché sottomodulo di M), $\operatorname{coker}(f)$ (perché quoziente di N) e $\operatorname{im}(f)$ (perché sottomodulo di N). Viceversa, M è noetheriano perché lo sono il suo sottomodulo $\ker(f)$ e $M/\ker(f) \cong \operatorname{im}(f)$ (per il primo teorema di isomorfismo); N è noetheriano perché lo sono il suo sottomodulo $\operatorname{im}(f)$ e $N/\operatorname{im}(f) \cong \operatorname{coker}(f)$.

   (b) Dall'ipotesi segue che

$$M \cong \ker(f) \oplus M/\ker(f) \cong \ker(f) \oplus \operatorname{im}(f),$$
$$N \cong \operatorname{im}(f) \oplus N/\operatorname{im}(f) = \operatorname{im}(f) \oplus \operatorname{coker}(f),$$

   e pertanto $M \oplus \operatorname{coker}(f) \cong \ker(f) \oplus \operatorname{im}(f) \oplus \operatorname{coker}(f) \cong \ker(f) \oplus N$.

   (c) Essendo $\ker(f)$ e $\operatorname{im}(f)$ sottomoduli di A/P^n, esistono unici interi i e j tali che $0 \leq i, j \leq n$, $\ker(f) = P^i/P^n$ e $\operatorname{im}(f) = P^j/P^n$. Per il terzo teorema di isomorfismo si ottiene quindi

$$\operatorname{im}(f) \cong M/\ker(f) = (A/P^n)/(P^i/P^n) \cong A/P^i,$$
$$\operatorname{coker}(f) = N/\operatorname{im}(f) = (A/P^n)/(P^j/P^n) \cong A/P^j.$$

   D'altra parte $P^i/P^n \cong A/P^{(n-i)}$ (perché, se $P = (p)$, $P^i/P^n = \langle x \rangle_A$ con $x := p^i + P^n$, per cui $P^i/P^n \cong A/\operatorname{Ann}_A(x) = A/(p^{(n-i)})$), e analogamente $P^j/P^n \cong A/P^{(n-j)}$. Se ne deduce che $A/P^i \cong \operatorname{im}(f) = P^j/P^n \cong A/P^{(n-j)}$, e da ciò segue $i = n - j$. Si conclude allora che $\ker(f) = P^i/P^n \cong A/P^{(n-i)} = A/P^j \cong \operatorname{coker}(f)$.

2. (a) Basta prendere come H un p-Sylow di G. Infatti, se $\#K = m$ e $\#(G/K) = p^l$ (con $m > 1$ e $l > 0$), per ipotesi $p \nmid m$ e per il teorema di Lagrange $\#G = \#K\#(G/K) = mp^l$. Dunque $\#H = p^l$ e $K \cap H = \{1\}$ perché i due sottogruppi hanno ordini coprimi; inoltre $\#(KH) = \#K\#H = mp^l = \#G$, per cui $KH = G$.

   (b) Per il punto precedente $G = K \rtimes H$ con H 7-Sylow di G. Essendo $K \cong C_{15}$ (dato che $\#K = 3 \cdot 5$ e $5 \not\equiv 1 \mod 3$) e $H \cong C_7$, si ha $G \cong C_{15} \rtimes_\theta C_7$ per qualche omomorfismo $\theta \colon C_7 \to \operatorname{Aut}(C_{15}) \cong \mathbb{Z}/15\mathbb{Z}^*$. Poiché $\#(\mathbb{Z}/15\mathbb{Z}^*) = \varphi(15) = \varphi(3)\varphi(15) = 2 \cdot 4 = 8$ è coprimo con 7, θ deve essere banale, cioè $G \cong C_{15} \times C_7 \cong C_{105}$.

   (c) Se $\#K = m$ e $\#(G/K) = n$, deve essere $mn = 225 = 3^2 \cdot 5^2$ con $\operatorname{mcd}(m, n) = 1$ e $1 < m < 225$, per cui $m = 9$ e $n = 25$ o $m = 25$

e $n = 9$. Poiché $n = p^2$ (con $p = 5$ o 3), per il primo punto esiste un p-Sylow H tale che $G = K \rtimes H$. Essendo K e H abeliani (perché di ordine il quadrato di un primo) e G non abeliano, non può essere $G = K \times H$, e dunque H non è normale in G. Ne segue che $p = 3$ (se fosse $p = 5$, il numero di 5-Sylow di G sarebbe 1, in quanto divisore di 9 e $\equiv 1 \mod 5$), e quindi $\#K = m = 25$. Se per assurdo K fosse ciclico, si avrebbe $G \cong C_{25} \rtimes_\theta H$ con $\theta\colon H \to \mathrm{Aut}(C_{25}) \cong \mathbb{Z}/25\mathbb{Z}^*$ omomorfismo necessariamente banale (perché $\#(\mathbb{Z}/25\mathbb{Z}^*) = \varphi(25) = 20$ è coprimo con $\#H = 9$), e $G \cong C_{25} \times H$ sarebbe abeliano.

3. Sia $g := X^2 + X + 2$ e $h := X^3 - 3X - 1$ (per cui $f = gh$).

   (a) Un campo di spezzamento di f su $\mathbb{R}$ è $\mathbb{C}$, visto che f si spezza su $\mathbb{C}$ (essendo $\mathbb{C}$ algebricamente chiuso) ma non su $\mathbb{R}$ (g non ha radici reali) e $\mathbb{C}$ è l'unico sottocampo di $\mathbb{C}$ che contiene strettamente $\mathbb{R}$ (perché $[\mathbb{C} : \mathbb{R}] = 2$). Dunque $\mathrm{G}_{\mathbb{R}}(f) \cong \mathrm{G}_{\mathbb{R}}(\mathbb{C}) \cong C_2$.

   (b) In ogni caso $\mathrm{G}_{\mathbb{F}_q}(f) \cong C_d$ con d minimo comune multiplo dei gradi dei fattori irriducibili di f in $\mathbb{F}_q[X]$.

   Se $q = 2$, $g = X(X + 1)$ mentre h è irriducibile (perché di grado 3 e senza radici in $\mathbb{F}_2$), per cui $d = \mathrm{mcm}(1, 1, 3) = 3$.

   Se $q = 3$, g è irriducibile (perché di grado 2 e senza radici in $\mathbb{F}_3$), mentre $h = (X - 1)^3$, per cui $d = \mathrm{mcm}(2, 1, 1, 1) = 2$.

   Se $q = 4 = 2^2$, la fattorizzazione di f è la stessa vista nel caso $q = 2$, per cui anche in questo caso $d = 3$. Per vedere questo basta verificare che h non ha radici nemmeno in $\mathbb{F}_4$. In effetti, se α è una radice di h (nel suo campo di spezzamento $\mathbb{F}_8$ su $\mathbb{F}_2$), si ha $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = \deg(h) = 3$, cioè $\mathbb{F}_2(\alpha) = \mathbb{F}_8$. Dunque $\alpha \notin \mathbb{F}_4$.

   (c) Sì, per esempio $q = 5$. Infatti g e h sono irriducibili in $\mathbb{F}_5[X]$ (perché di gradi 2 e 3 e senza radici), quindi, come visto nel punto precedente, $\mathrm{G}_{\mathbb{F}_5}(f) \cong C_6$, dato che $\mathrm{mcm}(\deg(g), \deg(h)) = 6$.

   D'altra parte, essendo monici e irriducibili in $\mathbb{F}_5[X]$, g e h sono irriducibili anche in $\mathbb{Q}[X]$. Inoltre $\Delta(h) = -4(-3)^3 - 27(-1)^2 = 81 = 9^2$ è un quadrato in $\mathbb{Q}$, per cui, indicando con $\alpha \in \mathbb{C}$ una radice di h, $\mathbb{Q}(\alpha)$ è campo di spezzamento di h su $\mathbb{Q}$; chiaramente è anche vero che, se $\beta \in \mathbb{C}$ è una radice di g, $\mathbb{Q}(\beta)$ è campo di spezzamento di g su $\mathbb{Q}$. Dunque $K := \mathbb{Q}(\alpha, \beta)$ è campo di spezzamento di f su $\mathbb{Q}$ e $[K : \mathbb{Q}] = 3 \cdot 2 = 6$ (essendo $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ e $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$ coprimi). Pertanto $\mathrm{G}_{\mathbb{Q}}(f) = \mathrm{G}_{\mathbb{Q}}(K)$ ha ordine 6, ed è ciclico perché contiene un sottogruppo normale di ordine 2, cioè $\mathrm{G}_{\mathbb{Q}(\alpha)}(K)$ (dato che $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ è normale di grado 3).