

Università degli studi di Modena e Reggio Emilia
Dipartimento di Ingegneria Enzo Ferrari

Matematica Discreta

Anno Accademico 2023/24

Indice

1	Complementi su insiemi e relazioni	1
1.1	Funzioni	1
1.2	Insiemi Discreti	2
1.2.1	Proprietà 1	4
1.2.2	Proprietà 2	4
1.2.3	Proprietà 3	5
1.2.4	Proprietà 4	6
1.3	Confronto tra Cardinalità	8
1.4	Relazioni di Equivalenza	11
1.5	Congruenza modulo n	12
2	Parte 3	14
2.1	Strutture algebriche elementari	14
2.1.1	Gruppi	14
2.1.2	Anelli	15
2.1.3	Campi	16
2.1.4	Domini d'integrità	16
2.2	L'anello dei numeri interi	16

Capitolo 1

Complementi su insiemi e relazioni

1.1 Funzioni

Una **funzione** o **applicazione** tra due insiemi A e B è rappresentata:

$$f : A \rightarrow B \text{ t.c. } \forall a \in A \exists! b \in B \mid f(a) = b$$

1. la funzione si dice **iniettiva** se:

$$\forall a, a' \in A, f(a) = f(a') \Rightarrow a = a'$$

2. la funzione si dice **suriettiva** se:

$$\forall b \in B, \exists a \in A \mid f(a) = b$$

3. una funzione $f : A \rightarrow B$ si dice **biettiva** o **biunivoca** se è contemporaneamente *iniettiva* e *suriettiva* ovvero se:

$$\forall b \in B \exists! a \in A \text{ t.c. } f(a) = b$$

1.2 Insiemi Discreti

Due insiemi A e B si dicono **equipotenti** (o con la stessa **cardinalità**) se:

$$f : A \rightarrow B, f \text{ biunivoca}$$

E utilizzeremo come notazione: $\text{card}(A) = \text{card}(B)$, $|A| = |B|$ oppure $\#A = \#B$. Un insieme A si dice finito se:

$$\exists n \in \mathbb{N}, f : A \rightarrow \mathbb{N}_n, f \text{ biunivoca}$$

In questo caso diremo che la **cardinalità** di A è **n**: $\text{card}(A) = \text{card}(\mathbb{N}_n) = n$

Un insieme A si dice **numerabile** se:

$$\exists f : A \rightarrow \mathbb{N}, f \text{ biunivoca}$$

In questo caso si dice che A ha cardinalità numerabile e si può rappresentare attraverso la lettera **aleph** (è la prima lettera dell'alfabeto ebraico): $\text{card}(A) = \text{card}(\mathbb{N}) = \aleph_0$.

Alcuni esempi:

1. l'insieme \mathbb{Z} è **numerabile** ($\#\mathbb{N} = \#\mathbb{Z}$):

$$\begin{array}{l} 0 \rightarrow 1 \\ 1 \rightarrow 2 \quad -1 \rightarrow 3 \\ 2 \rightarrow 4 \quad -2 \rightarrow 5 \end{array}$$

possiamo quindi mappare i valori **positivi** dell'insieme \mathbb{Z} sono mappati nei valori **pari** dell'insieme \mathbb{N} e in maniera complementare i valori **negativi** dell'insieme \mathbb{Z} sono mappati nei valori **dispari** dell'insieme \mathbb{N} . È quindi possibile verificare la biunivocità dell'applicazione che mappa i valori da \mathbb{Z} a \mathbb{N} .

2. l'insieme dei numeri **pari** \mathbb{P} può definirsi numerabile, infatti: $\#\mathbb{P} = \#\mathbb{N}$, in questo caso avremo l'applicazione biunivoca del tipo:

$$f : \mathbb{P} \rightarrow \mathbb{N} \mid \forall p = 2n \in \mathbb{P}, f(p) = \frac{1}{2}p = n$$

Un insieme A si dice **discreto** se è **finito** o **numerabile**.

Se A è finito di cardinalità n , i suoi elementi possono essere etichettati con gli elementi di \mathbb{N}_n :

$$A = \{a_1, a_2, \dots, a_n\}$$

Se A è numerabile, gli elementi possono essere “etichettati” con gli elementi di \mathbb{N} :

$$A = \{a_1, a_2, \dots, a_n, \dots\} = \{a_i \mid i \in \mathbb{N}\}$$

Dato un insieme discreto A ed un suo sottoinsieme $Y \subseteq A$ si dice **funzione caratteristica** di Y la funzione:

$$f_Y : A \rightarrow \{0, 1\} \quad \forall a \in A \quad f_Y(a) = \begin{cases} 1 & \text{se } a \in Y \\ 0 & \text{se } a \notin Y \end{cases}$$

Nel caso in cui A sia un insieme finito avremo che: $\#A = \sum_{a \in A} f_Y(a)$.

Se A è un insieme discreto, ed $f : A \rightarrow \{0, 1\}$ una applicazione a valori in $\{0, 1\}$, risulta univocamente determinato il sottoinsieme $Y \subseteq A$ tale che f sia una funzione caratteristica di Y :

$$Y = \{a \in A \mid f(a) = 1\}$$

Un esempio, definiamo $A = \mathbb{N}$ e sia $f : A \rightarrow \{0, 1\}$ definita da una **funzione caratteristica** del tipo: $n \rightarrow \frac{1+(-1)^n}{2}$. In questo caso la funzione f identifica, a partire dall'insieme \mathbb{N} , il sottoinsieme \mathbb{P} dei numeri pari.

Utilizzando la **funzione caratteristica** si può ricavare la seguente proprietà degli insiemi discreti:

- se A è finito di cardinalità n , l'insieme $\mathcal{P}(A)$ delle **parti di A** è in corrispondenza biunivoca con l'**insieme delle n -ple** a valori in $\{0, 1\}$.
- se A è numerabile, l'insieme $\mathcal{P}(A)$ delle parti di A è in corrispondenza biunivoca con l'**insieme delle successioni** a valori in $\{0, 1\}$.

1.2.1 Proprietà 1

Se X e Y sono insiemi **finiti**, con $\#X = n$, $\#Y = m$ e con $X \cap Y = \emptyset$, allora $\#(X \cup Y) = n + m$.

Dimostrazione: per Hp. esistono due funzioni biettive $f : X \rightarrow \mathbb{N}_n$ e $g : Y \rightarrow \mathbb{N}_m$.

Per dimostrare la proprietà occorre costruire una funzione biettiva $h : X \cup Y \rightarrow \mathbb{N}_{n+m}$.

Possiamo porre $\forall c \in X \cup Y$ come:

$$h(c) = \begin{cases} f(c) & \text{se } c \in X \\ g(c) + n & \text{se } c \in Y \end{cases}$$

1.2.2 Proprietà 2

Se X è un insieme **finito** con $\#X = n$ ed Y è un insieme **numerabile**, con $X \cap Y = \emptyset$ allora $\#(X \cup Y)$ è **numerabile**.

Dimostrazione: per Hp. esistono due funzioni biettive $f : X \rightarrow \mathbb{N}_n$ e $g : Y \rightarrow \mathbb{N}$.

Per dimostrare la proprietà occorre costruire una funzione biettiva $h : X \cup Y \rightarrow \mathbb{N}$.

Possiamo porre $\forall c \in X \cup Y$ come:

$$h(c) = \begin{cases} f(c) & \text{se } c \in X \\ g(c) + n & \text{se } c \in Y \end{cases}$$

Off-Topic:

Paradosso del Grand Hotel di Hilbert: il paradosso del *Grand Hotel* inventato dal matematico *David Hilbert* per mostrare alcune caratteristiche del concetto di infinito e le differenze fra opzioni con insieme finiti ed infiniti. Hilbert immagina un hotel con infinite stanze, tutte occupate, e afferma che qualsiasi sia il numero di altri ospiti che sopraggiungano, sarà sempre possibile ospitarli tutti, anche se il loro numero è infinito, purché numerabile.

Nel caso semplice, arriva un singolo nuovo ospite. Il furbo albergatore sposterà tutti i clienti nella camera successiva (l'ospite della 1 alla 2, quello della 2 alla 3, etc.); in questo modo, benché l'albergo fosse pieno è comunque, essendo infinito, possibile sistemare il nuovo ospite.

1.2.3 Proprietà 3

Se X e Y sono due insiemi **numerabili**, allora anche $X \cup Y$ è **numerabile**.

Dimostrazione: senza perdere di generalità, supponiamo che $X \cap Y = \emptyset$. Per ipotesi esistono due funzioni biettive $f : X \rightarrow \mathbb{N}$ e $g : Y \rightarrow \mathbb{N}$. Per dimostrare la proprietà occorre costruire una funzione biettiva $h : X \cup Y \rightarrow \mathbb{N}$. Ad esempio, $\forall c \in (X \cup Y)$, si può porre:

$$h(c) = \begin{cases} 2f(c) - 1 & \text{se } c \in X \\ 2g(c) & \text{se } c \in Y \end{cases}$$

Off-Topic:

Paradosso del Grand Hotel di Hilbert: Un caso meno intuitivo si ha quando arrivano infiniti nuovi ospiti. Sarebbe possibile procedere nel modo visto in precedenza, ma solo scomodando infinite volte gli ospiti (già spazientiti dal precedente spostamento): sostiene allora Hilbert che la soluzione sta semplicemente nello spostare ogni ospite nella stanza con numero doppio rispetto a quello attuale (dalla 1 alla 2, dalla 2 alla 4, etc.), lasciando ai nuovi ospiti tutte le camere con i numeri dispari, che sono essi stessi infiniti, risolvendo dunque il problema. Gli ospiti sono tutti dunque sistemati, benché l'albergo fosse pieno.

Proposizione: se X è un insieme numerabile e $Y \subseteq X$ allora Y è un insieme **discreto**.

1.2.4 Proprietà 4

Se $\{A_i \mid i \in \mathbb{N}\} = \{A_1, A_2, \dots, A_i, \dots\}$ è un **insieme numerabile** di **insiemi numerabili**, si ha che:

$$\#(\bigcup_{i \in \mathbb{N}} A_i) = \#\mathbb{N}$$

Dimostrazione: senza perdere di generalità, supponiamo che gli insiemi siano fra loro **disgiunti**: $A_i \cap A_j = \emptyset$, $\forall i \neq j$. Per dimostrare la tesi, utilizziamo il *procedimento diagonale di Cantor*, enumerando per righe gli elementi di ciascun insieme, dove avremo come primo indice l'identificativo dell'insieme e come secondo indice quello della colonna:

$$\begin{array}{ccccccc} A_1: & a_{11} & a_{12} & a_{13} & \dots & a_{1h} & \dots \\ A_2: & a_{21} & a_{22} & a_{23} & \dots & a_{2h} & \dots \\ A_3: & a_{31} & a_{32} & a_{33} & \dots & a_{3h} & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ A_i: & a_{i1} & a_{i2} & a_{i3} & \dots & a_{ih} & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{array}$$

Consideriamo le diagonali $D_1, D_2, \dots, D_k, \dots$, dove: $D_k = \{a_{ij} \mid i + j = k + 1\}$. E notiamo che sono composte da finiti elementi. Per dimostrare che $\#(\bigcup_{i \in \mathbb{N}} A_i)$ è **numerabile**, occorre costruire una applicazione biunivoca, tale che:

$$h : \bigcup_{i \in \mathbb{N}_n} A_i \rightarrow \mathbb{N}$$

Idealmente, vorremmo etichettare, ogni generico elemento a_{ij} che apparterrà alla k -esima diagonale:

$$\begin{aligned} a_{ij} &\in D_k \\ k &= i + j - 1 \\ a_{ij} &\in D_{(i+j-1)} \end{aligned}$$

Scorrendo ogni diagonale a partire dall'elemento che sta nell'insieme con indice maggiore, incontrerò l'elemento a_{ij} come j -esimo elemento della diagonale a cui esso appartiene, ovvero come j -esimo elemento della diagonale D_{i+j-1} .

Se noi vogliamo numerare la cardinalità delle n diagonali già prese in considerazione prima del nuovo elemento a_{ij} che stiamo esaminando, consideriamo $\#D_k = k$ e avremo:

$$\sum_{k=1}^{i+j-2} \#D_k = \frac{(i+j-2)(i+j-1)}{2}$$

Vista la costruzione delle diagonali questa somma non sarà altro che la somma dei primi $i + j - 2$ numeri naturali:

$$\begin{aligned} \sum_{k=1}^n k &= \frac{n(n+1)}{2} \\ \sum_{k=1}^{i+j-2} k &= \frac{(i+j-2)(i+j-1)}{2} \end{aligned}$$

In questo modo abbiamo trovato un metodo di etichettare tutte le diagonali (e quindi i loro elementi) fino alla diagonale che contiene l'elemento a_{ij} , ma siccome sappiamo che l'elemento a_{ij} è nella j -esima posizione della diagonale $i + j - 1$ allora possiamo definire una applicazione biunivoca che associa ogni elemento dell'unione degli insiemi a \mathbb{N} $h : \bigcup_{i \in \mathbb{N}_n} A_i \rightarrow \mathbb{N}$ definita, $\forall a_{ij} \in \bigcup_{i \in \mathbb{N}_n} A_i$, da:

$$h(a_{ij}) = j + \frac{(i+j-2)(i+j-1)}{2}$$

In questo modo siamo riusciti a “etichettare” tutti gli elementi una e una sola volta.

Conseguenze:

- \mathbb{Z} è numerabile: $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-n \mid n \in \mathbb{N}\}$.
- $\mathbb{N} \times \mathbb{N}$ è numerabile: $\mathbb{N} \times \mathbb{N} = \{(n, m) \mid n, m \in \mathbb{N}\} = \bigcup_{n \in \mathbb{N}} \{(n, m) \mid m \in \mathbb{N}\}$.
- \mathbb{Q} è numerabile.

1.3 Confronto tra Cardinalità

Si dice che un insieme A ha **cardinalità minore o uguale** ad un insieme B (e si indica con: $\#A \leq \#B$) se: $\exists f : A \rightarrow B$, f è *iniettiva*.

Proprietà:

- **riflessività:** $\forall A, \#A \leq \#A$.
- **transitività:** $\#A \leq \#B, \#B \leq \#C \Rightarrow \#A \leq \#C$.
- **antisimmetria:** $\#A \leq \#B, \#B \leq \#A \Rightarrow \#A = \#B$.
- **tricotomia:** $\forall A, B \Rightarrow \#A \leq \#B$ o $\#B \leq \#A$.

La relazione “ \leq ” fra cardinalità è una relazione di ordine totale.

$A \subseteq B \subseteq C$ con $\#A = \#B \Rightarrow \#A = \#B = \#C$.

Teorema di Cantor-Bernstein-Schroeder: Se $\exists f : A \rightarrow B$, f *iniettiva* ed $\exists g : B \rightarrow A$, g *iniettiva* allora $\exists h : A \rightarrow B$, h *biunivoca*.

Dimostrazione: poiché f e g sono iniettive se le restringiamo alla loro immagine biunivoca:

$$\#A = \#f(A) \text{ con } f(A) \subseteq B$$

$$\#B = \#g(B) \text{ con } g(B) \subseteq A$$

Avremo:

$$g(f(A)) \subseteq g(B) \subseteq A \Rightarrow \#g(f(A)) = \#f(A) = \#A$$

e per il [lemma](#) possiamo dire che $\#g(B) = \#A$ e $\#g(B) = \#B$ e quindi avremo che $\#A = \#B$, questo implica che esiste una funzione $h : A \rightarrow B$ biunivoca.

Teorema di Cantor: se A è un insieme **numerabile** allora $\mathcal{P}(A)$ ha cardinalità **maggiore** di A :

$$\#A \leq \#\mathcal{P}(A) \text{ con } \#A \neq \#\mathcal{P}(A)$$

Dimostrazione:

- dimostriamo per prima cosa che $\#A \leq \#\mathcal{P}(A)$ basta trovare una funzione definita $f : A \rightarrow \mathcal{P}(A)$ che sia **iniettiva** e non biunivoca.

$$f(a) = \{a\}$$

Utilizziamo una **dimostrazione per assurdo**: sappiamo che $\mathcal{P}(A)$ è in corrispondenza biunivoca con le successioni a valori in $\{0, 1\}$; allora se $\mathcal{P}(A)$ fosse numerabile sarebbe possibile elencare tutte le successioni a valori in $\{0, 1\}$:

$$\begin{array}{ccccccc} S_1: & S_{11} & S_{12} & S_{13} & \dots & S_{1n} & \dots \\ S_2: & S_{21} & S_{22} & S_{23} & \dots & S_{2n} & \dots \\ S_3: & S_{31} & S_{32} & S_{33} & \dots & S_{3n} & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ S_j & S_{j1} & S_{j2} & S_{j3} & \dots & S_{jn} & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{array}$$

Consideriamo la successione a valori in $\{0, 1\}$:

$$\bar{S} = \bar{S}_1, \bar{S}_2, \bar{S}_3, \dots, \bar{S}_j, \dots \text{ || dove } \bar{S}_j \neq S_{jj}$$

In questo modo la successione \bar{S} non coincide con nessuna delle successioni s_j , $\forall j \in \mathbb{N}$, poiché differisce dalla j -esima successione nel j -esimo elemento e quindi arriviamo ad un **assurdo**. Quindi l'insieme delle successioni a valori in $\{0, 1\}$ non può essere numerabile e, quindi, **non** è **numerabile** nemmeno $\mathcal{P}(A)$.

La Cardinalità di \mathbb{R} : anche \mathbb{R} **non** è **numerabile**, infatti: $\#\mathbb{R} = \#]0, 1[$, consideriamo un'applicazione biunivoca tale che $f : \mathbb{R} \rightarrow]0, 1[$, ad esempio:

$$f(x) = \frac{x}{|x|+1} \quad \forall x \in \mathbb{R}$$

che stabilisce biunivocità tra \mathbb{R} e $] - 1, 1[$ possiamo affermare che $\#\mathcal{P}(\mathbb{N}) = \#]0, 1[$, infatti considerando $\forall x \in]0, 1[$ come la rappresentazione binaria (con virgola) di x ; se ϵ_n è l' n -esima cifra dopo la virgola di tale sviluppo $(\epsilon_1, \epsilon_2, \dots, \epsilon_n, \dots)$ è una successione a valori in $\{0, 1\}$ quindi

$$0, \bar{9} = 1 \in \mathbb{R} \parallel \text{viene a perdersi la biunivocità} \\ \Rightarrow \#\mathbb{R} = \#\mathcal{P}(\mathbb{N})$$

Questa tipologia di cardinalità viene definita **cardinalità del continuo** e si denota con \mathfrak{c} o con 2^{\aleph_0} .

Congettura (ipotesi del continuo): non esistono cardinalità comprese fra $\#\mathbb{N}$ e $\#\mathbb{R}$.

Congettura (ipotesi generalizzata del continuo): non esistono cardinalità comprese tra $\#X$ e $\mathcal{P}(X) = 2^{\#X} \forall X$ di cardinalità non finita.

1.4 Relazioni di Equivalenza

Una **relazione** \mathcal{R} tra due insiemi A e B è un **sottoinsieme** del **prodotto cartesiano** fra A e B , ovvero $\mathcal{R} \in A \times B$.

Esempio: $\mathcal{R} = '\leq'$ è relazione tra i due insiemi $A = \mathbb{N}$ e $B = \mathbb{N}$, poiché definisce un sottoinsieme del prodotto cartesiano $\mathbb{N} \times \mathbb{N}$.

Ad esempio: $(1, 2) \in \mathcal{R}$ e $(2, 1) \notin \mathcal{R}$.

Una relazione \mathcal{R} su A si dice **relazione di equivalenza** se sono vere le seguenti proprietà:

- *riflessività*: $\forall a \in A \Rightarrow a\mathcal{R}a$
- *simmetria*: $\forall a, b \in A : a\mathcal{R}b \Rightarrow b\mathcal{R}a$
- *transitività*: $\forall a, b, c \in A : a\mathcal{R}b \text{ e } b\mathcal{R}c \Rightarrow a\mathcal{R}c$

Definizione: sia \mathcal{R} una **relazione di equivalenza** su A . Per ogni $a \in A$ si dice **classe di equivalenza** $[a] = \{x \in A \mid x\mathcal{R}a\}$.

Proprietà:

- $\forall a \in A, a \in [a]$

Dimostrazione: è conseguenza diretta della proprietà riflessiva.

- $\forall a, b \in A, a \in [b] \Rightarrow [b] = [a]$

Dimostrazione: poiché $a \in [b]$, $a\mathcal{R}b$. Se $x \in A$, $x \in [a]$, allora $x\mathcal{R}a$; per la **proprietà transitiva** segue $x\mathcal{R}b$ ovvero $x \in [b]$. Resta così dimostrato che $[a] \subseteq [b]$. Analogamente, se $y \in A$, $y \in [b]$, allora $y\mathcal{R}b$ per la **proprietà di simmetria**, $a\mathcal{R}b \Rightarrow b\mathcal{R}a$, per cui la transitività assicura $y\mathcal{R}a$, ovvero $y \in [a]$. Resta così dimostrato che $[b] \subseteq [a]$ e quindi $[b] = [a]$.

- $\forall a, b \in A, [a] = [b] \text{ oppure } [a] \cap [b] \neq \emptyset$

Dimostrazione: se $\exists c \in [a] \cap [b]$, si ha $c \in [a]$ e $c \in [b]$, ovvero $c\mathcal{R}a$ e $c\mathcal{R}b$. Applicando la **proprietà di simmetria** a $c\mathcal{R}a$ si ottiene $a\mathcal{R}c$, per cui la proprietà

transitiva assicura $a\mathcal{R}b$, ovvero $a \in [b]$. La seconda proprietà implica $[a] = [b]$.

Quindi, se due classi hanno un elemento in comune, le due classi coincidono.

Insieme Quoziente: sia A un insieme ed \mathcal{R} una relazione di equivalenza su A . Si definisce **insieme quoziente** di A rispetto ad \mathcal{R} ,

$$\frac{A}{\mathcal{R}} = \{[a] \mid a \in A\}$$

Rappresentante di una classe d'equivalenza: sia A un insieme ed \mathcal{R} una relazione di equivalenza su A . Ogni elemento $x \in [a]$, si dice **Rappresentante** di $[a] \in \frac{A}{\mathcal{R}}$. Sia \mathcal{R} la relazione di equivalenza su \mathbb{R} definita da:

$$(a, b) \in \mathcal{R} \text{ se e solo se } a - b \in \mathbb{Z}$$

L'insieme quoziente $\frac{\mathbb{R}}{\mathcal{R}}$ è in corrispondenza biunivoca con $[0, 1[$: ogni classe può infatti avere come rappresentante significativo il suo unico elemento nell'intervallo $[0, 1[$.

Esempio: sia \mathcal{R} la relazione di equivalenza su $\mathbb{N}_0 \times \mathbb{N}_0$ definita da:

$$(a, b)\mathcal{R}(a', b') \text{ se e solo se } a + b' = a' + b$$

In generale:

- se $a = b$, $[(a, b)] = \{(n, n) \mid n \in \mathbb{N}\}$
- se $a < b$, $[(a, b)] = \{(n, n + b - a) \mid n \in \mathbb{N}\}$
- se $a > b$, $[(a, b)] = \{n + a - b, n \mid n \in \mathbb{N}\}$

Allora l'insieme quoziente $\frac{\mathbb{N}_0 \times \mathbb{N}_0}{\mathcal{R}}$ è in relazione biunivoca con \mathbb{Z} .

1.5 Congruenza modulo n

Definizione: fissa un intero $n \in \mathbb{N}$, si definisce una relazione di equivalenza \equiv_n su \mathbb{Z} :

$$x \equiv_n y \text{ se e solo se } \exists h \in \mathbb{Z} \mid y - x = h \cdot n$$

Verifichiamo che \equiv_n è una **relazione di equivalenze**:

- **riflessività**: $\forall x \in \mathbb{Z}, x \equiv_n x$ è verificato, poiché $x - x = h \cdot n$ considerando $h = 0 \in \mathbb{Z}$.
- **simmetria**: se $x \equiv_n y$, per definizione $\exists h \in \mathbb{Z}$ tale che $y - x = h \cdot n$. Per dimostrare che $y \equiv_n x$ devo trovare un $h' \in \mathbb{Z} \mid x - y = h' \cdot n$. Basta prendere $h' = -h$.
- **transitività**: se $x \equiv_n y$ e $y \equiv_n z$, allora $\exists h \in \mathbb{Z} \mid y - x = h \cdot n$ ed $\exists k \in \mathbb{Z} \mid z - y = k \cdot n$. Sommando membro a membro, si ottiene $z - x = (h + k) \cdot n$; siccome $h + k \in \mathbb{Z}$ segue che $x \equiv_n z$.

Insieme delle classi resto modulo n: l'insieme quoziente \mathbb{Z}/\equiv_n è detto **insieme delle classi resto modulo n** ed è indicato con \mathbb{Z}_n : $\mathbb{Z}_n = \frac{\mathbb{Z}}{\equiv_n}$.

L'insieme delle classi resto modulo n è costituito da:

$$\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$$

Dimostrazione: Per ogni $x \in \mathbb{Z}$, la divisione euclidea per n assicura che $\exists q, r \in \mathbb{Z}, 0 \leq r < n$ tali che $x = q \cdot n + r$, ovvero che $x - r = q \cdot n$. Quindi, $x \equiv_n r$, da cui $[x] = [r]$, con $r \in \{0, 1, \dots, n-1\}$.

Occorre provare che le n classi $[0], [1], \dots, [n-1]$ sono a due a due disgiunte, ovvero che $\forall r, s \in \mathbb{Z}, 0 \leq r < s < n \Rightarrow [r] \neq [s]$. Per **assurdo** supponiamo $[r] = [s]$, questo significherebbe che $\exists h \in \mathbb{Z} \mid s - r = h \cdot n$. Per ipotesi $s > r$, per cui $0 < s - r < n$; quindi $s - r$ **non** può essere multiplo intero di n .

Divisione euclidea: $\forall a, b \in \mathbb{Z}, b \neq 0 \Rightarrow \exists q, r \in \mathbb{Z}, 0 \leq r < |b| \mid a = b \cdot q + r$.

Sia A un insieme; un sottoinsieme $\mathcal{B} \subseteq \mathcal{P}(A)$ è detto **ricoprimento** di A se $\forall x \in A, \exists B \in \mathcal{B} \mid x \in B$.

$\mathcal{B} \subseteq \mathcal{P}(A)$ è detto **partizione** di A se $\emptyset \notin \mathcal{B}$ e $\forall c \in A, \exists! B \in \mathcal{B} \mid x \in B$.

Se \mathcal{R} è relazione di equivalenza su A , allora l'insieme quoziente $\frac{A}{\mathcal{R}} = \mathcal{B}$ è una partizione di A . Viceversa se \mathcal{B} è una partizione di A , $\exists! \mathcal{R}$ relazione di equivalenza su A tale che $\frac{A}{\mathcal{R}} = \mathcal{B}$ allora \mathcal{R} è definita da:

$$x\mathcal{R}y \Leftrightarrow \exists B \in \mathcal{B} \mid x, y \in B$$

Capitolo 2

Parte 3

2.1 Strutture algebriche elementari

Una **operazione binaria intera** su un insieme G è un'applicazione

$$* : G \times G \rightarrow G$$

L'immagine della coppia (x, y) si denoterà con $x * y$.

- $e \in G$ si dice **elemento neutro** rispetto a $*$ se:

$$g * e = e * g = g \quad \forall g \in G$$

- un elemento $g \in G$ si dice invertibile se esiste $\bar{g} \in G$ tale che $g * \bar{g} = \bar{g} * g = e$

2.1.1 Gruppi

La coppia $(G, *)$, con $*$ operazione su G , si dice **gruppo** se vengono rispettate le seguenti proprietà:

- $*$ è **associativa**: $\forall g, g', g'' \in G$ si ha $(g * g') * g'' = g * (g' * g'')$
- esiste l'elemento **neutro**
- ogni elemento di G è invertibile

Il gruppo si dice **abeliano** o **commutativo** se:

$$\forall g, g' \in G, g * g' = g' * g \text{ (proprietà **commutativa**)}$$

Alcuni **esempi**:

- $(\mathbb{N}, +)$, (\mathbb{Z}, \cdot) non sono gruppi. in quanto non né in \mathbb{N} e \mathbb{Z} sono presenti per ogni elemento dell'insieme dell'elemento inverso, in \mathbb{N} non sono presenti elementi negativi, quindi nessun elemento avrà un'altro che sommato a se stesso dia 0, viceversa l'insieme \mathbb{Z} che sono presenti elementi positivi e negativi viene definita l'operazione \cdot richiede i reciproci dei singoli elementi affinché possano essere definiti gli elementi inversi.
- $(\mathbb{Z}, +)$, (\mathbb{Q}, \cdot) sono gruppi abelliani

2.1.2 Anelli

La terna $(\mathbb{A}, +, \cdot)$ con \mathbb{A} un insieme e $+$, \cdot (somma e prodotto) due operazione binarie interne a \mathbb{A} , si dice **anello** se:

- $(\mathbb{A}, +, \cdot)$ è un gruppo **abeliano** (con elemento neutro 0).
- il prodotto è **associativo**.
- per ogni $x, y, z \in \mathbb{K}$ si ha $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ e $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ (il prodotto è distribuito rispetto alla somma).

Un anello $(\mathbb{A}, +, \cdot)$ è detto **commutativo** se il prodotto è commutativo, mentre è detto **unitario** o con **unità** se (\mathbb{A}, \cdot) ammette l'elemento neutro. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sono anelli.

2.1.3 Campi

La terna $(\mathbb{K}, +, \cdot)$ con \mathbb{K} un insieme e $+$, \cdot (somma e prodotto) due operazioni binarie interne a \mathbb{K} , si dice **campo** se:

- $(\mathbb{K}, +)$ è un gruppo **abeliano** (con elemento neutro 0).
- $(\mathbb{K} - \{0\}, \cdot)$ è un gruppo **abeliano** (con elemento neutro 1).
- per ogni $x, y, z \in \mathbb{K}$ si ha $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ quindi il prodotto è distribuito rispetto alla somma.

In qualunque campo vale la **legge di annullamento del prodotto**:

$$x \cdot y = 0 \rightarrow x = 0 \text{ oppure } y = 0$$

2.1.4 Domini d'integrità

Divisori dello zero: sia $(A, +, \cdot)$ un anello. Due elementi $a, b \in A$ si dicono **divisori dello zero** se $a \neq 0$, $b \neq 0$, ma $a \cdot b = 0$. Ad **esempio** l'anello delle matrici quadrate presenta dei divisori dello zero.

Un anello commutativo privo di divisori dello zero si dice **dominio di integrità**, ad **esempio** $(\mathbb{Z}, +, \cdot)$ è un anello commutativo unitario privo di divisori dello zero. Quindi è dominio di integrità.

2.2 L'anello dei numeri interi

È noto che $\exists h \mid h : \mathbb{Z} \rightarrow \frac{\mathbb{N}_0 \times \mathbb{N}_0}{\mathcal{R}}$ dove la relazione di equivalenza che si vuole definire è \equiv_n . Su questo insieme vengono **ben poste** le seguenti operazioni:

$$\begin{aligned} \boxplus : \mathbb{Z} \times \mathbb{Z} &\rightarrow \mathbb{Z} \\ ((m, n), (m', n')) &\mapsto [(m, n)] \boxplus [(m', n')] \stackrel{\text{def}}{=} [(m + m', n + n')] \\ \boxdot : \mathbb{Z} \times \mathbb{Z} &\rightarrow \mathbb{Z} \\ ((m, n), (m', n')) &\mapsto [(m, n)] \boxdot [(m', n')] \stackrel{\text{def}}{=} [(mm' + nn', mn' + m'n)] \end{aligned}$$

Definito questo possiamo dire che $(\mathbb{Z}, \boxplus, \boxdot)$ è **dominio di integrità**.

2.3 Teoria della Divisibilità