Morfismi

Def

- **Morfismo di gruppi** > - $(G, \cdot), (H, \cdot)$ gruppi > - $f : G \to H$ > - f **morfismo di gruppi** $\iff f(x \cdot y) = f(x) \cdot f(y) \quad \forall x, y \in G$
- **Morfismo di anelli** > - $(A, +, \cdot), (B, +, \cdot)$ anelli > - $f : A \to B$ > - f **morfismo di anelli** $\iff f(x + y) = f(x) + f(y)$ e $f(x \cdot y) = f(x) \cdot f(y) \quad \forall x, y \in A$ > - la stessa definizione si applica per morfismo di campi

Oss

- **Hp**
  - $(G, \cdot), (H, \cdot)$ gruppi
  - 1_G neutro per G
  - 1_H neutro per H
  - $f : G \to H$ morfismo
- **Th**
  - $f(1_G) = 1_H$
- **Dim**
  - $\forall g \in G \quad f(g) = f(1_G \cdot g) = f(1_G) \cdot f(g)$ poiché f morfismo
  - quindi $f(g) = f(1_G) \cdot f(g) \implies f(g) \cdot f(g)^{-1} = f(1_G) \cdot f(g) \cdot f(g)^{-1} \implies 1_H = f(1_G) \cdot 1_H \implies 1_H = f(1_G)$ (poiché $f(g), f(g)^{-1} \in H$ per definizione di f)

Oss

- **Hp**
  - $(G, \cdot), (H, \cdot)$ gruppi
  - 1_G neutro per G
  - 1_H neutro per H
  - $f : G \to H$ morfismo
- **Th**
  - $f(g^{-1}) = f(g)^{-1}$
- **Dim**
  - per dimostrazione precedente, $1_H = f(1_G) = f(g \cdot g^{-1}) = f(g) \cdot f(g^{-1}) \implies 1_H = f(g) \cdot f(g^{-1}) \implies f(g)^{-1} = f(g^{-1})$

Isomorfismi

Def

- **Isomorfismo** > - f isomorfismo $\iff f$ morfismo e f biiettiva

Oss

- **Hp**
  - $f : G \to H$ isomorfismo
- **Th**

- $f^{-1} : H \to G$ isomorfismo
- **Dim**
  - $\forall g \in G, h \in H \quad \exists! f^{-1} \mid \begin{cases} f^{-1}(f(g)) = g \\ f\left(f^{-1}(h)\right) = h \end{cases}$
  - $\forall h, h' \in H \quad f^{-1}(hh') = f^{-1}(h) \cdot f^{-1}(h') \iff hh' = f\left(f^{-1}(hh')\right) = f(f^{-1}(h) \cdot f^{-1}(h')) = f(f^{-1}(h)) \cdot f($ hh', e dunque f^{-1} è un morfismo, e poiché è invertibile è un isomorfismo

Ex

- **Hp**
  - $z \in \mathbb{C} \mid z^n = 1$ sono le radici n-esime di 1
  - $\zeta := e^{i\frac{2\pi}{n}}$
  - $H := \{\zeta^0, \zeta^1, \zeta^k, \dots, \zeta^{n-1}\}$ è l'insieme delle radici n-esime di 1
- **Th**
  - $(H, \cdot) \subset (\mathbb{C} - \{0\}, \cdot)$ è un sottogruppo
- **Dim**
  - $\zeta^0 = 1 \implies 1 \in H$
  - $z, w \in H \iff z^n = w^n = 1$, allora $1 = z^n \cdot w^n = (z \cdot w)^n = 1 \implies z \cdot w \in H$ per definizione di H
  - $z^n = 1 \implies \dfrac{1}{z^n} = 1 \iff (z^{-1})^n = 1 \implies z^{-1} \in H$ per definizione di H

Ex

- **Hp**
  - $f : \mathbb{Z}_n \to H : [k] \to \zeta^k$
- **Th**
  - f isomorfismo di gruppi $(\mathbb{Z}_n, +)$ e $(H, \cdot)$
- **Dim**
  - f è biiettiva per costruzione di $\mathbb{Z}_n := \{[0], [1], \dots, [n-1]\}$ e $H := \{\zeta^0, \zeta^1, \dots, \zeta^{n-1}\}$
  - f morfismo
    - $f([i] + [j]) = f([i]) \cdot f([j])$
      - $[i] + [j] = [k]$ per un certo $k \in \mathbb{Z}_n \implies \exists h \in \mathbb{Z} \mid i + j = k + hn$
      - $f([i] + [j]) = f([k]) = \zeta^k$
      - $f([i]) \cdot f([j]) = \zeta^i \cdot \zeta^j = \zeta^{i+j}$, ma per osservazione precedente $\zeta^{i+j} = \zeta^{k+nh} = \zeta^k \cdot (\zeta^n)^h$
      - $\zeta^n = 1$ per definzione di $\zeta \implies$ entrambe i membri dell'equazione sono pari a ζ^k

Ex

- **Hp**
  - $(G, \cdot)$ gruppo
  - $f : \mathbb{Z} \to G : n \to g^n$ per qualche $g \in G$
- **Th**
  - f morfismo di gruppi $(\mathbb{Z}, +)$ e $(G, \cdot)$
- **Dim**
  - $f(n + m) = g^{n+m} = g^m \cdot g^n = f(m) \cdot f(n) \implies f$ morfismo

Ex

- **Hp**
  - $f : \mathbb{Z} \to \mathbb{Z}_n : k \to [k]$
- **Th**
  - f morfismo di anelli $(\mathbb{Z}, +, \cdot)$ e $(\mathbb{Z}_n, +, \cdot)$
- **Dim**
  - per come le operazioni $+$ e $\cdot$ sono state definite, $f([x + y]) = f([x]) + f([y])$ e $f([x \cdot y]) = f([x]) \cdot f([y])$

Ex

- **Hp**
  - $n, m \in \mathbb{Z} : n \mid m$
  - $f : \mathbb{Z}_m \to \mathbb{Z}_n : x \pmod{m} \to x \pmod{n}$
- **Th**
  - f morfismo di anelli $(\mathbb{Z}_m, +, \cdot)$ e $(\mathbb{Z}_n, +, \cdot)$
- **Dim**
  - $\forall [x], [y] \in \mathbb{Z}_m \quad x \pmod{m} + y \pmod{m} = x + y \pmod{m}$
  - $f(x + y \pmod{m}) = x + y \pmod{n} = x \pmod{n} + y \pmod{n} = f(x \pmod{m}) + f(y \pmod{m})$
  - il ragionamento è analogo per l'operazione $\cdot$, e dunque segue la tesi

Ex

- **Hp**
  - G gruppo
  - $f : G \to G : h \to g \cdot h \cdot g^{-1}$ per qualche $g \in G$
- **Th**
  - f morfismo di gruppi $(G, \cdot)$ e $(G, \cdot)$
- **Dim**
  - $\forall h, h' \in G \quad f(h) \cdot f(h') = \left(ghg^{-1}\right) \cdot \left(gh'g^{-1}\right) = gh(g^{-1} \cdot g)h'g^{-1} = ghh'g^{-1} = f(hh')$

---

kernel e Immagine

Def

- **kernel e Immagine di gruppi** > - G, H gruppi > - $f : G \to H$ morfismo > - $\ker(f) := \{g \in G \mid f(g) = 1_H\}$ > - $\mathrm{Im}(f) := \{h \in H \mid \exists g \in G : f(g) = h\}$
- **kernel e Immagine di anelli** > - A, B gruppi > - $f : A \to B$ morfismo > - $\ker(f) := \{a \in A \mid f(a) = 0_B\}$ > - $\mathrm{Im}(f) := \{b \in B \mid \exists a \in A : f(a) = b\}$

Oss

- **Hp**
  - G, H gruppi
  - $f : G \to H$ morfismo
- **Th**

- $\ker(f) \subset G$ è sottogruppo
- **Dim**
  - per dimostrazione precedente, $f(1_G) = 1_H \implies 1_G \in \ker(f)$ per definizione
  - $x, y \in \ker(f) \implies f(x) = f(y) = 1_H$ per definizione, dunque $f(x) \cdot f(y) = 1_H \cdot 1_H = 1_H$, e $f(x) \cdot f(y) = f(x \cdot y) = 1_H$ perché f morfismo, quindi $x \cdot y \in \ker(f)$ per definizione
  - $g \in \ker(f) \implies f(g) = 1_H \implies f(g)^{-1} = 1_H^{-1} = 1_H$, ma poiché per dimostrazione precedente $f(g)^{-1} = f(g^{-1}) \implies f(g^{-1}) = 1_H \implies g^{-1} \in \ker(f)$ per definizione

Oss

- **Hp**
  - G, H gruppi
  - $f : G \to H$ morfismo
- **Th**
  - $\mathrm{Im}(f) \subset G$ è sottogruppo
- **Dim**
  - per dimostrazione precedente $f(1_G) = 1_H \implies 1_H \in \mathrm{Im}(f)$ per definizione
  - $x, y \in \mathrm{Im}(f) \implies \exists g, g' \in G \mid x = f(g) \wedge y = f(g') \implies x \cdot y = f(g) \cdot f(g') = f(g \cdot g')$ perché f morfismo, quindi $x \cdot y \in \mathrm{Im}(f)$ per definizione
  - $x \in \mathrm{Im}(f) \implies \exists g \in G \mid f(g) = x \implies x^{-1} = f(g)^{-1} = f(g^{-1})$ per dimostrazione precedente, quindi $x^{-1} \in \mathrm{Im}(f)$ per definizione

Oss

- **Hp**
  - G, H gruppi
  - $f : G \to H$ morfismo
- **Th**
  - f iniettiva $\iff \ker(f) = \{1_G\}$
- **Dim**
  - f iniettiva $\implies \ker(f) = \{1_G\}$
    * $f(1_G) = 1_H$ per dimostrazione precedente, dunque $1_G \in \ker(f)$ per definizione
    * f iniettiva $\implies \nexists x, y \in G \mid x \neq y \implies f(x) = f(y)$, di conseguenza è unico $1_G \in G \mid f(1_G) = 1_H$, dunque $\ker(f)$ conterrà esclusivamente 1_G per definizione
  - f iniettiva $\impliedby \ker(f) = \{1_G\}$
    * $\forall g, g' \in G \quad f(g) = f(g') \iff f(g)^{-1} \cdot f(g) = f(g)^{-1} \cdot f(g') \iff 1_H = f(g) \cdot f(g') = f(g \cdot g')$
    * $\ker(f) = \{1_G\} \implies f(1_G) = 1_H$ per definizione, allora $f(g \cdot g') = 1_H \implies g \cdot g' = 1_G$ necessariamente, e $g \cdot g' = 1_G \iff g = g' \implies f(g) = f(g') \implies g = g' \implies f$ iniettiva

Oss

- **Hp**
  - A, B anelli
  - $f : A \to B$ morfismo di anelli
- **Th**
  - $\ker(f)$ ideale
- **Dim**

- $(\ker(f), +) \subset (A, +)$ sottogruppo per dimostrazione precedente
  - per analogia con dimostrazione precedente, $f(0_A) = 0_B$
  - $x \in \ker(f) \implies f(x) = 0_B$ per definizione, quindi $\forall x \in \ker(f), y \in A \quad f(x \cdot y) = f(x) \cdot f(y)) = 0_B \cdot f(y) = 0_B \implies x \cdot y \in \ker(f)$ per definizione, quindi $\ker(f) \cdot A \subset \ker(f)$

Oss

- **Hp**
  - A, B anelli
  - $f : A \to B$ morfismo di anelli
- **Th**
  - $\mathrm{Im}(f)$ sottoanello
- **Dim**
  - $(\mathrm{Im}(f), +) \subset (A, +)$ sottogruppo per dimostrazione precedente
  - $x, y \in \mathrm{Im}(f) \implies \exists a, a' \mid x = f(a) \wedge y = f(a') \implies x \cdot y = f(a) \cdot f(a') = f(a \cdot a')$ perche f morfismo, quindi $\exists a \cdot a' \mid x \cdot y = f(a \cdot a') \implies x \cdot y \in \mathrm{Im}(f) \implies \mathrm{Im}(f) \cdot \mathrm{Im}(f) \subset \mathrm{Im}(f)$

Oss

- **Hp**
  - $f : \mathbb{Z} \to \mathbb{C} - \{0\} : k \to \zeta^k$
  - f morfismo di gruppi $(\mathbb{Z}, +)$ e $(\mathbb{C} - \{0\}, \cdot)$
  - $I(n)$ ideale generato da n **!!! CONTROLLA SE SERVE QUESTA COSA**
- **Th**
  - $\ker(f) = I(n)$
- **Dim**
  - pass

Oss

- **Hp**
  - G, H gruppi
  - $f : G \to H$ morfismo
- **Th**
  - $\ker(f)$ è sottogruppo normale
- **Dim**
  - per la formulazione 2 della definizione di sottogruppo normale, $\forall g \in G, h \in \ker(f) \implies ghg^{-1} \in \ker(f)$
  - $f(ghg^{-1}) = f(g) \cdot f(h) \cdot f(g^{-1})$
  - $h \in \ker(f) \implies f(h) = 1_H$ per definizione
  - per dimostrazione precedente $f(g^{-1}) = f(g)^{-1}$
  - $f(ghg^{-1}) = f(g) \cdot 1_H \cdot f(g)^{-1} = 1_H \implies ghg^{-1} \in \ker(f)$ per definizione