ALGEBRA PER INFORMATICA 2020-21

FOGLIO DI ESERCIZI 11:
SOLUZIONE DI ALCUNI ESERCIZI

Esercizio 1. Si consideri il seguente sottoinsieme dei numeri complessi:

$$Z = \{a + ib : \ a, b \in \mathbb{Z}\}$$

con le operazioni di somma e prodotto indotte da $\mathbb{C}$. Gli elementi di Z vengono chiamati *interi di Gauss*.

(1) $(Z, +)$ è un sottomonoide di $(\mathbb{C}, +)$? È un sottogruppo?
(2) $(Z \setminus \{0\}, \cdot)$ è un sottomonoide di $(\mathbb{C}^*, \cdot)$? È un sottogruppo?

Soluzione.

(1) $(Z, +)$ è un sottogruppo, e quindi anche un sottomonoide, di $(\mathbb{C}, +)$.
(2) $(Z \setminus \{0\}, \cdot)$ è un sottomonoide di $(\mathbb{C}^*, \cdot)$, ma non è un sottogruppo. Ad esempio si ha che $2 \in Z$, ma $2^{-1} = \frac{1}{2} \notin Z$.

Esercizio 2. Stabilire se le seguenti coppie di gruppi sono isomorfe oppure no e in caso affermativo esibire un isomorfismo di gruppi:

(1) $(\mathbb{R}, +)$ e $(\mathbb{R}_{>0}, \cdot)$;
(2) $(\mathrm{U}(\mathbb{Z}_{36}), \cdot)$ e $(\mathbb{Z}_{36}, +)$;
(3) $(\mathrm{U}(\mathbb{Z}_7), \cdot)$ e $(\mathbb{Z}_6, +)$;
(4) $(\mathrm{U}(\mathbb{Z}_8), \cdot)$ e $(\mathbb{Z}_4, +)$;
(5) $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$ e $(\mathbb{Z}_6, +)$;
(6) $(\mathbb{Z}_3 \times \mathbb{Z}_3, +)$ e $(\mathbb{Z}_9, +)$;
(7) $(\mathbb{R} \times \mathbb{R}, +)$ e $(\mathbb{C}, +)$;
(8) $(\mathbb{R}^* \times \mathbb{R}^*, \cdot)$ e $(\mathbb{C}^*, \cdot)$;
(9) $(\mathbb{Q}, +)$ e $(\mathbb{R}, +)$.

Soluzione.

(1) Sì, un isomorfismo di gruppi è dato dalla funzione esponenziale $\exp : \mathbb{R} \to \mathbb{R}_{>0}$.
(2) No, perché $\mathbb{Z}_{36}$ ha ordine 36 mentre $\mathrm{U}(\mathbb{Z}_{36})$ ha ordine $\varphi(36) \neq 36$.
(3) Sì, un isomorfismo di gruppi è dato da $\varphi : \mathbb{Z}_6 \to \mathrm{U}(\mathbb{Z}_7)$ tale che $\varphi(x) = 3^x$.
(4) No, perché $\mathrm{U}(\mathbb{Z}_8) = \{1, 3, 5, 7\}$ non ha nessun elemento di ordine 4, mentre $\mathbb{Z}_4$ sì.
(5) Sì, un isomorfismo di gruppi è dato da $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ tale che $\varphi(1) = (1, 1)$.
(6) No, perché $\mathbb{Z}_3 \times \mathbb{Z}_3$ non ha nessun elemento di ordine 9, mentre $\mathbb{Z}_9$ sì.
(7) Sì, un isomorfismo di gruppi è dato da $\varphi : \mathbb{R} \times \mathbb{R} \to \mathbb{C}$ tale che $\varphi(a, b) = a + ib$.
(8) No, perché $\mathbb{C}^*$ ha un elemento di ordine 4, ad esempio i, mentre $\mathbb{R}^* \times \mathbb{R}^*$ non ha nessun elemento di ordine 4. Infatti $\nexists (a, b) \in \mathbb{R}^* \times \mathbb{R}^*$ tale che $(a^4, b^4) = (1, 1)$ e $(a^2, b^2) \neq (1, 1)$.
(9) No, perché $\mathbb{Q}$ e $\mathbb{R}$ non sono equipotenti, quindi non esiste nessuna bigezione tra i due insiemi e in particolare nessun isomorfismo.

Esercizio 3. Determinare tutti i sottogruppi di $(\mathbb{Z}_8,+)$ e tutti i sottogruppi di $(\mathbb{Z}_7,+)$.

Soluzione. I sottogruppi di $\mathbb{Z}_8$ sono: $\{0\}$, $\{0,4\}$, $\{0,2,4,6\}$, $\mathbb{Z}_8$.
I sottogruppi di $\mathbb{Z}_7$ sono: $\{0\}$, $\mathbb{Z}_7$.

Esercizio 5. Stabilire per quali $k \in \mathbb{Z}$ la funzione $f_k : \mathbb{Z} \to \mathbb{Z}$ definita da $f_k(n) = 2n+k$ è un omomorfismo di gruppi additivi[1]. Per quali k è un isomorfismo?

Soluzione. Affinchè f_k sia un omomorfismo di gruppi si deve avere $f_k(0) = 0$. Questo implica $0 = f_k(0) = 2 \cdot 0 + k = k$, cioè $k = 0$. E' facile verificare che $f_0(a+b) = 2(a+b) = 2a+2b = f_0(a) + f_0(b)$, quindi f_0 è un omomorfismo di gruppi. Non si tratta di un isomorfismo, perché f_0 non è surgettiva. Ad esempio $f_0^{-1}(1) = \emptyset$.

Esercizio 9. Si consideri la funzione valore assoluto $f(x) = |x|$.

(1) Stabilire se f è un omomorfismo di gruppi $f : (\mathbb{R},+) \to (\mathbb{R},+)$ e in caso affermativo determinarne il nucleo e l'immagine.
(2) Stabilire se f è un omomorfismo di gruppi $f : (\mathbb{R}^*,\cdot) \to (\mathbb{R}^*,\cdot)$ e in caso affermativo determinarne il nucleo e l'immagine.

Soluzione.

(1) Non si tratta di un omomorfismo di gruppi perché $f(1+(-1)) = f(0) = |0| = 0$, ma $f(1) + f(-1) = |1| + |-1| = 1+1 = 2$.
(2) f è un omomorfismo di gruppi perché $|1| = 1$ e $|a \cdot b| = |a| \cdot |b|$ per ogni $a, b \in \mathbb{R}^*$. Il nucleo di f è
$$\ker f = \{x \in \mathbb{R}^* : \ |x| = 0\} = \{0\}.$$
L'immagine di f è $\mathbb{R}_{\geq 0}$.

Esercizio 10. Siano $f, g : \mathbb{Z}_{36} \to \mathbb{Z}_{36}$ le funzioni date da $f(\overline{x}) = 2\overline{x}$ e $g(\overline{x}) = 7\overline{x}$. Determinare se f e g sono omomorfismi di gruppi. In caso affermativo, determinarne il rispettivo nucleo e stabilire se si tratta di isomorfismi.

Soluzione. Si verifica facilmente che sia f che g sono omomorfismi di gruppi. La funzione g è un isomorfismo, l'omomorfismo inverso è dato da $g^{-1}(\overline{x}) = \overline{7}^{-1}\overline{x}$, dove $\overline{7}^{-1}$ è l'inverso della classe di 7 in $\mathbb{Z}_{36}$. Tale inverso esiste perché $\mathrm{MCD}(7,36) = 1$. Al contrario $\overline{2}$ non è invertibile in $\mathbb{Z}_{36}$ perché $\mathrm{MCD}(2,36) = 2 \neq 1$. Pertanto l'omomorfismo f di moltiplicazione per $\overline{2}$ risulta non iniettivo in quanto $f(\overline{18}) = \overline{2} \cdot \overline{18} = \overline{36} = \overline{0} = f(\overline{0})$. Quindi f non è un isomorfismo.

I nuclei sono $\ker g = \{\overline{0}\}$ e
$$\ker f = \{\overline{x} \in \mathbb{Z}_{36} : \ \overline{2}\overline{x} = \overline{0}\} = \{\overline{0}, \overline{18}\},$$
dove gli elementi di $\ker f$ sono stati determinati risolvendo l'equazione diofantea $2x = 0 + 36k$ e prendendo le relative classi delle soluzioni.

Esercizio 12. Sia $G = \mathbb{Z}_3 \times S_3$, dove S_3 è il gruppo delle permutazioni di un insieme di 3 elementi (vedi esercizio 4).

(1) Qual è l'ordine di G? È abeliano?

[1] Cioè un omomorfismo $f_k : (\mathbb{Z},+) \longrightarrow (\mathbb{Z},+)$

(2) Determinare, se possibile, un sottogruppo di ordine 8 e uno di ordine 9 di G.

Soluzione.

(1) Abbiamo $|\mathbb{Z}_3| = 3$ e $|S_3| = 3! = 6$, pertanto l'ordine di G è $|G| = 3 \cdot 6 = 18$. Vediamo che G non è un gruppo abeliano. Se $\varphi, \psi \in S_3$ sono le funzioni tali che $\varphi(1) = 2$, $\varphi(2) = 1$, $\varphi(3) = 3$ e $\psi(1) = 2$, $\psi(2) = 3$, $\psi(3) = 1$, si ha $\varphi \circ \psi \neq \psi \circ \varphi$. Pertanto si ha

$$(0, \varphi) *_G (0, \psi) = (0, \varphi \circ \psi) \neq (0, \psi \circ \varphi) = (0, \psi) *_G (0, \varphi),$$

quindi G non è abeliano.

(2) Se H è un sottogruppo di G, per il teorema di Lagrange, l'ordine di H è un divisore di $|G| = 18$. Perciò non esiste un sottogruppo di ordine 8 di G. Un sottogruppo di ordine 9 è dato da

$$\begin{aligned} H &= \mathbb{Z}_3 \times \{\mathrm{Id}, \psi, \psi^2\} \\ &= \{(0, \mathrm{Id}), (0, \psi), (0, \psi^2), (1, \mathrm{Id}), (1, \psi), (1, \psi^2), (2, \mathrm{Id}), (2, \psi), (2, \psi^2)\}. \end{aligned}$$