BREVE CENNO DI LOGICA CLASSICA

La **logica** può essere definita come la scienza che studia le condizioni in base alle quali un ragionamento risulta *corretto* e *vero*. Un ragionamento è corretto se segue uno schema logico valido. Per esempio:

"se A è B e B è C allora A è C".

L'esempio più classico di questo tipo di ragionamento è:

" Socrate è un uomo, tutti gli uomini sono mortali, allora Socrate è mortale".

In questo caso

- A: Socrate
- B: uomo
- C: mortale

Si tratta di un ragionamento non solo corretto, ma anche vero nella sua conclusione. Il ragionamento:
"l'asino è un animale, gli animali sono volatili, allora l'asino vola" è corretto come il primo, ma non è vero nella sua conclusione, perchè si basa su un giudizio ("gli animali sono volatili") falso. Infine il ragionamento:

"il canguro è un marsupiale, i marsupiali sono animali, dunque Socrate è mortale"

non è corretto nel suo schema logico, ma il giudizio finale è corretto.

Si pongono alcune definizioni.

Definizione 1. Il **concetto** è la rappresentazione universale di qualcosa.

Bisogna fare attenzione a non confondere il concetto e l'immagine: entrambi contengono un certo messaggio, ma si distinguono in quanto uno dipende dal "pensare" e l'altra dal "sentire". Le immagini rappresentano aspetti sensibili delle cose, i concetti ne rappresentano il contenuto intelligibile. Ad esempio, quando si parla del concetto di uomo, non si pensa ad un particolare essere umano, ma all'essere vivente che ha tutte le caratteristiche umane. Se si vede un oggetto di colore giallo, se ne riconosce il colore proprio perchè si ha il concetto di giallo.

Definizione 2. Il **giudizio** è l'operazione per la quale viene negato o affermato un concetto rispetto ad un'altro: in altre parole, il giudizio, rispettivamente, unisce o divide tra loro due concetti.

Esempio 1. Dicendo: "l'informatico è un uomo", si uniscono i concetti "informatico" e "uomo"; dicendo "il serpente non è un mammifero", i concetti "serpente" e "mammifero" vengono separati.

Definizione 3. I due concetti che vengono "uniti" o "divisi" nel giudizio costituiscono la **materia** del giudizio. In particolare la materia è formata da

- **soggetto**
- **predicato**.

L'*affermazione* e la *negazione*, che, rispettivamente uniscono o dividono soggetto e predicato, costituiscono la **forma** del giudizio.

Esempio 2. Nell'Esempio 1, nel giudizio "l'informatico è un uomo", naturalmente "informatico" è il soggetto, "uomo" è predicato e la forma del giudizio è un'affermazione; nel giudizio "il serpente non è un mammifero" il soggetto è "serpente", il predicato è "mammifero" e il giudizio è una negazione.

La branca della logica detta **logica formale** si occupa della correttezza di un ragionamento, che dipende esclusivamente dalla *forma*, ovvero dal fatto che il ragionamento si adatti a certe regole formali.

D'altra parte, la **logica materiale** riguarda la *materia* del ragionamento e studia la verità di un ragionamento.

Definizione 4. Una **proposizione** è una frase mediante la quale un soggetto viene legato mediante il verbo essere (**copula**) ad un predicato. Quindi la proposizione è formata dai seguenti elementi:

- soggetto
- predicato
- copula.

Osservazione 1. Definita in questi termini, una proposizione potrebbe essere vera o falsa: questo può essere stabilito tramite il *giudizio*, che è un'operazione dell'intelletto.

Esempio 3. "L'informatico è un uomo" è una proposizione ed è vera, mentre "il serpente è un mammifero" è una proposizione falsa.

Bisogna dire che logica classica è riduttiva perchè incapace di render conto finanche del linguaggio naturale. Inoltre ci sono aspetti di questo linguaggio, come il contesto o l'intonazione, che certamente la logica non riesce ad esprimere, ma spesso il significato della frase dipende proprio da questi elementi.

Invece, nel caso del linguaggio matematico, la logica è abbastanza appropriata. Anche in questo caso, però non si usa rigorosamente la formalizzazione logica, perchè il discorso ne risulterebbe eccessivamente appesantito.

CENNI DI LOGICA

Alla base della logica (matematica) ci sono le così dette *proposizioni atomiche*, o *dichiarative*, ovvero le proposizioni (nel senso della logica classica) delle quali (tramite giudizio) si possa affermare con certezza se sono vere o false. Se una proposizione atomica è vera, ad essa si attribuisce valore di verità V (o T o anche 1), se è falsa si attribuisce ad essa valore di verità F (o 0).

Esempio 4.

1. P: 8 è un numero primo
2. Q: il cane è un mammifero.

Certamente la proposizione P è falsa, la proposizione Q è vera. Quindi il valore di verità di P è F, il valore di verità di Q è V.

Esempio 5. Le proposizioni

3. R: Marco è simpatico
4. S: x è pari

non possono essere classificate come proposizioni atomiche: R perchè presenta un predicato che non è di carattere oggettivo, per cui ciascuno può attribuire valore di verità V o F secondo i propri sentimenti; S presenta una variabile e quindi, come si vedrà in seguito, è una *funizone proposizionale*. Si può assegnare a S valore di verità se si definisce l'universo in cui varia x e inoltre si effettua una delle seguenti operazioni

(1) si sostituisce a x un determinato valore
(2) si fa precedere la x da un quantificatore.

I quantificatori sono:

- il *quantificatore universale* $\forall$ (si legge "per ogni")
- il *quantificatore esistenziale* $\exists$ (si legge "esiste")

Se l'universo nel quale varia x è l'insieme $\mathbb{Z}$ dei numeri interi, sostituendo a x i valori 6 e -3, per esempio, S diventa:
"6 è positivo" che ha valore di verità V;
"-3 è positivo" che ha valore di verità F.
Se si usano i quantificatori, si ha:
"$(\forall x)$ (x è positivo)" che ha valore di verità F;
"$(\exists x)$ (x è positivo)" che ha valore di verità V.

Le proposizioni atomiche possono essere combinate tramite i connettivi logici.

Definizione 5. (NEGAZIONE)
Data una proposizione P, la negazione della proposizione P si indica con

$$\bar{P} \text{ oppure } \neg P.$$

Se P è vera allora $\neg P$ è falsa. Se P è falsa allora $\neg P$ è vera.

Esempio 6. P: "Gli iscritti al primo anno di Informatica presso l'università di Bari sono meno di 100" ha valore di verità F.
Allora
$\neg P$: "Non è vero che gli iscritti al primo anno di Informatica presso l'università di Bari sono meno di 100" ha valore di verità V.
$\neg P$ si può scrivere anche: "Gli iscritti al primo anno di Informatica presso l'università di Bari sono più di 100" (sempre con valore di verità V).

Esempio 7. P: "L'Italia è una Repubblica" ha valore di verità V.
Allora
$\neg P$: "L'Italia non è una Repubblica" ha valore di verità F.

Dalla definizione si deduce subito la tavola di verità della negazione

P	$\neg P$
V	F
F	V

Definizione 6. (CONGIUNZIONE)
Siano P e Q due proposizioni. La proposizione "P e Q"(congiunzione di P e Q) si denota con

$$P \wedge Q.$$

È vera quando P e Q sono entrambe vere ed è falsa altrimenti (ovvero falsa quando almeno una delle due è falsa).

La tavola di verità della congiunzione è:

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

Esempio 8.

P: Torino è la capitale d'Italia.
Q: 16 è un numero pari.

Allora la congiunzione di P e Q è:

$P \wedge Q$: Roma è la capitale d'Italia e 16 è un numero pari.

Certamente $P \wedge Q$ ha valore di verità F perchè Q ha valore di verità V ma P ha valore di verità F.

Esempio 9.

P: 12 è multiplo di 3
Q: $\frac{1}{2}$ non è un numero intero.

Allora la congiunzione di P e Q è:

$P \wedge Q$: 12 è multiplo di 3 e $\frac{1}{2}$ non è un numero intero.

Certamente $P \wedge Q$ ha valore di verità V perchè P e Q hanno valore di verità V.

Definizione 7. (DISGIUNZIONE)
Siano P e Q due proposizioni. La proposizione "P o Q"(disgiunzione di P e Q) si denota con

$$P \vee Q$$

ed è falsa quando P e Q sono entrambe false ed è vera altrimenti (ovvero vera quando almeno una delle due è vera).

Si deduce la tavola di verità della disgiunzione:

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

Esempio 10.

P: La macchina ha il motore diesel.
Q: La macchina ha il motore a benzina.

Allora la disgiunzione di P e Q:

$P \vee Q$: La macchina ha il motore diesel o a benzina.

Naturalmente $P \vee Q$ ha valore di verità V.

Definizione 8. (IMPLICAZIONE)
Siano P e Q due proposizioni. La proposizione implicazione "P implica Q"si denota con

$$P \longrightarrow Q.$$

È falsa quando P è vera e Q è falsa ed è vera altrimenti.

Si può scrivere la tavola di verità della implicazione

P	Q	$P \longrightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Quindi se P è vera Q, è vera, se P è falsa non si può stabilire la verità di Q.

Esempio 11.

P: Il cellulare funziona.
Q: La batteria del cellulare è carica.

L'implicazione è:

$P \longrightarrow Q$: Se il cellulare funziona, allora la batteria è carica.

Se il cellulare non funziona, potrebbe essere scarica la batteria o potrebbe esserci qualche altro problema e quindi .

Definizione 9. (DOPPIA IMPLICAZIONE o EQUIVALENZA)
Due proposizioni P e Q si dicono equivalenti e si scrive

$$P \longleftrightarrow Q,$$

se $(P \longrightarrow Q) \wedge (Q \longrightarrow P)$.

La tavola di verità dell'equivalenza è:

P	Q	$P \longrightarrow Q$	$Q \longrightarrow P$	$(P \longrightarrow Q) \wedge (Q \longrightarrow P)$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

Definizione 1. Siano P e Q formule della logica proposizionale. Si dice che Q è conseguenza logica di P e si scrive

$$P \Longrightarrow Q$$

quando Q è vera ogni qualvolta è vera P.

Dalla definizione segue subito che Q non può essere falsa quando P è vera.

Osservazione 1. Dire che Q è conseguenza logica di P vuol dire che certamente Q ha valore di verità V quando P ha valore di verità V.

Definizione 2. Si dice che P e Q sono semanticamente equivalenti se P è conseguenza logica di Q e Q è conseguenza logica di P; ovvero se $P \Longrightarrow Q$ e $Q \Longrightarrow P$. Si scrive

$$P \Longleftrightarrow Q$$

Osservazione 2. Si può anche parlare di conseguenza logica di più di una formula della logica proposizionale: vale a dire se $P_1, \ldots, P_k, Q$ sono $k+1$ formule e se Q è vera quando sono vere $P_1, \ldots, P_k$, si dice che Q è consegueza logica di $P_1, \ldots, P_k$ e si scrive:

$$(P_1, \ldots, P_k) \Longrightarrow Q$$

Esempio 1. Siano P e Q due formule della logica proposizionale. Allora Q è conseguenza logica di P e di $P \longrightarrow Q$. In simboli:

$$(P, P \longrightarrow Q) \Longrightarrow Q.$$

Infatti, considerata la tavola di verità:

P	**Q**	**P** $\longrightarrow$ **Q**	**Q**
V	V	V	V
V	F	F	F
F	V	V	V
F	F	V	F

si osserva che nell'unico caso (il primo) nel quale sia P che $P \longrightarrow Q$ hanno valore di verità V, anche Q ha valore di verità V.
Dalla tavola di verità si evince anche che P non è conseguenza logica di Q e di $P \longrightarrow Q$, perchè nella terza riga Q e $P \longrightarrow Q$ hanno valore di verità V, ma P ha valore di verità F.

Esempio 2. Siano A e B due formule. Si osserva facilmente che $A \wedge B$ non è conseguenza logica di $A \vee B$, in quanto se A ha valore di verità V e B ha valore di verità F, allora $A \vee B$ ha valore di verità V, ma $A \wedge B$ ha valore di verità F.

Proposizione 1. *Siano P e Q due formule della logica proposizionale. Allora P e Q sono semanticamente equivalenti se e solo se hanno la stessa tavola di verità.*

Dimostrazione. Se P ha valore di verità V, allora anche Q deve avere valore di verità V, perchè Q è conseguenza logica di P. Se P ha valore di verità F, allora anche Q deve avere valore di verità F, altrimenti P non potrebbe essere conseguenza logica di Q. La dimostrazione si completa facilmente scambiando i ruoli di P e Q fra loro.

Osservazione 3. Si osserva facilmente, come conseguenza della precedente proposizione, che due formule sono semanticamente equivalenti se e soltanto se $P \longleftrightarrow Q$ è una tautologia.

Esempio 3. Siano P e Q formule. Allora sono semanticamente equivalenti $P \longrightarrow Q$ e $\neg Q \longrightarrow \neg P$, ovvero:

$$(P \longrightarrow Q) \Longleftrightarrow (\neg Q \longrightarrow \neg P).$$

Si prova utilizzando la proposizione precedente, con la seguente tavola di verità:

P	**Q**	$\neg$**P**	$\neg$**Q**	**P** $\longrightarrow$ **Q**	$\neg$**Q** $\longrightarrow$ $\neg$**P**
V	V	F	F	V	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

Esercizi 1. Siano P e Q formule. Provare che valgono le seguenti equivalenze semantiche:

(1) $P \longrightarrow Q \iff \neg(P \wedge \neg Q)$
(2) $P \longrightarrow Q \iff \neg P \vee Q$
(3) $\neg(P \vee Q) \iff \neg P \wedge \neg Q$
(4) $\neg(P \wedge Q) \iff \neg P \vee \neg Q$.

Una teoria matematica si basa su un certo numero di assiomi assegnati su una certe struttura, a partire dai quali si dimostrano i **Teoremi**. Ma cos'è una dimostrazione? è la costruzione di una serie di argomentazioni consistenti che portino infine ad un'affermazione vera. Per dimostrare la validità di un argomento si potrebbe sempre far ricorso alle tavole di verità. Però questo potrebbe essere un procedimento molto lungo e noioso: se ci sono molte variabili proposizionali, le relative tavole di verità possono diventare ingestibili. Per questo si utilizzano le **regole di inferenza** o **metateoremi** che forniscono dei modelli per costruire argomentazioni anche molto complicate. La più usata delle regole di inferenza è

$$(P \wedge (P \longrightarrow Q)) \Longrightarrow Q \quad \text{MODUS PONENS.}$$

Sostanzialmente: dalla validità in contemporanea di P e di $P \longrightarrow Q$ segue la validità di Q. Questa regola di inferenza dà luogo al classico metodo di dimostrazione diretta.

Un altra regola di inferenza è

$$(P \longrightarrow Q) \iff (\neg Q \longrightarrow \neg P) \quad \text{MODUS TOLLENS,}$$

che permette di eseguire le dimostrazioni usando il metodo di dimostrazione indiretta o per contrapposizione.

Si segnalano, inoltre:

$$((P \longrightarrow Q) \wedge (Q \longrightarrow R)) \longrightarrow (P \longrightarrow R)$$

$$(P \wedge Q) \longrightarrow P$$

$$P \longrightarrow (P \vee Q).$$

Un altro tipo di dimostrazioni sono quelle per **contraddizione** o **assurdo**. Si procede nel modo seguente: si vuol provare che P è vero, allora si suppone che $\neg P$ non sia vero e si ottiene una contraddizione di tipo $Q \wedge \neg Q$.

Predicati

La logica proposizionale naturalmente non è in grado di comprendere tutti i possibili enunciati della matematica. Si pone la seguente:

Definizione 3. Un **predicato** è un'affermazione che coinvolge una o più variabili: $x, y, z \ldots$, ciascuna delle quali sia variabile in un *dominio* o *universo* D_x, D_y, $D_z, \ldots$.

Ad un predicato, in generale, non si può attribuire valore di verità: lo si può a fare nel momento in cui si inseriscono opportunamente i quantificatori o si effettuano sostutuzioni al posto delle variabili.

Per approfondimenti sulla logica, lo studente può consultare il libro

A. FACCHINI: **ALGEBRA E MATEMATICA DISCRETA**, ed. ZANICHELLI

alle pagine 283-298 (capitolo 5)

Definizione 1. Si dice che due insiemi X e Y sono *equipotenti* Y se esiste una bigezione tra X e Y.

Definizione 2. Si dice che un insieme X è *infinito* se esiste un'applicazione ingettiva ma non surgettiva di X in X.

Esempio 1. Sicuramente l'insieme $\mathbb{N}$ dei numeri naturali è infinito in quanto per esempio l'applicazione $f : \mathbb{N} \to \mathbb{N}$ tale che per ogni $n \in \mathbb{N}$ $f(n) = 2n$, è ingettiva ma non surgettiva.

Osservazione 1. Se X è un insieme infinito ed è contenuto in un insieme Y, allora anche Y è infinito. Quindi gli insiemi numerici $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sono infiniti in quanto contengono $\mathbb{N}$.

Definizione 3. Si dice che un insieme X è *finito* se è vuoto o se non è infinito.

Teorema 1. *Sia X un insieme finito non vuoto. Allora esiste $n \in \mathbb{N}$ ed ed esiste un'applicazione bigettiva $\gamma : J_n \to X$, dove $J_n = \{1, 2, \ldots, n\}$.*

Osservazione 2. Nella situazione del Teorema 1, si può scrivere

$$X = \{\gamma(1), \gamma(2), \ldots, \gamma(n)\}.$$

Inoltre si dice che X ha *cardinalità* n e si scrive:

$$|X| = n.$$

Osservazione 3. Due insiemi finiti X e Y sono equipotenti se e solo se hanno la stessa cardinalità (verificata a lezione).

Definizione 4. Un'applicazione bigettiva di un insieme finito in se si dice *permutazione*

Osservazione 4. Si denoterà con $\mathcal{S}_n$ l'insieme delle permutazioni dell'insieme $J_n = \{1, 2, \ldots, n\}$. S_n si chiama insieme delle perumutazioni su n oggetti perché un qualunque insieme di cardinalità n è bigettivo a J_n e quindi studiare le permutazioni su J_n equivale a studiare le permutazioni su un qualunque insieme di cardinalità n.

Osservazione 5. Siano X, Y due insiemi finiti. Allora può esistere un'applicazione ingettiva avente X come insieme di partenza e Y come insieme di arrivo solo se $|X| \leq |Y|$; invece può esistere un'applicazione surgettiva solo se $|X| \geq |Y|$. Infine, se $|X| = |Y|$ allora un'applicazione $f : X \to Y$ è ingettiva se e soltanto se è surgettiva e quindi se e soltanto se è bigettiva.

Cenni di combinatorica

Definizione 5. Siano $n, k \in \mathbb{N}^*$. Si dice *disposizione con ripetizioni di k elementi di classe n* una n-pla ordinata con ripetizioni di k oggetti.
Si dice *combinazione con ripetizioni di k elementi di classe n* una n-pla non ordinata con ripetizioni di k oggetti.

Definizione 6. Siano $n, k \in \mathbb{N}^*$, $n \leq k$. Si dice *disposizione semplice di k elementi di classe n* una n-pla ordinata senza ripetizioni di k oggetti.
Si dice *combinazione semplice di k elementi di classe n* una n-pla non ordinata senza ripetizioni di k oggetti.

Proposizione 1. *Il numero delle disposizioni con ripetizioni di k elementi di classe n è k^n. (Dimostrato a lezione).*

Proposizione 2. *Il numero delle disposizioni semplici di k elementi di classe n è*

$$(k)_n = k \cdot (k-1) \cdot (k-2) \cdot \ldots \cdot (k-n+1).$$

(Dimostrato a lezione)
In particolare il numero delle disposizioni semplici di n elementi di classe n è

$$(n)_n = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-n+1) = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1 = n!$$

dove il numero $n!$ si indica con il nome di n fattoriale.

Osservazione 6. Si possono riguardare le disposizioni semplici o con ripetizioni come applicazioni tra insiemi finiti, queste ultime pensate con il modello delle parole. Allora è facile rendersi conto del fatto che il numero delle permutazioni di un insieme di cardinalità n è $n!$, ovvero:

$$|\mathcal{S}_n| = n!$$

Osservazione 7. Si definisce anche

$$0! = 1.$$

Corollario 1. *Sia A un insieme finito con $|A| = n$. Allora*

$$|\mathcal{P}(A)| = 2^n.$$

(Dimostrato a lezione)

Definizione 7. Siano r, s interi positivi, con $r \leq s$, $s \neq 0$. Si dice *coefficiente binomiale* il numero

$$\binom{s}{r} = \frac{(s)_r}{r!} = \frac{s \cdot (s-1) \cdot \ldots \cdot (s-r+1)}{r!} = \frac{s!}{r!(s-r)!}$$

Osservazione 8. Si ha: $\binom{s}{0} = 1$, $\binom{s}{1} = s$, $\binom{s}{s} = 1$, $\binom{s}{s-1} = s$, $\binom{s}{r} = \binom{s-1}{r} + \binom{s-1}{r-1}$.

Teorema 2. *Vale la formula del binomio di Newton:*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Proposizione 3. *Il numero dei sottoinsiemi di n elementi di un insieme di k elementi, ovvero il numero delle combinazioni semplici di k elementi di classe n è proprio $\binom{k}{n}$. (dimostrato a lezione)*

Osservazione 9. La Proposizione 3 e la formula del binomio di Newton forniscono una diversa dimostrazione del Corollario 1.

Proposizione 4. *Il numero delle combinazioni con ripetizione di k elementi di classe n è dato da $\binom{k+n-1}{n}$. (dimostrato a lezione)*

Proposizione 5. *Il numero delle applicazioni surgettive di un insieme di cardinalità n in un insieme di cardinalità m, $n \geq m$ è:*

$$\sum_{k=1}^{m} \binom{m}{k} (-1)^{m-k} k^n.$$

Esempio 2. Per $n = 3$, $m = 2$

$$\sum_{k=1}^{2} \binom{2}{k} (-1)^{2-k} k^3 = \binom{2}{1}(-1)^1 + \binom{2}{2}(-1)^0 8 = -2 + 8 = 6.$$

Esempio 3. Per $n = 4$, $m = 3$

$$\begin{aligned}\sum_{k=1}^{3} \binom{3}{k} (-1)^{3-k} k^4 &= \binom{3}{1}(-1)^2 + \binom{3}{2}(-1)^1 2^4 + \binom{3}{3}(-1)^0 3^4 \\ &= 3 - 3 \cdot 16 + 81 = 3 - 48 + 81 = 36.\end{aligned}$$

Definizione 1. Si dice che due insiemi X e Y sono *equipotenti* Y se esiste una bigezione tra X e Y.

Definizione 2. Si dice che un insieme X è *infinito* se esiste un'applicazione ingettiva ma non surgettiva di X in X.

Esempio 1. Sicuramente l'insieme $\mathbb{N}$ dei numeri naturali è infinito in quanto per esempio l'applicazione $f : \mathbb{N} \to \mathbb{N}$ tale che per ogni $n \in \mathbb{N}$ $f(n) = 2n$, è ingettiva ma non surgettiva.

Osservazione 1. Se X è un insieme infinito ed è contenuto in un insieme Y, allora anche Y è infinito. Quindi gli insiemi numerici $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sono infiniti in quanto contengono $\mathbb{N}$.

Definizione 3. Si dice che un insieme X è *finito* se è vuoto o se non è infinito.

Teorema 1. *Sia X un insieme finito non vuoto. Allora esiste $n \in \mathbb{N}$ ed ed esiste un'applicazione bigettiva $\gamma : J_n \to X$, dove $J_n = \{1, 2, \ldots, n\}$.*

Osservazione 2. Nella situazione del Teorema 1, si può scrivere

$$X = \{\gamma(1), \gamma(2), \ldots, \gamma(n)\}.$$

Inoltre si dice che X ha *cardinalità* n e si scrive:

$$|X| = n.$$

Osservazione 3. Due insiemi finiti X e Y sono equipotenti se e solo se hanno la stessa cardinalità (verificata a lezione).

Definizione 4. Un'applicazione bigettiva di un insieme finito in se si dice *permutazione*

Osservazione 4. Si denoterà con $\mathcal{S}_n$ l'insieme delle permutazioni dell'insieme $J_n = \{1, 2, \ldots, n\}$. S_n si chiama insieme delle perumutazioni su n oggetti perché un qualunque insieme di cardinalità n è bigettivo a J_n e quindi studiare le permutazioni su J_n equivale a studiare le permutazioni su un qualunque insieme di cardinalità n.

Osservazione 5. Siano X, Y due insiemi finiti. Allora può esistere un'applicazione ingettiva avente X come insieme di partenza e Y come insieme di arrivo solo se $|X| \leq |Y|$; invece può esistere un'applicazione surgettiva solo se $|X| \geq |Y|$. Infine, se $|X| = |Y|$ allora un'applicazione $f : X \to Y$ è ingettiva se e soltanto se è surgettiva e quindi se e soltanto se è bigettiva.

Cenni di combinatorica

Definizione 5. Siano $n, k \in \mathbb{N}^*$. Si dice *disposizione con ripetizioni di k elementi di classe n* una n-pla ordinata con ripetizioni di k oggetti.
Si dice *combinazione con ripetizioni di k elementi di classe n* una n-pla non ordinata con ripetizioni di k oggetti.

Definizione 6. Siano $n, k \in \mathbb{N}^*$, $n \leq k$. Si dice *disposizione semplice di k elementi di classe n* una n-pla ordinata senza ripetizioni di k oggetti.
Si dice *combinazione semplice di k elementi di classe n* una n-pla non ordinata senza ripetizioni di k oggetti.

Proposizione 1. *Il numero delle disposizioni con ripetizioni di k elementi di classe n è k^n. (Dimostrato a lezione).*

Proposizione 2. *Il numero delle disposizioni semplici di k elementi di classe n è*

$$(k)_n = k \cdot (k-1) \cdot (k-2) \cdot \ldots \cdot (k-n+1).$$

(Dimostrato a lezione)
In particolare il numero delle disposizioni semplici di n elementi di classe n è

$$(n)_n = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-n+1) = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1 = n!$$

dove il numero $n!$ si indica con il nome di n fattoriale.

Osservazione 6. Si possono riguardare le disposizioni semplici o con ripetizioni come applicazioni tra insiemi finiti, queste ultime pensate con il modello delle parole. Allora è facile rendersi conto del fatto che il numero delle permutazioni di un insieme di cardinalità n è $n!$, ovvero:

$$|\mathcal{S}_n| = n!$$

Osservazione 7. Si definisce anche

$$0! = 1.$$

Corollario 1. *Sia A un insieme finito con $|A| = n$. Allora*

$$|\mathcal{P}(A)| = 2^n.$$

(Dimostrato a lezione)

Definizione 7. Siano r, s interi positivi, con $r \leq s$, $s \neq 0$. Si dice *coefficiente binomiale* il numero

$$\binom{s}{r} = \frac{(s)_r}{r!} = \frac{s \cdot (s-1) \cdot \ldots \cdot (s-r+1)}{r!} = \frac{s!}{r!(s-r)!}$$

Osservazione 8. Si ha: $\binom{s}{0} = 1$, $\binom{s}{1} = s$, $\binom{s}{s} = 1$, $\binom{s}{s-1} = s$, $\binom{s}{r} = \binom{s-1}{r} + \binom{s-1}{r-1}$.

Teorema 2. *Vale la formula del binomio di Newton:*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Proposizione 3. *Il numero dei sottoinsiemi di n elementi di un insieme di k elementi, ovvero il numero delle combinazioni semplici di k elementi di classe n è proprio $\binom{k}{n}$. (dimostrato a lezione)*

Osservazione 9. La Proposizione 3 e la formula del binomio di Newton forniscono una diversa dimostrazione del Corollario 1.

Proposizione 4. *Il numero delle combinazioni con ripetizione di k elementi di classe n è dato da $\binom{k+n-1}{n}$. (dimostrato a lezione)*

Proposizione 5. *Il numero delle applicazioni surgettive di un insieme di cardinalità n in un insieme di cardinalità m, $n \geq m$ è:*

$$\sum_{k=1}^{m} \binom{m}{k} (-1)^{m-k} k^n.$$

Esempio 2. Per $n = 3$, $m = 2$

$$\sum_{k=1}^{2} \binom{2}{k} (-1)^{2-k} k^3 = \binom{2}{1}(-1)^1 + \binom{2}{2}(-1)^0 8 = -2 + 8 = 6.$$

Esempio 3. Per $n = 4$, $m = 3$

$$\begin{aligned}\sum_{k=1}^{3} \binom{3}{k} (-1)^{3-k} k^4 &= \binom{3}{1}(-1)^2 + \binom{3}{2}(-1)^1 2^4 + \binom{3}{3}(-1)^0 3^4 \\ &= 3 - 3 \cdot 16 + 81 = 3 - 48 + 81 = 36.\end{aligned}$$

NUMERI PRIMI E TEORMA FONDAMENTALE DELL'ARITMETICA

Teorema 1. *(Teorema fondamentale dell'Aritmetica) Sia $n \in \mathbb{Z}^*$, $n \neq \pm 1$. Allora esistono s numeri primi $p_1, \ldots, p_s$ e s interi naturali $h_1, \ldots, h_s$ tali che*

$$n = p_1^{h_1} \cdot \ \ldots \ \cdot p_s^{h_s}.$$

Questa decomposizione è essenzialmente unica, nel senso che se $q_1, \ldots, q_r$ sono numeri primi e $k_1, \ldots, k_r$ sono interi positivi tali che

$$n = q_1^{k_1} \ldots q_r^{k_r}$$

allora $s = r$ ed inoltre si può cambiare l'ordine dei fattori in modo che $q_1 = \pm p_1, \ldots, q_s = \pm p_s$, $h_1 = k_1, \ldots, h_s = k_s$.

Osservazione 1. Siano $n, m \in \mathbb{Z} - \{0, \pm 1\}$. Allora esistono $p_1, \ldots, p_s$ numeri primi, $h_1, \ldots, h_s, k_1, \ldots, k_s \in \mathbb{N}$ tali che

$$n = p_1^{h_1} \cdots p_s^{h_s}, \quad m = p_1^{k_1} \cdots p_s^{k_s};$$

cioè i due numeri possono essere fattorizzati usando gli stessi fattori primi, eventualmente elevati a potenza 0. Per esempio,

$$945 = 2^0 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^0 \cdot 17^0, \quad 3366 = 2 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11 \cdot 17.$$

Si può provare che

$$M.C.D.(n, m) = p_1^{min(h_1,k_1)} \cdots p_s^{min(h_s,k_s)},$$

$$m.c.m.(n, m) = p_1^{max(h_1,k_1)} \cdots p_s^{max(h_s,k_s)}.$$

Nel caso considerato:

$$M.C.D.(945, 3366) = 2^{min(0,1)} \cdot 3^{min(3,2)} \cdot 5^{min(1,0)} \cdot 7^{min(1,0)} \cdot 11^{min(0,1)} \cdot 17^{min(0,1)},$$

quindi $M.C.D.(945, 3366) = 3^2 = 18$. Inoltre

$$m.c.m.(945, 3366) = 2^{max(0,1)} \cdot 3^{max(3,2)} \cdot 5^{max(1,0)} \cdot 7^{max(1,0)} \cdot 11^{max(0,1)} \cdot 17^{max(0,1)},$$

per cui $m.c.m.(945, 3366) = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 = 353430$.

Metodi di fattorizzazione

CRIVELLO DI ERATOSTENE

Per determinare i numeri primi minori o uguali di un assegnato numero naturale $n \geq 4$, si scrive una tabella con tutti i numeri fino ad n e si comincia con il cancellare i multipli di 2. Finita questa operazione, si eliminano tutti i multipli del primo numero non cancellato, ovvero 3; dopo i multipli di 5, che è il primo numero non cancellato, dopo 7, e così via e ci si può fermare al più grande numero primo q più piccolo di $\sqrt{n}$. Infatti se p è un numero primo più grande di $\sqrt{n}$ un suo multiplo tramite un numero primo più piccolo di $\sqrt{n}$ eventualmente presente nella tabella è stato già scartato e già $p^2 > n$.

Osservazione 2. Tra i fattori primi di un numero naturale n non primo (ci si può sempre riferire a un numero positivo senza ledere la generalità) $n \geq 4$ ce n'è almeno uno minore o uguale di $\sqrt{n}$. Sia infatti

$$n = p_1^{h_1} \cdot \ldots \cdot p_s^{h_s}$$

la scomposizione di n in fattori primi. Se fosse

$$p_1 > \sqrt{n}, \ldots, p_s > \sqrt{n},$$

allora sarebbe

$$n = p_1^{h_1} \cdot \ldots \cdot p_s^{h_s} > n$$

il che è una contraddizione.

Esempio 1. Se si vuole fattorizzare il numero $n = 4187$, si considera la sua radice $\sqrt{n} \backsim 64,707$ e quindi si prendono in esame tutti i numeri primi minori di 64: essi sono:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61.$$

Effettuando (se necessario) le divisioni con la calcolatrice si ottiene un eventuale primo fattore. Se non si trova nessun fattore, il numero è irriducibile.
In queso caso si vede che n è divisibile per 53 e precisamente $n = 53 \cdot 79$.

METODO DI FATTORIZZAZIONE DI FERMAT

Osservazione 3. Si supponga di voler fattorizzare $n \in \mathbb{N}^*$, $n \neq \pm 1$. Si può ammettere che n sia dispari: se n fosse pari, si potrebbe dividere per 2 anche più volte, fino ad ottenenere un numero dispari. Si prova che:

$$(\exists a, b \in \mathbb{N} \text{ tali che } n = ab) \Longleftrightarrow (\exists x, y \in \mathbb{N} \text{ tali che } n = x^2 - y^2).$$

Infatti se $n = ab$, allora, sviluppando i calcoli, si vede facilmente che

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2,$$

dove $\frac{a \pm b}{2} \in \mathbb{N}$, poichè n è dispari e quindi a e b sono dispari, e la loro somma, come la loro differenza,è pari. Il viceversa è ovvio, perchè $x^2 - y^2 = (x + y) \cdot (x - y)$, per cui basta porre $a = x + y,\ b = x - y$ e si ha $n = ab$. Anche quando n è primo si ha la fattorizzazione banale:

$$n = \left(\frac{n+1}{2} + \frac{n-1}{2}\right) \cdot \left(\frac{n+1}{2} - \frac{n-1}{2}\right) = n \cdot 1.$$

In virtù della Osservazione 3, cercare una fattorizzazione di n equivale a cercare x tale che $x^2 - n$ sia un quadrato (cioè y^2). Allora si usa il seguente procedimento: si determina il più piccolo intero positivo $t \geq \sqrt{n}$ e si calcolano

$$t^2 - n;\quad (t+1)^2 - n;\quad (t+2)^2 - n; \ldots\ldots$$

e così via, finché si trova un quadrato.

Esempio 2. $n = 1183$, $\sqrt{n} \backsim 34, 39$, $t = 35$ allora si ha:

$$\begin{aligned}
t^2 - n &= 35^2 - 1183 = 1225 - 1183 = 42 \text{ non quadrato} \\
(t+1)^2 - n &= 36^2 - 1183 = 1296 - 1183 = 113 \quad " \quad " \\
(t+2)^2 - n &= 37^2 - 1183 = 1369 - 1183 = 186 \quad " \quad " \\
(t+3)^2 - n &= 38^2 - 1183 = 1444 - 1183 = 261 \quad " \quad " \\
(t+4)^2 - n &= 39^2 - 1183 = 1521 - 1183 = 338 \quad " \quad " \\
(t+5)^2 - n &= 40^2 - 1183 = 1600 - 1183 = 417 \quad " \quad " \\
(t+6)^2 - n &= 41^2 - 1183 = 1681 - 1183 = 498 \quad " \quad " \\
(t+7)^2 - n &= 42^2 - 1183 = 1764 - 1183 = 581 \quad " \quad " \\
(t+8)^2 - n &= 43^2 - 1183 = 1849 - 1183 = 646 \quad " \quad " \\
(t+9)^2 - n &= 44^2 - 1183 = 1936 - 1183 = 753 \quad " \quad " \\
(t+10)^2 - n &= 45^2 - 1183 = 2052 - 1183 = 842 \quad " \quad " \\
(t+11)^2 - n &= 46^2 - 1183 = 2116 - 1183 = 933 \quad " \quad " \\
(t+12)^2 - n &= 47^2 - 1183 = 2209 - 1183 = 1026 \quad " \quad " \\
(t+13)^2 - n &= 48^2 - 1183 = 2304 - 1183 = 1121 \quad " \quad " \\
(t+14)^2 - n &= 49^2 - 1183 = 2401 - 1183 = 1218 \quad " \quad " \\
(t+15)^2 - n &= 50^2 - 1183 = 2500 - 1183 = 1317 \quad " \quad " \\
(t+16)^2 - n &= 51^2 - 1183 = 1601 - 1183 = 1481 \quad " \quad " \\
(t+17)^2 - n &= 52^2 - 1183 = 2704 - 1183 = 1521 = 39^2.
\end{aligned}$$

Quindi: $52^2 - 1183 = 39^2$, cioè

$$1183 = 52^2 - 39^2 = (52 + 39)(52 - 39) = 91 \cdot 13$$

Bisogna scomporre 91, per esempio iterando il procedimento di Fermat: $m = 91$, $\sqrt{91} \backsim 9, 53$, $k = 10$,

$$k^2 - 91 = 100 - 91 = 9 = 3^2.$$

Segue che

$$91 = 10^2 - 3^2 = (10 + 3)(10 - 3) = 13 \cdot 7.$$

Allora

$$1183 = 13^2 \cdot 7.$$

Il procedimento di Fermat è un algoritmo, ovvero ha sempre una conclusione (anche se non si sa a priori qual è il numero dei passaggi da effettuare); nel caso in cui il numero n è primo, si conclude con il quadrato $\left(\frac{n+1}{2}\right)^2 - n$.

Piccolo Teorema di Fermat - Teorema di eulero

Lemma 1. *Siano $a, b, c, d \in \mathbb{Z}$, $k, n \in \mathbb{N}$, $n \neq 0, n \neq 1$. Si ha:*

(1) $(a \equiv b \ (\mathtt{mod}\ n) \wedge c \equiv d \ (\mathtt{mod}\ n)) \Rightarrow a + c \ \equiv b + d \ (\mathtt{mod}\ n)$
(2) $(a \equiv b \ (\mathtt{mod}\ n) \wedge c \equiv d \ (\mathtt{mod}\ n)) \Rightarrow ac \ \equiv b \ (\mathtt{mod}\ n)$
(3) $a \equiv b \ (\mathtt{mod}\ n) \Rightarrow a^k \equiv b^k \ (\mathtt{mod}\ n)$

Dimostrazione. Da $(a \equiv b \ (\mathtt{mod}\ n) \wedge c \equiv d \ (\mathtt{mod}\ n))$ segue $(n \mid (a - b) \wedge n \mid (c - d).)$ Allora $n \mid a-b+c-d$, ovvero $a \mid (a+c)-(b+d)$ e ciò vuol dire che $a+c \ \equiv b+d \ (\mathtt{mod}\ n)$, per cui (1) è provata.
Poichè $(a \equiv b \ (\mathtt{mod}\ n) \wedge c \equiv d \ (\mathtt{mod}\ n))$, esistono $h, k \in \mathbb{Z}$ tali che $a-b = nh$ e $c-d = nk$. Allora $(a - b)c = nhc$ e $(c - d)b = nkb$. Sommando $ac - bc + cb - db = nhc + nkb$, da cui $ac - bd = n(hc + kb)$ e pertanto $n \mid ac - bd$, ovvero $ac \ \equiv b \ (\mathtt{mod}\ n)$, e (2) risulta verificata.

Per provare (3) si procede per induzione completa. Per $k = 0$, certamente $a^0 \equiv b^0 \ (\texttt{mod}\ n)$ è verificato poichè $a^0 = b^0 = 1$ e la congruenza modulo n è riflessiva. Si suppone ora che $a \equiv b \ (\texttt{mod}\ n)$ e $a^k \equiv b^k \ (\texttt{mod}\ n)$ e si deve provare che $a^{k+1} \equiv b^{k+1} \ (\texttt{mod}\ n)$: ma basta ricordare che per ogni numero intero non nullo x, risulta $x^{k+1} = x^k \cdot x$ e usare (2).

Osservazione 4. Siano $a, b \in \mathbb{Z}$. Si osservi che, se $a \equiv b \ (\texttt{mod}\ n)$, allora, tenendo presente che $b \equiv b \ (\texttt{mod}\ n)$ e usando (2) del Lemma 1, si ha $a - b \equiv 0 \ (\texttt{mod}\ n)$.

Proposizione 1. *Siano $x, y \in \mathbb{Z}$, $p \in \mathbb{N}$, p primo. Allora*

$$(x + y)^p \equiv x^p + y^p (\texttt{mod}\ p).$$

La dimostrazione viene omessa.

Teorema 2. *(Piccolo teorema di Fermat) Siano $a \in \mathbb{Z}$, $p \in \mathbb{N}$ un numero primo. Allora*

$$a^p \ \equiv \ a \ (\texttt{mod}\ p). \tag{1}$$

Dimostrazione. Si suppone in un primo momento che sia $a \geq 0$ e si procede per induzione completa su a. Per $a = 0$, $a^p = 0$ e (1) diviene $0 \ \equiv \ 0 \ (\texttt{mod}\ p)$, ovviamente vera. Si suppone che (1) sia vera e si prova $(a+1)^p \ \equiv \ a+1 \ (\texttt{mod}\ p)$. Per la Proposizione 1, la proprietà transitiva della congruenza modulo n e l'ipotesi di induzione risulta:

$$(a + 1)^p \ \equiv \ a^p + 1^p \ \equiv \ a + 1 \ (\texttt{mod}\ p).$$

quindi (1) è verificata quando $a \geq 0$. Se $a < 0$, allora $-a > 0$ e quindi $(-a)^p \ \equiv \ (-a) \ (\texttt{mod}\ p)$. Usando nuovamente la Proposizione 1, la proprietà transitiva della congruenza modulo n e l'ipotesi di induzione, si ha:

$$0 = (a + (-a))^p \ \equiv \ a^p + (-a)^p \ \equiv \ a^p + (-a) \ (\texttt{mod}\ p).$$

Pertanto $a^p + (-a) \ \equiv \ 0 \ (\texttt{mod}\ p)$ da cui, per l'Osservazione 4, $a^p \ \equiv \ a \ (\texttt{mod}\ p)$.

Corollario 1. Siano $a \in \mathbb{Z}$, $p \in \mathbb{N}$ un numero primo. Se $M.C.D.(a, p) = 1$ allora

$$a^{p-1} \equiv 1 (\texttt{mod}\ p).$$

Esercizi 1. Determinare il resto della divisione di 89741^{527} per 3.

Si osserva che

$$89741 \equiv 2 (\texttt{mod}\ 3)$$

e quindi

$$89741^{527} \equiv 2^{527} (\texttt{mod}\ 3).$$

Per il corollario, poichè $M.C.D.(2, 3) = 1$, si ha $2^{3-1} \equiv 1 (\texttt{mod}\ 3)$ (in questo caso è banale) e pertanto

$$89741^{527} \equiv 2^{527} = (2^2)^{263} \cdot 2 \equiv 1^{263} \cdot 2 = 2 (\texttt{mod}\ 3)$$

per cui il resto è 2.

2. Determinare il resto della divisione di 57432^{1142} per 9.

Si osserva che

$$57432 \equiv 3 (\texttt{mod}\ 9)$$

e quindi

$$57432^{1142} \equiv 3^{1142} \equiv (3^2)^{571} \equiv 0^{571} \equiv 0 (\texttt{mod}\ 9).$$

Definizione 1. Si dice *funzione di Eulero* l'applicazione

$$\varphi : \mathbb{N}^* \to \mathbb{N}$$

tale che $\forall n \in \mathbb{N}^*$,

$$\varphi(n) = \text{numero dei numeri minori di } n \text{ e primi con } n.$$

Osservazione 5. È ovvio che per ogni numero primo p

$$\varphi(p) = p - 1$$

Proposizione 2. La funzione di Eulero è moltiplicativa, cioè

$$\forall n, m \in \mathbb{N}^*,\ n > 1,\ m > 1 \text{ tali che } M.C.D.(n, m) = 1,$$
$$\varphi(n \cdot m) = \varphi(n)\varphi(m).$$

Proposizione 3. Sia p un numero primo. Allora

$$\varphi(p^h) = p^h - p^{h-1}.$$

Proposizione 4. Sia $n \in \mathbb{N}^*$, e sia $n = p_1^{h_1} \cdot \ldots \cdot p_s^{h_s}$ la sua fattorizzazione in numeri primi. Allora

$$\varphi(n) = \varphi(p_1^{h_1}) \cdot \ldots \cdot \varphi(p_s^{h_s}).$$

Teorema 3. *(Teorema di Eulero) Siano $a \in \mathbb{Z}^*$, $n \in \mathbb{N}^*$, con $M.C.D.(a, n) = 1$. Allora*

$$a^{\varphi(n)} \equiv 1(\texttt{mod}\ n).$$

Assegnato un insieme X, con $|X| \geq 2$, verrà denotato con $\mathscr{P}_2(X)$ l'insieme dei sottoinsiemi di X di cardinalità 2.

Definizione 1. Si dice *grafo* una terna ordinata $\mathcal{G} = (V, L, \varphi)$, dove V è un insieme tale che $|V| \geq 2$, i cui elementi sono detti *vertici* o *nodi*, L è un insieme non vuoto, i cui elementi sono detti *lati* o *archi*, e

$$\varphi : L \to \mathscr{P}_2(V).$$

Se $l_1, \ldots, l_h \in L$ sono lati di $\mathcal{G}$ tali che $\varphi(l_1) = \cdots = \varphi(l_h) = \{v, w\} \in \mathscr{P}_2(V)$, si dice che tra i vertici v e w c'è un *lato multiplo*. Se φ è ingettiva, il grafo $\mathcal{G}$ si dice *semplice*.

Nomenclatura Sia $\mathcal{G} = (V, L, \varphi)$ un grafo. Se $l \in L$ e $\varphi(l) = \{v, w\}$, si dice che v e w sono *estremi* di l e i due vertici v e w si dicono *adiacenti*. Un vertice che non sia estremo di alcun lato si dice *isolato*. Se due lati hanno un estremo in comune, allora si dice che sono *incidenti*. Infine, $|V|$ si dice *ordine* di $\mathcal{G}$.

Osservazione 1. Viene esclusa da questa trattazione la possibilità di considerare il caso limite di grafi con vertici tutti isolati, perché l'insieme dei lati è non vuoto. Inoltre viene escluso il caso che un vertice sia adiacente a se stesso, visto che l'applicazione φ è a valori in $\mathscr{P}_2(V)$.

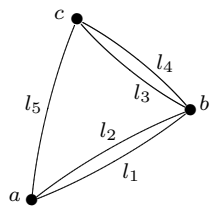
Nota Bene Nel seguito si considereranno esclusivamente grafi finiti, vale a dire con numero dei vertici e numero dei lati entrambi finiti. In tal caso i grafi possono essere rappresentati mediante un diagramma. Si osservi che ci sono diverse rappresentazioni di uno stesso grafo.

Definizione 2. Siano $\mathcal{G} = (V, L, \varphi)$ un grafo, $v \in V$. Si dice *grado* o *valenza* di v il numero $\mathtt{d}(v)$ dei lati dei quali v è estremo. Un vertice si dice *pari* se il suo grado è pari, si dice *dispari* se il suo grado è dispari.

Esempio 1. Si consideri il grafo $\mathcal{G} = (V, L, \varphi)$, dove $V = \{a, b, c\}$, $L = \{l_1, l_2, l_3, l_4, l_5\}$ e $\varphi : L \to \mathscr{P}_2(V)$ è così definita:

$$\varphi(l_1) = \varphi(l_2) = \{a, b\};\ \varphi(l_3) = \varphi(l_4) = \{b, c\};\ \varphi(l_5) = \{a, c\}.$$

Una rappresentazione di $\mathcal{G}$ è la seguente:



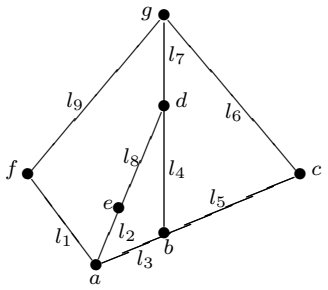
I gradi dei vertici di $\mathcal{G}$ sono: $\mathtt{d}(a) = 3,\ \mathtt{d}(b) = 4,\ \mathtt{d}(c) = 3$.

Esempio 2. Si consideri il grafo semplice $\mathcal{G} = (V, L, \varphi)$, dove $V = \{a, b, c, d, e, f, g\}$, $L = \{l_1, l_2, l_3, l_4, l_5, l_6, l_7, l_8, l_9\}$ e $\varphi : L \to \mathscr{P}_2(V)$ è tale che

$$\varphi(l_1) = \{a, f\},\ \varphi(l_2) = \{a, e\},\ \varphi(l_3) = \{a, b\},\ \varphi(l_4) = \{b, d\},\ \varphi(l_5) = \{b, c\},$$

$$\varphi(l_6) = \{c, g\},\ \varphi(l_7) = \{d, g\},\ \varphi(l_8) = \{d, e\},\ \varphi(l_9) = \{f, g\}.$$

Il grafo $\mathcal{G}$ si può rappresentare graficamente nel modo seguente:



I gradi dei vertici di $\mathcal{G}$ sono:

$$\mathtt{d}(a) = 3,\ \mathtt{d}(b) = 3,\ \mathtt{d}(c) = 2,\ \mathtt{d}(d) = 3,\ \mathtt{d}(e) = 2,\ \mathtt{d}(f) = 2,\ \mathtt{d}(g) = 3.$$

Osservazione 2. Si osservi che un grafo semplice $\mathcal{G} = (V, L, \varphi)$ può essere individuato soltanto dall'insieme V dei suoi vertici e dall'insieme L dei suoi lati. Infatti, se φ è ingettiva, si può identificare L con la sua immagine $\varphi(L)$ in $\mathscr{P}_2(V)$. Quindi, nel seguito, un grafo semplice verrà indicato con $\mathcal{G} = (V, L)$.

Definizione 3. Sia $\mathcal{G} = (V, L, \varphi)$ un grafo, con $V = \{v_1, \ldots, v_n\}$. Si dice *matrice di adiacenza di* $\mathcal{G}$ la matrice $A = (a^i_j)$, $i, j = 1, \ldots, n$, quadrata di ordine n, con $a^i_j =$ numero dei lati aventi v_i e v_j come estremi.

Osservazione 3. Si osservi la matrice di adiacenza è una matrice simmetrica. Inoltre, se $\mathcal{G}$ è un grafo semplice, gli elementi della matrice di adiacenza sono 0 o 1. Infine, per ogni $i = 1, \ldots, n$, la somma degli elementi della $i-$ma riga (o colonna) della matrice di adiacenza corrisponde al grado del vertice v_i.

Definizione 4. Sia $\mathcal{G} = (V, L, \varphi)$ un grafo, con $V = \{v_1, \ldots, v_n\}$, $L = \{l_1, \ldots, l_h\}$. Si dice *matrice di incidenza di* $\mathcal{G}$ la matrice $A = (a^j_i)$, $j = 1, \ldots, h,\ i = 1, \ldots, n$, di tipo h, n con $a^j_i = 1$ se v_i è estremo di l_j, $a^j_i = 0$ altrimenti.

Osservazione 4. Si osservi che, per ogni $i = 1, \ldots, n$, la somma degli elementi della $i-$ma colonna della matrice di incidenza corrisponde al grado del vertice v_i.

Esempio 3. La matrice di adiacenza del grafo dell'Esempio 1 è:

$$\begin{pmatrix} 0 & 2 & 1 \\ 2 & 0 & 2 \\ 1 & 2 & 0 \end{pmatrix}$$

dove si è considerato $v_1 = a, v_2 = b, v_3 = c$. Invece la matrice di incidenza è:

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

Esempio 4. Le matrici di adiacenza e di incidenza del grafo dell'Esempio 2 sono rispettivamente:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Proposizione 1. *(Lemma delle strette di mano) Sia $\mathcal{G} = (V, L, \varphi)$ un grafo. Risulta:*

$$\sum_{v \in V} \mathtt{d}(v) = 2|L|. \tag{1}$$

Dimostrazione. La somma

$$\sum_{v \in V} \mathtt{d}(v)$$

si dice *grado complessivo di* $\mathcal{G}$ e rappresenta il numero di tutti i possibili "estremi di lato". Poichè ogni lato ha due estremi, si ottiene (1).

Proposizione 2. *Il numero dei vertici dispari (cioè di grado dispari) di un grafo è pari.*

Dimostrazione. Sia $\mathcal{G} = (V, L, \varphi)$ un grafo. Poichè V è finito, senza ledere la generalità si può porre: $V = \{v_1, \ldots, v_n\}$. Siano V_d e V_p rispettivamente i sottoinsiemi di V formati dai vertici pari e dai vertici dispari. Si ha, ovviamente, $V_d \cup V_p = V$, $V_d \cap V_p = \emptyset$, per cui si può porre $V_d = \{v_1, \ldots, v_s\}$, $V_p = \{v_{s+1}, \ldots, v_n\}$. Risulta:

$$2|L| = \sum_{v \in V} \mathtt{d}(v) = \sum_{i=1}^{n} \mathtt{d}(v_i) = \sum_{i=1}^{s} \mathtt{d}(v_i) + \sum_{i=s+1}^{n} \mathtt{d}(v_i)$$

da cui si ha

$$\sum_{i=1}^{s} \mathtt{d}(v_i) + \sum_{i=s+1}^{n} \mathtt{d}(v_i) = 2|L|$$

e quindi

$$\sum_{i=1}^{s} \mathtt{d}(v_i) = 2|L| - \sum_{i=s+1}^{n} \mathtt{d}(v_i). \tag{2}$$

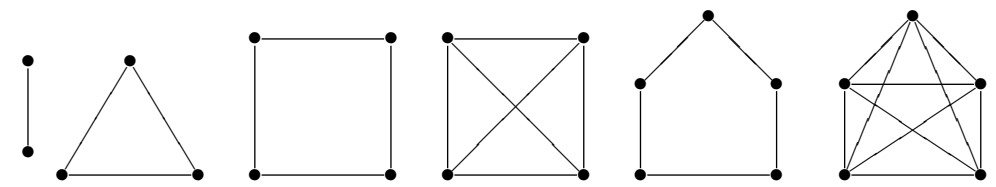
Si osservi che $\sum_{i=s+1}^{n} \mathtt{d}(v_i)$ è la somma dei gradi dei vertici pari, per cui è un numero pari. Segue che il termine a destra dell'uguale in (2) è pari e dunque è pari anche quello a sinistra, che rappresenta la somma dei gradi dei vertici dispari. Ma la somma di numeri dispari è pari solo quando il numero degli addendi è pari: ciò prova che il numero dei vertici dispari di $\mathcal{G}$ è pari.

Esercizio 1. Esiste un grafo semplice $\mathcal{G} = (V, L)$, con $V = \{v_1, v_2, \ldots, v_{15}\}$, in modo tale che per ogni $1 = 1, 2, \ldots, 15$, $\mathtt{d}(v_i) = i$?

Definizione 5. Si dice *regolare* di grado d un grafo semplice $\mathcal{G} = (V, L)$ tale che ogni suo vertice abbia grado d. Se $\mathcal{G}$ ha ordine n ed è regolare di grado $n-1$ si dice *completo*.

Osservazione 5. Se $\mathcal{G} = (V, L)$ è un grafo di ordine n, regolare di grado d, allora $|L| = \frac{1}{2}nd$. In particolare se $\mathcal{G}$ è completo allora $|L| = \frac{1}{2}n(n-1)$. Il grafo regolare completo di ordine n si denota con K_n.

I seguenti diagrammi mostrano grafi regolari. In particolare i grafi n.1,2,4,6 sono i grafi completi K_2, K_3, K_4, K_5 rispettivamente.



n.1 n.2 n.3 n.4 n.5 n.6

Osservazione 6. Si osservi che sono completi tutti e soli i grafi aventi i vertici adiacenti a due a due.

Esercizio 2. Esiste un grafo di ordine 9, regolare di grado 5?

Definizione 6. Siano $\mathcal{G} = (V, L, \varphi)$ un grafo, $v_0, \ldots, v_h \in V$. Si dice *cammino* da v_0 a v_h una successione $l_1, \ldots, l_h$ di lati di $\mathcal{G}$ distinti, tali che per ogni $i \in \{1, \ldots, h-1\}$, l_i risulti incidente a l_{i+1} e $\varphi(l_1) = \{v_0, v_1\}$, $\varphi(l_h) = \{v_{h-1}, v_h\}$; il numero h dei lati, si dice lunghezza del cammino. Se $v_0 = v_h$ si parla di *circuito* di lunghezza h da v_0 a v_0.

Osservazione 7. Siano $\mathcal{G} = (V, L, \varphi)$ un grafo, $v \in V$. Esiste un unico cammino di lunghezza 0 (ovvero privo di lati) da v a v che si dice *cammino nullo da v a v*.

Siano $\mathcal{G} = (V, L, \varphi)$ un grafo, $v, w \in V$. In generale ci sono più cammini da v a w, e di diversa lunghezza. Ciò giustifica la seguente:

Definizione 7. Siano $\mathcal{G} = (V, L, \varphi)$ un grafo, $v, w \in V$. Si dice *geodetica da v a w* un cammino di lunghezza minima da v a w. La lunghezza di una geodetica da v a w viene detta *distanza tra v e w*.

Esempio 5. Nel grafo dell'Esempio 2, si possono considerare i seguenti cammini da e a g: $c_1 = l_2, l_3, l_4, l_7$ di lunghezza 4, $c_2 = l_2, l_1, l_9$ di lunghezza 3, $c_3 = l_2, l_3, l_5, l_6$ di lunghezza 4 e $c_4 = l_8, l_7$ che ha lunghezza 2 ed è una geodetica (in questo caso l'unica) da e a g. Quindi la distanza tra e e g è 2.

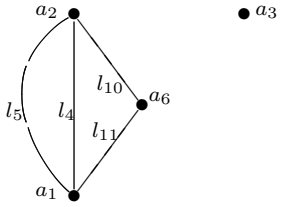
Definizione 8. Un grafo $\mathcal{G} = \{V, L, \varphi\}$ si dice *connesso* se comunque si considerino due vertici $v, w \in V$ esiste un cammino da v a w.

Osservazione 8. I grafi considerati fino a questo punto sono tutti connessi.

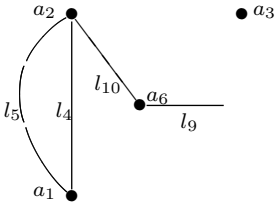
Definizione 9. Siano $\mathcal{G} = (V, L, \varphi)$ un grafo, $V' \subseteq V$, $L' \subseteq L$. Si dice che (V', L') è un sottografo di $\mathcal{G}$ se $\forall\ l \in L'$ si ha $\varphi(l) = \{v, w\}$ con $v, w \in V'$.

In altre parole, perché (V', L') sia un sottografo, gli estremi di ogni lato di L' devono essere in V'.

Esempio 6. Si consideri il grafo $\mathcal{G}$ dell'Esempio 10. La coppia (V', L'), dove $V' = \{a_1, a_2, a_3, a_6\}$, $L' = \{l_4, l_5, l_{10}, l_{11}\}$, è un sottografo di $\mathcal{G}$. Invece la coppia (V', L''), dove $L'' = \{l_4, l_5, l_{10}, l_9\}$ non forma un sottografo, in quanto l'estremo a_5 di l_9 non appartiene a V'.



(V', L')



(V', L'') *non sottografo*

Definizione 10. Siano $\mathcal{G} = \{V, L, \varphi\}$ un grafo, $v \in V$. Si dice *componente connessa di v* l'insieme

$$C_v = \{w \in V \ :\ \text{esiste un cammmino da } v \text{ a } w\}.$$

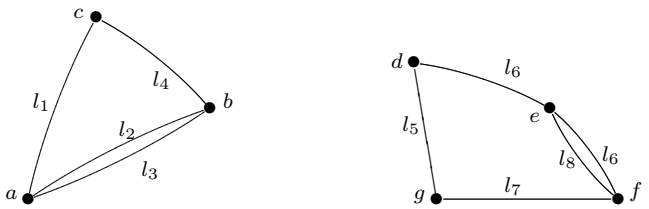
Osservazione 9. Se $\mathcal{G} = \{V, L, \varphi\}$ è un grafo connesso, allora $\forall v \in V$, $C_v = V$.

Osservazione 10. Siano $\mathcal{G} = \{V, L, \varphi\}$ un grafo, $v \in V$. Se si pone

$$L' = \{l \in L \ :\ \text{gli estremi di } l \text{ sono entrambi in } C_v\}$$

allora si vede che la coppia (C_v, L') è un sottografo di $\mathcal{G}$.

Esempio 7. Il grafo $\mathcal{G}$ rappresentato nella seguente figura non è connesso:

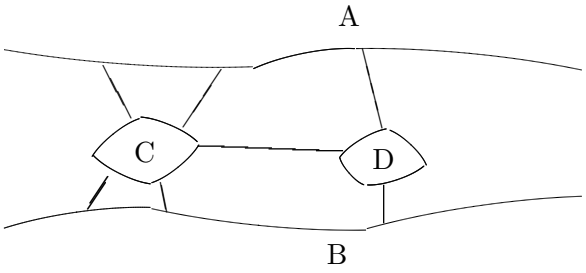


$\mathcal{G}$

Infatti non esiste un cammino tra i vertici c e g, per esempio. $\mathcal{G}$ presenta due componenti connesse $C_a = \{a, c, b\}$, $C_d = \{d, e, f, g\}$. I sottografi da esse individuati sono (C_a, L') e $(C_d, L")$, dove $L' = \{l_1, l_2, l_3, l_4\}$, $L" = \{l_5, l_6, l_7, l_8\}$.

Definizione 11. Sia $\mathcal{G}$ un grafo. Si dice *Euleriano* un cammino o un circuito che contenga tutti i lati di $\mathcal{G}$.

La teoria dei grafi fu originata da Eulero grazie ad un problema pratico: il famoso problema dei ponti di Könisberg, schematizzato in figura:



La città di Könisberg è attraversata da un fiume nel quale ci sono due isole, C e D della figura, collegate alle rive A e B e tra loro da sette ponti. Eulero si pose il seguente problema: è possibile partire da un punto e ritornare allo stesso punto percorrendo tutti i sette ponti una sola volta e passando per le due isole e per le due rive? La situazione geografica si può rappresentare con il seguente diagramma:

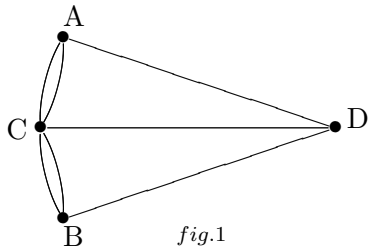


*fig.*1

e pertanto il problema di Eulero si traduce nel capire se esiste un circuito Euleriano del grafo rappresentato dal precedente diagramma. La risposta venne data da Eulero stesso.

Teorema 1. *(Eulero 1736) Un grafo privo di vertici isolati ammette un circuito Euleriano se e soltanto se è connesso e non ha vertici dispari.*

Quindi la risposta al problema dei ponti di Könisberg è negativa, poiché i vertici del grafo che lo schematizza sono tutti dispari. Usando il Teorema di Eulero si può provare il seguente risultato.

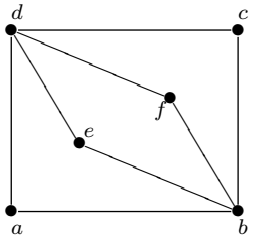
Teorema 2. *Un grafo privo di vertici isolati ammette un cammino Euleriano se e soltanto se è connesso e ha 0 o 2 vertici dispari.*

Esempio 8. Il grafo dell'esempio 1 ammette un cammino Euleriano, in quanto ha 2 vertici dispari: per esempio l_3, l_4, l_5, l_2, l_1 è un cammino Euleriano.

Definizione 12. Sia $\mathcal{G} = (V, L, \varphi)$ un grafo. Si dice *Hamiltoniano* un cammino o un circuito che passi per ogni vertice di $\mathcal{G}$ una sola volta (ad esclusione al più del primo vertice del cammino, se si tratta di circuito).

Osservazione 11. Non ci sono criteri generali che permettano di stabilire se un grafo ammette un cammino Hamiltoniano. Si vede che tutti i grafi completi ammettono un cammino Hamiltoniano, mentre non ammettono cammini Euleriani tutti i grafi completi di ordine n pari, $n \geq 4$, perché hanno un numero di vertici dispari superiore a 2.

Esempio 9. Il seguente grafo semplice



non ammette un cammino Hamiltoniano, ma ammette un circuito Euleriano perché non ha vertici dispari. Quindi, ci sono esempi di grafi che ammettono cammini Hamiltoniani ma non Euleriani ed esempi di grafi che ammettono cammini Euleriani ma non Hamiltoniani.

Definizione 13. Due grafi $\mathcal{G} = (V, F, \varphi)$, $\mathcal{G}' = (V', F', \varphi')$ si dicono isomorfi se esiste un'applicazione bigettiva

$$f : V \cup L \to V' \cup L'$$

tale che

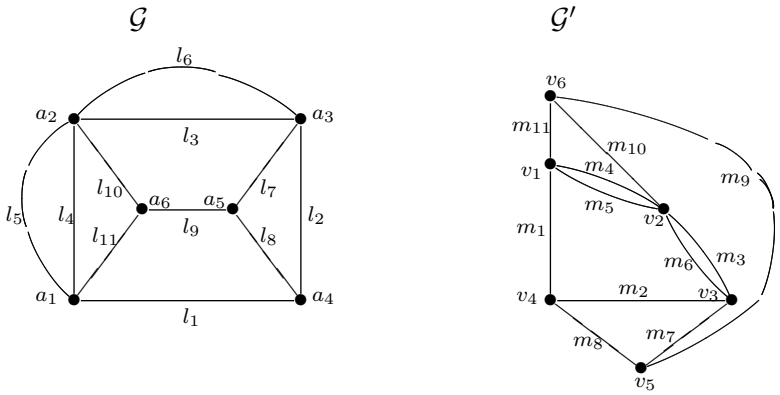
- $f(V) = V'$, $f(L) = L'$
- $\forall l \in L$ tale che $\varphi(l) = \{v, w\} \in \mathscr{P}_2(V)$ risulti $\varphi'(f(l)) = \{f(v), f(w)\}$.

Osservazione 12. Si verifica che se due grafi sono isomorfi allora hanno:

(a) lo stesso numero di vertici e lo stesso numero di lati
(b) lo stesso numero di vertici di grado fissato
(c) lo stesso numero di cammini di lunghezza fissata.

Nessuna di queste condizioni è sufficiente (da sola) per affermare che due grafi siano isomorfi. Si osservi infine che vertici di ugual grado nei due grafi non possono avere distanze diverse.

Esempio 10. I grafi $\mathcal{G} = (V, L, \varphi)$ $\mathcal{G}' = (V', L', \varphi')$ rappresentati nella seguente figura sono isomorfi.

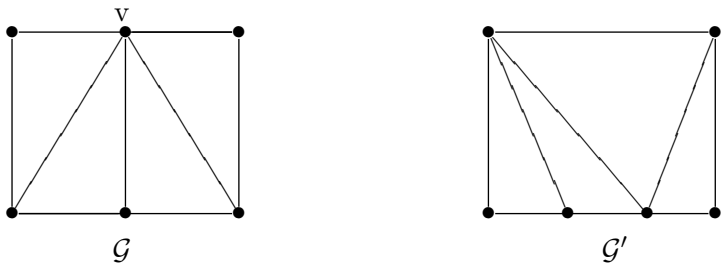


Come facilmente si verifica, l'isomorfismo è realizzato dall'applicazione

$$f : V \cup L \to V' \cup L'$$

tale che per ogni $i = 1, \ldots, 6$ risulti $f(a_i) = v_i$ e per ogni $j = 1, \ldots, 11$, $f(l_j) = m_j$.

Esempio 11. I grafi $\mathcal{G}$ e $\mathcal{G}'$ in figura



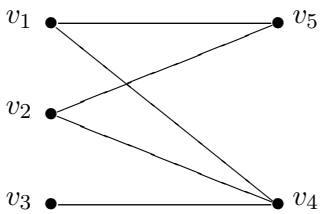
hanno entrambi 6 vertici e 9 lati, però non sono isomorfi perché $\mathcal{G}$ ha il vertice v di grado 5, mentre i vertici di $\mathcal{G}'$ hanno al massimo grado 4.

Definizione 14. Un grafo semplice $\mathcal{G} = (V, L)$ si dice *bipartito* se esistono due sottoinsiemi non vuoti V_1 e V_2 di V tali che

1. $V_1 \cap V_2 = \emptyset$, $V_1 \cup V_2 = V$
2. $\forall v, w \in V_1$, v e w non sono adiacenti
3. $\forall v, w \in V_2$, v e w non sono adiacenti.

Quando 1.,2.,3. sono verificate, V_1 e V_2 si dicono i due *partiti* di V.

Esempio 12. Il seguente grafo



è bipartito: i due partiti sono $V_1 = \{v_1, v_2, v_3\}$ e $V_2 = \{v_4, v_5\}$.

Teorema 3. *Un grafo è bipartito se e soltanto se non ammette circuiti di lunghezza dispari.*

Esempio 13. Il grafo dell'Esempio 2 non è bipartito: infatti ammette il circuito l_1, l_2, l_8, l_7, l_9 di lunghezza dispari.

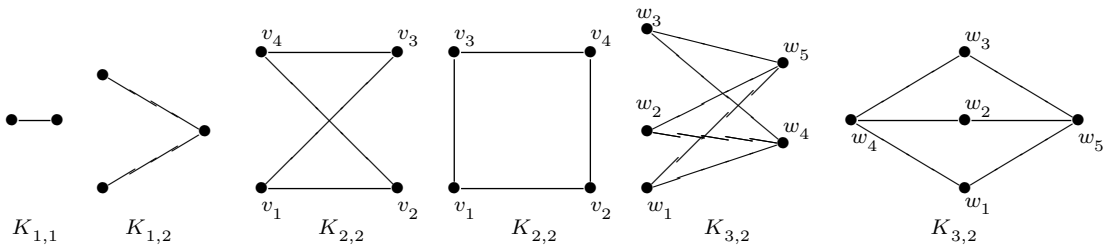
Esempio 14. Il grafo dell'Esempio 9 non ammette circuiti di lunghezza dispari, per cui è bipartito. I due partiti sono $V_1 = \{a, c, e, f\}$, $V_2 = \{b, d\}$

Definizione 15. Sia $G = (V, L)$ un grafo bipartito, con partiti V_1 e V_2. Si dice *bipartito completo* se ogni vertice di V_1 è adiacente a ogni vertice di V_2.

Osservazione 13. Fissati $n, m \in N^*$, a meno di una diversa rappresentazione, esiste un unico grafo bipartito completo tale che $|V_1| = n$, $|V_2| = m$, che si indica con $K_{n,m}$ (o con $K_{m,n}$).

Nella seguente figura sono rappresentati i grafi bipartiti completi $K_{1,1},\ K_{2,1},\ K_{2,2},\ K_{3,2}$. Si osservino le due diverse rappresentazioni di $K_{2,2}$ e di $K_{3,2}$.

fig.2



Definizione 16. Un grafo $\mathcal{G} = (V, L, \varphi)$ si dice *planare* se ammette una rappresentazione nella quale i suoi lati si intersecano soltanto negli estremi.

Teorema 4. *Per un grafo planare avente $|V|$ vertici, $|L|$ lati e $|F|$ facce, si ha:*

$$|V| - |L| + |F| = 2 \quad \text{formula di Eulero.}$$

Nel computo delle facce si tiene conto anche di quella esterna.

Proposizione 3. *Per un grafo planare avente $|V|$ vertici, $|L|$ lati risulta:*

$$|L| \leq 3|V| - 6$$

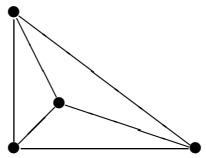
Corollario 1. *K_5 non è planare.*

Dimostrazione. Per K_5 si ha $|L| = \frac{1}{2}(5 \cdot 4) = 10$, mentre $3|V| - 6 = 15 - 6 = 9$. Poichè $10 > 9$, K_5 non può essere planare.

Osservazione 14. Si dimostra che anche $K_{3,3}$ non è planare.

Teorema 5. *(Kuratowski) Un grafo finito è planare se e solo se non ammette sottografi isomorfi a K_5 o a $K_{3,3}$.*

Esempio 15. Sono planari i grafi degli Esempi 1, 2, 9, 10, 11; inoltre sono planari K_1, K_2, K_3, K_4. In particolare K_4 ammette la seguente rappresentazione planare:



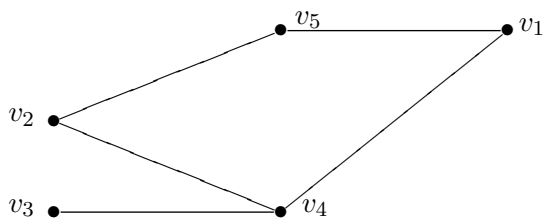
K_4

Sono planari $K_{1,1}$, $K_{2,1}$, $K_{2,2}$, $K_{3,2}$: in fig.2 ci sono anche le rappresentazioni planari di $K_{2,2}$ e di $K_{3,2}$. Infine è planare anche il grafo di fig.1, che schematizza il problema dei ponti di Könisberg,

Esercizio 3. Si verifichi la formula di Eulero per tutti i grafi planari menzionati.

Proposizione 4. *Un grafo con numero di lati $|L| < 9$ è planare.*

Esempio 16. Il grafo dell'esempio 12 è planare poichè ha 5 lati. Infatti ammette la seguente rappresentazione:



Definizione 17. Si dice *foresta* un grafo semplice privo di circuiti. Si dice *albero* un grafo connesso privo di circuiti.

Relativamente ad un albero si dimostrano i seguenti risultati.

Proposizione 5. *Sia $\mathcal{G} = (V, L)$ un albero. Se $|V| = n$, allora $|L| = n - 1$.*

Proposizione 6. *Un albero ammette sempre almeno un vertice di grado 1.*

Teorema 6. *Sia $\mathcal{G} = (V, L)$ un grafo, con $|V| = n$. Allora le seguenti proposizioni sono equivalenti:*

(a) *$\mathcal{G}$ è un albero*
(b) *$\forall v, w \in V$ esiste un unico cammino da v a w*
(c) *$\forall v, w \in V$ tali che $\{v, w\} \notin L$, il grafo $\mathcal{G}' = (V, L \cup \{\{v, w\}\})$ ammette un circuito*
(d) *$\forall l \in L$ il sottografo $= (V, L \setminus \{l\})$ non è connesso*
(e) *$\mathcal{G}$ ha $n - 1$ lati ed è connesso*
(f) *$\mathcal{G}$ ha $n - 1$ lati ed è privo di circuiti.*

Definizione 18. Sia $\mathcal{G} = (V, L)$ un albero. In virtù della (b) del Teorema 6, per ogni $v, w \in V$ esiste un unico cammino da v a w: la lunghezza di tale cammino si dice *distanza tra v e w.*

A questo punto si può chiarire il significato del nome "albero". Scelto arbitrariamente un vertice v_0 (al quale si da il nome di radice), si pongono su un livello più basso tutti i vertici che hanno distanza 1 da v_0, poi, su un livello ancora più basso, i vertici aventi distanza 2 da V_0 e così via, ponendo a livello sempre più basso i vertici che hanno

distanza maggiore da V_0. In questa maniera si ottiene la classica figura di albero con i rami rivolti verso il basso. Il procedimento è illustrato nella seguente figura.

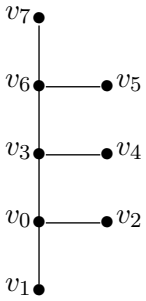
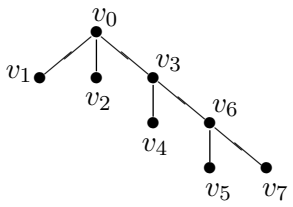


fig.3



Proposizione 7. *Un albero $\mathcal{G} = (V, L)$ è sempre un grafo bipartito.*

Osservazione 15. In generale, si possono individuare i due partiti V_1 e V_2 di un grafo bipartito fissando un vertice v_0 e considerando i due sottoinsiemi di V

$$V_1 = \{v \in V \ : \text{ la distanza di } v \text{ da } v_0 \text{ è pari } \}$$

$$V_2 = \{w \in V \ : \text{ la distanza di } w \text{ da } v_0 \text{ è dispari } \}.$$

Naturalmente $v_0 \in V_1$.

Esempio 17. Nel grafo illustrato in fig.3, i due partiti sono

$$V_1 = \{v_0, v_4, v_6\} \quad V_2 = \{v_1, v_2, v_3, v_5, v_7\}.$$

Esempio 18. Il grafo dell'Esempio 9 è bipartito, perchè non ammette circuiti di lunghezza dispari. I due partiti sono

$$V_1 = \{a, e, f, c\} \quad V_2 = \{b, d\}.$$

Proposizione 8. *Un albero è sempre un albero planare.*

Osservazione 16. Un albero $\mathcal{G}$ ha, ovviamente, un'unica faccia. In tal caso la fomula di Eulero si riduce a:

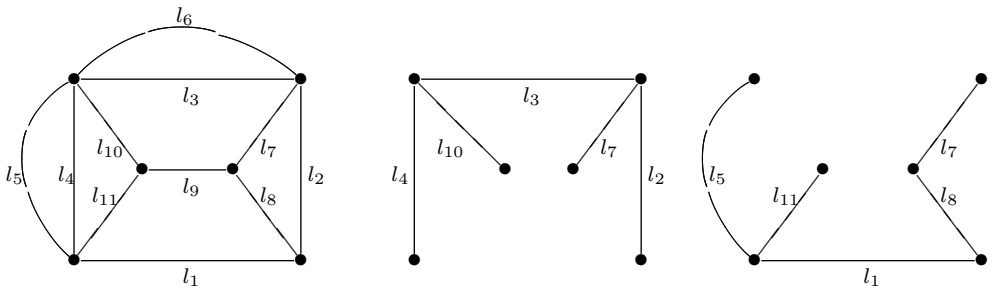
$$n - (n - 1) + 1 = 2,$$

dove n è l'ordine di G.

Definizione 19. Sia $\mathcal{G} = (V, L, \varphi)$ un grafo. Si dice *albero di supporto* o *albero generatore* di $\mathcal{G}$ un albero avente V come insieme dei vertici e insieme dei lati contenuto in L.

Osservazione 17. Ogni grafo ammette almeno un albero di supporto: basta eliminare alcuni lati in modo tale che non ci siano circuiti. Ne consegue che un grafo di ordine n non può avere meno di $n - 1$ lati.

Esempio 19. Nel seguente diagramma sono rappresentati due alberi di supporto $\mathcal{G}'$ e $\mathcal{G}$" dello stesso grafo $\mathcal{G}$.



$\mathcal{G}$ $\mathcal{G}'$ $\mathcal{G}''$

Si osservi che $\mathcal{G}'$ e $\mathcal{G}$" non sono isomorfi perchè $\mathcal{G}'$ ha due vertici di grado 3, mentre $\mathcal{G}$" ha un solo vertice di grado 3.

Definizione 1. Sia $f\colon A \to B$ una funzione. La funzione f si dice INIETTIVA o INGETTIVA se

$$\forall a, a' \in A, \quad a \neq a' \implies f(a) \neq f(a'),$$

cioè se elementi distinti di A hanno necessariamente immagini distinte in B.

Tenendo conto che $P \implies Q$ è equivalente a $\neg Q \implies \neg P$, si ottiene la seguente definizione equivalente alla precedente.

Definizione 2. Sia $f\colon A \to B$ una funzione. La funzione f si dice INIETTIVA o INGETTIVA se

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

Esempio 1. Si consideri la funzione

$$f\colon \mathbb{Z} \to \mathbb{Z} \quad \text{tale che} \quad f(n) = 3n - 4 \quad \forall n \in \mathbb{Z}$$

f è iniettiva??
La risposta è affermativa perchè $\forall n, n' \in \mathbb{Z}$ se $f(n) = f(n') \implies 3n - 4 = 3n' - 4 \implies 3n = 3n' \implies n = n'$, quindi è verificata la seconda definizione.

Esempio 2. Si consideri la funzione

$$f\colon \mathbb{Z} \to \mathbb{N} \quad \text{tale che} \quad f(n) = n^2 \quad \forall n \in \mathbb{Z}$$

f è iniettiva??
La risposta è NO perchè se, per esempio, si considerano i due numeri interi $n = 2$ e $n' = -2$ si ha che $f(2) = 4 = f(-2)$, quindi non è soddisfatta la prima definizione.

Esempio 3. Si consideri la funzione

$$f\colon \mathbb{Z} \to \mathbb{N} \quad \text{tale che} \quad f(n) = |n| \quad \forall n \in \mathbb{Z}$$

f è iniettiva??
La risposta è NO perchè se, per esempio, si considerano i due numeri interi $n = 3$ e $n' = -3$ si ha che $f(3) = 3 = f(-3)$, quindi non è soddisfatta la prima definizione.

Osservazione 1. Se $f\colon A \to B$ è una funzione iniettiva, allora per ogni $b \in B$ l'insieme controimmagine $f^{-1}(b)$ ha al più un elemento.

Osservazione 2. La nozione di iniettività dipende dall'insieme di partenza della funzione. Infatti se consideriamo la funzione

$$f\colon \mathbb{N} \to \mathbb{N} \quad \text{tale che} \quad f(n) = n^2 \quad \forall n \in \mathbb{N}$$

questa è iniettiva in quanto, comunque si scelgono due numeri naturali distinti i loro quadrati sono ancora distinti.
Se invece consideriamo

$$f\colon \mathbb{Z} \to \mathbb{N} \quad \text{tale che} \quad f(n) = n^2 \quad \forall n \in \mathbb{Z}$$

allora in tal caso f non è iniettiva. (Esempio 2)

Definizione 3. Sia $f\colon A \to B$ una funzione. La funzione f si dice SURIETTIVA o SURGETTIVA se

$$\forall b \in B, \exists a \in A \quad \text{tale che} \quad f(a) = b,$$

cioè se $Im(f) = B$.

Esempio 4. Si consideri la funzione

$$f\colon \mathbb{Z} \to \mathbb{Z} \quad \text{tale che} \quad f(n) = 3n - 4 \quad \forall n \in \mathbb{Z}$$

f è suriettiva??
La risposta è NO perchè, $\forall n' \in \mathbb{Z}$ se $f(n) = n' \implies 3n - 4 = n' \implies 3n = n' + 4 \implies n = \frac{n'+4}{3}$, ma ora questo n tovato non appartiene sempre a $\mathbb{Z}$, al variare di n' in $\mathbb{Z}$.

Esempio 5. Si consideri la funzione

$$f\colon \mathbb{Q} \to \mathbb{Q} \quad \text{tale che} \quad f(q) = 3q - 4 \quad \forall q \in \mathbb{Q}$$

f è suriettiva??
La risposta è SI perchè $\forall q' \in \mathbb{Q}$ se $f(q) = q' \implies 3q - 4 = q' \implies q = \frac{q'+4}{3}$ e questo q tovato appartiene sempre a $\mathbb{Q}$, al variare di q' in $\mathbb{Q}$.

Osservazione 3. Questi due ultimi esempi mettono in mostra come la suriettività di una funzione dipenda sia dall'insieme di partenza che dall'insieme di arrivo della funzione stessa.

Osservazione 4. Una funzione $f\colon A \to B$ è suriettiva se e solo se $f^{-1}(b) \neq \varnothing$, per ogni $b \in B$.

Osservazione 5. Sia $f\colon A \to B$ una funzione. Allora $f\colon A \to Im(f)$ è suriettiva.

Definizione 1. Sia $f\colon A \to B$ una funzione. La funzione f si dice BIETTIVA o BIGETTIVA se è sia iniettiva che suriettiva, cioè

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

Esempio 1. Si consideri la funzione

$$f\colon \mathbb{R} \to \mathbb{R} \quad \text{tale che} \quad f(x) = x^5 - 4 \quad \forall x \in \mathbb{R}$$

f è biettiva??
La risposta è SI poichè f è sia iniettiva che suriettiva. Infatti:
$\forall x, y \in \mathbb{R}$ se $f(x) = f(y) \implies x^5 - 4 = y^5 - 4 \implies x^5 = y^5 \implies x = y$, quindi f è iniettiva; inoltre $\forall y \in \mathbb{R}$ se $f(x) = y \implies x^5 - 4 = y \implies x^5 = y + 4 \implies x = \sqrt[5]{y+4}$ e tale x appartiene ad $\mathbb{R}$, comunque si scelga $y \in \mathbb{R}$. Quindi f è anche suriettiva.

Esempio 2. Si consideri la funzione

$$f\colon \mathbb{Z} \to \mathbb{N} \quad \text{tale che} \quad f(n) = n^2 \quad \forall n \in \mathbb{Z}$$

f è biettiva??
Osserviamo che f è non iniettiva, infatti se si considerano gli interi $n = 2$ e $n' = -2$, pur essendo diversi, le loro immagini, mediante f, coincidono.
Quindi la funzione f NON è biettiva, poichè per esserlo dovrebbe essere sia iniettiva che suriettiva.

Definizione 2. Siano $f\colon A \to B$ e $g\colon B \to C$ due funzioni. Si chiama FUNZIONE COMPOSIZIONE di f e g, si indica con $g \circ f$ (si legge g cerchietto f), la funzione

$$g \circ f\colon A \to C \quad \text{tale che} \quad \forall a \in A, (g \circ f)(a) = g(f(a)),$$

cioè

$$\underset{a}{A} \xrightarrow[\mapsto]{f} \underset{f(a)}{B} \xrightarrow[\mapsto]{g} \underset{g(f(a))}{C}$$

Osservazione 1. Come si evince dalla definizione precedente, affinchè esita la funzione composta $g \circ f$ è fondamentale che l'insieme di arrivo di f (funzione che si trova scritta più a destra, cioè quella che viene applicata per prima) coincida con l'insieme di partenza di g (funzione più a sinistra).
Questa è la regola generale per stabilire se, assegnate due funzioni f e g esiste la loro funzione composizione $g \circ f$

Osservazione 2. Se esiste la funzione $g \circ f$, come si evince dalla definizione, $g \circ f$ ha come insieme di partenza l'insieme di partenza di f e come insieme di arrivo quello della funzione g.

Osservazione 3. Come segue dalla definizione, assegnate due funzioni f e g è ben diverso determinare, se è possibile, $g \circ f$ e $f \circ g$.
Nell'ipotesi che esistano entrambe le funzioni composizioni, in generale si ha $g \circ f \neq f \circ g$. Spesso questo si esprime dicendo che l'operazione di composizione $\circ$, in generale, non è commutativa.

Esempio 3. Si considerino le seguenti funzioni:

$$f\colon \mathbb{N} \to \mathbb{N} \quad \text{tale che} \quad f(n) = n^2 \quad \forall n \in \mathbb{N}$$

$$g\colon \mathbb{N} \to \mathbb{N} \quad \text{tale che} \quad f(t) = t + 2 \quad \forall t \in \mathbb{N}$$

Esiste $g \circ f$? La risposta è SI poichè l'insieme di arrivo di f coincide con l'insieme di partenza di g.
Esiste $f \circ g$? La risposta è SI poichè l'insieme di arrivo di g coincide con l'insieme di partenza di f.
Osservato ciò, tenendo conto dell' Osservazione 2 e della Definizione 2, si ha

$$g \circ f\colon \mathbb{N} \to \mathbb{N} \quad \text{tale che} \quad \forall n \in \mathbb{N}$$

$$(g \circ f)(n) = g(f(n)) = g(n^2) = n^2 + 2$$

e

$$f \circ g\colon \mathbb{N} \to \mathbb{N} \quad \text{tale che} \quad \forall n \in \mathbb{N}$$

$$(f \circ g)(n) = f(g(n)) = f(n + 2) = (n + 2)^2$$

Osserviamo che $g \circ f \neq f \circ g$

Esempio 4. Si considerino le seguenti funzioni:

$$h\colon \mathbb{N} \to \mathbb{Q}^* \quad \text{tale che} \quad h(n) = \frac{n}{3} + 1 \quad \forall n \in \mathbb{N}$$

$$f\colon \mathbb{Q}^* \to \mathbb{Q} \quad \text{tale che} \quad f(q) = \frac{1}{q} \quad \forall q \in \mathbb{Q}^*$$

Esiste $h \circ f$? La risposta è NO poichè l'insieme di arrivo di f non coincide con l'insieme di partenza di h.
Esiste $f \circ h$? SI, perchè l'insieme di arrivo di h è uguale all'insieme di partenza di f. In tal caso si ha:

$$f \circ h\colon \mathbb{N} \to \mathbb{Q} \quad \text{tale che} \quad \forall n \in \mathbb{N}$$

$$(f \circ h)(n) = f(h(n)) = f(\frac{n}{3} + 1) = \frac{1}{\frac{n}{3} + 1} = \frac{3}{n + 3}$$

PROPRIETA' 1. *1) (Associativa) Siano* $f\colon A \to B$, $g\colon B \to C$ *e* $h\colon C \to D$ *tre funzioni.Allora*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

2) Sia $f\colon A \to B$ *una funzione e siano* id_A *e* id_B *le funzioni identità su* A *e* B*, rispettivamente. Allora*

$$f \circ id_A = f = id_B \circ f.$$

3) Siano $f\colon A \to B$ *e* $g\colon B \to C$ *due funzioni.*
Se f *e* g *sono iniettive, allora* $g \circ f$ *è iniettiva.*
Se f *e* g *sono suriettive, allora* $g \circ f$ *è suriettiva.*
Se f *e* g *sono biettive, allora* $g \circ f$ *è biettiva.*

Osservazione 1. Per ciascuna di queste tre implicazioni non vale il viceversa. A supporto di tale affermazione, forniamo il seguente controesempio.
Si considerino i seguenti tre insiemi:

$$A = \{1\}; \quad B = \{a, b, c\}; \quad C = \{t\}.$$

A partire da essi, definiamo le seguenti due funzioni:

$$f\colon A \to B \quad \text{tale che} \quad f(1) = a$$

$$g\colon B \to C \quad \text{tale che} \quad g(a) = g(b) = g(c) = t.$$

Si osserva, facilmente, per come sono definite, che f è una funzione iniettiva ma non suriettiva e g è una funzione suriettiva ma non iniettiva.
Inoltre possiamo considerare la funzione composta

$$g \circ f\colon A \to C \quad \text{tale che} \quad (g \circ f)(1) = t.$$

Si verifica facilmente che $g \circ f$ è una funzione iniettiva e suriettiva, quindi anche biettiva.
Dunque, $g \circ f$ è una funzione iniettiva ma f e g non sono entrambe iniettive. Questo mostra che non vale il viceversa della prima implicazione della Proprietà 3.
Analogamente per le altre due implicazioni.

Definizione 1. Sia $f\colon A \to B$ una funzione. La funzione f si dice INVERTIBILE se esiste una funzione $g\colon B \to A$ tale che $f \circ g = id_B$ e $g \circ f = id_A$.
Tale funzione g si dice FUNZIONE INVERSA di f

Osservazione 2. Se f è una funzione invertibile, la sua funzione inversa è UNICA.

Proposizione 1. *Sia $f\colon A \to B$ una funzione. f è invertibile se e solo se f è biettiva.*
Inoltre, nell'ipotesi che f sia invertibile, la funzione inversa di f è la funzione $f^{-1}\colon B \to A$ tale che $b \in B \mapsto f^{-1}(b) \in A$

Dimostrazione. Per provare l'equivalenza bisogna provare la doppia implicazione.
Iniziamo col provare la seconda implicazione, cioè proviamo che se f è biettiva allora f è invertibile.
Supponiamo f biettiva, dunque, per definizione, si ha che $\forall b \in B, \exists! a \in A$ tale che $f(a) = b$ ma questo equivale a dire che $\forall b \in B, \exists! a \in A$ tale che $f^{-1}(b) = \{a\}$.
Dunque ha senso definire la funzione $f^{-1}\colon B \to A$ tale che $b \in B \mapsto f^{-1}(b) \in A$.
Per provare che f è invertibile, resta da dimostrare che f^{-1} è la sua funzione inversa, cioè $f \circ f^{-1} = id_B$ e $f^{-1} \circ f = id_A$. Questo è di verifica immediata.
Proviamo, ora, la prima implicazione.
Supponiamo f invertibile, dunque, per definizione, esiste (ed è unica) $g\colon B \to A$ tale che $f \circ g = id_B$ e $g \circ f = id_A$.
Sotto tale ipotesi dimostriamo che f è biettiva, cioè iniettiva e suriettiva.
Per ogni $x, x' \in A$ se $f(x) = f(x') \implies g(f(x)) = g(f(x')) \implies (g \circ f)(x) = (g \circ f)(x') \implies id_A(x) = id_A(x') \implies x = x'$, dunque f è iniettiva.
Ora, per ogni $b \in B$ possiamo considerare $g(b) \in A$.
Poniamo $a = g(b) \in A$ e dunque $f(a) = f(g(b)) = (f \circ g)(b) = id_B(b) = b$.
Ciò dimostra che f è suriettiva.
Infine, è facile osservare che questa funzione g è proprio la funzione f^{-1}. □

Osservazione 3. Se f è una funzione invertibile(equivalentemente, biettiva), allora lo è anche la sua funzione inversa f^{-1}.

PROPRIETA' 2. *1) Siano $f\colon A \to B$ e $g\colon B \to C$ due funzioni invertibili. Allora $g \circ f$ è una funzione invertibile, inoltre*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

2) La funzione identità id_A è invertibile, inoltre $(id_A)^{-1} = id_A$.
3) Sia $f\colon A \to B$ una funzione invertibile. Allora $(f^{-1})^{-1} = f$.

Definizione 1. Sia A un insieme non vuoto. Un'applicazione

$$* : A \times A \to A$$

si dice *legge di composizione interna* o *operazione* su A. La coppia ordinata $(A, *)$ si dice *struttura algebrica*, della quale A è il *sostegno*.

Osservazione 1. Se è assegnata una struttura algebrica $(A, *)$, allora invece di scrivere $*(x, y)$ si scrive $x * y$.

Definizione 2. Sia $(A, *)$ una struttura algebrica. Si dice che la legge di composizione $*$ verifica la proprietà *associativa* se

$$\forall x, y, z \in A, \quad (x * y) * z = x * (y * z).$$

Definizione 3. Sia $(A, *)$ una struttura algebrica. Se la legge di composizione $*$ verifica la proprietà associativa si dice che $(A, *)$ è un *monoide* (o un *semigruppo*).

Definizione 4. Sia $(A, *)$ una struttura algebrica. Si dice che $(A, *)$ ammette *elemento neutro* se

$$\exists e \in A \text{ tale che } \forall x \in A \quad x * e = e * x = x.$$

Naturalmente e si dice elemento neutro della struttura algebrica $(A, *)$.

Proposizione 1. *Se una struttura algebrica $(A, *)$ ammette elemento neutro, esso è unico.*

Dimostrazione. Siano e_1 ed e_2 elementi neutri della struttura algebrica $(A, *)$. Allora $e_1 = e_1 * e_2 = e_2$.

Osservazione 2. Nei testi spesso è chiamato monoide una struttura algebrica associativa e con elemento neutro.

Sono esempi di monoidi con unità: $(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$, il monoide delle parole (definito a lezione).

Definizione 5. Sia $(A, *)$ una struttura algebrica dotata di elemento neutro e, e sia $x \in A$. Si dice che x è simmetrizzabile se esiste $x' \in A$ tale che $x * x' = x' * x = e$; x' si dice il *simmetrico di x*.

Definizione 6. Si dice che una struttura algebrica $(A, *)$ è un *gruppo* se è associativa, se ammette elemento neutro e se ogni elemento è simmetrizzabile. In altri termini $(A, *)$ è un gruppo se sono verificate le seguenti proprietà

- $\forall x, y, z \in A, \quad (x * y) * z = x * (y * z)$.
- $\exists e \in A$ tale che $\forall x \in A \quad x * e = e * x = x$.
- $\forall x \in a \quad \exists x' \in A$ tale che $x * x' = x' * x = e$.

Esempi di gruppi sono: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$.

Definizione 7. Sia $(A, *)$ una struttura algebrica. Si dice che la legge di composizione $*$ verifica la proprietà *commutativa* se

$$\forall x, y \in A, \quad x * y = y * x.$$

In tal caso la struttura algebrica $(A, *)$ si dice commutativa. Un gruppo commutativo si dice *abeliano*.

Osservazione 3. Il monoide delle parole non è commutativo, mentre sono commutativi i monoidi $(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$. I gruppi $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ sono tutti abeliani. Si vedranno in seguito alcuni esempi di gruppi non abeliani.

Definizione 8. Sia $(A, *)$ una struttura algebrica, $\mathcal{R}$ una relazione di equivalenza su A. Si dice che $\mathcal{R}$ è *compatibile con* $*$ se

$$\forall a, b, c, d \in A, \quad ((a, b) \in \mathcal{R} \ \wedge \ (c, d) \in \mathcal{R}) \ \Rightarrow \ (a * c, b * d) \in \mathcal{R}.$$

Osservazione 4. Se una relazione di equivalenza $\mathcal{R}$ è compatibile con una legge di composizione interna $*$, allora è possibile definire sull'insieme quoziente $A/\mathcal{R}$ una legge di composizione interna $*_{\mathcal{R}}$ come segue:

$$\forall\ [a]_{\mathcal{R}}, [b]_{\mathcal{R}} \in A/\mathcal{R}, \quad [a]_{\mathcal{R}}\ *_{\mathcal{R}}\ [b]_{\mathcal{R}} = [a * b]_{\mathcal{R}}.$$

Si dimostra che $*_{\mathcal{R}}$ verifica tutte le proprietà di $*$. Quindi, in particolare, se $(A, *)$ è un monoide o un gruppo, allora $(A/\mathcal{R}, *_{\mathcal{R}})$ è monoide o un gruppo, rispettivamente. Inoltre, se $(A, *)$ è una struttura commutativa, allora anche $(A/\mathcal{R}, *_{\mathcal{R}})$ è una struttura commutativa.

Esempio 1. La congruenza ($\mathtt{mod}n$) è compatibile sia con la somma che con il prodotto di $\mathbb{Z}$ (verificato a lezione) e quindi si possono considerare le leggi di composizione interne indotte sull'insieme quoziente $\mathbb{Z}_n$.

$$\forall\ [a]_n,\ [b]_n \in \mathbb{Z}_n \quad [a]_n + [b]_n = [a+b]_n, \quad [a]_n \cdot [b]_n = [a \cdot b]_n.$$

Risultano, quindi, le due strutture algebriche $(\mathbb{Z}_n, +)$, che è un gruppo abeliano, e $(\mathbb{Z}_n, \cdot)$, che è un monoide commutativo.

Gruppi

Osservazione 5. Un gruppo G può essere denotato moltiplicativamente, per esempio con $\cdot$, con $\bullet$, con $\odot$, ecc.: in tal caso si usa generalmente la notazione 1_G o semplicemente 1 per l'elemento neutro e per ogni $x \in G$ si indica con x^{-1} l'elemento simmetrico di x, che dice *inverso di* x. Può anche essere denotato additivamente con $+$, con $\oplus$ ecc.: allora si usa generalmente la notazione 0_G o semplicemente 0 per l'elemento neutro e per ogni $x \in G$ si indica con $-x$ l'elemento simmetrico di x, che si dice *opposto di* x.

Definizione 9. Sia $(G, \cdot)$ un gruppo. Fissato $n \in \mathbb{Z}$, definisce la *potenza n-ma* di g nel modo che segue:

- ricorsivamente per $n \in \mathbb{N}$:
$$\begin{cases} g^0 = 1_G \\ g^n = g^{n-1} g, \quad n > 0 \end{cases}$$
- per $n < 0$, si pone $g^n = (g^{-n})^{-1}$.

Osservazione 6. Se $(G, +)$ è un gruppo denotato additivamente, allora fissato $n \in \mathbb{Z}$, si parla non di potenza n-ma di g, ma di *multiplo secondo* n di g. Si definisce in modo analogo:

- ricorsivamente per $n \in \mathbb{N}$:
$$\begin{cases} 0\ g = 0 \\ n\ g = (n-1)\ g + g, \quad n > 0 \end{cases}$$
- per $n < 0$, si pone $n\ g = -(-n\ g)$.

Proposizione 2. *Sia $(G, \cdot)$ un gruppo. Allora si ha*

(1) $\forall g \in G, \quad \forall m, n \in \mathbb{Z} \quad g^m \cdot g^n = g^{m+n}$
(2) $\forall g \in G, \quad \forall m, n \in \mathbb{Z} \quad (g^m)^n = g^{mn}$
(3) *se $(G, \cdot)$ è abeliano, allora* $\forall g, h \in G, \quad \forall n \in \mathbb{Z} \quad (g \cdot h)^n = g^n \cdot h^n$.

Osservazione 7. Se il gruppo $(G, +)$ è denotato additivamente, allora le precedenti proprietà si riscrivono nel modo seguente:

(1) $\forall g \in G, \quad \forall m, n \in \mathbb{Z} \quad (m+n)\ g = m\ g + n\ g$
(2) $\forall g \in G, \quad \forall m, n \in \mathbb{Z} \quad m\ (n\ g) = (mn)\ g$
(3) se $(G, +)$ è abeliano, allora $\forall g, h \in G, \quad \forall n \in \mathbb{Z} \quad n\ (g + h) = n\ g + n\ h$.

Definizione 10. Sia $(G, \cdot)$ un gruppo, $H \subseteq G$. Si dice che H è un *sottogruppo* di G se verifica le seguenti 3 condizioni

SG_1) $H \neq \emptyset$
SG_2) $\forall x, y \in H, \quad x \cdot y \in H$
SG_3) $\forall x \in H, \quad x^{-1} \in H$.

Osservazione 8. Nel caso di un gruppo $(G, +)$ denotato additivamente, le condizioni SG_2), SG_3) della precedente Definizione si riscrivono come segue:

SG_2) $\forall x, y \in H, \quad x + y \in H$
SG_3) $\forall x \in H, \quad -x \in H$.

Teorema 1. *Sia $(G, \cdot)$ un gruppo, $H \subseteq G$. Allora H è un sottogruppo di G se e soltanto se sono verificate le seguenti 2 condizioni*

SG'$_1$) $1_G \in H$
SG'$_2$) $\forall x, y \in H, \quad x \cdot y^{-1} \in H$.

Osservazione 9. Nel caso di un gruppo $(G, +)$ denotato additivamente, le condizioni SG'$_1$), SG'$_2$) del precedente Teorema si riscrivono come segue:

SG_2) $0_G \in H$
SG_3) $\forall x, y \in H, \quad x - y \in H$.

Esempio 2. Sia $(G, \cdot)$ un gruppo. Allora G e $\{1_G\}$ sono sottogruppi di $(G, \cdot)$.

Proposizione 3. *Sia $(G, \cdot)$ un gruppo. Allora l'intersezione di due sottogruppi di G è un sottogruppo di G (si verifichi per esercizio).*

Osservazione 10. In generale l'unione di due sottogruppi di G non è un sottogruppo di G: ciò si può vedere con degli esempi.

Definizione 11. Sia $(G, \cdot)$ un gruppo. Si indica con $|G|$ la cadinalità (finita o infinita di G), che si chiama *ordine* di G. La stessa notazione vale ovviamente per i sottogruppi.

Teorema 2. *(Lagrange) Sia $(G, \cdot)$ un gruppo finito di ordine n, H un suo sottogruppo di ordine h. Allora $h|n$ (h è un divisore di n).*

Proposizione 4. Sia $(G, \cdot)$ un gruppo, $g \in G$. Allora il sottoinsieme

$$< g >= \{a \in G : \exists h \in \mathbb{Z} \text{ tale che } a = g^h\} = \{g^h : h \in \mathbb{Z}\}$$

è un sottogruppo di G.
(verificata a lezione)

Definizione 12. Sia $(G, \cdot)$ un gruppo, $g \in G$. Il sottogruppo $< g >$ si dice *sottogruppo ciclico generato da g.*

Osservazione 11. Se il gruppo $(G, +)$ è denotato additivamente e $g \in G$, allora il sottogruppo ciclico generato da g si scrive

$$< g >= \{a \in G : \exists h \in \mathbb{Z} \text{ tale che } a = hg\} = \{hg \mid h \in \mathbb{Z}\}.$$

Osservazione 12. Si osservi che un gruppo infinito può anche ammettere sottogruppi finiti: per esempio il sottogruppo ciclico di $(\mathbb{Q}^*, \cdot)$ generato da -1 è finito in quanto $< -1 >= \{1, -1\}$.

Proposizione 5. *Sia $(G, \cdot)$ un gruppo, $g \in G$. Allora si ha una delle seguenti possibilità:*

(1) $(\forall\ h, k \in \mathbb{Z})\ (g^h \neq g^k) \ \Leftrightarrow < g >$ *è infinito*
(2) $(\exists\ h, k \in \mathbb{Z})\ (g^h = g^k) \ \Leftrightarrow < g >$ *è finito.*

Definizione 13. Sia $(G, \cdot)$ un gruppo, $g \in G$. Si dice che g *ha ordine infinito*, e si scrive $|g| = +\infty$, se $| < g > | = +\infty$; si dice che g *ha ordine o periodo* $k \in \mathbb{N}^*$, e si scrive $|g| = k$, se $| < g > | = k$. (Si noti che in ogni caso $|g| = | < g > |$.)

Definizione 14. Si dice che un gruppo $(G, \cdot)$ è *ciclico* se esiste $g \in G$ tale che $< g >= G$. In tal caso g si dice *generatore* di G.

Osservazione 13. Sia $(G, \cdot)$ un gruppo finito di ordine n. Allora $(G, \cdot)$ è ciclico se e solo se esiste un elemento $g \in G$ tale che $|g| = n$.

Esempio 3. Sono gruppi ciclici:

(1) $(\mathbb{Z}, +)$, in quanto 1 e -1 ne sono generatori
(2) $(\mathbb{Z}_n, +)$, in quanto $[1]_n$ ne è generatore.

Teorema 3. *Ogni sottogruppo di un gruppo ciclico è ciclico.*

Quindi, per esempio, sono ciclici tutti i sottogruppi di $(\mathbb{Z}, +)$ e tutti i sottogruppi di $(\mathbb{Z}_n, +)$

Teorema 4. *(Inverso del Teorema di Lagrange per i gruppi ciclici) Sia $(G, \cdot)$ un gruppo ciclico di ordine n. Allora per ogni h divisore di n esiste un unico sottogruppo di $(G, \cdot)$ avente ordine h.*

Proposizione 6. *Sia $(G, \cdot)$ un gruppo ciclico finito di ordine n e ne sia g un generatore, ovvero $G =< g >$. Pertanto, per ogni elemento $a \in G$ esiste $h \in \mathbb{Z}$ tale che $a = g^h$. Risulta allora:*

$$|a| = |g^h| = \frac{n}{M.C.D.(h, n)} \tag{1}$$

Osservazione 14. Segue da (1) che per ogni numero intero h primo con n, g^h è un generatore di G. In particolare, i generatori del gruppo $(\mathbb{Z}_n, +)$ sono tutti e soli gli elementi $[h]_n \in \mathbb{Z}_n$ tali che h sia primo con n e quindi i generatori di $(\mathbb{Z}_n, +)$ sono esattamente $\varphi(n)$ (φ funzione di Eulero).

Esercizio 1. Verificare che:

1. un gruppo finito di ordine p primo è ciclico.
2. un gruppo ciclico è abeliano.

Proposizione 7. *Siano $(G, \cdot)$ un gruppo, $a \in G$, con $|a| = m$. Allora si ha:*

$$m = min\{h \in \mathbb{N}^* : a^h = 1_G\}$$

Proposizione 8. *Sia $n \in \mathbb{N}$, $n > 1$. Allora un elemento $[a]_n \in \mathbb{Z}_n^*$ è invertibile nel monoide $(\mathbb{Z}_n, \cdot)$ se e soltanto se $M.C.D.(a, n) = 1$.*

Dimostrazione. Un elemento $[a]_n \in \mathbb{Z}_n^*$ è invertibile se esiste $[x]_n \in \mathbb{Z}_n$ tale che

$$[a]_n \cdot [x]_n = [1]_n,$$

ovvero

$$[a \cdot x]_n = [1]_n.$$

Pertanto, per trovare $[x]_n$, laddove esista, bisogna risolvere la congruenza lineare

$$a\ x \equiv 1\ (\texttt{mod}\ n), \tag{2}$$

che ha soluzioni se e solo se $M.C.D.(a, n)|1$. Inoltre, nel caso in cui (2) abbia soluzioni, ce nè soltanto una $\texttt{mod}\ n$. Questo a conferma dell'unicità dell'inverso.

Corollario 1. *Se $p \in \mathbb{Z}$ è un numero primo, allora $\mathbb{Z}_p^*$ è chiuso rispetto a $\cdot$.*

Dimostrazione. Per la proposizione precedente, ogni elemento di $\mathbb{Z}_p^*$ ha inverso rispetto a $\cdot$. Siano $[a]_p,\ [b]_p \in \mathbb{Z}_p^*$ se fosse

$$[a]_p \cdot [b]_p = 0,$$

moltiplicando a sinistra per l'inverso $[a]_p^{-1}$ di $[a]_p$ si avrebbe

$$[a]_p^{-1} \cdot [a]_p \cdot [b]_p = [a]_p^{-1} \cdot 0,$$

ossia $[b]_p = 0$ che contraddice $[b]_p \in \mathbb{Z}_p^*$. Quindi $[a]_p \cdot [b]_p \in \mathbb{Z}_p^*$, ovvero $\mathbb{Z}_p^*$ è chiuso rispetto a $\cdot$.

Corollario 2. *Se $p \in \mathbb{Z}$ è un numero primo, allora la struttura algebrica $(\mathbb{Z}_p^*, \cdot)$ è un gruppo abeliano.*

Un esempio di gruppo non abeliano si costruisce nel modo che segue. Sia A un insieme e sia $\mathcal{S}(A)$ l'insieme delle applicazioni bigettive su A. Si prova facilmente che la struttura algebrica $(\mathcal{S}(A), \circ)$ è un gruppo non abeliano (dimostrato a lezione).
Sia S_n l'insieme delle permutazioni su n oggetti, ovvero su un insieme di cardinalità n. Non è lesivo della generalità considerare S_n come l'insieme delle permutazioni sui primi numeri naturali non nulli

$$\{1, 2, \ldots, n\}.$$

Si è visto che $|S_n| = n!$. La composizione di applicazioni fornisce una legge di composizione interna su S_n:

$$\circ : S_n \times S_n \to S_n.$$

$(S_n, \circ)$ è un gruppo, (è un caso particolare di $(\mathcal{S}(A), \circ)$) e per $n > 2$ è *non* abeliano. Quindi non può essere ciclico per $n > 2$ (cf. Esercizio 1).

Definizione 15. Si sice che una permutazione f *muove* un elemento a se $f(a) \neq a$; si dice che *fissa* a se $f(a) = a$.

Definizione 16. Si dice che due permutazioni f e g sono *disgiunte* se gli elementi mossi da f sono fissati da g.

Osservazione 15. Se due permutazioni f e g sono disgiunte, allora

$$f \circ g = g \circ f.$$

Definizione 17. Si dice *ciclo di lunghezza* r, e si indica con il simbolo $(c_1 c_2 \ldots c_r)$, $r \leq n$ la permutazione $f \in S_n$ tale che

$$f(c_1) = c_2, f(c_2) = c_3, \ldots, f(c_{r-1}) = c_r, f(c_r) = c_1$$

e tutti gli altri elementi vengono fissati da f. Un ciclo di lunghezza 2 si chiama scambio.

Osservazione 16. Si osservi che si ha $(c_1 c_2 \ldots c_r) = (c_2 \ldots c_r c_1) = (c_3 \ldots c_r c_1 c_2) = \ldots (c_r c_1 \ldots c_{r-1})$.

Teorema 5. Sia $f \in S_n$. Allora f è un ciclo oppure può essere scritta, in modo unico a meno dell'ordine, come prodotto di cicli disgiunti.

Osservazione 17. Si può scrivere il ciclo $(c_1 c_2 \ldots c_r)$ come

$$(c_1 c_2 \ldots c_r) = (c_1 c_r) \circ \cdots \circ (c_1 c_3) \circ (c_1 c_2).$$

Quindi ogni ciclo può essere scritto come prodotto di scambi e dunque ogni permutazione può essere scritta prima come prodotto di cicli e poi come prodotto di scambi. La scomposizione in scambi non è unica. Per esempio:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} = (1\ 3\ 2) \circ (4\ 5) = (1\ 2) \circ (1\ 3) \circ (4\ 5)$$
$$= (1\ 2) \circ (3\ 4) \circ (3\ 4) \circ (1\ 3) \circ (4\ 5).$$

Teorema 6. Due scomposizioni in scambi di una stessa permutazione hanno la stessa parità.

Il precedente Teorema giustifica la seguente:

Definizione 18. Si dice che una permutazione è *di classe pari* (rispettivamente *di classe dispari*) se una sua qualunque scomposizione è costituita da un numero pari (rispettivamente dispari) di scambi.

Si può quindi definire l'applicazione

$$\Delta : S_n \to \{+1, -1\} \text{ tale che } \Delta(f) = \begin{cases} 1 & \text{se } f \text{ è di classe pari} \\ -1 & \text{se } f \text{ è di classe dispari.} \end{cases}$$

Proposizione 9. Il sottoinsieme formato dalle permutazioni di classe pari costituisce un sottogruppo di S_n, che si chiama gruppo alterno.

Osservazione 18. Sia σ un ciclo di lunghezza r. Allora l'ordine di σ nel gruppo $(S_n, \circ)$ è r.

Proposizione 10. *Sia $f \in S_n$, e sia $f = \sigma_1 \circ \cdots \circ \sigma_h$ la sua scomposizione in cicli disgiunti. Allora*

$$|f| = m.c.m.(|\sigma_1|, \ldots, |\sigma_h|).$$

Osservazione 19. Il gruppo $(S_n, \circ)$ non è ciclico per $n \geq 3$.

Definizione 19. Siano $(A, *)$, $(B, \cdot)$ due strutture algebriche. Si può allora considerare sul prodotto cartesiano $A \times B$ la legge di composizione interna $\odot$ definita come segue:

$$\forall (a, b),\ (a', b') \in A \times B, \quad (a, b) \odot (a', b') = (a * a', b \cdot b'). \tag{3}$$

Si può verificare facilmente la seguente:

Proposizione 11. *Siano $(A, *)$, $(B, \cdot)$ due strutture algebriche, e sia $(A \times B, \odot)$ la struttura algebrica definita in* (3)*. Allora si ha:*

- *se le due strutture $(A, *)$ e $(B, \cdot)$ sono entrambe associative, allora $(A \times B, \odot)$ è associativa*
- *se la struttura $(A, *)$ ammette elemento neutro e_A e la struttura $(B, \cdot)$ ammette elemento neutro e_B allora $(A \times B, \odot)$ ammette elemento neutro (e_A, e_B)*
- *se a è un elemento simmetrizzabile di A avente a' come simmetrico e b è un elemento simmetrizzabile di B avente b' come inverso, allora la coppia (a, b) è simmetrizzabile in $(A \times B, \odot)$ ed ha come simmetrico (a', b')*
- *se le due strutture $(A, *)$ e $(B, \cdot)$ sono commutative, allora $(A \times B, \odot)$ è commutativa*
- *quindi, se $(A, *)$ e $(B, \cdot)$ sono monoidi (commutativi), allora $(A \times B, \odot)$ è un monoide (commutativo); se $(A, *)$ e $(B, \cdot)$ sono gruppi (abeliani), allora $(A \times B, \odot)$ è un gruppo (abeliano), che si dice* gruppo somma diretta *dei gruppi $(A, *)$ e $(B, \cdot)$, che si indica con $A \oplus B$.*

Osservazione 20. Si può verificare che se $(A, *)$ e $(B, \cdot)$ sono gruppi, $a \in A$, $b \in B$, entrambi di ordine finito, allora si ha la seguente formula nel gruppo somma diretta $A \oplus B$

$$|(a, b)| = m.c.m(|a|, |b|).$$

Esempio 4. Fissati $n, m \in \mathbb{N}^*$, $n \neq 1$, si può considerare il gruppo somma diretta $\mathbb{Z}_n \oplus \mathbb{Z}_m$ di $(\mathbb{Z}_n, +)$ e $(\mathbb{Z}_m, +)$, che è un gruppo abeliano finito di ordine $n \cdot m$.

Esercizio 2. In quali ipotesi su n ed m, $\mathbb{Z}_n \oplus \mathbb{Z}_m$ è ciclico?

Esercizio 3. Studiare il gruppo $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ (gruppo di Klein).

Anelli

Definizione 20. Sia A un insieme non vuoto, dotato di due leggi di composizione interne $+$ e $\cdot$. Si dice che la struttura algebrica $(A, +, \cdot)$ è un *anello* se;

(1) $(A, +)$ è un gruppo abeliano
(2) $(A, \cdot)$ è un monoide (ovvero $\cdot$ è associativa)
(3) valgono le proprietà distibutive, ovvero $\forall a, b, c \in A$ si ha

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Se $(A, \cdot)$ è un monoide con unità, allora si parla di *anello con unità*; se $(A, \cdot)$ è commutativo, allora $(A, +, \cdot)$ si dice *anello commutativo.*

Nel seguito ci si riferirà sempre ad anelli con unità, anche se verranno chiamati semplicemente anelli.

Esempio 5. Sono esempi di anelli commutativi gli insiemi $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$.

Tra le proprietà di un anello , che per ragioni di tempo vengono tralasciate, si evidenzia la seguente:

Proposizione 12. *Sia $(A, +, \cdot)$ un anello. Allora si ha:*

$$\forall\ a \in A \quad a \cdot 0 = 0 \cdot a = 0.$$

Dimostrazione. Sia $A \in A$. Per la proprietà distributiva, si ha:

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

e, per le leggi di cancellazione applicate al gruppo $(A, +)$, segue $a \cdot 0 = 0$; analogamente si vede che $0 \cdot a = 0$.

Definizione 21. Si dice che un anello $(A, +, \cdot)$ è un *corpo* se ogni elemento non nullo di A è invertibile rispetto a $\cdot$; un corpo commutativo si chiama *campo.*

Esempio 6. Sono campi, per esempio, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_p, +, \cdot)$, p numero primo.

Osservazione 21. Nell'anello $(\mathbb{Z}_6, +, \cdot)$ il prodotto $[3]_6 \cdot [2]_6 = [0]_6$, pur essendo $[3]_6 \neq [0]_6$ e $[2]_6 \neq [0]_6$; d'altra parte $[5]_6$ ammette come inverso moltiplicativo $[5]_6$. Pertanto hanno senso le seguenti definizioni:

Definizione 22. Sia $(A, +, \cdot)$ un anello. Un elemento $a \in A$ si dice *divisore dello zero* se

(1) $a \neq 0$
(2) $\exists\ b \in A,\ b \neq 0,$ tale che $a \cdot b = 0.$

In tal caso b si dice *codivisore dello zero* di a

Osservazione 22. Si noti che un divisore dello zero di un anello in generale ammette più di un codivisore dello zero: nell'anello $(\mathbb{Z}_6, +, \cdot)$, si può notare che $[2]_6$ e $[4]_6$ sono entrambi codivisori dello zero di $[3]_6$.

Definizione 23. Sia $(A, +, \cdot)$ un anello. Un elemento $a \in A$ si dice *unitario* se è inveritibile rispetto a $\cdot$.

Proposizione 13. *Sia $(A, +, \cdot)$ un anello. Allora un elemento unitario di A non può essere un divisore dello zero.*

Dimostrazione. Sia $a \in A$ un elemento unitario. Se per assurdo a fosse un divisore dello zero, sarebbe $a \neq 0$ ed inoltre esisterebbe $b \in A$, $b \neq 0$ tale che

$$a \cdot b = 0. \tag{4}$$

Moltiplicando per a^{-1}, da (4) si avrebbe

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$$

ovvero, per l'associatività di $\cdot$,

$$b = (a^{-1} \cdot a) \cdot b = 0$$

che dà luogo a contraddizione.

Segue immediatamente il:

Corollario 3. *In un campo non ci sono divisori dello zero.*

Osservazione 23. L'anello $(\mathbb{Z}, +, \cdot)$ non ha divisori dello zero: per questo motivo si chiama *dominio di integrità*.

Osservazione 24. Si dimostra che in un anello *finito* ogni elemento non nullo è divisore dello zero oppure è unitario. Per esempio si è osservato (Proposizione 8) che in $\mathbb{Z}_n$, n non primo, sono unitari gli elementi primi con n e quindi gli elementi unitari sono in numero di $\varphi(n)$ (φ funzione di Eulero); i rimanenti $n - 1 - \varphi(n)$ elementi non nulli di $\mathbb{Z}_n$ sono quindi divisori dello zero.

I numeri interi

Teorema 1. *(divisione in $\mathbb{Z}$) Siano $a, b \in \mathbb{Z}$, $b \neq 0$. Allora esistono e sono unici $q, r \in \mathbb{Z}$ tali che*

(1) $a = bq + r$
(2) $0 \leq r < |b|$.

Si 1 dice che q è il **quoziente** ed r il **resto** della **divisione** di a per b. Inotre, si ha ovviamente:

$$r = 0 \iff b|a.$$

Proposizione 1. *Per ogni $a, b, c \in \mathbb{Z}$, $a \neq 0$ si ha:*

1. $a \mid b \Rightarrow (a \mid (-b) \wedge -a \mid b \wedge -a \mid (-b))$
2. $(a \mid b \wedge a \mid c) \Rightarrow a \mid (b \pm c)$
3. se $b \neq 0$ $(a \mid b \wedge b \mid c) \Rightarrow a \mid c$
4. se $b \neq 0$ $(a \mid b \wedge b \mid a) \Rightarrow b = \pm a$
5. $a \mid b \Rightarrow a \mid bc$.

Dimostrazione.

1. Siano $a, b \in \mathbb{Z}$ con $a \neq 0$ e $a|b$. Allora esiste $q \in \mathbb{Z}$ tale che $b = qa$. Quindi

(1) $$-b = (-q)a \Rightarrow a|(-b)$$

   Inoltre $-a = (-q)b$ e pertanto $-a|b$ da cui, usando (1), $-a|(-b)$.
2. Siano $a, b, c \in \mathbb{Z}$ con $a \neq 0$, $a|b$ e $a|c$. Allora esistono $p, q \in \mathbb{Z}$ tali che $b = pa$ e $c = qa$. Quindi $b \pm c = pa \pm qa = (p \pm q)a$ e pertanto $a|(b \pm c)$
3. Siano $a, b, c \in \mathbb{Z}$ con $a \neq 0$, $b \neq 0$, $a|b$ e $b|c$. Allora esistono $r, s \in \mathbb{Z}^*$ tali che $b = ra$ e $c = sb$. Segue che $c = sb = s(ra) = (sr)a$, da cui certamente $a \mid c$
4. Siano $a, b \in \mathbb{Z}^*$ con $a|b$ e $b|a$. Allora esistono $h, k \in \mathbb{Z}^*$ tali che $b = ha$ e $a = kb$. Segue che $b = ha = h(kb) = (hk)b$ e quindi h e k sono due interi il cui prodotto è 1 e pertanto $h = k = 1$ oppure $h = k = -1$, ovvero $b = \pm a$.
5. Siano Siano $a, b \in \mathbb{Z}$ con $a \neq 0$ e $a|b$. Allora esiste $q \in \mathbb{Z}$ tale che $b = qa$. Allora $bc = (qa)c = (qc)a$ e dunque $a|bc$.

Definizione 1. Siano $a, b \in \mathbb{Z}$, a, b non entrambi nulli. Si dice *massimo comun divisore* tra a e b un intero $d \in \mathbb{Z}$ tale che

- $d|a \wedge d|b$
- $\forall d' \in \mathbb{Z}$ tale che $d'|a \wedge d'|b$ si ha $d'|d$.

Osservazione 1. Dalla Proposizione 1 segue subito che se d è un massimo comun divisore tra a e b lo è anche tra $-a$ e b, tra a e $-b$, tra $-a$ e $-b$. Inoltre, nella Definizione 1 si richiede che almeno uno tra a e b sia non nullo: se per esempio $a = 0$, allora b è massimo comun divisore tra a e b. Infatti $b|b$, $b|0$ e se $d' \in \mathbb{Z}$ è tale che $d'|a$ e $d'|b$, allora $d'|b$.

Teorema 2. *Siano $a, b \in \mathbb{Z}^*$. Allora sicuramente esiste un massimo comun divisore d tra a e b. Inoltre esistono due numeri interi x_0 e y_0 tali che $d = ax_0 + by_0$ (identità di Bézout). Infine, l'unico altro massimo comun divisore è $-d$.*

Nella dimostrazione del Teorema 2 si usa l'algoritmo delle divisioni successive:

$$\begin{aligned}
a &= bq_1 + r_1 \quad & 0 \leq r_1 \leq |b| \\
b &= r_1q_2 + r_2 \quad & 0 \leq r_2 \leq r_1 \\
r_1 &= r_2q_3 + r_3 \quad & 0 \leq r_3 \leq r_2 \\
&\vdots & \\
r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1} \quad & 0 \leq r_{n-2} \leq r_{n-1} \\
r_{n-2} &= r_{n-1}q_n \quad & r_n = 0
\end{aligned}$$

Osservazione 2. Siano $a, b \in \mathbb{Z}$, a, b non entrambi nulli. Allora esiste un unico massimo comun divisore positivo tra a e b che si indica con $M.C.D.(a, b)$.

Definizione 2. Siano $a, b \in \mathbb{Z}^*$. Si dice *minimo comune multiplo* tra a e b un intero $m \in \mathbb{Z}$ tale che

- $a|m \quad \wedge \quad b|m$
- $\forall m' \in \mathbb{Z}$ tale che $a|m' \quad \wedge \quad b|m'$ si ha $m|m'$.

Teorema 3. *Siano $a, b \in \mathbb{Z}^*$. Se d è un massimo comun divisore tra a e b, allora $\frac{ab}{d}$ è un minimo comune multiplo tra a e b. Inoltre se m' è un altro minimo comune multiplo tra a e b, allora $m' = -m$.*

Osservazione 3. Nella stessa situazione del Teorema 2 esiste un unico esiste un unico minimo comune multiplo positivo tra a e b che si indica con $m.c.m.(a, b)$.

Osservazione 4. In virtù della Definizione 1, per ogni $a, b \in \mathbb{N}^*$, $M.C.D.(a, b)$ è l'estremo inferiore tra a e b rispetto alla relazione d'ordine " | "; d'altra parte, per la Definizione 2 $m.c.m.(a, b)$ è l'estremo superiore tra a e b rispetto alla relazione d'ordine " | ". Si può concludere che l'insieme ordinato $(\mathbb{N}^*, \ | \ )$ è un reticolo. Si osservi inoltre che per ogni $n \in \mathbb{N}$, $n \geq 2$, anche l'insieme ordinato $(D_n, \ | \ )$ è un reticolo, in quanto si prova che per ogni $a, b \in \mathbb{N}^*$, $M.C.D.(a, b) \in D_n$ e $m.c.m.(a, b) \in D_n$

Definizione 3. Si dice *equazione Diofantea* un'equazione in $\mathbb{Z}$ nelle incognite x, y della forma

$$ax + by = c \tag{2}$$

dove $a, b \in \mathbb{Z}$, a, b non entrambi nulli.

Teorema 4. *Siano $a, b, c \in \mathbb{Z}$, a, b non entrambi nulli, e sia $d = M.C.D.(a, b)$. Allora si ha:*

1. *l'equazione Diofantea (2) ha soluzioni se e soltanto se $d \mid c$*
2. *se (2) ha soluzioni, detta (x_0, y_0) una di esse, tutte le altre sono di tipo*

$$(x_0 + \bar{b}h, y_0 - \bar{a}h), \quad h \in \mathbb{Z},$$

dove $\bar{a} = \frac{a}{d}$, $\bar{b} = \frac{b}{d}$.

Dimostrazione. Per provare 1. si osservi preliminarmente che $\bar{a} = \frac{a}{d} \in \mathbb{Z}$, $\bar{b} = \frac{b}{d} \in \mathbb{Z}$, poichè d è un divisore di a e di b e si ha

$$a = \bar{a}d, \quad b = \bar{b}d. \tag{3}$$

Si suppone che (2) ammetta soluzioni: sia (x_0, y_0) una di esse. Sarà allora

$$ax_0 + by_0 = c.$$

In virtù di (3) $\bar{a}dx_0 + \bar{b}dy_0 = c$ da cui $d(\bar{a}x_0 + \bar{b}y_0) = c$ e pertanto esiste $h = \bar{a}x_0 + \bar{b}y_0 \in \mathbb{Z}$ tale che $c = dh$ e quindi $d \mid c$.
Viceversa, sia $d \mid c$: quindi esiste $\bar{c} \in \mathbb{Z}$ tale che $c = \bar{c}d$. Per l'identità di Bezout, esistono $x_1, y_1 \in \mathbb{Z}$ tali che

$$d = ax_1 + by_1. \tag{4}$$

Moltiplicando l'identità (4) per $\bar{c}$ si ha $\bar{c}d = \bar{c}ax_1 + \bar{c}by_1$, ovvero $c = (\bar{c}x_1)a + (\bar{c}y_1)b$ e dunque, posto $x_0 = \bar{c}x_1, y_0 = \bar{c}y_1$, risulta evidente che la coppia (x_0, y_0) è soluzione di (2).
Fissata una soluzione (x_0, y_0) di (2), si vuol provare che per ogni $h \in \mathbb{Z}(x_0 + \bar{b}h, y_0 - \bar{a}h)$ è ancora una soluzione di (2). Infatti si ha:

$$a(x_0 + \bar{b}h) + b(y_0 - \bar{a}h) = ax_0 + a\bar{b}h + by_0 - b\bar{a}h = ax_0 + by_0 + \bar{a}d\bar{b} - \bar{b}d\bar{a} = ax_0 + by_0 = c.$$

La dimostrazione del fatto le soluzioni di (2) sono tutte del tipo descritto in 2. viene omessa.

Principio d'induzione completa (1^a forma)

Siano $n_0 \in \mathbb{Z}$, $\mathbb{Z}(n_0) := \{x \in \mathbb{Z} \mid x \geq n_0\}$. Si supponga che $P(n)$ sia una proprietà che ha senso $\forall x \in X(n_0)$. Se sono soddisfatte le seguenti due condizioni:

(1) $P(n_0)$ è vera
(2) $(\forall n > n_0,\ P(n)$ vera$) \Longrightarrow P(n+1)$ vera

allora $P(x)$ è vera $\forall x \in \mathbb{Z}(n_0)$

Dimostrazione. Sia $X = \{x \in \mathbb{Z}(n_0) \ : \ P(n_0)$ è falsa$\}$. Si deve provare che $X = \emptyset$. Si suppone che sia $X \neq \emptyset$. In tal caso, per il buon ordinamento di $\mathbb{Z}$ esiste $x_0 = minX$ e quindi certamente $P(x_0)$ è falsa. $x_0 \neq n_0$, perchè $P(n_0)$ è vera, e quindi $n_0 < x_0$. Si osservi inoltre che $n_0 \leq x_0 - 1 \notin X$ (perchè $x_0 = minX$) e quindi $P(x_0 - 1)$ è vera. Allora, per (2), $P(x_0)$ è vera e ciò costituisce una contraddizione.

Principio d'induzione completa (2^a forma)

Si supponga che $P(n)$ sia una proprietà che ha senso $\forall x \in \mathbb{Z}(n_0)$. Se sono soddisfatte le seguenti due condizioni:

(1) $P(n_0)$ è vera
(2) $(\forall m \in \mathbb{Z}(n_0),\ n_0 \leq m < n,\ P(m)$ vera$) \Longrightarrow P(n)$ vera

allora $P(x)$ è vera $\forall x \in \mathbb{Z}(n_0)$.

Definizione 4. Sia $p \in \mathbb{Z}^*$, $p \neq \pm 1$. Si dice che p è *primo* se

$$(\forall a, b \in \mathbb{Z})\ (p \mid ab \Longrightarrow (p \mid a \ \vee \ p \mid b).$$

Definizione 5. Sia $p \in \mathbb{Z}^*$, $p \neq \pm 1$. Si dice che p è *irriducibile* se

$$(\forall a, b \in \mathbb{Z})\ (a \mid p \Longrightarrow (a = \pm 1 \vee \ a = \pm p).$$

Teorema 5. *Sia $p \in \mathbb{Z}^*$, $p \neq \pm 1$. Allora p è primo se e solo se p è irriducibile.* (dimostrato a lezione)

Proposizione 2. *Esistono infiniti numeri primi.*

Proof. Si supponga per assurdo che esistano soltanto h numeri primi $p_1, p_2, \ldots, p_h \in \mathbb{N}^*$. Allora $q = p_1 \cdot p_2 \cdot \ \ldots \ \cdot p_h$ non è un numero primo e non lo è neppure $q+1$, perché $q+1$ non può essere un divisore di q ed è pertanto diverso da ogni p_i, $i = 1, \ldots, h$. Quindi esiste $j = 1, \ldots, h$ tale che $p_j | (q+1)$. Però risulta anche $p_j | q$ e quindi $p_j | (q+1-q)$, ovvero $p_j | 1$, e quindi $p_j = 1$, il che non può succedere, poichè i numeri primi sono diversi da 1. □

Teorema 6. *(Teorema fondamentale dell'Aritmetica)*
Sia $n \in \mathbb{Z}^*$, $n \neq \pm 1$. Allora esistono s numeri primi $p_1, \ldots, p_s$ e s interi naturali $h_1, \ldots, h_s$ tali che

$$n = p_1^{h_1} \cdot \ \ldots \ \cdot p_s^{h_s}.$$

Questa decomposizione è essenzialmente unica, nel senso che se $q_1, \ldots, q_r$ sono numeri primi e $k_1, \ldots, k_r$ sono interi positivi tali che

$$n = q_1^{k_1} \ldots q_r^{k_r}$$

allora $s = r$ ed inoltre si può cambiare l'ordine dei fattori in modo che $q_1 = \pm p_1, \ldots, q_s = \pm p_s$, $h_1 = k_1, \ldots, h_s = k_s$.

Osservazione 5. Siano $n, m \in \mathbb{Z} - \{0, \pm 1\}$. Allora esistono $p_1, \ldots, p_s$ numeri primi, $h_1, \ldots, h_s$, $k_1, \ldots, k_s \in \mathbb{N}$ tali che

$$n = p_1^{h_1} \cdots p_s^{h_s}, \quad m = p_1^{k_1} \cdots p_s^{k_s};$$

cioè i due numeri possono essere fattorizzati usando gli stessi fattori primi, eventualmente elevati a potenza 0. Per esempio,

$$945 = 2^0 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^0 \cdot 17^0, \quad 3366 = 2 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11 \cdot 17.$$

Si può provare che

$$M.C.D.(n, m) = p_1^{min(h_1, k_1)} \cdots p_s^{min(h_s, k_s)},$$
$$m.c.m.(n, m) = p_1^{max(h_1, k_1)} \cdots p_s^{max(h_s, k_s)}.$$

Nel caso considerato:

$$M.C.D.(945, 3366) = 2^{min(0,1)} \cdot 3^{min(3,2)} \cdot 5^{min(1,0)} \cdot 7^{min(1,0)} \cdot 11^{min(0,1)} \cdot 17^{min(0,1)},$$

quindi $M.C.D.(945, 3366) = 3^2 = 18$. Inoltre

$$m.c.m.(945, 3366) = 2^{max(0,1)} \cdot 3^{max(3,2)} \cdot 5^{max(1,0)} \cdot 7^{max(1,0)} \cdot 11^{max(0,1)} \cdot 17^{max(0,1)},$$

per cui $m.c.m.(945, 3366) = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 = 353430$.

Definizione 1. Sia A insieme, naturalmente non vuoto, $\mathcal{R}$ relazione su A. Si dice che $\mathcal{R}$ è una *relazione di equivalenza* se è **riflessiva, simmetrica e transitiva**.

Esercizio 1. Sono di equivalenza le seguenti relazioni:

(1) $\mathcal{R}_5 = \{(\alpha,\alpha),(\beta,\beta),(\gamma,\gamma),(\alpha,\beta),(\beta,\alpha)\}$ su $A = \{\alpha,\beta,\gamma\}$
(2) $\mathcal{R}_6 = \{(n,m) \in \mathbb{Z}\times\mathbb{Z}\ ; 2|\ (n-m)\}$
(3) $\mathcal{R}_7 = \{(a,b) \in \mathbb{Z}\times\mathbb{Z}\ ;\ a^2 = b^2\}$
(4) $\mathcal{R}_8 = \{(x,y) \in \mathbb{Z}^*\times\mathbb{Z}^*\ ;\ x\cdot y > 0\}$.

Esercizio 2. Siano A un insieme non vuoto, $f : A \to B$ un'applicazione. La relazione $\mathcal{R}_f$ così definita:

$$\forall x, y \in A\ \ (x,y) \in \mathcal{R}_f \Leftrightarrow\ f(x) = f(y)$$

è una relazione di equivalenza.

Definizione 2. Siano A un insieme, $\mathcal{A} = \{A_i; i \in I\}$ un sottoinsieme dell'insieme $\mathscr{P}(A)$ delle parti di A. Si dice unione degli degli elementi di $\mathcal{A}$ o unione degli A_i, $i \in I$, l'insieme

$$\bigcup_{i\in I} A_i := \{a \in A; \exists i \in I \text{ tale che } a \in A_i\}$$

Osservazione 1. Ovviamente si ha

$$\bigcup_{i\in I} A_i \subseteq A.$$

Definizione 3. Siano A un insieme, $\mathcal{R}$ una relazione di equivalenza su A, $a \in A$. Si dice *classe di equivalenza di* a il sottoinsieme di A:

$$[a]_{\mathcal{R}} = \{x \in A; (a,x) \in \mathcal{R}\}.$$

Esempio 1. Considerata sull'insieme $A = \{a,b,c,d\}$ la relazione di equivalenza

$$\mathcal{R} = \{(a,a)(b,b),(c,c)(d,d),(a,b)(b,a),(a,c),(c,a),(b,c),(c,b)\}$$

si ha: $[a]_{\mathcal{R}} = [b]_{\mathcal{R}} = [c]_{\mathcal{R}} = \{a,b,c\}$; $[d]_{\mathcal{R}} = \{d\}$.

Esempio 2. Sia Σ l'insieme delle rette di un piano fissato e $\mathcal{E}$ la relazione su Σ così definita: per ogni $r, s \in \Sigma$, $(r,s) \in \mathcal{E} \Leftrightarrow r$ e s sono parallele. Sapendo che ogni retta è parallela a sè stessa, si si vede subito che $\mathcal{E}$ è una relazione di equivalenza. Inoltre fissata una retta r, la sua classe di equivalenza è

$$[r]_{\mathcal{E}} = \text{insieme di tutte le rette parallele ad r.}$$

Esempio 3. Nella stessa situazione dell'Esempio 2, la perpendicolarità tra rette non è una relazione di equivalenza: infatti non è riflessiva ne' transitiva.

Proposizione 1. *Siano A un insieme, $\mathcal{R}$ una relazione di equivalenza su A. Allora si ha:*

(1) $(\forall a \in A)\ ([a]_{\mathcal{R}} \neq \emptyset)$
(2) $(\forall a,b \in A)\ ((a,b) \notin \mathcal{R}\ \iff\ [a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} = \emptyset)$
(3) $(\forall a,b \in A)\ ((a,b) \in \mathcal{R}\ \iff\ [a]_{\mathcal{R}} = [b]_{\mathcal{R}})$
(4) $\bigcup_{a\in A}[a]_{\mathcal{R}} = A$.

Dimostrazione. (1) discende subito dalla riflessività: infatti

$$\forall a \in A,\ \ (a,a) \in \mathcal{R}\ \iff a \in [a]_{\mathcal{R}}$$

Per provare (2) si considerino $a, b \in A$ in modo che $(a,b) \notin \mathcal{R}$. Usando la tecnica di dimostrazione per assurdo, si suppone che esista $c \in [a]_{\mathcal{R}} \cap [b]_{\mathcal{R}}$. Allora, per la definizione di classe di equivalenza, risulterebbe: $(a,c) \in \mathcal{R}\ \wedge\ (b,c) \in \mathcal{R}$ e quindi, per la simmetria di $\mathcal{R}$ $(a,c) \in \mathcal{R} \wedge (c,b) \in \mathcal{R}$ da cui, per la transitività di $\mathcal{R}$, $(a,b) \in \mathcal{R}$, in contraddizione con $(a,b) \notin \mathcal{R}$.

Viceversa, se $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} = \emptyset$, non può essere $(a,b) \in \mathcal{R}$, altrimenti $a \in [a]_{\mathcal{R}} \cap [b]_{\mathcal{R}}$ (si osservi che si è usata la tecnica di dimostrazione per contrapposizione).
Per dimostrare (3), si considerino $a, b \in A$, con $(a,b) \in \mathcal{R}$. Poichè si deve provare che i due insiemi $[a]_{\mathcal{R}}$ e $[b]_{\mathcal{R}}$ coincidono, si dimostrano le due inclusioni:

$$[a]_{\mathcal{R}} \subseteq [b]_{\mathcal{R}} \ \wedge \ [b]_{\mathcal{R}} \subseteq [a]_{\mathcal{R}}.$$

Sia $x \in [a]_{\mathcal{R}}$; questo vuol dire che $(a,x) \in \mathcal{R}$. Però anche $(a,b) \in \mathcal{R}$ e quindi, per la simmetria, $(b,a) \in \mathcal{R}$. Per la transitività di $\mathcal{R}$, $(b,x) \in \mathcal{R}$ e ciò significa che $x \in [b]_{\mathcal{R}}$, pertanto $[a]_{\mathcal{R}} \subseteq [b]_{\mathcal{R}}$. L'inclusione $[b]_{\mathcal{R}} \subseteq [a]_{\mathcal{R}}$ si prova nella stessa maniera.
Viceversa, se $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$, allora $a \in [a]_{\mathcal{R}} = [b]_{\mathcal{R}}$ e quindi $(a,b) \in \mathcal{R}$.
Infine per l'Osservazione 1, si ha $\bigcup_{a\in A}[a]_{\mathcal{R}} \subseteq A$. Per provare l'altra inclusione, si fissi $x \in A$; per (1), $x \in [x]_{\mathcal{R}}$ e quindi $x \in \bigcup_{a\in A}[a]_{\mathcal{R}}$. Pertanto le due inclusioni sono verificate e quindi vale (4).

Definizione 4. Siano A un insieme, $\mathcal{R}$ una relazione di equivalenza su A. L'insieme

$$A/\mathcal{R} = \{[a]_{\mathcal{R}}; a \in A\}$$

si chiama *insieme quoziente di A per $\mathcal{R}$.*

Definizione 5. Siano A un insieme, $\mathcal{A} = \{A_i; i \in I\}$ un sottoinsieme (non vuoto) dell'insieme $\mathscr{P}(A)$ delle parti di A. Si dice che $\mathcal{A}$ è una *partizione* se

- $\forall i \in I, \ A_i \neq \emptyset$
- $\forall i, j \in I, \ i \neq j, \ A_j \cap A_j = \emptyset$
- $\bigcup_{i\in I} A_i = A$.

Osservazione 2. Sia A un insieme, $\mathcal{R}$ una relazione di equivalenza su A. Per la Proposizione 1, sicuramente l'insieme quoziente di A rispetto ad una relazione di equivalenza $\mathcal{R}$ è una partizione. Si può verificare anche il viceversa: sia $\mathcal{A} = \{A_i; i \in I\}$ una partizione sull'insieme A. Si definisce la relazione $\mathcal{R}$ nel modo che segue:

$$(a,b) \in \mathcal{R} \iff \exists i \in I \text{ tale che } a, b \in A_i.$$

Si prova che $\mathcal{R}$ è di equivalenza e che $A/\mathcal{R} = \mathcal{A}$.

Esercizio 3. È assegnata su $\mathbb{Z}$ la relazione

$$\mathcal{R} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \ ; \ 5 \mid (4x+y)\}.$$

(1) Verificare che $\mathcal{R}$ è di equivalenza
(2) determinare la classe di equivalenza di 2.

SOLUZIONE

1.(a) Si ricorda che se a, b, n sono numeri interi, $n \neq 0$ allora vale la proprietà:

$$\big(n \mid a \ \wedge \ n \mid b\big) \ \Rightarrow \ n \mid (a \pm \ b).$$

- Poichè per ogni $x \in \mathbb{Z}$, $5 \mid (4x+x)$, certamente $(x,x) \in \mathcal{R}$ e quindi la relazione è <u>riflessiva</u>.
- Sia $(x,y) \in \mathcal{R}$, ovvero $5 \mid (4x+y)$. Allora, poichè $5 \mid (5x+5y)$ si ha

  $$5 \mid (4x+y-(5x+5y)) \ \Rightarrow \ 5 \mid (-x-4y) \ \Rightarrow \ 5 \mid (4y+x).$$

  Pertanto $(y,x) \in \mathcal{R}$, cioè $\mathcal{R}$ è <u>simmetrica</u>.
- Siano $(x,y) \in \mathcal{R}$ e $(y,z) \in \mathcal{R}$. Quindi

  $$\big(5 \mid (4x+y) \wedge 5 \mid (4y+z)\big) \ \Rightarrow \ 5 \mid (4x+y+4y+z)$$

  $$\Rightarrow \ 5 \mid (4x+5y+z) \ \Rightarrow \ 5 \mid \big((4x+5y+z)-5y\big) \ \Rightarrow \ 5 \mid (4x+z),$$

  ovvero $(x,z) \in \mathcal{R}$. Si è pertanto provato che $\mathcal{R}$ <u>transitiva</u> e quindi la relazione è di equivalenza.

1.(b) $x \in [2] \Leftrightarrow (2,x) \in \mathcal{R} \Leftrightarrow 5 \mid (8+x) \Leftrightarrow (\exists h \in \mathbb{Z} \text{ tale che } x = -8+5h)$
$\Leftrightarrow (\exists k \in \mathbb{Z} \text{ tale che } x = 2+5k)$. Quindi

$$[2] = \{2+5k \ ; \ k \in \mathbb{Z}\}.$$

Definizione 1. Siano A e B insiemi. Si definisce *prodotto cartesiano* l'insieme:

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

Osservazione 1. Si osservi che nella Definizione 1. le coppie sono **ordinate**, vale a dire la coppia $(x, y) \neq (y, x)$ se $x \neq y$. È quindi chiaro che $A \times B \neq B \times A$, se $A \neq B$. Risulta inoltre: $A \times \emptyset = \emptyset \times A = \emptyset$.

Da ora in poi, in questo capitolo, si supporrà di considerare insiemi non vuoti, a meno di esplicito avviso contrario.

Definizione 2. Siano A e B insiemi. Si dice *relazione tra gli A elementi di A e gli elementi di B* un qualunque sottoinsieme del prodotto cartesiano $A \times B$. Se $A = B$, si parla semplicemente di *relazione tra gli elementi di A*; quindi, in questo caso, $\mathcal{R} \subset A \times A$.

Esempio 1. L'insieme

$$\mathcal{R} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \ ; \ y = -x\}$$

è una relazione tra gli elementi di $\mathbb{N}$ e $\mathbb{Z}$. Si ha

$$\mathcal{R} = \{(0, 0), (1, -1), (2, -2), (3, -3), \dots\}.$$

Esempio 2. L'insieme

$$\mathcal{R}' = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \ ; \ y = -x\}$$

è una relazione tra gli elementi di $\mathbb{Z}$. Risulta

$$\mathcal{R}' = \{\dots, (-2, 2), (-1, 1), (0, 0), (1, -1), (2, -2), \dots\}.$$

Definizione 3. Siano A un insieme non vuoto, $\mathcal{R}$ una relazione tra gli elementi di A. Si dice che $\mathcal{R}$ è *riflessiva* se è verificata la sequente condizione:

$$(\forall a \in A) \ ((a, a) \in \mathcal{R}).$$

Osservazione 2. Ovviamente, perchè $\mathcal{R}$ non sia riflessiva basta che esista un solo elemento $x \in A$ tale che $(x, x) \notin A$.

Esempio 3. Non ha senso chiedersi se la relazione $\mathcal{R}$ dell'Esempio 1 sia riflessiva, visto che si tratta di una relazione tra elementi di due insiemi diversi.

Esempio 4. Delle relazioni sull'insieme $A = \{\alpha, \beta, \gamma\}$

$$\mathcal{R}_1 = \{(\alpha, \alpha), (\beta, \beta), (\gamma, \gamma), (\alpha, \beta), (\alpha, \gamma)\}$$
$$\mathcal{R}_2 = \{(\alpha, \alpha), (\beta, \beta), (\alpha, \beta), (\beta, \gamma)\}$$
$$\mathcal{R}_3 = \{(\alpha, \beta), (\beta, \alpha), (\gamma, \beta), (\beta, \gamma), (\gamma, \gamma)\}$$
$$\mathcal{R}_4 = \{(\alpha, \beta), (\beta, \alpha), (\alpha, \gamma)\}$$
$$\mathcal{R}_5 = \{(\alpha, \alpha), (\beta, \beta), (\gamma, \gamma), (\alpha, \beta), (\beta, \alpha)\}$$

sono riflessive $\mathcal{R}_1$ e $\mathcal{R}_5$ mentre $\mathcal{R}_2$, $\mathcal{R}_3$ e $\mathcal{R}_4$ non sono riflessive.

Definizione 4. Siano A un insieme non vuoto, $\mathcal{R}$ una relazione tra gli elementi di A. Si dice che $\mathcal{R}$ è *simmetrica* se è verificata la sequente condizione:

$$(\forall a, b \in A) \ ((a, b) \in \mathcal{R} \ \Rightarrow \ (b, a) \in \mathcal{R}).$$

Osservazione 3. Naturalmente è sufficiente che esista una sola coppia $(x, y) \in \mathcal{R}$, con $x \neq y$, tale che $(y, x) \notin \mathcal{R}$, perchè $\mathcal{R}$ non sia simmetrica.

Definizione 5. Si dice che $\mathcal{R}$ è *antisimmetrica* se è verificata la sequente condizione:

$$(\forall a, b \in A) \ \big(\ ((a, b) \in \mathcal{R} \ \wedge (b, a) \in \mathcal{R}) \ \Rightarrow \ a = b \big).$$

Osservazione 4. La condizione di antisimmetria può essere riscritta nel modo che segue:

$$\forall a, b \in A, a \neq b \ \ \big((a, b) \in \mathcal{R}\big) \Rightarrow (b, a) \notin \mathcal{R}.$$

Esempio 5. $\mathcal{R}_1$ e $\mathcal{R}_2$ sono antisimmetriche, $\mathcal{R}_3$ e $\mathcal{R}_5$ sono simmetriche, $\mathcal{R}_4$ non è simmetrica ne' antisimmetrica.

Definizione 6. Siano A un insieme non vuoto, $\mathcal{R}$ una relazione tra gli elementi di A. Si dice che $\mathcal{R}$ è *transitiva* se è verificata la sequente condizione:

$$(\forall a, b, c \in A) \ \big(\ ((a,b) \in \mathcal{R} \ \wedge (b,c) \in \mathcal{R}) \ \Rightarrow \ (a,c) \in \mathcal{R} \ \big).$$

Osservazione 5. Anche in questo caso è sufficiente che esistano $(x,y),\ (y,z) \in \mathcal{R}$ tali che $(x,z) \notin \mathcal{R}$ perchè $\mathcal{R}$ non sia transitiva.

Esempio 6. $\mathcal{R}_1$ e $\mathcal{R}_5$ sono transitive, $\mathcal{R}_2$, $\mathcal{R}_3$ e $\mathcal{R}_4$ non lo sono.

Esempio 7. La relazione $\mathcal{R}'$ dell'Esempio 2 non è riflessiva perchè, per esempio, $(1,1) \notin \mathcal{R}$, è simmetrica, perchè

$$(x,y) \in \mathcal{R}' \Rightarrow y = -x \Rightarrow x = -y \Rightarrow (x,y) \in \mathcal{R}'$$

$\mathcal{R}'$ e non è transitiva: $((1,-1) \in \mathcal{R} \wedge (-1,1) \in \mathcal{R})$ ma $(1,1) \notin \mathcal{R}$

Osservazione 6. Si osservi che spesso si usa la notazione $a\mathcal{R}b$ in luogo di $(a,b) \in \mathcal{R}$.

Definizione 7. Si dice che $\mathcal{R}$ è *una relazione d'ordine* se è **riflessiva, antisimmetrica e transitiva**. La coppia ordinata $(A, \mathcal{R})$ (ovvero l'insieme A munito della relazione d'ordine) si chiama insieme ordinato.

Esempio 8. La relazione

$$\mathcal{R}_1 = \{(\alpha,\alpha), (\beta,\beta), (\gamma,\gamma), (\alpha,\beta), (\alpha,\gamma)\}$$

è d'ordine.

Esempio 9. Sia X un insieme. Allora la relazione " $\subset$ " è una relazione d'ordine su $\mathscr{P}(X)$. Infatti si è osservato in precedenza che per ogni A, B, C sottoinsiemi di X

(1) $A \subset A$
(2) se $A \subset B$ e $B \subset A$ allora $A = B$
(3) se $A \subset B$ e $B \subset C$ allora $A \subset C$.

Esempio 10. L'ordinamento naturale " $\leq$ " sull'insieme $\mathbb{Z}$ dei numeri relativi è la relazione definita come segue:
$\forall m, n \in \mathbb{Z}$, si dice che $m \leq n$ se e solo se $\exists h \in \mathbb{N}$ tale che $n = m + h$.
Si verifica che " $\leq$ " è una relazione d'ordine su $\mathbb{Z}$.

- riflessività:
  se $n \in \mathbb{Z}$, allora $\exists\ 0 \in \mathbb{N}$ tale che $n = n + 0$ e pertanto $n \leq n$
- antisimmetria:
  siano $n, m \in \mathbb{Z}$, in modo che $n \leq m \wedge m \leq n$. Si ha:

$$(n \leq m \wedge m \leq n) \Rightarrow (\exists h \in \mathbb{N} \text{ tale che } n = m + h) \wedge (\exists k \in \mathbb{N} \text{ tale che } n = m + k)$$

$$\Rightarrow n = m + h = n + k + h \Rightarrow h + k = 0 \Rightarrow h = k = 0 \Rightarrow n = m.$$

- transitività:
  siano $n, m, p \in \mathbb{Z}$, in modo che $m \leq n \wedge n \leq p$. Allora:

$$(m \leq n \wedge n \leq p) \Rightarrow (\exists h \in \mathbb{N} \text{ tale che } m = m + h) \wedge (\exists k \in \mathbb{N} \text{ tale che } p = n + k)$$

$$\Rightarrow p = n + k = m + h + k \Rightarrow \exists h + k \in \mathbb{N} \text{ tale che } p = m + (h + k) \Rightarrow m \leq p.$$

Esempio 11. Si può considerare su $\mathbb{Z}$ la seguente relazione: $\forall m, n \in \mathbb{Z}$, si pone $m < n$ se e solo se $\exists\ h \in \mathbb{N}^*$ tale che $n = m + h$. Questa relazione non è d'ordine in quanto non riflessiva. Si osservi che

$$m < n \Leftrightarrow (m \leq n \ \wedge \ m \neq n).$$

Definizione 8. Siano $a, b \in \mathbb{Z}$, $a \neq 0$. Si dice che a *divide* b o che *è un divisore di* b o anche che b *moltiplica* a o b *è un multiplo di* a e si scrive $a \mid b$ se esiste $h \in \mathbb{Z}$ tale che $b = ha$. Quindi

$$a \mid b \;\Leftrightarrow\; \exists h \in \mathbb{Z} \text{ tale che } b = ha$$

Esercizio 1. La relazione " $\mid$ " sull'insieme $\mathbb{N}^* := \mathbb{N} \setminus \{0\}$ dei numeri naturali non nulli è una relazione d'ordine. Si tratta di provare che la relazione definita $\forall m, n \in \mathbb{N}^*$ da

$$m \mid n \Longleftrightarrow\; \exists h \in \mathbb{N}^* \text{ tale che } n = hm$$

è riflessiva, antisimmetrica e transitiva. La verifica è del tutto analoga a quella dell'Esempio 10.

Osservazione 7. Sia $(A, \leq)$ un insieme ordinato, $B \subset A$. Allora si può considerare la relazione $\leq_B$ tra gli elementi di B definita come segue:

$$(\forall x, y \in B)\ \big(\ x \leq_B y \;\Leftrightarrow\; x \leq y\ \big).$$

Si verifica facilmente che $\leq_B$ è una relazione d'ordine su B che si dice *relazione d'ordine indotta* da A su B. Per non appesantire la notazione, la relazione d'ordine indotta su B si denota con lo stesso simbolo "$\leq$".

Esempio 12. Per ogni $n \in \mathbb{N}^*$ si indica con $\mathcal{D}_n$ l'insieme dei divisori di n. Di particolare interesse è la relazione d'ordine " $\mid$ " indotta sull'insieme $\mathcal{D}_n$.
Se in particolare $n = 30$, $\mathcal{D}_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ e per ogni $x \in \mathcal{D}_{30}$ risulta

$$1 \mid x, \quad x \mid x, \quad x \mid 30$$

e inoltre

$$2 \mid 6, \;\; 2 \mid 10, \;\; 3 \mid 6, \;\; 3 \mid 15, \;\; 5 \mid 10, \;\; 5 \mid 15.$$

Definizione 9. Sia $(A, \leq)$ un insieme ordinato, X un sottoinsieme di A, $x_0 \in X$. Si dice che x_0 *è minimo di* X se:

$$(\forall x \in X)\ (x_0 \leq x).$$

Si dice che x_0 *è massimo di* X se

$$(\forall x \in X)\ (x \leq x_0).$$

Se $X = A$, si parla di minimo o di massimo di A.

Proposizione 1. *Sia $(A, \leq)$ un insieme ordinato, X un sottoinsieme di A. Se esiste un massimo (o un minimo) di X, esso è unico.*

Dimostrazione. Siano, infatti, x_0 e x_1 due massimi di X. Allora, poichè x_0 è massimo e $x_1 \in X$, si ha $x_1 \leq x_0$ e, scambiando i ruoli di x_0 e x_1, si ha $x_0 \leq x_1$. Per la proprietà antisimmetrica delle relazioni d'ordine deve essere $x_0 = x_1$. (Analoga la dimostrazione dell'unicità del minimo.)

Sia $(A, \leq)$ un insieme ordinato, X un sottoinsieme di A, $x_0 \in X$. Grazie alla Proposizione 1, è possibile utilizzare un simbolo specifico per il minimo (che si dice anche *il più piccolo elemento*) di X, e per il massimo (che si dice anche *il più grande elemento*) di X, quando esistono. Essi sono rispettivamenete

$$min(X) \;\text{ e }\; max(X).$$

Esempio 13.

1. Sia $(A, \mathcal{R}_1)$ l'insieme ordinato dell'esempio 4. È evidente che $\alpha = min(A)$ ma non esiste il massimo di A.
2. se si considera l'insieme $(\mathbb{N}, \leq)$, dove "$\leq$" è l'ordinamento naturale di $\mathbb{N}$, risulta $0 = min(\mathbb{N})$, ma non esiste il massimo
3. nell'insieme ordinato $(\mathbb{N}^*, \mid)$ dell'esempio 1, si ha $1 = min(\mathbb{N}^*)$, ma non esiste il massimo di $\mathbb{N}^*$

4. considerando il sottoinsieme $X = \{2, 3, 9, 18\}$ come sottoinsieme dell'insieme ordinato $(\mathbb{N}^*, \mid)$, esiste $max(X) = 18$ ma non esiste il minimo di X
5. nell'insieme ordinato $(D_n, \mid)$ dell'Esempio 12, si ha $min(D_n) = 1, max(D_n) = n$.

Definizione 10. Sia $(A, \leq)$ un insieme ordinato, $X \subset A$. Un elemento $y \in A$ si dice *minorante* di X se

$$(\forall x \in X)(y \leq x).$$

Se X è dotato di minoranti si dice *minorato* o *limitato inferiormente*.

Definizione 11. Sia $(A, \leq)$ un insieme ordinato, $X \subset A$. Un elemento $y \in A$ si dice *maggiorante* di X se

$$(\forall x \in X)(x \leq y).$$

Se X è dotato di maggioranti si dice *maggiorato* o *limitato superiormente*.

Osservazione 8. Sia $(A, \leq)$ un insieme ordinato, $X \subset A$. Si osservi che se X ha minimo (rispettivamente un massimo), esso è sicuramente un minorante (rispettivamente maggiorante), ma in generale un minorante (rispettivamente maggiorante) non è un minimo (rispettivamente un massimo) perchè non appartiene a X.

Definizione 12. Sia $(A, \leq)$ un insieme ordinato, X un sottoinsieme di A, limitato inferiormente, $\alpha \in A$. Si dice che α è *estremo inferiore di* X se è il più grande dei minoranti.

In altri termini α è estremo inferiore di se verifica le seguenti condizioni:

(1) $(\forall x \in X)\ (\alpha \leq x)$
(2) $\forall\ \beta \in A$ tale che $(\forall x \in X)\ (\beta \leq x)$ si ha $\beta \leq \alpha$.

Si vede subito che se esiste un estremo inferiore, esso è unico, per cui è lecito scrivere $\alpha = inf(X)$.

Definizione 13. Sia $(A, \leq)$ un insieme ordinato, X un sottoinsieme di A, limitato superiormente, $\alpha \in A$. Si dice che α è *estremo superiore* di X se è il più piccolo dei maggioranti.

In altre parole α è estremo superiore verifica le seguenti condizioni:

(1) $(\forall x \in X)\ (x \leq \alpha)$
(2) $\forall\ \beta \in A$ tale che $(\forall x \in X)\ (x \leq \beta)$ si ha $\alpha \leq \beta$.

Si vede subito che se esiste un estremo superiore di X, esso è unico, per cui è lecito scrivere $\alpha = sup(X)$.

Osservazione 9. Sia $(A, \leq)$ un insieme ordinato, $X \subset A$. Se X ammette minimo esso è anche estremo inferiore di X. Non vale il viceversa: ovvero se X ammette estremo inferiore, non è detto che questo sia il minimo di X. Ciò accade soltanto nel caso in cui l'estremo inferiore appartenga a X. Naturalmente lo stesso discorso vale per l'eventuale massimo o estremo inferiore di X.

Osservazione 10. Sia $(A, \leq)$ un insieme ordinato. Nel caso $X = \{x, y\} \subset A$, $\alpha = sup(x, y)$ vuol dire

(1) $x \leq \alpha,\ y \leq \alpha$
(2) $\forall\ \beta \in A$ tale che $x \leq \beta,\ y \leq \beta$ si ha $\alpha \leq \beta$.

Analogamente $\alpha = inf(x, y)$ si scrive

(1) $\alpha \leq x,\ \alpha \leq y$
(2) $\forall\ \beta \in A$ tale che $\beta \leq x,\ \beta \leq y$ si ha $\beta \leq \alpha$.

Esercizio 2. Esplicitando la definizione di estremo superiore e inferiore per una coppia sottoinsiemi di un insieme X nell'insieme ordinato in $(\mathscr{P}(X), \subset)$ cosa si ottiene ?

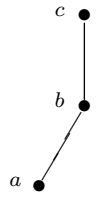
Definizione 14. Sia $(A, \leq)$ un insieme ordinato. Si dice che "$\leq$ " è una *relazione di ordine totale* ovvero che $(A, \leq)$ è *totalmente ordinato* se e soltanto se

$$(\forall x, y \in A)\ (x \leq y \vee y \leq x).$$

Nel caso contrario, cioè se $\exists x, y$ tali che $x \not\leq y \wedge y \not\leq x$, si dice che "$\leq$ " è una *relazione di ordine parziale* oppure che $(A, \leq)$ è *parzialmente ordinato*.

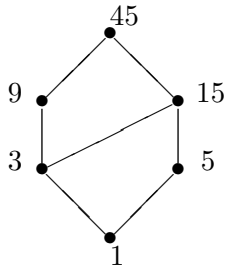
Esempio 14. Sono totalmente ordinati $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$; sono parzialmente ordinati $(\mathbb{N}^*, \mid)$, $(D_n, \mid)$, $(\mathscr{P}(A), \subset)$, $(A, \mathcal{R}_1)$.

Un insieme $(A, \leq)$ ordinato finito può essere rappresentato mediante un *diagramma di Hasse*: se $a, b \in A$, $a \leq b$ e se non ci sono elementi intermedi basta collegare a con b mediante un segmento ascendente. Siano ora $a, b, c \in A$, con $a \leq b$ e $b \leq c$. Poichè vale la proprietà transitiva, a viene collegato con b mediante un segmento ascendente, b viene collegato con c mediante un altro segmento ascendente, e a sarà collegato con c mediante una spezzata ascendente.

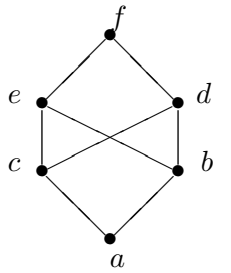


Quindi, guardando semplicemente il diagramma si può stabilire se due elementi x e y si possono paragonare.

Esempio 15. Per esempio il diagramma di Hasse dei divisori di 45 ordinato per divisibilità $(D_{45}, \mid)$ è:



Esercizio 3. Si consideri l'insieme $X = \{a, b, c, d, e, f\}$ sul quale sia assegnata la relazione d'ordine "$\leq$" rappresentata dal seguente diagramma di Hasse:



(1) Descrivere la relazione d'ordine "$\leq$"
(2) determinare l'insieme dei minoranti di $A = \{e, d\}, B = \{e, d, b\}$
(3) determinare l'insieme dei maggioranti di $C = \{c, b\}, D = \{c, b, d\}$

(4) determinare gli eventuali estremi inferiori di A, B, X
(5) determinare gli eventuali estremi superiori di C, D, X
(6) determinare gli eventuali massimi e minimi di A, B, C, D, X.

Soluzione

(1) Poichè si è specificato che "$\leq$" è una relazione d'ordine, la riflessività è scontata. Si deduce dal diagramma che:

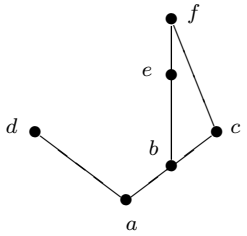
$$\forall x \in X \ a \leq x, \quad x \leq f;$$

inoltre

$$c \leq e, \ c \leq d, \ b \leq e, \ b \leq d.$$

(2) L'insieme dei minoranti di A è $\{c, b, a\}$, quello di B è $\{a\}$.
(3) L'insieme dei maggioranti di C è $\{e, d, f\}$, quello di D è $\{f\}$.
(4) Poichè b e c non sono paragonabili, non esiste l'estremo inferiore di A, ma esiste l'estremo inferiore di B, che ne è l'unico minorante: a. X ha estremo inferiore a.
(5) Poichè e e d non sono paragonabili, non esiste l'estremo superiore di C, ma esiste l'estremo superiore di D, che ne è l'unico maggiorante: f. X ha estremo superiore f.
(6) X ha minimo e massimo: rispettivamente a e f. A, B, C, D non hanno ne' minimo ne' massimo.

Esercizio 4. Si consideri l'insieme $X = \{a, b, c, d, e, f\}$ sul quale sia assegnata la relazione d'ordine "$\leq$" rappresentata dal seguente diagramma di Hasse:



(1) Descrivere la relazione d'ordine "$\leq$"
(2) determinare l'insieme dei minoranti e dei maggioranti di $A = \{e, d, b\}$
(3) determinare l'insieme dei minoranti e dei maggioranti di $B = \{c, e\}$
(4) determinare gli eventuali estremi inferiori e superiori di A, B, X
(5) determinare gli eventuali massimi e minimi di A, B, X.

Definizione 15. Un insieme ordinato $(R, \leq)$ si dice *reticolo ordinato* se ogni coppia di elementi di R ammette estremo superiore ed estremo inferiore. In altri termini

$$\forall x, y \in R \ \ \exists \sup(x, y), \quad \exists \inf(x, y).$$

Esempio 16.

1. Sia X un insieme. Allora l'insieme $\mathscr{P}(X)$ delle parti di X, ordinato per inclusione, ovvero $(\mathscr{P}(X), \subset)$, è un reticolo ordinato in quanto
$$\forall A, B \in \mathscr{P}(X) \quad \inf(A, B) = A \cap B, \quad \sup(A, B) = A \cup B.$$
2. L'insieme ordinato $(D_{45}, \ | \ )$ dell'esempio 15 è un reticolo, come si può facilmente verificare. Questo fa parte della più ampia classe di esempi $(\mathcal{D}_n, \ | \ )$ che verrà esaminata più a fondo.
3. L'insieme ordinato $(X, \leq)$ dell'Esercizio 3 non è un reticolo, perchè la coppia (e, d) non ammette estremo inferiore.

Esercizio 5. Verificare che l'insieme ordinato dell'esercizio 4 non è un reticolo.

Proposizione 1. *Sia $n \in \mathbb{N} - \{0,1\}$. La relazione $\mathcal{R}_n = \{(a,b) \in \mathbb{Z} \times Z : n \mid a-b\}$ è una relazione di equivalenza su $\mathbb{Z}$.*

La dimostrazione viene lasciata per esercizio.

Definizione 1. La relazione di equivalenza $\mathcal{R}_n$ si dice *congruenza modulo n*.

Notazione Per ogni $a, b \in \mathbb{Z}$, invece che $(a,b) \in \mathcal{R}_n$ si scrive

$$a \equiv b \ (\mathtt{mod} n)$$

e si legge "a congruo b modulo n".

Teorema 1. L'insieme quoziente di $\mathbb{Z}$ per $\mathcal{R}_n$ ha esattamente n elementi, cioè:

$$\mathbb{Z}/\mathcal{R}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\},$$

dove $[x]_n$ indica la classe di equivalenza di $x \in \mathbb{Z}$.

Dimostrazione. Si dimostra prima che le classi di equivalenza $[0]_n, [1]_n, \ldots, [n-1]_n$ sono distinte fra loro. Siano $a, b \in \mathbb{N}$, con $a \neq b$, $0 \leq a \leq n-1$, $0 \leq b \leq n-1$, e si può supporre che sia $a < b$. Se fosse $[a]_n = [b]_n$ allora sarebbe $b \equiv a \ (\mathtt{mod} n)$ cioè $n \mid b-a$. Però $b - a \leq n-1$ e quindi n potrebbe essere un divisore di $b-a$ solo se $b-a = 0$, il che contraddice l'ipotesi $a \neq b$.
Resta da provare che non ci sono classi di equivalenza diverse da $[0]_n, [1]_n, \ldots, [n-1]_n$ in $\mathbb{Z}/\mathcal{R}_n$. A tale scopo, sia $m \in \mathbb{Z}$. Per il teorema sulla divisione, esistono $q, r \in \mathbb{Z}$, con $0 \leq r < n$ tali che $m = nq + r$. Allora $m - r = nq$, per cui $n \mid m - r$, ovvero $m \equiv r \ (\mathtt{mod} n)$ e quindi $[m]_n = [r]_n$. Segue che:

$$\forall [m]_n \in \mathbb{Z}/\mathcal{R}_n \ \exists r \in \mathbb{N}, \text{ con } 0 \leq r \leq n-1 \text{ tale che } [m]_n = [r]_n$$

e ciò conclude la dimostrazione.

Definizione 2. L'insieme quoziente di $\mathbb{Z}$ per $\mathcal{R}_n$ si chiama *insieme dei resti modulo n* e si indica con il simbolo $\mathbb{Z}_n$.

Definizione 3. Siano $a, b \in \mathbb{Z}$, $a \neq 0$, $n \in \mathbb{N} - \{0,1\}$. Si dice *congruenza lineare* l'espressione

$$ax \equiv b \ (\mathtt{mod}\ n). \tag{1}$$

Si dice soluzione di (1) ogni intero x_0 tale che $ax_0 \equiv b \ (\mathtt{mod}\ n)$.

Teorema 2. *Siano $a, b \in \mathbb{Z}$, $a \neq 0$, $n \in \mathbb{N} - \{0,1\}$ e sia $d = M.C.D.(a,n)$. Allora*

1. *la congruenza lineare (1) ammette soluzioni se e solo se $d \mid b$.*
2. *se x_0 è una soluzione di (1), posto $\bar{n} = \frac{n}{d}$, tutte le altre soluzioni di (1) sono $x_0 + k\bar{n}$, al variare di $k \in \mathbb{Z}$*
3. *ci sono esattamente d soluzioni non congrue tra loro $\mathtt{mod}\ n$, cioè $x_0, x_0+\bar{n}, \ldots, x_0+(d-1)\bar{n}$.*

Dimostrazione. Per provare 1., si osserva che, affermare che la congruenza lineare (1) ha soluzioni equivale a dire che esiste $x_0 \in \mathbb{Z}$ tale che

$$n \mid ax_0 - b,$$

ovvero che esistono $x_0, y_0 \in \mathbb{Z}$ tali che

$$ax_0 - b = ny_0,$$

ossia

$$ax_0 + n(-y_0) = b. \tag{2}$$

Questo vuol dire che l'equazione diofantea $ax + ny = b$ ammette soluzione $(x_0, -y_0)$. Dal teorema sulle equazioni diofantee è noto che 2 ha soluzioni se e solo se $M.C.M.(a,n)|b$.

Anche la 2. segue subito dal teorema sulle equazioni diofantee. La dimostrazione della 3. si tralascia.

Definizione 1. Sia R un insieme dotato di due leggi di composizione interne $\wedge$ e $\vee$. Si dice che la struttura algebrica $(R, \wedge, \vee)$ è un *reticolo* (algebrico) se $\wedge$ e $\vee$ verificano le proprietà:

(1) $\forall x, y, z \in R, \quad (x \wedge y) \wedge z = x \wedge (y \wedge z); \quad (x \vee y) \vee z = x \vee (y \vee z)$ associativa
(2) $\forall x, y \in R, \quad x \wedge y = y \wedge x; \quad x \vee y = y \vee x$ commutativa
(3) $\forall x, y \in R, \quad x \vee (x \wedge y) = x; \quad x \wedge (x \vee y) = x$ assorbimento.

Osservazione 1. In un reticolo vale il *principio di dualità*, ovvero se si dimostra un teorema, vale lo stesso teorema scambiando tra loro le operazioni $\vee$ e $\wedge$. Questo perchè le proprietà associativa e commutativa valgono per entrambe le leggi di composizione interne e nella proprietà di assorbimento le due leggi sono intercambiabili.

Esempio 1. Un classico esempio di reticolo è fornito dall'insieme delle parti di un assegnato insieme X sul quale si considerino le leggi di composizione interne $\cap$ e $\cup$. Quindi $(\mathscr{P}(X), \cap, \cup)$ è un reticolo, come facilmente si può verificare.

Esempio 2. Si può provare che l'insieme $\mathbb{N}^*$ con le leggi di composizione interne $\wedge = M.C.D.$, $\vee = m.c.m.$ è un reticolo.

Esempio 3. Per ogni $n \in \mathbb{N}$, $n \geq 2$, anche la struttura $(D_n, \wedge, \vee)$, dove D_n è l'insieme dei divisori di n, $\wedge = M.C.D.$, $\vee = m.c.m.$, è un reticolo.

Definizione 2. Sia $(R, \wedge, \vee)$ un reticolo. Un sottoinsieme R' di R si dice sottoreticolo se è chiuso rispetto alle operazioni $\wedge$ e $\vee$, ovvero se

$$\forall x, y \in R' \quad x \wedge y \in R', \quad x \vee y \in R'.$$

Osservazione 2. Se R' è un sottoreticolo di $(R, \wedge, \vee)$, allora diventa a sua volta reticolo con le operazioni indotte.

Osservazione 3. Si può provare che D_n è chiuso rispetto alle due leggi $\wedge$ e $\vee$ del reticolo $(\mathbb{N}^*, \wedge, \vee)$ dell'esempio 2. Quindi $(D_n, \wedge, \vee)$ è un sottoreticolo di $(\mathbb{N}^*, \wedge, \vee)$.

Definizione 3. Un reticolo $(R, \wedge, \vee)$ si dice *distributivo* se

$$\forall x, y, z \in R \quad (x \wedge y) \vee z = (x \vee z) \wedge (y \vee z); \quad (x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z).$$

Notazione 1. Sia $(R, \wedge, \vee)$ un reticolo. Se esiste l'elemento neutro rispetto a $\wedge$, esso si indica con $\widehat{1}$; se esiste l'elemento neutro rispetto a $\vee$, si indica con $\widehat{0}$. Quindi, nel caso esistano $\widehat{0}$ e $\widehat{1}$, si ha:

$$\forall x \in R \quad x \wedge \widehat{1} = x; \quad x \vee \widehat{0} = x.$$

Esempio 4. Nell'esempio 1, si ha: $\widehat{0} = \emptyset$, $\widehat{1} = X$.

Definizione 4. Siano $(R, \wedge, \vee)$ un reticolo dotato di $\widehat{0}$ e $\widehat{1}$, $a \in R$. Si dice che a è *complementato* se esiste un elemento a' tale che:

$$a \vee a' = \widehat{1}, \quad a \wedge a' = \widehat{0};$$

in tal caso si dice che a' è un *complemento* di a.

Esempio 5. Nel caso dell'esempio 1, per ogni $A \in \mathscr{P}(X)$ esiste il complemento di A, $A' = \complement_X A$. Infatti $A \cap \complement_X A = X = \widehat{1}$, $A \cup \complement_X A = \emptyset = \widehat{0}$.

Proposizione 1. *Sia $(R, \wedge, \vee)$ un reticolo distributivo dotato di $\widehat{0}$ e $\widehat{1}$, $a \in R$. Allora, se a ammette complemento, esso è unico*

Dimostrazione. Siano a' e a'' complementi di a. Allora si ha:

$$\begin{aligned} a'' &= a'' \vee \widehat{0} = a'' \vee (a' \wedge a) = (a'' \vee a') \wedge (a'' \vee a) = (a'' \vee a') \wedge \widehat{1} \\ &= (a'' \vee a') \wedge (a \vee a') = (a'' \wedge a) \vee a' = \widehat{0} \vee a' = a' \end{aligned}$$

In seguito si vedranno esempi di reticoli che non sono distributivi contenenti elementi che ammettono più di un complemento.

Definizione 5. Si dice che un reticolo $(R, \wedge, \vee)$ è *di Boole* se

B_1) è distributivo
B_2) ammette $\widehat{0}$ e $\widehat{1}$
B_3) ogni elemento è complementato.

Esempio 6. Sia X un insieme. Allora il reticolo $(\mathscr{P}(X), \cap, \cup)$ è di Boole: infatti valgono le proprietà distributive e, come si è già osservato, esistono $\widehat{0} = \emptyset$, $\widehat{1} = X$ e ogni elemento A di $\mathscr{P}(X)$ ha complemento che è $\complement_X A$.

Esempio 7. Il reticolo $(\mathbb{N}^*, \wedge, \vee)$ dell'esempio 2 non è un reticolo di Boole, perchè pur ammettendo $\widehat{0} = 1$, non ammette $\widehat{1}$.

Esempio 8. In generale, il reticolo $(D_n, \wedge, \vee)$ dell'esempio dei divisori di un intero $n \geq 2$ (cf. esempio 3) non è di Boole. Si può dimostrare che lo è se e soltanto se n è prodotto di numeri primi distinti.

Definizione 6. Un insieme ordinato $(R, \leq)$ si dice *reticolo* (ordinato) se ogni coppia di elementi di R ammette estremo superiore ed estremo inferiore. In altri termini

$$\forall x, y \in R \ \ \exists \sup(x, y), \quad \inf(x, y).$$

Esempio 9. L'insieme $(\mathbb{N}^*, |\ )$ è un reticolo ordinato, in quanto, com'è facile osservare, per ogni $a, b \in \mathbb{N}^*$ si ha, rispetto a "|"

$$\inf(a, b) = M.C.D.(a, b), \quad \sup(a, b) = m.c.m.(a, b).$$

Esempio 10. Per ogni intero $n \geq 2$, l'insieme dei divisori di n ordinato per divisibilità $(D_n, |\ )$ è un sottoinsieme ordinato di $(\mathbb{N}^*, |\ )$ e, come si è già osservato, $\forall a, b \in D_n$, $M.C.D.(a, b) \in D_n$ e $m.c.m.(a, b) \in D_n$, per cui anche $(D_n, |\ )$ è un reticolo ordinato.

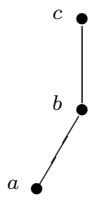
Esempio 11. Sia X un insieme. Allora l'insieme $\mathscr{P}(X)$ delle parti di X, ordinato per inclusione, ovvero $(\mathscr{P}(X), \subseteq)$, è un reticolo ordinato in quanto

$$\forall A, B \in \mathscr{P}(X) \quad \inf(A, B) = A \cap B, \quad \sup(A, B) = A \cup B.$$

Esempio 12. Sia $(G, \cdot)$ un gruppo, H, K ne siano sottogruppi. È noto che $H \cap K$ è un sottogruppo di G, ma $H \cup K$ non lo è, in generale. Si considera allora il più piccolo sottogruppo (per inclusione) $\widehat{H \cup K}$ che contiene $H \cup K$. Si può verificare che la struttura $(\mathcal{H}(G), \subseteq)$, dove $\mathcal{H}(G)$ è l'insieme dei sottogruppi di G è un reticolo ordinato poichè

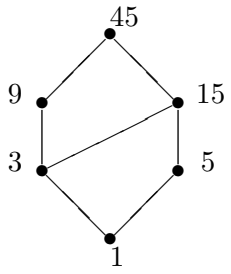
$$\forall H, K \in \mathcal{H}(G) \ \ \inf(H, K) = H \cap K, \quad \sup(H, K) = \widehat{H \cup K}.$$

Osservazione 4. Un insieme $(A, \leq)$ ordinato finito può essere rappresentato mediante un *diagramma di Hasse*. Se $a, b, c \in A$, se $a \leq b$ e se non ci sono elementi intermedi, basta collegare a con b mediante un segmento ascendente. Poichè vale la proprietà transitiva, se $a \leq b$ e $b \leq c$, a sarà collegato con b mediante un segmento ascendente, b sarà collegato con c mediante un altro segmento ascendente, e a sarà collegato con c mediante una spezzata ascendente:

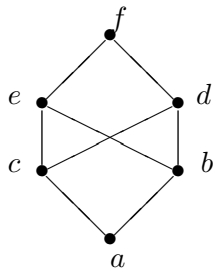


In particolare questo può essere fatto per un reticolo.

Esempio 13. Il diagramma di Hasse del reticolo $(D_{45}, \mid)$ dei divisori di 45 ordinato per divisibilità è:

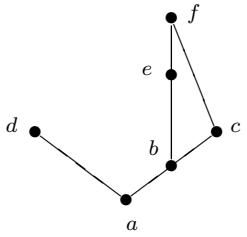


Esempio 14. L'insieme ordinato rappresentato dal seguente diagramma di Hasse



non è un reticolo, poichè la coppia $\{e, d\}$ ha come insieme dei minoranti $X = \{a, b, c\}$ che non presenta massimo.

Esercizio 1. Stabilire perchè l'insieme ordinato rappresentato dal seguente diagramma:



non è un reticolo.

Lemma 1. Sia $(R, \wedge, \vee)$ un reticolo. Allora si ha

$$\forall x, y \in R, \quad (x \wedge y = x) \;\Leftrightarrow\; (x \vee y = y).$$

Dimostrazione. Siano $x, y \in R$, tali che $x \wedge y = x$, allora, per l'assorbimento,

$$x \vee y = (x \wedge y) \vee y = y.$$

Viceversa, se $x \vee y = y$, allora, in modo analogo

$$x \wedge y = x \wedge (x \vee y) = x.$$

Teorema 1. *Sia $(R, \wedge, \vee)$ un reticolo (algebrico). Se $\forall x, y \in R$ si pone*

$$x \leq y \Longleftrightarrow x \wedge y = x \overset{Lemma1}{\Longleftrightarrow} x \vee y = y,$$

allora " $\leq$ " è una relazione di ordine rispetto alla quale R risulta essere un reticolo (ordinato).

Vale anche il teorema inverso

Teorema 2. *Sia $(R, \leq)$ un reticolo (ordinato). Se $\forall x, y \in R$ si pone*

$$x \wedge y = \inf(x, y), \quad x \vee y = \sup(x, y)$$

allora $(R, \wedge, \vee)$ è un reticolo (algebrico).

In virtù del Teorema 2, si hanno i seguenti esempi:

Esempio 15. I reticoli (ordinati) $(\mathbb{N}^*, |\ )$ e $(D_n, |\ )$ diventano reticoli (algebrici) ponendo

$$\forall a, b \ \ a \wedge b = M.C.D.(a, b) \quad a \vee b = m.c.m.(a, b).$$

Esempio 16. Sia X un insieme. Allora il reticolo (ordinato) $\mathscr{P}(X)$ diventa reticolo (algebrico) ponendo

$$\forall A, B \in \mathscr{P}(X) \quad A \wedge B = A \cap B \quad A \vee B = A \cup B.$$

Esempio 17. Sia $(G, \cdot)$ un gruppo. Allora il reticolo (ordinato) $(\mathcal{H}(G), \subseteq)$ dei sottogruppi di $(G, \cdot)$ ordinato per inclusione diventa reticolo (algebrico) ponendo

$$\forall H, K \in \mathcal{H}(G) \ \ H \wedge K = H \cap K, \quad H \vee K = \widehat{H \cup K}.$$

Esercizio 2. Usando il Teorema 1, fare il procedimento inverso nei tre esempi precedenti.

Osservazione 5. Sia $(R, \leq)$ un reticolo ordinato. Se il reticolo algebrico associato ammette $\widehat{0}$, questo è il più piccolo elemento di R rispetto a $\leq$. Infatti, per il Teorema 9,

$$\forall x \in R \ \ x = x \vee \widehat{0} \ \Leftrightarrow \ \widehat{0} \leq x.$$

Analogamente, Se il reticolo algebrico associato ammette $\widehat{1}$, questo è il più grande elemento di R rispetto a $\leq$.

Osservazione 6. Sia $(R, \leq)$ un reticolo ordinato. Se il reticolo algebrico associato ammette $\widehat{0}$, allora si ha:

$$\forall x \in R, \ \ x \vee \widehat{0} = x \overset{Lemma1}{\Longleftrightarrow} x \wedge \widehat{0} = \widehat{0}.$$

Se il reticolo algebrico associato ammette $\widehat{1}$, allora

$$\forall x \in R, \ \ x \wedge \widehat{1} = x \overset{Lemma1}{\Longleftrightarrow} x \vee \widehat{1} = \widehat{1}.$$

Osservazione 7. Si dimostra che ogni reticolo finito ha necessariamente $\widehat{0}$ e $\widehat{1}$.

Proposizione 2. *Sia $(R, \wedge, \vee)$ un reticolo di Boole. Allora $\forall a, b \in R$ risulta*

$$(a \vee b)' = a' \wedge b'; \quad (a \wedge b)' = a' \vee b' \quad \text{Leggi di De Morgan.}$$

Dimostrazione. Bisogna provare che $\forall a, b \in R$

$$(a \vee b) \wedge (a' \wedge b') = \widehat{0}; \quad (a \vee b) \vee (a' \wedge b') = \widehat{1}$$

$$(a \wedge b) \wedge (a' \vee b') = \widehat{0}; \quad (a \wedge b) \vee (a' \vee b') = \widehat{1}.$$

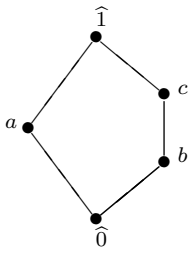
Si prova solamente la prima delle quattro: la seconda si verifica in maniera analoga, le altre due seguono per il principio di dualità.

$$\begin{aligned}
(a \vee b) \wedge (a' \wedge b') &= (a \wedge (a' \wedge b')) \vee (b \wedge (a' \wedge b')) \\
&= ((a \wedge a') \wedge b') \vee (b \wedge (b' \wedge a')) \\
&= (\widehat{0} \wedge b') \vee ((b \wedge b') \wedge a') \\
&= \widehat{0} \vee (\widehat{0} \wedge a') = \widehat{0} \vee \widehat{0} = \widehat{0}.
\end{aligned}$$

Osservazione 8. Dato un reticolo algebrico, si può considerare il reticolo ordinato ad esso canonicamente associato e viceversa. Pertanto da ora in avanti si parlerà indifferentemente di struttura algebrica o ordinata di un assegnato reticolo.

Definizione 7. Si dice *pentagonale*, e si indica con N_5, un reticolo ordinato $R = \{\widehat{0}, a, b, c, \widehat{1}\}$ con la condizione che $b \leq c$.

Il diagramma di Hasse di N_5 è:



Si osserva che a ha due complementi che sono b e c. Pertanto non è detto che il reticolo sia distributivo (cf. Proposizione 4). Poiché risulta

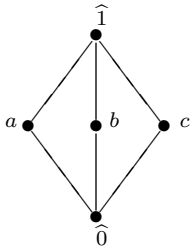
$$b \vee (a \wedge c) = b \vee \widehat{1} = \widehat{1}$$

$$(b \vee a) \wedge (b \vee c) = \widehat{1} \wedge c = c$$

il reticolo non è distributivo.

Definizione 8. Si dice *trirettangolo*, e si indica con M_3, un reticolo ordinato isomorfo al seguente: $R = \{\widehat{0}, a, b, c, \widehat{1}\}$, senza ulteriori condizioni.

Il diagramma di Hasse del reticolo trirettangolo è il seguente:



Si osservi che a ha due complementi, ovvero b e c; b ha due complementi, ovvero a e c; c ha due complementi, ovvero a e d. Quindi, come nel caso di N_5 non è detto si tratti di un reticolo distributivo: e infatti si ha:

$$a \wedge (b \vee c) = a \wedge \widehat{1} = a$$

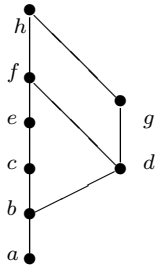
$$(a \wedge b) \vee (a \wedge c) = \widehat{0} \vee \widehat{0} = \widehat{0}.$$

Se si deve provare che un reticolo finito è distributivo e non lo si può fare con tre generici suoi elementi, non è consigliabile verificare tutti i possibili casi. Infatti si ricorre al seguente criterio.

Teorema 3. *Un reticolo finito $(R, \wedge, \vee)$ è distributivo se e soltanto se non ammette sottoreticoli isomorfi a N_5 o a M_3.*

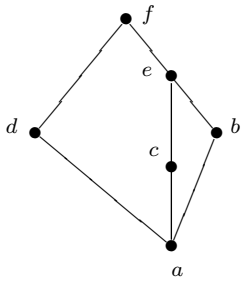
Osservazione 9. Per vedere se un tale sottoreticolo esiste, si utilizzano i diagrammi di Hasse, come nei seguenti esempi.

Esempio 18. Il reticolo rappresentato dal seguente diagramma di Hasse, non è distributivo:



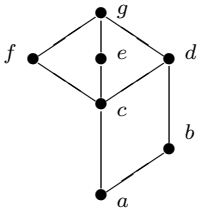
Infatti $\{b, d, c, e, f\}$ formano un sottoreticolo isomorfo a N_5.

Esempio 19. Analogo discorso vale per il reticolo individuato dal diagramma di Hasse:



poichè $\{a, c, d, e, f\}$ formano un sottoreticolo isomorfo a N_5.

Esempio 20. Il reticolo il cui diagramma di Hasse è:



non è distributivo, in quanto $\{c, d, e, f, g\}$ è un sottoreticolo isomorfo a M_3.

Esercizio 3. Nell'esempio precedente $\{a, b, c, f, g\}$ non forma un sottoreticolo: perchè?

Definizione 9. Si dice che un anello $(A, +, \cdot)$ è *di Boole* se

$$\forall a \in A \quad a^2 = a$$

Proposizione 3. *Sia $(A, +, \cdot)$ un anello di Boole. Allora*

$$\forall a \in A \quad a + a = 0$$

Dimostrazione Sia $a \in A$, allora

$$a + a = (a + a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a.$$

Per le leggi di cancellazione $a + a = 0$.

Esempio 21. $(\mathbb{Z}_2, +, \cdot)$ è anello di Boole.

Osservazione 10. Siano $(A_1, +, \cdot), \ldots, (A_n, +, \cdot)$ anelli e sia

$$A = A_1 \times \cdots \times A_n.$$

Si può munire A della struttura di anello ponendo

$$\forall (a_1, \ldots, a_n), (b_1, \ldots, b_n) \in A$$

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$
$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot b_1, \ldots, a_n \cdot b_n).$$

In particolare, se $(B, +, \cdot)$ è un anello, si può considerare l'anello $(B^n, +, \cdot)$, dove $B^n = B \times \cdots \times B$. È facile osservare che se $(B, +, \cdot)$ è un anello di Boole, allora anche $(B^n, +, \cdot)$ è di Boole. Quindi per ogni $n \in \mathbb{N}^*$, $(\mathbb{Z}_2^n, +, \cdot)$ è un anello di Boole.

Teorema 4. *Sia $(A, +, \cdot)$ un anello di Boole. Posto*

$$\forall a, b \in A \quad a \wedge b = a \cdot b, \quad a \vee b = a + b + a \cdot b,$$

si ha che $(A, \wedge, \vee)$ è un reticolo di Boole. Viceversa se $(R, \wedge, \vee)$ è un reticolo di Boole, allora le due leggi di composizione "$+$" e "$\cdot$" così definite

$$\forall x, y \in R \quad x + y = (x \wedge y') \vee (x' \wedge y) \quad x \cdot y = x \wedge y$$

conferiscono a R la struttura di anello di Boole.

Esempio 22. Dato X insieme, $(\mathscr{P}(X), \cap, \cup)$ è un reticolo di Boole. Allora si pone per ogni $A, B \in \mathscr{P}(X)$

$$A + B = (A \cap \complement_X(B)) \cup (\complement_X(A) \cap B) = (A \setminus B) \cup (B \setminus A) = A \Delta B$$

che si chiama anche *differenza simmetrica* di A e B,

$$A \cdot B = A \cap B.$$

Quindi $(\mathscr{P}(X), \Delta, \cdot)$ è un anello di Boole.

Definizione 10. Si dice che due anelli $(A_1, +, \cdot)$ e $(B, +.\cdot)$ sono *isomorfi* se esiste un'applicazione bigettiva $f : A \to B$ tale che:

- $\forall a, a' \in A \quad f(a + a') = f(a) + f(a')$
- $\forall a, a' \in A \quad f(a \cdot a') = f(a) \cdot f(a')$
- $f(1_A) = 1_B$.

In tal caso f si dice *isomorfismo di anelli.*

Osservazione 11. Si può provare che per un isomorfismo di anelli $f(0_A) = 0_B$.

Teorema 5. *Sia $(A, +, \cdot)$ anello di Boole finito. Allora esiste $n \in \mathbb{N}^*$ tale che $(A, +, \cdot)$ sia isomorfo all'anello di Boole $(\mathbb{Z}_2^n, +, \cdot)$.*

Osservazione 12. Ogni anello di Boole finito ha cardinalità che è una potenza di 2. Quindi se un anello ha cardinalità diversa da una potenza di 2, sicuramente non è di Boole. Inoltre, dal Teorema 4 si sa che ogni reticolo di Boole si può riguardare come un anello di Boole e dunque un reticolo di Boole finito ha cardinalità una potenza di 2. Pertanto se un reticolo non ha come cardinalità una potenza di 2 non è di Boole, ma non è vero che se un reticolo ha cardinalità una potenza di 2 allora è un reticolo di Boole!