es. 1)

Consideriamo l'insieme $\mathbb{Z}$ e definiamo l'operazione $\oplus$:

$$m \oplus n = m + n + 2 \quad \forall m, n \in \mathbb{Z}$$

$\Rightarrow (\mathbb{Z}, \oplus, \cdot)$ è un anello?

Verifichiamo gli assiomi degli anelli:

1) $(\mathbb{Z}, \oplus)$ deve rispettare i seguenti assiomi:

- associatività:

$$(m \oplus n) \oplus l = (m + n + 2) + l + 2$$
$$= m + (n + 2 + l + 2) = m \oplus (n \oplus l)$$

- commutatività:

$$m \oplus n = \dots = n \oplus m$$

- $\exists!$ elemento neutro:

$$m \oplus e = m \iff m + e + 2 = m$$
$$\iff e = -2 \in \mathbb{Z}$$

- $\exists!$ elemento inverso:

$$m \oplus n = -2 \iff m + n + 2 = -2$$
$$\iff n = -m - 4 \in \mathbb{Z}$$

$\Rightarrow (\mathbb{Z}, \oplus)$ è un gruppo (abeliano)

2) $(\mathbb{Z}, \cdot)$ deve rispettare la proprietà distributiva:

- $m \cdot (n \oplus l) = m \cdot (n + l + 2)$
$= mn + ml + 2m \neq mn + ml + 2 = mn \oplus ml$

$\Rightarrow (\mathbb{Z}, \oplus, \cdot)$ NON è un anello.

es. 2)

Consideriamo $\mathbb{Z}/4\mathbb{Z}$ (gruppo quoziente). Sappiamo che $(\mathbb{Z}/4\mathbb{Z}, +)$ è un gruppo dove $[m] + [n] = [m+n]$ e gli elementi sono $\{[0], [1], [2], [3]\}$. Definiamo la seguente operazione:

$$[a] \cdot [b] = [a \cdot b] \quad \forall a, b \in \mathbb{Z}/4\mathbb{Z}$$

1) • è ben definita?

⇒ deve essere indipendente dai rappresentanti:

$$a_1 \sim a_2 \Rightarrow [a_1][b] = [a_2][b]$$

$$\Leftrightarrow a_1 b \sim a_2 b_2 \Leftrightarrow a_1 b - a_2 b \in 4\mathbb{Z}$$

$\Leftrightarrow (a_1 - a_2) b \in 4\mathbb{Z}$. Si ha:

$$a_1 - a_2 = 4k \Rightarrow 4kb \in 4\mathbb{Z} \quad \checkmark$$

$\Rightarrow [a_1 b - a_2 b] = [0] \Rightarrow \cdot$ è indipendente dai rappresentanti

2) $(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$ è un anello?

⇒ scriviamo le tabelle di Cayley di $+$ e $\cdot$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

⇒ dalla tabella della $\cdot$ notiamo che:

1) $x \cdot 1$ e $x \cdot 3$ mandano $\mathbb{Z}/4\mathbb{Z}$ in se stesso

2) $2 \cdot 2 = 0 \iff 2$ è UN DIVISORE DELLO 0

$\Rightarrow \mathbb{Z}/4\mathbb{Z}$ NON è un dominio (possiede divisori di 0)

3) Quali sono gli elementi invertibili di $\mathbb{Z}/4\mathbb{Z}$?

a invertibile $\iff \exists b$ t.c. $ab = ba = 1$

$\Rightarrow 1, 3$ sono gli unici elementi invertibili con inversi $1, 3$ rispettivamente ($1 \cdot 1 = 1$, $3 \cdot 3 = 1$)

$\Rightarrow$ verificando gli assiomi si trova che $(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$ è un anello.

---

es. 3) Come sopra, con $\mathbb{Z}/3\mathbb{Z}$:

$\Rightarrow$ scriviamo le tabelle di Cayley di $+$ e $\cdot$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\Rightarrow$ dalla tabella della $\cdot$ notiamo che:

1) Tutti gli elementi $\neq 0$ sono invertibili:

$2 \cdot 1 = 1 \cdot 2 = 1$

$\Rightarrow$ un anello con tale proprietà è detto ANELLO CON DIVISIONE

3) è un anello commutativo

4) è un dominio (NON HA DIVISORI DELLO 0 ED È COMMUTATIVO)

5) è un campo (è un anello con divisione commutativo)

---

es. 4) Divisione tra polinomi:

Dato $R = \mathbb{Z}/4\mathbb{Z}$, consideriamo l'anello dei polinomi a coefficienti in R, $R[X]$. Calcolare le seguenti divisioni:

1)
$$\begin{array}{r|l} x^2 - x + 2 & x - 1 \\ \hline x^2 - x & x \\ \hline // \quad // + 2 & \end{array}$$

← N.B. possiamo fare la divisione con resto dato che $x-1$ è MONICO !!!

$$\Rightarrow \quad x^2 - x + 2 = (x-1)x + 2$$
$$= x^2 - x + 2 \quad \checkmark$$
$$= x^2 + 3x - 2$$

usiamo altri rappresentanti

2) È possibile dividere $x^2 - x + 2$ per $2x - 1$?

$2x - 1$ NON È MONICO, quindi la teoria NON ci ASSICURA che tale divisione sia possibile, dobbiamo controllare:

$\Rightarrow$ cerchiamo $q, r \in R[X]$ t.c.:

1) $(2x - 1)q + r = x^2 - x + 2$
2) $\deg r < 1$

$\Rightarrow \deg r \leq 0 \Rightarrow q$ deve contenere un termine di grado 1 ax t.c. $(2x)(ax) = x^2 \Rightarrow 2a = 1$ ↯

Come abbiamo visto sopra, $\exists\, b \in \mathbb{Z}/4\mathbb{Z}$ t.c.

$$2b = b \cdot 2 = 1$$

$\Rightarrow \nexists\, q \quad \Rightarrow$ NON POSSIAMO EFFETTUARE LA DIVISIONE CON RESTO

---

es. 5) Come sopra ma in $R = \mathbb{Z}/3\mathbb{Z}$.

1) È possibile dividere $x^2 + 2x + 2$ per $2x + 2$?

Si, anche se $2x+2$ NON è MONICO, infatti possiamo calcolare:

$$\begin{array}{r|l} x^2 + 2x + 2 & 2x+2 \\ \cancel{(4)}x^2 + \cancel{(4)}x & \hline 2x + 2 \\ \hline // \quad x + 2 & \\ \cancel{(4)}x + 1 & \\ \hline // \quad 1 & \end{array}$$

$$\Rightarrow x^2 + 2x + 2 = (2x+2)(2x+2) + 1$$
$$\overset{!}{=} 4x^2 + 4x + 4x + 4 + 1$$
$$\overset{!}{=} 4x^2 + 8x + 5$$
$$\overset{!}{=} x^2 + 2x + 2 \quad \checkmark$$
