

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

Teorema 1

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

Teorema 2

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

Teorema 3

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

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 $\frac{360^\circ}{n}$ 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 | $D_n \cong X$
 - * $D_3 \cong S_3$

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

- **Semigrupp**

- S insieme
- $m : S \times S \rightarrow S$
- (S, m) **semigrupp** $\iff \forall x, y, z \in S \quad m(x, m(y, z)) = m(m(x, y), z)$
- **Monoide**
 - S insieme
 - $m : S \times S \rightarrow S$
 - (S, m) **monoide** $\iff (S, m)$ semigrupp e $\forall x \in S \quad \exists e \in S \mid m(x, e) = m(e, x) = x$
- **Gruppo**
 - S insieme
 - $m : S \times S \rightarrow S$
 - (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
 - $m : S \times S \rightarrow S$
 - (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,
 - $Y^X = \{f \mid f : X \rightarrow Y\}$
- **Th**
 - (X^X, \circ) è monoide

Teorema 16

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

- **Th**
 - $|Y^X| = |Y|^{|X|}$
-

Anelli

Definizione 5

- **Anello**
 - A insieme
 - $+: A \times A \rightarrow A$
 - $\cdot: A \times A \rightarrow A$
 - $(A, +, \cdot)$ **anello** $\iff (A, +)$ gruppo abeliano, (A, \cdot) monoide e $\forall a, b, c \in A \quad a \cdot (b + c) = a \cdot b + a \cdot c$
 - $a \cdot b = b \cdot a \quad \forall a, b \in A \implies (A, \cdot, +)$ è un **anello commutativo**
- **Campo**
 - $(A, +, \cdot)$ anello
 - $(A, +, \cdot)$ è un **campo** $\iff \forall x \in A \quad \exists x^{-1}$ rispetto a \cdot
- **Semianello commutativo**
 - A insieme
 - $+: A \times A \rightarrow A$
 - $\cdot: A \times A \rightarrow A$
 - $(A, +, \cdot)$ **semianello commutativo** $\iff (A, +)$ monide commutativo, (A, \cdot) monoide commutativo e $\forall a, b, c \in A \quad a \cdot (b + c) = a \cdot b + a \cdot c$
- **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** $\iff \nexists x : x \mid 0$, oltre a $x = 0$
 - **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** $\iff \exists e \in H \mid e \text{ è l'elemento neutro, } H * H \subset H$
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** $\iff xH = Hx \quad \forall x \in G$

Teorema 22

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

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**
 - $(H(g), \cdot) \subset (G, \cdot)$ è sottogruppo

Teorema 24

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

Teorema 25

- **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 26

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

Teorema 27

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

Teorema 28

- **Hp**

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

Teorema 29

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

Teorema 30

- **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 31

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

Teorema 32

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

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

Teorema 33

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

Teorema 34

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

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 35

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

Teorema 36

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

Teorema 37

- **Hp**

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

Definizione 14

- **Massimo Comun Divisore**
 - $a_1, \dots, a_n \in \mathbb{Z}$
 - $\exists! d \in \mathbb{N} \mid I(a_1, \dots, a_n) = I(d)$, ed è detto **massimo comun divisore degli**
 a_1, \dots, a_n
 - per dimostrazione precedente $I(a_1, \dots, a_n)$ 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, \dots, a_n per dimostrazione precedente

Teorema 38

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

Teorema 39

- !!! 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 40

- **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 41

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

Definizione 17

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

Definizione 18

- **\cdot tra ideali**
 - $(A, +, \cdot)$ anello commutativo
 - $I, J \subset A$ ideali
 - $I \cdot J = \{i_1 j_1 + \dots + i_k j_k \mid k \geq 1, \forall i_1, \dots, i_k \in I, j_1, \dots, j_k \in J\}$

Teorema 42

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

Teorema 43

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

Teorema 44

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

Induzione

Definizione 19

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

Teorema 45

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

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

Teorema 46

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

Teorema 47

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

Teorema 48

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

Teorema 49

- **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 50

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

Teorema 51

- **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 52

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

Teorema 53

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

Teorema 54

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

Teorema 55

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

Matrici

Definizione 23

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

Definizione 24

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

Teorema 56

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

Teorema 57

- **!!! WIP**
-

Morfismi

Definizione 25

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

Teorema 58

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

Teorema 59

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

Isomorfismi

Definizione 26

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

Teorema 60

- **Hp**
 - $f : G \rightarrow H$ isomorfismo

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

Teorema 61

- **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 62

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

Teorema 63

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

Teorema 64

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

Teorema 65

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

Teorema 66

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

Kernel e immagine

Definizione 27

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

Teorema 67

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

Teorema 68

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

Teorema 69

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

Teorema 70

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

Teorema 71

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

Teorema 72

- **Hp**
 - $f : \mathbb{Z} \rightarrow \mathbb{C} - \{0\} : k \rightarrow \zeta^k$
 - f morfismo di gruppi $(\mathbb{Z}, +)$ e $(\mathbb{C} - \{0\}, \cdot)$
 - $I(n)$ ideale generato da n !!! **CONTROLLA SE SERVE QUESTA COSA**
- **Th**
 - $\ker(f) = I(n)$

Teorema 73

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

Numeri complessi

Definizione 28

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

Teorema 74

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

Definizione 29

- **Coniugato**
 - $z = a + ib$

- $\bar{z} := a - ib$ è il **coniugato** di z

Teorema 75

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

Teorema 76

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

Definizione 30

- **Raggio**
 - $z = a + ib$
 - $|z| := \sqrt{a^2 + b^2}$ è il **raggio** di z
 - è la distanza di z dall'origine nel piano di Gauss

Forma polare

- $\forall z \in \mathbb{C} - 0 \implies z = |z| \cdot e^{i\theta}$

Definizione 31

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

Teorema 77

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

Teorema 78

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

Teorema 79

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

Permutazioni

Definizione 32

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

Teorema 80

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

Definizione 33

- **Ciclo di una permutazione**
 - $n \in \mathbb{N}$
 - $\sigma \in S_n$
 - $\exists 1 \leq i_1, \dots, i_d \leq n \in \mathbb{N} \mid \left\{ \begin{array}{l} \sigma(i_1) = i_2 \\ \sigma(i_2) = i_3 \\ \vdots \\ \sigma(i_{d-1}) = i_d \\ \sigma(i_d) = i_1 \end{array} \right. \implies i_1, \dots, i_n \text{ costituiscono un ciclo di } \sigma$

Teorema 81

- **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 82

- **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 83

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

Trasposizioni

Definizione 34

- **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
 - $\tau_{i,j}^2 = \text{id} \iff \tau_{i,j} = \tau_{i,j}^{-1}$
- **Trasposizione adiacente**
 - $n \in \mathbb{N}$
 - $i, j \in \mathbb{N} \mid 1 \leq i < j \leq n \wedge j = i + 1$
 - $\tau_{i,j} = \tau_{i,i+1}$ è detta **trasposizione adiacente**, poiché inverte esclusivamente due elementi, adiacenti, tra loro

Teorema 84

- **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 35

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

Teorema 85

- **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 86

- **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 87

- **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 88

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

Teorema 89

- **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 90

- **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 91

- **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 36

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

Teorema 92

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

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

Definizione 37

- **Grado del polinomio**
 - \mathbb{K} campo
 - $a(x) = a_0x^0 + \dots + a_nx^n \in \mathbb{K}[x]$
 - $\deg(a(x)) := \begin{cases} n & a(x) \neq 0 \\ -\infty & a(x) = 0 \end{cases}$

Teorema 93

- **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 94

- **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 95

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

Teorema 96

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

Definizione 38

- **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 97

- **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 98

- **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 99

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

Teorema 100

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

Teorema 101

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

Teorema 102

- **Hp**
 - \mathbb{K} campo
 - $a_1(x), \dots, a_n(x) \in \mathbb{K}[x]$
 - $c \in \mathbb{K}$

- $d(x) := \text{MCD}(a_1(x), \dots, a_n(x))$
- **Th**
 - $a_1(c) = \dots = a_n(c) = 0 \iff d(c) = 0$

Teorema 103

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

Teorema 104

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

Teorema 105

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

Teorema 106

- **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 107

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

Teorema 108

- !!! MANCA UN TEOREMA ENORME

Relazioni

Definizione 39

- **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 109

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

Teorema 110

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

Teorema 111

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

Teorema 112

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

Teorema 113

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

Partizioni

Definizione 40

- **Partizione**

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

Teorema 114

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

Teorema 115

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

Classi laterali

Teorema 116

- **Hp**
 - G gruppo
 - $H \subset G$ sottogruppo
 - $x, y \in G$
- **Th**
 - $x \sim_S y \iff x^{-1}y \in H$ è una relazione di equivalenza

Definizione 41

- **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 117

- **Hp**

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

Teorema 118

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

Teorema 119

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

Teorema 120

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

Spazi Vettoriali

Definizione 42

- **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 $\cdot : K \times V \rightarrow V$ che ammetta elemento neutro, inoltre $\forall s, t \in \mathbb{K}, v \in V$ $s \cdot (t \cdot v) = (s \cdot t) \cdot v, (s + t) \cdot v = s \cdot v + t \cdot v$ e infine $\forall s \in \mathbb{K}, v, w \in V$ $s \cdot (v + w) = s \cdot v + s \cdot w$
 - $x \in V$ è detto **vettore**

Teorema 121

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

Definizione 43

- **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 44

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

Teorema 122

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

Definizione 45

- **Vettori generatori**
 - $n \in \mathbb{N}$
 - \mathbb{K} campo
 - V spazio vettoriale su \mathbb{K}
 - $v_1, \dots, v_n \in V$
 - v_1, \dots, v_n sono **generatori di V** $\iff \text{span}(v_1, \dots, v_n) = V$
 - equivalentemente, ogni altro vettore in V è una combinazione lineare degli v_1, \dots, v_n
- **Indipendenza lineare**
 - $n \in \mathbb{N}$

- \mathbb{K} campo
- V spazio vettoriale su \mathbb{K}
- $v_1, \dots, v_n \in V$
- v_1, \dots, v_n sono **linearmente indipendenti** se e solo se $\lambda_1 v_1 + \dots + \lambda_n v_n = 0_V \iff \lambda_1 = \dots = \lambda_n = 0_{\mathbb{K}}$
 - equivalentemente, nessuno degli v_1, \dots, 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}
 - $v_1, \dots, v_n \in V$
 - v_1, \dots, v_n sono una **base di V** $\iff v_1, \dots, v_n$ sono generatori di V e linearmente indipendenti
 - n è detta **cardinalità della base di V**

Teorema 123

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

Teorema 124

- **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 linearmente indipendenti $\iff v_1, \dots, v_{n-1}$ linearmente indipendenti $\wedge v_n \notin \text{span}(v_1, \dots, v_{n-1})$

Teorema 125

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

Teorema 126

- **Hp**

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

Definizione 46

- **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 127

- **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 $V \iff \forall v \in V \quad \exists! \lambda_1, \dots, \lambda_n \in \mathbb{K} \mid v = \lambda_1 v_1 + \dots + \lambda_n v_n$
-

Applicazioni lineari

Definizione 47

- **Applicazioni lineari**
 - \mathbb{K} campo
 - V e W spazi vettoriali su \mathbb{K}
 - $f : V \rightarrow W$ **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 128

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

Teorema 129

- !!! QUI C'È UN BUCONE

Teorema 130

- **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 131

- **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 132

- **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 133

- **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 fondamentale dell'algebra

- **Hp**

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

Teorema della divisione euclidea con il resto

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

Teorema 134

- **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 135

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

Teorema 136

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

Teorema 137

- **Hp**
 - $n \in \mathbb{N}$
 - $a_1, \dots, a_n \in \mathbb{Z}_{\geq 2} \mid \forall i, j \in [1, n] \quad i \neq j \implies \text{MCD}(a_i, a_j) = 1$
 - $b_1, \dots, b_n \in \mathbb{Z} \mid 0 \leq b_1 < a_1, \dots, 0 \leq b_n < a_n$
 - $m := \text{mcm}(a_1, \dots, a_n)$
- **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 138

- **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 139

- !!! 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 140

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

Teorema 141

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

Teorema 142

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

Teorema 143

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

Teorema di Cauchy

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

Teorema 144

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