

## Insieme quoziente

### Def

- **Insieme quoziente**  $> - G$  gruppo  $> - \sim$  relazione di equivalenza in  $G > - \forall x \in G \quad [x] := \{y \in G \mid x \sim y\} > - G/\sim := \{[x] \mid x \in G\}$  è l'**insieme quoziente**, ovvero l'insieme delle classi di equivalenza determinate da  $\sim$

### Def

- **Insieme quoziente**  $\mathbb{Z}_n > - (\mathbb{Z}, +, \cdot)$  anello, in particolare  $(\mathbb{Z}, +)$  gruppo  $> - n \in \mathbb{Z} > - \mathbb{Z}/\equiv$  è l'insieme delle classi di equivalenza definite dalla relazione di equivalenza  $\equiv > - m \equiv r \pmod{n} \iff r \equiv m \pmod{n} \implies n \mid m - r \implies \exists q : nq = m - r \implies m = nq + r \quad 0 \leq r < n > - 0 \leq r < n \implies$  è possibile definire  $\mathbb{Z}_n := \{[0], [1], \dots, [n-1]\}$ , che coincide con  $\mathbb{Z}/\equiv$

### Oss

- **Hp**
  - $n \in \mathbb{Z}$
  - $I(n) := \{nk \mid k \in \mathbb{Z}\}$
- **Th**
  - $(\mathbb{Z}_n, +)$  è un gruppo
- **Dim**
  - per dimostrazione precedente,  $I(n)$  è un sottogruppo, quindi ha senso definire  $\mathbb{Z}/I(n)$ , che conterrà le classi laterali sinistre definite in  $\mathbb{Z}$  rispetto a  $I(n)$ , che per dimostrazione precedente corrispondono alle classi di equivalenza definite da  $\equiv$
  - di conseguenza,  $\mathbb{Z}/I(n) = \mathbb{Z}/\equiv = \mathbb{Z}_n$  per definizione precedente
  - per dimostrazione precedente, la somma tra classi di equivalenza è ben definita, di conseguenza è possibile definire la struttura di gruppo  $(\mathbb{Z}_n, +)$

### Lem

- **Hp**
  - $p \in \mathbb{P}$
  - $a, b \in \mathbb{Z}$
  - $p \mid ab$
- **Th**
  - $p \mid a \vee p \mid b$
- **Dim**
  - $p \mid ab \implies p$  compare nella fattorizzazione in numeri primi di  $ab$
  - allora  $p$  è nella fattorizzazione di  $a$ , e quindi  $p \mid a$ , oppure  $p$  è nella fattorizzazione di  $b$ , e quindi  $p \mid b$

### Oss

- **Hp**
  - $n \in \mathbb{Z}$
- **Th**
  - $\mathbb{Z}_n$  dominio di integrità  $\iff n$  primo

- **Dim**
  - $\mathbb{Z}_n$  dominio di integrità  $\implies n$  primo
    - \* ipotizzando che  $n \notin \mathbb{P} \implies \exists a, b \in \mathbb{Z} \mid n = ab \quad 0 < a, b < n$  per definizione
      - in particolare  $a, b \neq 0$
    - \*  $n = ab \iff [n] = [ab]$  in  $\mathbb{Z}_n$
    - \*  $[n] = [0]$  in  $\mathbb{Z}_n$ , dunque  $[ab] = [0]$
    - \*  $\mathbb{Z}_n$  dominio di integrità  $\implies$  in  $\mathbb{Z}_n$  vale la legge di annullamento del prodotto, e dunque  $[ab] = [0] \iff [a] = 0 \vee [b] = [0] \perp$
  - $n$  primo  $\implies \mathbb{Z}_n$  dominio di integrità
    - \* ipotizzando che  $\mathbb{Z}_n$  non sia dominio di integrità, e dunque  $\exists [a] \in \mathbb{Z}_n : [a] \neq [0], a \mid 0$
    - \*  $a \mid 0 \implies \exists b \in \mathbb{Z} \mid [a][b] = [0] \quad b \neq 0$
    - \*  $[0] = [a][b] \iff [0] = [ab] \iff 0 \equiv ab \pmod{n} \iff n \mid ab - 0 \iff n \mid ab$
    - \*  $n$  primo, allora  $n \mid ab \implies n \mid a \vee n \mid b$  per dimostrazione precedente
      - $n \mid a \implies [a] = [n] = [0]$  in  $\mathbb{Z}_n \perp$
      - $n \mid b \implies [b] = [n] = [0]$  in  $\mathbb{Z}_n$ , ma  $b \neq 0$  in ipotesi, dunque necessariamente  $[a] = [0] \perp$

**Oss**

- **Hp**
  - $n \in \mathbb{Z}$
- **Th**
  - $\forall [a] \in \mathbb{Z}_n \quad \text{MCD}(a, n) = 1 \iff [a] \in \mathbb{Z}_n^*$
- **Dim**
  - $[a] \in \mathbb{Z}_n^* \implies \text{MCD}(a, n) = 1$ 
    - \*  $[a] \in \mathbb{Z}_n^* \implies \exists b \in \mathbb{Z} \mid [a][b] = [1] \quad 0 < b < n \iff ab \equiv 1 \pmod{n} \iff n \mid 1 - ab \iff \exists k \in \mathbb{Z} \mid nk = 1 - ab$
    - \* allora  $\exists b, k \in \mathbb{Z} \mid nk = 1 - ab \iff 1 = nk + ab$
    - \*  $d := \text{MCD}(a, n)$
    - \* per definizione,  $d \mid a \wedge d \mid n$ 
      - $d \mid a \implies \exists x \in \mathbb{Z} \mid dx = a$
      - $d \mid n \implies \exists y \in \mathbb{Z} \mid dy = n$
    - \*  $1 = nk + ab \iff 1 = dyk + dxb = d(yk + xb) \implies \exists yk + xb \in \mathbb{Z} \mid 1 = d(yk + xb) \implies d \mid 1$
    - \*  $d \mid 1 \iff d = \pm 1$ , ma  $d := \text{MCD}(a, n) \implies d \geq 0 \implies d = 1$
  - $\text{MCD}(a, n) = 1 \implies [a] \in \mathbb{Z}_n^*$ 
    - \*  $d := \text{MCD}(a, n) = 1$
    - \* per dimostrazione precedente,  $I(d) = I(a, n) \implies d \in I(a, n) \implies \exists b, k \in \mathbb{Z} \mid d = ab + nk$  per definizione di  $I(a, n)$ , allora  $d = 1 = ab + nk \iff nk = 1 - ab \iff n \mid 1 - ab \iff ab \equiv 1 \pmod{n} \implies [a][b] = [1]$  in  $\mathbb{Z}_n$ , dunque sono uno l'inverso dell'altro, e in particolare  $[a] = [b]^{-1} \implies \exists [b] \in \mathbb{Z}_n \mid [a] \in \mathbb{Z}_n^*$

**Oss**

- **Hp**
  - $p \in \mathbb{P}$
- **Th**
  - $\mathbb{Z}_p$  campo
- **Dim**

- $\mathbb{Z}_p^* := \{[x] \in \mathbb{Z}_p \mid \exists [x]^{-1} \in \mathbb{Z}_p\}$
  - $p \in \mathbb{P} \implies$  ogni numero è coprimo con  $p$
  - per dimostrazione precedente, allora tutti gli elementi di  $\mathbb{Z}_p$  sono invertibili, tranne  $[0]$  in quanto  $[0]$  non ha inversi
  - allora  $\mathbb{Z}_p^* = \mathbb{Z}_p - \{[0]\}$ , che per definizione implica che  $\mathbb{Z}_p$  campo
- 

## Funzione totiente di Eulero

### Def

- **Funzione totiente di Eulero**  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  -  $\varphi(n) := |\mathbb{Z}_n^*|$

### Lem

- **Hp**
  - $n, m \in \mathbb{N}$
- **Th**
  - $[a] \in \mathbb{Z}_{mn}^* \iff [a] \in \mathbb{Z}_m^* \wedge [a] \in \mathbb{Z}_n^*$
- **Dim**
  - *prima implicazione*
    - \*  $a \pmod{n} \in \mathbb{Z}_{mn}^* \implies \exists x \in \mathbb{Z} \mid ax \equiv 1 \pmod{mn}$
    - per dimostrazione precedente  $\left. \begin{array}{l} a \mid b \\ x \equiv y \pmod{b} \end{array} \right\} x \equiv y \pmod{a} \implies$
    - $\left\{ \begin{array}{l} m, n \mid mn \\ ax \equiv 1 \pmod{mn} \end{array} \right\} \iff \left\{ \begin{array}{l} ax \equiv 1 \pmod{m} \\ ax \equiv 1 \pmod{n} \end{array} \right\} \implies \left\{ \begin{array}{l} [a] \in \mathbb{Z}_m^* \\ [a] \in \mathbb{Z}_n^* \end{array} \right.$
  - *seconda implicazione*
    - \*  $[a] \in \mathbb{Z}_m^* \wedge [a] \in \mathbb{Z}_n^* \implies \exists y, z \mid \left\{ \begin{array}{l} ay \equiv 1 \pmod{m} \\ az \equiv 1 \pmod{n} \end{array} \right.$ , e per il teorema cinese dei resti  $\exists! [x] \in \mathbb{Z}_{mn}$ , che si trova ponendo  $\left\{ \begin{array}{l} x \equiv y \pmod{m} \\ x \equiv z \pmod{n} \end{array} \right. \implies$
    - $\left\{ \begin{array}{l} ax \equiv ay \pmod{m} \\ ax \equiv az \pmod{n} \end{array} \right.$  moltiplicando entrambe le equazioni per  $a$ , e per il sistema precedente  $\left\{ \begin{array}{l} ax \equiv 1 \pmod{m} \\ ax \equiv 1 \pmod{n} \end{array} \right.$ , e poiché  $m$  e  $n$  sono coprimi in ipotesi, per il teorema cinese dei resti  $ax \equiv 1 \pmod{mn} \implies [a] \in \mathbb{Z}_{mn}^*$

### Oss

- **Hp**
  - $m, n \in \mathbb{N} \mid \text{MCD}(m, n) = 1$
- **Th**
  - $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$
- **Dim**
  - per dimostrazione precedente, esiste una biezione definita come  $\mathbb{Z}_{mn}^* \rightarrow \mathbb{Z}_m^* \times \mathbb{Z}_n^*$
  - $\varphi(m \cdot n) := |\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*|$  perché è una biezione, e dunque è pari a  $|\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*| = \varphi(m) \cdot \varphi(n)$  per definizione

Oss

- **Hp**
  - $p \in \mathbb{P}$
  - $k \in \mathbb{N} \mid k \geq 1$
- **Th**
  - $\varphi(p^k) = p^{k-1}(p-1)$
- **Dim**
  - $0 \leq a < p^k \in \mathbb{Z}_{p^k}^* \iff \text{MCD}(a, p^k) = 1$ , che è vero quando  $p \nmid a$  poiché  $p \in \mathbb{P}$
  - simmetricamente,  $0 \leq a < p^k \notin \mathbb{Z}_{p^k}^* \iff \exists n \in \mathbb{Z} \mid a = np$ 
    - \* i multipli di  $p$  sono tutti  $0 \leq np < p^k \implies 0 \leq n < p^{k-1}$  !!! **INCOMPLETA**
  - $\varphi(p^k) := \left| \mathbb{Z}_{p^k}^* \right| = \left| \mathbb{Z}_{p^k} - \{[a] \in \mathbb{Z}_{p^k} \mid \nexists [a]^{-1} \in \mathbb{Z}_{p^k}\} \right| = p^k - p^{k-1} = p^{k-1}(p-1)$

Oss

- **Hp**
  - $k \in \mathbb{N} \mid k \geq 1$
  - $p_1, \dots, p_k \in \mathbb{P}$
  - $i_1, \dots, i_k \geq 1$
  - $n \in \mathbb{N} \mid n = p_1^{i_1} \cdot \dots \cdot p_k^{i_k}$
- **Th**
  - $\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$
- **Dim**
  - per dimostrazione precedente  $\varphi(n) = \varphi(p_1^{i_1}) \cdot \dots \cdot \varphi(p_k^{i_k}) = p_1^{i_1-1}(p_1-1) \cdot \dots \cdot p_k^{i_k-1}(p_k-1) = p_1^{i_1} \cdot \dots \cdot p_k^{i_k} \cdot \frac{p_1-1}{p_1} \cdot \dots \cdot \frac{p_k-1}{p_k} = n \cdot \frac{p_1-1}{p_1} \cdot \dots \cdot \frac{p_k-1}{p_k} \implies$
  - $\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$