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**
  - $p \,\middle|\, \displaystyle\binom{p}{k}$

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 $\mathbb{Z}_p$

Gruppi diedrali

Definizione 2

- **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 8

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

- $|D_n| = 2n$

Teorema 9

- **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 10

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

Teorema 11

- **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 3

- **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 12

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

Gruppi

Definizione 4

- **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 13

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

Teorema 14

- **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 15

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

Teorema 16

- **Hp**
    - X, Y insiemi finiti

- **Th**
  - $\left|Y^X\right| = |Y|^{|X|}$

Anelli

Definizione 5

- **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 6

- **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 17

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

Teorema 18

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

Definizione 7

- **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 19

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

Teorema 20

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

Definizione 8

- **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 21

- **Hp**
  - A dominio di integrità

- **Th**
  - a primo $\implies$ a irriducibile

Sottogruppi

Definizione 9

- **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 10

- **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 22

- **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 tre formulazioni sono equivalenti

Ordine

Definizione 11

- **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 23

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

Teorema 24

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

Teorema 25

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

Teorema 26

- **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 27

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

Teorema 28

- **Hp**

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

Teorema 29

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

Teorema 30

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

Teorema 31

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

Ideali

Definizione 12

- **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 32

- **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 33

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

Teorema 34

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

Teorema 35

- **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* $a_1, \ldots, a_n \in A$

Definizione 13

- **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 36

- **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 37

- **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 38

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

Definizione 14

- **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 39

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

Teorema 40

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

Operazioni sugli ideali

Definizione 15

- **+ tra ideali**

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

Teorema 41

- **Hp**

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

Definizione 16

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

Teorema 42

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

Definizione 17

- **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 18

- **$\cdot$ 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 43

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

Teorema 44

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

- **Th**
  - $I(a) + I(b) = I(d)$

Teorema 45

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

Induzione

Definizione 19

- **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 46

- **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 20

- **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 21

- **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 47

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

Teorema 48

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

Teorema 49

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

Teorema 50

- **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 51

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

Teorema 52

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

Funzione totiente di Eulero

Definizione 22

- **Funzione totiente di Eulero**

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

Teorema 53

- **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 54

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

Teorema 55

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

Teorema 56

- **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 23

- **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 24

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

Teorema 57

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

Definizione 25

- **Prodotto scalare**

- $\mathbb{K}$ campo
- $m, n \in \mathbb{N} - \{0\}$
- $A \in \mathrm{Mat}_{1\times n}(\mathbb{K})$
- $B \in \mathrm{Mat}_{m\times 1}(\mathbb{K})$
- $A \cdot B := \sum_{i=1}^{n} a_i \cdot b_i$ è il **prodotto scalare tra A e B**

Teorema 58

- **!!! WIP**

Definizione 26

- **Prodotto tra matrici**
  - $\mathbb{K}$ campo
  - $l, m, n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{l\times m}(\mathbb{K}) \mid A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{l,1} & \cdots & a_{l,m} \end{pmatrix}$
  - $B \in \mathrm{Mat}_{m\times n}(\mathbb{K}) \mid B = \begin{pmatrix} b_{1,1} & \cdots & b_{1,n} \\ \vdots & \ddots & \vdots \\ b_{m,1} & \cdots & b_{m,n} \end{pmatrix}$
  - $C \in \mathrm{Mat}_{l\times n}(\mathbb{K}) \mid C = A \cdot B$ 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 59

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

Teorema 60

- **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

---

Rango

Definizione 27

- **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 61

- **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 62

- **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 28

- **Moltiplicazione sinistra**

  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $x \in \mathrm{Mat}_{n\times 1}(\mathbb{K})$
  - $\forall A \in \mathrm{Mat}_{m\times n}(\mathbb{K}) \quad L_A : \mathbb{K}^n \to \mathbb{K}^m : x \to A \cdot x$

Teorema 63

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

- $x \in \mathrm{Mat}_{n\times 1}(\mathbb{K})$
- **Th**
  - $\forall A \in \mathrm{Mat}_{m\times n}(\mathbb{K}) \quad L_A$ è una trasformazione lineare

Teorema 64

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

Definizione 29

- **Rango di una matrice**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$
  - $x \in \mathrm{Mat}_{n\times 1}(\mathbb{K})$
  - $\mathrm{rk}(A) := \mathrm{rk}(L_A)$ è il **rango di** A

Teorema 65

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

Definizione 30

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

Operazioni su righe e colonne

Definizione 31

- **Scambio di righe di una matrice**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$
  - $\forall A_1, \ldots, A_m$ righe di A, scambiare A_i e A_j lascia invariato $\ker(L_A)$
- **Moltiplicazione di una riga per una costante**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$
  - $\lambda \in \mathbb{K}^*$
  - $\forall A_1, \ldots, A_m$ 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
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$
  - $\lambda \in \mathbb{K}^*$
  - $\forall A_1, \ldots, A_m$ 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
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$
  - $\forall A^1, \ldots, A^m$ colonne di A, scambiare A^i e A^j lascia invariato $\mathrm{im}(L_A)$
- **Moltiplicazione di una colonna per una costante**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$
  - $\lambda \in \mathbb{K}^*$
  - $\forall A^1, \ldots, A^m$ colonne di A, moltiplicare A^i per λ lascia invariato $\mathrm{im}(L_A)$
- **Somma di una colonna con un multiplo di un'altra**
  - $\mathbb{K}$ campo
  - $m, n \in \mathbb{N} - \{0\}$
  - $A \in \mathrm{Mat}_{m\times n}(\mathbb{K})$
  - $\lambda \in \mathbb{K}^*$
  - $\forall A^1, \ldots, A^m$ righe di A, sommare ad A^i un certo $\lambda \cdot A^j$ lascia invariato $\mathrm{im}(L_A)$

Teorema 66

- **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 67

- **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**
  - $A \equiv B \implies \ker(L_A) = \ker(L_B) \wedge \text{rk}(A) = \text{rk}(B)$

Teorema 68

- **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 colonne definite precedentemente
- **Th**
  - $\equiv$ una relazione di equivalenza

Teorema 69

- **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 colonne definite precedentemente
- **Th**
  - $A \equiv B \implies \text{im}(L_A) = \text{im}(L_B) \wedge \text{rk}(A) = \text{rk}(B)$

Morfismi

Definizione 32

- **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 70

- **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 71

- **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 33

- **Isomorfismo**

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

Teorema 72

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

Teorema 73

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

- $\cong$ è una relazione di equivalenza

Teorema 74

- **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 75

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

Teorema 76

- **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 77

- **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 78

- **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 79

- **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 $(G, \cdot)$

Kernel e immagine

Definizione 34

- **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 80

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

Teorema 81

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

Teorema 82

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

Teorema 83

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

Teorema 84

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

Teorema 85

- **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 86

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

Numeri complessi

Definizione 35

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

Teorema 87

- **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 36

- **Coniugato**

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

Teorema 88

- **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 89

- **Hp**
  - $0 \leq \theta < 2\pi$
- **Th**
  - $e^{i\theta} = \cos\theta + i \sin\theta$

Definizione 37

- **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 38

- **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 39

- **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 90

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

Teorema 91

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

Teorema 92

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

Permutazioni

Definizione 40

- **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 93

- **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 41

- **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 94

- **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 95

- **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 96

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

Trasposizioni

Definizione 42

- **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 97

- **Hp**
  - $n \in \mathbb{N}$
  - $\sigma \in S_n$
- **Th**
  - $\exists 1 \leq i_1, \ldots, i_k < n \mid \sigma = \tau_{i_1, i_1+1} \ldots \tau_{i_k, i_k+1}$, quindi ogni permutazione può essere riscritta come composizione di trasposizioni adiacenti

---

Segno

Definizione 43

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

Teorema 98

- **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 99

- **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 100

- **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 101

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

Teorema 102

- **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 103

- **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 104

- **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 44

- **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 105

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

Definizione 45

- **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 106

- **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 107

- **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 108

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

Teorema 109

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

Definizione 46

- **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 110

- **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 111

- **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 112

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

Teorema 113

- **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**
  - $d(x) = \mathrm{MCD}(a_1(x), \ldots, a_n(x))$

Teorema 114

- **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**
  - $m(x) = \mathrm{mcm}(a_1(x), \ldots, a_n(x))$

Teorema 115

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

Teorema 116

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

Teorema 117

- **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 118

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

Teorema 119

- **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 120

- **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**
  - $a \mid a_0 \wedge b \mid a_n$

Teorema 121

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

Relazioni

Definizione 47

- **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** $\iff \forall x, y, z \in R \quad (x, y) \in R \wedge (y, z) \in R \implies (x, z) \in R$
- **Relazione antisimmetrica**
  - S insieme
  - R relazione in $S \times S$

  - R **transitiva** $\iff \forall x, y \in R \quad (x,y) \in R \wedge (y,x) \in R \implies x = y$
- **Relazione totale**
  - S insieme
  - R relazione in $S \times S$
  - R **totale** $\iff \forall x, y \in R \quad (x,y) \in R \vee (y,x) \in R$
- **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 122

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

Teorema 123

- **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 124

- **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 125

- **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 $\dfrac{a}{d}x \equiv \dfrac{b}{d} \left(\mathrm{mod}\ \dfrac{n}{d}\right)$

Teorema 126

- **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 48

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

Teorema 127

- **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 128

- **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 129

- **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 49

- **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 130

- **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 131

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

Teorema 132

- **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 133

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

Teorema 134

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

Spazi Vettoriali

Definizione 50

- **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**

Teorema 135

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

Definizione 51

- **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 52

- **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 136

- **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 53

- **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** $V \iff \text{span}(v_1, \ldots, v_n) = V$
    - 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 137

- **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 138

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

Teorema 139

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

Teorema 140

- **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 54

- **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 141

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

Teorema 142

- **Hp**
  - $\mathbb{K}$ campo
  - W spazio vettoriale su $\mathbb{K}$
  - $n := \dim(W)$
  - $k \in \mathbb{N} \mid k < n$
  - $w_1, \dots, w_k \in W$ linearmente indipendenti
- **Th**
  - $\exists w_{k+1}, \dots, w_n \in W \mid w_1, \dots, w_n$ è una base di W

Teorema 143

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

Teorema 144

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

Teorema 145

- **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 146

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

Teorema 147

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

Applicazioni lineari

Definizione 55

- **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 148

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

Teorema 149

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

Teorema 150

- **Hp**
  - $\mathbb{K}$ campo
  - V, W spazi vettoriali su $\mathbb{K}$

- **Th**
  - $V \cong W \iff \dim(V) = \dim(W)$

Definizione 56

- **Kernel e immagine**

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

Teorema 151

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

Teorema 152

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

Definizione 57

- **Rango di un'applicazione lineare**

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

---

Sottospazi affini

Teorema 153

- !!! **TODO**

Teorema 154

- **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 155

- **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 156

- **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 157

- **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 158

- **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 159

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

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

- **Th**
  - $o = \text{mcm}(o_1, \dots, o_k)$

Teorema del binomio di Newton

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

Teorema 160

- !!! **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 161

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

Teorema 162

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

Teorema 163

- **!!! 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 164

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

Teorema 165

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

Teorema di Cauchy

- **Hp**
  - G gruppo finito
  - $p \in \mathbb{P}$

- $p \,\Big|\, |G|$

- **Th**
  - $\exists g \in G \mid o(g) = p$

Teorema 166

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

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**
  - $\exists x \in \mathrm{Mat}_{n\times 1}(\mathbb{K}) \mid A \cdot x = b \iff \mathrm{rk}(A) = \mathrm{rk}(A_b)$