Università Roma Tre - Corso di Laurea in Matematica
AL110-Algebra 1 - A.A. 2018-2019
Esercizi foglio n.9

Esercizio 1. Siano dati i numeri interi $a, b, c \in \mathbb{Z}$ non nulli. Si ponga poi per definizione

$$a\mathbb{Z} = \{\, ka \mid k \in \mathbb{Z} \,\}.$$

Provare che:

(i) $a\mathbb{Z} \subseteq b\mathbb{Z} \quad \Leftrightarrow \quad b|a$

(ii) Detto $h = \mathrm{mcm}(a, b)$, allora $a\mathbb{Z} \cap b\mathbb{Z} = h\mathbb{Z}$.

(iii) $\mathrm{mcm}(ac, bc) = |c|\mathrm{mcm}(a, b)$

(iv) Se $\mathrm{MCD}(a, b) = 1$, allora $\mathrm{mcm}(a, b) = |ab|$

(v) $\mathrm{MCD}(a, b) \cdot \mathrm{mcm}(a, b) = |ab|$

(vi) $\mathrm{mcm}(a, b) = |b| \quad \Leftrightarrow \quad a|b \quad \Leftrightarrow \quad \mathrm{MCD}(a, b) = |a|$

Esercizio 2. Determinare gli inversi aritmetici degli elementi invertibili modulo m, con $m = 1, ..., 40$.

Esercizio 3. Dimostrare che presi due qualsiasi numeri dispari a e b si ha che $a^2 \equiv b^2 \pmod 4$.

Esercizio 4. Dimostrare che se k è pari allora 5 non divide $13^{k+1} \pm 1$.

Esercizio 5. Dimostrare che se k è dispari allora 7 divide $13^{k+1} - 1$.

Esercizio 6. Si definisca su $G \overset{\text{def}}{=} \mathbb{R}^* \times \mathbb{R}$ l'operazione

$$(a, b) \bullet (c, d) = (ac, ad + b).$$

(i) Provare che $\bullet$ è effettivamente un'operazione interna su G.

(ii) Calcolare esplicitamente $[(-2, 3) \bullet (\frac{4}{3}, -\frac{1}{2})] \bullet (\sqrt{2}, 0)$.

(iii) Provare che $(G, \bullet)$ è un gruppo.

(iv) Calcolare l'inverso di $(7, \frac{\sqrt{3}}{2})$.

(v) Stabilire se $(G, \bullet)$ è gruppo abeliano.

Esercizio 7. Si definisca su $G \overset{\text{def}}{=} [0, 1[$ l'operazione

$$x \bullet y = \begin{cases} x + y & \text{se } x + y < 1 \\ x + y - 1 & \text{se } x + y \geqslant 1 \end{cases}.$$

(i) Provare che $\bullet$ è effettivamente un'operazione interna su G.

(ii) Calcolare esplicitamente $(\sqrt{2} - 1) \bullet \frac{1}{3}$.

(iii) Provare che $(G, \bullet)$ è un gruppo.

(iv) Stabilire se $(G, \bullet)$ è gruppo abeliano.

Esercizio 8. Si consideri il sottoinsieme di $\mathbb{R}$ così definito:

$$G = \left\{ 2n + \sqrt{2}m \;\middle|\; m, n \in \mathbb{Z} \right\}.$$

Si doti G dell'usuale somma tra numeri reali. Provare che $(G, +)$ è un gruppo abeliano.

Esercizio 9. Si consideri il sottoinsieme di $\mathbb{R}$ così definito:

$$G = \left\{ n + \sqrt{2}m \;\middle|\; m, n \in \mathbb{Q} \right\}.$$

Si doti G delle usuali operazioni di somma e moltiplicazione tra numeri reali. Provare che $(G, +, \cdot)$ è un campo.

Esercizio 10. Sia G un gruppo. Siano dati $a, b \in G$ tali che $a^{-1}b^2a = ba$. Provare che a e b commutano rispetto all'operazione di G.

Esercizio 11. Considerare l'applicazione $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ definita come $f(a) = 3a^2 - 2a - 1$. Stabilire se f è un endomorfismo di $\mathbb{Z}_6$. Calcolare le controimmagini degli elementi di $\mathbb{Z}_6$ sotto l'azione di f.