Def. (Anello):

Un ANELLO è una struttura costituita da 1 insieme dotato di 2 operazioni binarie $(R, +, \cdot)$ t.c.:

1) Associatività di $+$:

$$(a+b)+c = a+(b+c) \quad \forall a,b,c \in R$$

2) $\exists!$ elemento neutro di $+$:

$$\exists\, 0 \in R \text{ t.c. } a+0 = a = 0+a \quad \forall a \in R$$

3) $\exists!$ elemento inverso rispetto a $+$:

$$\forall a \in R \ \exists b \in R \text{ t.c. } a+b = 0 = b+a$$

4) Associatività di $\cdot$:

$$(ab)c = a(bc) \quad \forall a,b,c \in R$$

5) Distributività di $\cdot$ rispetto a $+$ (1):

$$a(b+c) = ab+ac \quad \forall a,b,c \in R$$

6) Distributività di $\cdot$ rispetto a $+$ (2):

$$(a+b)c = ac+bc \quad \forall a,b,c \in R$$

7) $\exists!$ elemento neutro di $\cdot$:

$$\exists\, 1 \in R \text{ t.c. } a1 = a = 1a \quad \forall a \in R$$

Si ha che un anello $(R,+,\cdot)$ è un gruppo abeliano rispetto a $+$. Tutto ciò che valeva per i gruppi, continua a valere anche per gli anelli:

$$a0 = a(0+0) = a0 + a0 = 0$$
$$0a = (0+0)a = 0a + 0a = 0$$
$$(x = x+x \Rightarrow x = 0)$$

Verifichiamo l'unicità di $1 \in R$:

sia $u \in R$ t.c. $ua = a = au \quad \forall a \in R$

$\Rightarrow$ prendo $a = 1$ e ottengo:

$$u1 = 1 = 1u \quad \Rightarrow \quad u = 1$$

Inoltre:

$$(-a)b = a(-b) = -(ab)$$

$$ab + (-a)b = (a + (-a))b = 0b = 0$$

$\Rightarrow$ $(-a)b$ è un elemento che sommato ad (ab) da 0, quindi $(-a)b = -(ab)$

$$ab + a(-b) = a(b + (-b)) = a0 = 0$$

$\Rightarrow$ $a(-b)$ è l'opposto di (ab)

Verifichiamo che $(R,+)$ è un gruppo abeliano:

$$(1+1)(a+b) = 1(a+b) + 1(a+b) = 1a + 1b + 1a + 1b = a + b + a + b$$

$$(1+1)(a+b) = (1+1)a + (1+1)b = 1a + 1a + 1b + 1b = a + a + b + b$$

$$\Rightarrow b + a = a + b$$

Se fosse $(R, \cdot)$:

$$xyxy = xxyy \Rightarrow \cancel{x^{-1}x}yx\cancel{yy^{-1}} = \cancel{x^{-1}x}xy\cancel{yy^{-1}}$$

$$\Rightarrow yx = xy$$

N.B.

In generale $(R,\cdot)$ NON PUÓ ESSERE UN GRUPPO, NON è richiesta l'esistenza di $a^{-1} \in R$ t.c. $aa^{-1} = 1 = a^{-1}a$

$\Rightarrow$ infatti supponiamo che $\exists\, 0^{-1} \in R$, allora:

$$00^{-1} = 1 \iff 0 = 1$$

$\Rightarrow$ se $a \in R$ allora:

$$a = a1 \underset{\substack{\uparrow \\ 0=1}}{=} a0 = 0$$

$\Rightarrow$ se $0 = 1$, allora $R = \{0\}$ e $(R, +, \cdot) = (\{0\}, +, \cdot)$

<u>esempi di anelli:</u>

1) $(\mathbb{Z}, +, \cdot)$ è un anello (Zahlring)
2) $(\mathbb{Q}, +, \cdot)$ è un anello
3) $(\mathbb{R}, +, \cdot)$ è un anello
4) $(\mathbb{C}, +, \cdot)$ è un anello
5) $\mathbb{F}_2 = \{0, 1\} \Rightarrow (\mathbb{F}_2, +, \cdot)$ è un anello, definiamo $+, \cdot$ t.c.:

   1) $0 + 0 = 0$
   2) $0 + 1 = 1 = 1 + 0$
   3) $1 + 1 = 0$
   4) $0 \cdot 0 = 0$
   5) $0 \cdot 1 = 0 = 1 \cdot 0$
   6) $1 \cdot 1 = 1$

   $\Rightarrow (\mathbb{F}_2, +)$ è gruppo ciclico con generatore 1.
   $\Rightarrow 1$ è elemento neutro di $\cdot$
6) Dato R anello, sia $M_{n \times n}(R)$ insieme delle matrici quadrate $n \times n$ a coefficienti in R. Allora $(M_{n\times n}(R), +, \cdot)$ è un anello con $+ =$ somma di matrici, $\cdot =$ prodotto matriciale. Ovviamente, se $0 \neq 1$ in R e $n > 1$,
   $\cdot$ NON è COMMUTATIVA
7) esempio NON standard:
   dato X insieme qualsiasi, sia $\mathcal{P}(X)$ l'insieme delle parti di X. Definiamo l'operazione Δ:

$$A \triangle B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$$

$\Rightarrow x \in A \triangle B \iff (x \in A \vee x \in B) \wedge x \notin A \cap B$

$\Rightarrow \triangle$ rende $\mathcal{P}(X)$ un gruppo abeliano ($\triangle$ è associativa e commutativa) con elemento neutro ϕ ($A \triangle A = \phi$) ed elemento inverso l'insieme stesso.

$\Rightarrow \mathcal{P}(X)$ è un anello con operazioni $\triangle, \cap$ (intersezione), infatti

1) elemento neutro di $\cap$ è X

2) verifichiamo che vale:

$$A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$$

$\Rightarrow x \in A \cap (B \triangle C)$

$\iff (x \in A \wedge x \in B \cup C \wedge x \notin B \cup C)$

$\iff x \in A \cap B \vee x \in A \cap C$

MA $x \notin (A \cap B) \cap (A \cap C) \subseteq B \cap C$

Quindi $x \in (A \cap B) \triangle (A \cap C)$

$\Rightarrow A \cap (B \triangle C) \subseteq (A \cap B) \triangle (A \cap C)$

ecc.

$\Rightarrow (\mathcal{P}(X), \triangle, \cap)$ è un anello con la seguente proprietà:

$$A \cap A = A \quad \forall A \in \mathcal{P}(X)$$

8) Un anello R in cui $a^2 = a \quad \forall a \in R$ è detto BOOLEANO. Si ha che ogni anello booleano è commutativo ($ab = ba \quad \forall a, b \in R$). Inoltre

$$1+a = (1+a)^2 = (1+a)(1+a) = 1+a+a+a^2$$

$$= 1+a+a+a$$

$a^2=a$

$$\Rightarrow -\cancel{1+1}+\cancel{a-a} = -\cancel{1+1}+a+a+\cancel{a-a}$$

$\Rightarrow a+a=0 \iff -a=a \Rightarrow$ In un anello booleano l'opposto di un elemento è l'elemento stesso.

Verifichiamo che è un anello commutativo:

$$a+b = (a+b)^2 = (a+b)(a+b) = a^2+ba+ab+b^2$$

$$= a+ba+ab+b$$

$a^2=a$, $b^2=b$

$$\Rightarrow -\cancel{a+a}+\cancel{b-b} = -\cancel{a+a}+ba+ab+\cancel{b-b}$$

$$\Rightarrow ba+ab=0 \Rightarrow ba=-ab$$

$$\Rightarrow ba=ab \quad \forall a,b\in R$$

$-a=a$

Inoltre, sugli anelli booleani si può definire una relazione d'ordine:

$$a\le b \iff ab=a \quad \forall a,b\in R$$

1) Riflessività:

$$a\le a \iff a^2=a \ \checkmark$$

2) $a\le b,\ b\le a \Rightarrow ab=a \wedge ba=b \Rightarrow a=b$

3) Transitività:

$$a\le b \wedge b\le c \Rightarrow ab=a \wedge bc=b \Rightarrow a\le c$$

9) Sia D l'insieme dei divisori di 7530. Definiamo le seguenti operazioni:

$$a+b = \mathrm{mcm}\left(\mathrm{MCD}\left(a, \frac{7530}{b}\right), \mathrm{MCD}\left(\frac{7530}{a}, b\right)\right)$$

$ab = MCD(a,b)$

$\Rightarrow (D, +, \cdot)$ è un anello booleano

<u>Anelli speciali:</u>

1) Anelli commutativi: $\cdot$ è commutativa $(ab = ba)$

2) Domini di integrità:

R è un dominio se è commutativo e si ha:

$$ab = 0 \Rightarrow a = 0 \vee b = 0 \quad \forall a, b \in R$$

(NON È VERO IN GENERALE, nemmeno negli anelli commutativi)

$\Rightarrow \mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{R}$ sono domini, $(P(X), \Delta, \cap)$ NON è un dominio se $|X| \geq 2$

3) Campi:

R è un campo se è un anello commutativo con $0 \neq 1$ e in cui $\forall a \neq 0 \ \exists a^{-1}$ t.c. $aa^{-1} = a^{-1}a = 1$ ovvero $(R \setminus \{0\}, \cdot)$ è un gruppo abeliano

$\Rightarrow$ un campo è un dominio:

$$ab = 0 \Rightarrow \text{se } a = 0 \ \checkmark, \text{ altrimenti:}$$

$$a^{-1}ab = a^{-1}0 = 0 \Rightarrow b = 0$$

$\Rightarrow \mathbb{Z}$ NON è un campo, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono campi

$\Rightarrow \mathbb{F}_2 = \{0, 1\}$ è un campo.

$\Rightarrow$ esercizio: trovare un campo con 3 elementi

$\{a, 0, 1\}$

$\Rightarrow$

$\cdot$	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

$\Rightarrow$

+	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

N.B.

$\exists$ almeno un anello NON commutativo in cui ogni elemento $\neq 0$ è invertibile rispetto a $\cdot$