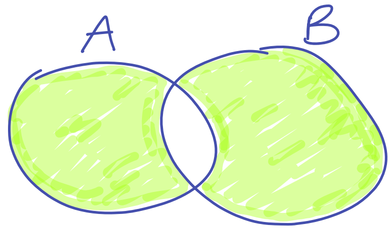
ANELLO DI BOOLE

X insieme

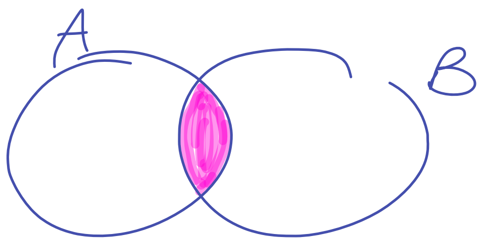
$P(X)$ = insieme delle parti

$A, B \in P(X)$

$A + B := (A \setminus B) \cup (B \setminus A)$



$A \cdot B := A \cap B$

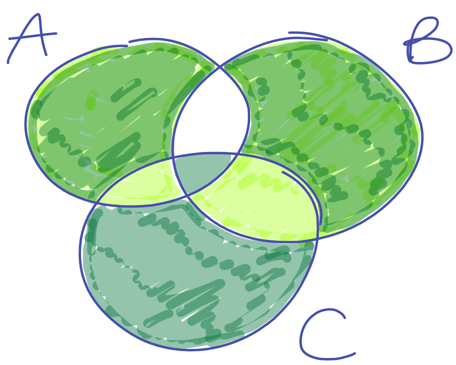


$(P(X), +, \cdot)$ è un anello commutativo con unità, dove tutti gli elt. sono divisori dello zero.

$(P(X), +)$ sono un gruppo abeliano:

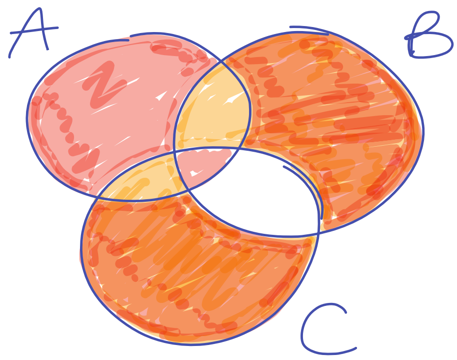
- $+$ è commutativa ✓
- $+$ è associativa:

$A, B, C \in P(X)$ $\qquad (A+B)+C \overset{?}{=} A+(B+C)$



$A+B = (A \setminus B) \cup (B \setminus A)$

$(A+B)+C = (A+B) \setminus C \cup C \setminus (A+B)$



$B + C = B \setminus C \cup C \setminus B$

$A + (B+C) = A \setminus (B+C) \cup (B+C) \setminus A$

- elemento neutro per $+$:

$Y: \quad A = A + Y = (A \setminus Y) \cup (Y \setminus A)$

$Y = \emptyset: \quad A + \emptyset = A \setminus \emptyset \cup \emptyset \setminus A = A$

- opposto di un elemento $A \in P(X)$:

$-A = ? \quad A + Z = \emptyset$

$A \setminus Z \cup Z \setminus A = \emptyset$

$Z = A \quad \boxed{-A = A}$

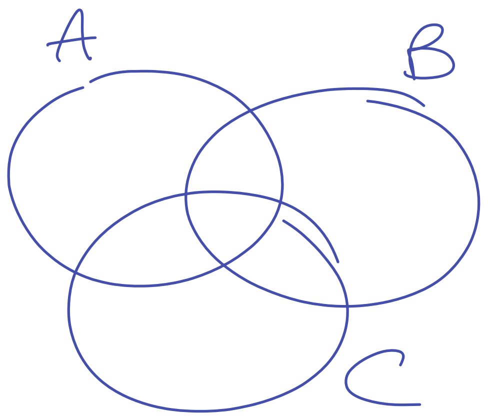
- associatività del prodotto:

$A \cdot B = A \cap B$

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

- proprietà distributive: (per casa)

$$A\cdot(B+C) \stackrel{?}{=} A\cdot B + A\cdot C$$



- unità $1 = ?$ Y t.c. $A\cdot Y = A$

$$A \cdot Y = A \cap Y$$

$1 = X$ elt. neutro per il prodotto è X

$A \in \mathcal{P}(X)$, $A \neq \emptyset$

$A\cdot A^c = A\cap A^c = \emptyset$

Cioè ogni $A\in\mathcal{P}(X)$ è divisore dello zero.

Def: Un sottoinsieme non vuoto S di un anello A é detto SOTTOANELLO se é un anello rispetto alla restrizione delle 2 operazioni di A.

OSS: $S \subseteq A$ é un sottoanello se:
- S é un sottogruppo additivo
- S é chiuso rispetto al prodotto:
  $a, b \in S \Rightarrow a \cdot b \in S$

Criterio per sottoanelli:

Un sottoinsieme non vuoto S di un anello A é un sottoanello se e solo se:
- $\forall a, b \in S: a - b \in S$
- $\forall a, b \in S: ab \in S$

Esempi:

① $n\mathbb{Z}$ é un sottoanello di $\mathbb{Z}$ $\forall n$
(e sono gli unici sottoanelli)

$a, b \in n\mathbb{Z}$ $\quad a = np,\ b = nq \Rightarrow ab = (np)(nq) \in n\mathbb{Z}$

② Anello degli interi di Gauss:
(sottoanello di $\mathbb{C}$)

$$\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$

Usiamo il criterio: siano $x, y \in \mathbb{Z}[i]$, dobbiamo verificare:
- $x - y \in \mathbb{Z}[i]$
- $xy \in \mathbb{Z}[i]$

$x = a+ib$, $y = c+id$ $\quad a,b,c,d \in \mathbb{Z}$

$$\Rightarrow x-y = (a+ib)-(c+id) = \underbrace{(a-c)}_{\in \mathbb{Z}} + i\underbrace{(b-d)}_{\in \mathbb{Z}} \in \mathbb{Z}[i]$$

$$x \cdot y = (a+ib)(c+id) = \underbrace{(ac-bd)}_{\in \mathbb{Z}} + i\underbrace{(ad+bc)}_{\in \mathbb{Z}} \in \mathbb{Z}[i]$$

3 $\quad \mathbb{Z}[\sqrt{2}] = \{a+\sqrt{2}b \in \mathbb{R} \mid a,b \in \mathbb{Z}\}$

<u>per casa:</u> mostrare che $\mathbb{Z}[\sqrt{2}]$ è un sottoanello di $\mathbb{R}$.

<u>Esercizio:</u> $\mathbb{R}^{2,2}$

$L = \{A = (a_{ij}) \in \mathbb{R}^{2,2} \mid a_{12} = 0\} = \left\{\begin{pmatrix} a_{11} & 0 \\ a_{21} & a_{22}\end{pmatrix}\right\}$

$X = \{A \in \mathbb{R}^{2,2} \mid a_{11} = a_{22} = 0\} = \left\{\begin{pmatrix} 0 & a_{12} \\ a_{21} & 0\end{pmatrix}\right\}$

$Y = \{A \in \mathbb{R}^{2,2} \mid a_{11} = a_{22} = a_{21} = 0\} = \left\{\begin{pmatrix} 0 & a_{12} \\ 0 & 0\end{pmatrix}\right\}$

$Z = \{A \in \mathbb{R}^{2,2} \mid a_{12} = a_{22} = a_{21} = 0\} = \left\{\begin{pmatrix} a_{11} & 0 \\ 0 & 0\end{pmatrix}\right\}$

L è un sottoanello unitario: $A = \begin{pmatrix} a_{11} & 0 \\ a_{21} & a_{22}\end{pmatrix}$, $B = \begin{pmatrix} b_{11} & 0 \\ b_{21} & b_{22}\end{pmatrix}$

$$A - B = \begin{pmatrix} a_{11}-b_{11} & 0 \\ a_{21}-b_{21} & a_{22}-b_{22}\end{pmatrix} \in L$$

$$A \cdot B = \begin{pmatrix} a_{11} & 0 \\ a_{21} & a_{22}\end{pmatrix}\begin{pmatrix} b_{11} & 0 \\ b_{21} & b_{22}\end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & 0 \\ a_{21}b_{11}+a_{22}b_{21} & a_{22}b_{22}\end{pmatrix} \in L$$

l'unità è $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix} \in L$

$$X = \{ A \in \mathbb{R}^{2,2} \mid a_{11} = a_{22} = 0 \} = \left\{ \begin{pmatrix} 0 & a_{12} \\ a_{21} & 0 \end{pmatrix} \right\}$$

$$\underset{\substack{\cap \\ X}}{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}} \underset{\substack{\cap \\ X}}{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin X$$

non chiuso risp. prodotto :
non è un sottoanello

$$Y = \{ A \in \mathbb{R}^{2,2} \mid a_{11} = a_{22} = a_{21} = 0 \} = \left\{ \begin{pmatrix} 0 & a_{12} \\ 0 & 0 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 0 & a_{12} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & b_{12} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in Y$$

è un sottoanello commutativo, che però non ha unità.

$$Z = \{ A \in \mathbb{R}^{2,2} \mid a_{12} = a_{22} = a_{21} = 0 \} = \left\{ \begin{pmatrix} a_{11} & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

$$\begin{pmatrix} a_{11} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b_{11} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11} b_{11} & 0 \\ 0 & 0 \end{pmatrix} \in Z$$

è un sottoanello commutativo con unità: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

(che è diversa dall'unità I_2 di $\mathbb{R}^{2,2}$)

Def: Un sottoinsieme I di un anello A si dice IDEALE (IDEALE BILATERO) di A se valgono le seguenti proprietà:

- $\forall x, y \in I$: $x - y \in I$
  (cioè I è sottogruppo additivo)
- $\forall x \in I$ e $\forall a \in A$: $ax \in I$ e $xa \in I$
  (cioè I "ingloba" per moltiplicazione tutti gli elt. di A)

OSS/esempi:

- ogni ideale è un sottoanello
- A e $\{0_A\}$ sono detti ideali impropri
- $\mathbb{Z} \subseteq \mathbb{Q}$ è un sottoanello, ma non è un ideale.
- $n\mathbb{Z} \subseteq \mathbb{Z}$ è un ideale:

  $np \in n\mathbb{Z},\ z \in \mathbb{Z} \implies (np)z \in n\mathbb{Z}$

- A anello con unità 1_A
  se I ideale contiene $1_A \implies I = A$.

Esempio: $\mathbb{R}[x]$ anello dei polinomi nella variabile x a coeff. reali

$$I = \{ p(x) = \sum_{i \in \mathbb{N}_0} a_i x^i \in \mathbb{R}[x] \mid a_0 = 0 \}$$

$$p(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots$$

I é un ideale:

$p(x), q(x) \in \mathbb{R}[x]$ $\deg(p) = n$, $\deg(q) = m$

$p(x) = a_0 + a_1 x + \dots + a_n x^n$

$q(x) = b_0 + b_1 x + \dots + b_m x^m$

Il termine noto di $p(x) - q(x)$ é $a_0 - b_0$

In particolare, se $p, q \in I$: $a_0 = b_0 = 0$

$\Longrightarrow p - q \in I$.

Il termine noto di $p(x)q(x)$ é $a_0 b_0$.

In particolare, se $p \in I$ e $q \in \mathbb{R}[x]$ é un polin. qualsiasi, $pq \in I$.