

# Algebra

## Gruppi

- $S$  insieme e  $m : S \times S \rightarrow S$ 
  - $(S, m)$  **semigrupp**  $\iff$  vale la **proprietà associativa** in  $m$  su  $S$ 
    - $m(x, m(y, z)) = m(m(x, y), z) \quad \forall x, y, z \in S$
  - $(S, m)$  **monoide**  $\iff$  è un semigrupp in cui **esiste l'elemento neutro** rispetto a  $m$ 
    - $\exists e \mid m(x, e) = m(e, x) = x \quad \forall x \in S$
    - se esiste,  $e$  è unico
      - per assurdo,  $\exists e_1, e_2 \mid e_1 \neq e_2$  elementi neutri, allora
$$\left. \begin{aligned} m(x, e_1) &= m(e_1, x) = x \\ m(x, e_2) &= m(e_2, x) = x \end{aligned} \right\} \Rightarrow m(e_1, x) = m(e_2, x) \Rightarrow e_1 = e_2 \text{ necessariamente}$$
  - $(S, m)$  **gruppo**  $\iff$  è un monoide in cui **esiste l'inverso** per ogni elemento di  $S$ 
    - $\exists x^{-1} \mid m(x, x^{-1}) = m(x^{-1}, x) = e \quad \forall x \in S$
    - se esiste,  $x^{-1}$  è unico
      - $\triangle$  MANCA DIMOSTRAZIONE
  - $(S, m)$  **gruppo abeliano**  $\iff$  è un gruppo in cui vale la **proprietà commutativa** in  $m$  su  $S$ 
    - $m(x, y) = m(y, x) \quad \forall x, y \in S$

## Esempi

- $X, Y$  insiemi,  $Y^X = \{f \mid f : X \rightarrow Y\}$ 
  - $X, Y$  finiti  $\Rightarrow |Y^X| = |Y|^{|X|}$ 
    - $\triangle$  MANCA DIMOSTRAZIONE
  - $(X^X, \circ)$  è **monoide**
    - $(f \circ g) \circ h = f \circ (g \circ h)$
    - $\forall X, \exists \text{id}_X \mid \text{id}_X : X \rightarrow X : x \rightarrow x$ , che costituisce dunque l'elemento neutro, mappando ogni elemento in sé stesso
  - $S_X = \{f \mid f : X \rightarrow Y \text{ biettiva}\}$  è detto **gruppo simmetrico di  $X$** 
    - $|S_X| = |X|!$
    - $(S_X, \circ)$  è un **gruppo**, non commutativo se  $|X| \geq 3$

## Anelli

- $A$  insieme
- $+: A \times A \Rightarrow A$
- $*: A \times A \Rightarrow A$
- $(A, +, *)$  anello  $\iff$ 
  - $(A, +)$  **gruppo abeliano**
  - $(A, *)$  **monoide**
  - vale la **proprietà distributiva** della forma  $a * (b + c) = a * b + a * c$
- $a * b = b * a \quad \forall a, b \in A \Rightarrow (A, *, +)$  è un **anello commutativo**
- $\exists x^{-1} \quad \forall x \in A \mid x * x^{-1} = x^{-1} * x = e \Rightarrow (A, +, *)$  è un **campo**

## Esempi

- $(\mathbb{Z}, +, \cdot)$  è un **anello commutativo**
- $(\mathbb{C}, +, \cdot)$  è un **campo**
- $\triangle$  MANCA DIMOSTRAZIONE polinomi a coefficienti in  $A$

## Numeri complessi

- $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}, i \mid i^2 = -1\}$
- $z \in \mathbb{C} \Rightarrow \begin{cases} a := \text{Re}(z) \\ b := \text{Im}(z) \end{cases}$
- $\mathbb{R} \subset \mathbb{C}$

- $\begin{cases} z = a + ib \\ w = c + id \end{cases} \implies z + w = (ac - bd) + i(ad + bc)$
- $z = a + ib \implies \bar{z} := a - ib$ 
  - $\bar{\bar{z}} = z$
  - $\overline{z + w} = \bar{z} + \bar{w}$
  - $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$
- $|z| = \sqrt{a^2 + b^2}$ 
  - $z \in \mathbb{C}, z \neq 0 \implies z = |z|e^{i\theta}$  dove  $e^{i\theta} = \cos \theta + i \sin \theta$  è detta **formula di Eulero**
  - $\arg(z) := \begin{cases} \cos \theta = \frac{a}{|z|} \\ \sin \theta = \frac{b}{|z|} \end{cases} \implies \exists! 0 \leq \theta \leq 2\pi$ 
    - $\text{Arg}(z) := \theta$
    - $\arg(z) \subset \mathbb{R}$  è l'insieme delle soluzioni del sistema, mentre  $\text{Arg}(z)$  è la **soluzione principale**
- $\begin{cases} z \cdot \bar{z} = (a + ib)(a - ib) = a^2 - (ib)^2 \\ i^2 = -1 \end{cases} \implies a^2 - i^2 b^2 = a^2 + b^2 = |z|^2$ 
  - $z \cdot \bar{z} = |z|^2 \implies z = \frac{|z|^2}{\bar{z}} \implies z^{-1} = \frac{z}{|z|^2} = \frac{a}{a^2 + b^2} - i \frac{b}{a^2 + b^2}$
  - $\frac{z \cdot \bar{z}}{|z|^2} = 1 \implies \mathbb{C}$  ammette inversi moltiplicativi  $\implies (\mathbb{C}, +, *)$  è un **campo**
- $|z \cdot w| = |z||w|, \arg(z \cdot w) = \arg(z) + \arg(w)$
- $|\bar{w}| = |w|, \arg(\bar{w}) = -\arg(w)$
- $|w^{-1}| = |w|^{-1}, \arg(w^{-1}) = -\arg(w)$
- $\left| \frac{z}{w} \right| = \frac{|z|}{|w|}, \arg\left(\frac{z}{w}\right) = \arg(z) - \arg(w)$
- **Formula di de Moivre**
  - $z^n = r^n e^{in\theta}, \arg(z^n) = n \arg(z)$

## Teorema fondamentale dell'algebra

Data un'equazione  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n = 0$ , con  $a_0, a_1, a_2, \dots, a_n \in \mathbb{C}, n \geq 1, a_n \neq 0 \implies \exists x \in \mathbb{C}$

## Relazioni

- dato un insieme  $S$ , allora  $R := R \mid R \subseteq S \times S$
- $R$  è una **relazione di equivalenza**  $\iff$ 
  - **riflessiva**:  $R$  riflessiva  $\iff xRx \quad \forall x \in S$
  - **simmetrica**:  $R$  simmetrica  $\iff xRy \implies yRx \quad \forall x, y \in S$
  - **transitiva**:  $R$  transitiva  $\iff xRy, yRz \implies xRz \quad \forall x, y, z \in S$
- $R$  è un **ordine parziale**  $\iff$ 
  - $R$  riflessiva, transitiva e antisimmetrica
    - $R$  antisimmetrica  $\iff xRy, yRx \implies x = y \quad \forall x, y \in S$
- $R$  **ordine totale**  $\iff$ 
  - $R$  ordine parziale in cui vale la **totalità**
    - $R$  totale  $\iff xRy \vee yRx \quad \forall x, y \in S$

## Esempi

- $\forall X, A, B \subset P(X), A \subset B$  è **ordine parziale** su  $P(X)$ 
  - $\triangle$  MANCA DIMOSTRAZIONE
- $m, n \in \mathbb{N}, m \mid n$  ("m divide n")  $\iff \exists p \in \mathbb{N} \mid mp = n$ 
  - è **ordine parziale**
    - **riflessività**:  $\forall x \in \mathbb{N}, x \mid x \Rightarrow \exists p \in \mathbb{N} \mid xp = x \implies p = 1 \in \mathbb{N}$
    - **transitività**:  $\forall d, m, n \in \mathbb{N}, d \mid m \wedge m \mid n \implies d \mid n$ 
      - $\left. \begin{matrix} d \mid m \Rightarrow \exists p_1 \in \mathbb{N} \mid dp_1 = m \\ m \mid n \Rightarrow \exists p_2 \in \mathbb{N} \mid mp_2 = n \end{matrix} \right\} \Rightarrow dp_1p_2 = n \Rightarrow d \mid n$  poiché  $p_1 \in \mathbb{N} \wedge p_2 \in \mathbb{N} \implies p_1p_2 \in \mathbb{N}$
    - **antisimmetria**:  $\forall m, n \in \mathbb{N}, m \mid n \wedge n \mid m \implies m = n$ 
      - $\left. \begin{matrix} m \mid n \Rightarrow \exists p_1 \in \mathbb{N} \mid mp_1 = n \\ n \mid m \Rightarrow \exists p_2 \in \mathbb{N} \mid np_2 = m \end{matrix} \right\} \Rightarrow mp_1p_2 = m \implies p_1p_2 = 1 \implies p_1 = p_2 = 1$  perché  $p_1, p_2 \in \mathbb{N}$ , quindi  $np_2 = m \wedge p_2 = 1 \implies n = m$
- $a, b \in \mathbb{Z}, a \equiv b \pmod{n} \iff m \mid b - a$  detta **congruenza modulo n**
  - è una **relazione di equivalenza**
    - **riflessività**:  $\forall a \in \mathbb{Z}, a \equiv a \pmod{n} \implies n \mid a - a \implies n \mid 0$ , e  $n \mid 0 \implies \exists p \in \mathbb{Z} \mid n \cdot p = 0 \implies p = 0 \in \mathbb{Z}$

- *simmetria*:  $\forall a, b \in \mathbb{Z}, a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$ 
    - $a \equiv b \pmod{n} \implies n \mid b - a \implies \exists p_1 \in \mathbb{Z} \mid n \cdot p_1 = b - a$
    - $b \equiv a \pmod{n} \implies n \mid a - b \implies \exists p_2 \in \mathbb{Z} \mid n \cdot p_2 = b - a$
    - $\left. \begin{array}{l} np_1 = b - a \implies b = np_1 + a \\ np_2 = a - b \end{array} \right\} \implies np_2 = a - np_1 - a = -np_1 \implies n(p_2 + p_1) = 0$
    - $n \neq 0$ , quindi  $p_2 + p_1 = 0 \implies p_2 = -p_1$
    - per definizione di  $p_2$ ,  
 $np_2 = b - a \implies n(-p_1) = b - a \implies (-1) \cdot np_1 = b - a \implies np_1 = a - b \implies n \mid b - a$
  - *transitività*:  $\forall a, b, c \in \mathbb{Z}, a \equiv b \pmod{n}, b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$ 
    - $a \equiv b \pmod{n} \implies n \mid b - a \implies \exists p_1 \in \mathbb{Z} \mid n \cdot p_1 = b - a$
    - $b \equiv c \pmod{n} \implies n \mid c - b \implies \exists p_2 \in \mathbb{Z} \mid n \cdot p_2 = c - b$
    - $\left. \begin{array}{l} np_1 = b - a \implies b = np_1 + a \\ np_2 = c - b \end{array} \right\} \implies np_2 = c - np_1 - a \implies np_2 + np_1 = c - a \implies n(p_2 + p_1) = c - a$
    - $p_1, p_2 \in \mathbb{Z} \implies p_1 + p_2 \in \mathbb{Z} \implies \exists p_1 + p_2 \in \mathbb{Z} \mid n(p_1 + p_2) = c - a \implies n \mid c - a$  per definizione
- $x \sim y \iff x^{-1}y \in H$ 
    - è una **relazione di equivalenza**
      - $\triangle$  MANCA DIMOSTRAZIONE

## Teorema della divisione euclidea con il resto

$$m, n \in \mathbb{Z}, n > 0 \implies \exists! q, r \in \mathbb{Z} \mid m = nq + r, 0 \leq r < n$$

## Sottogruppi

- $H \subset G$  **sottogruppo** di un gruppo  $(G, *) \iff$ 
  - $\exists e \in H \mid e$  è l'**elemento neutro**
  - $H$  è **chiuso rispetto all'operazione  $*$** 
    - $\forall x, y \in H, x * y \in H$
  - $H$  è **chiuso rispetto agli inversi**
    - $\forall x \in H, \exists x^{-1} \in H$
- $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +) \subset (\mathbb{C}, +)$  tutti sottogruppi

## Classi di equivalenza

- $[x] := \{y \in S \mid x \sim y\}$ 
  - $x \in [x] \quad \forall x \in S$ 
    - $x \sim x \quad \forall x \in S$  per definizione
  - $\forall x, y \in S, [x] = [y] \iff x \sim y \vee [x] \cap [y] = \emptyset \iff x \sim y$ , quindi **due classi di equivalenza o coincidono, o non si intersecano**
    - se  $x \sim y, \exists z \in [x] \Rightarrow \left. \begin{array}{l} z \sim x \\ x \sim y \end{array} \right\} z \sim y$  per transitività, quindi  $z \in [y]$
    - se  $y \sim x, \exists z \in [y] \Rightarrow \left. \begin{array}{l} z \sim y \\ y \sim x \end{array} \right\} z \sim x$  per transitività, quindi  $z \in [x]$
    - quindi  $\forall z \in [x], x \sim y \implies z \in [y]$  e  $\forall z \in [y], y \sim x \implies z \in [x]$ , quindi  $[x] = [y]$  necessariamente
    - se  $x \not\sim y$ , e per assurdo  $[x] \cap [y] \neq \emptyset$  allora  $\exists z \mid z \in [x] \wedge z \in [y] \Rightarrow z \sim x \wedge z \sim y \implies x \sim y$  per transitività
- $S / \sim = \{[x] \mid x \in S\}$  è l'insieme di tutte le classi di equivalenza, detto **insieme quoziente**
  - presa come relazione di equivalenza la congruenza modulo  $n$ , si definisce  $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\} \implies |\mathbb{Z}_n| = n$ , in cui ogni elemento è la classe di equivalenza di ogni intero fino ad  $n-1$ , e  $[x] = \{y \in \mathbb{Z} \mid y \equiv x \pmod{n}\}$
  - $\exists! q, r \in \mathbb{Z} \mid m = nq + r \quad \forall m, n \in \mathbb{Z}$  per il teorema della divisione euclidea con il resto, dunque  $\exists q \mid m = nq + r \implies nq = m - r \implies n \mid m - r \implies \exists q \mid m \equiv r \pmod{n} \implies [x] \in [\mathbb{Z}]_n, [x] \neq \emptyset \quad \forall n \in \mathbb{Z}$

## Teorema di Lagrange (teoria dei gruppi)

- $xH = \{xh \mid h \in H\}$  dove  $H \subset G$  e  $x \in G$ , è detta **classe laterale sinistra** di  $H$  in  $G$ 
  - quando  $G$  è finito,  $|xH| = |H|$  perché per ogni elemento  $x$  che genera  $xH$ ,  $xH$  è l'insieme dei prodotti di  $x$  con ogni elemento di  $H$

- $H \rightarrow xH$  è biunivoca  $\forall x \in G$
- $G/H = \{xH \mid x \in G\}$  è l'insieme delle classi laterali sinistre, e poiché sono disgiunte a due a due, e la loro unione equivale a  $G$ , allora ogni  $xH$  è una **partizione** di  $G$
- $|G| = |H| \cdot |G : H|$  è il **teorema di Lagrange**
  - $|G|$  è la cardinalità di  $G$
  - $|H|$  è la cardinalità di  $H$ , che equivale a  $|xH| \forall x \in G$
  - $|G : H|$  è la cardinalità di  $|G/H|$ , ovvero il numero di classi laterali sinistre

## Ideali

- $(A, +, *)$  anello commutativo
- $I \subset A$  **ideale**  $\iff$ 
  - $(I, +) \subset (A, +)$  è un **sottogruppo**
  - $\forall x \in I, a \in A \implies ax \in I \implies A \cdot I \subset I$
- nel caso in cui  $(A, +, *)$  non sia commutativo, basta aggiungere che  $I \cdot A \subset I$
- $I \subset \mathbb{Z}$  ideale  $\implies \exists! d \geq 0 \mid I = I(d) := \{xd \mid x \in \mathbb{Z}\}$ , dove  $I(d)$  è un ideale, detto **ideale principale generato da  $d$** 
  - *esistenza*
    - $d := \min(I \cap \mathbb{Z}_{>0})$ 
      - se  $I = \{0\} \implies I = I(0)$ , altrimenti  $I \cap \mathbb{Z}_{>0} \neq \emptyset$ 
        - $\forall x \in I \mid x < 0 \implies (-x) > 0$ , e  $(-x) \in I$  per definizione di  $I$ , quindi anche se ho un numero negativo, posso considerare il suo opposto per la dimostrazione
    - $I(d) = I \implies I(d) \subset I \wedge I \subset I(d)$ 
      - $I(d) \subset I$ 
        - $\forall x \in I(d), \exists y \in \mathbb{Z} \mid x = dy$  per definizione
        - $d \in I$  per definizione, quindi  $dy \in I \implies x \in I \implies I(d) \subset I$  in quanto  $I \subset \mathbb{Z}$  ideale, e dunque  $I \cdot \mathbb{Z} \subset I$  (poiché  $\mathbb{Z}$  è anello commutativo)
      - $I \subset I(d)$ 
        - $\forall x \in I, \exists! q, r \in \mathbb{Z} \mid x = dq + r, \quad 0 \leq r < d$ , per il teorema della divisione euclidea con il resto, e  $d \neq 0$  per ipotesi
          - $r = 0 \implies x = dq \implies x \in I(d)$  per definizione, dunque  $I \subset I(d)$
          - se, per assurdo,  $r \neq 0$ 
            - $x \in I$  per ipotesi,  $dq \in I(d) \implies dq \in I$  per dimostrazione precedente, quindi  $x = dq + r \implies r = x - dq \in I$ , ma poiché  $r \neq 0$  per ipotesi, allora  $r \in I \cap \mathbb{Z}_{>0}$
            - per definizione,  $0 \leq r < d$ , ma  $d := \min(I \cap \mathbb{Z}_{>0})$ , quindi il minimo numero che  $d$  può assumere è 1, e poiché  $r < d \implies r = 0$  necessariamente
    - *unicità*
      - $I(d) = I(-d)$ , quindi l'unicità deriva dal fatto che  $d := \min(I \cap \mathbb{Z}_{>0})$ , e dunque nella dimostrazione è preso  $d$  positivo, ma vale il ragionamento analogo per  $d < 0$  considerando  $I(-d)$ 
        - $I(a) = I(b) \iff a = \pm b \quad \forall a, b \in \mathbb{Z} \mid a \neq b$ 
          - $a = \pm b \implies I(a) = I(b)$ 
            - $a = b \implies I(a)$  e  $I(b)$  coincidono
            - $a = -b$  allora  $I(-b) = \{k(-b) \mid k \in \mathbb{Z}\} = \{(-k)b \mid (-k) \in \mathbb{Z}\} = I(b)$ , e  $k, -k \in \mathbb{Z} \quad \forall k \in \mathbb{Z}$
        - $I(a) = I(b) \implies a = \pm b$ 
          - $I(a) = I(b) \implies a \in I(b)$  e  $b \in I(a) \implies \exists p, q \in \mathbb{Z} \mid a = pb \wedge b = qa$ , di conseguenza
            - $b = q(pb) \implies b = (qp)b \implies pq = 1 \implies p = q = 1 \vee p = q = -1 \implies a = \pm b$
    - $I(d)$  ideale
      - $\triangle$  **MANCA DIMOSTRAZIONE**
      - più in generale,  $I(a_1, \dots, a_n) = \{a_1b_1 + \dots + a_nb_n \mid b_1, \dots, b_n \in A\}$  è l'**ideale di  $A$  generato dagli  $a_1, \dots, a_n \in A$** 
        - $I$  induce una relazione di equivalenza su  $A$  detta **congruenza modulo  $I$** 
          - $a \equiv b \pmod{I} \iff b - a \in I$

## Massimo comun divisore

- $\forall a_1, \dots, a_n \in \mathbb{Z}, \quad \exists! d \geq 0 : I(a_1, \dots, a_n) = I(d), \quad d := \text{MCD}(a_1, \dots, a_n)$ 
  - $\triangle$  **MANCA DIMOSTRAZIONE**
    - $\forall x \in I(a_1, \dots, a_n), d \mid x$ , dunque  $d$  è *divisore comune*
    - $d$  è il *massimo tra i divisori comuni*
  - **identità di Bézout**
    - $\exists x, y \in \mathbb{Z} \mid ax + by = d \quad \forall a, b \in \mathbb{Z}$

## Operazioni sugli ideali

- su  $I, J \subset A$  ideali in  $A$  anello commutativo, è possibile definire  $I + J$ ,  $I \cap J$  e  $I \cdot J$ 
  - $I + J = \{i + j \mid i \in I, j \in J\}$ 
    - $I + J$  **sottogruppo**
      - $0 \in I, 0 \in J, 0 + 0 = 0 \implies 0 \in I + J$  per definizione
      - la chiusura rispetto a  $+$ , implica che  $\forall i_1, i_2 \in I, j_1, j_2 \in J \quad (i_1 + j_1) + (i_2 + j_2) \in I + J$ , e poiché  $(i_1 + j_1) + (i_2 + j_2) = (i_1 + i_2) + (j_1 + j_2)$ , e  $i_1 + i_2 \in I, j_1 + j_2 \in J$ , allora per definizione di  $I + J$ ,  $(i_1 + i_2) + (j_1 + j_2) \in I + J$
      - $\forall i \in I, j \in J \quad i + j \in I + J$ , l'opposto rispetto a  $+$  di  $i + j$  è  $-(i + j) = (-i) + (-j)$ , e  $-i \in I, -j \in J \quad \forall i \in I, j \in J \implies (-i) + (-j) \in I + J$  per definizione
    - $A \cdot I \subset I \implies \forall a \in A, i \in I, j \in J \quad a(i + j) \in I + J$ 
      - $i + j \in I + J$  per definizione, e  $a(i + j) = ai + aj$ , e  $ai \in I, aj \in J$  per definizione, quindi  $ai + aj \in I + J$  per definizione
  - $I \cap J = \{x \in I \wedge x \in J\}$ 
    - $\triangle$  MANCA DIMOSTRAZIONE
  - $I \cdot J = \{i_1 j_1 + \dots + i_k j_k \mid k \geq 1, i_1, \dots, i_k \in I, j_1, \dots, j_k \in J\}$ 
    - $\triangle$  MANCA DIMOSTRAZIONE
- $\mathbb{Z}$  è un anello ad ideali principali
  - $\forall a, b \in \mathbb{Z} \quad I(a) + I(b) = I(d), \quad d := \text{MCD}(a, b)$ 
    - $I(a) + I(b) = \{i + j \mid i \in I(a), j \in I(b)\}$ , ma  $i \in I(a) \implies \exists x \in \mathbb{Z} \mid i = ax$  e  $j \in I(b) \implies \exists y \in \mathbb{Z} \mid j = by$ , quindi  $i + j = ax + by \implies I(a) + I(b) = \{ax + by \mid x, y \in \mathbb{Z}\} = I(a, b)$  per definizione, e per l'identità di Bézout,  $\exists x, y \in \mathbb{Z} \mid ax + by = d := \text{MCD}(a, b)$ , e per teoremi precedenti,  $I(a, b) = I(d)$
  - $\forall a, b \in \mathbb{Z} \quad I(a) \cdot I(b) = I(a \cdot b)$ 
    - $x \in I(a) \cdot I(b) \implies x \in I(a \cdot b)$ 
      - $x \in I(a) \cdot I(b) \implies x = i_1 j_1 + \dots + i_k j_k$  con  $i_1, \dots, i_k \in I(a), j_1, \dots, j_k \in I(b)$ , ma per definizione,  $i \in I(a) \implies \exists x \in \mathbb{Z} \mid i = ax$ , e dunque  $i_1, \dots, i_k = ax_1, \dots, ax_k$  con  $x_1, \dots, x_k \in \mathbb{Z}$ , e analogamente  $j_1, \dots, j_k = by_1, \dots, by_k$  con  $y_1, \dots, y_k \in \mathbb{Z}$
      - segue che  $x = (ax_1)(by_1) + \dots + (ax_k)(by_k) = ab \cdot (x_1 y_1 + \dots + x_k y_k)$ , e poiché  $(x_1 y_1 + \dots + x_k y_k) \in \mathbb{Z}$ , per definizione segue che  $x \in I(a \cdot b)$
    - $x \in I(a \cdot b) \implies x \in I(a) \cdot I(b)$ 
      - $x \in I(a \cdot b) \implies \exists k \in \mathbb{Z} \mid x = ab \cdot k$ , ma  $x = abk \implies \begin{cases} x = a \cdot bk \implies \exists bk \in \mathbb{Z} \mid x = a \cdot bk \implies x \in I(a) \\ x = b \cdot ak \implies \exists ak \in \mathbb{Z} \mid x = b \cdot ak \implies x \in I(b) \end{cases}$  **INCOMPLETA**

## Minimo comune multiplo

- $\forall a_1, \dots, a_n \in \mathbb{Z} \quad \exists! m \in \mathbb{N} \mid m := \text{mcm}(a_1, \dots, a_n) : I(m) = I(a_1) \cap \dots \cap I(a_n) = \bigcap_{i=1}^n I(a_i)$

## Invertibili e divisori dello 0

- $(A, +, \cdot)$  anello commutativo
  - $a \in A$  è detto **invertibile**  $\iff \exists a^{-1} \in A \mid a \cdot a^{-1} = e$ 
    - $A^* := \{a \in A \mid a \text{ invertibile}\} \subset A$
    - $(A^*, \cdot)$  è un **sottogruppo** di  $(A, \cdot)$ 
      - $1^{-1} = 1 \implies 1$  invertibile  $\implies 1 \in A^*$  per definizione di  $A^* \implies \exists e \in A^*$
      - $\forall x, y \in A^* \quad x \cdot y \in A^*$
      - $\forall x \in A^* \quad \exists x^{-1}$  per definizione di  $A^*$ , ma poiché  $x^{-1}$  è inverso di  $x$ , allora  $x^{-1} \in A^*$  per definizione
    - $(A^*, \cdot)$  è un **gruppo**
      - $(xy)z = x(yz)$
      - $\exists e$  ed  $e \in A^*$
      - $\forall x \in A^* \quad \exists x^{-1}$  per definizione
  - $a \in A$  è detto **divisore dello 0**  $\iff \exists b \in A, b \neq 0 \mid a \cdot b = 0$ 
    - $A$  è detto **dominio di integrità**  $\iff \nexists x \mid x$  divisore dello 0 oltre a  $x = 0$
    - $A$  è dominio di integrità  $\iff$  in  $A$  vale la legge di annullamento del prodotto
      - un divisore dello 0 non è invertibile

## Insiemi quoziente $\mathbb{Z}_n$

- $\mathbb{Z}_n$  dominio  $\iff n$  primo
- $\triangle$  MANCA DIMOSTRAZIONE
- $\forall [x] \in \mathbb{Z}_n, \text{MCD}(x, n) = 1 \iff [x] \in \mathbb{Z}_n^*$
- $\triangle$  MANCA DIMOSTRAZIONE
  - $p$  primo  $\implies \mathbb{Z}_p^* = \{[x] \in \mathbb{Z}_p \mid 0 < x < p\} = \mathbb{Z}_p - \{0\}$ 
    - $p$  primo  $\implies$  ogni numero è coprimo con  $p$
    - $\exists x \mid [0]$  invertibile
    - $[p] \notin \mathbb{Z}_p$  per definizione di  $\mathbb{Z}_p$
    - $p$  primo  $\implies \mathbb{Z}_p$  campo

## Teorema fondamentale dell'aritmetica

- $\forall a, b \in \mathbb{N} \quad \text{mcm}(a, b) \cdot \text{MCD}(a, b) = a \cdot b$ 
  - $a = 0 \vee b = 0 \vee a, b = 0 \implies \text{mcm}(a, b) = 0$  INCOMPLETA
  - $a, b > 0$ 
    - $\mathbb{P} = \{p \in \mathbb{N} \mid p \text{ primo}\}$
    - $\forall n \in \mathbb{N} - \{0\} \quad \exists! n_2, n_3, n_5, \dots, n_p \in \mathbb{N} \mid p \in \mathbb{P} : n = 2^{n_2} \cdot 3^{n_3} \cdot \dots \cdot p^{n_p}$ 
      - $p \nmid n \implies n_p = 0 \implies p^{n_p} = 1$ , dunque non influisce nella produttoria
    - $n = \prod_{p \in \mathbb{P}} p^{n_p}$ , quindi possiamo riscrivere anche  $a$  e  $b$  tramite i loro fattori primi
      - $a = \prod_{p \in \mathbb{P}} p^{a_p}$  e  $b = \prod_{p \in \mathbb{P}} p^{b_p}$
    - $d := \text{MCD}(a, b)$  e  $m := \text{mcm}(a, b)$ 
      - per definizione di  $d$  ed  $m$ , e attraverso le regole che permettono di trovarli tramite le fattorizzazioni di  $a$  e  $b$ , è possibile riscrivere  $d$  ed  $m$  come  $d = \prod_{p \in \mathbb{P}} p^{\min(a_p, b_p)}$  e  $m = \prod_{p \in \mathbb{P}} p^{\max(a_p, b_p)}$
      - $d \cdot m = \prod_{p \in \mathbb{P}} p^{\min(a_p, b_p)} \cdot \prod_{p \in \mathbb{P}} p^{\max(a_p, b_p)} = \prod_{p \in \mathbb{P}} p^{\min(a_p, b_p) + \max(a_p, b_p)}$
    - $\forall a, b \in \mathbb{N} \quad a + b = \min(a, b) + \max(a, b)$ 
      - $a = \min(a, b) \implies \max(a, b) = b$ , e viceversa
    - $d \cdot m = \prod_{p \in \mathbb{P}} p^{a_p + b_p} = \prod_{p \in \mathbb{P}} p^{a_p} \cdot \prod_{p \in \mathbb{P}} p^{b_p} = a \cdot b$

## Teorema cinese dei resti

### Lemma 1

### Lemma 2

### Teorema

- $\forall a_1, \dots, a_n \geq 2 \in \mathbb{Z} \mid \text{MCD}(a_i, a_j) = 1 \quad \forall i, j \in [1, n] \mid i \neq j$
- presi  $b_1, \dots, b_n \in \mathbb{Z} \mid 0 \leq b_1 < a_1, 0 \leq b_2 < a_2, \dots, 0 \leq b_n < a_n$
- $m := \text{mcm}(a_1, \dots, a_n) = a_1 \cdot \dots \cdot a_n$
- allora  $\exists! x \pmod{m} \begin{cases} x \equiv b_1 \pmod{a_1} \\ \vdots \\ x \equiv b_n \pmod{a_n} \end{cases}$ 
  - per il lemma 1  $m = a_1 \cdot \dots \cdot a_n$  poiché coprimi in ipotesi
  - per il lemma 2  $m = \text{mcm}(a_1, \dots, a_n) \implies \exists \phi : \mathbb{Z}_m \rightarrow \mathbb{Z}_{a_1} \times \dots \times \mathbb{Z}_{a_n}$  ben definita e iniettiva
  - $|X_1 \times \dots \times X_n| = |X_1| \cdot \dots \cdot |X_n| \implies |\mathbb{Z}_{a_1} \times \dots \times \mathbb{Z}_{a_n}| = |\mathbb{Z}_{a_1}| \cdot \dots \cdot |\mathbb{Z}_{a_n}|$ 
    - $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\} \implies |\mathbb{Z}_n| = n$ , quindi  $|\mathbb{Z}_{a_1}| \cdot \dots \cdot |\mathbb{Z}_{a_n}| = a_1 \cdot \dots \cdot a_n = m = |\mathbb{Z}_m|$  per ragionamento analogo
  - $|X| = |Y| < \infty \implies f : X \rightarrow Y$  iniettiva  $\iff f$  suriettiva
    - applicando questa osservazione,  $\phi$  iniettiva  $\implies \phi$  suriettiva, in quanto, per l'osservazione precedente, insieme di partenza e di arrivo di  $\phi$  hanno la stessa cardinalità  $|\mathbb{Z}_m|$
  - $\phi$  suriettiva  $\implies \exists x \mid x \pmod{m}$  è soluzione del sistema
    - $\varphi(x \pmod{m}) = (b_1 \pmod{a_1}, \dots, b_n \pmod{a_n})$ , e poiché  $\phi$  è suriettiva, allora ogni tupla di  $n$  elementi dell'insieme di arrivo, che descrive un sistema come in ipotesi, ha una controimmagine  $x \pmod{m}$ , e  $x \pmod{m} \in \mathbb{Z}_m$  per definizione, dunque **esiste sempre una soluzione**
  - $\phi$  iniettiva  $\implies \exists! x \mid x \pmod{m}$  è soluzione del sistema

- poiché  $\phi$  è iniettiva,  $x \pmod{m} \in \mathbb{Z}_m$  è unica, dunque la soluzione è sempre unica

## Criteri di divisibilità

## 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  $\forall n, P_n$  vera

## Fibonacci

- $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2} \quad \forall n \geq 2$ 
  - $x^2 - x - 1 = 0$  ha come soluzioni
    - $\phi := \frac{1 + \sqrt{5}}{2}$
    - $\psi := \frac{1 - \sqrt{5}}{2}$
  - $F_n = \frac{\phi^n - \psi^n}{\phi - \psi} = \frac{\phi^n - \psi^n}{\sqrt{5}}$
  - $n = 0 \implies F_0 = \frac{\phi^0 - \psi^0}{\sqrt{5}} = \frac{1 - 1}{\sqrt{5}} = 0$
  - $n = 1 \implies F_1 = \frac{\phi^1 - \psi^1}{\phi - \psi} = 1$
  - per il passo induttivo, invece di trovare il caso  $n$  nel caso  $n + 1$ , si trova il caso  $n - 1$  nel caso  $n$ 
    - $F_n = F_{n-1} + F_{n-2}$  per ipotesi induttiva, quindi
 
$$F_n = \frac{\phi^{n-1} - \psi^{n-1}}{\sqrt{5}} + \frac{\phi^{n-2} - \psi^{n-2}}{\sqrt{5}} = \frac{\phi^{n-1} - \psi^{n-1} + \phi^{n-2} - \psi^{n-2}}{\sqrt{5}}, \text{ e riordinando i termini}$$

$$\frac{(\phi^{n-1} + \phi^{n-2}) - (\psi^{n-1} - \psi^{n-2})}{\sqrt{5}} = \frac{\phi^{n-2}(\phi + 1) - \psi^{n-2}(\psi + 1)}{\sqrt{5}}$$
      - $\left. \begin{matrix} \varphi^2 = \varphi + 1 \\ \psi^2 = \psi + 1 \end{matrix} \right\} \implies \frac{\varphi^{n-2} \cdot \varphi^2 - \psi^{n-2} \cdot \psi^2}{\sqrt{5}} = \frac{\phi^n - \psi^n}{\sqrt{5}}$

## Coefficienti binomiali

- $\binom{n}{k} := \begin{cases} \frac{n!}{k!(n-k)!} & k \leq n \\ 0 & k > n \end{cases}$ 
  - $0! := 1$
- $\binom{n}{k} = \binom{n}{n-k}$ 
  - $\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$
- $\binom{n}{k} = \binom{n-1}{k+1} + \binom{n-1}{k}$ 
  - $\binom{n-1}{k+1} + \binom{n-1}{k} = \frac{(n-1)!}{(k+1)!(n-1-(k+1))!} + \frac{(n-1)!}{k!(n-1-k)!} = \frac{(n-1)!}{(k+1)k!(n-2-k)!} + \frac{(n-1)!}{k!(n-1-k)!} = \frac{(n-1-k)(n-1)! + (k+1)(n-1)!}{(k+1)!(n-k-1)!} = \frac{(n-1)!(n-1-k+k+1)}{(k+1)!(n-1-k)!} = \frac{(n-1)! \cdot n}{(n+1)!(n-1-k)!} = \frac{n!}{(k+1)!(n-k-1)!} = \binom{n}{k+1}$

## Teorema del binomio di newton

- $\forall a, b \in A$  anello commutativo,  $\forall n \in \mathbb{N} \quad (a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$ 
  - $n = 0 \implies (a+b)^0 = \sum_{k=0}^0 \binom{0}{k} a^k b^{0-k} = \binom{0}{0} a^0 b^0 = 1$
  - $(a+b)^{n+1} = (a+b)^n \cdot (a+b)$

