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.

Spazi Vettoriali

Teorema 1

- **Hp**
  - $n \in \mathbb{N}$
  - $\mathbb{K}$ campo
- **Th**
  - $\mathbb{K}^n$ spazio vettoriale su $\mathbb{K}$

Teorema 2

- **Hp**
  - $n \in \mathbb{N}$
  - $\mathbb{K}$ campo
  - V spazio vettoriale su $\mathbb{K}$
  - $v_1, \ldots, v_n \in V$
- **Th**
  - $\mathrm{span}(v_1, \ldots, v_n)$ è un sottospazio vettoriale di V

Teorema 3

- **Hp**
  - $n \in \mathbb{N}$
  - $\mathbb{K}$ campo
  - $e_1 := (1, 0, \ldots, 0), \ldots, e_n := (0, \ldots, 0, 1) \in \mathbb{K}^n$
- **Th**
  - $e_1, \ldots, e_n$ sono una base di $\mathbb{K}^n$, ed è detta *base canonica*

Teorema 4

- **Hp**
  - $n \in \mathbb{N}$
  - $\mathbb{K}$ campo
  - V spazio vettoriale su $\mathbb{K}$
  - $v_1, \ldots, v_n \in V$
- **Th**
  - $v_1, \ldots, v_n$ linearmente indipendenti $\iff$ $v_1, \ldots, v_{n-1}$ linearmente indipendenti $\land v_n \notin \mathrm{span}(v_1, \ldots, v_{n-1})$

Teorema 5

- **Hp**
  - $m, k \in \mathbb{N}$
  - $\mathbb{K}$ campo
  - V spazio vettoriale su $\mathbb{K}$
  - $w_1, \ldots, w_m \in V$
  - $v_1, \ldots, v_k \in \text{span}(w_1, \ldots, w_m) \mid v_1, \ldots, v_k$ linearmente indipendenti
- **Th**
  - $k \leq m$

Teorema 6

- **Hp**
  - $n, m \in \mathbb{N}$
  - $\mathbb{K}$ campo
  - V spazio vettoriale su $\mathbb{K}$
  - $w_1, \ldots, w_m \in V \mid w_1, \ldots, w_m$ base di V
  - $v_1, \ldots, v_n \in V \mid v_1, \ldots, v_n$ base di V
- **Th**
  - $n = m$, il che implica che la cardinalità delle basi di uno spazio vettoriale è unica

Teorema 7

- **Hp**
  - $n \in \mathbb{N}$
  - $\mathbb{K}$ campo
  - V spazio vettoriale su $\mathbb{K}$
  - $v_1, \ldots, v_n \in V$
- **Th**
  - $v_1, \ldots, v_n$ base di $V \iff \forall v \in V \quad \exists! \lambda_1, \ldots, \lambda_n \in \mathbb{K} \mid v = \lambda_1 v_1 + \ldots + \lambda_n v_n$

Teorema 8

- **Hp**
  - $\mathbb{K}$ campo
  - V spazio vettoriale su $\mathbb{K}$
  - $n := \dim(V)$
- **Th**
  - $V \cong \mathbb{K}^n$

Teorema 9

- !!! **QUI C'È UN BUCONE**

Teorema 10

- **Hp**
  - $\mathbb{K}$ campo
  - W spazio vettoriale su $\mathbb{K}$

- $n := \dim(W)$
- $k \in \mathbb{N} \mid k < n$
- $w_1, \ldots, w_k \in W$ linearmente indipendenti

- **Th**
  - $\exists w_{k+1}, \ldots, w_n \in W \mid w_1, \ldots, w_n$ è una base di W

Teorema 11

- **Hp**
  - $\mathbb{K}$ campo
  - W spazio vettoriale su $\mathbb{K}$
  - $n := \dim(W)$
  - $m \in \mathbb{N} \mid m \geq n$
  - $w_1, \ldots, w_m \in W \mid w_1, \ldots, w_m$ generatori di W
- **Th**
  - $\exists 1 \leq i_1, \ldots, i_n \leq m \mid w_{i_1}, \ldots, w_{i_n}$ è una base di W

Teorema 12

- **Hp**
  - $\mathbb{K}$ campo
  - W spazio vettoriale su $\mathbb{K}$
  - $n := \dim(W)$
  - $w_1, \ldots, w_n \in W$
- **Th**
  - $w_1, \ldots, w_n$ linearmente indipendenti $\iff$ $w_1, \ldots, w_n$ generatori di W

Numeri complessi

Teorema 13

- **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 14

- **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**
  - $\overline{z} + \overline{w} = \overline{z + w}$
  - $\overline{z} \cdot \overline{w} = \overline{z \cdot w}$

Teorema 15

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

Teorema 16

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

Teorema 17

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

Teorema 18

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

Permutazioni

Teorema 19

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

Teorema 20

- **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 21

- **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 22

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

Teorema 23

- **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 24

- **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 25

- **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 26

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

Teorema 27

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

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

Teorema 28

- **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 29

- **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 γ_j e d'_j è la lunghezza del ciclo γ'_j

Teorema 30

- **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 31

- **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 $a \in A$*

Teorema 32

- **Hp**

- A dominio di integrità
- $a, b \in A$

- **Th**
  - $I(a) = I(b) \iff \exists c \in A^* \mid a = bc$

Teorema 33

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

Teorema 34

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

Teorema 35

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

Teorema 36

- **Hp**
  - $I \subset \mathbb{Z}$ ideale
- **Th**
  - $\exists!\ d \in \mathbb{N} \mid I = I(d)$, o equivalentemente, in $\mathbb{Z}$ ogni ideale è principale

Teorema 37

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

Teorema 38

- **Hp**
  - $a_1, \ldots, a_n \in \mathbb{Z}$
  - $d := \mathrm{MCD}(a_1, \ldots, a_n)$

- **Th**
  - $\exists x_1, \ldots, x_n \in \mathbb{Z} \mid a_1x_1 + \ldots + a_nx_n = d$, che prende il nome di *identità di Bézout*

Teorema 39

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

Operazioni sugli ideali

Teorema 40

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

Teorema 41

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

Teorema 42

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

Teorema 43

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

Teorema 44

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

Polinomi

Teorema 45

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

Teorema 46

- **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 47

- **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 48

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

Teorema 49

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

Teorema 50

- **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 51

- **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 52

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

Teorema 53

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

Teorema 54

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

Teorema 55

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

Teorema 56

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

Teorema 57

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

Teorema 58

- **Hp**
  - $\mathbb{K}$ campo
  - $p(x) \in \mathbb{K}[x]$
- **Th**
  - $p(x)$ irriducibile $\iff \deg(p(x)) = 1$

Teorema 59

- **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 60

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

Teorema 61

- **!!! MANCA UN TEOREMA ENORME**

Coefficienti binomiali

Teorema 62

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

Teorema 63

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

Teorema 64

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

Teorema 65

- **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 66

- **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 67

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

Teorema 68

- **Hp**
  - $p \in \mathbb{P}$
  - $[a_1], \ldots, [a_n] \in \mathbb{Z}_p$
- **Th**

- $([a_1] + \ldots + [a_n])^p = [a_1]^p + \ldots + [a_n]^p$ in $\mathbb{Z}_p$

Gruppi

Teorema 69

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

Teorema 70

- **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 71

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

Teorema 72

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

Anelli

Teorema 73

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

Teorema 74

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

Teorema 75

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

Teorema 76

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

Teorema 77

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

Teorema 78

- **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 79

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

Teorema 80

- **Hp**
  - G gruppo
  - $g \in G$

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

Teorema 81

- **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 82

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

Teorema 83

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

Teorema 84

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

Teorema 85

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

Teorema 86

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

Insieme quoziente

Teorema 87

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

Teorema 88

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

Teorema 89

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

Teorema 90

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

Teorema 91

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

- $\mathbb{Z}_p$ campo

Teorema 92

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

Teorema 93

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

Teorema 94

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

Teorema 95

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

Teorema 96

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

Indice

Induzione

Teorema 97

- **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 $\begin{cases} \phi := \dfrac{1+\sqrt{5}}{2} \\ \psi := \dfrac{1-\sqrt{5}}{2} \end{cases}$

- **Th**
  - la formula chiusa della serie di Fibonacci è $F_n = \dfrac{\varphi^n - \psi^n}{\varphi - \psi} = \dfrac{\varphi^n - \psi^n}{\sqrt{5}}$

Matrici

Teorema 98

- **Hp**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
- **Th**
  - $\mathrm{Mat}_{m \times n}(\mathbb{K})$ è uno spazio vettoriale

---

Teorema fondamentale dell'algebra

- **Hp**
  - $\mathbb{K}$ campo
  - $p(x) \in \mathbb{K}[x] \mid p(x) = a_0 x^0 + \ldots + a_n x^n$
- **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 99

- **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 100

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

Teorema 101

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

Teorema 102

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

Teorema 103

- !!! **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 104

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

Teorema 105

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

Teorema 106

- !!! **NON HO CAPITO UN CAZZO**

Teorema di Eulero

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

Teorema 107

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

Teorema 108

- **Hp**

- G gruppo $\Big| \, |G| = 4$

- **Th**
  - $G \cong \mathbb{Z}_4$ oppure $G \cong K_4$

Relazioni

Teorema 109

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

Teorema 110

- **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 111

- **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 112

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

Teorema 113

- **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 114

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

Teorema 115

- **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 116

- **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 117

- **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 118

- **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 119

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

Teorema 120

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

Morfismi

Teorema 121

- **Hp**
  - $(G, \cdot), (H, \cdot)$ gruppi
  - 1_G neutro per G
  - 1_H neutro per H
  - $f : G \to H$ morfismo
- **Th**
  - $f(1_G) = 1_H$

Teorema 122

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

Teorema 123

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

Teorema 124

- **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 125

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

Teorema 126

- **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 $(G, \cdot)$

Teorema 127

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

Teorema 128

- **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 $(\mathbb{Z}_n, +, \cdot)$

Teorema 129

- **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 $(G, \cdot)$

Teorema 130

- **Hp**

- G, H gruppi
- $f : G \to H$ morfismo

- **Th**
  - $\ker(f) \subset G$ è sottogruppo

Teorema 131

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

Teorema 132

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

Teorema 133

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

Teorema 134

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

Teorema 135

- **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**
  - $\ker(f) = I(n)$

Teorema 136

- **Hp**
  - G, H gruppi

  - $f : G \to H$ morfismo
- **Th**
  - $\ker(f)$ è sottogruppo normale

Gruppi diedrali

Teorema 137

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

Teorema 138

- **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 139

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

Teorema 140

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

Teorema 141

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