Indice

1 Introduzione

1.1 Insiemistica

Sia X un insieme. Il concetto di insieme è primitivo[1] e non se ne dà una vera definizione, ma lo si può intendere come una *collezione di oggetti*. Per intenderci, X può essere esibito elencandone gli elementi tra parentesi graffe: $X = \{a, b, c, \ldots\}$, oppure tramite una caratteristica verificata da tutti e soli i suoi elementi $X = \{x \mid p(x)\}$ dove $p(x)$ è una proprietà verificata da x.

Esempio 1.1. $X = \{\text{le vocali dell'alfabeto italiano}\} = \{x \mid x \text{ è una vocale dell'alfabeto italiano}\} = \{a, e, i, o, u\}$.

Inoltre, se un elemento x appartiene all'insieme X scriveremo $x \in X$. Se x non appartiene ad X scriveremo $x \notin X$. Anche l'appartenenza è un concetto primitivo e, pertanto, viene dato come intuitivo[1]. Quindi definiamo i seguenti concetti.

Sottoinsieme: siano X e Y insiemi non necessariamente distinti. Diremo che Y è un *sottoinsieme* di X ($Y \subseteq X$) se e solo se per ogni $y \in Y$ si ha $y \in X$ (ogni elemento di Y appartiene ad X). Diremo che un sottoinsieme è *proprio* quando $Y \neq X$.

Uguaglianza: diremo che $X = Y$ se e solo se $X \subseteq Y$ e $Y \subseteq X$ (ogni elemento di X appartiene anche ad Y e viceversa).

Esempio 1.2. Consideriamo l'insieme $X = \{(x, y) \mid x, y \in \mathbb{Z} \wedge 3x + 4y = 1\}$ e l'insieme $Y = \{(-1 - 4z, 1 + 3z) \mid z \in \mathbb{Z}\}$. Essi[2] sono uguali.

Esercizio 1.1. Dimostra che $X = Y$ sfruttando la definizione[3].

Dato un insieme X e dei suoi sottoinsiemi A, B e C, definiamo come segue le operazioni di *intersezione* e *unione*.

Intersezione: $A \cap B = \{x \in X \mid x \in A \wedge x \in B\}$.

Unione: $A \cup B = \{x \in X \mid x \in A \vee x \in B\}$[4].

[1] Facciamo finta che lo sia, in realtà c'è un mondo dietro!

[2] Il simbolo $\wedge$ indica la *congiunzione logica* di due enunciati ed è, a sua volta, un enunciato che è vero solo quando i due enunciati di partenza sono entrambi veri. Altrimenti è falso.

[3] Hint: dimostra che gli elementi di Y risolvono l'equazione che definisce X e che tutte le soluzioni dell'equazione di X si scrivono come gli elementi di Y. Per il secondo punto un'idea è di sfruttare la scrittura parametrica di una retta.

[4] Il simbolo $\vee$ indica la *disgiunzione logica* di due enunciati ed è, a sua volta, un enunciato che è vero quando almeno uno dei due enunciati di partenza è vero. Altrimenti è falso.

Entrambe queste operazioni godono di alcune proprietà:

- **Commutatività**: $A \cap B = B \cap A$ e analogo per $\cup$.
- **Associatività**: $A \cap (B \cap C) = (A \cap B) \cap C$ e analogo per $\cup$.
- **Distributività di $\cap$**: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
- **Distributività di $\cup$**: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Esercizio 1.2. Dimostra le proprietà elencate.

Si definisce poi l'operazione di *sottrazione insiemistica* e, di conseguenza, l'operazione *unaria* di *complementare* come segue.

Sottrazione: $X \setminus A = \{x \in X \mid x \notin A\}$.

Complementare: il complementare di A in X è definito come $\overline{A} = X \setminus A$.

Leggi di De Morgan: $\overline{A \cup B} = \overline{A} \cap \overline{B}$ e $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Esercizio 1.3. Riscrivi le Leggi di De Morgan con la sottrazione e dimostrale.

Definiamo quindi alcuni concetti fondamentali della teoria degli insiemi:

Insieme finito: diremo che un insieme è *finito* sse (se e solo se) esiste una biiezione tra l'insieme stesso ed un insieme $\{1, 2, \ldots, n\}$ con $n \in \mathbb{N}$.

Cardinalità: la cardinalità di un insieme X finito è, informalmente, il numero di elementi contenuti in X e si indica con $|X|$. Se X è in corrispondenza con $\{1, 2, \ldots, n\}$, scriveremo $|X| = n$.

Insieme Infinito: un insieme si dice *infinito*[5] se non è finito, poniamo $|X| = \infty$. Una definizione alternativa è la seguente: un insieme si dice infinito quando può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio.

Insieme Vuoto: l'*insieme vuoto* $\varnothing$ come l'insieme che non contiene alcun elemento. Ovviamente, per ogni insieme X, $\varnothing \subseteq X$

Parti di X: l'*insieme delle Parti* di un insieme X è $\mathscr{P}(X) = \{Y \mid Y \subseteq X\}$, cioè l'insieme di tutti i sottoinsiemi di X.

Esempio 1.3. se $X = \{1, 2\}$ allora $\mathscr{P}(X) = \{\varnothing, \{1\}, \{2\}, X\}$, nota che la cardinalità dell'insieme delle parti è uguale a 2 elevato alla cardinalità di X, cioè:

$$|\mathscr{P}(X)| = 2^{|X|}.$$

Se consideriamo un insieme $\mathbb{I}$ di indici allora possiamo definire una famiglia di sottoinsiemi A_i di X indicizzati da $i \in \mathbb{I}$, in simboli: $\{A_i \mid i \in \mathbb{I}\}$ oppure $\{A_i\}_{i \in \mathbb{I}}$. Questa famiglia sarà finita o infinita a seconda della cardinalità di $\mathbb{I}$, indipendentemente dalla cardinalità di X.

[5] Ricodiamo che esistono diversi tipi di infinito! Per esempio $|\mathbb{R}| > |\mathbb{Q}| = |\mathbb{N}|$.

Utilizzeremo simboli specifici per indicare intersezioni e unioni di famiglie di insiemi indicizzati e questi sono:

$$\bigcap_{i\in\mathbb{I}} A_i \stackrel{\text{def}}{=} \{x \in X \mid \forall i \in \mathbb{I} :\ x \in A_i\};$$
$$\bigcup_{i\in\mathbb{I}} A_i \stackrel{\text{def}}{=} \{x \in X \mid \exists i \in \mathbb{I} :\ x \in A_i\}.$$

In altre parole, l'intersezione di tutti gli A_i è l'insieme degli elementi di X che appartengono a tutti gli A_i, mentre l'unione sarà data da tutti gli elementi di X che appartengono ad almeno uno degli A_i. Si tratta di ripetere l'operazione di intersezione o di unione per tutti gli insiemi della famiglia. Questa operazione è *ben definita* per la proprietà associativa.

Esempio 1.4. Sia $X = \{a, b, c, d\}$, $\mathbb{I} = \{1, 2\}$, $A_1 = \{a, c\}$ e $A_2 = \{b, c\}$; allora calcoliamo $\bigcap_{i\in\{1,2\}} A_i = A_1 \cap A_2 = \{c\}$. Prova con l'unione.

Esercizio 1.4. In cosa consistono $\bigcap_{i\in\mathbb{I}} A_i$ e $\bigcup_{i\in\mathbb{I}} A_i$ quando $\mathbb{I} = \varnothing$?[6]

Esercizio 1.5. Sia $X = [0, 1] \subset \mathbb{R}$ e sia $n \in \mathbb{N}$ e consideriamo la famiglia di sottoinsiemi $A_n = \{x \in X \mid \frac{1}{n} \leq x \leq 1\}$, verifica che $\bigcup_{n\in\mathbb{N}} A_n = (0, 1]$.[7]

Esercizio 1.6. Nelle stesse ipotesi dell'esercizio 1.5, verifica che $\bigcap_{n\in\mathbb{N}} A_n = \{1\}$.

È essenziale, adesso, introdurre alcune ulteriori definizioni:

Prodotto Cartesiano: dati due insiemi X e Y non necessariamente distinti, il *prodotto cartesiano* di essi è: $X \times Y = \{(x, y) \mid x \in X \wedge y \in Y\}$, ossia l'insieme delle coppie ordinate in cui il primo elemento appartiene al primo insieme e il secondo elemento al secondo insieme.

Per prodotti cartesiani di n insiemi si otterranno delle n-uple di elementi in cui l'i-esimo elemento appartiene all'i-esimo insieme ($i \leq n$).

Esempio 1.5. Se $X = Y = \mathbb{R}$ allora $X \times Y = \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ ossia il piano cartesiano. Lo spazio 3-dimensionale si indicherà con $\mathbb{R}^3$, mentre per un generico $n \in \mathbb{N}$ otteniamo lo spazio n-dimensionale $\mathbb{R}^n$. Riprenderemo questo esempio all'inizio del capitolo 2.

Partizione di un insieme: dato un insieme non vuoto X, una *partizione* $\mathcal{P}$ di X è una famiglia di sottoinsiemi non vuoti di X aventi due proprietà:

1. comunque presi due elementi distinti di questa famiglia, la loro intersezione è vuota. In simboli:

$$\forall A, B \in \mathcal{P},\ A \neq B \Rightarrow A \cap B = \varnothing$$

[6] Soluzione:
$\bigcup_{i\in\mathbb{I}} A_i = \varnothing$ infatti è l'insieme di tutte quelle x tali che per qualche $i \in \mathbb{I}$ appartengono al corrispondente A_i, ma non essendoci alcun A_i non può esistere alcuna x siffatta.
$\bigcap_{i\in\mathbb{I}} A_i = X$ infatti supponiamo per assurdo che un certo x_0 non appartenga all'intersezione, questo può succedere solo a patto che esista un certo i per cui il corrispondente A_i non contiene x_0, ma non esiste alcun A_i che escluda x_0 dato che non esiste proprio alcun A_i.

[7] Hint: ricorda che in un intervallo, quando la parentesi è tonda l'estremo è escluso, quando è quadra l'estremo è incluso. Per rispondere all'esercizio, poi, aiutati con la seguente domanda: è vero che, preso un numero x qualsiasi tale che $0 < x \leq 1$ esisterà un certo A_n che lo contiene?

2. l'unione di tutti gli elementi della famiglia è X. In simboli:

$$\bigcup_{A \in \mathcal{P}} A = X.$$

Esempio 1.6. L'insieme $\{X\}$ è una partizione banale di X.

Esempio 1.7. Un'altra banale è data dall'insieme dei singoletti: $\{\{x\} \mid x \in X\}$.

Esempio 1.8. $\mathcal{P} = \{\{1\}, \{2,3\}, \{4\}\}$ è una partizione di $X = \{1,2,3,4\}$.

Esercizio 1.7. Quale cardinalità può avere $\mathcal{P}$, al massimo, se $|X| = n \in \mathbb{N}$?

1.2 Relazioni e Funzioni

È interessante studiare l'interazione tra elementi di insiemi e tra insiemi stessi. Per questo motivo introduciamo la seguente definizione.

Corrispondenza: Siano A e B due insiemi non vuoti e non necessariamente distinti. Una *corrispondenza* tra A e B è un sottoinsieme $\mathcal{C}$ di $A \times B$.

Nota che le *funzioni* sono un particolare tipo di corrispondenza. Infatti, se consideriamo una funzione $f : A \to B$, il suo grafico $\mathcal{G} = \{(a, f(a)) \mid a \in A\}$ è una corrispondenza. Inoltre vale anche il viceversa: data una corrispondenza $\mathcal{C}$ tale che:

$$\forall a \in A \ \exists! b \in B \mid (a,b) \in \mathcal{C}, \quad [8]$$

allora certamente esiste una funzione $f_{\mathcal{C}} : A \to B$, eventualmente definita punto per punto, che ha $\mathcal{C}$ per grafico.

Relazione: una *relazione* $\mathcal{R}$ su A è un sottoinsieme di $A \times A = A^2$.

In effetti si potrebbe anche dire che una relazione è una particolare corrispondenza in cui $A = B$, ossia quando consideriamo due insiemi coincidenti.

Esempio 1.9. Sia $A = \mathbb{R}^2$, ossia A è il piano cartesiano standard, un esempio di relazione su $A \times A$ può essere dato da $\mathcal{R} = \{(x,y) \in A \times A \mid d_2(x,y) = 1\}$, ossia due punti sono in relazione se la loro distanza euclidea d_2 è uguale ad 1.

Esempio 1.10. Sia $A = \mathbb{R}$, possiamo considerare $\mathcal{R} = \{(x,y) \in A \times A \mid x \leq y\}$.

Esempio 1.11. Sia $A = \{\text{rette nel piano}\}$, $\mathcal{R} = \{(x,y) \in A \times A \mid x /\!/ y\}$.

Esempio 1.12. sia $A = \{\text{persone esistite}\}$, $\mathcal{R} = \{(x,y) \in A \times A \mid x \text{ è figlio di } y\}$.

L'idea di relazione esprime la necessità di legare tra loro elementi di A con una stessa caratteristica. A loro volta, le relazioni hanno delle proprietà che siamo interessati a studiare:

- $\mathcal{R}$ è **riflessiva** sse $\forall a \in A : \ (a,a) \in \mathcal{R}$.
- $\mathcal{R}$ è **simmetrica** sse $\forall a,b \in A : \ (a,b) \in \mathcal{R} \Rightarrow (b,a) \in \mathcal{R}$.
- $\mathcal{R}$ è **transitiva** sse $\forall a,b,c \in A : \ (a,b) \in \mathcal{R} \wedge (b,c) \in \mathcal{R} \Rightarrow (a,c) \in \mathcal{R}$.

[8] Il simbolo $\exists!$ denota contemporaneamente esistenza ed unicità.

- $\mathcal{R}$ è **di equivalenza** sse è riflessiva, simmetrica e transitiva.

Se X è un insieme non vuoto e $\mathcal{R}$ una relazione di equivalenza su X, definiamo per ogni $x \in X$ la sua classe di equivalenza.

Classe di equivalenza: la *classe di equivalenza* di $x \in X$, spesso chiamata solo *classe*, è $[x]_{\mathcal{R}} = \{a \in X \mid (x,a) \in \mathcal{R}\}$.

Esercizio 1.8. La relazione dell'esempio 1.9 è di equivalenza?

Esercizio 1.9. Dimostra che $[x]_{\mathcal{R}} \neq \varnothing$.

Proposizione 1.2.1. *Per ogni $x, y \in X$ accade una delle seguenti opzioni:*

1. $[x]_{\mathcal{R}} = [y]_{\mathcal{R}}$,
2. $[x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} = \varnothing$.

Dimostrazione. Le possibilità sono due: o l'intersezione è vuota, nel qual caso non abbiamo nulla da dimostrare, oppure esiste $z \in [x]_{\mathcal{R}} \cap [y]_{\mathcal{R}}$. Consideriamo quindi questo secondo caso. Vogliamo mostrare che ogni elemento $t \in [x]_{\mathcal{R}}$ è in relazione anche con y e, di conseguenza, appartiene anche a $[y]_{\mathcal{R}}$. Ma, per costruzione, $(x,t) \in \mathcal{R}$; inoltre, per ipotesi, $(z,x) \in \mathcal{R}$. Applicando la proprietà transitiva, $(z,t) \in \mathcal{R}$. Sempre per ipotesi, anche $(y,z) \in \mathcal{R}$ e, per transitività, $(z,t) \in \mathcal{R}$ implica $(y,t) \in \mathcal{R}$.

In altre parole, per l'arbitrarietà di t, ogni elemento di $[x]_{\mathcal{R}}$ sta anche in $[y]_{\mathcal{R}}$. Abbiamo dimostrato che $[x]_{\mathcal{R}} \subseteq [y]_{\mathcal{R}}$. In modo analogo dimostriamo che $[y]_{\mathcal{R}} \subseteq [x]_{\mathcal{R}}$ e quindi che $[x]_{\mathcal{R}} = [y]_{\mathcal{R}}$. Cioè, se l'intersezione non è vuota, le due classi coincidono e questo conclude la dimostrazione. □

Esercizio 1.10. Termina la dimostrazione mostrando che $[y]_{\mathcal{R}} \subseteq [x]_{\mathcal{R}}$.

Insieme Quoziente: definiamo l'*insieme quoziente* di un insieme X rispetto alla relazione di equivalenza $\mathcal{R}$ come l'insieme delle classi di equivalenza. In simboli: $X/\mathcal{R} = \{[x]_{\mathcal{R}} \mid x \in X\}$.

Esercizio 1.11. Dimostra che $X/\mathcal{R}$ è una partizione di X.

Esiste tuttavia anche una costruzione inversa: sia $\mathcal{P}$ una partizione di X, dirò che due elementi a e b di X sono in relazione se appartengono allo stesso elemento S di $\mathcal{P}$. Cioè: $\mathcal{R} = \{(a,b) \in X \times X \mid \exists S \in \mathcal{P} \wedge a, b \in S\}$. Quindi $\mathcal{R}$ è di equivalenza e $\mathcal{P} = X/\mathcal{R}$.

Esercizio 1.12. Dimostra che $\mathcal{R}$ così definita è di equivalenza.

Esercizio 1.13. Dato $n \in \mathbb{N}$ e data $\mathcal{R}_n = \{(a,b) \in \mathbb{Z}\times\mathbb{Z} \mid n \text{ divide}^9\ a-b\}$, dimostra che $\mathcal{R}_n$ è di equivalenza indipendentemente dal valore di n. Determina tutte le classi di equivalenza quando $n = 2$ e quando $n = 3$. Cosa succede se $n = 0$? E se $n = 1$?[10]

[9] Sia $a \in \mathbb{Z}$, diremo che $n \in \mathbb{N}$ divide a sse $\exists b \in \mathbb{Z} \mid a = b \cdot n$.

[10] Per $n = 2$ abbiamo $\mathcal{R}_2 = \{[0]_{\mathcal{R}}, [1]_{\mathcal{R}}\}$ ossia la relazione che distingue tra pari e dispari. Per $n = 3$ abbiamo $\mathcal{R}_3 = \{[0]_{\mathcal{R}}, [1]_{\mathcal{R}}, [2]_{\mathcal{R}}\}$ ossia distinguiamo tra quei numeri che hanno resto $0, 1, 2$ nella divisione per 3. Se $n = 0$ allora due numeri sono in relazione se e soltanto se sono uguali. Se $n = 1$ ogni numero è in relazione con ogni altro.

Con l'esercizio (1.13), abbiamo introdotto senza troppa sofferenza il concetto di *classi di resto modulo n*, alla base dell'artimetica modulare (chiamata anche, orribilmente, "aritmetica dell'orologio"). Sorprendentemente, l'aritmetica modulare e i suoi sviluppi sono un potente strumento nella risoluzione di questioni relative, principalmente, alla teoria dei numeri.

1.3 Operazioni Binarie

Sia X un insieme non vuoto. Un solo insieme è una struttura piuttosto "arida" con cui operare, abbiamo bisogno di aggiungergli *qualcosa*: definiamo un'operazione binaria tra coppie di elementi:

Operazione binaria: un'*operazione binaria* su X è un'applicazione[11]

$$\heartsuit : X \times X \to X$$

che, a ogni coppia di elementi $a, b \in X$, cioè a ogni coppia ordinata $(a, b) \in X \times X = X^2$, associa uno e un solo elemento di X, definito come $a \heartsuit b$.

Poiché l'operazione associa a coppie di elementi in X un "risultato" sempre in X, l'operazione viene definita *interna* a X.

Esempio 1.13. Se $X = \mathbb{N}$, oppure $X = \mathbb{Z}$ o, ancora, $X = \mathbb{R}$, allora un esempio di operazione interna può essere dato da $\heartsuit = +$ (formalmente sono "+" diversi!).

Esempio 1.14. Se $X = \{0, 1\}$ allora posso definire un'operzione interna punto per punto:

$$0 \heartsuit 0 = 0, \qquad 0 \heartsuit 1 = 1, \qquad 1 \heartsuit 0 = 1, \qquad 1 \heartsuit 1 = 0.$$

In questo caso si potrebbe provare a dare anche una caratterizzazione esplicita dell'operazione definita punto per punto, in effetti possiamo usare $a \heartsuit b = (a + b) \cdot (2 - a - b)$ e le due operazioni coincidono. Si noti che questo esempio corrisponde con lo *XOR* logico.

Ovviamente non è scontata la richiesta che il risultato dell'operazione faccia parte dell'insieme di partenza: si consideri l'operazione $a \star b = a^{-b}$ definita su $X = \mathbb{N}$: è chiaro che per qualsiasi valore di b diverso da 0, l'operazione restituisce un risultato $(= \frac{1}{a^b})$ non naturale. L'operazione $\star$ è però certamente interna ad $\mathbb{R}$, ma anche solo a $\mathbb{Q}$. Conviene quindi dare la seguente definizione:

Sottoinsieme Chiuso: sia $\heartsuit$ un'operazione binaria su X. Un sottoinsieme Y di X si dice *chiuso* rispetto a $\heartsuit$ se per ogni $y_1, y_2 \in Y$, $y_1 \heartsuit y_2 \in Y$. Cioè $\heartsuit$ è interna a Y.

Dato un sottoinsieme Y chiuso rispetto ad $\heartsuit$, posso definire la restrizione[12] di $\heartsuit$ ad Y, ossia l'operazione $\heartsuit_Y : Y \times Y \to Y$ tale da essere interna ad Y.

Di un'operazione, come al solito, possiamo chiederci che proprietà abbia e queste possono essere:

[11] "Applicazione" è un sinonimo di "funzione".

[12] Generalmente si tratta di una distinzione determinante, tuttavia per noi avrà soltanto un significato formale: l'operazione è sempre la stessa ma sottolineiamo che accetterà come fattori solo elementi di Y.

- **Commutatività**: se $a \heartsuit b = b \heartsuit a$;
- **Associatività**: se $(a \heartsuit b) \heartsuit c = a \heartsuit (b \heartsuit c) = a \heartsuit b \heartsuit c$.

Esercizio 1.14. Dimostra per induzione la proprietà associativa con n elementi

Fatto 1.3.1. *Ogni proprietà di tipo equazionale di $\heartsuit$ (come commutatività e associatività) è ereditata anche dalla sua restrizione $\heartsuit_Y$.*

In genere, a questo punto, si parlerebbe della presenza nell'insieme di un elemento neutro (unità[13]) rispetto all'operazione $\heartsuit$. Tuttavia, non potendo dare per scontata la commutatività, adotteremo un approccio diverso:

Unità sinistra: $u_s \in X$ si dice *unità sinistra* rispetto a $\heartsuit$ sse per ogni $x \in X$ si ha $u_s \heartsuit x = x$.

Unità destra: analogamente, $u_d \in X$ si dice *unità destra* rispetto a $\heartsuit$ sse per ogni $x \in X$ si ha $x \heartsuit u_d = x$.

Unità bilatera: $u \in X$ si dice *unità bilatera* rispetto a $\heartsuit$ sse per ogni $x \in X$ si ha $x \heartsuit u = u \heartsuit x = x$ (per l'unità bilatera vale la commutatività).

Proposizione 1.3.2. *Se in X esiste un'unità sinistra u_s e un'unità destra u_d rispetto a $\heartsuit$ allora:*

a. $u_s = u_d$;

b. u_s è l'unica unità sinistra e u_d l'unica destra;

c. $u_s = u_d = u$ è l'unica unità bilatera.

Dimostrazione. Dimostriamo punto per punto.

a. per definizione di unità sinistra abbiamo che $u_s \heartsuit x = x$ per qualsiasi $x \in X$, in particolare vale se $x = u_d$. Quindi $u_s \heartsuit u_d = u_d$. Analogamente, per definizione di unità destra abbiamo che $y \heartsuit u_d = u_d$ per qualsiasi $y \in X$, in particolare vale se $y = u_s$. Quindi $u_s \heartsuit u_d = u_s$. Concludendo: $u_d = u_s \heartsuit u_d = u_s$.

b. Supponiamo che $\overline{u}_s$ sia un'altra unità sinistra, allora per la dimostrazione precedente $\overline{u}_s = u_d$, ma anche $u_s = u_d$, quindi $\overline{u}_s = u_s$. L'unicità di u_d si dimostra in modo analogo.

c. Dato che $u_s = u_d$, possiamo rinominare il valore comune u e, dato che $x = u_s \heartsuit x = x \heartsuit u_d = x$, allora $x = u \heartsuit x = x \heartsuit u = x$ quindi u è unità bilatera. □

Analogamente a quanto detto per l'unità, data l'operazione $\heartsuit$ con unità u, anche per l'esistenza di un elemento inverso dobbiamo distinguere vari casi:

Inverso sinistro: x_s^{-1} si dice *inverso sinistro* di $x \in X$ sse $x_s^{-1} \heartsuit x = u$.

Inverso destro: x_d^{-1} si dice *inverso destro* di $x \in X$ sse $x \heartsuit x_d^{-1} = u$.

Inverso bilatero: x^{-1} si dice *inverso bilatero* di $x \in X$ sse $x \heartsuit x^{-1} = x^{-1} \heartsuit x = u$.

[13] Attenzione alla definizione di "unità": è diversa dall'idea che abbiamo in mente! Infatti l'1 è unità per l'operazione di moltiplicazione tra numeri, mentre l'unità (in senso algebrico) dell'addizione è lo 0.

La dicitura $^{-1}$ non deve trarre in inganno: non ha nulla a che vedere con la frazione $\frac{1}{x}$. È soltanto un metodo standard per indicare l'inverso in una generica operazione. Ad esempio, se identifichiamo $\heartsuit$ con l'usuale somma tra numeri, l'inverso x^{-1} di x si indicherà con $-x$. Inoltre, non sempre esiste un inverso per un'operazione.

Esercizio 1.15. Presi $X = \mathbb{R} \cup \{-\infty\}$ ed $a, b \in X$, dimostra che l'addizione tropicale ($a \oplus b = max\{a, b\}$) non ammette inverso.

Proposizione 1.3.3. *Se $\heartsuit$ è associativa e in X esistono un inverso sinistro x_s^{-1} e un inverso destro x_d^{-1} rispetto a $\heartsuit$ allora:*

a. $x_s^{-1} = x_d^{-1}$;

b. x_s^{-1} *e* x_d^{-1} *sono unici;*

c. $x_s^{-1} = x_d^{-1} = x^{-1}$ *è inverso bilatero di* $x \in X$.

Dimostrazione. Procediamo ancora per punti.

a. Scriviamo $(x_s^{-1} \heartsuit x) \heartsuit x_d^{-1}$, per associatività è uguale a $x_s^{-1} \heartsuit (x \heartsuit x_d^{-1})$. Ma la prima scrittura è $u \heartsuit x_d^{-1}$, a sua volta uguale alla seconda che vale $x_s^{-1} \heartsuit u$. Essendo uguali le due scritture ed essendo u elemento neutro, otteniamo che $x_s^{-1} = x_d^{-1}$

b. Supponiamo $x_s^{-1} \neq \tilde{x}_s^{-1}$ entrambi inversi sinistri, quindi $x_s^{-1} \heartsuit x = u = \tilde{x}_s^{-1} \heartsuit x$. Consideriamo solo $x_s^{-1} \heartsuit x = \tilde{x}_s^{-1} \heartsuit x$: moltiplichiamo a destra entrambi per x_d^{-1} e usiamo la proprietà associativa: $x_s^{-1} \heartsuit (x \heartsuit x_d^{-1}) = \tilde{x}_s^{-1} \heartsuit (x \heartsuit x_d^{-1})$ che, svolgendo i conti, porta a: $x_s^{-1} \heartsuit u = \tilde{x}_s^{-1} \heartsuit u$ ossia $x_s^{-1} = \tilde{x}_s^{-1}$

c. Esercizio. □

In effetti, ci siamo posti il problema di garantire che il risultato di un'operazione fosse interno all'insieme X su cui è definita. Ma non abbiamo pensato all'eventualità in cui uno dei fattori fosse esterno all'insieme X. Questo, in effetti, dà luogo a questioni parecchio interessanti che, sotto spoglie innocenti, si incontrano molto presto nel percorso di studi:

Operazione Esterna: dati due insiemi non vuoti E ed X, distinti, diremo che $* : E \times X \to X$ è un'*operazione esterna* (ad X), che associa alla coppia ordinata (e, x) un unico elemento $e * x$ di X.

Esempio 1.15. Sia $V = \{\text{insieme dei vettori a due componenti reali}\} = \mathbb{R}^2$ ed $E = \mathbb{R}$, un esempio elementare di operazione esterna è la moltiplicazione per scalare di un vettore: dato $r \in \mathbb{R}$ e $(a, b) \in V$, definiamo $r * (a, b) \stackrel{\text{def}}{=} (r \cdot a, r \cdot b)$.

In caso di operazione esterna, diremo che l'insieme E *agisce* su X.

1.4 Strutture Algebriche

Siamo estremamente interessati a classificare, tramite proprietà, gli insiemi e le loro operazioni. Perché questo interesse? La teoria che studieremo riguarda un caso molto specifico, ma il linguaggio che si introduce con le strutture algebriche permette di espanderla parecchio. Un'introduzione a queste nozioni ci serve quindi per dare un'idea della generalità delle idee di cui si parlerà e, ottimisticamente parlando, per dare una base utile a futuri approfondimenti.

Innanzitutto, insiemi dotati di una o più operazioni binarie (interne ed eventualmente anche esterne) sono detti *strutture algebriche* e si indicano con $(X, \heartsuit_1, \ldots, \heartsuit_n)$.

Gruppi

Sia X un insieme non vuoto e $\heartsuit$ un'operazione interna ad esso:

Gruppo: $(A, \heartsuit)$ è un *gruppo* se $\heartsuit$ è associativa, ammette elemento neutro e ogni elemento ha un inverso.

Gruppo Commutativo: se $(A, \heartsuit)$ è un gruppo e $\heartsuit$ gode della proprietà commutativa, allora si parla di gruppo *commutativo* o *abeliano*.

Esempio 1.16. $(\mathbb{N}, +)$ non è un gruppo in quanto non c'è l'inverso per nessun elemento diverso dallo 0 (infatti è detto ***monoide*** *commutativo* o *semigruppo commutativo con unità*).

Esempio 1.17. $(\mathbb{Z}, +)$ è un gruppo, ma $(\mathbb{Z}, \cdot)$ no.

Esempio 1.18. $\mathbb{Q}$ forma un gruppo con l'operazione di addizione ma, se considerassimo la moltiplicazione dovremmo togliere lo 0, altrimenti cadrebbe la richiesta di esistenza dell'inverso.

Esempio 1.19. Sia $X = \{\text{mosse del cubo di Rubik}\}$ e sia $\star$ l'operazione di composizione delle mosse (comporre due mosse vuol dire farle in sequenza). Questa struttura è un gruppo[14] ma non vale la commutatività.

Anelli

Abbiamo anticipato che una struttura algebrica può contemplare più operazioni: introduciamo quindi anche una seconda operazione $*$. Parleremo di *somma* e *prodotto* della struttura, senza tuttavia confonderli con la somma e il prodotto a cui siamo abituati: la somma e il prodotto usuali sono solo uno di tanti esempi di somme e prodotti.

Anello: una terna $(X, \heartsuit, *)$ è un *anello* quando $(X, \heartsuit)$ è un gruppo abeliano con elemento neutro e, $(X, *)$ è un monoide e valgono le proprietà distributive: per ogni $a, b, c \in A$:

$$a * (b \heartsuit c) = (a * b) \heartsuit (a * c);$$
$$(a \heartsuit b) * c = (a * c) \heartsuit (b * c).$$

Anello commutativo: un anello è commutativo quando $*$ è commutativa.

Esempio 1.20. $X = \{0\}$ allora $(X, +, \cdot)$ è un anello. In generale, $X = \{e\}$, con e elemento neutro della prima operazione, forma un anello detto *banale*.

Esempio 1.21. $(\mathbb{N}, +, \cdot)$ non è un anello, $(\mathbb{Z}, +, \cdot)$ invece lo è. Inoltre, anche $\mathbb{Z}$ con l'aggiunta di tutte le frazioni $\frac{z}{10^n}$ è un anello con le usuali operazioni.

Esempio 1.22. Sia $X = \{0, 1\}$, allora $(X, \dot\vee, \wedge)$ forma un anello finito (cioè con un numero finito di elementi) commutativo, dove $\dot\vee$ è lo XOR.

[14] Nel 1979, David Breyer Singmaster pubblicò il libro *Notes on Rubik's "Magic Cube"*, che includeva una trattazione matematica del cubo di Rubik e la possibilità di risolverlo in modo generale sfruttando la teoria dei gruppi. A quel tempo era molto difficile da reperire, infatti lo vide per la prima volta solo un anno prima al congresso internazionale dei matematici. Il mese dopo, per entrare in possesso di un cubo dovette scambiarlo con una copia di un libro di Escher.

Esempio 1.23. L'insieme delle classi di resto modulo n (si indica $\mathbb{Z}/n\mathbb{Z}$) forma un anello finito commutativo (avevamo già visto $\mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\}$).

Esempio 1.24. Un argomento che tratteremo più avanti sono le matrici[15], in effetti l'insieme delle matrici quadrate di "grandezza" $n \geq 2$ fissata forma un anello non commutativo.

Esercizio 1.16. I polinomi ad una variabile formano un anello commutativo?

Esercizio 1.17. Dimostra che $(\{0,1\}, \dot{\vee}, \wedge)$ è un anello commutativo.

Ogni anello $(X, \heartsuit, *)$ gode di alcune proprietà interessanti.

Proposizione 1.4.1 (Proprietà dello Zero[16])**.** $\forall a \in X,\ e * a = a * e = e$.

Dimostrazione. Consideriamo, usando la proprietà distributiva, $a * a = (a \heartsuit e) * a$ quindi, svolgendo i conti, otteniamo $a * a = (a * a) \heartsuit (e * a)$.

In un gruppo additivo valgono le leggi di cancellazione[17], quindi possiamo usarle per l'operazione $\heartsuit$ ed eliminare un $(a * a)$ da entrambe le parti, ottenendo $e = a * e$. Analogo per $e = e * a$. □

Da questo momento in poi chiameremo, quando non sarà ambiguo farlo, "0" l'elemento neutro della prima operazione e "1" l'elemento neutro della seconda. In caso di ambiguità, invece, ci serviremo di un pedice. Inoltre l'inverso della prima operazione, qui indicata con $\heartsuit$ e che di solito è la somma, sarà indicato con un "$-$" davanti (ad esempio $-a$ per a).

Questo cambio di nomi non è stato fatto già a partire dalla Proposizione precedente perché, a mio parere, ne avrebbe perso in bellezza. Invito tuttavia a riscriverla, dimostrazione inclusa, usando 0 al posto di e, per comprenderne il nome e renderla più illuminante e intuitiva.

Proposizione 1.4.2 (Regola dei Segni)**.** $\forall a, b \in X,\ (-a) * b = a * (-b) = -(a * b)$.

Dimostrazione. È una conseguenza della Proposizione precedente e di $0 = b \heartsuit (-b)$, in particolare possiamo scrivere

$$0 = a * 0 = a * (b \heartsuit (-b)) = a * b \heartsuit a * (-b).$$

In altre parole abbiamo ottenuto $0 = a * b \heartsuit a * (-b)$, cioè sappiamo che $a * (-b)$ è l'opposto di $(a * b)$ rispetto all'operazione $\heartsuit$, quindi è uguale a $-(a * b)$. □

Per le scritture utilizzate, un anello banale è l'unico anello in cui accade che lo 0 e l'1 coincidono, volendo: in un anello banale $0_A = 1_A$. Altrimenti vale quanto segue:

Proposizione 1.4.3. *Se $(A, \heartsuit, *)$ è un anello e $|A| \geq 2$ allora $1_A \neq 0$.*

Dimostrazione. Supponiamo $a \in A,\ a \neq 0_A$ allora $a * 1_A = a$ ma, per la proprietà dello zero, $a * 0_A = 0_A$, quindi avendo scelto $a \neq 0_A$ deduciamo che $1_A \neq 0_A$. □

In generale, non possiamo neppure dare per scontato che il prodotto di due numeri diversi da 0 sia, a sua volta, diverso da 0, anzi: in alcuni anelli è addirittura possibile che succeda.

[15] Per ora, ha senso immaginarle come delle "tabelle" di numeri

[16] Ricorda che e è l'elemento neutro dell'operazione $\heartsuit$

[17] Basta eseguire l'operazione di gruppo con l'inverso dell'elemento che si vuole cancellare

Divisore dello zero: un elemento $a \in A,\ a \neq 0$ si dice *divisore dello zero* sse esiste almeno un altro elemento, anch'esso diverso dallo zero, tale che $a * b = 0$ oppure $b * a = 0$ (l'anello non è necessariamente commutativo).

Dominio di Integrità: un anello commutativo privo di divisori dello zero si dice *dominio di integrità*.

In effetti, esiste un fatto interessante a riguardo, di cui però non ci interessa la dimostrazione (è semplice, si può provare a fare come esercizio):

Fatto 1.4.4. *Un anello A è privo di divisori dello zero se e solo se valgono le leggi di cancellazione per il prodotto, ovvero se $\forall a \neq 0, \forall x, y \in A$ si ha che $ax = ay \Rightarrow x = y$ (analogo per $xa = ya$).*

Potrebbe sembrare, a prima vista, molto difficile trovare esempi di *oggetti matematici* che siano allo stesso tempo utili e abbiano divisori dello zero. Un esempio, come anticipato, lo vedremo quando (all'inizio del prossimo capitolo) introdurremo matrici. Un altro esempio piuttosto semplice lo possiamo invece vedere già da ora:

Esempio 1.25. Consideriamo ancora una volta le classi di resto e, in particolare, $\mathbb{Z}/6\mathbb{Z}$ cioè l'insieme degli interi quozientato rispetto alla relazione "a ha lo stesso resto di b nella divisione per 6" con le usuali operazioni di somma e prodotto tra interi. L'insieme $\mathbb{Z}/6\mathbb{Z}$ è quindi un insieme di classi di equivalenza, cioè $\mathbb{Z}/6\mathbb{Z} = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$ che è l'insieme delle classi di tutti i possibili resti nella divisione per 6.

Per fissare le idee: 13 ha resto 1 nella divisione per 6, quindi sta nella classe $[1]_6$; 9 sta nella classe $[3]_6$ e, come ci si aspetterebbe, $22 (= 13+9)$ sta nella classe $[4]_6 = [1]_6 + [3]_6$ (ossia basta sommare il rappresentante). Inoltre $117 (= 13 \cdot 9)$ sta nella classe $[3]_6 = [1]_6 \cdot [3]_6$.

È evidente che $2 \notin [0]_6$ e che anche $3 \notin [0]_6$, infatti nessuno dei due numeri è divisibile per 6, ma $2 \cdot 3 = 6 \in [0]_6$. Quindi il prodotto di due elementi non nulli (ossia $[2]_6$ e $[3]_6$) in $\mathbb{Z}/6\mathbb{Z}$ ha risultato nullo.

Esercizio 1.18. Esistono degli $n \in \mathbb{N}$ per cui $\mathbb{Z}/n\mathbb{Z}$ non ha divisori dello zero?

Ne approfittiamo per dare due ulteriori definizioni:

Numero Primo: un numero $p \in \mathbb{Z},\ p \neq \pm 1$ si dice *primo* se ogni volta che $p \mid a \cdot b$,[18] allora o $p \mid a$ oppure $p \mid b$.

Numero Irriducibile: un numero p è *irriducibile* sse è divisibile soltanto per se stesso e per ± 1.

Quest'ultima definizione è quella che normalmente utilizziamo per indicare cos'è un numero primo. Il motivo è che, seppure in generale non siano definizioni equivalenti, per i numeri interi si può dimostrare che coincidono e, a quel punto, quella "solita" è la più semplice delle due da usare. Nota che 0 in un dominio di integrità è primo.

Esempio 1.26. Se consideriamo l'anello $\mathbb{Z}(\sqrt{-5}) = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ con l'usuale somma e prodotto, il numero 9 si può scomporre sia come $3 \cdot 3$ sia

[18] $a \mid b$ si legge "a divide b".

come $(2+\sqrt{-5})(2-\sqrt{-5})$. Si può provare che tutti e quattro questi fattori sono irriducibili, ma nessuno di essi è primo. Infatti, ad esempio, $3 \mid 9$, ma $3 \nmid (2+\sqrt{-5})$ e $3 \nmid (2-\sqrt{-5})$.

In ogni anello si può dimostrare che ogni primo è anche irriducibile. In realtà in anelli come $\mathbb{Z}$, in cui ogni elemento può essere decomposto in un unico modo come prodotto di irriducibili, si può dimostrare che i due concetti coincidono. Ciò giustifica il classico utilizzo di "numero primo" per indicare un numero che non può essere diviso da elementi diversi da 1 e se stesso[19]. Per ovvi motivi, non proseguiremo oltre in questa direzione. *«Non ti crucciare: vuolsi così colà dove si puote ciò che si vuole, e più non dimandare.»*.

Campi

Tuttavia, però, ci manca da introdurre la struttura algebrica più importante per il nostro obiettivo:

Campo: una terna $(\mathbb{K}, +, \cdot)$ è un *campo* sse $(\mathbb{K}, +, \cdot)$ è un anello commutativo ed ogni elemento di $\mathbb{K}$ diverso dallo zero ammette inverso moltiplicativo.

In genere si usano la lettera $\mathbb{K}$ o $\mathbb{F}$, rispettivamente dal tedesco e dall'inglese. Inoltre, quando le operazione sono ovvie dal contesto, indicheremo una struttura algebrica, specialmente se è un campo, solo tramite il suo insieme: diremo, ad esempio, "il campo $\mathbb{Q}$" per indicare il campo dei numeri razionali con la solita somma e prodotto.

Esempio 1.27. $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ sono, rispettivamente, il campo dei numeri razionali, quello dei numeri reali e quello dei numeri complessi.

Esempio 1.28. Le soluzioni dell'esercizio 1.18, oltre ad essere domini di integrità, sono anche campi. Infatti $\mathbb{Z}/p\mathbb{Z}$ è un campo ogni volta che p è un primo.

Esempio 1.29. Se $\mathbb{K} = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\} = \mathbb{Q}[\sqrt{2}]$, allora $(\mathbb{K}, +, \cdot)$ è un campo.

Esercizio 1.19. Verifica che $\mathbb{Q}[\sqrt{2}]$ è un campo. Che ne pensi di $\mathbb{Q}[\sqrt{-1}]$?[20]

Esercizio 1.20. Dimostra che $\mathbb{Z}/3\mathbb{Z}$ è un campo mentre $\mathbb{Z}/4\mathbb{Z}$ non lo è.

1.5 Introduzione agli Omomorfismi

Quando abbiamo a disposizione due strutture diverse siamo interessati a sapere se sia possibile studiare le caratteristiche di una delle due a partire da quelle, magari più semplici, dell'altra. Prima di tutto abbiamo bisogno di una funzione che leghi i due insiemi, poi, affinché questo "legame" ci sia utile, vorremmo che la funzione considerata si comportasse bene anche nei confronti delle operazioni definite sulle strutture. In che senso?

[19] In realtà, come al solito, è un pelo più complesso di così: si chiede che un irriducibile possa essere diviso solo per elementi invertibili, ovvero che ammettono un inverso multiplicativo,

[20] $\mathbb{Q}[\sqrt{-1}]$ è noto come "Campo dei Quozienti degli Interi di Gauss".

Omomorfismo: se $(A, +, \cdot)$ e $(B, \oplus, \odot)$ sono due anelli, un *omomorfismo* (morfismo di anelli) è un'applicazione $f : A \to B$ che conserva le operazioni nel senso chiarito qui di seguito:

$$f(a_1 + a_2) = f(a_1) \oplus f(a_2) = b_1 \oplus b_2$$
$$f(a_1 \cdot a_2) = f(a_1) \odot f(a_2) = b_1 \odot b_2$$
$$f(1_A) = 1_B$$

dove $b_i = f(a_i)$.

Esercizio 1.21 (*)**.** Secondo te, è essenziale la terza richiesta?[21]

Esercizio 1.22. È sempre vero che $f(0_A) = 0_B$?

La funzione f sugli insiemi può essere di iniettiva, suriettiva o biiettiva e, di conseguenza, classifichiamo l'omomorfismo dato da f:

- si chiama **monomorfismo** un omomorfismo iniettivo;
- si chiama **epimorfismo** un omomorfismo suriettivo;
- si chiama **isomorfismo** un omomorfismo che ammette una funzione inversa che è anch'essa un morfismo[22];
- quando $A = B$ abbiamo un **endomorfismo** che, nel caso sia un isomorfismo, si dirà **automorfismo**.

Fatto 1.5.1. *Se un morfismo di anelli è un monomorfismo e un epimorfismo (quindi se è biiettivo) allora è un isomorfismo*[23]*.*

L'insieme di tutti i possibili morfismi da A a B si indica con $Hom(A, B)$.

Infine, può essere utile introdurre già da ora la nozione di *kernel* (o *nucleo*) di un omomorfismo:

Kernel: il nucleo di un morfismo, indicato con $\ker(f)$, è l'insieme di tutti quegli elementi a di A tali che la loro immagine tramite f è lo 0_B di B, in simboli:

$$\ker(f) \stackrel{\text{def}}{=} \{a \in A \mid f(a) = 0_B\} \stackrel{\text{def}}{=} f^{-1}(0_B).$$

Per ora ci limitiamo ad una trattazione astratta poiché inevitabilmente alcuni esempi significativi di omomorfismo si incontreranno in modo naturale strada facendo.

[21] Considera l'insieme $\mathbb{Z} \times \mathbb{Z}$ con le operazioni seguenti: $(a, b) + (c, d) = (a + c, b + d)$ e $(a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$. (Quali sono lo zero e l'unità di questo anello?) Se prendiamo la funzione $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ data da $f(z) = (z, 0)$, si può mostrare facilmente che questa rispetta le prime due richieste ma l'immagine di 1 è $(1, 0)$ che non è l'unità di $\mathbb{Z}^2$. Quindi esistono funzioni che rispettano le prime due definizioni ma non la terza!

[22] L'idea di isomorfismo è incredibilmente utile: con un isomorfismo si può passare avanti e indietro senza perdere alcuna informazione riguardo alla struttura aggiuntiva che abbiamo messo sugli insiemi. Ovvero, anche di fronte ad insiemi di partenza estremamente diversi tra loro, possiamo identificarli come se fossero la stessa struttura.

[23] Esistono dei contesti più complessi delle strutture algebriche qui introdotte in cui la nozione di morfismo richiede di preservare l'ulteriore struttura che si definisce sugli oggetti. A differenza del caso degli anelli, esistono delle strutture per cui omomorfismo biettivo non implica isomorfismo.