

Algebra I - Soluzioni 2

5 Aprile

1 Esercizi

Esercizio 1. Dato $N = \{(t, s)\} \leq G := G_1 \times G_2$, l'obiettivo è dimostrare che i seguenti insiemi

$$T := \{t \in G_1 \mid (t, s) \in N\} \quad \text{e} \quad S := \{s \in G_2 \mid (t, s) \in N\}$$

sono sottogruppi di G_1 e G_2 rispettivamente. Infatti si ha da definizione che

$$N = T \times S,$$

da cui seguirebbe la tesi.

Studiamo il caso di T , e S seguirà per simmetria. Consideriamo la proiezione canonica

$$\pi : G \rightarrow G_1$$

che ad un elemento $(t, s) \in G$ associa $\pi((t, s)) = t \in G_1$. Tale proiezione è un omomorfismo, e si ha che

$$\pi(N) = T.$$

L'immagine di un omomorfismo di gruppi è un sottogruppo del codominio, da cui segue che $T \leq G_1$ e ciò conclude la dimostrazione.

Esercizio 2. Sia

$$f : A \rightarrow B$$

l'omomorfismo di anelli. Ci si avvale del seguente lemma.

Lemma 1.1. *Sia dato un omomorfismo suriettivo di anelli $\varphi : A \rightarrow B$ e $K \trianglelefteq A$ un ideale di A tale che $K \subseteq \ker \varphi$. Sia inoltre $\tilde{\varphi} : A/K \rightarrow B$ l'unico omomorfismo indotto da φ . $\tilde{\varphi}$ è un isomorfismo se e solo se $K = \ker \varphi$.*

Proof. Supponiamo per assurdo esista $x \in \ker \varphi \setminus K$. Questo vuol dire che in A/K la classe di x è diversa dalla classe di 0. Ma $\tilde{\varphi}([x]) = 0$ per com'è definita, e quindi $[x] \in \ker \tilde{\varphi}$. Questo è assurdo perché per ipotesi $\tilde{\varphi}$ è un isomorfismo. \ast □

L'idea quindi è cercare alcuni elementi del nucleo di f e poi sfruttare il lemma enunciato sopra per dimostrare che sono tutti.

Osservazione. Sia ζ_n una radice primitiva n -esima dell'unità. L'insieme $\mathbb{Q}[\omega_1, \dots, \omega_n]$ può essere riscritto quindi come $\mathbb{Q}[\zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}] = \mathbb{Q}[\zeta_n]$.

Questo dipende dal fatto che

$$\zeta_n^i \zeta_n^j = \zeta_n^{i+j}.$$

Si consideri il seguente ideale

$$K = \langle \{t_i - t_1^i \mid i = 2, \dots, n\} \cup \{\Phi(t_1)\} \rangle_A,$$

dove $\Phi_n(t_1)$ è l' n -esimo polinomio ciclotomico. Questo ideale è contenuto nel nucleo di f perché ogni elemento dell'insieme si annulla. Per osservare che

$$\tilde{f}: A/K \rightarrow B$$

è un isomorfismo, basta notare che, preso un polinomio $p \in A$, le variabili t_2, \dots, t_n si possono esprimere in funzione di t_1 e

$$\mathbb{Q}[t_1]/\Phi_n(t_1) \cong \mathbb{Q}[\zeta_n].$$

Per il lemma precedentemente enunciato si ha che $K = \ker f$.

Esercizio 3. Un'azione di G su un insieme X con cardinalità assegnate, è un omomorfismo

$$\rho: G \rightarrow \mathcal{S}_m.$$

Se l'azione è non banale inoltre, $\ker \rho \neq G$.

Osservazione. Essendo ρ un omomorfismo da G in un altro gruppo, $\ker \rho \trianglelefteq G$.

La richiesta è di trovare una condizione numerica su n e m tali che ci sia almeno un sottogruppo normale di G .

Un esempio di condizione numerica è

$$n \nmid m!$$

Infatti valesse $|\rho(G)| \neq n$ essendo $\rho(G)$ sottogruppo di \mathcal{S}_m . Da cui $|\ker \rho| > 1$, e avremmo trovato il sottogruppo normale non banale di G .

Esercizio 4. Le due ipotesi sono

- (1) $H \leq Z(G)$,
- (2) G/H ciclico.

Siano $y, z \in G$. Si consideri la proiezione canonica

$$G \twoheadrightarrow G/H,$$

e sia $[x] = xH \in G/H$ l'elemento che lo genera. Per ciclicità esistono t ed s tali che

$$yH = [y] = [x]^t = (xH)^t = xHxH \dots xH$$

e

$$zH = [z] = [x]^s = (xH)^s = xHxH \dots xH.$$

Per l'ipotesi (1) inoltre si ha $(xH)^t = xHxH \dots xH = x^tH$ e così per $(xH)^s$.

Dalle uguaglianze $yH = x^tH$ e $zH = x^sH$ si ottiene $\forall h \in H \exists h_1, h_2 \in H$ tali che

$$yh = x^t h_1 \quad \text{e} \quad zh^{-1} = x^s h_2.$$

La conclusione segue dalla seguente uguaglianza

$$yz = yz1 = yzhh^{-1} = yhz h^{-1} = x^t h_1 x^s h_2 = x^t x^s h_1 h_2 = x^s x^t h_2 h_1 = x^s h_2 x^t h_1 = z h^{-1} y h = z y h^{-1} h = z y 1 = z y.$$

Esercizio 5. Supponiamo $IJ \subseteq \mathfrak{p}$. Supponiamo inoltre per assurdo che $I \not\subseteq \mathfrak{p}$ e $J \not\subseteq \mathfrak{p}$. Siano $x \in I \setminus \mathfrak{p}$ e $y \in J \setminus \mathfrak{p}$. L'elemento xy si trova ambo in I e in J per la proprietà divorante, e si trova dunque in $IJ \subseteq \mathfrak{p}$. Da definizione, un ideale è primo se

$$(xy \in \mathfrak{p}) \rightarrow (x \in \mathfrak{p}) \vee (y \in \mathfrak{p}).$$

Ma ciò contraddice l'ipotesi assurda assunta inizialmente. \ast

Esercizio 6. Si svolgono i punti separatamente.

- ◇ Poiché φ è un omomorfismo di anelli, $\ker \varphi \trianglelefteq R$. Se R è un campo, gli unici ideali sono $\{0\}$ e R . Da cui φ è iniettiva e quindi $\ker \varphi = \{0\}$ oppure $\varphi = 0$ e allora $\ker \varphi = R$.
- ◇ Supponiamo φ sia suriettiva, e consideriamo $\varphi^{-1}(1_S)$. Sia $r \in \varphi^{-1}(1_S)$. Vale

$$1_S = \varphi(r) = \varphi(r \cdot 1_R) = \varphi(r) \cdot \varphi(1_R) = 1_S \cdot \varphi(1_R) = \varphi(1_R).$$

L'esempio è

$$\begin{aligned} \varphi_2 : \mathbb{Z} &\rightarrow \mathbb{Z} \\ z &\mapsto 2z \end{aligned}$$

Siano $x, y \in \mathbb{Z}$,

$$\varphi_2(x + y) = \varphi_2(x) + \varphi_2(y) = 2x + 2y = 2(x + y) = 2\varphi_2(x + y).$$

Esercizio 7. Sia

$$\rho : G \rightarrow \mathcal{S}_X$$

l'azione di G su X , cioè l'omomorfismo di G nel gruppo delle permutazioni di X . Si ricorda che \mathcal{S}_X è solo un modo compatto per scrivere "Supponiamo X abbia m elementi, allora consideriamo \mathcal{S}_m ". Un punto fisso $x \in X^G$ è un elemento $x \in X$ tale che $\rho(g)(x) = g.x = x \quad \forall g \in G$.

Osservazione. Data un'azione ρ , invece di scrivere $\rho(g)(x)$, si può anche scrivere $g.x$, dove, con la prima notazione si enfatizza l'omomorfismo ρ , e con la seconda invece si snellisce siccome ρ è già stato fissato.

Sia $G.x$ l'orbita di x , cioè

$$G.x := \{y \in X \mid \exists g \in G \quad g.x = y\}.$$

L'orbita è l'insieme di tutti gli elementi di X raggiungibili partendo da x e spostandosi tramite l'azione. Definiamo infine G_x lo stabilizzatore di x , cioè

$$G_x := \{g \in G \mid g.x = x\}.$$

Lo stabilizzatore è l'insieme di tutti gli elementi di g che non spostano un certo x fissato.

Fissato un qualsiasi $x \in X$, vale la seguente formula $|G| = |G_x| \cdot |G.x|$ e da ciò segue che $p \mid |G.x|$ oppure $|G.x| = 1$. La seconda si verifica però solo se $G.x = \{x\}$, cioè se x è un punto fisso dell'azione di G .

Ora consideriamo X . L'insieme può essere partizionato in orbite nel seguente modo:

- 1) Prendiamo $x_1 \in X$,
- 2) Consideriamo $G.x_1 \subseteq X$,
- 3) Prendiamo $x_2 \in X \setminus G.x_1$,
- 4) Consideriamo $G.x_2 \subseteq X \setminus G.x_1$,
- 5) Prendiamo $x_3 \in X \setminus (G.x_1 \cup G.x_2)$,
- 6) ...

Alla fine si otterrà che

$$X = G.x_1 \cup G.x_2 \cup \dots \cup G.x_k.$$

La cardinalità di X quindi è

$$|X| = \sum_{i=1}^k |G.x_i|.$$

Ma le cardinalità di $G.x_i$ sono tutte congrue a 0 modulo p , salvo quando x_i è un punto fisso, e in quel caso valgono 1. Da ciò segue che

$$|X| \equiv \sum_{i=1}^k |G.x_i| \equiv \sum_{x_i \text{ fisso}} |G.x_i| \equiv \sum_{x_i \text{ fisso}} 1 \equiv \#\text{punti fissi dell'azione} \pmod{p}$$

Esercizio 8. Verranno dimostrati i tre punti separatamente.

- ◇ Per mostrare che un Φ_x è un morfismo di anelli va testato sulle operazioni.

$$\Phi_x(f + g) = (f + g)(x) = f(x) + g(x), \quad (1)$$

$$\Phi_x(fg) = (fg)(x) = f(x)g(x). \quad (2)$$

Per mostrare la suriettività invece basta osservare che, $\forall r \in \mathbb{R}$, la funzione costante $f_r \equiv r$ è continua ed ha come immagine r stessa.

- ◇ No, perché, pur essendo un insieme chiuso per somma e prodotto, per $f \in C[(a, b)]$, $r \in \mathbb{R}$, rf non è una funzione costante.
- ◇ Essendo Φ_x suriettivo, vale il teorema di omomorfismo che dice

$$C[(a, b)] / \ker \Phi_x \cong \text{Im}(\Phi_x) \cong \mathbb{R}.$$

Siccome \mathbb{R} è un campo, allora $\ker \Phi_x$ è un ideale massimale.

2 Appendice

Sia \mathbb{Q} il campo dei razionali. Sia inoltre ζ_n una radice n -esima dell'unità, cioè un numero tale che

$$\zeta_n^n = 1.$$

È d'uso chiedersi, dato un numero ξ non in \mathbb{Q} , se esista un polinomio f a coefficienti in \mathbb{Q} che calcolato in ξ si annulli.

Esempio 1. Il polinomio

$$f = x^n - 1 \in \mathbb{Q}[x]$$

è un polinomio che annulla ζ_n .

Esempio 2. Il polinomio

$$g = (x^2 + 5x - 22)(x^n - 1) \in \mathbb{Q}[x]$$

è un polinomio che annulla ζ_n , infatti, quando calcolato in ζ_n il secondo fattore si annulla, e quindi tutto il polinomio si annulla.

Si nota però che il polinomio $x^n - 1$ non è il polinomio più piccolo che si annulla in ζ_n , infatti è già divisibile per $x - 1$, ad esempio. La domanda giusta da porsi quindi è: *Qual è il polinomio minimo che si annulla in ξ ?*

In questo caso, per le radici n -esime dell'unità la risposta sono i polinomi ciclotomici. Questi sono dei polinomi monici, irriducibili che si annullano nelle radici dell'unità. I primi polinomi ciclotomici, ad esempio sono

$$\Phi_1(x) = x - 1$$

$$\Phi_2(x) = x + 1$$

$$\Phi_3(x) = x^2 + x + 1$$

$$\Phi_4(x) = x^2 - 1$$

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

$$\Phi_6(x) = x^2 - x + 1$$

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\Phi_8(x) = x^4 + 1$$

$$\Phi_9(x) = x^6 + x^3 + 1$$

$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$$