Algebra I - Soluzioni 5

26 Aprile

1 Esercizi

Esercizio 1. Per prima cosa si calcola che $\varphi(10) = 4$ e $\varphi(12) = 4$. Il sistema, allora, è equivalente a

$$\begin{cases} 7^0 x \equiv 1 \pmod{10} \\ x \equiv 5 \pmod{12} \end{cases}$$

Una soluzione quindi è

$$10t + 1 = x = 12s + 5$$

per $s, t \in \mathbb{Z}$. Si ha dunque

$$10t - 12s = 4$$

e questo si verifica per $t = 4$ e $s = 3$, da cui $x = 41$. Le soluzioni sono pertanto

$$x = 41 + mcm(10, 12)t = 41 + 60t, \qquad t \in \mathbb{Z}.$$

Esercizio 2. Per il teorema di classificazione dei gruppi abeliani finiti si ha che i gruppi abeliani sono prodotto diretto di gruppi ciclici. Per prima cosa si ha $240 = 2^5 \cdot 3 \cdot 5$. Da cui segue che

$$G = C_3 \times C_5 \times H$$

e H è un gruppo abeliano di ordine 16. I gruppi quindi sono

1) $C_3 \times C_5 \times C_2^4 = C_{30} \times C_2 \times C_2 \times C_2$
2) $C_3 \times C_5 \times C_4 \times C_2^2 = C_{60} \times C_2 \times C_2$
3) $C_3 \times C_5 \times C_4 \times C_4 = C_{60} \times C_4$
4) $C_3 \times C_5 \times C_8 \times C_2 = C_{120} \times C_2$
5) $C_3 \times C_5 \times C_{16} = C_{240}$

Esercizio 3. Come prima cosa osserviamo che, per l'abelianità,

$$(xy)^{o(x)o(y)} = (x^{o(x)})^{o(y)}(y^{o(y)})^{o(x)} = e,$$

e dunque $o(xy) \mid o(x)o(y)$.

Supponiamo ora $o(xy) < o(x)o(y)$. Procediamo per assurdo suddividendo in due casi:

Caso 1: $o(x) \nmid o(xy)$ e $o(y) \mid o(xy)$. Tuttavia in questo caso

$$e = (xy)^o(xy) = x^{o(xy)}y^{o(xy)} = x^{o(xy)},$$

ed è assurdo perché $o(x) \nmid o(xy)$ ※.

Caso 2: Sia $o(x) \nmid o(xy)$ che $o(y) \nmid o(xy)$. Sia d il minimo numero tale che $o(y) \mid o(xy)$, nello specifico

$$d = \frac{o(y)o(x)}{mcm(o(xy), o(x))}.$$

Ci si è ricondotti al *Caso 2)*, infatti $o(x) \nmid o(xy) \cdot d$, $o(y) \mid o(xy) \cdot d$ e

$$(xy)^{o(xy)\cdot d} = e.$$

Da cui segue l'assurdo anche in questo caso ※.

Segue la tesi.

- ◇ Consideriamo il gruppo $(\mathbb{Z}/12\mathbb{Z}, +)$ e gli elementi 2 e 4. Si ha $o(2) = 6$ e $o(4) = 3$, ma $o(8) = 3 \neq 18$.
- ◇ Consideriamo il gruppo $\mathcal{S}_3$ e gli elementi (12) e (123). $o((12)) = 2$ e $O((123)) = 3$, ma

$$o((12)(123)) = o((132)) = 3 \neq 6.$$

Nota: Può venir da pensare che in generale valga

$$o(xy) = mcm(o(x), o(y)),$$

e che questa formula si ricongiunga al prodotto semplice quando $mcm(x, y) = 1$. Ciò è falso. Per esempio sia C_{2pq} il gruppo ciclico di ordine $2pq$ con p e q due primi dispari distinti, x un generatore e siano $a := x^q$ e $b := x^p$. Si ha

$$o(a) = 2p \quad \text{e} \quad o(b) = 2q.$$

$mcm(o(a), o(b)) = 2pq$, ma $ab = x^{p+q}$ ha ordine al più (in realtà precisamente) pq, siccome $p + q$ è pari.

Esercizio 4. Sia $\sigma \in Z(\mathcal{S}_n)$. Supponiamo non sia l'identità, e sia $x \notin \mathrm{Fix}(\sigma)$, i.e. $x, z \in \{1, 2, \ldots, n\}$ e

$$\sigma.x = z \neq x.$$

Siccome σ è nel centro, allora presa la trasposizione (xy),

$$\sigma \circ (xy) = (xy) \circ \sigma,$$

da cui

$$\sigma.y = \sigma \circ (xy).x = (xy) \circ \sigma.x = (xy).z$$

Consideriamo $y \in \{1, 2, \ldots, n\}$, $y \neq x$, $y \neq z$. Può essere scelto questo y perché per ipotesi $n \geq 3$. Si ha

$$\sigma.y = (xy).z = z,$$

ma ciò è assurdo perché per ipotesi anche $\sigma.x = z$ ※. Segue che σ è l'identità e dunque il centro è banale.

Esercizio 5. Ricordiamo che

$$\mathcal{S}_3 = \{s, r \mid s^2 = e, r^3 = e, srs = r^2\},$$

cioè $\mathcal{S}_3$ è generato da (12) e (123) e l'unica relazione tra i due è che

$$(12)(123)(12) = (123)(123).$$

Un automorfismo

$$\sigma : \mathcal{S}_3 \to \mathcal{S}_3$$

preserva gli ordini, quindi può mandare (12) in (12), in (23) o in (13), mentre può mandare (123) in (123) o in (132). Poiché generano, un omomorfismo è univocamente determinato da queste scelte (però non tutte le scelte potrebbero definire un omomorfismo!). Segue che gli automorfismi sono al più 6.

Una formula nota di un gruppo G è che

$$G/Z(G) \cong \mathrm{Inn}(G),$$

cioè il gruppo quozientato al suo centro è isomorfo al gruppo degli automorfismi interni. Siccome $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$, si ha che

$$6 = |\mathrm{Inn}(\mathcal{S}_3)| \leq |\mathrm{Aut}(\mathcal{S}_3)| \leq 6$$

e dunque

$$\mathcal{S}_3 \cong \mathrm{Inn}(\mathcal{S}_3) \cong \mathrm{Aut}(\mathcal{S}_3).$$

Esercizio 6. Si cercano in primis due coefficienti che semplifichino la parte reale o la parte immaginaria, per esempio -3 e 2,

$$2(3+5i) - 3(2+3i) = 6 + 10i - 6 - 9i = i,$$

e poi si aggiusta ciò che rimane, in questo caso moltiplicando per $-i$ si ottiene 1. Componendo il tutto

$$3i \cdot (2+3i) - 2i \cdot (3+5i) = 1$$

Esercizio 7. Applicando l'algoritmo di Euclide si trova il massimo comun divisore.

$$\begin{aligned} p - x^2 q + q &= -x^4 + x^3 + x^2 - x =: r \\ q + xr + r &= 2x^3 - 2x =: s \\ r - \frac{1}{2}xs - \frac{1}{2}s &= 0 \end{aligned}$$

Dunque $x^3 - x$ è il massimo comun divisore. Gli ideali massimali che contengono questo ideale sono

$$x\mathbb{Q}[x], \quad (x-1)\mathbb{Q}[x] \quad \text{e} \quad (x+1)\mathbb{Q}[x].$$

Esercizio 8. Il polinomio f è irriducibile se e solo se lo è anche $3f$. Il polinomio

$$3f = 2x^3 - 9x^2 + 3x + 6$$

è irriducibile per Eisenstein applicato al primo p, segue che f è irriducibile, e quindi $\mathbb{Q}[x]/I$ è un campo.

Per l'inverso di $I + x$, cerchiamo un polinomio $g \in \mathbb{Q}[x]$ tale per cui

$$x \cdot g = p \cdot f + 1$$

con $p \in \mathbb{Q}[x]$. Preso

$$g = \frac{2}{3}x^2 - 3x + 1,$$

si nota che

$$f - xg = 2 \implies xg = f - 2.$$

Moltiplicando tutto per $-\dfrac{1}{2}$ si ha

$$x \cdot \left(-\frac{1}{2}g\right) = \left(-\frac{1}{2}\right) \cdot f + 1.$$

Da ciò segue che

$$(x+I)^{-1} = -\frac{1}{2}g + I.$$

Esercizio 9. Per prima cosa dimostriamo che N è un ideale. Siano $x, y \in N$ e $z \in A$. Siano inoltre $o(x)$ e $o(y)$ i due minimi interi per cui $x^{o(x)} = y^{o(y)} = 0$. Valgono

+)

$$(x+y)^{o(x)+o(y)} = \sum_{j=0}^{o(x)+o(y)} \binom{o(x)+o(y)}{j} x^{o(x)+o(y)-j} y^j$$

Questa è una sommatoria a termini tutti nulli perché a turno o $x^{o(x)+o(y)-j} = 0$ o $y^j = 0$. Dunque $x + y \in N$.

·)

$$(xz)^{o(x)} = x^{o(x)} z^{o(x)} = 0.$$

Quando $A = \mathbb{Z}/(12)$,

$$N = \{0, 6\},$$

infatti un numero in N deve avere tutti i fattori primi di 12 per far sì che ad una certa potenza 12 lo divida.

Dimostriamo ora che

$$N = \bigcap_{\mathfrak{p} \text{ primo}} \mathfrak{p}$$

per doppia inclusione.

Caso $\subseteq$: Sia $x \in N$, allora $x^n = 0$ per un qualche n. Sia $\mathfrak{p}$ un ideale primo, e sia k il più piccolo naturale tale per cui

$$x^k \in \mathfrak{p}.$$

$k < +\infty$ perché $x^n = 0 \in \mathfrak{p}$. Supponiamo $k > 1$,

$$x^k = x^{k-1} \cdot x \in \mathfrak{p}$$

e siccome $\mathfrak{p}$ è un ideale primo

$$x^{k-1} \in \mathfrak{p} \quad \vee \quad x \in \mathfrak{p},$$

assurdo per le ipotesi su k. Dunque $k = 1$ e $x \in \mathfrak{p}$. Per la generalità di x e $\mathfrak{p}$ segue

$$N \subseteq \bigcap \mathfrak{p}.$$

Caso $\supseteq$: Sia $f \notin N$ e sia

$$\Sigma := \{J \trianglelefteq A \mid f^m \notin J \quad \forall m \in \mathbb{N}\}$$

l'insieme di tutti gli ideali di A che schivano f e tutte le sue potenze. σ è parzialmente ordinato secondo l'inclusione e ogni catena

$$J_1 \subseteq J_2 \subseteq \ldots \subseteq J_n \subseteq \ldots$$

ammette $J := \bigcup J_k$ come maggiorante in Σ. Infatti

1) J è un ideale perché unione di ideali inclusi l'uno dentro l'altro.

2) $J \in \Sigma$: Supponiamo per assurdo $\exists m \mid f^m \in J$, allora $f^m \in J_k$ per un qualche k, assurdo ※.

Possiamo dunque applicare il Lemma di Zorn, e otteniamo che Σ ammette un maggiorante I. I è un ideale primo. Per assurdo siano $s, r \notin I$ e $sr \in I$. Per massimalità

$$I \subsetneq I + (s) \quad \text{e} \quad I \subsetneq I + (s),$$

cioè esistono m_s e m_r tali che

$$f^{m_s} \in I + (s) \quad \text{e} \quad f^{m_r} \in I + (r).$$

Ma allora

$$f^{m_s} f^{m_r} \in I + (sr) = I,$$

che è assurdo ※. Dunque abbiamo dimostrato che, se $f \notin N$, allora esiste un ideale primo I che non contiene f, e quindi

$$f \notin \bigcup_{\mathfrak{p} \text{ primo}} \mathfrak{p}.$$

Segue l'inclusione cercata.