Esercizi su gruppi, anelli e numeri interi (tratti dalle tracce d'esame)

Traccia del 25 settembre 2020

(a) Si ha $\mathrm{Im}\varphi = \langle [n]_{n^2} \rangle \times \left\langle \left[n^2 \right]_{n^3} \right\rangle$, prodotto diretto di sottogruppi ciclici di $\mathbb{Z}_{n^2}$ e $\mathbb{Z}_{n^3}$, rispettivamente, i cui ordini sono pari ai periodi dei rispettivi generatori, ossia $o([n]_{n^2}) = n$ e $o\left(\left[n^2 \right]_{n^3}\right) = n$. Pertanto $|\mathrm{Im}\varphi| = n^2$.

(b) Per ogni $a, b \in \mathbb{Z}$, si ha che $([a]_{n^2}, [b]_{n^3}) \in \psi^{-1}([0]_n, [0]_n)$ se e solo se $n|a$ ed $n|b$, ossia se e solo se $([a]_{n^2}, [b]_{n^3}) \in \langle [n]_{n^2} \rangle \times \langle [n]_{n^3} \rangle$. Questo sottogruppo ha ordine $n \cdot n^2 = n^3$.

(c) L'applicazione ϑ non è iniettiva, dato che gli elementi distinti $([n]_{n^2}, [0]_{n^3})$ e $([0]_{n^2}, [0]_{n^3})$ vengono inviati nello stesso elemento $([0]_{n^2}, [0]_{n^3})$.

Traccia dell'11 settembre 2020

(a) Un omomorfismo siffatto è $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_5 \times \mathbb{Z}_6$, definito ponendo, per ogni $a \in \mathbb{Z}$, $\varphi([a]_4) = ([0]_5, [3a]_6)$. Si verificano facilmente la buona definizione e la conservazione della somma e del prodotto. L'omomorfismo è non nullo in quanto alla sua immagine appartiene l'elemento $([0]_5, [3]_6)$.

(b) Sia $\varphi : \mathbb{Z}_5 \to \mathbb{Z}_4 \times \mathbb{Z}_6$ un omomorfismo di gruppi. Sia $\varphi([1]_5) = (\alpha, \beta)$. Allora, dato che φ conserva i multipli, si avrà, per ogni $a \in \mathbb{Z}$,

(1) $\varphi([a]_5) = \varphi(a[1]_5) = a\varphi([1]_5) = a(\alpha, \beta) = (a\alpha, a\beta)$.

In particolare, per $a = 5$, si avrà

$(5\alpha, 5\beta) = \varphi([0]_5) = ([0]_4, [0]_6)$,

dove l'ultima uguaglianza è dovuta al fatto che un omomorfismo di gruppi additivi conserva lo zero. Ma allora, in $\mathbb{Z}_4$, $[5]_4\alpha = \alpha = [0]_4$, e, in $\mathbb{Z}_6$, $[5]_6\beta = -\beta = [0]_6$. Alla luce di (1), ne consegue che φ invia ogni elemento di $\mathbb{Z}_5$ nello zero di $\mathbb{Z}_4 \times \mathbb{Z}_6$, ossia è l'omomorfismo nullo.

(c) Supponiamo per assurdo che esista $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_5 \to \mathbb{Z}_6$ omomorfismo di gruppi surgettivo. Allora, in particolare, esiste $(\alpha, \beta) \in \mathbb{Z}_4 \times \mathbb{Z}_5$ tale che $\varphi(\alpha, \beta) = [1]_6$. Ma, dato che φ conserva lo zero e i multipli, si deduce che

$[0]_6 = \varphi(20\alpha, 20\beta) = 20\varphi(\alpha, \beta) = 20[1]_6 = [2]_6$, assurdo.

Traccia del 17 febbraio 2020

(a) Le coppie (m, n) cercate sono tutte e solo quelle per le quali vale la seguente condizione:

(*) per ogni $a, a', b, b' \in \mathbb{Z}$, $m|a - a'$ e $n|b - b' \implies m|ab - a'b'$.

Si noti che, per ogni $a, a', b, b' \in \mathbb{Z}$, $ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b')$.
Poiché, in base alla premessa di (*), il primo addendo è sempre divisibile per m, la (*) si può riformulare equivalentemente come segue:

(*)′ per ogni $a, a', b, b' \in \mathbb{Z}$, $m|a - a'$ e $n|b - b' \implies m|a'(b - b')$.

Data l'arbitrarietà di a' (che, in maniera del tutto indipendente da b, b', varia in tutto $\mathbb{Z}$), la condizione si può ancora riformulare nella forma:

(*)'' per ogni $a, a', b, b' \in \mathbb{Z},\ m|a-a'$ e $n|b-b' \implies m|b-b'$.

Infine, poiché la premessa su a, a' è del tutto ininfluente ai fini della conclusione, si giunge alla seguente formulazione:

(*)''' per ogni $b, b' \in \mathbb{Z},\quad n|b-b' \implies m|b-b'$,

ovvero, semplificando la scrittura:

(**) per ogni $x \in \mathbb{Z},\quad n|x \implies m|x$.

In conclusione, la condizione (*) vale se e solo se ogni multiplo di n è anche multiplo di m. Ciò avviene se e solo se $m|n$. Quindi le coppie cercate sono tutte e sole quelle della forma (m, qm), al variare di q in $\mathbb{Z}$.

(b) L'applicazione è ben definita, in quanto l'apparente dipendenza dalla scelta di a, b svanisce non appena si riscrive la sua definizione nella maniera seguente:

per ogni $(\alpha, \beta) \in \mathbb{Z}_{18} \times \mathbb{Z}_{18},\ \ \psi(\alpha, \beta) = 2\alpha\beta$.

Siano ora $a, b \in \mathbb{Z}$. Allora $[2ab]_{18} = [0]_{18}$ se e solo se $9|ab$. Ciò avviene se e solo se uno tra a e b è multiplo di 9, oppure entrambi sono multipli di 3. Le coppie $([a]_{18}, [b]_{18})$ verificanti la prima condizione sono $([0]_{18}, [0]_{18}),\ \ ([9]_{18}, [9]_{18}),\ ([0]_{18}, [9]_{18})$ e $([9]_{18}, [0]_{18})$, insieme alle restanti coppie della forma $([9]_{18}, \beta)$ o $([0]_{18}, \beta)$ o $(\alpha, [9]_{18})$ o $(\alpha, [0]_{18})$: il loro numero è dunque $4 + 4(18-2) = 68$. Le restanti coppie verificanti la seconda condizione si ottengono abbinando due elementi scelti tra $[3]_{18}$, $[6]_{18}$, $[12]_{18}$ e $[15]_{18}$, il che è possibile in esattamente $4^2 = 16$ modi.
In conclusione, il numero delle coppie considerate è $68 + 16 = 84$. Questo è $|\psi^{-1}([0]_{18})|$.

Per il secondo quesito, si noti che la congruenza lineare $2x \equiv 9 \pmod{18}$ non ha soluzione. Quindi l'insieme $\psi^{-1}([9]_{18})$ è vuoto. La sua cardinalità è zero.

<u>Traccia del 31 gennaio 2020</u>

(a) Due sottonanelli siffatti sono $\mathbb{Z}_5 \times \{[0]_6\}$ e $\{[0]_5\} \times \{[0]_6,\ [3]_6\}$, ottenuti come prodotti diretti di sottoanelli dei fattori diretti. Il primo sottoanello è integro in quanto n quanto isomorfo a $\mathbb{Z}_5$, il secondo è integro in quanto isomorfo a $\mathbb{Z}_2$.

(b) La buona definizione e la conservazione della somma sono di facile verifica. Consideriamo ora la conservazione del prodotto. Siano $a, b, c, d \in \mathbb{Z}$. Si ha

$$\varphi(([a]_5, [b]_6))([c]_5, [d]_6)) = \varphi([ac]_5, [bd]_6) = [6ac + 25bd]_{30},$$

mentre

$$\varphi([a]_5, [b]_6)\varphi([c]_5, [d]_6) = [6a + 25b]_{30}[6c + 25d]_{30} = [36ac + 150(bc + ad) + 625bd]_{30} = [6ac + 25bd]_{30},$$

dove l'ultima uguaglianza deriva dal fatto che $36 \equiv 6,\ 150 \equiv 0,\ 625 \equiv 25 \pmod{30}$.
Ciò prova che φ è un omomorfismo di anelli.

(c) Poiché i numeri 5 e 6 sono coprimi, allora, come risulta dalla dimostrazione del Teorema Cinese del Resto (seconda formulazione), ogni

elemento di $\mathbb{Z}_5 \times \mathbb{Z}_6$ può essere rappresentato nella forma $([a]_5, [a]_6)$, con $a \in \mathbb{Z}$. Dunque si può definire l'omomorfismo φ ponendo, per ogni $a \in \mathbb{Z}$, $\varphi([a]_5, [a]_6) = [31a]_{30} = [a]_{30}$. Quest'applicazione è chiaramente surgettiva, quindi bigettiva (essendo definita tra due insiemi finiti equipotenti). La sua inversa è l'applicazione

$\psi : \mathbb{Z}_{30} \to \mathbb{Z}_5 \times \mathbb{Z}_6$ tale che, per ogni $a \in \mathbb{Z}$, $\psi([a]_{30}) = ([a]_5, [a]_6)$.

Traccia del 15 gennaio 2020

(a) L'applicazione è ben definita se e solo se, per ogni $a, a' \in \mathbb{Z}$, se $n|a - a'$, allora $n^2|a + n - (a' + n) = a - a'$. Ossia: se e solo se, per ogni $h \in \mathbb{Z}$, se $n|\ h$, allora $n^2|h$. Non esiste un intero $n > 1$ siffatto: infatti per ogni intero $n > 1$, $n|n$, ma $n^2 \not| n$. Dunque l'insieme cercato è vuoto.

(b) L'applicazione φ è sempre un omomorfismo di gruppi ben definito, com'è facile verificare. Sarà un omomorfismo di anelli per tutti e soli i valori di n tali che, per ogni $a, b \in \mathbb{Z}$, si abbia $[nab]_{n^2} = \left[n^2 ab\right]_{n^2}$. Ora, la classe di congruenza a secondo membro è sempre $[0]_{n^2}$. Invece non è sempre $[0]_{n^2}$ la classe di congruenza a primo membro: ad esempio non lo è per $a = b = 1$, in quanto, come già osservato, $n^2 \not| n$. Ciò prova che φ non è mai un omomorfismo di anelli.

Traccia del 15 novembre 2019

(a) I valori di n cercati sono tutti e soli quelli per i quali vale la seguente condizione:

per ogni $a, a' \in \mathbb{Z}$, $n|a - a' \implies n^2|a^2 - a'^2$.

Ponendo $a = a' + hn$, la possiamo riscrivere nella forma seguente:

per ogni $a', h \in \mathbb{Z}, n^2|hn(2a' + hn)$, ove la relazione di divisibilità equivale a $n|2a'h$. Questa è verificata universalmente se e solo se $n = 2$: questo è infatti l'unico intero maggiore di 1 che divida ogni numero pari.

(b) Gli anelli considerati non sono isomorfi, in quanto non sono isomorfi i rispettivi gruppi additivi. Infatti il primo possiede un elemento di periodo n^3 (ovvero $([0]_n, [1]_{n^3})$), mentre nel secondo ogni elemento ha periodo al più n^2.

(c) Si ha $\mathrm{Ker}\psi = \langle \left[n^2\right]_{n^3} \rangle$, gruppo ciclico di ordine n. Inoltre $\mathrm{Im}\psi = \langle ([1]_n, [1]_{n^2}) \rangle$, gruppo ciclico di ordine n^2.

Traccia del 25 settembre 2019

(a) Se $3|n$, allora certamente $9|N$. Supponiamo dunque che $3 \not| n$. Allora, in base al Teorema di Eulero, essendo 9 coprimo con n, si ha $n^{\phi(9)} \equiv 1 \pmod 9$, ove $\phi(9) = 6$. Quindi, per tali valori di n, per ogni intero positivo a, n^a è congruo, $\mathrm{mod}\ 9$, a n^r, essendo r il resto della divisione di a per 6. Pertanto

$$N \equiv n^3 + 3n^2 - 4n = n\left(n^2 + 3n - 4\right) = n(n+4)(n-1) \pmod 9.$$

Ora, poiché per ipotesi $3 \not| n, N$ è dunque divisibile per 9 se e solo se il fattore 3 compare almeno due volte nel prodotto $(n+4)(n-1)$. Si noti che i due fattori non possono essere entrambi multipli di 3, perché differiscono di 5. Quindi la condizione voluta si ha se e solo se uno dei due è multiplo di 9. Di conseguenza, i valori di n cercati sono quelli aventi una delle seguenti tre forme:

$n = 3k, \quad n = 9k - 4, \quad n = 9k + 1$ (con $k \in \mathbb{Z}$).

(b) Il ragionamento è simile al precedente, con la necessaria variante dovuta al fatto che $\phi(25) = 20$. Ai valori di n multipli di 5, per i quali è certamente vero che $25|N$, si devono aggiungere quelli per i quali 5 divide

$n^3 + 3n^2 - 4n = n(n+4)(n-1)$

(Si noti che gli esponenti sono gli stessi di prima, ma solo in virtù di una circostanza particolare: sono infatti uguali i loro resti $\mathrm{mod}\ 6$ e $\mathrm{mod}\ 20$).
Poiché i due fattori $(n+4)$ e $(n-1)$ differiscono di 5, uno dei due è divisibile per 5 se e solo se lo è l'altro, ed in tal caso il prodotto è divisibile per 25. Quindi i valori di n cercati sono quelli aventi una delle seguenti due forme:

$n = 5k, \quad n = 5k + 1$ (con $k \in \mathbb{Z}$).

Traccia del 10 settembre 2019

(a) Si ha notoriamente un sottoanello quando $\alpha \in \mathbb{Z}$. Sia ora $\alpha \in \mathbb{Q}$ tale che $\langle \alpha \rangle$ sia un sottoanello di $\mathbb{Q}$. Possiamo supporre che sia $\alpha \neq 0$. Essendo il sottoanello chiuso rispetto al prodotto, vi dovrà appartenere α^2, ossia esisterà un intero k tale che $\alpha^2 = k\alpha$. Ma allora $\alpha = k$, e quindi $\alpha \in \mathbb{Z}$. Ciò prova che $\langle \alpha \rangle$ è un sottoanello di $\mathbb{Q}$ se e solo se $\alpha \in \mathbb{Z}$.

(b) Sia $a \in \mathbb{Z}$ tale che $\varphi\left(\frac{1}{n}\right) = [a]_n$. Allora $\mathrm{Im}\varphi = \langle [a]_n \rangle$. Dovendo questo sottogruppo essere uguale a $\mathbb{Z}_n$, sarà a coprimo con n. Sia ora $k \in \mathbb{Z}$. Allora $\frac{k}{n} \in \mathrm{Ker}\varphi$ se e solo se $[ka]_n = [0]_n$. A fronte della coprimalità tra a ed n ciò vale se e solo se $n|k$, ossia se e solo se $\frac{k}{n} \in \mathbb{Z}$.

(c) Poniamo $\varphi\left(\frac{1}{6}\right) = [2]_6$: aver scelto 2, non coprimo con 6, serve a impedire la surgettività. Per ogni $k \in \mathbb{Z}$ sarà dunque necessariamente $\varphi\left(\frac{k}{6}\right) = [2k]_6$. Questo è un omomorfismo di gruppi al cui nucleo appartiene il numero non intero $\frac{3}{6} = \frac{1}{2}$.