PRELIMINARI AL CORSO DI GEOMETRIA ANALITICA

MARIA GRAZIA MARINARI

Date: 15.3.2007.

1. Introduzione

Questi appunti contengono alcune nozioni di teoria degli insiemi e di algebra, utili per seguire il corso di Geometria Analitica.

2. Notazioni

Useremo (prevalentemente) le lettere maiuscole per indicare gli *insiemi* e le lettere minuscole per indicarne gli *elementi*, esprimeremo inoltre *relazioni* fra insiemi ed elementi mediante simboli[1].

Useremo liberamente anche le sigle: e.g, i.e., n.b.[2].

- $a \in A$ si legge *a appartiene ad A* e significa che l'oggetto a è elemento dell'insieme A;
- $a \notin A$ significa che $a \in A$ è falsa;
- $B \subseteq A$ si legge *B contenuto o uguale* ad A e significa che l'insieme B è *sottinsieme* dell'insieme A, ossia che vale $x \in A$ ogniqualvolta $x \in B$ (in simboli si scrive anche $x \in B \Longrightarrow x \in A$ e si legge *x appartenente a B implica x appartenente ad A*);
- $B \not\subseteq A$ significa che B non è sottinsieme di A[3];
- $B \subseteq A$ e $A \subseteq B \Longrightarrow A = B$;
- $B \subset A$ significa B contenuto in A e $A \neq B$ (ossia B è *sottinsieme proprio* di A);
- se tra due insiemi vale una fra $B \subseteq A$ o $A \subseteq B$ si dice che A e B sono *confrontabili*[4];
- $\emptyset$ denota l'insiem *vuoto*, quello cioè per cui $x \in \emptyset$ è falsa qualunque sia x;
- $\emptyset \subseteq A$ per ogni insieme A.

Osservazione **2.1.**
(1) I simboli introdotti possono essere letti anche da destra a sinistra: e.g. $A \ni a, A \supseteq B, A \not\supset B$;
(2) Per individuare un insieme se ne possono elencare esplicitamente (tra due parentesi graffe) tutti gli elementi[5] o, specialmente se questi sono 'tanti', si possono descrivere le proprietà distintive dei medesimi, e.g. se A denota l'insieme delle province della Liguria si possono usare le due scritture:
$A = \{Genova, Savona, Imperia, La\,Spezia\}$
$A = \{a :^{6} a \quad \text{è una provincia ligure}\}$

Esempio **2.2.**
(1) Siano A l'insieme di tutti gli esseri umani di sesso maschile viventi e a_1 =Ronaldo, a_2 =Roma, a_3 =Dante, a_4 =Mina, $a_i \in A$ è vera solo per $i = 1$.
(2) Siano A l'insieme delle province italiane e B l'insieme delle città capoluogo di regione (italiana), vale $B \subset A$.
(3) Siano A l'insieme delle province italiane e B l'insieme delle capitali europee, valgono $B \not\subseteq A$ e $A \not\subseteq B$.

---

[1] In particolare i quantificatori universali $\forall$ (per ogni) ed $\exists$ (esiste)

[2] Sono tutte abbreviazioni di frasi latine: exempli gratia (per esempio), idem est (cioè), nota bene.

[3] In generale, barrando un simbolo matematico se ne afferma la negazione (e.g. $\neq, \notin, \not<, \not\subset$ ecc.)

[4] n.b. in generale due insiemi A, B non sono confrontabili.

[5] n.b. a e $\{a\}$ sono due enti diversi!

[6] Il simbolo : si legge *tale che* e si usano allo stesso scopo anche il simbolo | o l'abbreviazione t.c..

I principali insiemi numerici[7]

- $\mathbb{N} := \{0, 1, 2, \ldots, n, \ldots\}$ insieme dei numeri *naturali*,
- $\mathbb{N}^* := \{1, 2, \ldots, n, \ldots\}$ insieme dei numeri *naturali* nonnulli,
- $\forall n \in \mathbf{N}$,
  $\underline{n} := \{0, 1, 2, ..., n-2, n-1\}$ *segmento* dei primi n numeri naturali[8],
  $\forall n \in \mathbf{N}^*$,
  $\underline{n}^* := \{1, 2, ..., n-1, n\}$ *segmento* dei primi n numeri naturali nonnulli,
- $\mathbb{Z} := \{0, \pm 1, \pm 2, \ldots, \pm n, \ldots\}$ insieme dei numeri *interi*,
- $\mathbb{Q} := \{[\frac{p}{q}]^9 : p, q \in \mathbb{Z}, q \neq 0\}$ insieme dei numeri *razionali*,
- $\mathbb{R} := \{x : x$ separa due classi contigue di numeri razionali$\}$, insieme dei numeri *reali*,
- $\mathbb{C} := \{a+ib : a, b \in \mathbb{R}, i^2 = -1\}$ insieme dei numeri *complessi*,
- $\forall a, b \in \mathbb{R} : a < b$,
  - $[a, b] := \{x \in \mathbb{R} : a \leq x \leq b\}$ *segmento* o *intervallo chiuso di estremi* a *e* b,
  - $[a, b) := \{x \in \mathbb{R} : a \leq x < b\}$ *segmento* o *intervallo chiuso a sinistra di estremi* a *e* b,
  - $(a, b] := \{x \in \mathbb{R} : a < x \leq b\}$ *segmento* o *intervallo chiuso a destra di estremi* a *e* b,
  - $(a, b) := \{x \in \mathbb{R} : a < x < b\}$ *segmento* o *intervallo aperto di estremi* a *e* b,
- $\forall a \in \mathbb{R}$,
  - $(-\infty, a] := \{x \in \mathbb{R} : x \leq a\}$ *semiretta chiusa di estremo destro* a,
  - $[a, +\infty) := \{x \in \mathbb{R} : a \leq x\}$ *semiretta chiusa di estremo sinistro* a,
  - $(-\infty, a) := \{x \in \mathbb{R} : a < x\}$ *semiretta aperta di estremo destro* a,
  - $(a, +\infty) := \{x \in \mathbb{R} : x < a\}$ *semiretta aperta di estremo sinistro* a.

3. Operazioni sugli insiemi

Definizione **3.1.** Se A, B sono due insiemi,

$$A \cap B := \{x : x \in A, x \in B\}$$

è l'insieme degli elementi che appartengono sia ad A che a B ed è detto *intersezione di* A *e* B, in particolare se vale $A \cap B = \emptyset$ i due insiemi sono detti *disgiunti*,

$$A \cup B := \{x : x \in A \,\text{o}\, x \in B\}$$

è l'insieme degli elementi che appartengono ad almeno uno fra A e B ed è detto *unione di* A *e* B.

Valgono le relazioni:

---

[7]Che noi introduciamo in modo del tutto naïf, ossia supponendoli noti insieme alla loro proprietà (che invece saranno studiate in altri corsi).

[8]$\underline{0} = \emptyset$.

[9]n.b. il simbolo $[\frac{p}{q}], p, q \in \mathbb{Z}, q \neq 0$ indica la totalità delle frazioni $\frac{np}{nq}$ al variare di $n \in \mathbb{Z}, n \neq 0$ i.e. scrivendo $[\frac{p}{q}]$ possiamo tacitamente supporre che M.C.D.$(p, q) = 1$.

- $A \cap B \subseteq A, A \cap B \subseteq B$,
- $A \subseteq A \cup B, B \subseteq A \cup B, A \cap B \subseteq A \cup B$.

ESEMPIO **3.2.** (1) Siano A l'insieme di tutti gli stati europei e B l'insieme degli stati che si affacciano sul Mediterraneo. È immediato verificare che $A \cap B = \{Spagna, Francia, P.di\, Monaco, Italia, Slovenia, Craozia, Bosnia-Erzegovina, Montenegro - Serbia, Albania, Grecia\}$.
L'elenco degli stati in $A \cup B$ è alquanto piú lungo e lasciato per esercizio.

(2) Siano A l'insieme delle province italiane e B l'insieme delle città capoluogo di regione (italiana), vale $B \subset A$.

(3) Siano A l'insieme dei comuni della Liguria, A_1 quello dei comuni della provincia di Genova, A_2 quello dei comuni della provincia di Savona, A_3 quello dei comuni della provincia di Imperia, A_4 quello dei comuni della provincia della Spezia. Si ha $A_j \subseteq A, \forall\, j \in \underline{4}^*$ e $A_i \cap A_j = \emptyset, \forall i \neq j \in \underline{4}^*$.

OSSERVAZIONE **3.3.** (1) Dati tre insiemi A, B, C,

- $A \cap (B \cap C) = (A \cap B) \cap C$ *associatività* dell'intersezione
- $A \cup (B \cup C) = (A \cup B) \cup C$ *associatività* dell'unione
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *distributività* dell'intersezione rispetto all'unione
- $A \cup (B \cap C) = (A \cup B) \cap (A \cap C)$ *distributività* dell'unione rispetto all'intersezione.
  Proviamo e.g. la prima $A \cap (B \cap C) = \{x : x \in A, x \in B \cap C\} = \{x : x \in A, x \in B, x \in C\} = \{x : x \in A \cap B, x \in C\} = (A \cap B) \cap C$.
- L'associatività permette di scrivere semplicemente $A \cap B \cap C$ e $A \cup B \cup C$.

(2) Lo stesso vale per una collezione finita di insiemi $A_1, \ldots, A_n$.

(3) Data una famiglia qualsiasi $\mathcal{F}$ di insiemi, $\bigcap_{A \in \mathcal{F}} A$ denota l'intersezione di tutti gli insiemi della famiglia, ossia l'insieme degli elementi comuni a tutti gli insiemi della famiglia. Se $\mathcal{F} = \{A_i : i \in I\}$ si scrive anche $\bigcap_{i \in I} A_i$, analogamente $\bigcup_{A \in \mathcal{F}} A$ o $\bigcup_{i \in I} A_i$, denota l'unione di tutti gli elementi della famiglia.

ESEMPIO **3.4.** Dato $n \in \mathbb{N}$, sia $A_n := [-n, n] \subseteq \mathbb{R}$ e sia $\mathcal{F} = \{A_n : n \in \mathbb{N}\}$
$\bigcap_{A \in \mathcal{F}} A = \bigcap_{n \in \mathbb{N}} A_n = \{0\}$ e $\bigcup_{A \in \mathcal{F}} A = \bigcup_{n \in \mathbb{N}} A_n = \mathbb{R}$.
Determinare $\bigcap_{A \in \mathcal{F}'} A$ e $\bigcup_{A \in \mathcal{F}'} A$ con $\mathcal{F}' \subset \mathcal{F}$ famiglia finita.

DEFINIZIONE **3.5.** Dati due insiemi A, B l'insieme

$$A \setminus B := \{x : x \in A, x \notin B\}$$

consiste nella totalità degli elementi di A non appartenenti a B ed è chiamato *complementare di B in A*. In particolare, se $B \subseteq A$ il complementare $A \setminus B$ è denotato $\mathcal{C}_A(B)$.

OSSERVAZIONE **3.6.** Si ha:

- $B \cap \mathcal{C}_A(B) = \emptyset$,
- $B \cup \mathcal{C}_A(B) = A$,
- $\mathcal{C}_A(\mathcal{C}_A(B)) = B$,
- $\mathcal{C}_A(\emptyset) = A$ e $\mathcal{C}_A(A) = \emptyset$,

- se $B_1 \subseteq B_2 \subseteq A \Longrightarrow \mathcal{C}_A(B_2) \subseteq \mathcal{C}_A(B_1)$,
- se $B_1 \subseteq B_2 \subseteq A$ valgono le seguenti *formule di De Morgan:*
  (1) $\mathcal{C}_A(\mathbf{B}_1 \cup B_2) = \mathcal{C}_A(B_1) \cap \mathcal{C}_A(B_2)$,
  (2) $\mathcal{C}_A(B_1 \cap B_2) = \mathcal{C}_A(B_1) \cup \mathcal{C}_A(B_2)$.
  Proviamo per esempio (1) (in due modi diversi),
  $\mathcal{C}_A(\mathbf{B}_1 \cup B_2) = \{a \in A : a \notin B_1 \cup B_2\} = \{a \in A : a \notin B_1, a \notin B_2\} =$
  $= \{a \in A : a \notin B_1\} \cap \{a \in A : a \notin B\} = \mathcal{C}_A(B_1) \cap \mathcal{C}_A(B_2)$,
  poiché $\mathbf{B}_1 \subseteq \mathbf{B}_1 \cup B_2$ e $\mathbf{B}_2 \subseteq \mathbf{B}_1 \cup B_2$ si ha $\mathcal{C}_A(\mathbf{B}_1 \cup B_2) \subseteq \mathcal{C}_A(\mathbf{B}_1)$ e $\mathcal{C}_A(\mathbf{B}_1 \cup B_2) \subseteq \mathcal{C}_A(\mathbf{B}_2) \Longrightarrow \mathcal{C}_A(\mathbf{B}_1 \cup B_2) \subseteq \mathcal{C}_A(\mathbf{B}_1) \cap \mathcal{C}_A(\mathbf{B}_2)$, d'altra parte $a \in \mathcal{C}_A(\mathbf{B}_1 \cap B_2)$ significa $a \in A, a \notin B_1, a \notin B_2$ ossia $a \in A, a \notin B_1 \cup B_2$ cioè proprio $a \in \mathcal{C}_A(\mathbf{B}_1 \cup B_2)$.
- $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ e in modo simile si definiscono $\mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*$, notiamo che $\mathbb{N}^*$ si scrive anche $\mathbb{Z}_+^*$.

Definizione **3.7.** Per ogni insieme A, $\mathcal{P}(A)$ è la famiglia di tutti i sottinsiemi (o parti) di A ed è detta insieme *delle parti di A*.

Si ha:

- $\emptyset \in \mathcal{P}(A), A \in \mathcal{P}(A)$,
- le operazioni $\bigcap$ e $\mathcal{P}$ commutano nel finito, ossia data una collezione finita di insiemi $A_1, \ldots, A_n$, $\bigcap_{i=1}^{n} \mathcal{P}(A_i) = \mathcal{P}(\bigcap_{i=1}^{n} A_i)$, mentre le operazioni $\bigcup$ e $\mathcal{P}$ non commutano tra loro in quanto $\bigcup_{i=1}^{n} \mathcal{P}(A_i) \subseteq \mathcal{P}(\bigcup_{i=1}^{n} A_i)$,

Esempio **3.8.** Siano $A_1 = \{-1, 0\}, A_2 = \{0, 1\}, A = A_1 \cup A_2$, si ha

- $\mathcal{P}(A_1) = \{\emptyset, \{-1\}, \{0\}, A_1\}$,
- $\mathcal{P}(A_2) = \{\emptyset, \{0\}, \{1\}, A_2\}$,
- $\bigcup_{i=1}^{2} \mathcal{P}(A_i) = \{\emptyset, \{-1\}, \{0\}, \{1\}, A_1, A_2\}$
- $\mathcal{P}(A_1 \cup A_2) = \mathcal{P}(A) = \{\emptyset, \{-1\}, \{0\}, \{1\}, A_1, A_2, \{-1, 1\}, A\}$.

Definizione **3.9.** a) Dati A, B insiemi disgiunti

$$A \times B := \{(a, b) : a \in A, b \in B\}$$

è detto *prodotto cartesiano di A per B*,

b) se $A \cap B \neq \emptyset$ occorre pensare il primo elemento di una coppia $(-, -)$ come elemento di A e il secondo elemento della coppia come elemento di B (anche qualora si tratti dello stesso elemento di $A \cap B$).

Si ha:

- in generale $A \times B \neq B \times A$,
- se $A = \emptyset$ o $B = \emptyset$ allora $A \times B = \emptyset$,
- dati tre insiemi A, B, C si pone $A \times B \times C := (A \times B) \times C$[10],
- data una collezione finita di insiemi $A_1, \ldots, A_n$, si pone $A_1 \times A_2 \times \cdots \times A_n := (A_1 \times \cdots \times A_{n-1}) \times A_n$, un elemento di $A_1 \times A_2 \times \cdots \times A_n$ è denotato con un'n-pla ordinata di elementi di $A_i, i \in \underline{n}^*$ ossia $(a_1, \ldots, a_n), a_i \in A_i, i \in \underline{n}^*$.

[10]Per come è definita l'operazione $\times$ non è commutativa infatti $(A \times B) \times C \neq A \times (B \times C)$.

ESEMPIO **3.10.** (1) Siano $A = \{\text{esseri umani viventi}\}, B = \{\text{gruppi sanguigni}\}$, si ha:
$A \times B = \{(a,b) : a \text{ è un essere umano vivo, } b \text{ è un gruppo sanguigno}\}$
$B \times A = \{(b,a) : b \text{ un gruppo sanguigno, } a \text{ è un essere umano vivo}\}$.
(2) Dati tre insiemi A, B, C
- $A \times (B \cup C) = A \times B \cup A \times C$,
- $A \times (B \cap C) = A \times B \cap A \times C$,
- $A \times (B \setminus C) = A \times B \setminus A \times C$.

4. Corrispondenze e Applicazioni

DEFINIZIONE **4.1.** Dati due insiemi A, B:

(1) una *corrispondenza fra A e B* è un qualunque sottinsieme del prodotto cartesiano $D \subseteq A \times B$. Si dice che un elemento $a \in A$ e un elemento $b \in B$ *si corrispondono secondo* D se vale $(a,b) \in D$,
(2) un' *applicazione di A in B* è il dato $\{A, D\} = \varphi$ soddisfacente le condizioni:
- D corrispondenza fra A e B,
- $\forall a \in A \, \exists! \, b \in B : (a,b) \in D$.

Data l'applicazione $\{A, D\} = \varphi$ anziché $(a,b) \in D$ si scrive $b = \varphi(a)$ e si dice che $\varphi(a)$ *è l'immagine di a secondo* φ e anziché $\{A, D\} = \varphi$ si scrive semplicemente $\varphi : A \longrightarrow B$ (o anche $A \xrightarrow{\varphi} B$) inoltre, per indicare che un elemento $b \in B$ è l'immagine mediante φ di un elemento $a \in A$ si scrive anche $a \overset{\varphi}{\mapsto} b$. L'insieme A è detto *dominio* di φ mentre l'insiem B è detto *codominio* o *rango* di φ[11].
(3) Per ogni insieme A l'*applicazione identica di A in sé* è $\iota_A : A \longrightarrow A$ definita da $\iota_A(a) = a$, $\forall \, a \in A$ (ι_A è indicata anche Id_A o 1_A).
(4) Per ogni sottinsieme $B \subseteq A$ l'*inclusione* o *immersione* di B in A è l'applicazione $\iota : B \longrightarrow A$ definita da $\iota(b) = b$, $\forall \, b \in B$.
(5) Data un'applicazione $\varphi : A \longrightarrow B$, se $C \in \mathcal{P}(A)$, l'*immagine di C secondo* φ è l'insieme
$$\varphi(C) := \{\varphi(a) : a \in C\},$$
l'insieme $\varphi(A)$ è chiamato *immagine di* φ ed è indicato anche $im\,\varphi$; se $D \in \mathcal{P}(B)$, l'*immagine inversa di D secondo* φ è l'insieme
$$\varphi^{-1}(D) := \{\, a \in A : \varphi(a) \in D\},$$
vale $\varphi^{-1}(B) = A$ e se $b \in B$ scriveremo $\varphi^{-1}(b)$ invece di $\varphi^{-1}\{(b)\}$ (quando non vi sia pericolo di confusione).
(6) Per ogni $C \in \mathcal{P}(A)$, un'applicazione $\varphi : A \longrightarrow B$ induce l'applicazione $\varphi_{|C} : C \longrightarrow B$, definita da $\varphi_{|C}(x) := \varphi(x) \, \forall \, x \in C$ e detta *restrizione di* φ a C.

ESEMPIO **4.2.** (1) Se $A = \emptyset, \Longrightarrow \exists! \, \varphi : A \longrightarrow B$ qualunque sia B e vale $\varphi(A) = \emptyset$, ossia $\varphi = \iota$.
(2) Siano $A = [0, 300] \subseteq \mathbb{R}$, $B = \{y : y \text{ è un essere umano}\}$ e $A \times B \supseteq D = \{(x,y) : x \text{ centimetri è l'altezza di } y\}$, chiaramente D non è un'applicazione (e.g. ci sono moltissimi esseri umani alti un metro e ottanta!).

[11] n.b. può essere $\{A, D\} = \varphi$ applicazione mentre $\{B, D\} = \psi$ non applicazione.

(3) Sia $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$ definita da $\varphi(x) = x^2$, $\forall\, x \in \mathbb{R}$, se $C = [-1, 1] \subseteq \mathbb{R}$(dominio) e $D = (0, \frac{1}{4}) \subseteq \mathbb{R}$(codominio), si ha: $\varphi(\mathbb{R}) = \mathbb{R}_+$, $\varphi(C) = [0, 1] \subseteq \mathbb{R}$(codominio) e $\varphi^{-1}(D) = (-\frac{1}{2}, \frac{1}{2}) \subseteq \mathbb{R}$(dominio).

OSSERVAZIONE **4.3.** (1) Un'applicazione $\varphi : A \longrightarrow B$ induce un'applicazione (ancora indicata φ!) $\varphi : \mathcal{P}(A) \longrightarrow \mathcal{P}(B)$ definita da $C \mapsto \varphi(C), \forall\, C \in \mathcal{P}(A)$ e un'applicazione $\varphi^{-1} : \mathcal{P}(B) \longrightarrow \mathcal{P}(A)$ definita da $D \mapsto \varphi^{-1}(D), \forall\, D \in \mathcal{P}(B)$.

- L'applicazione $\varphi^{-1} : \mathcal{P}(B) \longrightarrow \mathcal{P}(A)$ mantiene le operazioni elementari e precisamente, data una collezione$\{D_i\}_{i\in I} \subseteq \mathcal{P}(B)$, si ha:
  - $\varphi^{-1}(\bigcup\limits_{i\in I} D_i) = \bigcup\limits_{i\in I} \varphi^{-1}(D_i)$,
  - $\varphi^{-1}(\bigcap\limits_{i\in I} D_i) = \bigcap\limits_{i\in I} \varphi^{-1}(D_i)$,
  - $\varphi^{-1}(D_i \setminus D_j) = \varphi^{-1}(D_i) \setminus \varphi^{-1}(D_j), \forall\, i, j \in I$.

  Valgono infatti:
  - $x \in \varphi^{-1}(\bigcup\limits_{i\in I} D_i) \iff \varphi(x) \bigcup\limits_{i\in I} D_i \iff \exists \bar{i} \in I : \varphi(x) \in D_{\bar{i}} \iff x \in \varphi^{-1}(D_{\bar{i}})$ per qualche $\bar{i} \in I \iff x \in \bigcup\limits_{i\in I} \varphi^{-1}(D_i)$[12] ,
  - $x \in \varphi^{-1}(\bigcap\limits_{i\in I} D_i) \iff \varphi(x) \in \bigcap\limits_{i\in I} D_i \iff \varphi(x) \in D_i, \forall\, i \in I \iff x \in \varphi^{-1}(D_i), \forall\, i \in I \iff x \in \bigcap\limits_{i\in I} \varphi^{-1}(D_i)$,
  - $x \in \varphi^{-1}(D_i \setminus D_j) \iff \varphi(x) \in D_i \setminus D_j \iff \varphi(x) \in D_i, \varphi(x) \notin D_j \iff \varphi(x) \in \varphi^{-1}(D_i) \setminus \varphi^{-1}(D_j)$.
- L'applicazione $\varphi : \mathcal{P}(A) \longrightarrow \mathcal{P}(B)$ non mantiene le operazioni elementari e precisamente, data una collezione$\{C_i\}_{i\in I} \subseteq \mathcal{P}(A)$, si ha:
  - $\varphi(\bigcup\limits_{i\in I} C_i) = \bigcup\limits_{i\in I} \varphi(C_i)$,
  - $\varphi(\bigcap\limits_{i\in I} C_i) \subseteq \bigcap\limits_{i\in I} \varphi(C_i)$,
  - $\varphi(C_i \setminus C_j) \supseteq \varphi(C_i) \setminus \varphi(C_j), \forall\, i, j \in I$.

(2) Immagine e immagine inversa sono correlate dalle formule:
  (a) $\varphi^{-1}\varphi((C)) \supseteq C, \forall\, C \in \mathcal{P}(A)$,
  (b) $\varphi(\varphi^{-1}(D)) \subseteq D, \forall\, D \in \mathcal{P}(B)$.

ESEMPIO **4.4.** Sia $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$ l'applicazione costante definita da $\varphi(x) = 10, \forall\, x \in \mathbb{R}$,

(1) siano $C_1 = [0, 1], C_2 = [2, 3], C_3 = [1, 2]$, si ha:
  - $\emptyset = \varphi(C_1 \cap C_2) \neq \varphi(C_1) \cap \varphi(C_2) = \{10\}$,
  - $\{10\} = \varphi([0, 1)) = \varphi(C_1 \setminus C_3) \neq \varphi(C_1) \setminus \varphi(C_3) = \emptyset$;

(2) siano $C = (0, \frac{1}{2}), D = (-\frac{1}{4}, \frac{1}{4})$, si ha:
  - $C \subset \varphi^{-1}(\varphi(C)) = \varphi^{-1}(\{10\}) = \mathbb{R}$,
  - $D \supset \varphi(\varphi^{-1}((D)) = \varphi(\emptyset) = \emptyset$.

DEFINIZIONE **4.5.** Dati tre insieme A, B, C e due applicazioni $A \xrightarrow{\varphi} B, B \xrightarrow{\psi} C$, si definisce in modo naturale una terza applicazione

$$A \xrightarrow{\omega} C \text{ mediante } \omega(a) := \psi(\varphi(a)),$$

detta *composizione* (o prodotto) *di φ e ψ* e denotata $\psi \circ \varphi$, φ è detta *componente interna di $\psi \circ \varphi$* mentre ψ ne è detta *componente esterna*.

[12] n.b. il simbolo $\iff$ si legge "se e solo se".

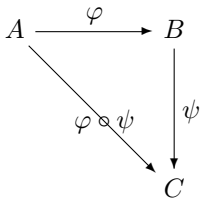
ESERCIZIO **4.6.** Date $\mathbb{N}\xrightarrow{\varphi}\mathbb{Z}\xrightarrow{\psi}\mathbb{Z}$, definite da

$$\varphi(n)=\begin{cases} n & \text{se } n=2h, h\in\mathbb{N} \\ -(n+1) & \text{se } n=2h+1, h\in\mathbb{N}\end{cases}, \quad \psi(m)=2m \quad \forall\, m\in\mathbb{Z},$$

Determinare $\psi\circ\varphi(\mathbb{N})$.

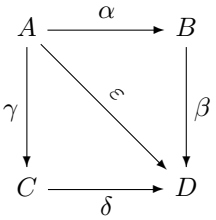
OSSERVAZIONE **4.7.** La composizione di due applicazioni $A\xrightarrow{\varphi}B, B\xrightarrow{\psi}C$, dà luogo a un *triangolo commutativo* (T).

(T)



In generale, un *diagramma* è un disegno fatto di lettere maiuscole (insiemi) e frecce (applicazioni), un diagramma si dice *commutativo* se, per ogni coppia di insiemi che compaiono nel diagramma, tutte le applicazioni dell'uno nell'altro che si ottengono come prodotti delle varie frecce coincidono.
(e.g. il seguente quadrato (Q)

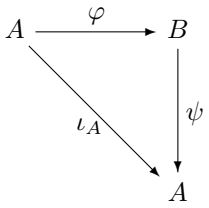
(Q)



è commutativo $\iff \beta\circ\alpha=\varepsilon=\delta\circ\gamma$, quali ulteriori condizioni implicherebbe la presenza di una $B\xrightarrow{\eta}C$)?

DEFINIZIONE **4.8.**
(1) L'applicazione $A\xrightarrow{\varphi}B$ è *surgettiva* (oppure *sopra, su, su tutto*) se $\varphi(A)=B$ o, equivalentemente, se $\forall\, b\in B \Longrightarrow \varphi^{-1}(\{b\})\neq\emptyset$,
(2) L'applicazione $A\xrightarrow{\varphi}B$ è *iniettiva* (oppure *uno-uno, biunivoca*) se $\varphi(a)=\varphi(a')\Longrightarrow a=a'$ o, equivalentemente, se $a\neq a'\Longrightarrow\varphi(a)\neq\varphi(a')$, o ancora, se $\forall\, b\in\varphi(A)$, $\exists!\, a\in\varphi^{-1}(\{b\})$,
(3) L'applicazione $A\xrightarrow{\varphi}B$ è *bigettiva* (oppure *biunivoca su tutto, corrispondenza biunivoca(=c.b.u) tra A e B*) se φ è sia iniettiva che surgettiva.

PROPOSIZIONE **4.9.** *Sia* $A\xrightarrow{\varphi}B$ *surgettiva,* $\exists\, B\xrightarrow{\psi}A$ *che rende commutativo il diagramma*



$\iff$ *φ è iniettiva.*

Dim. Sia φ iniettiva, $\forall\, b \in B$ si ponga $\psi(b) := a$ dove $a \in A$ è l'unico $a \in A : b = \varphi(a) \Longrightarrow (\psi\circ\varphi)(a) = \psi(\varphi(a)) = \psi(b) = a = \iota_A(a)$ (esistenza); se $B \xrightarrow{\psi'} A$ ha la stessa proprietà vale $\psi'(b) = \psi'(\varphi(a) = (\psi'\circ\varphi)(a) = a = \iota_A(a) = a = \psi(b)$ (unicità). Supponiamo viceversa che $\exists\,\psi$ che rende commutativo il diagramma, siano $a, a' \in A$ t.c. $\varphi(a) = \varphi(a') \Longrightarrow a = (\psi\circ\varphi)(a) = \psi(\varphi(a)) = \psi(\varphi(a')) = (\psi\circ\varphi)(a') = a'$, ossia φ è iniettiva.

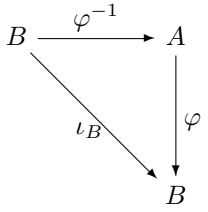
Esercizio **4.10.** Quali ipotesi su φ sono necessarie affinché le inclusioni di Oss.4.3 siano uguaglianze?

Definizione **4.11.** La ψ di Prop.4.9 dicesi *inversa* o *reciproca* di φ ed è indicata φ^{-1}[13].

Osservazione **4.12.**
(1) Se $A \xrightarrow{\varphi} B$ è iniettiva $\Longrightarrow \exists!\,\psi : \varphi(A) \longrightarrow B$ soddisfacente $\psi\circ\varphi = \iota_A$.
(2) Se $A \xrightarrow{\chi} B$ è surgettiva $\Longrightarrow \exists\,\omega : B \longrightarrow A : \chi\circ\omega = \iota_B$, (essendo $\chi^{-1}(\{b\}) \neq \emptyset, \forall\, b \in B$ c'è la possibilità di scegliere $\forall\, b \in B$ un $a \in A : \chi(a) = b \Longrightarrow$ ponendo $\omega(b) := a$ si ottiene un'applicazione con la proprietà voluta, in generale non unica!).

Esempio **4.13.**
(1) Sia $\mathbb{Z} \xrightarrow{\chi} \mathbb{N}$ definita da $\chi(n) = |n|$, le due applicazioni $\iota_+ : \mathbb{N} \longrightarrow \mathbb{Z}$ e $\iota_- : \mathbb{N} \longrightarrow \mathbb{Z}$ definite rispettivamente da $(\iota_+(n) = n)$ e $(\iota_-(n) = -n)$ soddisfano $\chi\circ\iota_+ = \iota_{\mathbb{N}} = \chi\circ\iota_+$.
(2) Date due applicazioni $A \xrightarrow{\varphi} A', B \xrightarrow{\psi} B'$ è definita anche una terza applicazione $\varphi\times\psi : A\times B \longrightarrow A'\times B'$ via $(a,b) \mapsto (\varphi(a), \psi(b))$ che è iniettiva, surgettiva, bigettiva $\iff$ tali sono sia φ che ψ.

Osservazione **4.14.**
(1) Sia $A \xrightarrow{\varphi} B$ tale che $\exists\,\varphi^{-1} \Longrightarrow$ si ha $\varphi\circ\varphi^{-1} = \iota_B$ e $(\varphi^{-1})^{-1} = \varphi$.



Infatti, $\forall\, b \in B$, sia $a \in A$ l'unico elemento tale che $b = \varphi(a)$, si ha $\varphi(\varphi^{-1}(b)) = \varphi(a)$, i.e. $(\varphi\circ\varphi^{-1})(b) = \iota_B(b) = b$, cioè φ rende commutativo il diagramma ossia proprio $(\varphi^{-1})^{-1} = \varphi$.
(2) Date $A \xrightarrow{\varphi} B \xrightarrow{\chi} C \xrightarrow{\psi} D$,
- considerando $\chi\circ\varphi$ e $\psi\circ\chi$, si costruiscono $\psi\circ(\chi\circ\varphi)$ e $(\psi\circ\chi)\circ\varphi$, poiché $\forall\, a \in A$ si ha $[(\psi\circ\chi)\circ\varphi](a) = (\psi\circ\chi)(\varphi(a)) = \psi(\chi(\varphi(a))) = \psi[(\chi\circ\varphi)(a)] = [\psi\circ(\chi\circ\varphi)](a)$, si scrive semplicemente $\psi\circ\chi\circ\varphi$;

[13] n.b. quando $\exists\, B \xrightarrow{\varphi^{-1}} A$ essa è altra cosa da $\mathcal{P}(B) \xrightarrow{\varphi^{-1}} \mathcal{P}(A)$ (in effetti i rispettivi domini sono insiemi diversi).

- se $\exists\,\varphi^{-1},\chi^{-1}\Longrightarrow\exists\,(\chi\circ\varphi)^{-1}$ (ossia la composizione di applicazioni bigettive è bigettiva) e vale $(\chi\circ\varphi)^{-1}=\varphi^{-1}\circ\chi^{-1}$, infatti, $\forall\,a\in A$ si ha $(\varphi^{-1}\circ\chi^{-1})\circ(\chi\circ\varphi)(a)=(\varphi^{-1}\circ(\chi^{-1}\circ\chi)\circ\varphi)(a)=(\varphi^{-1}\circ\iota_B\circ\varphi)(a)=(\varphi^{-1}\circ\varphi)(a)=\iota_A(a)=a$ e quindi per l'unicità dell'inversa $(\chi\circ\varphi)^{-1}=\varphi^{-1}\circ\chi^{-1}$.

(3) Piú in generale la composizione di applicazioni iniettive (rispettivamente surgettive) è iniettiva (risp. surgettiva), inoltre, se la composizione di due applicazioni è iniettiva (risp. surgettiva), allora la componente interna (risp. esterna) è iniettiva (risp. surgettiva).

5. Relazioni di equivalenza

Definizione **5.1.** Sia $D\subseteq A\times A$ una corrispondenza di A in se stesso, per indicare $(x,y)\in D$ scriveremo xDy e diremo che D è:

(1)
- *riflessiva* se vale xDx, $\forall\,x\in A$,
- *simmetrica* se vale yDx, ogniqualvolta xDy,
- *transitiva* se vale xDz, ogniqualvolta xDy, yDz,

equivalenza se D è riflessiva, simmetrica, transitiva.
Per indicare una relazione di equivalenza si usa il simbolo $\sim$[14].
Data una relazione di equivalenza $\sim$ su un insieme A, l'insieme di tutti gli elementi equivalenti a un $a\in A$ è detto *classe di equivalenza di a rispetto a* $\sim$ ed è denotata $[a]$ o anche $\overline{a}$;

(2)
- *semiordinamento* od *ordinamento parziale* se D è transitiva ma xDx, è falsa $\forall\,x\in A$, i semiordinamenti (anziché col generico D) sono indicati con simboli come $<,\prec,>,\succ$ e $x<y$ si legge x *precede* y o y *segue* x, se vale $x\prec y$ necessariamente $y\not\prec x$ perché altrimenti, per la proprietà transitiva, da $x\prec y, y\prec x\Longrightarrow x\prec x$.
  Espressioni del tipo $x\preceq y, x\leq y$ significano che vale una fra $x\prec y$ e $x=y$ (n.b. per taluni $\prec$ *semiordinamento* significa che $\prec$ è riflessiva, transitiva e antisimmetrica ossia $x\prec y, y\prec x\iff x=y$)..
- *ordinamento* od *ordinamento totale* se D è semiordinamento e vale almeno una (e quindi una sola) fra $xDy, x=y, yDx$, $\forall\,x,y\in A$, ossia, due qualsiasi elementi di A sono confrontabili rispetto a D.

Esempio **5.2.** (1) Sull'insieme U degli esseri umani da Adamo in poi classificare, $\forall\,x,y\in U$, le seguenti corrispondenze:
- $xD_1y\iff x$ e y si conoscono,
- $xD_2y\iff x$ e y abitano in paesi dello stesso continente,
- $xD_3y\iff x$ è piú basso di y, si
- $xD_4y\iff x$ è padre di y,
- $xD_5y\iff x$ e y hanno lo stesso padre,
- $xD_6y\iff x$ conosce la professione di y,
- $xD_7y\iff x$ non è nato prima di y.

(2) Data un'applicazione $\varphi:A\longrightarrow B$, ponendo $aDa'\iff\varphi(a)=\varphi(a')$ è definita una relazione di equivalenza su A, infatti la seconda condizione di Def. 4.1(2) garantisce che $\forall\,a\in A$ vale aDa, chiaramente se aDa', ossia $\varphi(a)=\varphi(a')$, vale anche $a'Da$ giacché $\varphi(a')=\varphi(a)$, se aDa', e $a'Da$",

[14] O anche $\approx,\simeq,\cong,\equiv$.

vale aDa" essendo $\varphi(a) = \varphi(a') = \varphi(a")$. Tale D è indicata $\sim_\varphi$ ed è detta *relazione di equivalenza indotta da* φ.

(3) Siano A l'insieme dei triangoli del piano e $T, T' \in A$, provare che porre $TDT' \iff T$ e T' sono simili definisce una relazione di equivalenza su A.
(4) Nell'insieme $\mathcal{P}(A)$ la relazione di inclusione definisce un ordinamento parziale.

DEFINIZIONE **5.3.** Se A è un insieme qualsiasi, una *partizione* di A è una famiglia $\mathcal{F} \subseteq \mathcal{P}(A)$ tale che

$$A = \bigcup_{C \in \mathcal{F}} C \text{ e } C \cap C' = \emptyset, \forall C \neq C' \in \mathcal{F}.$$

PROPOSIZIONE **5.4.** *Dati un insieme A e una partizione $\mathcal{F}$ di A, ponendo,*

$$\forall\, x, y \in A,\ x \sim_{\mathcal{F}} y \iff \exists\, C \in \mathcal{F} : x \in C, y \in C$$

si definisce una relazione di equivalenza su A e viceversa, data una relazione di equivalenza $\sim$ su Aè definita una partizione $\mathcal{F}_\sim$ di A nel modo seguente:

$$C \in \mathcal{F}_\sim \iff \exists\, x \in A : C = \{y : y \in A, y \sim x\}.$$

Questa corrispondenza fra partizioni di A e relazioni di equivalenza su A è biunivoca.

Dim. Verifichiamo che $\sim_{\mathcal{F}}$ è un'equivalenza per ogni partizione $\mathcal{F}$ di A :$\sim_{\mathcal{F}}$ è riflessiva perché essendo $A = \bigcup_{C \in \mathcal{F}} C, \forall\, a \in A\, \exists\, C \in \mathcal{F} : a \in C$, (ossia $a \sim_{\mathcal{F}} a$), $\sim_{\mathcal{F}}$ è simmetrica per definizione; $\sim_{\mathcal{F}}$ è transitiva infatti $x \sim_{\mathcal{F}} y$ significa che $\exists\, C \in \mathcal{F}$ con $x \in C, y \in C, y \sim_{\mathcal{F}} z$ significa che $\exists\, D \in \mathcal{F}$ con $y \in D, z \in D$, poiché $y \in C \cap D$ e gli elementi di $\mathcal{F}$ sono a due a due disgiunti, si ha $C = D$, ossia $x \sim_{\mathcal{F}} z$. Verifichiamo viceversa che $\mathcal{F}_\sim$ è una partizione su A. Proviamo innanzi tutto che se $C, C' \in \mathcal{F}_\sim \Longrightarrow C = C'$ o $C \cap C' = \emptyset$, per definizione $C \in \mathcal{F}_\sim \iff \exists\, x \in A : C = \{y : y \in A, y \sim x\}, C' \in \mathcal{F}_\sim \iff \exists\, z \in A : C = \{w : w \in A, w \sim z\}$, se $\exists\, c \in C \cap C'$ sarebbe $c \sim x, c \sim z \Longrightarrow x \sim z \Longrightarrow z \in C \Longrightarrow C' \subseteq C$ e analogamente $C \subseteq C'$. Verifichiamo che vale $A = \bigcup_{C \in \mathcal{F}_\sim} C, \forall\, y \in A$, essendo $y \sim y$ vale $y \in C_y := \{x : x \sim y\} \in \mathcal{F}_\sim$.

Il fatto che la corrispondenza sia biunivoca discende dal fatto che se $\mathcal{F}$ determina $\sim$ e $\sim$ determina $\mathcal{F}' \Longrightarrow \mathcal{F} = \mathcal{F}'$.

DEFINIZIONE **5.5.** (1) La partizione $\mathcal{F}_\sim$ individuata da un'equivalenza $\sim$[15] è detta *insieme quoziente di A rispetto a* $\sim$ (o anche *insieme quoziente di A modulo* $\sim$) ed è denotata $A/\sim$.

(2) L'applicazione $\pi : A \longrightarrow A/\sim$, definita da

$$y \mapsto C_y := \{x \in A : x \sim y\} \in A/\sim,$$

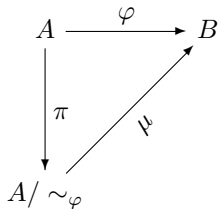
dicesi *applicazione naturale* (o *canonica*) di A su (tutto) $A/\sim$ o anche *riduzione di A modulo* $\sim$[16].

ESEMPIO **5.6.** (1) In $\mathbb{Z}$ sia $\sim_n$ la corrispondenza $a \sim_n b \iff a - b = nh$ per qualche $h \in \mathbb{Z}$, $\sim_n$ è una relazione di equivalenza infatti $a - a = 0n, \forall\, a \in \mathbb{Z}, a - b = hn \Longrightarrow b - a = -hn, \forall\, a, b \in \mathbb{Z}, a - b = hn.\, c - b = kn \Longrightarrow a - c = (h - k)n, \forall\, a, b \in \mathbb{Z}$, poiché $\forall x \in \mathbb{Z}$, $[x] = [r]$ con $x = nq + r, 0 \leq r \leq n - 1$ gli elementi di $\mathbb{Z}/\sim_n$ sono ordinatamente $[0], [1], \ldots, [n-1]$.

[15] Ossia, l'insieme delle classi di equivalenza di A rispetto a $\sim$.
[16] n.b. $x \sim y \iff \pi(x) = \pi(y)$.

(2) Nell'Es. 5.2 (3) l'insieme quoziente $A/\sim$ è in c.b.u. con l'insieme $B = \{(\alpha,\beta,\gamma) \in \mathbb{R}^3_+ : \alpha+\beta+\gamma = \pi\}$.

PROPOSIZIONE **5.7.** *Date un'applicazione $\varphi : A \longrightarrow B$, e la relazione di equivalenza $\sim_\varphi$ su A (definita in Es. 5.2 (2)), $\exists!\, \mu : A/\sim_\varphi \longrightarrow B$ che rende commutativo il diagramma (dove $\pi : A \longrightarrow A/\sim_\varphi$ è l'applicazione naturale), tale μ è iniettiva (ossia $A/\sim_\varphi$ è in c.b.u. con $\varphi(A)$).*



Dim. Abbiamo già visto in Es. 5.2 (2)) che $x \sim_\varphi y \iff \varphi(x) = \varphi(y)$ è un'equivalenza. $\forall\, C \in A/\sim_\varphi, c \in C$, poniamo $\mu(C) := \varphi(c)$ e verifichiamo che questa è una *buona definizione*[17], infatti, $\forall\, c' \in C \Longrightarrow c \sim_\varphi c' \iff \varphi(c) = \varphi(c')$. Inoltre, $\forall\, a \in A$ si ha $\mu(\pi(a)) = \mu(C_a) = \varphi(a)$, i.e. il triangolo è commutativo. Verifichiamo anche che μ è iniettiva, se $\mu(\pi(a)) = \mu(\pi(a')) \Longrightarrow \varphi(a) = \varphi(a')$ i.e. $a \sim_\varphi a'$ i.e. $\pi(a) = \pi(a)'$.

Infine, per quanto riguarda l'unicità di μ, se $\mu' : A/\sim_\varphi \longrightarrow B$ rende commutativo il triangolo $\Longrightarrow \forall\, C_x, x \in A$ risulta $\mu'(C_x) = \mu'(\pi(x)) = \varphi(x) = \mu(\pi(x)) = \mu(C_x)$ i.e. $\mu = \mu'$.

ESEMPIO **5.8.** (1) Se $A = \{\text{giorni di un anno}\}, B = \{\text{nomi dei giorni della settimana}\}$ e $A \xrightarrow{\varphi} B$ è l'applicazione che dà a ogni giorno dell'anno il suo nome (settimanale) e quindi $\sim_\varphi$ è l'equivalenza secondo cui due giorni sono equivalenti se hanno lo steso nome, ossia $A/\sim_\varphi$ è un insieme costituito da 7 elementi (il primo costituito da tutti i lunedí dell'anno, il secondo costituito da tutti i martedí dell'anno, ecc.), μ fa corrispondere alla classe di tutti i lunedí il nome i lunedí, ecc. ed è chiaramente una c.b.u.;

(2) Data $E : \mathbb{R} \longrightarrow \mathbb{Z}$ l'applicazione definita da
$$E(x) = [x] := \max\{n \in \mathbb{Z} : n \le x\},$$
si prova che $\mathbb{R}/\sim_E$ "è" $\mathbb{Z}$.

[17] Ossia, dipende dalla classe di equivalenza C e non dal rappresentante scelto $c \in C$.

6. Cardinalità

Definizione **6.1.** Due insiemi A, B sono *equipotenti*, e si scrive $A \sim B$, $\iff$ $\exists$ fra loro almeno una c.b.u..

Osservazione **6.2.** L'equipotenza è una relazione di equivalenza sulla "sulla classe U di tutti gli insiemi" (*l'insieme* Ω *di tutti gli insiemi* è infatti un ente alquanto malefico che dà luogo ad antinomie logiche, quali per esempio il paradosso di Russel).

Paradosso di Russel **6.3.** *Sia* Ω l'insieme di tutti gli insiemi *e sia* $F = \{J \in \Omega : J \notin J\}$*, se* $F \notin F$*, per definizione risulta* $F \in F$ *e parimenti se* $F \in F$ *risulta* $F \notin F$*,* (tertium non datur, ergo....).

Per ovviare ai paradossi logici, insiti nella teoria degli insiemi, si è stabilito di considerare un qualsiasi insieme come sottinsieme di *un grande insieme o universo* U (fissato una volta per tutte in ogni teoria), tale che tutto quello che si desidera costruire possa essere realizzato senza uscire da esso, tale artificio permette di evitare tutti i paradossi logici noti, ma non è dimostrato che in tal modo si evitino tutti i paradossi possibili.

Definizione **6.4.**
(1) Gli elementi della partizione $U/\sim$ sono detti *cardinalità* o *potenze* o *(numeri) cardinali*, piú precisamente, se un insieme A appartiene all'elemento α della partizione, si dice che α è la *cardinalità* o *potenza* di A e si scrive $\alpha = card(A)$ o $\alpha = \#A$ o $\alpha = \big|A\big|$.
(2) La cardinalità del segmento $\underline{n}$ è n. La cardinalità di $\emptyset$ è 0, in tal modo i numeri naturali $0, 1, 2, \ldots$, diventano anche numeri cardinali, a due a due distinti fra loro, e sono detti *cardinali finiti*, mentre gli altri cardinali sono detti *transfiniti*; gli insiemi di potenza finita sono detti *finiti*, gli altri *infiniti*.
(3) $\mathbb{N}$ è infinito e la sua potenza è denotata $\aleph_0$, un insieme di potenza $\aleph_0$ è detto *numerabile*.

Esempio **6.5.**
(1) *Gli insiemi* $\mathbb{P} := \{n \in \mathbb{N} : n = 2h, h \in \mathbb{N}\}$ *(dei numeri pari) e* $\mathbb{D} := \{n \in \mathbb{N} : n = 2h + 1, h \in \mathbb{N}\}$ *(dei numeri dispari) sono numerabili infatti si ha* $\mathbb{P} \sim \mathbb{N}$ *grazie alla bigezione* $\mathbb{N} \xrightarrow{\cdot 2} \mathbb{P}$*, definita da* $i \mapsto 2i, \mathbb{D} \sim \mathbb{N}$ *grazie alla bigezione* $\mathbb{N} \xrightarrow{\cdot 2+1} \mathbb{D}$*, definita da* $i \mapsto 2i + 1$.
(2) $\mathbb{Z}$ *è numerabile si ha infatti* $\mathbb{Z} \sim \mathbb{N}$ *grazie alla bigezione* $\mathbb{Z} \xrightarrow{\varphi} \mathbb{N}$*, definita da*

$$\varphi(n) = \begin{cases} 0 & \text{se } n = 0 \\ 2n & \text{se } n > 0 \\ -2n - 1 & \text{se } n < 0 \end{cases}$$

Proposizione-Definizione **6.6.** *Siano* α, β *numeri cardinali e siano* A, B *due insiemi (disgiunti) di cardinalità rispettive* α, β*,*
(1) *le cardinalità di* $A \cup B$ *e* $A \times B$*, dipendono solo da* α *e* β *e si chiamano rispettivamente* somma $\alpha + \beta$ *e* prodotto $\alpha \cdot \beta$ *di* α *e* β*, se* α *e* β *sono cardinali finiti,* $\alpha + \beta$ *e* $\alpha \cdot \beta$ *sono la solita somma e il solito prodotto di numeri naturali (come è immediato verificare);*
(2) *se* $A \neq \emptyset$*, l'insieme delle applicazioni di* A *in* B *è indicato* B^A *e la sua cardinalità è* β^α*, in particolare se* $B = \{0, 1\}$*,* B^A *è indicato* 2^A*;*
(3) *vale* $n + \aleph_0 = \aleph_0 + \aleph_0 = \aleph_0$ *per ogni cardinale finito* n*, inoltre, se* $n \neq 0$ *vale anche* $n \cdot \aleph_0 = \aleph_0$.

Dim. Siano $\alpha = \#A = \#A'$ e $\beta = \#B = \#B'$, per ipotesi $\exists\, A \xrightarrow{\varphi} A'$ e $B \xrightarrow{\psi} B'$ bigettive, porre $\sigma : A \cup B \longrightarrow A' \cup B'$ via

$$\sigma(x) = \begin{cases} \varphi(x) & \text{se } x \in A \\ \psi(x) & \text{se } x \in B \end{cases}$$

definisce una bigezione fra $A \cup B$ e $A' \cup B'$, ossia $\alpha + \beta = \#(A \cup B)$ è una buona definizione, inoltre, siccome $A \cup B = B \cup A$, vale $\alpha + \beta = \beta + \alpha$.

Analogamente per quanto riguarda $\alpha \cdot \beta = \#(A \times B)$, vedi Es. 6.18 (2).

Se α e β sono finiti e nonnulli β^α è la potenza di un numero naturale con esponente $\neq 0$, se $\beta \neq 0$ si definisce $\beta^0 = 1$ (se $A = \emptyset \Longrightarrow \exists!\, \varphi : A \longrightarrow B, \forall\, B \neq \emptyset$ e vale $\varphi(A) = \emptyset \subset B$, i.e. $\varphi = \iota_A$), non si definisce 0^0.

Sia $\mathbb{N}_n := \{m \in \mathbb{N} : m \geq n\}$, si ha $\mathbb{N} \sim \mathbb{N}_n$ grazie alla bigezione $\mathbb{N} \xrightarrow{+n} \mathbb{N}_n$ definita da $i \mapsto i + n$. Poiché $\mathbb{N} = \underline{n} \cup \mathbb{N}_n$ si ha $n + \aleph_0 = \aleph_0$.

Essendo $\mathbb{P} \sim \mathbb{N}$ e $\mathbb{D} \sim \mathbb{N}$, vedi Es.6.5, e $\mathbb{N} = \mathbb{P} \cup \mathbb{D}$ vale $\aleph_0 + \aleph_0 = \aleph_0$.

Infine, per ogni $n \in \mathbb{N}^*, \underline{n} \times \mathbb{N} \sim \mathbb{N}$ via la bigezione[18] $\underline{n} \times \mathbb{N} \xrightarrow{\varphi} \mathbb{N}$, definita da $\varphi(i,k) = i + nk$ con $0 \leq i \leq n-1, k \in \mathbb{N}$.

Definizione **6.7.** Dati due cardinali α, β, si dice che α *è minore di* β o che β *è maggiore di* α e si scrive $\alpha \prec \beta$ (o $\beta \succ \alpha$) se $\alpha \neq \beta$ ed $\exists$ due insiemi A, B di cardinalità rispettive α, β con $A \subset B$[19].

Definizione **6.8.** Dato un insieme A, per ogni $X \in \mathcal{P}(A)$ l'applicazione $\kappa_X \in 2^A$ definita da:

$$\kappa_X(a) = \begin{cases} 1 & \text{se } a \in X \\ 0 & \text{se } a \notin X \end{cases}$$

è detta *funzione caratteristica di* X.

Osservazione **6.9.** Dato un insieme A, ogni $\alpha \in 2^A$, $X := \alpha^{-1}(\{1\}) \in \mathcal{P}(A) \Longrightarrow \alpha$ è la funzione caratteristica $\kappa_X = \kappa_{\alpha^{-1}(\{1\})}$.

Proposizione **6.10.** *Per ogni insieme* A, $\#\mathcal{P}(A) = \#2^A$.

Dim. Definiamo un'applicazione $\Phi : 2^A \longrightarrow \mathcal{P}(A)$ mediante $\Phi(\kappa) := \kappa^{-1}(\{1\})$, poiché $\forall\, X \in \mathcal{P}(A), \exists\, \kappa_X \in 2^A : \Phi(\kappa_X) = X, \Phi$ è surgettiva, inoltre Φ è anche iniettiva in quanto se $\kappa \neq \lambda \in 2^A \Longrightarrow \exists\, a \in A$ con $\kappa(a) \neq \lambda(a)$, ossia, a appartiene a uno solo fra $\kappa^{-1}(\{1\})$ e $\lambda^{-1}(\{1\})$, pertanto $\Phi(\kappa) \neq \Phi(\lambda)$.

Proposizione **6.11.** *Per ogni cardinale* α, *si ha* $2^\alpha \succ \alpha$.

Dim. Sappiamo da Prop.6.10 che vale $2^A \sim \mathcal{P}(A)$, basta quindi provare che $\#\mathcal{P}(A) \succ \#A$. Chiaramente $\mathcal{P}(A)$ contiene un sottinsieme equipotente ad A(l'insieme di tutti i sottinsiemi $\{a\}$, al variare di $a \in A$). Basta quindi dimostrare che A e $\mathcal{P}(A)$ non sono equipotenti. Supponiamo (per assurdo) che lo siano e che $\mu : A \longrightarrow \mathcal{P}(A)$ sia una bigezione. Sia $B := \{a \in A : a \notin \mu(a),\}$ poiché $B \in \mathcal{P}(A)$ si ha che $B = \mu(b)$ per un ben determinato $b \in A$ (stiamo infatti supponendo che μ sia una bigezione!), se $b \in B = \mu(b)$ risulta $b \notin B$, deve quindi essere $b \notin B = \mu(b)$, ma allora $b \in B$, assurdo. Pertanto $\nexists$ alcuna bigezione fra A e $\mathcal{P}(A)$.

---

[18] n.b. $\underline{n} \subset \mathbb{N}$ i.e i due insiemi non sono disgiunti $\Longrightarrow$ negli elementi del prodotto cartesiano $\underline{n} \times \mathbb{N}$, occorre distinguere le componenti e verificare che si tratta realmente di una bigezione.

[19] n.b. quando α e β siano due numeri naturali(=cardinali finiti), questa definizione coincide con la solita!

DEFINIZIONE **6.12.** Dati un insieme *(di indici)* I e, $\forall\, i \in I$, un insieme A_i, il *prodotto cartesiano degli* A_i, indicato

$$\prod_{i\in I} A_i$$

è l'insieme delle applicazioni $\varphi : I \longrightarrow \bigcup_{i\in I} A_i \,:\, \varphi(i) \in A_i, \forall\, i \in I$.

Se I è finito, e.g. $I = \underline{n}^*$, anziché $\prod_{i\in I} A_i$si scrive $A_1 \times \cdots \times A_n$[20].

ASSIOMA DELLA SCELTA **6.13.** (Primo enunciato) *Data una famiglia (non vuota)* $\mathcal{F}$ *di insiemi non vuoti a due a due disgiunti,* $\exists\, G \subseteq \bigcup_{A\in\mathcal{F}} A \,:\, \#A \cap G = 1, \forall\, A \in \mathcal{F}$. (Secondo enunciato) *Un prodotto cartesiano di insiemi è vuoto* $\iff$ *è vuoto almeno uno dei fattori*[21].

LEMMA **6.14.** *Un insieme* A *è infinito* $\iff$ *A contiene un sottinsieme numerabile*[22].

Dim. Un insieme finito A certamente non contiene sottinsiemi numerabili, basta quindi dimostrare che un insieme A non finito[23] contiene almeno un sottinsieme numerabile. A tale scopo, $\forall\, n \in \mathbb{N}^*$, sia $F_n := \{\varphi : \underline{n} \xrightarrow{\varphi} A, \varphi \text{ iniettiva}\}$. Gli F_n son non vuoti e a due a due disgiunti (provarlo!) $\Longrightarrow$, per la validità dell'assiome della scelta, $\exists\, G \subseteq \bigcup_{n\in\mathbb{N}^*} F_n \,:\, \#F_n \cap G = 1, \forall\, n \in \mathbb{N}^*$, denotiamo φ_n quest'unico elemento. Si definisce un'applicazione iniettiva $\Phi : \mathbb{N} \longrightarrow A$ ponendo $\Phi(0) := \varphi_1(0)$ e, supposti definiti $\Phi(0), \Phi(1), \ldots, \Phi(n-1)$, $\Phi(n) := \varphi_{n+1}(h)$, se h è il minimo intero tale che $\varphi_{n+1}(h) \notin \Phi(\{0, 1, \ldots, n-1\})$. L'insieme $\{\Phi(n) : n \in \mathbb{N}\}$, è chiaramente un sottinsieme numerabile di A.

PROPOSIZIONE **6.15.** *Un insieme è infinito* $\iff$ *è equipotente a un suo sottinsieme proprio.*

Dim. Un insieme finito certamente non è equipotente a un suo sottinsieme proprio, pertanto, se un insieme è equipotente a un suo sottinsieme proprio non è finito. Dal Lemma6.14 sappiamo che un insieme infinito A contiene un sottinsieme numerabile B. Siano $b \in B, B' := \mathbf{B}\setminus\{b\}, C := A \setminus B, A' := B' \cup C$, chiaramente $B \sim B'$[24]. Poiché $B \cap C = B' \cap C = \emptyset$, si ha $A = B \cup C \sim B' \cup C = A' \subset A$.

ESEMPIO **6.16.**
(1) $\mathbb{R} \sim J := (-1, 1)$, infatti l'applicazione $x \mapsto \frac{x}{1+|x|}$ è una bigezione di $\mathbb{R}$ in J;
(2) Ogni intevallo aperto $(a, b) \subseteq \mathbb{R}$ è equipotente a J, infatti $x \mapsto x\frac{b-a}{2} + \frac{b+a}{2}$ è una bigezione di J in (a, b)[25];
(3) Ne segue che $\forall\, (a, b) \subseteq \mathbb{R}$ si ha $(a, b) \sim \mathbb{R}$.

---

[20] n.b. questo dà una definizione di $A_1 \times \cdots \times A_n$ (apparentemente) diversa da quella introdotta in Def.3.9, per esempio, se $n = 2$, si verifica che le due definizioni dànno luogo a due insiemi equipotenti associando alla coppia $(a_1, a_2) \in A_1 \times A_2$ (prima definizione) l'applicazione $(\varphi : \{\mathbf{1}, 2\} \longrightarrow A_1 \cup A_2) \in A_1 \times A_2$ (seconda definizione) definita da $\varphi(1) = a_1, \varphi(2) = a_2$ (per ulteriori approfondimenti sul tema vedi, per esempio, I. Barsotti, *Appunti di Algebra,* 1965, p. 14).

[21] Si dimostra che i due enunciati sono equivalenti.

[22] In altre parole: un cardinale α è transfinito $\iff$ $\alpha \succeq \aleph_0$.

[23] i.e $\#A \neq n, \forall\, n \in \mathbb{N}$.

[24] $B \sim \mathbb{N}, B' \sim \mathbb{N}^*$ e $\mathbb{N} \sim \mathbb{N}^*$ via la bigezione $n \mapsto n + 1$.

[25] Si verifica facilmente che $\forall\, \alpha \in (a, b)\, \exists!\, x = \frac{2\alpha-b-a}{b-a} \in J : x \mapsto \alpha$.

TEOREMA **6.17** (Cantor-Bernstein)**.** *Due insiemi, ciascuno dei quali è equipotente a un sottinsieme dell'altro, sono equipotenti fra loro.*

Dim. Siano A, B', gli insiemi ed $\alpha : A \longrightarrow B', \beta' : B' \longrightarrow A$ due applicazioni iniettive. Poniamo $B := \beta'(B') \subseteq A, A' := \beta'(\alpha(A)) \subseteq A$, dall'essere $\alpha(A) \subseteq B'$ discende che $A' = \beta'(\alpha(A)) \subseteq \beta'(B') = B$, ossia $A' \subseteq B \subseteq A$ e $\varphi := \beta' \circ \alpha$ è una bigezione di A su A'. Provando che $A \sim B$ otterremo $A \sim B'$ come richiesto, giacché chiaramente $B \sim B'$.

Poniamo

$$C := A \setminus B,\ D := C \cup \varphi(C) \cup \varphi^2(C) \cup \cdots$$

e definiamo $\psi : A \longrightarrow A$ nel modo seguente:

$$\psi(a) = \begin{cases} \varphi(a) & \text{se } a \in D \\ a & \text{se } a \in A \setminus D \end{cases}$$

e verifichiamo che ψ è una bigezione di A su B.

$-\ a \in D \Longrightarrow \psi(a) = \varphi(a) \in A' \subseteq B$, $a \in A \setminus D \Longrightarrow \psi(a) = a \in A \setminus D \subseteq A \setminus C = B$, ossia ψ manda A su B;

$-\ \forall\, b \in B$, vale $b \in D$ oppure $b \in B \cap (A \setminus D) = B \setminus D$; se $b \notin D \Longrightarrow \psi(b) = b \in B$, se $b \in D := C \cup \varphi(C) \cup \varphi^2(C) \cup \cdots$, essendo $C := A \setminus B$ risulta $b \notin C \Longrightarrow b \in \varphi(C) \cup \varphi^2(C) \cup \cdots = \varphi(C \cup \varphi(C) \cup \varphi^2(C) \cup \cdots) = \varphi(D)$ i.e. $b = \varphi(a) = \psi(a)$ per qualche $a \in D$, ossia ψ è surgettiva su B;

$-$ proviamo che ψ è iniettiva attraverso un ragionamento per assurdo: se fosse $\psi(a) = \psi(a')$ per qualche $a \neq a'$, a e a' non potrebbero appartenere entrambi ad $A \setminus D$ (perché per definizione ψ opera su $A \setminus D$ come $\iota_{A \setminus D}$), né potrebbero entrambi appartenere a D (perché per definizione ψ opera su D come φ, che è iniettiva). Supponiamo allora per esempio che $a \in A \setminus D, a' \in D$, poiché $\psi(a) = a \notin D$ e $\psi(a') = \varphi(a') \in \varphi(D) \subset D$, abbiamo ottenuto l'assurdo voluto.

ESEMPIO **6.18.**

(1) $\forall\, n \in \mathbb{N}^*$, $\mathbb{N} \sim \underbrace{\mathbb{N} \times \cdots \times \mathbb{N}}_{k-\text{volte}}$, infatti $\varphi : \mathbb{N} \longrightarrow \underbrace{\mathbb{N} \times \cdots \times \mathbb{N}}_{k-\text{volte}}$ definita da $\varphi(n) := (n, 0, \ldots, 0)$ è iniettiva, e pure $\psi : \underbrace{\mathbb{N} \times \cdots \times \mathbb{N}}_{k-\text{volte}} \longrightarrow \mathbb{N}$ definita da $\psi(n_1, \ldots, n_k) := 2^{n_1} \cdot 3^{n_2} \cdots p_k^{n_k}$ è parimenti iniettiva.

(2) $\mathbb{Q} \sim \mathbb{N}$ (ossia $\mathbb{Q}$ è numerabile) infatti
- $\mathbb{Q} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ definita da $[\frac{p}{q}] \mapsto (p, q)$, con M.C.D.$(p, q) = 1$ è iniettiva,
- $\mathbb{Z} \times \mathbb{Z} \sim \mathbb{N} \times \mathbb{N}$,
- $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$,

pertanto, poiché la composizione di applicazioni iniettive è iniettiva, $\exists\, \alpha : \mathbb{Q} \longrightarrow \mathbb{N}$ iniettiva, e infine
- $\iota : \mathbb{N} \longrightarrow \mathbb{Q}$ definita da $\iota(n) = [\frac{n}{1}]$ è chiaramente iniettiva.

(3) Ogni intervallo $K \subset \mathbb{R}$ è equipotente a $\mathbb{R}$, infatti, per ogni intervallo $K \subset \mathbb{R}, \exists$ intervalli aperti $L, L' \subset \mathbb{R} :\ L \subset K \subset L'$ e vale $L \sim L' \sim \mathbb{R}$.

(4) $\mathbb{R}$ non è numerabile.

Proviamo che $\#\mathbb{R} = 2^{\aleph_0}$ dando una bigezione di $\mathcal{P}(\mathbb{N})$ in $I = [0, 1]$. Usiamo il seguente fatto: $\forall\, \alpha \in I$ si scrive in modo unico nella forma:

$$\alpha = \sum_{n=1}^{\infty} \frac{a_n}{2^n} \text{ con } a_n = 0, \text{ oppure } a_n = 1,$$

modulo la seguente identificazione:

$$\frac{a_1}{2}+\frac{a_2}{2^2}+\cdots\frac{a_{n-1}}{2^{n-1}}+\frac{0}{2^n}+\frac{1}{2^{n+1}}+\frac{1}{2^{n+2}}+\cdots=\frac{a_1}{2}+\frac{a_2}{2^2}+\cdots\frac{a_{n-1}}{2^{n-1}}+\frac{1}{2^n}+\frac{0}{2^{n+1}}+\frac{0}{2^{n+2}}+\cdots .$$

Da Prop.6.10 sappiamo che $\mathcal{P}(\mathbb{N})\sim 2^{\mathbb{N}}$, consideriamo il sottinsieme $X\subseteq 2^{\mathbb{N}}$ costituito dalla totalità delle funzioni caratteristiche che assumono il valore 1 infinite volte. Definiamo $\Psi : 2^{\mathbb{N}}\longrightarrow\mathbb{R}$ ponendo:

$$\Psi(x)=\begin{cases}\sum\limits_{n=1}^{\infty}\frac{\kappa(n)}{2^n} & \text{se } x\in X\\ 2+\sum\limits_{n=1}^{\infty}\frac{\kappa(n)}{2^n} & \text{se } x\notin X,\end{cases},$$

chiaramente Ψ è iniettiva e $(0,1]\subset\Psi(2^{\mathbb{N}})\subset\mathbb{R}$, dall'essere $\#(0,1]=\#\mathbb{R}$ discende la tesi

(5) *Ipotesi del continuo generalizzata:* Se A è un insieme infinito, $\exists$ un insieme B con $\#A\prec\#B\prec 2^{\#A}$?

Definizione **6.19.** Un elemento $a\in A$, con A insieme semiordinato mediante $\prec$, è
minimo o *primo* se $a\prec b$, $\forall\, b\in A$,
massimo o *ultimo* se $b\prec a$, $\forall\, b\in A$,
minimale se $\nexists\, b\in A:\ b\prec a$,
massimale se $\nexists\, b\in A:\ a\prec b$.

Osservazione **6.20.** Il minimo (risp.il massimo) di A, se $\exists$, è unico.

Definizione **6.21.** Se $B\subseteq A$ con A insieme semiordinato mediante $\prec$,
un *maggiorante* di B è ogni $a\in A$ con $a\succeq b$, $\forall\, b\in B$,
un *minorante* di B è ogni $a\in A$ con $a\preceq b$, $\forall\, b\in B$,
l'*estremo superiore* di B, se $\exists$, è il minimo maggiorante di B,
l'*estremo inferiore* di B, se $\exists$, è il massimo minorante di B,

Definizione **6.22.** Un insieme semiordinato A è detto *induttivo* se ogni suo sottinsieme totalmente ordinato ha in A estremo superiore.

Lemma di Zorn **6.23.** *In un insieme, semiordinato (mediante $\prec$), induttivo A, $\forall\, a\in A$, $\exists$ qualche elemento massimale $\succeq a$.*

Osservazione **6.24.** Il Lemma di Zorn è equivalente all'assioma della scelta (o Lemma di Zermelo), ossia, se il lemma di Zorn è soddisfatto, anche l'assioma della scelta lo è e reciprocamente.

7. Calcolo combinatorio

Definizione **7.1.** Un'applicazione bigettiva di un insieme finito $A=\{a_1,a_2,\ldots,a_n\}$ in sé è detta *permutazione* di A.

Osservazione **7.2.**
Poiché $i\mapsto a_i$ è una bigezione di $\underline{n}^*$ in $A=\{a_1,a_2,\ldots,a_n\}$, le permutazioni di A possono essere pensate come bigezioni di $\underline{n}^*$ in A.

Piú in generale, $\forall\, 1\leq k\leq n$:

Definizione **7.3.** Un'applicazione iniettiva $\varphi:\underline{k}^*\longrightarrow A=\{a_1,a_2,\ldots,a_n\}$, è detta *disposizione di classe k* di A.

OSSERVAZIONE **7.4.** Una disposizione φ di classe k di n elementi è individuata da una k-pla

$$(a_{i_1}, a_{i_2}, \dots, a_{i_k}) \in \underbrace{A \times \cdots \times A}_{k-\text{volte}}, \text{ con } j \overset{\varphi}{\mapsto} a_{i_j}, 1 \le j \le k \tag{1}$$

PROPOSIZIONE **7.5.** *Il numero* $\mathbf{D}_{n,k}$ *delle disposizioni di classe* k *di* n *elementi è* $n(n-1)\cdots(n-k+1)$, $\forall\, 1 \le k \le n$.

Dim. Per (1) bisogna contare il numero delle diverse k-ple $(a_{i_1}, a_{i_2}, \dots, a_{i_k})$ di elementi distinti di A. In una k-pla di elementi distinti di $A, (a_{i_1}, a_{i_2}, \dots, a_{i_k})$

a_{i_1} può essere scelto fra gli n elementi di A,
a_{i_2} può essere scelto fra gli $n-1$ elementi di $A \setminus \{a_{i_1}\}$,
a_{i_3} può essere scelto fra gli $n-2$ elementi di $A \setminus \{a_{i_1}, a_{i_2}\}$,
$\vdots$
a_{i_k}, può essere scelto fra gli $n-k+1$ elementi di $A \setminus \{a_{i_1}, a_{i_2}, \dots, a_{i_{k-1}}\}$.

OSSERVAZIONE **7.6.** Se $k = n$, poiché un'applicazionie iniettiva di $\underline{k}^*$ in A è bigettiva, $\mathbf{D}_{n,n} = n(n-1)\cdots 2\cdot 1$ coincide con $\mathbf{P}_n$, il numero delle permutazioni di A ed è indicato col simbolo $n!$. Per convenzione $0! = 1$; $\forall\, n \ge 1$, $n! = n \cdot (n-1)!$

DEFINIZIONE **7.7.** Un sottinsieme di k elementi di A, cioè $\{a_{i_1}, a_{i_2}, \dots, a_{i_k}\} \subseteq A = \{a_1, a_2, \dots, a_n\}$, è detto *combinazione di classe* k di elementi di A.

PROPOSIZIONE **7.8.** *Il numero* $\mathbf{C}_{n,k}$ *delle combinazioni di classe* k *di* n *elementi è*

$$\frac{n(n-1)\cdots(n-k+1)}{k!} =: \binom{n}{k}.$$

Dim. L'immagine di un'applicazione iniettiva di $\underline{k}^*$ in A è un sottinsieme di k elementi $A = \{a_1, a_2, \dots, a_n\}$, fissato un $\{a_{i_1}, a_{i_2}, \dots, a_{i_k}\} \subset A$, il numero delle permutazioni dei suoi elementi è $k!$, pertanto $\mathbf{D}_{n,k} = \mathbf{C}_{n,k} \cdot k!$, ossia la tesi.

DEFINIZIONE **7.9.** Il numero $\binom{n}{k}$ è detto *coefficiente binomiale*[26].

OSSERVAZIONE **7.10.** (1) Si ha $\binom{n}{k} = \binom{n}{n-k}$, infatti

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)(n-k)!}{k!(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k},$$

(2) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}'$
(3) $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n-1}{k} + \cdots + \binom{k+1}{k} + \binom{k}{k}$.

DEFINIZIONE **7.11.** $\forall\, 1 \le k \le n$, un'applicazione di $\sigma : \underline{k}^* \longrightarrow A = \{a_1, a_2, \dots, a_n\}$, è detta *disposizione con ripetizione di classe* k degli elementi di A.

OSSERVAZIONE **7.12.** Mentre gli elementi della k-pla che individua una disposizione classe k di A sono tutti distinti fra loro, nel caso di una disposizione con ripetizione questo non è piú necessariamente vero, infatti per l'applicazione $\sigma : \underline{k}^* \longrightarrow A$ corrispondente non è richiesta l'iniettività.

PROPOSIZIONE **7.13.** *Il numero* $\mathbf{D}'_{n,k}$ *delle disposizioni con ripetizione di classe* k *di* n *elementi è* n^k.

[26]Per convenzione $\binom{n}{0} = 1$, infatti $\emptyset \subseteq A$ è l'unico sottinsieme di 0 di elementi di A.

Dim. Il numero delle k-ple distinte $(a_{i_1}, a_{i_2}, \dots, a_{i_k})$ di elementi di. A è quello dichiarato perché in una k-pla di elementi di A, $(a_{i_1}, a_{i_2}, \dots, a_{i_k})$, $\forall\, j \in \underline{k}^*$ l'elemento a_{i_j} può essere scelto fra gli n elementi di A.

Definizione **7.14.** Se $n, k \in \mathbb{N}^*, A = \{a_1, a_2, \dots, a_n\}$ e $B = \underbrace{A \times \cdots \times A}_{k-\text{volte}}$, ogni elemento di

$$C := \{(a_{i_1}, a_{i_2}, \dots, a_{i_k}) \in B : 1 \leq i_1 \leq i_2, \dots \leq i_k \leq n\},$$

è detto *combinazione con ripetizione di classe k* di elementi di A.

Proposizione **7.15.** *Il numero $C'_{n,k}$ delle combinazioni con ripetizione di classe k di n elementi è*

$$\binom{n+k-1}{k}.$$

Dim. Vogliamo calcolare $\#C$ al variare di $n, k \in \mathbb{N}^*$, se $n = 1, \Longrightarrow \#C = 1$ e vale $1 = \binom{1+k-1}{k}$, $\forall\, k \in \mathbb{N}^*$ i.e. $C'_{1,k} = 1$; se $k = 1, \Longrightarrow \#C = n$ e vale $n = \binom{n+1-1}{1}$, $\forall\, n \in \mathbb{N}^*$ i.e. $C'_{n,1} = n$. Supponiamo quindi di avere dimostrato che vale $C'_{r,s} = \binom{r+s-1}{s}$, $\forall r \leq n, s \leq k$ e facciamo vedere che valgono:

- $C'_{n+1,k} = \binom{n+1+k-1}{k} = \binom{n+k}{k}$,
- $C'_{n,k+1} = \binom{n+(k+1)-1}{k+1} = \binom{n+k}{k+1}$.

Posto $A' = \{a_1, \dots, a_{n+1}\}$

- $\tilde{C} := \{(a_{i_1}, a_{i_2}, \dots, a_{i_{k+1}}) \in \underbrace{A \times \cdots \times A}_{(k+1)-\text{volte}} : 1 \leq i_1 \leq i_2, \dots \leq i_k \leq n\}$, è l'insieme delle combinazioni con ripetizione di classe $k+1$ di n elementi,
- $\hat{C} := \{(a_{i_1}, a_{i_2}, \dots, a_{i_k}) \in \underbrace{A' \times \cdots \times A'}_{k-\text{volte}} : 1 \leq i_1 \leq i_2, \dots \leq i_{k+1} \leq n+1\}$, è l'insieme delle combinazioni con ripetizione di classe k di $n+1$ elementi, cosí $C'_{n,k+1} = \#\tilde{C}, C'_{n+1,k} = \#\hat{C}$.

Le $k+1$-ple di elementi di $\tilde{C}$ sono ottenute dalle k-ple di C nel modo seguente:

1) anteponendo a_1 a ogni k-pla di C,
2) anteponendo a_2 a ogni k-pla di C che coinvolge solo $a_2, \dots, a_n$,

⋮

j) anteponendo a_j a ogni k-pla di C che coinvolge solo $a_j, \dots, a_n$,

⋮

n) anteponendo a_n all'unica k-pla di C che coinvolge solo a_n.

In tal modo da 1) si ottengono $C'_{n,k}$ contributi, da 2) si ottengono $C'_{n-1,k}$ contributi, ..., da j) si ottengono $C'_{n-(j-1),k}$ contributi, ..., da n) si ottiene $1 = C'_{1,k}$ contributo. Pertanto,

$$\#\tilde{C} = \binom{n+k-1}{k} + \binom{n-1+k-1}{k} + \cdots + \binom{n-j+1+k-1}{k} + \cdots + \binom{1+k-1}{k}$$

e quindi $\#\tilde{C} = \binom{n+k}{k+1}$, applicando Oss. 7.10(3).

Le k-ple di elementi di $\hat{C}$ sono esattamentente:

1) la k-pla $(a_1, a_1, \dots, a_1, a_1)$,

2) le $C'_{n,1}$ k-ple del tipo $(a_1, a_1, \dots, a_1, a_i)$, con $2 \le i \le n$,
3) le $C'_{n,2}$ k-ple del tipo $(a_1, a_1, \dots, a_{i_1}, a_{i_2})$, con $2 \le i_1 \le i_2 \le n$,

$\vdots$

j) le $C'_{n,j}$ k-ple del tipo $(a_1, a_1, \dots, a_{i_1}, a_{i_2}, \dots, a_{i_j})$, con $2 \le i_1 \le i_2 \le \dots \le i_j \le n$,

$\vdots$

k-1) le $C'_{n,k-1}$ k-ple del tipo $(a_1, a_{i_1}, \dots, a_{i_{k-2}}, a_{i_{k-1}})$, con $2 \le i_1 \le i_2 \le \dots \le i_{k-1} \le n$,
k) le $C'_{n,k}$ k-ple del tipo $(a_{i_1}, \dots, a_{i_{k-1}}, a_{i_k})$, con $2 \le i_1 \le i_2 \le \dots \le i_k \le n$.

In tal modo da 1) si ottiene $1 = \binom{n+0-1}{0} = \binom{n-1}{0} = \binom{n}{0}$ contributo, da 2) si ottengono $\binom{n+1-1}{1}$ contributi, da 3) si ottengono $\binom{n+2-1}{2}$ contributi, ..., da j) si ottengono $\binom{n+j-1-1}{j-1}$ contributi, ..., da $k-1$) si ottengono $\binom{n+k-3}{k-1}$ contributi, da k) si ottengono $\binom{n+k-2}{k}$ contributi. Pertanto,

$$\#\hat{C} = \binom{n}{0} + \binom{n}{1} + \binom{n+1}{2} + \binom{n+2}{3} + \cdots + \binom{n+k-2}{k-1} + \binom{n+k-1}{k}$$

e quindi $\#\tilde{C} = \binom{n+k}{k}$, applicando ripetutamente Oss. 7.10(2).

Esempio **7.16.** (1) I monomi di grado 6 in 8 variabili non sono altro che le combinazioni con ripetizione di 8 elementi a 6 a 6, ossia il loro numero è $\binom{13}{6} = 1716$.
(2) Le possibili colonne vincenti al totocalcio non sono altro che le disposizioni con ripetizione di classe 13 dei 3 elementi $1, X, 2$ quindi il loro numero è 3^{13}.

8. Elementi di teoria dei gruppi

Definizione **8.1.** Un *gruppo* è un insieme non vuoto G dotato di una *legge di composizione,* cioè di un'applicazione

$$G \times G \xrightarrow{*} G, \text{ definita da } (g,h) \overset{*}{\mapsto} g * h$$

- $*$ è *associativa*, ossia $(g * h) * k = g * (h * k), \quad \forall\, g, h, k \in G$,
- $*$ ha *identità sinistra*, ossia $\exists\, e \in G : e * g = g, \quad \forall\, g \in G$,
- $*$ ha *reciproco sinistro*, ossia $\forall\, g \in G, \exists\, h \in G : h * g = e$.

Un gruppo G con legge di composizione $*$ è indicato $(G, *)$.
In un gruppo $(G, *)$, l'elemento $g * h$ è chiamato *composto* di g e h o anche *prodotto* (indicato $g \cdot h$) o *somma* (indicata $g + h$) [27]
Un gruppo $(G, *)$, in cui $g * h = h * g$, $\forall\, h, g \in G$ è chiamato *commutativo* o *abeliano.*

Esempio **8.2.** (1) $(\mathbb{N}, +)$ (risp. $(\mathbb{N}, \cdot)$ non è un gruppo infatti, $\forall\, n \in \mathbb{N}^* \ \nexists\, m \in \mathbb{N} : m + n = 0$, $\forall n \in \mathbb{N} \setminus \{1\} \ \nexists\, m \in \mathbb{N} : m \cdot n = 1$. peraltro, poiché si ha $n + (m + h) = (n + m) + h, n \cdot (m \cdot h) = (n \cdot m) \cdot h$, $\forall\, h, m, n$, le operazioni $+$ e $\cdot$ sono in $\mathbb{N}$ solo associative, rispettivamente con 0 e 1 come identità sinistre.

[27] Nel primo caso il gruppo è detto *moltiplicativo*, nel secondo *additivo*.

(2) $(\mathbb{Z},+)$ è un gruppo additivo infatti l'addizione è associativa poiché $n+(m+h)=(n+m)+h, \forall\, h,m,n\in\mathbb{Z}, 0\in\mathbb{Z}$ è l'elemento neutro rispetto all'addizione e $\forall\, m\in\mathbb{Z}, \exists\, -m\in\mathbb{Z}: (-m)+m=0$; invece né $(\mathbb{Z},\cdot)$ né $(\mathbb{Z},-)$ sono gruppi infatti, $\forall\, n\in\mathbb{Z}\setminus\{1,-1\}\ \nexists\, m\in\mathbb{Z}: m\cdot n=1$ e l'operazione $-$ non è associativa: e.g. $3=(7-3)-1\neq 7-(3-1)=5$.
(3) Provare che $(\mathbb{Q},+),(\mathbb{Q}^*,\cdot),(\mathbb{R},+),(\mathbb{R}^*,\cdot),(\mathbb{C},+),(\mathbb{C}^*,\cdot)$ sono tutti gruppi.
(4) Dato un insieme A, introducendo sull'insieme $\mathcal{P}(A)$ la legge di composizione Δ definita $\forall\, X,Y\in\mathcal{P}(A)$ da $X\Delta Y=X\cup Y\setminus X\cap Y$ si ottiene un gruppo abeliano:
- Δ è associativa:

$$\begin{aligned}(X\Delta Y)\Delta Z &= [(X\cup Y\setminus X\cap Y)\cup Z]\setminus[(X\cup Y\setminus X\cap Y)\cap Z]=\\ &= [X\setminus(Y\cup Z)]\cup[(Y\setminus(X\cup Z)]\cup[Z\setminus(X\cup Y)]\cup X\cap Y\cap Z=\\ &= [X\cup(Y\cup Z\setminus Y\cap Z)]\setminus[X\cap(Y\cup Z\setminus Y\cap Z)]=\\ &= X\Delta(Y\Delta Z);\end{aligned}$$

- $\exists$ elemento neutro $\emptyset$ tale che $X\Delta\emptyset=X, \forall\, X\in\mathcal{P}(A)$;
- $\forall\, X\in\mathcal{P}(A)\,\exists$ inverso X tale che $X\Delta X=\emptyset$;
- Δ è commutativa: $X\Delta Y=X\cup Y\setminus X\cap Y=Y\Delta X, \forall\, X,Y\in\mathcal{P}(A)$.

LEMMA **8.3.** *Sia $(G,*)$ un gruppo,*
(1) $\exists!\, e\in G: e*g=g*e, \forall g\in G$ *(tale e è detto* identità *o* elemento neutro *di G)*;
(2) $\forall\, g\in G\ \exists!$ *elemento* $G\ni g^{-1}: g^{-1}*g=e=g*g^{-1}$ *(tale g^{-1} è detto* reciproco *o* inverso *od o* opposto *di $g\in G$)*;
(3) $(g^{-1})^{-1}=g, \forall\, g\in G$ *e* $(g*h)^{-1}=h^{-1}*g^{-1}, \forall\, g,h\in G$.

Dim. Per definizione di gruppo, $\forall\, g\in G, \exists$ reciproco sinistro $h\in G$ (a priori non unico!) tale che $h*g=e\Longrightarrow h*(g*h)=(h*g)*h=e*h=h$, moltiplicando ambo i membri di $h*(g*h)=h$ a sinistra per un reciproco sinistro k di h si ottiene:

$$e=k*h=k*[h*(g*h)]=(k*h)*(g*h)=e*(g*h)=g*h,$$

ossia h è anche reciproco destro di g.

Inoltre, avendo appena visto che h è reciproco destro e sinistro di g, si ha

$$g*e=g*(h*g)=(g*h)*g=e*g=g,$$

ossia un'identità sinistra è anche destra. Se $e'\in G$ è tale che $e'*g=g, \forall\, g\in G$, (poiche e funziona anche a destra) si ha in particolare:

$$e'=e'*e=e.$$

Proviamo l'unicità del reciproco, se $h'\in G$ è un altro reciproco di $g\in G$, si ha:

$$h'=h'*e=h'*(g*h)=(h'*g)*h=e*h=h, \Longrightarrow \text{si scrive semplicemente } g^{-1}.$$

L'uguaglianza $(g^{-1})^{-1}=g, \forall\, g\in G$ discende allora immediatamente dall'unicità del reciproco e dal fatto che vale $g*(g^{-1})=e, \forall\, g\in G$. Infine, l'uguaglianza $(g*h)^{-1}=h^{-1}*g^{-1}, \forall\, g,h\in G$, discende ancora dall'unicità del reciproco e dal fatto che vale $(g*h)(h^{-1}*g^{-1})=g*(h*h^{-1})*g^{-1}=g*g^{-1}=e, \forall\, g,h\in G$.

OSSERVAZIONE **8.4.** (1) In un gruppo $(G,*)$ valgono le *leggi di cancellazione destra e sinistra*, ossia:

$$g*h=g'*h\Longrightarrow g=g' \qquad \text{(moltiplicando ambo i membri a destra per } h^{-1}),$$

$k * g = k * g' \Longrightarrow g = g'$ (moltiplicando ambo i membri a sinistra per k^{-1}).

(2) Spesso per i gruppi abeliani si usa la notazione additiva, nel qual caso l'opposto di un elemento $h \in G$ è $-h$ e, $\forall\, g \in G$, si scrive $g - h$ anziché $g * h^{-1}$. In un gruppo moltiplicativo $(G, \cdot)$, spesso viene omesso il simbolo $\cdot$ fra gli elementi, ossia si scrive gh anziché $g \cdot h$.

(3) In un gruppo additivo (risp. moltiplicativo) l'elemento neutro è indicato 0 (risp. 1).

NOTAZIONE **8.5.** In un gruppo $(G, *), \forall\, g \in G$ ed $m \in \mathbb{Z}$, il simbolo g^m è definito come segue:

- se $m > 0$ $\quad g^m := \underbrace{g * \cdots * g}_{m-\text{volte}}$,
- se $m = 0$ $\quad g^0 := e$,
- se $m < 0$ $\quad g^m := \underbrace{g^{-1} * \cdots * g^{-1}}_{-m-\text{volte}}$, infatti $-m > 0$.

TEOREMA **8.6.** *Siano G un gruppo ed $m, n \in \mathbb{Z}$, $\forall g \in G$ valgono:*

(1) $\quad g^{m+n} = g^m * g^n$,

(2) $\quad g^{mn} = (g^m)^n$.

Inoltre, se $h, g \in G$ soddisfano $g * h = h * g$,

(3) $\quad (g * h)^n = g^n * h^n$.

Dim. Se m, n sono entrambi positivi o nulli, oppure sono entrambi negativi o nulli, (1) è conseguenza delle definizioni. Il caso non banale è che n ed m siano discordi, supponiamo, per esempio, $n < 0, m > 0$. Supponiamo preliminarmente che sia $-n < m$ ossia $0 < n + m$, si ha:

$$g^n * g^m = (g^{-1})^{-n} * g^m = \underbrace{g^{-1} * \cdots * g^{-1}}_{-n-\text{volte}} * \underbrace{g * \cdots * g}_{-n-\text{volte}} * \underbrace{g * \cdots * g}_{n+m-\text{volte}},$$

sia ora $n < 0$ qualsiasi (ossia non supponiamo piú $0 < n + m$) e sia q un intero positivo molto grande (in simboli $q \gg 0$), in modo che risulti $q > -(n + m)$ (e quindi $q + m > -n, q > -m$), vale:

$$g^{n+m} * g^q = g^{n+m+q} = g^n * g^{m+q} = g^n * g^m * g^q,$$

infatti $g^{n+m} * g^q = g^{n+m+q}$ perché $q > -(n + m)$, $g^{n+m+q} = g^n * g^{m+q}$ perché $q + m > -n$, $g^n * g^{m+q} = g^n * g^m * g^q$ perché m e q sono entrambi positivi. Infine, moltiplicando ambo i membri di $g^{n+m} * g^q = g^n * g^m * g^q$ a destra per $(g^q)^{-1}$, si ottiene la tesi.

Per quanto riguarda (2), se m, n sono entrambi positivi o nulli

$$(g^m)^n = \underbrace{g^m * \cdots * g^m}_{n-\text{volte}} = \underbrace{\underbrace{g * \cdots * g}_{m-\text{volte}} \cdots \underbrace{g * \cdots * g}_{m-\text{volte}}}_{n-\text{volte}},$$

se m ed n sono discordi, supponiamo per esempio $m \geq 0$ ed $n \leq 0$ si ha $mn \leq 0$ e quindi $g^{mn} = (g^{-1})^{-mn}$, d'altra parte

$$(g^m)^n = \underbrace{(g^m)^{-1} * \cdots (g^m)^{-1}}_{-n-\text{volte}} = \underbrace{\underbrace{g^{-1} * \cdots g^{-1}}_{m-\text{volte}} * \cdots \underbrace{g^{-1} * \cdots g^{-1}}_{m-\text{volte}}}_{-n-\text{volte}} = (g^{-1})^{-mn};$$

infine, se m, n sono entrambi negativi o nulli si ha si ha $mn \geq 0$ e quindi $g^{mn} = \underbrace{g * \cdots * g}_{mn-\text{volte}}$, mentre essendo $g^m := \underbrace{g^{-1} * \cdots * g^{-1}}_{-m-\text{volte}}$, si ha

$$(g^m)^n = \underbrace{(g^m)^{-1} * \cdots (g^m)^{-1}}_{-n-\text{volte}} = \underbrace{\underbrace{(g^{-1})^{-1} * \cdots (g^{-1})^{-1}}_{-m-\text{volte}} * \cdots \underbrace{(g^{-1})^{-1} * \cdots * (g^{-1})^{-1}}_{-m-\text{volte}}}_{-n-\text{volte}} = g^{mn}.$$

Per quanto riguarda (3), se $n > 0$ si ha

$$\begin{aligned}
(g*h)^n &= \underbrace{(g*h)*(g*h)*\cdots*(g*h)}_{n-\text{volte}} = \\
&= g*(g*h)*h*\underbrace{(g*h)*\cdots*(g*h)}_{n-2-\text{volte}} = \\
&= g*g*h*h*\underbrace{(g*h)*\cdots*(g*h)}_{n-2-\text{volte}} = \\
&= \cdots\cdots\cdots = \\
&= \underbrace{g*g*\cdots*g}_{n-\text{volte}} * \underbrace{h*h*\cdots*h}_{n-\text{volte}} = g^n * h^n;
\end{aligned}$$

se $n = 0$ si ha $(g*h)^n = e = e*e = g^n * h^n$;
se $n < 0$ osserviamo che da $g*h = h*g$ discende $h^{-1}*g^{-1} = (g*h)^{-1} = (h*g)^{-1} = g^{-1}*h^{-1}$, inoltre

$$\begin{aligned}
(g*h)^n &= [(g*h)^{-1}]^{-n} = \underbrace{(g*h)^{-1}*\cdots*(g*h)^{-1}}_{-n-\text{volte}} = \\
&= \underbrace{(h^{-1}*g^{-1})*(h^{-1}*g^{-1})*\cdots*(h^{-1}*g^{-1})}_{-n-\text{volte}} = \\
&= h^{-1}*(g^{-1}*h^{-1})*h^{-1}*\underbrace{(h^{-1}*g^{-1})*\cdots*(h^{-1}*g^{-1})}_{-n-2-\text{volte}} = \\
&= h^{-1}*h^{-1}*g^{-1}*g^{-1}*\underbrace{((h^{-1}*g^{-1})*\cdots*((h^{-1}*g^{-1})}_{-n-2-\text{volte}} = \\
&= \cdots\cdots\cdots = \\
&= \underbrace{h^{-1}*h^{-1}*\cdots*h^{-1}}_{-n-\text{volte}} * \underbrace{g^{-1}*g^{-1}*\cdots*g^{-1}}_{-n-\text{volte}} = h^n * g^n.
\end{aligned}$$

DEFINIZIONE **8.7.** Un gruppo $(G, *)$ si dice *finito* se $\#G \prec \aleph_0$ e la cardinalità di G è detta *ordine* $|G|$ del gruppo.

ESEMPIO **8.8.** (1) Siano $\emptyset \neq A$ un insieme e $\mathfrak{T}(A) = \{f \in A^A : f \text{ è bigettiva}, \}$ l'insieme $(\mathfrak{T}(A), \circ)$ è un gruppo.
Sappiamo che la composizione di applicazioni è associativa e che la composizione di due applicazioni bigettive è bigettiva, $\iota_A \in \mathfrak{T}(A), \forall\, A$, e vale $\iota_A \circ f = f = f \circ \iota_A$, infine, $\forall\, f \in \mathfrak{T}(A), \exists!\, f^{-1} \in \mathfrak{T}(A) : f^{-1} \circ f = \iota_A = f \circ f^{-1}$.
$(\mathfrak{T}(A), \circ)$ è detto *gruppo delle trasformazioni* o *gruppo simmetrico*[28] di A.

[28]Indicato anche $\Sigma(A)$.

Se $\#A = n, \Longrightarrow$ anziché $\mathfrak{T}(A)$, si scrive $\mathfrak{T}_n$ e $|\mathfrak{T}_n| = n!$, inoltre $\forall\, f \in \mathfrak{T}_n$, identificando gli elementi di A con i loro indici, è indicata con una tabella

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}$$

- Se $\#A = 1 \Longrightarrow \exists!\, f = \iota_A \in \mathfrak{T}(A)$,
- Se $\#A = 2 \Longrightarrow \exists!\, f \neq \iota_A \in \mathfrak{T}(A)$, i.e. $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$,
- Se $\#A = 3 \Longrightarrow \#\mathfrak{T}(A) = 6$ i.e.

$$\mathfrak{T}_3 = \left\{ \iota_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, h = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \right.$$
$$\left. k = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, l = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

Vale $f^2 = h^2 = k^2 = g^3 = \iota_3, g^2 = l$, e, per esempio, $k = g \circ f \neq f \circ g = h$, ossia in particolare, $\mathfrak{T}_3$ non è commutativo. Piú precisamente, si dimostra che $\mathfrak{T}_n$ è commutativo $\iff n \leq 2$.

(2) Si prova che su un insieme A con $\#A \leq 3$ esiste essenzialmente un'unica struttura di gruppo. Per esempio, se $A = \{a, b\}$ vale

	a	b
a	a	b
b	b	a

oppure

	a	b
a	b	a
b	a	b

i.e un elemento è l'identità e l'altro è l'inverso di se stesso, esempi concreti sono: $(\{0,1\}, +), (\{-1,1\}, \cdot), (\mathfrak{T}_2, \circ)$.

Similmente, se $A = \{a, b, c\}$ un elemento deve essere l'identità e gli altri due sono uno l'inverso dell'altro, ossia la tabella che dà la legge di composizione è

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

si ottiene un esempio concreto prendendo $a =$ rotazione di ampiezza $\frac{2\pi}{3}$ di un triangolo equilatero attorno al suo baricentro, $= a^2$.

(3) Su un insieme A con $\#A \leq 4$ esistono essenzialmente due strutture di gruppo, cioè:

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

oppure

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

si ottiene un esempio concreto per il primo prendendo $a =$ rotazione di ampiezza $\frac{2\pi}{4}$ di un quadrato attorno al suo centro ($b = a^2, c = a^3$), per il secondo considerando le simmetrie di un rettangolo (non quadrato!) attorno al suo centro.

Complessivamente, $\exists$ un solo gruppo di ordini $2, 3$, $\exists$ due gruppi distinti di ordine 4 (tutti commutativi).

OSSERVAZIONE **8.9.** (1) Nel Teor.8.6 (3) l'ipotesi $g * h = h * g$ è essenziale, infatti se, per esempio, $G = \mathfrak{T}_3$, $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, h = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ risulta $l = (f \circ h)^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f^2 \circ h^2 = \iota_3$, (si ha infatti $f \circ h \neq h \circ f$).

(2) Un gruppo $(G, *)$ è commutativo $\iff \forall\, h, g \in G$, vale $(h * g)^2 = h^2 * g^2$, chiaramente se vale $g * h = h * g, \forall\, h, g \in G$, si ha

$$(h*g)^2 = (h*g)*(h*g) = h*(g*h)*g = h*(h*g)*g = (h*h)*(g*g) = h^2*g^2,$$

viceversa, da $(h*g)*(h*g) = h^2*g^2$ moltiplicando ambo i membri a destra per h^{-1} e a sinistra per g^{-1} si ha

$$h^{-1} * (h * g) * (h * g) * g^{-1} = h^{-1} * (h^2 * g^2) * g^{-1} \text{ e quindi}$$

$$(h^{-1} * h) * (g * h) * (g * g^{-1}) = (h^{-1} * h) * (h * g) * (g * g^{-1}) \text{ i.e. } g * h = h * g.$$

DEFINIZIONE **8.10.** Un sottinsieme $\emptyset \neq H \subseteq G$ di un gruppo G si dice *sottogruppo di* G se H è gruppo rispetto alla legge di composizione di G.

Il sottinsieme $\{e\}$ di un gruppo G è detto *sottogruppo banale di* G, un sottogruppo $H \subset G$ è detto *sottogruppo proprio di* G, mentre $G \subseteq G$ è detto *sottogruppo improprio di* G.

PROPOSIZIONE **8.11.** *Un sottinsieme $H \subseteq G$ di un gruppo è un sottogruppo $\iff$ è chiuso rispetto alla legge di composizione di G, all'identità di G, all'inverso di G*[29]*.*

In particolare, un sottinsieme $\emptyset \neq H \subseteq G$ di un gruppo finito G è sottogruppo $\iff$ è chiuso rispetto alla legge di composizione di G.

Dim. Se H è un sottogruppo di G, per definizione esso è chiuso rispetto alla legge di composizione di G, inoltre $\exists$ un elemento neutro $e_H \in H$ per cui in particolare vale $e_H e_H = e_H$, poiché in G vale anche $e_H e = e_H$ si ha in G, $e_H e = e_H e_H$, da cui, per la legge di cancellazione $e_H = e$. Analogamente, $\forall\, h \in H$, $\exists h' \in H$ con $hh' = e_H = e$, da cui, moltiplicando a sinistra per l'inverso $h^{-1} \in G$ di h, si ottiene $h^{-1} = h'$. Viceversa, se H è chiuso rispetto alla legge di composizione di G, all'identità di G, all'inverso di G chiaramente H è un gruppo rispetto alla legge di composizione di G, ossia, è un sottogruppo di G.

In particolare, se $|G| < \aleph_0$, $\forall\, g \in G$ le potenze $g, g^2, g^3, \ldots$ non sono tutte distinte, pertanto $\exists \overline{m} := \min\{m \in \mathbb{N} : g^m = e\}$[30], pertanto $gg^{\overline{m}-1} = e \Longrightarrow g^{\overline{m}-1} = g^{-1}$. Quindi se $\emptyset \neq H \subseteq G$ è chiuso rispetto alla legge di composizione di G esso è anche chiuso rispetto all'identità di G e all'inverso di G.

ESEMPIO **8.12.** (1) $\mathbb{N} \subset \mathbb{Z}$ non è sottogruppo (vedi Es.8.2 (1)),

(2) $2\mathbb{Z} := \{2n : n \in \mathbb{Z}\}$ è un sottogruppo di $\mathbb{Z}$, infatti:
- $\mathbf{2}n + 2n' = 2(n + n') \in 2\mathbb{Z}$, $\forall\, 2n, 2n' \in 2\mathbb{Z}$,,
- $0 = 2 \cdot 0 \in 2\mathbb{Z}$,
- $\forall\, 2n \in 2\mathbb{Z}$, $\exists\, 2(-n) \in \mathbb{Z} : 2n + 2(-n) = 0$.

Analogamente, $\forall\, m \in \mathbb{N}$, $m\mathbb{Z} := \{mn : n \in \mathbb{Z}\}$ è un sottogruppo di $\mathbb{Z}$.

(3) Un sottinsieme $\emptyset \neq H \subseteq G$ di un gruppo G è un sottogruppo di G se $\forall\, h', h \in H$ si ha $h'h^{-1} \in H$.

---

[29] Ossia se $\forall\, h, h' \in H$, vale : $hh' \in H$, se $e \in H$, se $\forall\, h \in H \Longrightarrow h^{-1} \in H$.

[30] Tale minimo è detto *periodo di* g.

OSSERVAZIONE **8.13.** Dato un gruppo G

(1) se $H, K \subseteq G$ sono sottogruppi, anche $H \cap K$ è tale, infatti $\forall\, g', g \in H \cap K$ si ha $g'g^{-1} \in H \cap K$ essendo per ipotesi $g'g^{-1} \in H, g'g^{-1} \in K$;
piú in generale, se $\{H_i\}_{i\in I}$ è una famiglia arbitraria di sottogruppi di G, anche $\bigcap_{i\in I} H_i$ è tale;
(2) per contro, in generale, se $H, K \subseteq G$ sono sottogruppi, $H \cup K$ non è sottogruppo, per esempio, dati $2\mathbb{Z}, 3\mathbb{Z} \subset \mathbb{Z}, 2\mathbb{Z} \cup 3\mathbb{Z}$ non è un sottogruppo, e.g $5 = 2 + 3 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.
(3) Sia $\{H_i\}_{i\in I}$ una famiglia di sottogruppi di G tali che $\forall\, i, j \in I$ si abbia $H_i \subseteq H_j$ oppure $H_j \subseteq H_i, \Longrightarrow H := \bigcup_{i\in I} H_i$ è un sottogruppo di G infatti $\emptyset \neq H$, siano $x, y \in H \Longrightarrow \exists\, \bar{i}, \tilde{j} \in I : x \in H_{\bar{i}}, y \in H_{\tilde{j}}$, siccome per ipotesi si ha $H_{\bar{i}} \subseteq H_{\tilde{j}}$ o $H_{\tilde{j}} \subseteq H_{\bar{i}}$, supponendo e.g. $H_{\bar{i}} \subseteq H_{\tilde{j}}$ si ha $x, y \in H_{\tilde{j}}$, ma allora, essendo $H_{\tilde{j}}$ sottogruppo, $xy^{-1} \in H_{\tilde{j}}$ e quindi $xy^{-1} \in H$, $\forall\, x, y \in H$.
(4) sia $X \in \mathcal{P}(G)$ un sottinsieme qualsiasi,
   - sia $\{H_i\}_{i\in I}$ la famiglia dei sottogruppi di G tali che $X \subseteq H_i$, $\forall\, i \in I$ (n.b. $\{H_i\}_{i\in I}$ è una famiglia non vuota essendo $G \in \{H_i\}_{i\in I}$), pertanto, $T_X := \bigcap_{i\in I} H_i$ è il piú piccolo sottogruppo di G contenente X (perché?) ed è detto *sottogruppo generato da* X;
   - l'insieme $Y := \{y_1 \cdots y_n : n > 0, y_i \in X \text{ o } y_i^{-1} \in X, \forall\, 1 \leq i \leq n\}$ è chiuso rispetto all'identità, all'inverso e al prodotto, pertanto è un sottogruppo di G e contiene X, d'altra parte, $\forall\, X \subseteq H$, con $H \subseteq G$ sottogruppo risulta $Y \subseteq H$, ossia $Y = T_X$.
   - se vale $T_X = G$, X dicesi *sistema di generatori* di G.

ESEMPIO **8.14.** Trovare un sistema di generatori di:

(1) $2\mathbb{Z} \cup 3\mathbb{Z}$,
(2) $4\mathbb{Z} \cup 6\mathbb{Z}$,
(3) $\mathfrak{T}_3$.

DEFINIZIONE **8.15.** In un gruppo G, $\forall\, g \in G$, l'insieme $< g >:= \{g^n : n \in \mathbb{Z}\}$ è un sottogruppo di G che è commutativo, qualunque sia G ed è detto *sottogruppo ciclico generato da* g; se $< g >$ è un gruppo finito, il suo ordine è detto *periodo* di g e denotato $\pi(g)$.

Se $\exists\, x \in G$ tale che $G =< x >$, allora il gruppo G è detto *ciclico* e l'elemento x, è detto *generatore di* G.

ESEMPIO **8.16.**
(1) $\mathbb{Z}$ è un gruppo ciclico infinito generato da 1 e -1.
(2) Ogni sottogruppo di $\mathbb{Z}$ è della forma $m\mathbb{Z}$ e quindi è ciclico e piú in generale ogni sottogruppo di un gruppo ciclico infinito generato da un $g \in G$ è della forma $< g^m >$ per qualche $m \in \mathbb{Z}$.
(3) Ogni gruppo ciclico è commutativo.
(4) In un gruppo ciclico G di ordine n e generatore g (i.e. $g^n = e_G$ ogni sottogruppo $H \subseteq G$ è ciclico con generatore g^k con $k|n$ e $\pi(g^k) = \frac{n}{k}$.
(5) se $\#A \geq 3, \mathfrak{T}(A)$ non è ciclico.

(6) I gruppi finiti (non ciclici) hanno *insiemi di relazioni di definizione* sull'insieme dei generatori[31].
(7) $\forall\, n \in \mathbb{N} \setminus \{0,1,2\}$, il gruppo Δ_n, di ordine $2n$ con due generatori ρ, τ soddisfacenti le relazioni: $\rho^n = e_{\Delta_n} = \tau^2, \tau\rho = \rho^{-1}\tau$[32] è detto *n-gruppo diedrale* ed "è" il gruppo delle simmetrie di un poligono regolare di n lati.
(8) Il gruppo Q di ordine 8 con due generatori a e b soddisfacenti le relazioni $a^4 = e_Q, a^2 = b^2, b^{-1}ab = a^{-1}$ è detto *gruppo dei quaternioni*.

Osservazione **8.17.** Dato un sottogruppo $H \subseteq G$ di un gruppo G, al variare di $g \in G$, la totalità degli insiemi non vuoti

$$gH := \{gh : h \in H\} \,(\text{risp. } Hg := \{hg : h \in H\})$$

dà una partizione di G (basta provarlo per gli insiemi gH perché la situazione è simmetrica). L'ipotesi H sottogruppo significa in particolare che $e_G \in H$, cosí $\forall\, g \in G, g \in gH$, i.e. $\bigcap_{g\in G} gH = G$. Verifichiamo che gli insiemi gH sono a due a due disgiunti: dati $g, g' \in G$ si ha:

$$x \in gH \cap g'H \iff \exists\, h,k \in H : x = gh = g'k, \Longrightarrow hk^{-1} = g^{-1}g', \text{ ossia } g^{-1}g' \in H,$$

pertanto, $\exists\, \ell \in H$ con $g^{-1}g' = \ell \Longrightarrow g' = g\ell$, i.e. $gH = g'H$.

Definizione **8.18.** Se $(G, *), (G', *')$ sono due gruppi il *(gruppo) prodotto di G e G'* è l'insieme $G \times G'$ (prodotto cartesiano degli insiemi G e G' con la legge di composizione $\square$ definita da:

$$(g, g')\square(h, h') := (g * h, g' *' h').$$

Esempio **8.19.** Il prodotto E di due gruppi ciclici $B =< b >$ e $C =< c >$, con $|B| = n$ e $|C| = m$ è generato da $\beta := (b, e_C)$ con $\beta^n = e_E, \gamma := (e_B, c)$ con $\gamma^m = e_E$ e $\beta\gamma = \gamma\beta$[33], inoltre $|E| = nm$.

Definizione **8.20.** Ogni sottogruppo G del gruppo delle trasformazioni $\mathfrak{T}(A)$ di un insieme A è detto *gruppo di trasformazioni di A*.
In particolare, per ogni $a \in A$ l'insieme $\{\varphi \in \mathfrak{T}(A) : \varphi(a) = a\}$ è un gruppo di trasformazioni di A, detto *stabilizzatore di a*.

Osservazione **8.21.** Dato un sottogruppo $H \subseteq G$, di un gruppo G, al variare di $g \in G$, la totalità degli insiemi non vuoti

$$gH := \{gh : h \in H\} \,(\text{risp. } Hg := \{hg : h \in H\})$$

dà una partizione di G (basta provarlo per gli insiemi gH perché la situazione è simmetrica). L'ipotesi H sottogruppo significa in particolare che $e_G \in H$, cosí $\forall\, g \in G, g \in gH$ i.e. $\bigcap_{g\in G} gH = G$. Verifichiamo che gli insiemi gH sono a due a due disgiunti: dati $g, g' \in G$ si ha:

$$x \in gH \cap g'H \iff \exists\, h,k \in H : x = gh = g'k, \Longrightarrow hk^{-1} = g^{-1}g', \text{ ossia } g^{-1}g' \in H,$$

pertanto, $\exists\, \ell \in H$ con $g^{-1}g' = \ell \Longrightarrow g' = g\ell$ i.e. $gH = g'H$.

---

[31] I gruppi ciclici finiti sono precisamente quelli per cui $\exists$ insiemi di generatori consistenti in un solo elemento e insiemi di relazioni anch'essi consistenti in un solo elemento.

[32] Essendo $\rho^n = e_{\Delta_n} \Longrightarrow \rho^{-1} = \rho^{n-1}$, la terza relazione può anche essere scritta: $\tau\rho = \rho^{n-1}\tau$.

[33] In particolare, quindi è commutativo non ciclico!

DEFINIZIONE **8.22.** Dati un gruppo G e un suo sottogruppo $H \subseteq G$, gli insiemi gH (risp. Hg, di Oss.8.21 sono detti *classi laterali sinistre* (risp. *destre*) di G modulo H e la partizione da esse individuate è denotata G/H[34].

OSSERVAZIONE **8.23.** Se il gruppo G non è abeliano e $H \subseteq G$ è un sottogruppo G, in generale $gH \neq Hg$.
e.g siano $G = \mathfrak{T}_3, f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ e $H =< f >= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$, se $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ si ha $gH = \{g, k\} \neq \{g, h\} = Hg$.

TEOREMA **8.24.** *L'ordine di un sottogruppo $H \subseteq G$ di un gruppo finito G è un divisore di $|G|$.*

Dim. Sia $H \subseteq G$ il sottogruppo e sia m il suo ordine che è finito perché $|G|$ è finito per ipotesi, possiamo supporre che H non sia banale perché 1 divide qualsiasi numero. Poiché se $h, k \in H, h \neq k$, vale $gh \neq gk$, ogni gH ha m elementi. Sia d il numero delle classi laterali (sinistre) distinte[35], poiché per Oss. 8.21 le $\{gH\}_{g \in G}$ dànno una partizione di G, vale $md = |G|$.

COROLLARIO **8.25.** *Un gruppo (finito) G tale che $|G|$ è un numero primo è ciclico.*

Dim. Per ogni $e_G \neq g \in G$ il sottogruppo $< g >$ coincide con G perché i soli divisori di $|G|$ sono 1 e $|G|$ stesso e per ipotesi $< g > \neq < e_G >$.

OSSERVAZIONE **8.26.** Un gruppo G privo di sottogruppi propri è ciclico di ordine primo[36]. Se infatti G non fosse ciclico, $\exists\, g \in G$ con $< g > \subset G$ (altrimenti G sarebbe sarebbe ciclico). Supponiamo allora che G sia ciclico infinito con generatore x, dall'essere le potenze $e_G, x, x^2, \ldots, x^n, \ldots$ tutte distinte, discenderebbe che $\forall\, h \in \mathbb{Z} \setminus \{1, -1\}$ il sottogruppo $< x^h > \subset G$ sarebbe proprio, se infine G fosse ciclico di ordine non primo m e generatore $x, \forall\, h$ divisore di m, il sottogruppo $< x^h > \subset G$ sarebbe proprio.

DEFINIZIONE **8.27.** Un sottogruppo $H \subseteq G$, è detto *invariante* o *normale* se ogni classe laterale sinistra di G modulo H è contenuta in una classe laterale destra [37]. Per indicare che $H \subseteq G$, è sottogruppo invariante, si scrive talvolta $H \subset| G$,

ESEMPIO **8.28.**
(1) Se G è abeliano ogni suo sottogruppo è invariante.
(2) $H =< f > \subset \mathfrak{T}_3$ non è invariante.
(3) Per ogni sottogruppo $H \subseteq G$, $N_G(H) := \{g \in G : gHg^{-1} = H\}$ è un sottogruppo invariante di G, detto *normalizzatore di* H e $H \subseteq N_G(H)$ è sottogruppo invariante
(4) Per ogni gruppo G, $Z(G) := \{a \in G : ag = ga, \forall\, g \in G\}$ è un sottogruppo invariante di G, detto *centro di* G e G è abeliano $\iff G = Z(G)$,

---

[34] Qual è la relazione di equivalenza corrispondente alla partizione gH al variare di $g \in G$?

[35] Poiché $|G| < \aleph_0$ implica $\#\mathcal{P}(G) < \aleph_0$, si ha $d < \aleph_0$.

[36] In particolare G è finito.

[37] i.e. $\forall\, g \in G, \exists g' \in G : gH \subseteq Hg'$, ossia, $g = kg'$ per qualche $k \in H, \Longrightarrow g' = k^{-1}g$ e quindi da $gH \subseteq Hg'$ si ricava $gH \subseteq Hk^{-1}g = Hg$, ossia, $H \subseteq G$, è invariante $\iff gH \subseteq Hg, \forall\, g \in G, \Longrightarrow H \subseteq g^{-1}Hg, H \subseteq gHg^{-1} \Longrightarrow H \subseteq g^{-1}Hg$ e quindi $H = g^{-1}Hg, \forall g \in G$ e questo equivale infine a $gH = Hg, \forall g \in G$.

DEFINIZIONE **8.29.** Dato un gruppo $G, \forall\,(X,Y) \in \mathcal{P}(G)\times\mathcal{P}(G)$ il *prodotto* o *composto* di X e Y è l'insieme

$$XY := \{xy \in G :\ x \in X, y \in Y\} \in \mathcal{P}(G).$$

PROPOSIZIONE **8.30.** *Se $H \subseteq G$ è un sottogruppo normale, l'insieme $G/H \subseteq \mathcal{P}(G)$ costituito dalla totalità delle classi laterali di G modulo H*[38] *è un gruppo rispetto al prodotto di sottinsiemi e G/H è detto* gruppo residuo *o* quoziente *di G modulo H.*

Dim. Il prodotto di due classi laterali è una classe laterale: $\forall\, gH, g'H \in G/H$ vale

$$(gH)(g'H) = g(Hg')H = g(g'H)H = gg'H \in G/H,$$

tale prodotto è associativo, infatti $\forall\, gH, g'H, g"H \in G/H$ vale

$$\begin{aligned} gH[(g'H)(g"H)] &= (gH)(g'g"H) = g(g'g")H = (gg')g"H = (gg'H)(g"H) = \\ &= [(gH)(g'H)]g"H. \end{aligned}$$

$\exists$ identità sinistra $H = e_GH$,infatti $(e_GH)(gH) = (e_Gg)H = gH$, $\forall\, gH \in G/H$;
$\exists$ reciproco sinistro, infatti $\forall\, gH \in G/H$ la clase laterale $g^{-1}H \in G/H$ soddisfa $(gH)(g^{-1}H) = gg^{-1}H = e_GH = H$.

DEFINIZIONE **8.31.** Se $H \subseteq G$ è un sottogruppo normale, l'ordine del gruppo G/H è detto *indice* di H in G e denotato $[G : H]$.

ESERCIZIO **8.32.** (1) Risulta dalle definizioni che $\forall\, n \in \mathbb{Z}$, $n\mathbb{Z}$ ha indice n in $\mathbb{Z}$ e precisamente:

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

(2) Provare che per ogni gruppo G, un sottogruppo $H \subset G$ con $[G : H] = 2$ è normale.
(3) Determinare tutti i sottogruppi di $\mathbb{Z}/12\mathbb{Z}$.

DEFINIZIONE **8.33.** Dati due gruppi $(G, *), (K, \square)$ un'applicazione $\varphi : G \longrightarrow K$ è un *omomorfismo di gruppi* se vale:

$$\varphi(g * g') = \varphi(g)\square\varphi(g'),\ \forall\ g, g' \in G.$$

OSSERVAZIONE **8.34.** (1) Per ogni omomorfismo di gruppi $\varphi : G \longrightarrow K$ risulta $\varphi(e_G) = e_K$, basta infatti, applicare la legge di cancellazione (tra elementi di K) all'identità $\varphi(e_G) = \varphi(e_Ge_G) = \varphi(e_G)\varphi(e_G)$.
Inoltre, $\forall\, g \in G$, risulta $\varphi(g^{-1}) = \varphi(g)^{-1}$, vale infatti $e_K = \varphi(e_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$, da cui la tesi per l'unicità dell'inverso.
(2) Se $H \subseteq G$ è un sottogruppo normale, la proiezione canonica:

$$\pi : G \longrightarrow G/H \text{ definita da } \pi(g) := [g] = gH,\ \forall\, g \in G$$

è un omomorfismo di gruppi. Da Prop.8.30 sappiamo che G/H è un gruppo, e che vale $\pi(gg') = gg'H = (gH)(g'H) = \pi(g)\pi(g')$.

ESERCIZIO **8.35.** (1) Siano $\varphi_i : \mathbb{Z} \longrightarrow \mathbb{Z}$, al variare di $i \in \underline{3}^*$ definite da:
- $\varphi_1(n) = kn$, $\forall n \in \mathbb{Z}$, per qualche $k \in \mathbb{N}$ fissato;
- $\varphi_2(n) = n + h$, $\forall n \in \mathbb{Z}$, per qualche $h \in \mathbb{N}$ fissato;
- $\varphi_3(n) = n^3$, $\forall n \in \mathbb{Z}$;

[38] Essendo H normale in G, le classi laterali destre e sinistre coincidono.

determinare per quali $i \in \underline{5}^*, \varphi_i$ è un omomorfismo di gruppi.

(2) $\forall\, m \in \mathbb{Z}$, studiare la proiezione canonica $\pi_m : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$.

(3) Provare che se G è un gruppo finito, l'unico omomorfismo $\varphi : G \longrightarrow \mathbb{Z}$ è l'omomorfismo nullo.

(4) Studiare gli omomorfismi $\varphi : \mathbb{Z} \longrightarrow \mathfrak{T}_3$.

DEFINIZIONE **8.36.** (1) - Un omomorfismo di gruppi $\varphi : G \longrightarrow K$ è detto *isomorfismo* se è iniettivo e surgettivo;

- un omomorfismo di un gruppo G in sé è detto *endomorfismo* di G , un isomorfismo di un gruppo G in sé è detto *automorfismo* di G;
- gli automorfismi di un gruppo G in sé formano un gruppo rispetto a $\circ$ (la composizione di applicazioni), denotato $\mathrm{Aut}(G)$;
- per ogni gruppo G l'applicazione $\varphi_h : G \longrightarrow G$, definita da $\varphi_h(g) = hgh^{-1}$, per qualche $h \in G$, è un automorfismo di G detto *automorfismo interno individuato da* h;

(2) Per ogni omomorfismo di gruppi $\varphi : G \longrightarrow K$,

- $\mathrm{im}\ \varphi := \{y \in K : y = \varphi(g), \text{per qualche} \, g \in G\}$ è un sottogruppo di K, infatti $y, y' \in \mathrm{im}\ \varphi, \iff \exists\, x, x' \in G : y = \varphi(x), y' = \varphi(x')$ e vale $y'y^{-1} = \varphi(x')(\varphi(x))^{-1} = \varphi(x')\varphi(x^{-1}) = \varphi(xx^{-1}) \in \mathrm{im}\ \varphi$;
- $\ker \varphi := \{g \in G : \varphi(g) = e_K\}$ è un sottogruppo (invariante) di G, detto *nucleo* di φ, infatti $x, x' \in \ker \varphi, \iff \varphi(x) = \varphi(x') = e_K$ e vale $\varphi(x'x^{-1}) = \varphi(x')\varphi(x^{-1}) = \varphi(x')(\varphi(x))^{-1} = e_K e_K = e_K$, cioè $xx' \in \ker \varphi$.

OSSERVAZIONE **8.37.** (1) L'applicazione bigettiva di un gruppo G in sé definita da $\varphi(g) = g^{-1}$ è un automorfismo di gruppi se e solo se G è commutativo, infatti se G è commutativo vale $gh = hg, \forall g, h \in G$ e quindi $\varphi(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \varphi(g)\varphi(h)$, se vale $h^{-1}g^{-1} = (gh)^{-1} = \varphi(gh) = \varphi(g)\varphi(h) = g^{-1}h^{-1}$, $\forall g, h \in G$, moltiplicando $h^{-1}g^{-1} = g^{-1}h^{-1}$ a sinistra per g, si ottiene $gh^{-1}g^{-1} = h^{-1}$, da cui moltiplicando a destra per g, si ottiene $gh^{-1} = h^{-1}g$, da cui moltiplicando a destra per h si ottiene $g = h^{-1}gh$, da cui moltiplicando a sinistra per h si ottiene $hg = gh$,

(2) un omomorfismo di gruppi $\varphi : G \longrightarrow K$ è iniettivo $\iff \ker \varphi = \{e_G\}$, chiaramente basta dimostrare che $\ker \varphi = \{e_G\} \Longrightarrow \varphi$ è iniettivo, se $\varphi(g) = \varphi(g')$, vale $\varphi(gg'^{-1}) = \varphi(g)\varphi(g'^{-1}) = \varphi(g)\varphi(g')^{-1} = \varphi(g)\varphi(g)^{-1} = e_K$ e quindi $gg'^{-1} = e_G$, ossia $g = g'$, i.e φ iniettivo.

ESERCIZIO **8.38.** (1) Sia $\varphi : \mathbb{R} \longrightarrow \mathbb{Z}$ un omomorfismo di gruppi, provare che se $\ker \varphi \neq \mathbb{Z}, \Longrightarrow \varphi$, è iniettivo.

(2) Sia $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ un endomorfismo, è vero che φ surgettivo $\Longrightarrow \varphi$ automorfismo? φ iniettivo $\Longrightarrow \varphi$ automorfismo?

(3) Provare che ogni gruppo ciclico infinito G è isomorfo a $\mathbb{Z}$[39].

[39]Pertanto se $g \in G$ è un generatore, G ha solo g^{-1} come altro generatore.

9. Anelli e campi

In ciascuno degli insiemi $X = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ oltre all'addizione $+$, rispetto alla quale essi sono gruppi commutativi, è definita una seconda operazione, detta *moltiplicazione* e indicata $\cdot$. La moltiplicazione è:

- associativa: i.e. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, $\forall\, x, y, z \in X$,
- commutativa: i.e. $x \cdot y = y \cdot x, \forall\, x, y \in X$,
- legata all'addizione dalla *distributività del prodotto rispetto alla somma*: i.e.

$$x \cdot (y + z) = x \cdot y + x \cdot z,\ \forall\, x, y, z \in X.$$

Inoltre $\exists\ 1 \in X$ tale che:

- $1 \cdot x = x, \forall\, x \in X$.

Definizione **9.1.** Un *anello* A è un insieme con due leggi di composizione dette *addizione* e *moltiplicazione* e indicate rispettivamente $+$ e $\cdot$, soddisfacenti i seguenti assiomi:

- A è un gruppo abeliano (denotato $(A, +)$) rispetto a $+$ la cui identità è denotata 0,
- $\cdot$ è associativa,
- si ha *distributività del prodotto rispetto alla somma*: i.e.

$$x \cdot (y + z) = x \cdot y + x \cdot z,\ \forall\, x, y, z \in X,$$
$$(y + z) \cdot x = y \cdot x + z \cdot x,\ \forall\, x, y, z \in X.$$

n.b.: differenza di quanto accade negli insiemi numerici non si richiede che la moltiplicazione sia commutativa, ossia che valga $x \cdot y = y \cdot x, \forall\, x, y \in A$, se la moltiplicazione è commutativa, le due condizioni di distributività del prodotto (a destra e a sinistra) rispetto alla somma sono equivalenti e l'anello è detto *commutativo*.

Un elemento $\alpha \in A$ è un'*identità sinistra* (risp. *destra*) se $\alpha \cdot a = a$ (risp. $a\alpha = a$) $\forall\, a \in A$, è un'*identità*[40] se è sia identità sinistra che destra.

Lemma **9.2.** *Se un anello A ha identità sinistra α e identità destra $\beta \Longrightarrow \alpha = \beta$ è l'unica identità di A, ossia A non possiede altre identità né sinistre né destre. L'identità (moltiplicativa) di un anello è indicata semplicemente 1 (o anche 1_A).*

Dim. Si ha $\beta = \alpha \cdot \beta = \alpha$, se α' è un'altra identità sinistra essendo anche $\beta = \alpha' \cdot \beta = \alpha'$ discende $\alpha = \alpha'$.

Esempio **9.3.**
(1) $(\mathbb{N}, +, \cdot)$ non è un anello,
(2) $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sono anelli commutativi con 1,
(3) L'insieme $M_n(\mathbb{R})$ delle matrici quadrate a elementi in $\mathbb{R}$ è un anello con 1, non commutativo, rispetto all'addizione e alla moltiplicazione righe per colonne di matrici.

Osservazione **9.4.**
(1) Di solito si considerano anelli con identità.
(2) In un anello $A, \forall\, a \in A$ si ha $0 \cdot a = a \cdot 0 = 0$, infatti, da $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$, da cui per la legge di cancellazione nel gruppo $(A, +)$, $0 = 0 \cdot a$.
(3) In un anello $A, \forall\, a, b \in A$ si ha $(-a) \cdot b = a \cdot (-b) = -a \cdot b$, infatti vale $(-a) \cdot b + a \cdot b = (-a + a) \cdot b = 0 \cdot b = 0$, ossia $(-a) \cdot b = -a \cdot b$ e analogamente per $a \cdot (-b)$.

[40] $2\mathbb{Z}$ è un anello senza identità né sinistra né destra.

DEFINIZIONE **9.5.** Un elemento $0 \neq a$ di un anello A per cui $\exists\, A \ni b \neq 0$ tale che $a \cdot b = 0$ (risp. $b \cdot a = 0$) è detto *divisore sinistro* (risp. *destro) di* 0*, divisore di* 0 se è sia divisore sinistro che destro di 0.

Un anello commutativo (con identità) e privo di divisori di zero è detto *dominio di integrità*

ESEMPIO **9.6.** (1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono domini di integrità[41].

(2) $\forall\, n \in \mathbb{N}^*, \mathbb{Z}/n\mathbb{Z}$ è un dominio di integrità $\iff$ n è primo.

(3) per ogni anello A, l'insieme $\mathcal{F}_A := \{f : A \longrightarrow A\}$ delle applicazioni di A in sé con le operazioni $+$ e $\cdot$, definite $\forall\, f, g \in \mathcal{F}_A, \forall\, x \in A$ da:
- $(f+g)(x) := f(x) + g(x)$,
- $(f \cdot g)(x) := f(x) \cdot g(x)$.

è un anello (commutativo se A è tale) non integro.
Per l'addizione valgono $\forall\, f, g, h \in \mathcal{F}_A$:
- $(f+g)+h = f+(g+h)$, infatti $[(f+g)+h](x) = (f+g)(x)+h(x) = f(x)+g(x)+h(x) = f(x)+(g+h)(x) = [f+(g+h)](x)$,
- $\exists\, 0 : 0+f = f$, infatti l'applicazione nulla (definita da $x \mapsto 0_A, \forall\, x \in A$) soddisfa $(0+f)(x) = 0_A + f(x) = f(x)$,
- $\exists\, -f$ tale che $f + (-f) = 0$ infatti l'applicazione $-f$ (definita da $x \mapsto -f(x), \forall\, x \in A$) soddisfa $((-f)+f)(x) = -f(x) + f(x) = 0_A$,
- $(f+g) = (g+f)$, infatti $(f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x)$.

Per la moltiplicazione valgono $\forall\, f, g, h \in \mathcal{F}_A$:
- $(f \cdot g) \cdot h = f \cdot (g \cdot h)$, infatti $[(f \cdot g) \cdot h](x) = (f \cdot g)(x) \cdot h(x) = f(x) \cdot g(x) \cdot h(x) = f(x) \cdot (g \cdot h)(x) = [f \cdot (g \cdot h)](x)$,
- $\exists\, 1 : 1 \cdot f = f$, infatti l'applicazione $1 : A \longrightarrow A$ definita da $x \mapsto 1_A, \forall\, x \in A$ soddisfa $(1 \cdot f)(x) = 1_A \cdot f(x) = f(x)$,
- $(f+g) \cdot h = f \cdot h + g \cdot h$ e $h \cdot (f+g) = h \cdot f + h \cdot g$ infatti per esempio $[(f+g) \cdot h](x) = (f+g)(x) \cdot h(x) = [f(x) + g(x)] \cdot h(x) = f(x) \cdot h(x) + g(x) \cdot h(x) = [f \cdot h + g \cdot h](x)$.

Inoltre, se A è commutativo,
- $f \cdot g = g \cdot f$, infatti $(f \cdot g)(x) = f(x) \cdot g(x) = g(x) \cdot f(x) = (g \cdot f)(x)$

Infine, $\forall\, X \in \mathcal{P}(A), \emptyset \neq X \neq A$ se $\kappa_X, \kappa_{\mathcal{C}_A(X)}$ sono funzioni caratteristiche, vale $\kappa_X \cdot \kappa_{\mathcal{C}_A(X)} = 0$ con $\kappa_X \neq 0$ e $\kappa_{\mathcal{C}_A(X)} \neq 0$.

DEFINIZIONE **9.7.** Un *sottoanello* di un anello A è un $B \in \mathcal{P}(A)$ che è anello rispetto alle operazioni di A.

ESEMPIO **9.8.** Via l'inclusione canonica $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$, definita da $\iota(n) = [\frac{n}{1}], \forall\, n \in \mathbb{Z}, \mathbb{Z}$ è un sottoanello di $\mathbb{Q}$, e similmente $\mathbb{Q}$ è un sottoanello di $\mathbb{R}$.

DEFINIZIONE **9.9.** Un *campo* o *corpo commutativo* è un anello commutativo A tale che $(A^*, \cdot)$ sia un gruppo.

ESEMPIO **9.10.** (1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono campi, mentre $\mathbb{Z}$ non lo è.

(2) Ogni campo $\mathbf{k}$ è un dominio di integrità, infatti se $0 \neq x \in \mathbf{k}$ soddisfa $x \cdot y = 0$, moltiplicando $x \cdot y = 0$ a sinistra per x^{-1} si ottiene $x^{-1} \cdot x \cdot y = x^{-1} \cdot 0 = 0$ i.e $y = 0$, ma non vale il viceversa ossia esistono domini di integrità (e.g. $\mathbb{Z}$ che non sono campi) .

[41] n.b.$(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$ sono gruppi a differenza di $(\mathbb{Z}^*, \cdot)$.

DEFINIZIONE **9.11.** In un anello con identità A un elemento u per cui $\exists\, A \ni v \neq 0$ tale che $u \cdot v = 1_A$ è detto *unità* o *elemento invertibile*, l'insieme delle unità di A è denotato $U(A)$.

ESEMPIO **9.12.** (1) In un campo $\mathbf{k}$, $U(\mathbf{k}) = \mathbf{k}^*$,
(2) $U(\mathbb{Z}) = \{1, -1\}$
(3) $U(M_n(\mathbf{k})) = \{A \in M_n(\mathbf{k}) : \det(A) \neq 0\}$.

DEFINIZIONE **9.13.** (1) Un *omomorfismo* di anelli con identità (risp. campi) è un'applicazione $\varphi : A \longrightarrow A'$ tra due anelli (risp. campi) compatibile con le leggi di composizione, cioè $\forall\, a, b \in A$:
- $\varphi(a + b) = \varphi(a) + \varphi(b)$,
- $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$,
- $\varphi(1_A) = 1_{A'}$.

(2) Un *isomorfismo* di anelli con identità (risp. campi) è un omomorfismo bigettivo.
(3) Il *nucleo* di un omomorfismo di anelli con identità (risp. campi) $\varphi : A \longrightarrow A'$ è $\ker(\varphi) := \{a \in A : \varphi(a) = 0_{A'}\}$.

ESERCIZIO **9.14.** Dire quali fra le seguenti applicazioni sono omomorfismi di anelli:
(1) $\mathbb{Z} \longrightarrow \mathbb{Z}$ definita da $n \mapsto n + 1$,
(2) $\mathbb{Z} \longrightarrow \mathbb{Z}$ definita da $n \mapsto an$ con $a \in \mathbb{Z}$ fissato,
(3) $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ definita da $(n, m) \mapsto n + m$,
(4) $A \longrightarrow A$ definita da

$$\varphi(a) = \begin{cases} a^{-1} & \text{se } a \in U(A) \\ a & \text{altrimenti} \end{cases}$$ [42],

(5) $\mathbb{C} \longrightarrow \mathbb{C}$ definita da $z \mapsto \overline{z}$.

PROPOSIZIONE **9.15.** *Per ogni anello arbitrario A, $\exists!$ omomorfismo $\varphi : \mathbb{Z} \longrightarrow A$, dato dall'applicazione definita da $\varphi(n) = n1_A = \underbrace{1_A + \cdots + 1_A}_{n-volte}$, se $n > 0$, $\varphi(0) = 0$, $\varphi(n) = (-n)(-1_A) = \underbrace{-1_A + \cdots + (-1_A)}_{-n-volte}$, se $n < 0$.*

Dim. Si verifica che valgono tutte le tre condizioni di Def. 9.13.

DEFINIZIONE **9.16.** Un *ideale* di un anello A è un sottinsieme $I \subseteq A$ con le proprietà:
(1) I è un sottogruppo di $(A, +)$,
(2) $\forall\, a \in I$ e $\forall\, r \in A$ risulta $ar \in I$.

ESEMPIO **9.17.** (1) In un campo $\mathbf{k}$ i soli ideali sono $\{0\}$[43] e $\mathbf{k}$,
(2) per ogni omomorfismo di anelli $\varphi : A \longrightarrow A', \ker\varphi$ è un ideale di A,
(3) un omomorfismo di anelli $\varphi : A \longrightarrow A'$ è iniettivo $\iff \ker\varphi = (0_A)$.
(4) un omomorfismo di un campo $\mathbf{k}$ in un anello nonnullo A è iniettivo o nullo.

DEFINIZIONE **9.18.** (1) Un ideale I di un anello A è *pricipale* se $\exists\, a \in A$ tale che $I = (a) := \{ax : x \in A\}$;
(2) Un ideale I di un anello A è *primo* se $xy \in I, x \notin I$ implica $y \in I$;

[42] Dire se $\exists$ anelli A per i quali φ sia omomorfismo, se si quali.
[43] Per indicare la struttura di ideale anziché $\{0\}$ si scrive (0).

(3) Un ideale I di un anello A è *massimale* se non è contenuto in nessun ideale proprio.

ESEMPIO **9.19.** In $\mathbb{Z}$ ogni ideale è principale della forma $m\mathbb{Z}$, per qualche $m \in \mathbb{Z}$, gli ideali primi nonnulli sono tutti massimali della forma $p\mathbb{Z}$ per qualche primo $p \in \mathbb{N}$.

DEFINIZIONE **9.20.** *La* caratteristica *di un anello è l'intero non negativo n che genera il nucleo dell'omomorfismo di Prop.9.15.*

ESEMPIO **9.21.** (1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *hanno tutti caratteristica* 0,
(2) $\mathbb{Z}/n\mathbb{Z}$ *ha caratteristica* n.

BINOMIO DI NEWTON **9.22.** *Per ogni $x, y \in \mathbf{k}$*[44] *si ha*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Dim. Si ha : $(x+y)^1 = x+y = \sum_{k=0}^{1} \binom{1}{k} x^{1-k} y^k = \binom{1}{0} x^1 y^0 + \binom{1}{1} x^0 y^1$, supponiamo di avere dimostrato che $(x+y)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-1-k} y^k$ e deduciamone che allora $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$, si ha

$$(x+y)^n = (x+y)(x+y)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-k} y^k + \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-1-k} y^{k+1} =$$

$= \binom{n-1}{0} x^n y^0 + \binom{n-1}{1} x^{n-1} y^1 + \cdots \binom{n-1}{n-1} x^1 y^{n-1} + \binom{n-1}{0} x^{n-1} y^1 + \binom{n-1}{1} x^{n-2} y^2 + \cdots \binom{n-1}{n-1} x^0 y^n =$
$= \binom{n-1}{0} x^n y^0 + [\binom{n-1}{1} + \binom{n-1}{0}] x^{n-1} y^1 + [\binom{n-1}{2} + \binom{n-1}{1}] x^{n-2} y^2 + \cdots [\binom{n-1}{n-1} + \binom{n-1}{n-2}] x^1 y^{n-1} + \cdots \binom{n-1}{n-1} x^0 y^n =$
$= \binom{n}{0} x^n y^0 + \binom{n}{1} x^{n-1} y^1 + \binom{n}{2} x^{n-2} y^2 + \cdots + \binom{n}{n-1} x^1 y^{n-1} + \binom{n}{n} x^0 y^n.$

OSSERVAZIONE **9.23.** Il binomio di Newton fornisce un metodo esplicito per calcolare il numero di tutti i sottinsiemi di un insieme di n elementi (ossia $\#2^{\underline{n}^*}$), si ha infatti $(1+1)^n = \sum_{k=0}^{n} \binom{n}{k}$.

10. Anelli di polinomi a coefficienti in un anello A

DEFINIZIONE **10.1.** Dato un anello A (con identità 1_A)[45]

(1) Un' *indeterminata* su A è un elemento $X \notin A$ tale che $X^n \neq X^m, \forall\, n \neq m \in \mathbb{N}^*, X^0 = 1$.
(2) Un *polinomio in una indeterminata* X a coefficienti in A è una combinazione lineare (a coefficienti in A) delle potenze di X, ossia è un'espressione formale

$$P(X) = \sum_{i=0}^{n} a_i X^i = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n, a_i \in \mathbf{k}, n \in \mathbb{N}.$$

(3) Due polinomi $P(X) = \sum_{i=0}^{n} a_i X^i, Q(X) = \sum_{i=0}^{m} b_i X^i$ sono *uguali* se vale $m = n, a_i = b_i, \forall\, i \in \underline{n}^*$ *(Principio di identità dei polinomi).*

[44] $\mathbf{k}$ campo di caratteristica 0.
[45] Per comodità scriveremo 1 anziché 1_A.

(4) Dato un polinomio $P(X)$, un elemento $a \in A : P(a) = 0$ è detto *radice* o *zero* dell'equazione polinomiale $P(X) = 0$.
Risolvere un'equazione polinomiale significa determinarne tutte le radici.

NOTAZIONE **10.2.** L'insieme dei polinomi in un'indetermita a coefficienti in un anello A (con identità) è denotato $A[X]$.

DEFINIZIONE **10.3.** (1) Il *supporto* di un polinomio nonnullo $P(X) = a_0 + a_1X + \cdots + a_nX^n \in A[X]$, è l'insieme

$$\mathrm{Supp}P(X) := \{i \in \mathbb{N} : a_i \neq 0\}^{46}.$$

(2) Il *grado* di un polinomio nonnullo $P(X) \in A[X]$ è $\max \mathrm{Supp}P(X)^{47}$, in particolare gli elementi di A possono essere pensati come polinomi di grado 0, il coefficiente di grado massimo di un polinomio nonnullo $P(X)$ è detto *coefficiente direttivo* di $P(X)$, un polinomio *monico* è un polinomio con coefficiente direttivo 1.

OSSERVAZIONE **10.4.** (1) Grazie a Prop.9.15 ogni polinomio a coefficienti interi può essere pensato come polinomio a coefficienti in un anello qualsiasi A.
(2) A ogni $P(X) \in A[X]$ corrisponde l'applicazione o *funzione polinomiale*

$$A \xrightarrow{P} A \text{ definita da } x \overset{P}{\mapsto} \sum_{i=0}^{n} a_i x^i, \ \forall x \in A.$$

(3) Il polinomio $P(X) = X^2 + X$, può essere pensato con coefficienti in $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$) (precisamente $a_0 = \overline{0}, a_1 = \overline{1}, a_2 = \overline{1}, a_{2+i} = \overline{0}, \forall\, i$). La corrispondente funzione polinomiale $\mathbb{Z}/2\mathbb{Z} \xrightarrow{P} \mathbb{Z}/2\mathbb{Z}$, definita, $\forall\, x \in \mathbb{Z}/2\mathbb{Z}$, da $x \mapsto x^2 + x$, è la funzione nulla infatti $P(\overline{0}) = \overline{0}^2 + \overline{0} = \overline{0}$ e $P(\overline{1}) = \overline{1}^2 + \overline{1} = \overline{0}$, anche se il polinomio $P(X)$ è nonnullo.
(4) Si dimostra che se $A = \mathbf{k}$, con $\mathbf{k}$ campo di cardinalità infinita, $\exists$ c.b.u tra l'insieme dei polinomi in un'indeterminata a coefficienti in $\mathbf{k}$ e funzioni polinomiali di $\mathbf{k}$ in $\mathbf{k}$.

DEFINIZIONE **10.5.** $A[X]$ può essere dotato di una struttura di anello e precisamente, dati

$P(X) = a_0 + a_1X + \cdots + a_nX^n, Q(X) = b_0 + b_1X + \cdots + b_mX^m \in A[X]$, sia $s := \max\{m, n\}$, la *somma di* $P(X)$ *e* $Q(X)$ è il polinomio
$(P + Q)(X)$ i cui coefficienti c_i, $i \in \{0, 1, \ldots, s\}$ sono definiti da $c_i := \tilde{a}_i + \tilde{b}_i$, con

$$\tilde{a}_i \ (\text{risp. } \tilde{b}_i) = \begin{cases} a_i \ (\text{risp. } b_i) & \text{se } i \in \mathrm{Supp}\, P(X) \ (\text{risp. } i \in \mathrm{Supp}\ Q(X)) \\ 0 & \text{altrimenti} \end{cases},$$

inoltre, posto $t := n + m$, il *prodotto di* $P(X)$ *e* $Q(X)$ è il polinomio
$(PQ)(X)$ i cui coefficienti c_i, $i \in \{0, 1, \ldots, t\}$ sono definiti da

$$c_i := \sum_{j+h=i} \tilde{a}_j + \tilde{b}_h, \text{ con}$$

[46]Per definizione la cardinalità del supporto di un polinomio nonnullo è finita; al polinomio nullo si associa per convenzione come supporto l'insieme vuoto.
[47]Non è definito il grado del polinomio nullo, per convenzione lo si pone uguale a -1.

$$\tilde{a}_j \ (\text{risp. } \tilde{b}_h) = \begin{cases} a_j \ (\text{risp.} \quad b_h) & \text{se } j \in \operatorname{Supp} P(X) \ (\text{risp. } h \in \ \operatorname{Supp} Q(X)) \\ 0 & \text{altrimenti} \end{cases},$$

OSSERVAZIONE **10.6.** (1) Identificando gli elementi di A con i polinomi di grado 0, A può essere pensato come sottoanello di $A[X]$.

(2) Ogni omomorfismo di anelli $\varphi : A \longrightarrow A'$ si estende a omomorfismo di anelli $\varphi[X] : A[X] \longrightarrow A'[X]$ mediante $\varphi[X](\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \varphi(a_i) X^i$.

(3) $\forall\, a \in \mathbb{R}$, l'applicazione $\mathbb{R}[X] \xrightarrow{v_a} \mathbb{R}$ definita da $v_a(P(X)) := P(a)$ è un omomorfismo di anelli, chi è $\ker v_a$?

DEFINIZIONE **10.7.** Per ogni anello A, a partire dall'anello dei polinomi in una indeterminata $A[X]$ e da un'indeterminata Y su $A[X]$[48], si costruisce l'anello $A[X, Y] := (A[X])[Y]$, detto *anello dei polinomi in due indeterminate* su A.

Iterativamente, in modo simile, $\forall\, n \in \mathbb{N}^*$, si costruiscono gli $A[X_1, \ldots, X_n]$ *anelli dei polinomi in n indeterminate* su A.

ESEMPIO **10.8.** In $\mathbb{R}[X, Y, Z]$,
(X) è un ideale primo principale,
$(X, Y) := \{P(X, Y, Z) \in \mathbb{R}[X, Y, Z] : P(X, Y, Z) = XQ(X, Y, Z) + YR(X, Y, Z),$
$Q(X, Y, Z), R(X, Y, Z) \in \mathbb{R}[X, Y, Z]\}$ è un ideale primo non principale,
$(X, Y, Z) := \{P(X, Y, Z) \in \mathbb{R}[X, Y, Z] : P(X, Y, Z) = XQ(X, Y, Z) + YR(X, Y, Z) + ZS(X, Y, Z), Q(X, Y, Z), R(X, Y, Z), S(X, Y, Z) \in \mathbb{R}[X, Y, Z]\}$ è un ideale primo non principale e massimale,
vale inoltre $(0) \subset (X) \subset (X, Y) \subset (X, Y, Z)$.

[48]Ossia un $Y \notin A[X]$ tale che $Y^n \neq Y^m$, $\forall\, n \neq m \in \mathbb{N}^*, Y^0 = 1$

Dipartimento di Matematica, Università di Genova, 16146 Genova, Italy
E-mail address: marinari@dima.unige.it