

---

ДОМАШНЯ РОБОТА №6  
З ПРЕДМЕТУ  
”МАТЕМАТИЧНІ ОСНОВИ КРИПТОЛОГІЇ”  
ФІ-12 Бекешева Анастасія

---

1.

**одиниця** Множина складається з оборотних елементів, а отже  $1 \cdot 1^{-1} = 1$  та  $1^{-1} \cdot 1 = 1$ .  
Тобто 1 належить множині.

**замкнен.**  $\forall a, b \in \mathbb{R}^*, \quad c = a \cdot b, \quad c \cdot (a \cdot b)^1 = 1 \implies a \cdot b \in \mathbb{R}^*$

**нейт. ел.**  $\langle \mathbb{R}^*, \cdot \rangle$  - кільце з одиницею  $\implies$  моноїд  $\implies$  має нейтральний елемент.

**обер. ел.** Так як множина складається з оборотних елементів, то  $\exists a^{-1} \forall a$ .

**асоціат.**  $\langle \mathbb{R}^*, \cdot \rangle$  - кільце з одиницею  $\implies$  моноїд  $\implies \mathbb{R}^*$  - асоціативна.

**комутат.**  $\langle \mathbb{R}^*, \cdot \rangle$  - кільце з одиницею  $\implies$  моноїд  $\implies \mathbb{R}^*$  - комутативна.

2. (a)  $\text{char } \mathbb{Z}_5 = 5$   
 (b)  $\text{char } \mathbb{Z}_{10} = 10$   
 (c)  $\text{char } \mathbb{Z} = 0$   
 (d)  $\text{char } \mathbb{Q} = 0$   
 (e)  $\text{char } \mathbb{M}_n = 2$

3.

	кільце	комутативне кільце	кільце з одиницею	цілісне кільце	поле
$(\mathbb{N}, +, \cdot)$	-	-	-	-	-
$\mathbb{N} \cup \{0\}, +, \times$	-	-	-	-	-
$\mathbb{Z}_7, + \text{ mod } 7, \times \text{ mod } 7$	+	+	+	+	+
$(\mathbb{Z}_8, + \text{ mod } 8, \times \text{ mod } 8)$	+	+	+	-	-
$(\mathbb{Z}_8 \setminus \{0\}, + \text{ mod } 8, \times \text{ mod } 8)$	-	-	-	-	-
$(6\mathbb{Z}, +, \times)$	+	+	-	-	-
$(3\mathbb{Z} + 2, +, \times)$	-	-	-	-	-
$(\mathbb{R}, +, \times)$	+	+	+	+	+
$(\mathbb{Q} \setminus \{0\}, +, \times)$	-	-	-	-	-
$(\mathbb{M}_n, +, \times)$	+	-	+	-	-