DISCLAIMER

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

Coefficienti binomiali

Definizione 1

- **Coefficiente binomiale**
  - $0! := 1$
  - $n, k \in \mathbb{N}$
  - $\displaystyle \binom{n}{k} := \begin{cases} \frac{n!}{n!(n-k)!} & k \leqslant n \\ 0 & k > n \end{cases}$

Teorema 1

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

Teorema 2

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

Teorema 3

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

Teorema 4

- **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 5

- **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 6

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

Teorema 7

- **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 $\mathbb{Z}_p$

Determinante

Definizione 2

- **Applicazione multilineare**
  - $\mathbb{K}$ campo
  - $k \in \mathbb{N}$
  - $V_1, \dots, V_k, W$ spazi vettoriali
  - $f : V_1 \times \dots \times V_k \to W : (v_1, \dots, v_k) \to w$
  - f **multilineare** $\iff \forall i \in [1, k],\ \forall v_1 \in V_1, \dots, v_i', v_i'' \in V_i, \dots, v_k \in V_k,\ \forall \lambda, \mu \in \mathbb{K} \quad f(v_1, \dots, \lambda v_i' + \mu v_i'', \dots, v_k) = \lambda f(v_1, \dots, v_i', \dots, v_k) + \mu f(v_1, \dots, v_i'', \dots, v_k)$
- **Determinante**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $\det : \mathrm{Mat}_{n \times n}(\mathbb{K}) \to \mathbb{K}$

- 1. $\forall A \in \text{Mat}_{n\times n}(\mathbb{K})$ det multilineare su $A_1, \dots A_n$ e $A^1, \dots, A^n$
- 2. $\forall A \in \text{Mat}_{n\times n}(\mathbb{K})$ $A_1, \dots A_n$ e $A^1, \dots, A^n$ basi di $\mathbb{K}^n \iff \det(A) \neq 0$
- 3. $\det(I_n) = 1$
- 4. per $\mathbb{K} \mid 1 \neq -1$ scambiando due righe o due colonne $\det(A)$ cambia segno
- det è il **determinante** $\iff$ det verifica 1, 2 e 3, oppure 1, 3 e 4
  - poiché è possibile dimostrare che la funzione che verifica tali condizioni esiste ed è unica, allora il det è totalmente determinato da tali caratteristiche

Teorema 8

- **Hp**
  - $\mathbb{K}$ campo $\mid 1 \neq -1$
  - $n \in \mathbb{N} - \{0\}$
  - $f : \text{Mat}_{n\times n}(\mathbb{K}) \to \mathbb{K}$
  4. **!!! SCRIVI**
- **Th**
  - **!!! DETERMINANTE ALTERNANTE**

Definizione 3

- **Matrice singolare**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{n\times n}(\mathbb{K})$
  - A è detta **singolare** $\iff \det(A) = 0$

Teorema 9

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{n\times n}(\mathbb{K})$
  1. A invertibile
  2. $\text{rk}(A) = n$
  3. $A_1, \dots, A_n$ base di $\mathbb{K}^n$
  4. $A^1, \dots, A^n$ base di $\mathbb{K}^n$
  5. $\det(A) \neq 0$
  6. $A \equiv I_n$ tramite la relazione di equivalenza delle operazioni sulle righe
  7. $A \equiv I_n$ tramite la relazione di equivalenza delle operazioni sulle colonne
- **Th**
  - le proposizioni sono equivalenti

Teorema 10

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$

- $A \in \text{Mat}_{n\times n}(\mathbb{K}) \mid \exists i \in [1,n] : A_i = 0_{\mathbb{K}^n} \vee \exists j \in [1,n] : A^j = 0_{\mathbb{K}^n}$, ovvero in A è presente o una riga, o una colonna nulla
- **Th**
  - $\det(A) = 0$

Teorema 11

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{n\times n}(\mathbb{K})$
- **Th**
  - $\det(A) = \det(A^T)$

Teorema 12

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A, B \in \text{Mat}_{n\times n}(\mathbb{K}) \mid A$ simile a B
- **Th**
  - $\det(A) = \det(B)$

Teorema 13

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{n\times n}(\mathbb{K})$
- **Th**
  - $\det(A) = \displaystyle\sum_{\sigma \in S_n} \text{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma_i}$

Teorema 14

- **Hp**
  - $\mathbb{K}$ campo
  - $A \in \text{Mat}_{2\times 2}(\mathbb{K})$
  - $A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$
- **Th**
  - $\det(A) = a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$

Teorema 15

- **Hp**
  - $\mathbb{K}$ campo
  - $A \in \text{Mat}_{3\times 3}(\mathbb{K})$

- $A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$

- **Th**
  - $\det(A) = a_{1,1}a_{2,2}a_{3,3}+a_{1,3}a_{2,1}a_{3,2}+a_{1,2}a_{2,3}a_{3,1}-a_{1,3}a_{2,2}a_{3,1}-a_{1,1}a_{2,3}a_{3,2}-a_{1,2}a_{2,1}a_{3,3}$

Teorema 16

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K}) \mid A$ triangolare
- **Th**
  - $\det(A) = a_{1,1} \cdot \ldots \cdot a_{n,n}$

Teorema 17

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $\lambda \in \mathbb{K}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
  - $A' = \begin{pmatrix} A_1 \\ \vdots \\ \lambda A_i \\ \vdots \\ A_n \end{pmatrix}$
- **Th**
  - $\det(A') = \lambda \cdot \det(A)$

Teorema 18

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
- **Th**
  - $\forall 1 \leq i,j \leq n \quad \det(A) = \sum_{k=1}^{n} (-1)^{i+k} \cdot a_{i,k} \cdot \det(A_i^k) = \sum_{h=1}^{n} (-1)^{h+j} \cdot a_{h,j} \cdot \det(A_h^j)$

Definizione 4

- **Aggiunta di una matrice**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
  - A^* è detta **aggiunta di** $A \iff \forall i,j \in [1,n] \quad a^*_{i,j} = (-1)^{i+j} \cdot \det(A_i^j)$

Teorema 19

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K}) \mid \det(A) \neq 0$
- **Th**
  - $A^{-1} = \dfrac{(A^*)^T}{\det(A)}$

Teorema 20

- **Hp**
  - $\mathbb{K}$ campo
  - $A \in \mathrm{Mat}_{2\times 2}(\mathbb{K}) \mid \det(A) \neq 0$
  - $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$
- **Th**
  - $A^{-1} = \dfrac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Polinomio caratteristico

Definizione 5

- $\mathbb{K}$ campo
- $n \in \mathbb{N} - \{0\}$
- $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
- $p_A(x) := \det(x \cdot I_n - A)$ è detto **polinomio caratteristico di** A

Teorema 21

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
- **Th**
  - $p_A(x) = x^n - \mathrm{tr}(A) \cdot x^{n-1} + \ldots + (-1)^n \cdot \det(A)$

Teorema 22

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A, B \in \mathrm{Mat}_{n\times n}(\mathbb{K}) \mid A$ simile a B
- **Th**
  - $p_A(x) = p_B(x)$

Definizione 6

- **Autovalore**
    - $\mathbb{K}$ campo
    - $n \in \mathbb{N} - \{0\}$
    - $A \in \text{Mat}_{n \times n}(\mathbb{K})$
    - $\lambda \in \mathbb{K} \mid p_A(\lambda) = 0$ è detto **autovalore di** A
- **Spettro**
    - $\mathbb{K}$ campo
    - $n \in \mathbb{N} - \{0\}$
    - $A \in \text{Mat}_{n \times n}(\mathbb{K})$
    - $\text{sp}(A) := \{\lambda \in \mathbb{K} \mid p_A(\lambda) = 0\}$ è detto **spettro di** A

Teorema 23

- **Hp**
    - $\mathbb{K}$ campo
    - $n \in \mathbb{N} - \{0\}$
    - $A, B \in \text{Mat}_{n \times n}(\mathbb{K}) \mid A$ simile a B
- **Th**
    - $\text{sp}(A) = \text{sp}(B)$

Teorema 24

- **Hp**
    - $\mathbb{K}$ campo
    - $n \in \mathbb{N} - \{0\}$
    - $A \in \text{Mat}_{n \times n}(\mathbb{K})$
    - $\lambda \in \mathbb{K}$
- **Th**
    - λ autovalore $\iff \exists v \in \mathbb{K}^n - \{0\} \mid A \cdot v = \lambda \cdot v$

Definizione 7

- **Autovettore relativo ad un autovalore**
    - $\mathbb{K}$ campo
    - $n \in \mathbb{N} - \{0\}$
    - $A \in \text{Mat}_{n \times n}(\mathbb{K})$
    - $\lambda \in \text{sp}(A)$
    - $v \in \mathbb{K}^n - \{0\}$ è detto **autovettore di** A **relativo a** $\lambda \iff (A - \lambda \cdot I_n) \cdot v = 0$

Teorema 25

- **Hp**
    - $\mathbb{K}$ campo
    - $n \in \mathbb{N} - \{0\}$
    - $A \in \text{Mat}_{n \times n}(\mathbb{K})$
    - $\lambda_1, \ldots, \lambda_k \in \text{sp}(A)$

- $v_1, \dots, v_k$ autovettori di A relativi rispettivamente a $\lambda_1, \dots, \lambda_k$
- **Th**
  - $v_1, \dots, v_k$ linearmente indipendenti

Definizione 8

- **Autospazio relativo ad un autovalore**

  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n \times n}(\mathbb{K})$
  - $\lambda \in \mathrm{sp}(A)$
  - $\mathrm{E}_\lambda(A) := \{v \in \mathbb{K}^n \mid (A - \lambda \cdot I_n) \cdot v = 0\}$ è detto **autospazio di A relativo a λ**
    - in particolare $0_{\mathbb{K}^n} \in \mathrm{E}_\lambda(A)$

Teorema 26

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n \times n}(\mathbb{K})$
  - $\lambda \in \mathrm{sp}(A)$
- **Th**
  - $\mathrm{E}_\lambda(A) \subset \mathbb{K}$ sottospazio vettoriale

Definizione 9

- **Molteplicità algebrica di un autovalore**

  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n \times n}(\mathbb{K})$
  - $\lambda \in \mathrm{sp}(A)$
  - $\mu(\lambda) := \max(\{\varepsilon \in \mathbb{N} : (x - \lambda)^\varepsilon \mid p_A(x)\})$ è detta **molteplicità algebrica di λ**

Teorema 27

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A, B \in \mathrm{Mat}_{n \times n}(\mathbb{K}) \mid A$ simile a B
  - $\lambda \in \mathrm{sp}(A) = \mathrm{sp}(B)$
- **Th**
  - $\mu_A(\lambda) = \mu_B(\lambda)$

Definizione 10

- **Molteplicità geometrica di un autovalore**

  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$

- $A \in \text{Mat}_{n \times n}(\mathbb{K})$
- $\lambda \in \text{sp}(A)$
- $\nu(\lambda) := \dim(\text{E}_\lambda(A))$ è detta **molteplicità geometrica di λ**

Teorema 28

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A, B \in \text{Mat}_{n \times n}(\mathbb{K}) \mid A$ simile a B
  - $\lambda \in \text{sp}(A) = \text{sp}(B)$
- **Th**
  - $\nu_A(\lambda) = \nu_B(\lambda)$

Teorema 29

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{n \times n}(\mathbb{K})$
  - $\lambda \in \text{sp}(A)$
- **Th**
  - $\nu(\lambda) = n - \text{rk}(A - \lambda \cdot I_n)$

Teorema 30

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{n \times n}(\mathbb{K})$
  - $\lambda \in \text{sp}(A)$
- **Th**
  - $\nu(\lambda) \leq \mu(\lambda)$

Teorema 31

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{n \times n}(\mathbb{K})$
  1. A triangolarizzabile
  2. $\displaystyle\sum_{\lambda \in \text{sp}(A)} \mu(\lambda) = n$
  3. $p_A(x) = \displaystyle\prod_{\lambda \in \text{sp}(A)} (x - \lambda)^{\mu(\lambda)}$, ovvero $p_A(x)$ è completamente fattorizzabile
- **Th**
  - le proposizioni sono equivalenti

Teorema 32

- **Hp**
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$
- **Th**
  - A è triangolarizzabile

Teorema 33

- **Hp**
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$
- **Th**
  - A triangolarizzabile $\iff \exists \lambda \in \mathrm{sp}(A) \mid \lambda \in \mathbb{R}$

Teorema 34

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
  1. A diagonalizzabile
  2. $\displaystyle\sum_{\lambda \in \mathrm{sp}(A)} \nu(\lambda) = n$
  3. $\exists B^1, \dots, B^n$ autovettori di $A \mid B^1, \dots, B^n$ base di $\mathbb{K}^n$
- **Th**
  - le proposizioni sono equivalenti

Teorema 35

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
  - $B^1, \dots, B^n$ autovettori di $A \mid B = (B^1, \dots, B^n) \in \mathrm{GL}(n, \mathbb{K}) \land B^1, \dots, B^n$ base di $\mathbb{K}^n$
- **Th**
  - A diagonalizzabile

Gruppi diedrali

Definizione 11

- **Gruppo diedrale**
  - $n \in \mathbb{N}_{\geq 2}$
  - D_n è l'**insieme delle simmetrie dell'n-gono regolare**
    - l'insieme delle rotazioni che lasciano l'n-gono invariato, e delle riflessioni rispetto agli assi di simmetria

- $\rho :=$ rotazione di $\frac{360\text{ř}}{n}$ gradi di un n-gono regolare
- $\sigma_i :=$ riflessione rispetto all'i-esimo asse di simmetria dell'n-gono regolare

Teorema 36

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

Teorema 37

- **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 38

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

Teorema 39

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

Definizione 12

- **Gruppo di Klein**

  - $K_4 := \{1, a, b, c\}$
  - $a^2 = b^2 = c^2 = 1$
  - $ab = c = ba$
  - $ac = b = ca$
  - $cb = a = bc$

Teorema 40

- **Hp**
  - K_4 è il gruppo di Klein

- **Th**
  - $K_4 \cong D_2$

Gruppi

Definizione 13

- **Semigruppo**
  - S insieme
  - $m : S \times S \to S$
  - (S, m) **semigruppo** $\iff \forall x, y, z \in S \quad m(x, m(y, z)) = m(m(x, y), z)$
- **Monoide**
  - S insieme
  - $m : S \times S \to S$
  - (S, m) **monoide** $\iff$ (S, m) semigruppo e $\forall x \in S \quad \exists e \in S \mid m(x, e) = m(e, x) = x$
- **Gruppo**
  - S insieme
  - $m : S \times S \to S$
  - (S, m) **gruppo** $\iff$ (S, m) monoide e $\forall x \in S \quad \exists x^{-1} \in S \mid m(x, x^{-1}) = m(x^{-1}, x) = e$
- **Gruppo abeliano**
  - S insieme
  - $m : S \times S \to S$
  - (S, m) **gruppo abeliano** $\iff$ (S, m) gruppo e $\forall x, y \in S \quad m(x, y) = m(y, x)$

Teorema 41

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

Teorema 42

- **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 43

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

Teorema 44

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

Anelli

Definizione 14

- **Anello**

  - A insieme
  - $+ : A \times A \to A$
  - $* : A \times A \to A$
  - $(A, +, *)$ **anello** $\iff$ $(A, +)$ gruppo abeliano, $(A, *)$ monoide e $\forall a, b, c \in A \quad a * (b + c) = a * b + a * c$
  - $a * b = b * a \quad \forall a, b \in A \implies (A, *, +)$ è un **anello commutativo**

- **Campo**

  - $(A, +, *)$ anello
  - $(A, +, *)$ è un **campo** $\iff \forall x \in A \quad \exists x^{-1}$ rispetto a $*$

- **Semianello commutativo**

  - A insieme
  - $+ : A \times A \to A$
  - $* : A \times A \to A$
  - $(A, +, *)$ **semianello commutativo** $\iff$ $(A, +)$ monide commutativo, $(A, *)$ monoide commutativo e $\forall a, b, c \in A \quad a * (b + c) = a * b + a * c$

- **Sottoanello**

  - $(A, +, \cdot)$ anello
  - $(B, +, \cdot) \subset (A, +, \cdot)$ **sottoanello** $\iff$ $(B, +) \subset (A, +)$ sottogruppo e $B \cdot B \subset B$

Definizione 15

- **Invertibili**

  - $(A, +, \cdot)$ anello commutativo

- $a \in A$ **invertibile** $\iff \exists a^{-1} \in A \mid a \cdot a^{-1} = e$, dove e è l'elemento neutro dell'anello rispetto a $\cdot$
- $A^* := \{a \in A \mid a \text{ invertibile}\}$ è l'**insieme degli invertibili di** A

Teorema 45

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

Teorema 46

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

Definizione 16

- **Divisori dello** 0
  - $(A, +, \cdot)$ anello commutativo
  - $a \in A$ **divisore dello** $0 \iff \exists b \in A - \{0\} \mid a \cdot b = 0$
- **Dominio di integrità**
  - $(A, +, \cdot)$ anello commutativo
  - A **dominio di integrità** $\iff \nexists x \neq 0 : x \mid 0$
  - alternativamente, A è dominio di integrità $\iff$ in A vale la legge di annullamento del prodotto

Teorema 47

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

Teorema 48

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

Definizione 17

- **Elementi irriducibili**
  - A anello commutativo
  - $a \in A - \{0\} \mid a \in A^*$

- a **irriducibile** $\iff \exists b, c \in A \mid a = bc \implies b \in A^* \vee c \in A^*$

- **Elementi primi**

  - A anello commutativo
  - $a \in A - \{0\} \mid a \in A^*$
  - a **primo** $\iff \exists b, c \in A : a \mid bc \implies a \mid b \vee a \mid c$

Teorema 49

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

Sottogruppi

Definizione 18

- **Sottogruppo**

  - $(G, *)$ gruppo
  - $(H, *) \subset (G, *)$ **sottogruppo** $\iff \exists e \in H \mid e$ è l'elemento neutro, $H * H \subset H$ e $\exists x^{-1} \in H \quad \forall x \in H$

Definizione 19

- **Sottogruppo normale**

  - $(G, *)$ gruppo
  - $(H, *) \subset (G, *)$ sottogruppo
  - $x \in G$
  - $xH := \{xh \mid h \in H\}$
  - $Hx := \{hx \mid h \in H\}$
  - H **sottogruppo normale** $\iff \forall x \in G \quad xH = Hx$

Teorema 50

- **Hp**
  - G gruppo
  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 proposizioni sono equivalenti

Ordine

Definizione 20

- **Ordine di un elemento in un gruppo**
  - G gruppo
  - $g \in G$
  - $H(g) := \{g^n \mid n \in \mathbb{Z}\}$ è detto **sottogruppo ciclico**
    - prende il nome di *sottogruppo ciclico* poiché, a seconda del gruppo, le potenze di g possono essere infinite o finite, ma quest'ultimo caso si verifica esclusivamente quando le potenze ciclano su loro stesse
  - $o(g) := |H(g)|$ è detto **ordine di** $g \in G$
    - tale valore può dunque essere infinito o finito, e in quest'ultimo caso l'ordine costituisce il valore più piccolo, non nullo, per cui $g^{o(g)} = e$, poiché per valori maggiori le potenze ricicleranno infinitamente

Teorema 51

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

Teorema 52

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

Teorema 53

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

Teorema 54

- **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 55

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

Teorema 56

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

Teorema 57

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

Teorema 58

- **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 59

- **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**
  - $o(gh) = o(hg) = m$

Ideali

Definizione 21

- **Ideali**
  - $(A, +, \cdot)$ anello
  - $I \subset A$ **ideale** $\iff (I, +) \subset (A, +)$ è un sottogruppo e $A \cdot I \subset I$ e $I \cdot A \subset I$

Teorema 60

- **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 61

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

Teorema 62

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

Teorema 63

- **Hp**
  - $(A, +, \cdot)$ anello
  - $a_1, \ldots, a_n \in \mathbb{Z}$
  - $I(a_1, \ldots, a_n) := \{a_1b_1 + \ldots + a_nb_n \mid b_1, \ldots, b_n \in A\}$
- **Th**
  - $I(a_1, \ldots, a_n)$ è un ideale, e prende il nome di *ideale di A generato dagli* $a_1, \ldots, a_n \in A$

Definizione 22

- **Congruenza modulo di un ideale**
  - $(A, +, \cdot)$ anello
  - $I \subset A$ ideale
  - per definizione, I ideale $\implies (I, +) \subset (A, +)$ sottogruppo, dunque ha senso definire A/I, e infatti I induce una relazione di equivalenza su A detta **congruenza modulo** I, dove $\forall a, b \in A \quad a \equiv b \pmod{I} \iff b - a \in I$

- $b - a \in I \iff (-a) + b \in I$, di conseguenza questa congruenza coincide con la classe laterale sinistra di $(A, +)$

Teorema 64

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

Teorema 65

- **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 66

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

Definizione 23

- **Massimo Comun Divisore**
  - $a_1, \ldots, a_n \in \mathbb{Z}$
  - $\exists! d \in \mathbb{N} \mid I(a_1, \ldots, a_n) = I(d)$, ed è detto **massimo comun divisore degli** $a_1, \ldots, a_n$
    - per dimostrazione precedente $I(a_1, \ldots, a_n)$ è un ideale, e per dimostrazione precedente ogni ideale in $\mathbb{Z}$ è principale, dunque per un certo d coincide con $I(d)$, e in particolare d è proprio il massimo comun divisore degli $a_1, \ldots, a_n$ per dimostrazione precedente

Teorema 67

- **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 68

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

Operazioni sugli ideali

Definizione 24

- **+ tra ideali**

  - $(A, +, \cdot)$ anello commutativo
  - $I, J \subset A$ ideali
  - $I + J = \{i + j \mid \forall i \in I, j \in J\}$

Teorema 69

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

Definizione 25

- **$\cap$ tra ideali**

  - $(A, +, \cdot)$ anello commutativo
  - $I, J \subset A$ ideali
  - $I \cap J = \{x \in I \wedge x \in J\}$

Teorema 70

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

Definizione 26

- **Minimo Comune Multiplo**

  - $a_1, \ldots, a_n \in \mathbb{Z}$
  - $\exists! m \in \mathbb{N} \mid I(m) = I(a_1) \cap \ldots \cap I(a_n) = \bigcap_{i=1}^{n} I(a_i)$, ed è detto **minimo comune multiplo degli** $a_1, \ldots, a_n$

Definizione 27

- **$\cdot$ tra ideali**

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

- $I \cdot J = \{i_1 j_1 + \ldots + i_k j_k \mid k \geq 1, \forall i_1, \ldots, i_k \in I, j_1, \ldots, j_k \in J\}$

Teorema 71

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

Teorema 72

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

Teorema 73

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

Induzione

Definizione 28

- **Induzione**
  - successione di proposizioni infinita $P_1, P_2, P_3, \ldots$
  - $\begin{cases} P_1 \text{ vera} \\ P_1, P_2, P_3, \ldots, P_n \implies P_{n+1} \quad \forall n \geq 1 \end{cases}$
  - allora P_n vera $\forall n$

Teorema 74

- **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**
  - $\forall n \in \mathbb{N} \quad F_n = \dfrac{\varphi^n - \psi^n}{\varphi - \psi} = \dfrac{\varphi^n - \psi^n}{\sqrt{5}}$

Insieme quoziente

Definizione 29

- **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 $\sim$

Definizione 30

- **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 $\mathbb{Z}_n := \{[0], [1], \ldots, [n-1]\}$, che coincide con $\mathbb{Z}/\equiv$

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**
  - $p \mid a \lor p \mid b$

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

Funzione totiente di Eulero

Definizione 31

- **Funzione totiente di Eulero**

  - $n \in \mathbb{N}$
  - $\varphi(n) := |\mathbb{Z}_n^*|$

Teorema 81

- **Hp**
  - $n, m \in \mathbb{N} \mid \text{MCD}(a, n) = 1$
- **Th**
  - $[a] \in \mathbb{Z}_{mn}^* \iff [a] \in \mathbb{Z}_m^* \land [a] \in \mathbb{Z}_n^*$

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

Matrici

Definizione 32

- **Matrici**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $\mathrm{Mat}_{m \times n}(\mathbb{K})$ è l'**insieme delle matrici aventi m righe e n colonne a coefficienti in $\mathbb{K}$**
- **Vettori riga e vettori colonna**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $\forall A \in \mathrm{Mat}_{1 \times n}(\mathbb{K}) \quad A = (x_1, \ldots, x_n)$ è detto **vettore riga**
  - $\forall A \in \mathrm{Mat}_{m \times 1}(\mathbb{K}) \quad A = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$ è detto **vettore colonna**
  - $\forall A \in \mathrm{Mat}_{m \times n}(\mathbb{K}) \quad \exists A^1, \ldots, A^n \in \mathbb{K}^m$ vettori colonna e $A_1, \ldots, A_m \in \mathbb{K}^n$ vettori riga $\mid A = \left(A^1, \ldots, A^n\right) = \begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix}$

Definizione 33

- **Somma tra matrici**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $\forall i \in [1, m], j \in [1, n] \quad a_{i,j}, b_{i,j} \in \mathbb{K}$
  - $A, B \in \mathrm{Mat}_{m \times n}(\mathbb{K}) \mid A = \begin{pmatrix} \ddots & & \\ & a_{i,j} & \\ & & \ddots \end{pmatrix} \wedge B = \begin{pmatrix} \ddots & & \\ & b_{i,j} & \\ & & \ddots \end{pmatrix}$

- $A + B = \begin{pmatrix} \ddots & & \\ & a_{i,j} + b_{i,j} & \\ & & \ddots \end{pmatrix}$ è la **somma tra** A **e** B

Teorema 85

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

Definizione 34

- **Prodotto tra matrici**
  - $\mathbb{K}$ campo
  - $l, m, n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{l\times m}(\mathbb{K}) \mid A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{l,1} & \cdots & a_{l,m} \end{pmatrix}$
  - $B \in \text{Mat}_{m\times n}(\mathbb{K}) \mid B = \begin{pmatrix} b_{1,1} & \cdots & b_{1,n} \\ \vdots & \ddots & \vdots \\ b_{m,1} & \cdots & b_{m,n} \end{pmatrix}$
  - $C \in \text{Mat}_{l\times n}(\mathbb{K}) \mid C = AB$ è il **prodotto tra** A **e** B, ed è definito come $\begin{pmatrix} a_{1,1}b_{1,1} + \ldots + a_{1,m}b_{m,1} & \cdots & a_{1,1}b_{1,n} + \ldots + a_{1,m}b_{m,n} \\ \vdots & \ddots & \vdots \\ a_{l,1}b_{1,1} + \ldots + a_{l,m}b_{m,1} & \cdots & a_{l,1}b_{1,n} + \ldots + a_{l,m}b_{m,n} \end{pmatrix}$

Teorema 86

- **Hp**
  - $\mathbb{K}$ campo
  - $\lambda \in \mathbb{K}$
  - $l, m, n, k \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{l\times m}(\mathbb{K})$
  - $B \in \text{Mat}_{m\times n}(\mathbb{K})$
- **Th**
  - **!!! TODO**
  - $\forall C \in \text{Mat}_{n\times k}(\mathbb{K}) \quad (AB)C = A(BC)$
  - $\forall C \in \text{Mat}_{m\times n}(\mathbb{K}) \quad A(B + C) = AB + AC$
  - $\forall C \in \text{Mat}_{n\times k}(\mathbb{K}) \quad (A + B)C = AC + BC$
  - $\lambda(AB) = (\lambda A)B = A(\lambda B)$

Teorema 87

- **Hp**
  - $\mathbb{K}$ campo

- $\lambda \in \mathbb{K}$
- $n \in \mathbb{N} - \{0\}$

- **Th**
  - $(\mathrm{Mat}_{n\times n}(\mathbb{K}), +, \cdot)$ è un anello

---

Interpretazione geometrica dei vettori

Definizione 35

- **Prodotto scalare**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $u, v \in \mathbb{K}^n \mid u = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, v = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$
  - $u \cdot v := \sum\limits_{i=1}^{n} x_i \cdot y_i$ è il **prodotto scalare tra** u **e** v

Teorema 88

- **Hp**
  - $n \in \mathbb{N} - \{0\}$
  - $u, v \in \mathbb{K}^n$
- **Th**
  - $u \cdot v = v \cdot u$
  - $\forall w \in \mathbb{K}^n \quad u \cdot (v + w) = u \cdot v + u \cdot w$
  - $u \cdot (\lambda v) = \lambda(u \cdot v)$

Definizione 36

- **Norma di un vettore**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $u \in \mathbb{K}^n \mid u = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$
  - $||u|| := \sqrt{x_1^2 + \ldots + x_n^2}$ è detta **norma di** u
    - graficamente, corrisponde alla lunghezza del vettore u nel piano cartesiano

Teorema 89

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$

- $u \in \mathbb{K}^n \mid u = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

- **Th**
  - $||u|| = \sqrt{u \cdot u}$

Matrici particolari

Definizione 37

- **Vettore trasposto**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N}$
  - $v \in \mathrm{Mat}_{n\times 1}(\mathbb{K}) \mid \exists x_1, \ldots, x_n \in \mathbb{K} : v = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$
  - $v^T = (x_1, \ldots, x_n)$ è il **vettore trasposto di** v
    - vicendevolmente, se v è un vettore riga, il suo trasposto sarà il corrispondente vettore colonna
- **Matrice trasposta**
  - $m, n \in \mathbb{N} - \{0\}$
  - $\mathbb{K}$ campo
  - $A \in \mathrm{Mat}_{m\times n}(\mathbb{K}) \mid A = \left(A^1, \ldots, A^n\right)$
  - $A^T = \begin{pmatrix} {A^1}^T \\ \vdots \\ {A^n}^T \end{pmatrix}$ è la **matrice trasposta di** A
    - vale il ragionamento analogo considerando le righe di A al posto delle colonne
- **Matrice simmetrica**
  - $n \in \mathbb{N} - \{0\}$
  - $\mathbb{K}$ campo
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
  - A è detta **simmetrica** $\iff A^T = A$

Teorema 90

- **Hp**
  - $m, n \in \mathbb{N} - \{0\}$
  - $\mathbb{K}$ campo
  - $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$
  - $B \in \mathrm{Mat}_{m\times n}(\mathbb{K})$
- **Th**
  - $(A \cdot B)^T = B^T \cdot A^T$

Definizione 38

- **Matrice identità**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $I_n = \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \left(e_1^T, \ldots, e_n^T\right) = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ \vdots & \ddots & & & \vdots \\ 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$ è detta **matrice identità**
- **Matrice invertibile**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
  - A **invertibile** $\iff \exists A^{-1} \in \mathrm{Mat}_{n\times n}(\mathbb{K}) \mid A \cdot A^{-1} = A^{-1} \cdot A = I_n$
- **Gruppo Generale Lineare**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $\mathrm{GL}(n, \mathbb{K}) := \{A \in \mathrm{Mat}_{n\times n}(\mathbb{K}) \mid A \text{ invertibile}\}$ è detto **gruppo generale lineare invertibile**

Teorema 91

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
- **Th**
  - $(\mathrm{GL}(n, \mathbb{K}), \cdot)$ è un gruppo

Teorema 92

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $f : \mathrm{GL}(n, \mathbb{K}) \to \mathbb{K}^*$
- **Th**
  - f morfismo di gruppi

Definizione 39

- **Matrice ortogonale**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{GL}(n, \mathbb{K})$
  - A è detta **ortogonale** $\iff A \cdot A^T = A^T \cdot A = I_n$

    - in particolare $A^{-1} = A^T$

- **Gruppo ortogonale**
    - $\mathbb{K}$ campo
    - $n \in \mathbb{N} - \{0\}$
    - $A \in \mathrm{GL}(n, \mathbb{K})$
    - $O(n) := \{A \in \mathrm{GL}(n, \mathbb{K}) \mid A \text{ ortogonale}\}$ è detto **gruppo ortogonale**

Definizione 40

- **Gruppo Speciale Lineare**
    - $\mathbb{K}$ campo
    - $n \in \mathbb{N} - \{0\}$
    - $\mathrm{SL}(n, \mathbb{K}) := \{A \in \mathrm{Mat}_{n\times n}(\mathbb{K}) \mid \det(A) = 1\}$ è detto **gruppo generale lineare invertibile**

Definizione 41

- **Matrici simili**
    - $\mathbb{K}$ campo
    - $n \in \mathbb{N} - \{0\}$
    - $A, B \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
    - A **simile a** $B \iff \exists C \in \mathrm{GL}(n, \mathbb{K}) \mid A = C^{-1}BC$

Definizione 42

- **Traccia**
    - $\mathbb{K}$ campo
    - $n \in \mathbb{N} - \{0\}$
    - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
    - $\mathrm{tr}(A) := a_{1,1} + \ldots + a_{n,n}$ è detta **traccia di** A

Teorema 93

- **Hp**
    - $\mathbb{K}$ campo
    - $n \in \mathbb{N} - \{0\}$
    - $A, B \in \mathrm{Mat}_{n\times n}(\mathbb{K}) \mid A$ simile a B
- **Th**
    - $\mathrm{tr}(A) = \mathrm{tr}(B)$

Definizione 43

- **Matrice triangolare superiore**
    - $\mathbb{K}$ campo
    - $n \in \mathbb{N} - \{0\}$
    - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
    - A è detta **triangolare superiore** $\iff \forall i, j \in [1, n], i > j \quad a_{i,j} = 0$

- **Matrice triangolare inferiore**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
  - A è detta **triangolare superiore** $\iff \forall i, j \in [1, n], i < j \quad a_{i,j} = 0$
- **Matrice triangolare**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
  - A è detta **triangolare** $\iff$ A triangolare superiore o triangolare inferiore
- **Matrice triangolarizzabile**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
  - A è detta **triangolarizzabile** $\iff \exists B \in \mathrm{Mat}_{n\times n}(\mathbb{K}) \mid B$ triangolare $\wedge$ B simile ad A
- **Matrice diagonale**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
  - A è detta **diagonale** $\iff \forall i, j \in [1, n], i \neq j \quad a_{i,j} = 0$
    - in particolare, A è diagonale $\iff$ A triangolare superiore ed inferiore
- **Matrice diagonalizzabile**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
  - A è detta **diagonalizzabile** $\iff \exists B \in \mathrm{Mat}_{n\times n}(\mathbb{K}) \mid B$ diagonale $\wedge$ B simile ad A

Definizione 44

- **Sottomatrice di una matrice**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$
  - A_i^j è una **sottomatrice di** A $\iff$ A_i^j si ottiene rimuovendo A_i e A^j da A
- **Minore di una matrice**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$
  - M è un **minore di** A $\iff$ M è una sottomatrice quadrata di A
- **Orlato di un minore**

- $\mathbb{K}$ campo
- $m, n, r \in \mathbb{N} - \{0\} \mid r < m \wedge r < n$
- $A \in \text{Mat}_{m \times n}(\mathbb{K})$
- $M \in \text{Mat}_{r \times r}(\mathbb{K})$ è un minore di A
- $M' \in \text{Mat}_{(r+1)\times(r+1)}(\mathbb{K})$ è un **orlato di** $M \iff M'$ è un minore di A e M si ottiene rimuovendo una riga e una colonna da M'

Teorema 94

- **Hp**
  - $\mathbb{K}$ campo
  - $m, n, r \in \mathbb{N} - \{0\} \mid r < m \wedge r < n$
  - $A \in \text{Mat}_{m \times n}(\mathbb{K})$
  - $M \in \text{Mat}_{r \times r}(\mathbb{K})$ è un minore di A
- **Th**
  - M ha $(m - r) \cdot (n - r)$ orlati in A

Definizione 45

- **Matrice completa**

  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{m \times n}(\mathbb{K})$
  - $b \in \text{Mat}_{m \times 1}(\mathbb{K})$
  - $A_b := \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m,1} & \cdots & a_{m,n} & b_m \end{pmatrix}$

Definizione 46

- **Matrice di un'applicazione lineare**

  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - V, W spazi vettoriali su $\mathbb{K}$
  - $\mathcal{B} = \{v_1, \ldots, v_n\}$ base di V
  - $\mathcal{C} = \{w_1, \ldots, w_m\}$ base di W
  - $f : V \to W$ isomorfismo
  - $\varphi_{\mathcal{B}} : \mathbb{K}^N \to V$ isomorfismo
  - $\varphi_{\mathcal{C}} : \mathbb{K}^M \to W$ isomorfismo
  - $A \in \text{Mat}_{m \times n}(\mathbb{K}) \mid f = \varphi_{\mathcal{C}} \cdot L_A \cdot \varphi_{\mathcal{B}}^{-1}$ è detta **matrice di** f
    - è possibile dimostrare che $\forall f$ applicazione lineare $\quad \exists! A \in \text{Mat}_{m \times n}(\mathbb{K})$

Rango

Definizione 47

- **Sottospazio ortogonale**

    - $\mathbb{K}$ campo
    - $n \in \mathbb{N} - \{0\}$
    - $V \subset \mathbb{K}^n$ sottospazio vettoriale
    - $V^\perp := \{w \in \mathbb{K}^n \mid \forall v \in V \quad w \cdot v = 0_{\mathbb{K}^n}\}$ è detto **sottospazio ortogonale di** $\mathbb{K}^n$
        - la definizione ha significato poiché il prodotto scalare tra due vettori è nullo esattamente quando i due vettori sono perpendicolari tra loro, per osservazione precedente

Teorema 95

- **Hp**
    - $\mathbb{K}$ campo
    - $n \in \mathbb{N} - \{0\}$
    - $V \subset \mathbb{K}^n$ sottospazio vettoriale
- **Th**
    - $V^\perp$ è sottospazio vettoriale di $\mathbb{K}^n$

Teorema 96

- **Hp**
    - $\mathbb{K}$ campo
    - $n \in \mathbb{N} - \{0\}$
    - $V \subset \mathbb{K}^n$ sottospazio vettoriale
- **Th**
    - $\dim(V^\perp) = \dim(\mathbb{K}^n) - \dim(V)$

Definizione 48

- **Moltiplicazione sinistra**

    - $\mathbb{K}$ campo
    - $m, n \in \mathbb{N} - \{0\}$
    - $A \in \mathrm{Mat}_{m \times n}(\mathbb{K})$
    - $L_A : \mathbb{K}^n \to \mathbb{K}^m : x \to A \cdot x$ è detta **moltiplicazione sinistra di** A

Teorema 97

- **Hp**
    - $\mathbb{K}$ campo
    - $m, n \in \mathbb{N} - \{0\}$
    - $A \in \mathrm{Mat}_{m \times n}(\mathbb{K})$
- **Th**
    - L_A è una trasformazione lineare

Teorema 98

- **Hp**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{m \times n}(\mathbb{K})$
- **Th**
  - $\ker(L_A) = \text{span}(A_1, \ldots, A_m)^\perp$
  - $\text{im}(L_A) = \text{span}(A^1, \ldots, A^n)$

Definizione 49

- **Rango di una matrice**

  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{m \times n}(\mathbb{K})$
  - $\text{rk}(A) := \text{rk}(L_A)$ è il **rango di** A

Teorema 99

- **Hp**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{m \times n}(\mathbb{K})$
- **Th**
  - $\text{rk}(A) = \dim(\text{span}(A^1, \ldots, A^n)) = \dim(\text{span}(A_1, \ldots, A_n))$

Operazioni su righe e colonne

Definizione 50

- **Scambio di righe di una matrice**

  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{m \times n}(\mathbb{K})$
  - $\forall A_1, \ldots, A_m$ righe di A, scambiare A_i e A_j lascia invariato $\ker(L_A)$

- **Moltiplicazione di una riga per una costante**

  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{m \times n}(\mathbb{K})$
  - $\lambda \in \mathbb{K}^*$
  - $\forall A_1, \ldots, A_m$ righe di A, moltiplicare A_i per λ lascia invariato $\ker(L_A)$

- **Somma di una riga con un multiplo di un'altra**

  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$

- $A \in \text{Mat}_{m\times n}(\mathbb{K})$
- $\lambda \in \mathbb{K}^*$
- $\forall A_1, \dots, A_m$ righe di A, sommare ad A_i un certo $\lambda \cdot A_j$ lascia invariato $\ker(L_A)$

- **Scambio di colonne di una matrice**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{m\times n}(\mathbb{K})$
  - $\forall A^1, \dots, A^m$ colonne di A, scambiare A^i e A^j lascia invariato $\text{im}(L_A)$
- **Moltiplicazione di una colonna per una costante**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{m\times n}(\mathbb{K})$
  - $\lambda \in \mathbb{K}^*$
  - $\forall A^1, \dots, A^m$ colonne di A, moltiplicare A^i per λ lascia invariato $\text{im}(L_A)$
- **Somma di una colonna con un multiplo di un'altra**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \text{Mat}_{m\times n}(\mathbb{K})$
  - $\lambda \in \mathbb{K}^*$
  - $\forall A^1, \dots, A^m$ righe di A, sommare ad A^i un certo $\lambda \cdot A^j$ lascia invariato $\text{im}(L_A)$

Teorema 100

- **Hp**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A, B \in \text{Mat}_{m\times n}(\mathbb{K})$
  - $A \equiv B \iff$ è possibile ricavare B da A eseguendo operazioni *tra righe* definite precedentemente
- **Th**
  - $\equiv$ una relazione di equivalenza

Teorema 101

- **Hp**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A, B \in \text{Mat}_{m\times n}(\mathbb{K})$
  - $A \equiv B \iff$ è possibile ricavare B da A eseguendo operazioni *tra righe* definite precedentemente
- **Th**
  - $A \equiv B \implies \ker(L_A) = \ker(L_B) \land \text{rk}(A) = \text{rk}(B)$

Teorema 102

- **Hp**

- $\mathbb{K}$ campo
- $m, n \in \mathbb{N} - \{0\}$
- $A, B \in \mathrm{Mat}_{m \times n}(\mathbb{K})$
- $A \equiv B \iff$ è possibile ricavare B da A eseguendo operazioni *tra colonne* definite precedentemente

- **Th**
  - $\equiv$ una relazione di equivalenza

Teorema 103

- **Hp**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A, B \in \mathrm{Mat}_{m \times n}(\mathbb{K})$
  - $A \equiv B \iff$ è possibile ricavare B da A eseguendo operazioni *tra colonne* definite precedentemente
- **Th**
  - $A \equiv B \implies \mathrm{im}(L_A) = \mathrm{im}(L_B) \land \mathrm{rk}(A) = \mathrm{rk}(B)$

Morfismi

Definizione 51

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

Teorema 104

- **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 105

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

Isomorfismi

Definizione 52

- **Isomorfismo**

  - f isomorfismo $\iff$ f morfismo e f biiettiva

Teorema 106

- **Hp**
  - $(G, \cdot), (H, \cdot)$ gruppi
  - $f : G \to H$ isomorfismo
- **Th**
  - $f^{-1} : H \to G$ isomorfismo

Teorema 107

- **Hp**
  - $\cong$ è la relazione di isomorfismo
- **Th**
  - $\cong$ è una relazione di equivalenza

Teorema 108

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

Teorema 109

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

Teorema 110

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

Teorema 111

- **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 112

- **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 113

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

Kernel e immagine

Definizione 53

- **Kernel e immagine di gruppi**
  - G, H gruppi
  - $f : G \to H$ morfismo
  - $\ker(f) := \{g \in G \mid f(g) = 1_H\}$ è detto **kernel/nucleo di** f
  - $\mathrm{im}(f) := \{h \in H \mid \exists g \in G : f(g) = h\}$ è detta **immagine di** f
- **Kernel e immagine di anelli**
  - A, B gruppi
  - $f : A \to B$ morfismo
  - $\ker(f) := \{a \in A \mid f(a) = 0_B\}$ è detto **kernel/nucleo di** f
  - $\mathrm{im}(f) := \{b \in B \mid \exists a \in A : f(a) = b\}$ è detto **immagine di** f

Teorema 114

- **Hp**
  - G, H gruppi
  - $f : G \to H$ morfismo
- **Th**
  - $\ker(f) \subset G$ è sottogruppo

Teorema 115

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

Teorema 116

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

Teorema 117

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

Teorema 118

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

Teorema 119

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

Teorema 120

- **Hp**
  - G, H gruppi
  - $f : G \to H$ morfismo
- **Th**
  - $\ker(f) \subset G$ sottogruppo normale

Numeri complessi

Definizione 54

- **Insieme dei complessi**

  - $\mathbb{C} := \{a + ib \mid a, b \in \mathbb{R},\ i : i^2 = -1\}$ è l'**insieme dei complessi**
  - $\forall z \in \mathbb{C} \quad \begin{cases} a := \mathrm{Re}(z) \\ b := \mathrm{Im}(z) \end{cases}$

Teorema 121

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

Definizione 55

- **Coniugato**

  - $a, b \in \mathbb{R}$
  - $z \in \mathbb{C} \mid z = a + ib$
  - $\bar{z} := a - ib$ è il **coniugato** di z

Teorema 122

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

Teorema 123

- **Hp**

- $0 \leq \theta < 2\pi$

- **Th**
  - $e^{i\theta} = \cos\theta + i\sin\theta$

Definizione 56

- **Raggio**

  - $a, b \in \mathbb{R}$
  - $z \in \mathbb{C} \mid z = a + ib$
  - $|z| := \sqrt{a^2 + b^2}$ è il **raggio** di z
    - corrisponde alla distanza di z dall'origine nel piano di Gauss

Definizione 57

- **Forma polare**

  - $a, b \in \mathbb{C}$
  - $z \in \mathbb{C} - \{0\}$
  - $z = |z| \cdot e^{i\theta}$ è detta **forma polare di** z

Definizione 58

- **Soluzione principale**

  - $a, b \in \mathbb{R}$
  - $z \in \mathbb{C} \mid z = a + ib$
  - $\arg(z) \subset \mathbb{R}$ è l'**insieme delle soluzioni** del sistema $\begin{cases} \cos\theta = \frac{a}{|z|} \\ \sin\theta = \frac{b}{|z|} \end{cases}$
  - per definizione, $\arg(z) \implies \exists! \theta \mid 0 \leq \theta \leq 2\pi$ tale che θ sia soluzione del sistema, e questo prende il nome di $\mathrm{Arg}(z)$, detta **soluzione principale**

Teorema 124

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

Teorema 125

- **Hp**
  - $z, w \in \mathbb{C}$
- **Th**
  - $|z \cdot w| = |z| \cdot |w| \quad \arg(z \cdot w) = \arg(z) + \arg(w)$
  - $|\overline{w}| = |w| \quad \arg(\overline{w}) = -\arg(w)$
  - $|w^{-1}| = |w|^{-1} \quad \arg(w^{-1}) = -\arg(w)$
  - $\left|\frac{z}{w}\right| = \frac{|z|}{|w|} \quad \arg\left(\frac{z}{w}\right) = \arg(z) - \arg(w)$

Teorema 126

- **Hp**
  - $z \in \mathbb{C}$
- **Th**
  - $z^n = |z|^n e^{i\theta n} \quad \arg(z^n) = n\arg(z)$

Permutazioni

Definizione 59

- **Permutazioni**
  - X insieme
  - $S_X := \{f \mid f : X \to X \text{ biiettiva }\}$ è l'**insieme delle permutazioni di** X
  - $X = \{1, \ldots, n\} \implies S_n$ è detto **gruppo simmetrico di** n

Teorema 127

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

Definizione 60

- **Ciclo di una permutazione**
  - $n \in \mathbb{N}$
  - $\sigma \in S_n$
  - $\exists 1 \leq i_1, \ldots, i_d \leq n \in \mathbb{N} \mid \begin{cases} \sigma(i_1) = i_2 \\ \sigma(i_2) = i_3 \\ \vdots \\ \sigma(i_{d-1}) = i_d \\ \sigma(i_d) = i_1 \end{cases} \implies i_1, \ldots, i_n$ costituiscono un **ciclo di** σ

Teorema 128

- **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 129

- **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 130

- **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 $\gamma_j \quad \forall j \in [1, k]$
  - $m := \mathrm{mcm}(d_1, \dots, d_k)$
  - $I(\sigma) := \{n \in \mathbb{Z} \mid \sigma^n = \mathrm{id}\}$
- **Th**
  - $o(\sigma) = m$

Trasposizioni

Definizione 61

- **Trasposizione**

  - $n \in \mathbb{N}$
  - $i, j \in \mathbb{N} \mid 1 \leq i < j \leq n$
  - $k \in [1, n]$
  - $\tau_{i,j} \in S_n \mid \tau_{i,j} = \begin{cases} j & k = i \\ i & k = j \\ k & k \neq i, j \end{cases}$ è detta **trasposizione**, ovvero una permutazione che inverte esclusivamente due elementi tra loro
    - $\tau_{i,j}^2 = \mathrm{id} \iff \tau_{i,j} = \tau_{i,j}^{-1}$

- **Trasposizione adiacente**

  - $n \in \mathbb{N}$
  - $i, j \in \mathbb{N} \mid 1 \leq i < j \leq n \land j = i + 1$
  - $\tau_{i,j} = \tau_{i,i+1}$ è detta **trasposizione adiacente**, poiché inverte esclusivamente due elementi, adiacenti, tra loro

Teorema 131

- **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

Segno

Definizione 62

- **Segno di una permutazione**
  - $n \in \mathbb{N}$
  - $\sigma \in S_n$
  - $\text{Inv}(\sigma) := \{(i, j) \mid 1 \le i < j < n : \sigma(i) > \sigma(j)\}$ è l'**insieme delle inversioni di** σ
  - $\text{sgn}(\sigma) := (-1)^{|\text{Inv}(\sigma)|} = \begin{cases} +1 & |\text{Inv}(\sigma)| \equiv 0 \pmod 2 \\ -1 & |\text{Inv}(\sigma)| \equiv 1 \pmod 2 \end{cases} \implies$ σ **pari** $\iff$ $\text{sgn}(\sigma) = +1$
    - $\text{sgn}(\text{id}) = (-1)^0 = 1$, in quando la funzione identità non ha inversioni

Teorema 132

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

Teorema 133

- **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 134

- **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 135

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

Teorema 136

- **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 137

- **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 138

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

Polinomi

Definizione 63

- **Polinomi**
  - $\mathbb{K}$ campo
  - $a(x) := \sum_{k=0}^{n} a_k x^k = a_0 x^0 + \ldots + a_n x^n$ è un **polinomio**
  - $\mathbb{K}[x] := \{a_0 x^0 + \ldots + a_n x^n \mid a_0, \ldots, a_n \in \mathbb{K}\}$ è l'**insieme dei polinomi a coefficienti in $\mathbb{K}$**
  - $p(x) = a_0 x^0 + \ldots + a_n x^n \in \mathbb{K}[x]$ è detto **polinomio monico** $\iff a_n = 1$

Teorema 139

- **Hp**
  - $(\mathbb{K}, +, \cdot)$ anello
- **Th**

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

Definizione 64

- **Grado del polinomio**
  - $\mathbb{K}$ campo
  - $a(x) = a_0 x^0 + \ldots + a_n x^n \in \mathbb{K}[x]$
  - $\deg(a(x)) := \begin{cases} n & a(x) \neq 0 \\ -\infty & a(x) = 0 \end{cases}$

Teorema 140

- **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 141

- **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 142

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

Teorema 143

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

Definizione 65

- **Radici di un polinomio**
  - $\mathbb{K}$ campo
  - $p(x) \in \mathbb{K}[x]$
  - $\{c \in \mathbb{K} \ \mid p(c) = 0\}$ è l'**insieme delle radici di** $p(x)$

Teorema 144

- **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 145

- **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 146

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

Teorema 147

- **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 148

- **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 149

- **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 150

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

Teorema 151

- **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 152

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

Teorema 153

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

Teorema 154

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

Teorema 155

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

Relazioni

Definizione 66

- **Relazioni**
  - S insieme
  - ogni elemento $R \subseteq S \times S$ è una **relazione** su S
- **Relazione riflessiva**
  - S insieme
  - R relazione in $S \times S$
  - R **riflessiva** $\iff \forall x \in R \quad (x, x) \in R$
- **Relazione simmetrica**
  - S insieme
  - R relazione in $S \times S$
  - R **simmetrica** $\iff \forall x, y \in R \quad (x, y) \in R \implies (y, x) \in R$
- **Relazione transitiva**
  - S insieme
  - R relazione in $S \times S$
  - R **transitiva** $\iff \forall x, y, z \in R \quad (x, y) \in R \land (y, z) \in R \implies (x, z) \in R$
- **Relazione antisimmetrica**
  - S insieme
  - R relazione in $S \times S$
  - R **transitiva** $\iff \forall x, y \in R \quad (x, y) \in R \land (y, x) \in R \implies x = y$
- **Relazione totale**
  - S insieme
  - R relazione in $S \times S$
  - R **totale** $\iff \forall x, y \in R \quad (x, y) \in R \lor (y, x) \in R$
- **Relazione di equivalenza**
  - S insieme
  - R relazione in $S \times S$
  - R è una **relazione di equivalenza** $\iff$ R riflessiva, simmetrica e transitiva
- **Ordine parziale**
  - S insieme
  - R relazione in $S \times S$
  - R **ordine parziale** $\iff$ R riflessiva, transitiva e antisimmetrica
- **Ordine totale**
  - S insieme
  - R relazione in $S \times S$
  - R **ordine totale** $\iff$ R ordine parziale in cui vale la totalità

Teorema 156

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

Teorema 157

- **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 158

- **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 159

- **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 160

- **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

Partizioni

Definizione 67

- **Partizione**

- X insieme
- I insieme di indici
- $\forall i \in I \quad X_i \subset X$
- $X = \coprod_{i \in I} X_i$

Teorema 161

- **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 162

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

Classi laterali

Teorema 163

- **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

Definizione 68

- **Classi laterali**

  - $(G, \cdot)$ gruppo
  - $(H, \cdot) \subset (G, \cdot)$ sottogruppo
  - $\forall x, y \in G \quad x \sim_S y \iff x^{-1}y \in H$ è una relazione di equivalenza
  - $\forall x, y \in G \quad x \sim_D y \iff xy^{-1} \in H$ è una relazione di equivalenza
  - $x \in G$
  - $[x] = \{y \in G \mid y \sim_S x\}$ è detta **classe laterale sinistra**
  - $[x] = \{y \in G \mid y \sim_D x\}$ è detta **classe laterale destra**
  - $G/H := \{[x] \mid x \in G\}$ è l'**insieme delle classi laterali sinistre o destre**

Teorema 164

- **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 165

- **Hp**
  - G gruppo
  - $H \subset G$ sottogruppo
- **Th**
  - $H = [1] \in G/H$

Teorema 166

- **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 167

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

Teorema 168

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

Spazi Vettoriali

Definizione 69

- **Spazio vettoriale**

- $\mathbb{K}$ campo
- $x \in \mathbb{K}$ è detto **scalare**
- V è **spazio vettoriale su** $\mathbb{K} \iff (V, +)$ gruppo abeliano, è ben definita un'operazione di $\cdot : K \times V \to V$ che ammetta elemento neutro, inoltre $\forall s, t \in \mathbb{K}, v \in V \quad s \cdot (t \cdot v) = (s \cdot t) \cdot v, (s+t) \cdot v = s \cdot v + t \cdot v$ e infine $\forall s \in \mathbb{K}, v, w \in V \quad s \cdot (v + w) = s \cdot v + s \cdot w$
- $x \in V$ è detto **vettore**

- **Spazio di Hilbert**

  - $\mathbb{K}$ campo
  - V spazio vettoriale su $\mathbb{K}$
  - V spazio di Hilbert $\iff$ in V è ben definito il prodotto scalare

Teorema 169

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

Definizione 70

- **Sottospazio vettoriale**

  - $\mathbb{K}$ campo
  - V spazio vettoriale su $\mathbb{K}$
  - W è **sottospazio vettoriale di** $V \iff (W, +) \subset (V, +)$ sottogruppo, e $\forall w \in W, \lambda \in \mathbb{K} \quad \lambda \cdot w \in W$

Definizione 71

- **Span di vettori**

  - $n \in \mathbb{N}$
  - $\mathbb{K}$ campo
  - V spazio vettoriale su $\mathbb{K}$
  - $v_1, \ldots, v_n \in V$
  - $\text{span}(v_1, \ldots, v_n) := \{\lambda_1 v_1 + \ldots + \lambda_n v_n \mid \lambda_1, \ldots, \lambda_n \in \mathbb{K}\}$, ovvero l'insieme delle combinazioni lineari degli $v_1, \ldots, v_n$

Teorema 170

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

Definizione 72

- **Vettori generatori**
    - $n \in \mathbb{N}$
    - $\mathbb{K}$ campo
    - V spazio vettoriale su $\mathbb{K}$
    - $v_1, \ldots, v_n \in V$
    - $v_1, \ldots, v_n$ sono **generatori di** $V \iff \mathrm{span}(v_1, \ldots, v_n) = V$
        - equivalentemente, ogni altro vettore in V è una combinazione lineare degli $v_1, \ldots, v_n$
- **Indipendenza lineare**
    - $n \in \mathbb{N}$
    - $\mathbb{K}$ campo
    - V spazio vettoriale su $\mathbb{K}$
    - $v_1, \ldots, v_n \in V$
    - $v_1, \ldots, v_n$ sono **linearmente indipendenti** se e solo se $\lambda_1 v_1 + \ldots + \lambda_n v_n = 0_V \iff \lambda_1 = \ldots = \lambda_n = 0_{\mathbb{K}}$
        - equivalentemente, nessuno degli $v_1, \ldots, v_n$ è combinazione lineare degli altri
- **Base di uno spazio vettoriale**
    - $n \in \mathbb{N}$
    - $\mathbb{K}$ campo
    - V spazio vettoriale su $\mathbb{K}$
    - $v_1, \ldots, v_n \in V$
    - $v_1, \ldots, v_n$ sono una **base di** $V \iff v_1, \ldots, v_n$ sono generatori di V e linearmente indipendenti
    - n è detta **cardinalità della base di** V

Teorema 171

- **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 172

- **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 $\wedge v_n \notin \mathrm{span}(v_1, \ldots, v_{n-1})$

Teorema 173

- **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 174

- **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

Definizione 73

- **Base ortogonale di uno spazio di Hilbert**
  - $n \in \mathbb{N}$
  - $\mathbb{K}$ campo
  - V spazio di Hilbert su $\mathbb{K}$
  - $v_1, \ldots, v_n$ base di V
  - $v_1, \ldots, v_n$ **base ortogonale di** $V \iff \forall i, j \in [1, n], i \neq j \quad v_i \cdot v_j = 0$
- **Base ortonormale di uno spazio di Hilbert**
  - $n \in \mathbb{N}$
  - $\mathbb{K}$ campo
  - V spazio di Hilbert su $\mathbb{K}$
  - $v_1, \ldots, v_n$ base ortogonale di V
  - $v_1, \ldots, v_n$ **base ortonormale** di $V \iff \forall i, j \in [1, n] \quad v_i \cdot v_j = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$
    - in particolare, è possibile ottenere $v_1, \ldots, v_n$ a partire da $e_1, \ldots, e_n$ tramite rotazioni e riflessioni

Teorema 175

- **Hp**
  - $n \in \mathbb{N}$
  - $\mathbb{K}$ campo
  - $v \in \mathbb{K}^n$
  - $v_1, \ldots, v_k$ base ortonormale di $\mathbb{K}^n$
- **Th**
  - $v = (v \cdot v_1)v_1 + \ldots + (v \cdot v_n)v_n$

Teorema 176

- **Hp**
  - $n \in \mathbb{N}$
  - $\mathbb{K}$ campo
  - $A \in O(n)$
- **Th**
  - $A_1, \ldots, A_n$ e $A^1, \ldots, A^n$ basi ortonormali di $\mathbb{K}^n$

Definizione 74

- **Dimensione di uno spazio vettoriale**

  - $\mathbb{K}$ campo
  - V spazio vettoriale su $\mathbb{K}$
  - $\dim(V)$ è detta **dimensione di** V, ed è la cardinalità delle basi di V

Teorema 177

- **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 178

- **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 179

- **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 180

- **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

Teorema 181

- **Hp**
  - $\mathbb{K}$ campo
  - W spazio vettoriale su $\mathbb{K}$
  - $U, V \subset W$ sottospazi vettoriali
- **Th**
  - $\dim(U + V) = \dim(U) + \dim(V) - \dim(U \cap V)$

Teorema 182

- **Hp**
  - $\mathbb{K}$ campo
  - V spazio vettoriale su $\mathbb{K}$
  - $W \subset V$ sottospazio vettoriale
- **Th**
  - V/W sottospazio vettoriale

Teorema 183

- **Hp**
  - $\mathbb{K}$ campo
  - V spazio vettoriale su $\mathbb{K}$
  - $W \subset V$ sottospazio vettoriale
- **Th**
  - $\dim(V/W) = \dim(V) - \dim(W)$

Teorema 184

- **Hp**
  - $\mathbb{K}$ campo
  - $k \in \mathbb{N}$
  - $V_1, \ldots, V_k$ spazi vettoriali su $\mathbb{K}$
- **Th**
  - $\dim(V_1 \times \ldots \times V_k) = \dim(V_1) \cdot \ldots \cdot \dim(V_k)$

Applicazioni lineari

Definizione 75

- **Applicazioni lineari**

  - $\mathbb{K}$ campo
  - V e W spazi vettoriali su $\mathbb{K}$
  - $f : V \to W$ **morfismo di spazi vettoriali** $\iff \forall x, y \in V \quad f(x+y) = f(x) + f(y)$ e $\forall v \in V, \lambda \in \mathbb{K} \quad f(\lambda v) = \lambda f(v)$
    - un morfismo su spazi vettoriali è detto anche **applicazione lineare** o **trasformazione lineare**

Teorema 185

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

Teorema 186

- !!! **QUI C'È UN BUCO DI COSE CHE NON HO CAPITO**

Teorema 187

- **Hp**
  - $\mathbb{K}$ campo
  - V, W spazi vettoriali su $\mathbb{K}$
- **Th**
  - $V \cong W \iff \dim(V) = \dim(W)$

Definizione 76

- **Kernel e immagine**

  - $\mathbb{K}$ campo
  - V, W spazi vettoriali su $\mathbb{K}$
  - $f : V \to W$ trasformazione lineare
  - $\ker(f) = \{v \in V \mid f(v) = 0_W\}$
  - $\mathrm{im}(f) = \{w \in W \mid \exists v \in V : w = f(v)\}$

Teorema 188

- **Hp**
  - $\mathbb{K}$ campo
  - V, W spazi vettoriali su $\mathbb{K}$
  - $f : V \to W$ trasformazione lineare
- **Th**

- $\ker(f) \subset V$ sottospazio

Teorema 189

- **Hp**
  - $\mathbb{K}$ campo
  - V, W spazi vettoriali su $\mathbb{K}$
  - $f : V \to W$ trasformazione lineare
- **Th**
  - $\mathrm{im}(f) \subset W$ sottospazio

Definizione 77

- **Rango di un'applicazione lineare**

  - $\mathbb{K}$ campo
  - V e W spazi vettoriali su $\mathbb{K}$
  - $f : V \to W$ applicazione lineare
  - $\mathrm{rk}(f) := \dim(\mathrm{im}(f))$ è detto **rango di** f

---

Sottospazi affini

Teorema 190

- !!! **TODO**

Teorema 191

- **Hp**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$
  - $b \in \mathrm{Mat}_{m\times 1}(\mathbb{K})$
  - $X := \{x \in \mathrm{Mat}_{n\times 1}(\mathbb{K}) \mid A \cdot x = b\}$
  - $X \neq \varnothing$
- **Th**
  - X sottospazio affine di $\mathbb{K}^n$, con dimensione pari a $n - \mathrm{rk}(A)$

Teorema fondamentale dell'algebra

- **Hp**
  - $\mathbb{K}$ campo
  - $p(x) \in \mathbb{K}[x] \mid p(x) = a_0x^0 + \ldots + a_nx^n$
- **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 192

- **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 fondamentale dell'aritmetica

- **Hp**
  - $a, b \in \mathbb{N}$
- **Th**
  - $\text{mcm}(a, b) \cdot \text{MCD}(a, b) = a \cdot b$

Teorema cinese dei resti

Teorema 193

- **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 194

- **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 195

- **Hp**
  - $n \in \mathbb{N}$
  - $a_1, \ldots, a_n \in \mathbb{Z}_{\geq 2} \mid \forall i, j \in [1, n] \quad i \neq j \implies \text{MCD}(a_i, a_j) = 1$
  - $b_1, \ldots, b_n \in \mathbb{Z} \mid 0 \leq b_1 < a_1, \ldots, 0 \leq b_n < a_n$
  - $m := \text{mcm}(a_1, \ldots, a_n)$
- **Th**
  - $\exists! x \pmod m \mid \begin{cases} x \equiv b_1 \pmod{a_1} \\ \vdots \\ x \equiv b_n \pmod{a_n} \end{cases}$

Teorema 196

- **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 del binomio di Newton

- **Hp**
  - A anello commutativo
  - $a, b \in A$
  - $n \in \mathbb{N}$
- **Th**
  - $(a+b)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

Teorema 197

- !!! **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 198

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

Teorema 199

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

Teorema 200

- !!! **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 fondamentale di isomorfismo

- **Hp**
  - A, B anelli
  - $f : A \to B$ morfismo di anelli
- **Th**
  - $A/\ker(f) \cong \text{im}(f)$, ovvero $\exists \varphi \mid \varphi : A/\ker(f) \to \text{im}(f) : [a] \to f(a)$ isomorfismo di anelli

Teorema 201

- **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 202

- **Hp**
  - $\mathbb{K}$ campo
  - V, W spazi vettoriali su $\mathbb{K}$
  - $f : V \to W$ trasformazione lineare
- **Th**
  - $V/\ker(f) \cong \mathrm{im}(f)$, o alternativamente $\exists \varphi \mid \varphi : V/\ker(f) \to \mathrm{im}(f) : [v] \to f(v)$

Teorema di Cauchy

- **Hp**
  - G gruppo finito
  - $p \in \mathbb{P}$
  - $p \Big| |G|$
- **Th**
  - $\exists g \in G \mid o(g) = p$

Teorema 203

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

Teorema di Carnot

- **Hp**
  - $n \in \mathbb{N} - \{0\}$
  - $u, v \in \mathbb{K}^n \mid u = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, v = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$
  - θ l'angolo compreso tra u e v
- **Th**

- $||v-u||^2 = ||u||^2 + ||v||^2 - 2\cos(\theta) \cdot ||u|| \cdot ||v||$

Teorema 204

- **Hp**
  - $n \in \mathbb{N} - \{0\}$
  - $u, v \in \mathbb{K}^n \mid u = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, v = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$
  - θ l'angolo compreso tra u e v
- **Th**
  - $\cos(\theta) = \dfrac{u \cdot v}{||u|| \cdot ||v||}$

Teorema del rango

- **Hp**
  - $\mathbb{K}$ campo
  - V, W spazi vettoriali su $\mathbb{K}$
  - $f : V \to W$ trasformazione lineare
- **Th**
  - $\mathrm{rk}(f) = \dim(V) - \dim(\ker(f))$

Teorema di Rouché-Capelli

- **Hp**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$
  - $b \in \mathrm{Mat}_{m\times 1}(\mathbb{K})$
- **Th**
  - $\exists x \in \mathrm{Mat}_{n\times 1}(\mathbb{K}) \mid A \cdot x = b \iff \mathrm{rk}(A) = \mathrm{rk}(A_b)$

Teorema di Cramer

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K}) \mid \det(A) \neq 0$
  - $b \in \mathrm{Mat}_{n\times 1}(\mathbb{K})$
- **Th**

- $\begin{cases} x_1 = \dfrac{1}{\det(A)} \cdot \det \begin{pmatrix} b_1 & a_{1,2} & \cdots & a_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_n & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \\ \vdots \\ x_n = \dfrac{1}{\det(A)} \cdot \det \begin{pmatrix} a_{1,1} & \cdots & a_{1,n-1} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{n,1} & \cdots & a_{n,n-1} & b_n \end{pmatrix} \end{cases}$ sono le componenti del vettore $x \in \mathrm{Mat}_{n\times 1}(\mathbb{K}) \mid A \cdot x = b$

Teorema di Kronecker

- **Hp**
  - $\mathbb{K}$ campo
  - $n, r, r' \in \mathbb{N} - \{0\} \mid r < r' < n$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
  - $M_1 \in \mathrm{Mat}_{r\times r}(\mathbb{K}) \mid M_1$ minore di $A \wedge \det(A) \neq 0$
- **Th**
  - $\mathrm{rk}(A) = r \iff \forall M_1'$ orlato di $M_1 \quad \det(M_1') = 0 \iff \forall M_2 \in \mathrm{Mat}_{r'\times r'}(\mathbb{K}) \mid M_2$ minore di $A \quad \det(M_2) = 0$

Teorema di Binet

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A, B \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
- **Th**
  - $\det(A \cdot B) = \det(A) \cdot \det(B)$

Teorema 205

- **Hp**
  - $\mathbb{K}$ campo
  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$
- **Th**
  - $\det(A)^{-1} = \det(A^{-1})$

Teorema spettrale

- **Hp**

  - $n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{n \times n}(\mathbb{R}) \mid A$ simmetrica

  1. $\forall \lambda \in \mathrm{sp}(A) \quad \lambda \in \mathbb{R}$
  2. A diagonalizzabile
  3. $\exists B^1, \ldots, B^n$ autovettori di $A \mid B^1, \ldots, B^n$ base ortonormale di $\mathbb{R}^n$
  4. $\exists B \in O(n) \mid B^{-1}AB$ diagonale

- **Th**
  - le proposizioni sono equivalenti