Algebra I - Soluzioni 4

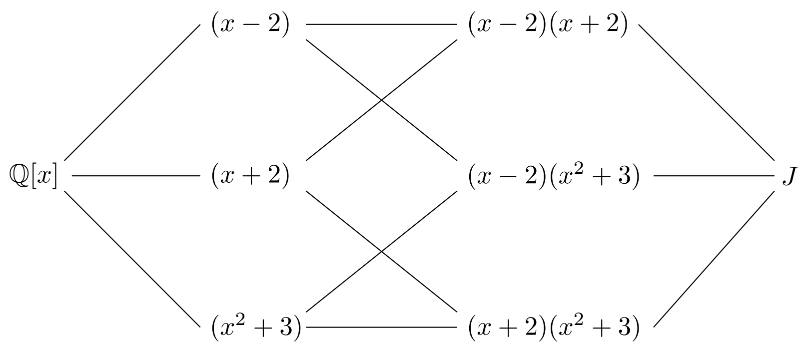
19 Aprile

1 Esercizi

Esercizio 1. Il polinomio $f = x^4 - x^2 - 12 \in \mathbb{Q}[x]$ si può scomporre in irriducibili come

$$x^4 - x^2 - 12 = (x^2 - 4)(x^2 + 3) = (x - 2)(x + 2)(x^2 + 3).$$

Nell'anello $\mathbb{Q}[x]/J$, per il teorema di corrispondenza, gli ideali sono



Esercizio 2. *Primo metodo:* Ricordiamo il criterio di Eisenstein

Teorema 1.1 (Criterio di Eisenstein)**.** *Sia $p \in \mathbb{Z}[x]$ un polinomio primitivo, i.e.*

$$p = a_n x^n + \cdots + a_1 x + a_0$$

e $mcd(a_n, \ldots, a_0) = 1$. Se esiste un numero primo $p \in \mathbb{Z}$ tale che

- *p non divide a_n,*
- *p divide $a_{n-1}, \ldots, a_0$,*
- *p^2 non divide a_0.*

Allora p è irriducibile come polinomio in $\mathbb{Z}[x]$.

Per questo criterio, scelto il primo p, come il termine noto del polinomio

$$f = x^n - p,$$

segue che f è irriducibile.

Secondo metodo: Il polinomio

$$f = x^n - p$$

si decompone in $\mathbb{C}$ come

$$x^n - p = (x - \xi_1) \dots (x - \xi_n), \tag{1}$$

con $\xi_i = \sqrt[n]{p} \cdot \zeta_n^i$. Cioè sono gli n numeri complessi disposti sui vertici di un n-agono regolare inscritto in una circonferenza di raggio $\sqrt[n]{p}$.

Supponiamo quindi, per assurdo, che f non sia irriducibile, e sia $f = gh$ una sua scomposizione. In $\mathbb{C}[x]$, questi due polinomi si scompongono

$$g = (x - \xi_{i_1}) \dots (x - \xi_{i_t})$$

e

$$h = (x - \xi_{j_1}) \dots (x - \xi_{j_s}).$$

Cioè un po' di monomi della scomposizione (1) vanno nella scomposizione di g e un po' di monomi in quella di h. Ora, il termine noto di g, indicato con a_g, è il prodotto delle radici di g, cioè

$$a_g = \xi_{i_1} \cdot \dots \cdot \xi_{i_t}.$$

La norma complessa di questo numero è

$$|a_g| = |\xi_{i_1}| \cdot \dots \cdot |\xi_{i_t}| = (\sqrt[n]{p})^t \notin \mathbb{Z}.$$

Ma ciò è assurdo perché $g \in \mathbb{Z}[x]$ ha un termine noto intero, e quindi dovrebbe avere norma complessa intera. ※

Esercizio 3. Il nucleo dell'omomorfismo

$$\begin{aligned} \varphi : \mathbb{Z}[x] &\to \mathbb{R} \\ 1 &\mapsto 1 \\ x &\mapsto 1 + \sqrt{2} \end{aligned}$$

è l'insieme dei polinomi che valutati in $1 + \sqrt{2}$ si annullano. Infatti sia

$$p(x) = a_n x^n + \dots + a_1 x + a_0,$$

si ha

$$\varphi(p(x)) = \varphi(a_n x^n + \dots + a_1 x + a_0) = \varphi(a_n)\varphi(x)^n + \dots + \varphi(a_1)\varphi(x) + \varphi(a_0).$$

Siccome $\varphi(1) = 1$, allora $\varphi(a_i) = a_i$, e dunque $p \in \ker \varphi$ sse

$$0 = a_n(1 + \sqrt{2})^n + \dots + a_1(1 + \sqrt{2}) + a_0 = p(1 + \sqrt{2}).$$

A questo punto bisogna trovare il polinomio minimo di $1 + \sqrt{2}$, cioè un polinomio monico irriducibile che divide ogni polinomio che si annulla in $1 + \sqrt{2}$.

passo 1) Costruiamo un polinomio che si annulla in $1 + \sqrt{2}$,

passo 2) Mostriamo che questo polinomio è irriducibile,

passo 3) Mostriamo infine che ogni polinomio nel nucleo di φ è multiplo del primo polinomio trovato.

Procediamo.

passo 1) Chiamiamo $\alpha := 1 + \sqrt{2}$ per semplicità. Poiché

$$\alpha - 1 = \sqrt{2},$$

si ha

$$(\alpha - 1)^2 - 2 = 0.$$

Da cui il polinomio

$$p = (x - 1)^2 - 2 = x^2 - 2x - 1$$

si annulla in $\alpha = 1 + \sqrt{2}$.

passo 2) p è irriducibile in $\mathbb{Z}[x]$ perché le sue uniche due radici sono $1+\sqrt{2}$ e $1-\sqrt{2}$, entrambe non appartengono a $\mathbb{Z}$ ed è un polinomio di 2^o grado.

passo 3) Supponiamo per assurdo esista $q \in \ker\varphi$ che non sia multiplo di p. q non può essere di grado 0 o 1 per quanto visto nel passo 2. Quindi il grado di q deve essere 2 o più. In $\mathbb{Z}[x]$ si può dividere un polinomio di grado $\delta(q) = n$ per un polinomio monico di grado inferiore. Sia quindi

$$q = hp + r,$$

con resto $r \in \mathbb{Z}[x]$ di grado $\delta(r) = 0$ o $\delta(r) = 1$. Siccome sia p che q si annullano in $1+\sqrt{2}$, anche r dovrebbe, ma $\delta(r) \leq 1$, che è assurdo. ※

Esercizio 4. *Primo metodo*:

1) Siano $f, g \in \mathcal{I}$, e sia $h \in A[x]$.

$$(f+g)(a) = f(a) + g(a) \in I \implies (f+g) \in \mathcal{I},$$
$$(fh)(a) = f(a)h(a) \in I \implies (fh) \in \mathcal{I}.$$

Il primo perché I è chiuso per somma e il secondo perché $f(a) \in I$ e vale la proprietà divorante.

2) "I primo $\implies \mathcal{I}$ primo":

$$fg \in \mathcal{I} \implies f(a)g(a) \in I \implies f(a) \in I \vee g(a) \in I \implies f \in \mathcal{I} \vee g \in \mathcal{I}.$$

"$\mathcal{I}$ primo $\implies I$ primo":

$$\alpha\beta \in I \implies (x-a+\alpha)(x-a+\beta) \in \mathcal{I} \implies (x-a+\alpha) \in \mathcal{I} \vee (x-a+\beta) \in \mathcal{I} \implies \alpha \in I \vee \beta \in I.$$

Secondo metodo: Si considerino gli omomorfismi di anelli valutazione e proiezione canonica

$$\begin{aligned} ev_a : A[x] &\to A \\ f &\mapsto f(a) \end{aligned}$$

$$\begin{aligned} \pi : A &\to A/I \\ a &\mapsto [a] \end{aligned}$$

Si consideri inoltre la loro composizione $ev_a \circ \pi(f) = [f(a)]$, l'insieme $\mathcal{I}$ non è altro che il nucleo di questo omomorfismo. Da questo si può dedurre immediatamente che $\mathcal{I}$ è un ideale. Per i teoremi di omomorfismo invece si ha

$$A[x]/\mathcal{I} \cong A/I.$$

Da questo si osserva che il primo è un dominio se e solo se il secondo è un dominio, da cui il primo ideale è primo se e solo se lo è anche il secondo.

Esercizio 5. *Gruppo di ordine 33*: Studiamo i Sylow di G. Sia n_p il numero di p-Sylow di G. Per il terzo teorema di Sylow

$$\begin{cases} n_3 \equiv 1 \pmod 3 \\ n_3 \mid 11 \end{cases}$$

da cui $n_3 = 1$. E ancora

$$\begin{cases} n_{11} \equiv 1 \pmod{11} \\ n_{11} \mid 3 \end{cases}$$

da cui $n_{11} = 1$. Otteniamo quindi che $G = 3S \times 11S$.

Gruppo di ordine 77: Allo stesso modo di prima

$$\begin{cases} n_7 \equiv 1 \pmod 7 \\ n_7 \mid 11 \end{cases}$$

e

$$\begin{cases} n_{11} \equiv 1 \pmod{11} \\ n_{11} \mid 7 \end{cases}$$

E quindi $G = 7S \times 11S$.

Esercizio 6. Ricordiamo il gruppo Q_8 delle unità dei quaternioni è l'insieme

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

Equipaggiato con l'operazione

$$ij = k \quad jk = i \quad ki = j,$$

e

$$ji = -k \quad kj = -i \quad ik = -j.$$

I sottogruppi sono

$$H_0 = \{1\}$$
$$H_1 := \{1, -1\}$$
$$H_2^{(1)} := \{1, -1, i, -i\} \quad H_2^{(2)} := \{1, -1, j, -j\} \quad H_2^{(3)} := \{1, -1, k, -k\}$$
$$H_3 = Q_8.$$

Ricordiamo invece il gruppo D_4 il gruppo delle simmetrie del quadrato è il gruppo libero presentato

$$D_4 := \{s, r \mid s^2 = e, r^4 = e, srs = r^{-3}\}.$$

I sottogruppi di D_4 invece sono

$$H_0 := \{e\}$$
$$H_1^{(1)} := \{1, s\} \quad H_2^{(1)} := \{1, r^2\}$$
$$H_1^{(2)} := \{1, r^2, s, sr^2\} \quad H_2^{(2)} := \{1, r, r^2, r^3\}$$
$$H_3 = D_4$$

Esercizio 7. Sia a il generatore del gruppo C_6. Un omomorfismo φ da C_6 a $\mathcal{S}_3$ è univocamente determinato dall'immagine di a. Gli elementi di $\mathcal{S}_3$ sono

$$\{e, (12), (13), (23), (123), (132)\}$$

- Se $\varphi(a)$ ha struttura ciclica $()$, allora è l'omomorfismo banale,
- Se $\varphi(a)$ ha struttura ciclica (xx) allora l'immagine è il gruppo $\{e, \varphi(a)\}$,
- Se $\varphi(a)$ ha struttura ciclica (xxx) allora l'immagine è il gruppo $\{e, \varphi(a), \varphi(a)^2\}$.

Per quanto riguarda l'altra direzione il metodo è diverso.

Supponiamo di avere

$$\varphi : \mathcal{S}_3 \to C_6.$$

Si ha che $\ker \varphi \trianglelefteq \mathcal{S}_3$. Da teoria sappiamo che gli unici due sottogruppi normali di $\mathcal{S}_3$ sono

$$\{e\} \trianglelefteq \mathcal{S}_3 \quad \text{e} \quad \{e, (123), (132)\} =: N \trianglelefteq \mathcal{S}_3,$$

quindi se φ non è l'omomorfismo banale deve avere uno di questi due come nucleo.

Caso 1: $\ker \varphi = \{e\}$. L'omomorfismo è in realtà un isomorfismo. Ma questa cosa è impossibile perché $\mathcal{S}_3$ e C_6 non sono isomorfi.

Caso 2: $\ker \varphi = N$. Allora $\varphi((123)) = e$. Rimane solo da capire chi è $\varphi((12))$, infatti una volta deciso dove vanno i cicli (123) e (12), si sa come si comporta φ su ogni elemento di $\mathcal{S}_3$.

Osservazione. Siccome $o((12)) = 2$ e $(12) \notin \ker\varphi$, allora $o(\varphi((12))) = 2$. Dunque

$$\varphi((12)) = a^3.$$

Da cui si conclude che l'unico omomorfismo non banale da $\mathcal{S}_3$ in C_6 è l'omomorfismo

$$\begin{aligned} \varphi : \mathcal{S}_3 &\to C_6 \\ (12) &\mapsto a^3 \\ (123) &\mapsto e \end{aligned}$$

Esercizio 8. $\diamond$ Per dimostrare che è un sottogruppo delle bigezioni basta verificare che

$$\forall \varphi, \psi \in G, \varphi\psi^{-1} \in G.$$

Si ha che $\varphi(x) = ax + b$, $\psi(x) = cx + d$ e $\psi^{-1}(x) = c^{-1}x + c^{-1}d$. La loro composizione fa

$$\varphi(\psi^{-1}(x)) = \varphi(c^{-1}x + c^{-1}d) = ac^{-1}x + ac^{-1}d + b.$$

Poiché $ac^{-1} \in \mathbb{R}^*$ e $ac^{-1}d + b \in \mathbb{R}$, segue la tesi. La commutatività invece è falsa: prendendo ad esempio

$$\varphi(x) = 2x \quad \text{e} \quad \psi(x) = x + 2$$

si hanno $\varphi(\psi(x)) = 2x + 4$ e $\psi(\varphi(x)) = 2x + 2$.

$\diamond$ Sia φ elemento di T, e σ elemento di G. Il coniugio

$$\sigma^{-1}\varphi\sigma(x) = \sigma^{-1}(\varphi(\sigma(x))) = \sigma^{-1}(\varphi(ax + b)) = \sigma^{-1}(ax + b + t) = x + a^{-1}t$$

è una traslazione, pertanto $\sigma^{-1}T\sigma \subseteq T$.

A questo punto bisogna studiare il quoziente G/T. L'idea è che un elemento $g \in G$ è parametrizzato da due numeri $g = \mathbb{R}^*x + \mathbb{R}$, e a meno del parametro della traslazione, rimane solo $\mathbb{R}^*$. Formalizziamo questa intuizione. Consideriamo la funzione

$$\begin{aligned} \rho : G &\to \mathbb{R}^* \\ ax + b &\mapsto a \end{aligned}$$

1) È un omomorfismo: Siano $g = ax + b$ e $h = cx + d$.

$$\rho(g \circ h) = \rho(acx + ad + b) = ac = \rho(ax + b)\rho(cx + d) = \rho(g)\rho(h).$$

2) $\ker\rho = T$:

$$ax + b \in \ker\rho \iff a = 1 \iff ax + b \in T.$$

3) ρ è suriettiva: Sia $a \in \mathbb{R}^*$, si ha $ax \in G$ e $\rho(ax) = a$.

Dunque per i teoremi di omomorfismo $G/T \cong \mathbb{R}^*$.

$\diamond$ Sia

$$M = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \mid \alpha, \beta, \gamma \in \mathbb{R} \right\},$$

e sia

$$N = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{R}^*, y \in \mathbb{R} \right\}.$$

È di facile verifica che N è un sottogruppo di M. Vogliamo mostrare che $G \cong N$. Consideriamo la funzione

$$\begin{aligned} \vartheta : G &\to M \\ ax + b &\mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Verifichiamo sia un omomorfismo:

$$\vartheta(ax{+}b)\vartheta(cx{+}d) = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad + b \\ 0 & 1 \end{pmatrix} = \vartheta(acx{+}ad{+}b) = \vartheta((ax{+}c)\circ(cx{+}d)).$$

Inoltre siccome il nucleo di questo omomorfismo è banale, segue la tesi.