Appunti di Aritmetica

Gabriel Antonio Videtta

24 settembre 2022

Indice

Capitolo 1

Teoria degli insiemi

Il concetto di insieme è primitivo e pertanto non definito formalmente in questa sede. Viene tuttavia definita la terminologia che riguarda le teoria dei suddetti insiemi.

Quando si leggerà $a \in S$, s'intenderà che "a appartiene all'insieme S", mentre $a \notin S$ si legge "a non appartiene all'insieme S". Un insieme A si dice sottoinsieme di B ($A \subseteq B$) quando $a \in A \to a \in B$; in particolare si dice sottoinsieme proprio di B ($A \subset B$) quando $A \subseteq B \wedge \exists\, b \in B \mid b \notin A$.

Due insiemi A e B sono uguali se e solo se $A \subseteq B \wedge B \subseteq A$. L'insieme vuoto è l'insieme che non ha elementi, ed è sottoinsieme di ogni insieme.

1.1 L'operazione di unione

L'unione di due insiemi A e B è un'operazione che restituisce un insieme $A \cup B = \{x \mid x \in A \vee x \in B\}$.

Tale operazione si può estendere a più insiemi mediante l'introduzione di un *insieme di indici* T per una famiglia di insiemi. Un insieme di indici T rispetto a un famiglia $F = \{A_t\}$ ha la seguente proprietà: $\forall\, t \in T, \exists\, A_t \in F$; ossia è in grado di enumerare gli insiemi della famiglia F.

L'unione è pertanto definita su una famiglia F come $\bigcup_{t \in T} A_t = \{x \mid (\exists\, t \in T \mid x \in A_t)\}$.

L'unione gode delle seguente proprietà: $A \subseteq B \to A \cup B = B$ (in particolare, $A \cup \varnothing = A$).

1.2 L'operazione di intersezione

Analogamente a come è stata definita l'unione, l'intersezione è un'operazione che resistuisce un insieme $A \cap B = \{x \mid x \in A \wedge x \in B\}$; ossia estesa a più insiemi: $\bigcap_{t \in T} A_t = \{x \mid (\forall\, t \in T \mid x \in A_t)\}$.

In modo opposto all'unione, l'intersezione è tale per cui $A \subseteq B \to A \cap B = A$ (in particolare, $A \cap \varnothing = \varnothing$).

1.2.1 Relazioni tra l'operazione di intersezione e di unione

Si può facilmente dimostrare la seguente relazione, valida per qualunque scelta di insiemi A, B e C: $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

Dimostrazione. Prima di tutto, un elemento di entrambi i due insiemi appartiene obbligatoriamente a C: nel caso del primo membro, il motivo è banale; riguardo al secondo membro, invece, ci accorgiamo che esso appartiene almeno a uno dei due insiemi dell'unione, riconducendoci a un'intersezione con l'insieme C.

Ogni elemento di $(A \cup B) \cap C$ appartiene inoltre ad almeno A o B, e quindi, appartenendo anche a C, appartiene a $A \cap C$ o $B \cap C$, e quindi a $(A \cap C) \cup (B \cap C)$. Pertanto $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$.

In direzione opposta, ogni elemento di $(A \cap C) \cup (B \cap C)$ appartiene almeno ad uno di dei due insiemi dell'unione. Per appartenere all'intersezione, tale elemento appartiene ad almeno A o B; e quindi appartiene ad $A \cup B$. Appartenendo anche a C, appartiene anche $(A \cup B) \cap C$. Quindi $(A \cap C) \cup (B \cap C) \subseteq (A \cup B) \cap C$.

Valendo l'inclusione in entrambe le direzioni, $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$. ■

1.3 L'operazione di sottrazione e di complemento

L'operazione di sottrazione su due insiemi A e B è definita come $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$. Si può facilmente verificare che $A = (A \cap B) \cup (A \setminus B)$.

Dimostrazione. Ogni elemento di A può appartenere o non appartenere a B: nel primo caso, appartiene anche a $A \cap B$, e quindi a $(A \cap B) \cup (A \setminus B)$; altrimenti appartiene per definizione a $A \setminus B$, e quindi sempre a $(A \cap B) \cup (A \setminus B)$. Pertanto $A \subseteq (A \cap B) \cup (A \setminus B)$.

Ogni elemento di $(A \cap B) \cup (A \setminus B)$ appartiene ad almeno uno dei due operandi dell'unione; in entrambi i casi deve appartenere ad A. Quindi $(A \cap B) \cup (A \setminus B) \subseteq A$. ■

In particolare, se $B \subseteq A$, $A \setminus B$ si dice **complemento di B in A**.

L'operazione di complemento viene indicata con A' qualora sia noto l'universo di riferimento U per cui $A' = U \setminus A$.

1.3.1 Le leggi di De Morgan

Si possono dimostrare le seguenti proprietà:

- $(A \cup B)' = A' \cap B'$
- $(A \cap B)' = A' \cup B'$

Prima legge di De Morgan. Un elemento che appartiene a $(A \cup B)'$ non appartiene né a A né a B, e quindi appartiene sia a A' che a B', pertanto anche alla loro intersezione $A' \cap B'$ [$(A \cup B)' \subseteq A' \cap B'$].

Allo stesso modo, un elemento di $A' \cap B'$ non appartiene né ad A né a B, e quindi non appartiene ad $A \cup B$, appartenendo dunque a $(A \cup B)'$ [$A' \cap B' \subseteq (A \cup B)'$]. Pertanto $(A \cup B)' = A' \cap B'$. ■

Seconda legge di De Morgan. Un elemento che appartiene a $(A \cap B)'$ può appartenere al più ad A o esclusivamente a B; pertanto appartiene ad almeno A' o B', e qunidi alla loro unione $[(A \cap B)' \subseteq A' \cup B']$.

Allo stesso modo, un elemento di $A' \cup B'$ appartiene ad almeno A' o B', e quindi non può appartenere a entrambi A e B, appartenendo dunque a $(A \cap B)'$ $[A' \cup B' \subseteq (A \cap B)']$. Pertanto $(A \cap B)' = A' \cup B'$. ■

1.3.2 La logica affrontata con gli insiemi

In modo veramente interessante, ogni operatore logico segue la logica dell'insiemistica (e viceversa); laddove l'operatore $\cup$ (o $\cap$) ha una certa proprietà, la soddisfa anche $\vee$ (o $\wedge$).

Quindi valgono tutte le leggi sopracitate:

- $(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$
- $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$
- $\neg(a \wedge b) = \neg\, a \vee \neg\, b$
- $\neg(a \vee b) = \neg\, a \wedge \neg\, b$

1.4 Il prodotto cartesiano

Il prodotto cartesiano di una famiglia ordinata di insiemi F con un certo insieme di indici T è l'insieme $\bigtimes_{t \in T} A_t = \{(a_{t_0}, a_{t_1}, \ldots) \mid a_{t_0} \in A_{t_0} \wedge a_{t_1} \in A_{t_1} \wedge \ldots\}$. In particolare, il prodotto cartesiano di due due insiemi A e B si indica con $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$.

Una n-tupla ordinata, ossia la forma in cui è raccolto un certo elemento di un prodotto cartesiano, è uguale ad una altra tupla se e solo se ogni elemento di una tupla è uguale a quello corrispondente in ordine dell'altra: pertanto, in generale, $(a, b) \neq (b, a)$.

Inoltre, il prodotto cartesiano $A \times A$ viene indicato con A^2 (analogamente, $A^n = \bigtimes_{i=1}^{n} A$).

Capitolo 2

Relazioni di equivalenza e applicazioni

2.1 Le relazioni di equivalenza

Utilizzando le nozioni di base della teoria degli insiemi è possibile definire formalmente il concetto di relazione di equivalenza.

Dato un sottoinsieme R di $A \times A$, R si dice relazione di equivalenza se:

- $(a, a) \in R$ (proprietà riflessiva)
- $(a, b) \in R \implies (b, a) \in R$ (proprietà simmetrica)
- $(a, b), (b, c) \in R \implies (a, c) \in R$ (proprietà transitiva)

Tale definizione può essere semplificata implementando l'operazione binaria $\sim$ tale per cui $a \sim b \iff (a, b) \in R$. In questo modo, le condizioni di una relazione di equivalenza R diventano:

- $a \sim a$
- $a \sim b \implies b \sim a$
- $a \sim b \wedge b \sim c \implies a \sim c$

Lemma 2.1.1. *Definita una relazione di equivalenza R con operazione binaria $\sim$, $a \sim b \wedge c \sim b \implies a \sim c$.*

Dimostrazione. Dalla proprietà riflessiva di R, $c \sim b \implies b \sim c$. Verificandosi sia $a \sim b$ che $b \sim c$, si applica la proprietà transitiva di R, che implica $a \sim c$. ■

2.1.1 Classi di equivalenza

Si definisce classe di equivalenza di a per un certo insieme A e una certa relazione di equivalenza R l'insieme $\text{cl}(a) = \{x \in A \mid a \sim x\}$, ossia l'insieme di tutti i punti che si relazionano ad a mediante tale relazione di equivalenza.

Teorema 2.1.2. *Le classi di equivalenza partizionano l'insieme di relazione in insiemi a due a due disgiunti.*

Dimostrazione. Prima di tutto è necessario dimostrare che l'unione di tutte le classi di equivalenza dà luogo all'insieme di relazione A.

Per ogni elemento $a \in A$, a appartiene a $\mathrm{cl}(a)$ per la proprietà riflessiva di R, ossia della relazione di equivalenza su cui cl è definita. Pertanto $\bigcup_{a \in A} \mathrm{cl}(a)$, che contiene solo elementi di A, è uguale ad A.

In secondo luogo, è necessario dimostrare che le classi di equivalenza sono o disgiunte o identiche. Ponendo l'esistenza di un $a \in \mathrm{cl}(x) \cap \mathrm{cl}(y)$, la dimostrazione deriva dalle proprietà di R: sia $b \in cl(x)$, allora $b \sim a$; dunque, dal momento che $b \sim a$ e che $a \sim y$, $b \sim y$, ossia $\mathrm{cl}(x) \subseteq \mathrm{cl}(y)$ (analogamente si ottiene $\mathrm{cl}(y) \subseteq \mathrm{cl}(x)$, e quindi $\mathrm{cl}(x) = \mathrm{cl}(y)$). ■

Teorema 2.1.3. *Data una partizione di un insieme che lo compone in insiemi a due a due disgiunti, è sempre possibile costruire delle classi di equivalenza.*

Dimostrazione. Vogliamo dimostrare che, data la stessa appartenenza ad un insieme come relazione, essa è una relazione di equivalenza.

Sicuramente $a \sim a$ (proprietà riflessiva). Inoltre, $a \sim b \implies a, b \in A_\alpha \implies b \sim a$ (proprietà simmetrica). Infine, $a \sim b$, $b \sim c \implies a, b, c \in A_\alpha \implies a \sim c$ (proprietà transitiva).

In particolare, dato $a \in A_\alpha$, $\mathrm{cl}(a) = A_\alpha$. ■

2.2 Le applicazioni

La nozione di applicazione di un insieme in un altro ci permette di generalizzare, ma soprattutto di definire, il concetto di funzione.

Definizione 2.2.1 (Applicazione)**.** Dati due insiemi S e T, si dice che σ è un'applicazione da S a T, se $\sigma \subseteq (S \times T) \land \forall\, s \in S, \exists!\, t \in T \mid (s,t) \in \sigma$. Tale applicazione allora si scrive come $\sigma : S \to T$.

Si scrive $\sigma : s \rightarrowtail \sigma(s)$ per sottintendere che $\forall\,(s,t) \in \sigma, (s,t) = (s, \sigma(t))$. Dato $t = \sigma(s)$, si dice che t è l'*immagine* di s appartenente al *codominio* T, enunciato come $\mathrm{Cod}(\sigma)$, mentre s è la *preimmagine* di t, appartenente al *dominio* S, detto $\mathrm{Dom}(\sigma)$. L'insieme $(s,t) \in \mathrm{Dom}(\sigma) \times \mathrm{Cod}(\sigma) \mid (s,t) \in \sigma$ è detto *grafico* di σ, ossia $\mathrm{Gr}(\sigma)$.

2.2.1 Proprietà delle applicazioni

Definizione 2.2.2 (Iniettività)**.** Un'applicazione si dice iniettiva se ad ogni immagine è corrisposto al più un elemento, ossia anche che $s_1 \neq s_2 \implies \sigma(s_1) \neq \sigma(s_2)$.

Definizione 2.2.3 (Surgettività)**.** Un'applicazione si dice surgettiva (o talvolta *su* T) se ad ogni immagine è corrisposto almeno un elemento, ossia anche che $\forall\, t \in T, \exists\, s \mid \sigma(s) = t$.

Definizione 2.2.4 (Bigettività)**.** Un'applicazione si dice bigettiva se è sia iniettiva che suriettiva, ossia se $\forall\, t \in T, \exists!\, s \in S \mid \sigma(s) = t$.

2.2.2 Composizione di applicazioni

Definizione 2.2.5 (Composizione)**.** Date due applicazioni $\sigma : S \to T$ e $\tau : T \to U$, si può definire un'applicazione detta composizione $(\tau \circ \sigma) : S \to U$, tale per cui $(\tau \circ \sigma) : s \mapsto \tau(\sigma(s))$.

Dobbiamo tuttavia assicurarci che tale applicazione possa esistere, ossia verificare che $\forall\, s \in S\, \exists!\, u \in U \mid (s, u) \in S \times U$; quindi che $\tau(\sigma(s))$ sia unico. Tuttavia questa proprietà è banale: $\sigma(s)$ è Sicuramente unico poiché σ è un'applicazione, e pertanto $\tau(\sigma(s))$ lo è, essendo anch'essa un'applicazione.

Proprietà associativa della composizione

È inoltre interessante dimostrare che la composizione rispetta la proprietà associativa, ossia che $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$.

Lemma 2.2.1 (Proprietà associativa della composizione)**.** *Date tre applicazioni α, β, γ, $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$.*

Dimostrazione. Preso un a appartenente al dominio di γ, per il primo membro abbiamo:

$$((\alpha \circ \beta) \circ \gamma)(a) = (\alpha \circ \beta)(\gamma(a)) = \alpha(\beta(\gamma(a)))$$

Analogamente per il secondo membro abbiamo:

$$(\alpha \circ (\beta \circ \gamma))(a) = \alpha((\beta \circ \gamma)(a)) = \alpha(\beta(\gamma(a)))$$

■

Iniettività, surgettività e bigettività della composizione

L'iniettività, la surgettività e la bigettività di una composizione sono ereditate dalle applicazioni di cui è composta se tutte queste le rispettano, ossia:

- $(\tau \circ \sigma)$ è iniettiva se τ e σ lo sono.
- $(\tau \circ \sigma)$ è surgettiva se τ e σ lo sono.
- $(\tau \circ \sigma)$ è bigettiva se τ e σ lo sono.

Lemma 2.2.2 (Iniettività della composizione)**.** *$(\tau \circ \sigma)$ è iniettiva se τ e σ lo sono.*

Dimostrazione. Dal momento che σ è iniettiva $s_1 \neq s_2 \implies \sigma(s_1) \neq \sigma(s_2)$, ma a sua volta, essendo τ iniettiva, $\sigma(s_1) \neq \sigma(s_2) \implies \tau(\sigma(s_1)) \neq \tau(\sigma(s_2))$. ■

Lemma 2.2.3 (Surgettività della composizione)**.** *$(\tau \circ \sigma)$ è surgettiva se τ e σ lo sono.*

Dimostrazione. Dal momento che τ è surgettiva, allora $\forall\, u \in \mathrm{Cod}(\tau), \exists\, t \in \mathrm{Dom}(\tau) \mid u = \tau(t)$. Poiché $t \in \mathrm{Cod}(\sigma)$, allora, poiché anche σ è surgettiva, $\exists\, s \in \mathrm{Dom}(\sigma) \mid t = \sigma(s)$. Pertanto $\exists\, s \in \mathrm{Dom}(\sigma) \mid u = \tau(\sigma(s))$. ■

Lemma 2.2.4 (Bigettività della composizione)**.** *$(\tau \circ \sigma)$ è bigettiva se τ e σ lo sono.*

Dimostrazione. Se τ e σ sono bigettive, sono sia iniettive che surgettive; pertanto $(\tau \circ \sigma)$ è sia iniettiva che bigettiva per i lemmi 2.2.2 e 2.2.3. ■

2.3 Applicazione inversa

Qualora un'applicazione $\sigma : S \to T$ sia bigettiva, si dice che essa crea una *corrispondenza biunivoca* tra S e T, ossia che dato un elemento qualsiasi appartenente a S è possibile associarlo ad un unico elemento di T, e viceversa. Questo è possibile dal momento che σ è sia iniettiva $(\forall\, t \in T, \exists! \vee \nexists\, s \in S \mid t = \sigma(s))$ che surgettiva $(\forall\, t \in T, \exists\, s \in S \mid t = \sigma(s))$, prescrivendo che $\forall\, t \in T, \exists!\, s \in S \mid t = \sigma(s)$.

Da questa conclusione è possibile definire l'*applicazione inversa* di σ, detta σ^{-1}, che è l'applicazione che associa ad ogni $t \in T$ un unico $s \in S$. Quindi, $t = \sigma(s) \iff s = \sigma^{-1}(t)$.

In particolare, $(\sigma \circ \sigma^{-1}) = (\sigma^{-1} \circ \sigma) = \mathrm{Id}$, ossia l'identità di σ, per la quale ogni elemento viene associato a sé stesso. Banalmente, per ogni applicazione α, $(\alpha \circ \mathrm{Id}) = (\mathrm{Id} \circ \alpha) = \alpha$.

Lemma 2.3.1. *$\sigma : S \to T$ è una corrispondenza biunivoca se e solo se esiste un'applicazione $\mu : T \to S$ tale per cui $(\sigma \circ \mu) = (\mu \circ \sigma) = \mathrm{Id}$.*

Dimostrazione. Dal momento che σ è bigettiva, σ^{-1} esiste, e questa è tale per cui $(\sigma \circ \mu) = (\mu \circ \sigma) = \mathrm{Id}$.

In direzione opposta, se esiste una μ tale per cui $(\sigma \circ \mu) = (\mu \circ \sigma) = \mathrm{Id}$, allora:

- σ è iniettiva: $\sigma(s_1) = \sigma(s_2) \implies \mu(\sigma(s_1)) = \mu(\sigma(s_2)) \implies s_1 = s_2$.
- σ è surgettiva: $\forall\, t \in T, t = \sigma(\mu(t)) \implies \exists\, s = \mu(t) \in S \mid t = \sigma(s)$.

■

Lemma 2.3.2 (Unicità dell'applicazione inversa)**.** *Per ogni applicazione bigettiva σ, σ^{-1} è unica.*

Dimostrazione. Poniamo $\alpha \neq \beta$ come due applicazioni inverse distinte di σ. Allora $\alpha = \alpha \circ (\sigma \circ \beta) = (\alpha \circ \sigma) \circ \beta = \beta$, che è una contraddizione. ■

2.4 Il gruppo $A(S)$ delle corrispondenze biunivoche

Si definisce $A(S)$ come l'insieme $\{\sigma : S \to S \mid \sigma \text{ sia biunivoca}\} = \{\sigma : S \to S \mid \forall\, s \in S\, \exists!\, t \in S \mid t = \sigma(s)\}$.

Prendendo in considerazione l'operazione di composizione $\circ$, si può dimostrare che $(A(S), \circ)$ è un gruppo:

- $\forall\, \alpha, \beta \in A(S), \alpha \circ \beta \in A(S)$ (vd. Lemma 2.2.4).
- $\forall\, \alpha, \beta, \gamma \in A(S), (\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$ (vd. Lemma 2.2.1).
- $\exists\, \mathrm{Id} \in A(S) \mid \forall\, \alpha \in A(S), (\mathrm{Id} \circ \alpha) = (\alpha \circ \mathrm{Id}) = \alpha$.
- $\forall\, \alpha \in A(S), \exists\, \alpha^{-1} \in A(S) \mid (\alpha \circ \alpha^{-1}) = (\alpha^{-1} \circ \alpha) = \mathrm{Id}$ (vd. Lemma 2.3.1).

Lemma 2.4.1. *Se S consta di più di due elementi ($\|S\| > 2$), allora esistono sicuramente due applicazioni $\alpha, \beta \in A(S)$ tale per cui $(\alpha \circ \beta) \neq (\beta \circ \alpha)$.*

Dimostrazione. Se S consta di due elementi, S possiede almeno tre elementi s_1, s_2, s_3, possiamo definire due applicazioni σ e τ come segue:

- $\sigma(s_1) = s_2$, $\sigma(s_2) = s_3$, $\sigma(s_3) = s_1$.
- $\tau(s_1) = s_1$, $\tau(s_2) = s_2$, $\tau(s_3) = s_3$.
- $\sigma(a) = \tau(a) = a \,\forall\, a \notin \{s_1, s_2, s_3\}$.

Allora $(\sigma \circ \tau)(s_1) = \sigma(s_1) = s_2$ e $(\tau \circ \sigma)(s_1) = \tau(s_2) = s_3$, ma $s_2 \neq s_3$. ■