

# DISCLAIMER

Questo è un file che contiene una lista di tutti i teoremi, osservazioni, esempi, lemmi, corollari, formule e proposizioni **senza alcuna dimostrazione né definizione**, di conseguenza molte informazioni risulteranno essere senza alcun contesto se già non si conosce la materia. Detto questo, buona lettura

---

## Numeri complessi

### Teorema 1

- **Hp**
  - $a, b \in \mathbb{R}, z \in \mathbb{C} \mid z = a + ib$
  - $c, d \in \mathbb{R}, w \in \mathbb{C} \mid w = c + id$
- **Th**
  - $z + w = (a + b) + i(c + d)$
  - $z \cdot w = (ac - bd) + i(ad + bc)$

### Teorema 2

- **Hp**
  - $a, b \in \mathbb{R}, z \in \mathbb{C} \mid z = a + ib$
  - $c, d \in \mathbb{R}, w \in \mathbb{C} \mid w = c + id$
- **Th**
  - $\bar{z} + \bar{w} = \overline{z + w}$
  - $\bar{z} \cdot \bar{w} = \overline{z \cdot w}$

### Teorema 3

- $\forall \theta \quad e^{i\theta} = \cos \theta + i \sin \theta$

### Teorema 4

- **Hp**
  - $(\mathbb{C}, +, \cdot)$  è un gruppo
- **Th**
  - $(\mathbb{C}, +, \cdot)$  è un campo

### Teorema 5

- $|z \cdot w| = |z| \cdot |w| \quad \arg(z \cdot w) = \arg(z) + \arg(w)$
- $|\bar{w}| = |w| \quad \arg(\bar{w}) = -\arg(w)$
- $|w^{-1}| = |w|^{-1} \quad \arg(w^{-1}) = -\arg(w)$
- $\left| \frac{z}{w} \right| = \frac{|z|}{|w|} \quad \arg\left(\frac{z}{w}\right) = \arg(z) - \arg(w)$

### Teorema 6

- $z^n = |z|^n e^{in\theta} \quad \arg(z^n) = n \arg(z)$
- 

## Permutazioni

### Teorema 7

- **Hp**
  - $S_X := \{f \mid f : X \rightarrow Y \text{ biiettiva}\}$
- **Th**
  - $(S_X, \circ)$  è un gruppo, non abeliano se  $|X| \geq 3$

### Teorema 8

- **Hp**
  - $n \in \mathbb{N}$
  - $\sigma \in S_n$
  - $1 \leq i < n \in \mathbb{N}$
  - $I(\sigma, i) := \{n \in \mathbb{Z} \mid \sigma^n(i) = i\}$
- **Th**
  - $(I(\sigma, i), +) \subset (\mathbb{Z}, +)$  è un ideale

### Teorema 9

- **Hp**
  - **!!! RISCRIVI TUTTO**
  - $I(\sigma, i)$  è **ideale principale** in  $\mathbb{Z}$  generato da  $I(d)$ , dove  $d$  è la lunghezza del ciclo di  $i$ , quindi  $I(\sigma, i) = I(d)$
  - $I(\sigma, i) = I(d) \implies d \in I(\sigma, i)$

### Teorema 10

- **Hp**
  - $n \in \mathbb{N}$
  - $\sigma \in S_n \mid \sigma = \gamma_1 \dots \gamma_k$  sia la sua decomposizione in cicli
  - $d_j := \text{lunghezza di } \gamma_j \quad \forall j \in [1, k]$
  - $m := \text{lcm}(d_1, \dots, d_k)$
  - $I(\sigma) := \{n \in \mathbb{Z} \mid \sigma^n = \text{id}\}$
- **Th**
  - $o(\sigma) = m$

### Teorema 11

- **Hp**
  - $n \in \mathbb{N}$
  - $\sigma \in S_n$
- **Th**

- $\exists 1 \leq i_1, \dots, i_k < n \mid \sigma = \tau_{i_1, i_1+1} \dots \tau_{i_k, i_k+1}$ , quindi ogni permutazione può essere riscritta come composizione di trasposizioni adiacenti

### Teorema 12

- **Hp**
  - $n \in \mathbb{N}$
  - $\sigma \in S_n \mid \sigma = \tau_1 \dots \tau_k$  dove  $\forall j \in [1, k] \quad \tau_j = \tau_{j, j+1}$ , dunque tutte le trasposizioni sono adiacenti
- **Th**
  - $\text{sgn}(\sigma) = (-1)^k$

### Teorema 13

- **Hp**
  - $n \in \mathbb{N}$
  - $\sigma, \sigma' \in S_n \mid \begin{cases} \sigma = \tau_1 \dots \tau_k \\ \sigma' = \tau'_1 \dots \tau'_h \end{cases}$ , dove ogni trasposizione è adiacente
- **Th**
  - $\text{sgn}(\sigma\sigma') = \text{sgn}(\sigma) \cdot \text{sgn}(\sigma')$

### Teorema 14

- **Hp**
  - $n \in \mathbb{N}$
  - $\sigma \in S_n$
- **Th**
  - $\text{sgn}(\sigma^{-1}) = \text{sgn}(\sigma)$

### Teorema 15

- **Hp**
  - $n \in \mathbb{N}$
  - $A_n := \{\sigma \in S_n \mid \sigma \text{ pari}\}$
- **Th**
  - $A_n \subset S_n$  è un sottogruppo, detto *gruppo alterno di ordine n*

### Teorema 16

- **Hp**
  - $n \in \mathbb{N}$
  - $\sigma, \sigma' \in S_n$
  - $\sigma \sim \sigma' \iff \exists \alpha \in S_n \mid \sigma' = \alpha\sigma\alpha^{-1}$
- **Th**
  - $\text{sgn}(\sigma') = \text{sgn}(\sigma)$

### Teorema 17

- **Hp**
  - $n \in \mathbb{N}$

- $\sigma, \sigma' \in S_n \mid \sigma := \gamma_1 \dots \gamma_k, \sigma' := \gamma'_1 \dots \gamma'_h$
- $\sigma \sim \sigma' \iff \exists \alpha \in S_n \mid \sigma' = \alpha \sigma \alpha^{-1}$ , che costituisce dunque la relazione di coniugio
- **Th**
  - $\sigma \sim \sigma' \iff \begin{cases} k = h \\ d = d'_1 \\ \vdots \\ d_k = d'_h = d'_k \end{cases}$ , dove  $d_j$  è la lunghezza del ciclo  $\gamma_j$  e  $d'_j$  è la lunghezza del ciclo  $\gamma'_j$

### Teorema 18

- **Hp**
    - $n \in \mathbb{N}$
    - $\sigma \in S_n \mid \sigma := \gamma_1 \dots \gamma_k$
  - **Th**
    - $\text{sgn}(\sigma) = (-1)^{n-k}$
- 

## Ideali

### Teorema 19

- **Hp**
  - $(A, +, \cdot)$  anello
  - $a \in \mathbb{Z}$
  - $I(a) := \{ax \mid x \in A\}$
- **Th**
  - $I(a)$  è un ideale, e prende il nome di *ideale di A generato da a*  $a \in A$

### Teorema 20

- **Hp**
  - $A$  dominio di integrità
  - $a, b \in A$
- **Th**
  - $I(a) = I(b) \iff \exists c \in A^* \mid a = bc$

### Teorema 21

- **Hp**
  - $a, b \in \mathbb{Z} - \{0\}$
- **Th**
  - $I(a) = I(b) \iff a = \pm b$

### Teorema 22

- **Hp**
  - $(A, +, \cdot)$  anello

- $a_1, \dots, a_n \in \mathbb{Z}$
- $I(a_1, \dots, a_n) := \{a_1 b_1 + \dots + a_n b_n \mid b_1, \dots, b_n \in A\}$
- **Th**
  - $I(a_1, \dots, a_n)$  è un ideale, e prende il nome di *ideale di A generato dagli*  $a_1, \dots, a_n \in A$

### Teorema 23

- **Hp**
  - $(A, +, \cdot)$  anello
  - $+: A/I \times A/I \rightarrow A/I$
  - $\cdot: A/I \times A/I \rightarrow A/I$
- **Th**
  - $(A/I, +, \cdot)$  è un anello

### Teorema 24

- **Hp**
  - $I \subset \mathbb{Z}$  ideale
- **Th**
  - $\exists! d \in \mathbb{Z}_{\geq 0} \mid I = I(d)$ , o equivalentemente,  $\mathbb{Z}$  è un anello a ideali principali

### Teorema 25

- **Hp**
  - $a_1, \dots, a_n \in \mathbb{Z}$
- **Th**
  - $\exists! d = \text{MCD}(a_1, \dots, a_n) \mid I(a_1, \dots, a_n) = I(d)$

### Teorema 26

- **Hp**
  - $a_1, \dots, a_n \in \mathbb{Z}$
  - $d := \text{MCD}(a_1, \dots, a_n)$
- **Th**
  - $\exists x_1, \dots, x_n \in \mathbb{Z} \mid a_1 x_1 + \dots + a_n x_n = d$ , che prende il nome di *identità di Bézout*

### Teorema 27

- !!! MANCA DIMOSTRAZIONE SISTEMA DI IDENTITÀ DI BÉZOUT
- 

## Operazioni sugli ideali

### Teorema 28

- **Hp**
  - $(A, +, \cdot)$  anello commutativo
  - $I, J \subset A$  ideali
- **Th**

- $I + J$  è un ideale

### Teorema 29

- **Hp**
  - $(A, +, \cdot)$  anello commutativo
  - $I, J \subset A$  ideali
- **Th**
  - $I \cap J$  è un ideale

### Teorema 30

- **Hp**
  - $(A, +, \cdot)$  anello commutativo
  - $I, J \subset A$  ideali
- **Th**
  - $I \cdot J$  è un ideale

### Teorema 31

- **Hp**
  - $a, b \in \mathbb{Z}$
  - $d := \text{MCD}(a, b)$
- **Th**
  - $I(a) + I(b) = I(d)$

### Teorema 32

- **Hp**
    - $a, b \in \mathbb{Z}$
  - **Th**
    - $I(a) \cdot I(b) = I(a \cdot b)$
- 

## Polinomi

### Teorema 33

- **Hp**
  - $(\mathbb{K}, +, \cdot)$  anello
- **Th**
  - $(\mathbb{K}[x], +, \cdot)$  è un anello

### Teorema 34

- **Hp**
  - $\mathbb{K}$  campo
  - $a(x), b(x) \in \mathbb{K}[x]$
- **Th**

$$- \deg(a(x) \cdot b(x)) = \deg(a(x)) + \deg(b(x))$$

### Teorema 35

- **Hp**
  - $\mathbb{K}$  campo
  - $a(x) \in \mathbb{K}[x] \mid \deg(a(x)) \geq 1$
- **Th**
  - $\nexists a^{-1}(x) \in \mathbb{K}[x]$

### Teorema 36

- **Hp**
  - $\mathbb{K}$  campo
- **Th**
  - $\mathbb{K}[x]^* = \mathbb{K}^* \subset \mathbb{K}[x]$

### Teorema 37

- **Hp**
  - $\mathbb{K}$  campo
- **Th**
  - $\mathbb{K}[x]$  è un dominio

### Teorema 38

- **Hp**
  - $\mathbb{K}$  campo
  - $p(x) \in \mathbb{K}[x]$
  - $c \in \mathbb{K}$
- **Th**
  - $p(c) = 0 \iff x - c \mid p(x)$

### Teorema 39

- **Hp**
  - $\mathbb{K}$  campo
  - $p(x) \in \mathbb{K}[x]$
  - $n := \deg(p(x))$
- **Th**
  - $|\{c \in \mathbb{K} \mid p(c) = 0\}| \leq n$

### Teorema 40

- **Hp**
  - $\mathbb{K}$  campo
  - $I \subset \mathbb{K}[x]$  ideale
- **Th**
  - $I$  è un ideale principale

### Teorema 41

- **Hp**
  - $\mathbb{K}$  campo
  - $I(a_1(x)), \dots, I(a_n(x)) \subset \mathbb{K}[x]$  ideali
  - $\exists d(x) \in \mathbb{K}[x] \mid I(a_1(x), \dots, a_n(x)) = I(d(x))$
- **Th**
  - $d(x) = \text{MCD}(a_1(x), \dots, a_n(x))$

### Teorema 42

- **Hp**
  - $\mathbb{K}$  campo
  - $I(a_1(x)), \dots, I(a_n(x)) \subset \mathbb{K}[x]$  ideali
  - $\exists m(x) \in \mathbb{K}[x] \mid I(a_1(x)) \cap \dots \cap I(a_n(x)) = I(m(x))$
- **Th**
  - $m(x) = \text{mcm}(a_1(x), \dots, a_n(x))$

### Teorema 43

- **Hp**
  - $\mathbb{K}$  campo
  - $a_1(x), \dots, a_n(x) \in \mathbb{K}[x]$
  - $c \in \mathbb{K}$
  - $d(x) := \text{MCD}(a_1(x), \dots, a_n(x))$
- **Th**
  - $a_1(c) = \dots = a_n(c) = 0 \iff d(c) = 0$

### Teorema 44

- **Hp**
  - $\mathbb{K}$  campo
  - $p(x) \in \mathbb{K}[x]$
- **Th**
  - $p(x) \in \mathbb{K}[x]$  irriducibile  $\iff p(x)$  primo

### Teorema 45

- **Hp**
  - $\mathbb{K}$  campo
  - $p(x) \in \mathbb{K}[x] - \{0\}$
- **Th**
  - $\exists! q_1(x), \dots, q_k(x) \in \mathbb{K}[x]$  irriducibili e monici,  $c \in \mathbb{K} - \{0\} \mid p(x) = c \cdot q_1(x) \cdot \dots \cdot q_k(x)$
  - in particolare, i polinomi sono unici a meno di un riordinamento

### Teorema 46

- **Hp**
  - $\mathbb{K}$  campo
  - $p(x) \in \mathbb{K}[x]$



- **Th**
  - $p(x)$  irriducibile  $\iff \deg(p(x)) = 1$

#### Teorema 47

- **Hp**
  - $p(x) \in \mathbb{R}[x]$
- **Th**
  - $p(x)$  irriducibile  $\iff \deg(p(x)) = 1$  oppure  $\deg(p(x)) = 2 \wedge \Delta < 0$

#### Teorema 48

- **Hp**
  - $a_0, \dots, a_n \in \mathbb{Z} \mid a_0, a_n \neq 0$
  - $p(x) \in \mathbb{Z}[x] \mid p(x) = a_0 + \dots + a_n x^n$
  - $a, b \in \mathbb{Z} \mid \text{MCD}(a, b) = 1$
  - $p(\frac{a}{b}) = 0$
- **Th**
  - $a \mid a_0 \wedge b \mid a_n$

#### Teorema 49

- !!! MANCA UN TEOREMA ENORME
- 

## Coefficienti binomiali

#### Teorema 50

- **Hp**
  - $n, k \in \mathbb{N}$
- **Th**
  - $\binom{n}{k} = \binom{n}{n-k}$

#### Teorema 51

- **Hp**
  - $n, k \in \mathbb{N}$
- **Th**
  - $\binom{n}{k+1} = \binom{n-1}{k+1} \binom{n-1}{k}$

#### Teorema 52

- **Hp**
  - $p \in \mathbb{P}$
  - $k \in \mathbb{N} \mid 0 < k < p$
- **Th**

$$- p \mid \binom{p}{k}$$

### Teorema 53

- **Hp**
  - $n \in \mathbb{Z}$
  - $p \in \mathbb{P} : p \mid n$
  - $[a] \in \mathbb{Z}_p$
- **Th**
  - $n \cdot [a] = [0]$  in  $\mathbb{Z}_p$

### Teorema 54

- **Hp**
  - $n \in \mathbb{Z}$
  - $p \in \mathbb{P} : p \mid n$
  - $[a] \in \mathbb{Z}_p$
  - $k \in \mathbb{N} \mid 0 < k < p$
- **Th**
  - $\binom{p}{k} \cdot [a] = [0]$  in  $\mathbb{Z}_p$

### Teorema 55

- **Hp**
  - $p \in \mathbb{P}$
  - $[a], [b] \in \mathbb{Z}_p$
- **Th**
  - $([a] + [b])^p = [a]^p + [b]^p$  in  $\mathbb{Z}_p$

### Teorema 56

- **Hp**
    - $p \in \mathbb{P}$
    - $[a_1], \dots, [a_n] \in \mathbb{Z}_p$
  - **Th**
    - $([a_1] + \dots + [a_n])^p = [a_1]^p + \dots + [a_n]^p$  in  $\mathbb{Z}_p$
- 

## Gruppi

### Teorema 57

- **Hp**
  - $G$  monoide
  - $\exists e \in G$  elemento neutro
- **Th**
  - $e$  è unico in  $G$

### Teorema 58

- **Hp**
  - $(G, m)$  gruppo
  - $x \in G$
  - $\exists x^{-1} \in G$  inverso di  $x$  rispetto ad  $m$
- **Th**
  - $x^{-1}$  è unico in  $G$  per  $x$  rispetto a  $m$

### Teorema 59

- **Hp**
  - $X, Y$  insiemi,
  - $Y^X = \{f \mid f : X \rightarrow Y\}$
- **Th**
  - $(X^X, \circ)$  è monoide

### Teorema 60

- **Hp**
    - $X, Y$  insiemi finiti
  - **Th**
    - $|Y^X| = |Y|^{|X|}$
- 

## Anelli

### Teorema 61

- **Hp**
  - $(A, +, \cdot)$  anello commutativo
- **Th**
  - $(A^*, \cdot)$  è un gruppo

### Teorema 62

- **Hp**
  - $(A, +, \cdot)$  anello commutativo
- **Th**
  - $(A^*, \cdot) \subset (A, \cdot)$  è un sottogruppo

### Teorema 63

- **Hp**
  - $(A, +, \cdot)$  anello commutativo
- **Th**
  - $x \mid 0 \iff x \notin A^*$

### Teorema 64

- **Hp**
  - $A$  campo
- **Th**
  - $A$  dominio di integrità

### Teorema 65

- **Hp**
  - $A$  dominio di integrità
- **Th**
  - $a$  primo  $\implies a$  irriducibile

### Teorema 66

- **Hp**
  - 1)  $H$  è sottogruppo normale
  - 2)  $\forall g \in G, h \in H \quad g \cdot h \cdot g^{-1} \in H$
  - 3)  $\forall g \in G, h \in H \quad \exists k \in H \mid g \cdot h = k \cdot g$
- **Th**
  - le tre formulazioni sono equivalenti

### Teorema 67

- **Hp**
  - $G$  gruppo
  - $g \in G$
- **Th**
  - $(H(g), \cdot) \subset (G, \cdot)$  è sottogruppo

### Teorema 68

- **Hp**
  - $G$  gruppo
  - $g \in G$
  - $I(g) := \{n \in \mathbb{Z} \mid g^n = e\}$
- **Th**
  - $I(g)$  è un ideale

### Teorema 69

- **Hp**
  - $G$  gruppo
  - $g \in G$
  - $\exists! d \geq 0 \mid I(g) = I(d)$
- **Th**
  - $d = 0 \implies o(g) := |H(g)| = |\mathbb{Z}|$ , dunque infinito
  - $d > 0 \implies d = o(g)$

### Teorema 70

- **Hp**
  - $G$  gruppo finito
  - $g \in G \mid d := o(g)$  finito
- **Th**
  - $g^{|G|} = e$

### Teorema 71

- **Hp**
  - $G$  gruppo finito
  - $g \in G$
- **Th**
  - $o(g) = o(g^{-1})$

### Teorema 72

- **Hp**
  - $G$  gruppo finito
  - $k \in \mathbb{Z}$
- **Th**
  - $\forall g \in G \quad o(g^k) \mid o(g)$

### Teorema 73

- **Hp**
  - $G$  gruppo finito
  - $g, h \in G \mid gh = hg$
  - $d := \text{MCD}(o(g), o(h))$
  - $m := \text{mcm}(o(g), o(h))$
- **Th**
  - $\frac{m}{d} \mid o(gh) \wedge o(gh) \mid m$

### Teorema 74

- **Hp**
    - $G$  gruppo finito
    - $g, h \in G \mid gh = hg$
    - $d := \text{MCD}(o(g), o(h)) = 1$
    - $m := \text{mcm}(o(g), o(h))$
  - **Th**
    - $o(gh) = o(hg) = m$
-

## Insieme quoziente

### Teorema 75

- **Hp**
  - $n \in \mathbb{Z}$
  - $I(n) := \{nk \mid k \in \mathbb{Z}\}$
- **Th**
  - $(\mathbb{Z}_n, +)$  è un gruppo

### Teorema 76

- **Hp**
  - $p \in \mathbb{P}$
  - $a, b \in \mathbb{Z}$
  - $p \mid ab$
- **Th**
  - $p \mid a \vee p \mid b$

### Teorema 77

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

### Teorema 78

- **Hp**
  - $n \in \mathbb{Z}$
- **Th**
  - $\forall [a] \in \mathbb{Z}_n \quad \text{MCD}(a, n) = 1 \iff [a] \in \mathbb{Z}_n^*$

### Teorema 79

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

### Teorema 80

- **Hp**
  - $p \in \mathbb{P}$
- **Th**
  - $(\mathbb{Z}_p^*, \cdot)$  è ciclico

### Teorema 81

- **Hp**

- $n, m \in \mathbb{N}$
- **Th**
  - $[a] \in \mathbb{Z}_{mn}^* \iff [a] \in \mathbb{Z}_m^* \wedge [a] \in \mathbb{Z}_n^*$

### Teorema 82

- **Hp**
  - $m, n \in \mathbb{N} \mid \text{MCD}(m, n) = 1$
- **Th**
  - $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

### Teorema 83

- **Hp**
  - $p \in \mathbb{P}$
  - $k \in \mathbb{N} \mid k \geq 1$
- **Th**
  - $\varphi(p^k) = p^{k-1}(p-1)$

### Teorema 84

- **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**
    - $\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$
- 

## Induzione

### Teorema 85

- **Hp**
    - $\begin{cases} F_0 = 0 \\ F_1 = 1 \\ F_n = F_{n-1} + F_{n-2} \quad \forall n \geq 2 \end{cases}$  è detta *sequenza di Fibonacci*
    - $x^2 - x - 1 = 0$  ha come soluzioni  $\begin{cases} \phi := \frac{1 + \sqrt{5}}{2} \\ \psi := \frac{1 - \sqrt{5}}{2} \end{cases}$
  - **Th**
    - la formula chiusa della serie di Fibonacci è  $F_n = \frac{\phi^n - \psi^n}{\phi - \psi} = \frac{\phi^n - \psi^n}{\sqrt{5}}$
-

## Teorema fondamentale dell'algebra

- **Hp**
    - $\mathbb{K}$  campo
    - $p(x) \in \mathbb{K}[x] \mid p(x) = a_0x^0 + \dots + a_nx^n$
  - **Th**
    - $\exists z \in \mathbb{C} \mid p(z) = 0$
- 

## Teorema della divisione euclidea con il resto

- **Hp**
  - $m \in \mathbb{Z}$
  - $n \in \mathbb{Z} - \{0\}$
- **Th**
  - $\exists! q, r \in \mathbb{Z} \mid m = nq + r \quad 0 \leq r < n$

## Teorema 86

- **Hp**
    - $\mathbb{K}$  campo
    - $a(x), b(x) \in \mathbb{K}[x] \mid b(x) \neq 0$
  - **Th**
    - $\exists! q(x), r(x) \in \mathbb{K}[x] \mid a(x) = b(x) \cdot q(x) + r(x) \quad \deg(r(x)) < \deg(b(x))$ , che è detto *teorema della divisione con il resto tra polinomi*
- 

## Teorema di Lagrange

- **Hp**
  - $G$  gruppo finito
  - $H \subset G$  sottogruppo finito
- **Th**
  - $|G| = |H| \cdot |G/H|$

## Teorema 87

- **Hp**
  - $a_1, \dots, a_n \geq 2 \in \mathbb{Z} \mid \text{MCD}(a_i, a_j) = 1 \quad \forall i, j \in [1, n] : i \neq j$
  - $m := \text{mcm}(a_1, \dots, a_n)$
- **Th**
  - $m = a_1 \cdot \dots \cdot a_n$

## Teorema 88

- **Hp**
  - $n \in \mathbb{N}$



- $a_1, \dots, a_n \in \mathbb{Z}_{n \geq 2}$
- $m := \text{mcm}(a_1, \dots, a_n)$
- **Th**
  - $\exists \phi \mid \phi : \mathbb{Z}_m \rightarrow \mathbb{Z}_{a_1} \times \dots \times \mathbb{Z}_{a_n} : x \pmod{m} \rightarrow (x \pmod{a_1}, \dots, x \pmod{a_n})$
  - $\phi$  è una funzione ben definita, ed è iniettiva

### Teorema 89

- **Hp**
  - $k \in \mathbb{N}$
  - $n_1, \dots, n_k \in \mathbb{N} - \{0\} \mid \forall i, j \in [1, k] \quad i \neq j \implies \text{MCD}(n_i, n_j) = 1$
  - $N := \text{mcm}(n_1, \dots, n_k)$
  - $[a] \in \mathbb{Z}_N^*$
  - $o := o([a])$  in  $\mathbb{Z}_N^*$
  - $\forall h \in [1, k] \quad o_h := o([a])$  in  $\mathbb{Z}_{n_h}^*$
- **Th**
  - $o = \text{mcm}(o_1, \dots, o_k)$

### Teorema 90

- !!! NON HO CAPITO UN CAZZO
- 

### Piccolo teorema di Fermat

- **Hp**
  - $p \in \mathbb{P}$
  - $a \in \mathbb{Z}$
- **Th**
  - $a^p \equiv a \pmod{p}$

### Teorema 91

- **Hp**
  - $p \in \mathbb{P}$
  - $[a] \in \mathbb{Z}_p - \{0\}$
- **Th**
  - $[a]^{-1} = [a]^{p-2}$

### Teorema 92

- **Hp**
  - $p \in \mathbb{P}$
- **Th**
  - $\prod_{0 < a < p} (x - a) \equiv x^{p-1} - 1 \pmod{p}$

### Teorema 93

- !!! NON HO CAPITO UN CAZZO
- 

### Teorema di Eulero

- Hp
  - $a, n \in \mathbb{N} \mid \text{MCD}(a, n) = 1$
- Th
  - $a^{\varphi(n)} \equiv 1 \pmod{n}$

### Teorema 94

- Hp
  - $G, H$  gruppi
  - $f : G \rightarrow H$  morfismo di gruppi
- Th
  - $G/\text{Ker}(f) \cong \text{Im}(f)$ , o alternativamente  $\exists \varphi \mid \varphi : G/\text{Ker}(f) \rightarrow \text{Im}(f) : [g] \rightarrow f(g)$  isomorfismo di gruppi

### Teorema 95

- Hp
    - $G$  gruppo  $\mid |G| = 4$
  - Th
    - $G \cong \mathbb{Z}_4$  oppure  $G \cong K_4$
- 

## Relazioni

### Teorema 96

- Hp
  - $m, n \in \mathbb{N}$
  - $m \mid n \iff \exists p \in \mathbb{N} \mid mp = n$
- Th
  - $\mid$  è ordine parziale

### Teorema 97

- Hp
  - $a, b \in \mathbb{Z}$
  - $a \equiv b \pmod{n} \iff m \mid b - a$  è detta congruenza modulo  $n$
- Th
  - $\equiv$  è una relazione di equivalenza

### Teorema 98

- **Hp**
  - $x, y \in \mathbb{Z} \mid x \equiv y \pmod{n}$
  - $d \in \mathbb{Z} : d \mid n$
- **Th**
  - $x \equiv y \pmod{d}$

### Teorema 99

- **Hp**
  - $n \in \mathbb{N}$
  - $[a], [b] \in \mathbb{Z}_n$
  - $d := \text{MCD}(a, n)$
- **Th**
  - $d \nmid b \implies \nexists [x] \in \mathbb{Z}_n \mid ax \equiv b \pmod{n}$
  - $d \mid b \implies \forall [x] \in \mathbb{Z}_n \mid ax \equiv b \pmod{n} \quad x \text{ è anche tale che } \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$

### Teorema 100

- **Hp**
  - $G$  gruppo
  - $g, h \in G$
  - $g \sim h \iff \exists a \in G \mid h = a \cdot g \cdot a^{-1}$  è detta *relazione di coniugio*
- **Th**
  - $\sim$  è una relazione di equivalenza

### Teorema 101

- **Hp**
  - $G$  gruppo
- **Th**
  - $\forall x, y \in G \quad x \approx y \iff [x] \cap [y] = \emptyset \vee x \sim y \iff [x] = [y]$

### Teorema 102

- **Hp**
  - $G$  gruppo
  - $\sim$  è una relazione di equivalenza in  $G$
- **Th**
  - $\sim$  induce una partizione di  $G$ , dunque  $G = \coprod_{[x] \in X/\sim} [x]$

### Teorema 103

- **Hp**
  - $G$  gruppo
  - $H \subset G$  sottogruppo
  - $x, y \in G$
- **Th**

- $x \sim_S y \iff x^{-1}y \in H$  è una relazione di equivalenza

### Teorema 104

- **Hp**
  - $(\mathbb{Z}, +)$  anello
  - $n \in \mathbb{N}_{\geq 2}$
  - $I(n) := \{nk \mid k \in \mathbb{Z}\}$
  - $a, b \in \mathbb{Z}$
- **Th**
  - $a \sim_S b \iff a \equiv b \pmod{n}$

### Teorema 105

- **Hp**
  - $G$  gruppo
  - $H \subset G$  sottogruppo
  - $x \in G$
  - $[x] = \{y \in G \mid y \sim_S x\}$
- **Th**
  - $xH := \{xh \mid h \in H\} = [x]$

### Teorema 106

- **Hp**
  - $G$  gruppo
  - $H \subset G$  sottogruppo
  - $x \in G$
- **Th**
  - $|xH| = |H|$

### Teorema 107

- **Hp**
    - $G$  gruppo
    - $H \subset G$  sottogruppo
    - $+: G/H \times G/H \rightarrow G/H$
  - **Th**
    - $(G/H, +)$  è gruppo abeliano
- 

## Morfismi

### Teorema 108

- **Hp**
  - $(G, \cdot), (H, \cdot)$  gruppi
  - $1_G$  neutro per  $G$
  - $1_H$  neutro per  $H$

- $f : G \rightarrow H$  morfismo
- **Th**
  - $f(1_G) = 1_H$

### Teorema 109

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

### Teorema 110

- **Hp**
  - $f : G \rightarrow H$  isomorfismo
- **Th**
  - $f^{-1} : H \rightarrow G$  isomorfismo

### Teorema 111

- **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

### Teorema 112

- **Hp**
  - $f : \mathbb{Z}_n \rightarrow H : [k] \rightarrow \zeta^k$
- **Th**
  - $f$  isomorfismo di gruppi  $(\mathbb{Z}_n, +)$  e  $(H, \cdot)$

### Teorema 113

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

### Teorema 114

- **Hp**
  - !!! MANCA UN TEOREMA CHE NON HO CAPITO NIENTE
- **Th**

**Teorema 115**

- **Hp**
  - $f : \mathbb{Z} \rightarrow \mathbb{Z}_n : k \rightarrow [k]$
- **Th**
  - $f$  morfismo di anelli  $(\mathbb{Z}, +, \cdot)$  e  $(\mathbb{Z}_n, +, \cdot)$

**Teorema 116**

- **Hp**
  - $n \mid m$
  - $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_n : x \pmod{m} \rightarrow x \pmod{n}$
- **Th**
  - $f$  morfismo di anelli  $(\mathbb{Z}_m, +, \cdot)$  e  $(\mathbb{Z}_n, +, \cdot)$

**Teorema 117**

- **Hp**
  - $G$  gruppo
  - $f : G \rightarrow G : h \rightarrow g \cdot h \cdot g^{-1}$  per qualche  $g \in G$
- **Th**
  - $f$  morfismo di gruppi  $(G, \cdot)$  e  $(G, \cdot)$

**Teorema 118**

- **Hp**
  - $G, H$  gruppi
  - $f : G \rightarrow H$  morfismo
- **Th**
  - $\text{Ker}(f) \subset G$  è sottogruppo

**Teorema 119**

- **Hp**
  - $G, H$  gruppi
  - $f : G \rightarrow H$  morfismo
- **Th**
  - $\text{Im}(f) \subset G$  è sottogruppo

**Teorema 120**

- **Hp**
  - $G, H$  gruppi
  - $f : G \rightarrow H$  morfismo
- **Th**
  - $f$  iniettiva  $\iff \text{Ker}(f) = \{1_G\}$

**Teorema 121**

- **Hp**

- $A, B$  anelli
- $f : A \rightarrow B$  morfismo di anelli
- **Th**
  - $\text{Ker}(f)$  ideale

### Teorema 122

- **Hp**
  - $A, B$  anelli
  - $f : A \rightarrow B$  morfismo di anelli
- **Th**
  - $\text{Im}(f)$  sottoanello

### Teorema 123

- **Hp**
  - $f : \mathbb{Z} \rightarrow \mathbb{C} - \{0\} : k \rightarrow \zeta^k$
  - $f$  morfismo di gruppi  $(\mathbb{Z}, +)$  e  $(\mathbb{C} - \{0\}, \cdot)$
  - $I(n)$  ideale generato da  $n$  !!! **CHI È N**
- **Th**
  - $\text{Ker}(f) = I(n)$

### Teorema 124

- !!! coso finale su **H** che non ho capito niente

### Teorema 125

- **Hp**
    - $G, H$  gruppi
    - $f : G \rightarrow H$  morfismo
  - **Th**
    - $\text{Ker}(f)$  è sottogruppo normale
- 

## Gruppi diedrali

### Teorema 126

- **Hp**
  - $n \in \mathbb{N}_{\geq 2}$
  - $D_n$  insieme delle simmetrie dell' $n$ -gono regolare
- **Th**
  - $|D_n| = 2n$

### Teorema 127

- **Hp**
  - $n \in \mathbb{N}_{\geq 2}$

- $D_n$  insieme delle simmetrie dell' $n$ -gono regolare
- $\cdot$  è l'operazione di composizione delle simmetrie
- **Th**
  - $(D_n, \cdot)$  è un gruppo

### Teorema 128

- **Hp**
  - $D_2$  gruppo diedrale
- **Th**
  - $(D_2, \cdot)$  è l'unico gruppo diedrale abeliano

### Teorema 129

- **Hp**
  - $D_n$  gruppo diedrale
- **Th**
  - $D_n \hookrightarrow S_n$
  - $\exists X \subset S_n$  sottogruppo di  $S_n$  |  $D_n \cong X$
  - \*  $D_3 \cong S_3$

### Teorema 130

- **Hp**
    - $K_4$  è il gruppo di Klein
  - **Th**
    - $K_4 \cong D_2$
-