Alcuni esercizi risolti di **MATEMATICA DISCRETA**
C.L. **Informatica**

1. Sia $\oplus : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ la legge di composizione interna su $\mathbb{Z}$ così definita:

$$\forall x, y \in \mathbb{Z},\ \ x \oplus y = x + y + 2.$$

a) Verificare che $\oplus$ è associativa

b) determinare l'elemento neutro della struttura $(\mathbb{Z}, \oplus)$

c) determinare l'elemento opposto di ogni elemento di $\mathbb{Z}$ rispetto alla legge di composizione $\oplus$

d) verificare che $(\mathbb{Z}, \oplus)$ è un gruppo abeliano

e) (*) usando il principio di induzione completa, verificare che per ogni $n \in \mathbb{N}$ e per ogni $x \in \mathbb{Z}$ il multiplo $n \cdot x$ di x secondo n rispetto a $\oplus$ è:
$$n \cdot x = nx + 2n - 2; \tag{1}$$

f) (*) verificare che (1) vale per ogni $n \in \mathbb{Z}$ e per ogni $x \in \mathbb{Z}$

g) (*) verificare che $(\mathbb{Z}, \oplus)$ è ciclico, in quanto generato da -1.

Soluzione

1a) Si ha $\forall x, y, z \in \mathbb{Z}$

$$\begin{aligned}(x \oplus y) \oplus z &= (x + y + 2) \oplus z = (x + y + 2) + z + 2 = x + y + z + 4 \\ x \oplus (y \oplus z) &= x \oplus (y + z + 2) = x + (y + z + 2) + 2 = x + y + z + 4,\end{aligned}$$

da cui segue l'associatività della struttura.

1b) Si deve cercare un elemento $e \in \mathbb{Z}$ tale che $\forall x \in \mathbb{Z}\ \ x \oplus e = e \oplus x = x$. Ponendo $x \oplus e = x$ si ha
$$x + e + 2 = x$$
e quindi $e = -2$. Poichè si ha anche $(-2) \oplus x = -2 + x + 2 = x$, $\forall x \in \mathbb{Z}$, l'elemento neutro della struttura algebrica $(\mathbb{Z}, \oplus)$ esiste ed è proprio -2.

1c) Fissato $x \in \mathbb{Z}$, si deve cercare un elemento $x' \in \mathbb{Z}$ tale che $x \oplus x' = x' \oplus x = -2$. Si pone $x \oplus x' = -2$, ottenendo

$$x + x' + 2 = -2$$

da cui si ottiene $x' = -x - 4$. Poichè risulta $x' \oplus x = -x + x - 4 + 2 = -2$, certamente x', che si indicherà con $\ominus x$, è l'opposto di x, cioè

$$\ominus x = -x - 4.$$

Quindi, $\forall x \in \mathbb{Z}\ \exists\ (\ominus x) = -x - 4 \in \mathbb{Z}$ tale che $x \oplus (\ominus x) = (\ominus x) \oplus x = -2$

1d) Basta provare la commutatività di $\oplus$. Infatti si ha:

$$\forall x, y \in \mathbb{Z}\ \ x \oplus y = x + y + 2 = y + x + 2 = y \oplus x.$$

1e) Per $n = 0$, risulta, dalla definizione di multiplo secondo n,

$$0 \cdot x = -2$$

in quanto -2 è l'elemento neutro, e $nx + 2n - 2 = -2$, quando $n = 0$. Si suppone che (1) sia vera: si vuol provare che allora:

$$(n+1) \cdot x = (n+1)x + 2(n+1) - 2.$$

Infatti

$$(n{+}1){\cdot}x = n{\cdot}x{\oplus}x = n{\cdot}x{+}x{+}2 = (nx{+}2n{-}2){+}x{+}2 = (n{+}1)x{+}2(n{+}1){-}2.$$

1f) Per ogni $n \in \mathbb{Z}$, $n \leq -1$ e per ogni $x \in \mathbb{Z}$, essendo $-n > 0$ si ha:

$$n{\cdot}x = \ominus\big((-n){\cdot}x\big) = \ominus(-nx{+}2(-n){+}2) = -(-nx{-}2n{+}2){-}4 = nx{+}2n{-}2.$$

1g) Da (1) si sa che per ogni $n \in \mathbb{Z}$

$$n \cdot (-1) = n(-1) + 2n - 2 = -n + 2n - 2 = n - 2.$$

Sia, ora, $m \in \mathbb{Z}$. Certamente $m = (m+2) - 2$ e quindi, posto $n = m + 2$, si ha $m = n \cdot (-1)$, ovvero

$$\forall m \in \mathbb{Z} \ \Rightarrow \ \exists\, n \in \mathbb{Z} \text{ tale che } m = n \cdot (-1),$$

cioè ogni elemento m di $\mathbb{Z}$ è multiplo di -1 secondo l'intero $n = m + 2$.

2. Si consideri il gruppo $(\mathbb{Z}_{11}^*, \cdot)$.
   (a) Determinare un generatore di $(\mathbb{Z}_{11}^*, \cdot)$
   (b) calcolare l'ordine di ogni elemento di $\mathbb{Z}_{11}^*$
   (c) determinare i sottogruppi di $(\mathbb{Z}_{11}^*, \cdot)$

Soluzione

2a) $\mathbb{Z}_{11}^* = \{[1]_{11}, [2]_{11}, [3]_{11}, [4]_{11}, [5]_{11}, [6]_{11}, [7]_{11}, [8]_{11}, [9]_{11}, [10]_{11}\}$.Poichè $|\mathbb{Z}_{11}^*| = 10$, in virtù del Teorema di Lagrange, gli ordini dei suoi elementi possono essere $1, 2, 5, 10$. Si verifica se 2 è un generatore:

$$\begin{aligned}
[2]_{11}^2 &= [4]_{11} \\
[2]_{11}^3 &= [8]_{11} \\
[2]_{11}^4 &= [16]_{11} = [5]_{11} \\
[2]_{11}^5 &= [2]_{11}^4 \cdot [2]_{11} = [5]_{11} \cdot [2]_{11} = [10]_{11}
\end{aligned}$$

allora, poichè $\mid [2]_{11} \mid \neq 2$ e $\mid [2]_{11} \mid \neq 5$, sicuramente 2 è un generatore (come osservato prima, non ci sono altre possibilità).

2b) Si continua con l'elevamento di $[2]_{11}$ alle restanti potenze, così tutti gli elementi di $\mathbb{Z}_{11}^*$ saranno espressi come potenza di $[2]_{11}$.

$$\begin{aligned}
[2]_{11}^6 &= [2]_{11}^5 \cdot [2]_{11} = [10]_{11} \cdot [2]_{11} = [20]_{11} = [9]_{11} \\
[2]_{11}^7 &= [2]_{11}^6 \cdot [2]_{11} = [9]_{11} \cdot [2]_{11} = [18]_{11} = [7]_{11} \\
[2]_{11}^8 &= [2]_{11}^7 \cdot [2]_{11} = [7]_{11} \cdot [2]_{11} = [14]_{11} = [3]_{11} \\
[2]_{11}^9 &= [2]_{11}^8 \cdot [2]_{11} = [3]_{11} \cdot [2]_{11} = [6]_{11} \\
[2]_{11}^{10} &= [2]_{11}^9 \cdot [2]_{11} = [6]_{11} \cdot [2]_{11} = [12]_{11} = [1]_{11}.
\end{aligned}$$

Quindi si ha:

$$\mathbb{Z}_{11}^* = \{[1]_{11} = [2]_{11}^0, [2]_{11}, [3]_{11} = [2]_{11}^8, [4]_{11} = [2]_{11}^2, [5]_{11} = [2]_{11}^4,$$

$$[6]_{11} = [2]_{11}^9, [7]_{11} = [2]_{11}^7, [8]_{11} = [2]_{11}^3, [9]_{11} = [2]_{11}^6, [10]_{11} = [2]_{11}^5\}.$$

A questo punto è sufficiente applicare la formula generale per un gruppo ciclico $(G, \cdot)$ generato da un elemento g

$$|g^h| = \frac{n}{M.C.D(n,h)}.$$

Si ha:

$$\begin{aligned}
\mid [3]_{11} \mid &= \mid [2]_{11}^8 \mid = \frac{10}{M.C.D(10,8)} = \frac{10}{2} = 5 \\
\mid [4]_{11} \mid &= \mid [2]_{11}^2 \mid = \frac{10}{M.C.D(10,2)} = \frac{10}{2} = 5 \\
\mid [5]_{11} \mid &= \mid [2]_{11}^4 \mid ; = \frac{10}{M.C.D(10,4)} = \frac{10}{2} = 5 \\
\mid [6]_{11} \mid &= \mid [2]_{11}^9 \mid = \frac{10}{M.C.D(10,9)} = \frac{10}{1} = 10 \\
\mid [7]_{11} \mid &= \mid [2]_{11}^7 \mid = \frac{10}{M.C.D(10,7)} = \frac{10}{1} = 10 \\
\mid [8]_{11} \mid &= \mid [2]_{11}^3 \mid = \frac{10}{M.C.D(10,3)} = \frac{10}{1} = 10 \\
\mid [9]_{11} \mid &= \mid [2]_{11}^6 \mid = \frac{10}{M.C.D(10,6)} = \frac{10}{2} = 5 \\
\mid [10]_{11} \mid &= \mid [2]_{11}^5 \mid = \frac{10}{M.C.D(10,5)} = \frac{10}{5} = 2.
\end{aligned}$$

Si noti che sono generatori di $\mathbb{Z}_{11}^*$, oltre a $[2]_{11}$, anche $[6]_{11}, [7]_{11}, [8]_{11}$. Naturalmente, come per tutti i gruppi, c'è l'elemento neutro $[1]_{11}$ che è l'unico di ordine 1.

2c) Poichè il gruppo in esame è ciclico, ogni suo sottogruppo è ciclico. Inoltre, per il Teorema inverso del Teorema di Lagrange per i gruppi ciclici, per ogni divisore h di 10 c'è un unico sottogruppo che ha ordine h. Allora esiste un unico sottogruppo di ordine 2, un unico di ordine 5, oltre a quello banale $< [1]_{11} >= \{[1]_{11}\}$ e tutto $\mathbb{Z}_{11}^*$. Essi sono:

$$< [10]_{11} >= \{[10]_{11}, [10]_{11}^2 = [100]_{11} = [1]_{11}\}$$

$$\begin{aligned} < [3]_{11} > &= \{[3]_{11}, [3]_{11}^2 = [9]_{11}, [3]_{11}^3 = [27]_{11} = [5]_{11}, [3]_{11}^4 = [3]_{11}^3 \cdot [3]_{11} \\ &= [5]_{11} \cdot [3]_{11} = [4]_{11}, [3]_{11}^5 = [3]_{11}^4 \cdot [3]_{11} = [4]_{11} \cdot [3]_{11} = [1]_{11}\}. \end{aligned}$$

Si osservi che $< [10]_{11} >$ e $< [3]_{11} >$ non sono paragonabili rispetto all'inclusione.

3. Sia G il gruppo somma diretta dei gruppi $(\mathbb{Z}_3, +)$ e $(\mathbb{Z}_6, +)$, ovvero $G = \mathbb{Z}_3 \oplus \mathbb{Z}_6$.

   (a) Determinare gli ordini degli elementi di G

   (b) stabilire se G è ciclico

   (c) verificare che

   $$H = \{([0]_3, [0]_6), ([1]_3, [0]_6), ([2]_3, [0]_6), ([0]_3, [3]_6), ([1]_3, [3]_6), ([2]_3, [3]_6)\}$$

   è un sottogruppo di G non ciclico di ordine 6.

Soluzione

3a) È opportuno calcolare gli ordini degli elementi dei gruppi $(\mathbb{Z}_3, +)$ e di $(\mathbb{Z}_6, +)$, per poter utilizzare la formula $|(a, b)| = m.c.m.(|a|, |b|)$. Ogni elemento diverso da 0 è generatore $(\mathbb{Z}_3, +)$, poichè 3 è un numero primo. Quindi $| [1]_3 | = | [2]_3 | = 3$. In $\mathbb{Z}_6$, invece, tenendo conto che 1 è generatore, si ha:

$$\begin{aligned} | [2]_6 | &= \frac{6}{M.C.M.(6,2)} = 3, \ | [3]_6 | = \frac{6}{M.C.M.(6,3)} = 2, \\ | [4]_6 | &= \frac{6}{M.C.M.(6,4)} = 3, \ | [5]_6 | = \frac{6}{M.C.M.(6,5)} = 6. \end{aligned}$$

Allora

$$\begin{aligned} |([0]_3, [0]_6)| &= 1, \ |([0]_3, [1]_6)| = m.c.m.(|0|, |1|) = m.c.m.(1, 6) = 6 \\ |([0]_3, [2]_6)| &= m.c.m.(|0|, |2|) = m.c.m.(1, 3) = 3 \end{aligned}$$

In maniera analoga si ottiene:

$$\begin{aligned} &|([0]_3, [3]_6)| = 2, \ |([0]_3, [4]_6)| = 3, \ |([0]_3, [5]_6)| = 6, \ |([1]_3, [0]_6)| = 3, \\ &|([1]_3, [1]_6)| = 6, \ |([1]_3, [2]_6)| = 3, \ |([1]_3, [3]_6)| = 6, \ |([1]_3, [4]_6)| = 3, \\ &|([1]_3, [5]_6)| = 6, \ |([2]_3, [0]_6)| = 3, \ |([2]_3, [1]_6)| = 6, \ |([2]_3, [2]_6)| = 3, \\ &|([2]_3, [3]_6)| = 6, \ |([2]_3, [4]_6)| = 3, \ |([2]_3, [5]_6)| = 6. \end{aligned}$$

3b) Si può dedurre che G non è ciclico sia dal punto precedente (infatti non ci sono elementi di ordine 12) sia dalla teoria: poichè 3 e 6 non sono primi tra loro, il gruppo somma diretta $\mathbb{Z}_3 \oplus \mathbb{Z}_6$ non è ciclico.

3c) Ovviamente $H \neq \emptyset$, per cui SG_1) del Teorema 1 della caratterizzazione dei sottogruppi, è verificata. Inoltre è facile verificare che per ogni coppia di elementi di H, la loro somma è ancora un elemento di H, ovvero è verificata SG_2). Infine, per provare SG_3) si osserva che:

$$-([1]_3, [0]_6) = ([2]_3, [0]_6), \quad -([0]_3, [3]_6) = ([0]_3, [3]_6),$$

$$-([2]_3, [3]_6) = ([1]_3, [3]_6).$$

Si può anche scrivere la tabella di H relativa a $+$, dove vengono omessi per motivi di spazio $[\dots]_3$ e $[\dots]_6$.:

+	(0,0)	(1,0)	(2,0)	(0,3)	(1,3)	(2,3)
(0,0)	(0,0)	(1,0)	(2,0)	(0,3)	(1,3)	(2,3)
(1,0)	(1,0)	(2,0)	(0,0)	(1,3)	(2,3)	(0,3)
(2,0)	(2,0)	(0,0)	(1,0)	(2,3)	(0,3)	(1,3)
(0,3)	(0,3)	(1,3)	(2,3)	(0,0)	(1,0)	(2,0)
(1,3)	(1,3)	(2,3)	(0,3)	(1,0)	(2,0)	(0,0)
(2,3)	(2,3)	(0,3)	(1,3)	(2,0)	(0,0)	(1,0)

e da essa si desumono SG_2) e SG_3).