

ALGEBRA



INTRODUZIONE

ESTRATTO

Il presente documento è una raccolta di appunti accuratamente riorganizzati e arricchiti da un layout grafico migliorato, basato sul corso di Algebra tenuto dal docente G. Cutolo per il Corso di Laurea in Informatica A.A. 2023-2024 dell'Università Federico II di Napoli.

Si precisa che questo documento non è destinato a sostituire libri di testo, appunti del docente o lezioni frontali, pur essendo basato su tali fonti. Il suo scopo principale è offrire una risorsa unificata per lo studio dell'intero programma del corso, integrando il materiale più complesso con approfondimenti, esempi ed esercizi pensati per chiarire dubbi, colmare lacune e facilitare il superamento delle difficoltà riscontrate durante lo studio individuale.

Si ringrazia **Valentino Bocchetti**, curatore dell'aspetto grafico di questo documento, per il prezioso contributo.

Un ringraziamento speciale va a tutti i revisori che hanno fornito consigli e proposte di modifica, migliorando ulteriormente la qualità del contenuto. Infine, si ringraziano i lettori per la loro attenzione e si invita chiunque riscontri errori o abbia suggerimenti a contattare gli autori, con l'augurio che questo lavoro possa essere di grande utilità per il loro percorso di studio.

Redazione a cura di **Giorgio Di Fusco**

Revisione testo a cura di Mario Majorano, Andrea Di Donato, Luigi Ruggiero, Luigi Ferrara

Documento aggiornato al **05 September 2025** (Revisione documento **3d59ec1**)



Attenzione ➤

Esistono diverse versioni di questo documento in circolazione. È fondamentale assicurarsi di **consultare sempre la versione più recente**, in quanto potrebbe contenere informazioni aggiornate o correzioni rispetto alle versioni precedenti. Per evitare di studiare da fonti non esatte si raccomanda vivamente di verificare la data di pubblicazione e il numero di revisione riportati alla fine di questa pagina.

Revisione	Data
67dfc7c	15/03/2024
00a8221	28/08/202
343cc71	29/08/2024
9087dcf	11/09/2024
83a3f0f	01/10/2024
3af1354	19/02/2025

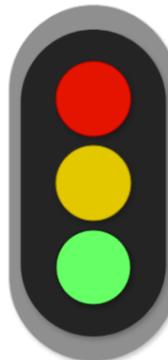
**Documento deprecato****Attenzione, possono esserci errori****Ultima versione**

Tabella 1: Cronologia revisioni del documento



Tutte le versioni del documento, insieme al codice sorgente e ai materiali aggiuntivi, sono disponibili nella **repository** ufficiale su GitHub.

Ti invitiamo a consultare la repository per eventuali aggiornamenti, contributi o per segnalare problemi direttamente tramite issue.

0.2.1 ■ In caso di errori

È sempre ben gradito ricevere feedback.

Feedback generali: se hai domande rispetto qualsiasi aspetto del libro non esitare a contattarmi:

- Email: giorgio99difusco@gmail.com

INDICE

0 INTRODUZIONE	3
0.1 Sulle versioni del documento	4
0.2 Repository del progetto	4
0.2.1 In caso di errori	4
1 LOGICA RUDIMENTALE	8
1.1 Proposizioni logiche	8
1.1.1 I connettivi logici	8
1.1.2 Il connettivo condizionale	11
1.2 Proprietà dei connettivi logici	12
1.2.1 Le leggi di De Morgan	13
1.2.2 Le tautologie dell'implicazione	14
1.2.3 Tautologie dello XOR	17
1.3 I quantificatori	18
1.3.1 Formule e quantificatori	18
1.3.2 Occorrenze libere e vincolate	19
1.3.3 Sostituzioni	20
1.3.4 Predicati	20
1.3.5 I quantificatori ristretti	20
1.3.6 Regole di manipolazione dei quantificatori	21
1.3.7 Negazione dei quantificatori	21
1.4 Esercizi svolti	23
2 TEORIA DEGLI INSIEMI	32
2.1 Definizione e rappresentazione degli insiemi	32
2.1.1 Rappresentazione degli insiemi	34
2.2 Notazione insiemistica	34
2.2.1 Sottoinsiemi e relazione di inclusione	34
2.2.2 L'insieme delle parti	35
2.3 Operazioni insiemistiche	36
2.3.1 Intersezione	36
2.3.2 Unione	37
2.3.3 Differenza insiemistica	38
2.3.4 Le leggi di De Morgan e differenza simmetrica	39
2.3.5 Operazioni unarye	40
2.4 Prodotto Cartesiano di Insiemi	41
2.4.1 Copie ordinate	41
2.4.2 Prodotti cartesiani	42
2.5 Esercizi svolti	43
3 CORRISPONDENZE E RELAZIONI DI EQUIVALENZA	55
3.1 Corrispondenze e relazioni binarie	55
3.1.1 Proprietà delle relazioni binarie	56
3.1.2 Rappresentazione delle corrispondenze	56
3.1.3 Prodotto relazionale	57
3.2 Applicazioni	57
3.2.1 Questione della ``buona posizione'' delle applicazioni	58
3.2.2 Composizione tra applicazioni	63

3.3 Suriettività e iniettività	64
3.3.1 Funzioni iniettive	64
3.3.2 Funzioni suriettive	65
3.3.3 Funzioni biettive	68
3.4 Sezioni e Retrazioni	68
3.4.1 Applicazioni inverse	69
3.5 Partizioni e relazioni di equivalenza	70
3.5.1 Partizioni	70
3.5.2 Relazioni di equivalenza	71
3.6 Esercizi svolti	78
3.6.1 Corrispondenze e applicazioni	78
3.6.2 Relazioni di equivalenza e partizioni	85
4 TECNICHE DI ENUMERAZIONE	86
4.1 Cardinalità degli insiemi	86
4.1.1 Il principio di inclusione-esclusione	86
4.1.2 Insiemi finiti	87
4.1.3 La funzione caratteristica e la cardinalità dell'insieme delle parti	91
4.2 Il principio di induzione	94
4.3 Esercizi svolti	95
5 OPERAZIONI E STRUTTURE ALGEBRICHE	98
5.1 Generalità sulle operazioni	98
5.1.1 Proprietà delle operazioni	98
5.2 Strutture algebriche	101
5.2.1 Semigruppi	101
5.2.2 I monoidi	102
5.2.3 Elementi simmetrizzabili	105
5.2.4 Elementi cancellabili	106
5.3 Gruppi	108
5.3.1 Sottogruppi di un gruppo	110
5.3.2 Parti chiuse e generatori	110
5.3.3 Il gruppo delle permutazioni	111
5.3.4 Gruppi ciclici	113
5.4 Omomorfismi tra strutture algebriche	114
5.5 Anelli	117
5.5.1 Regole di calcolo in un anello	117
5.5.2 Tipologie di anello	119
5.6 Esercizi svolti	122
6 RETICOLI E ALGEBRE DI BOOLE	133
6.1 Relazioni d'ordine	133
6.1.1 Insiemi ordinati	135
6.1.2 Minimo, massimo, minimali e massimali	136
6.1.3 Intervalli e coperture	137
6.1.4 Diagrammi di Hasse	138
6.1.5 Maggioranti, minoranti, estremo superiore ed inferiore	140
6.2 Reticoli	143
6.2.1 Operazioni reticolari	145
6.2.2 Sottoreticolari	146
6.2.3 Omomorfismi tra reticolari	147
6.2.4 Dualità reticolare	147
6.2.5 Reticoli distributivi e complementati	147
6.3 Strutture booleane	150
6.3.1 Anelli booleani	150
6.3.2 Reticoli booleani	151
6.3.3 Algebre di Boole	151
6.3.4 Anelli booleani e algebre di Boole	153
6.4 Esercizi svolti	156
6.4.1 Relazioni d'ordine e reticolari	156
7 ARITMETICA E POLINOMI	164

7.1 Aritmetica nell'insieme degli interi	164
7.1.1 Il principio di buon ordinamento	164
7.1.2 Insiemi naturalmente ordinati	164
7.1.3 Divisibilità e fattorizzazione	165
7.1.4 Algoritmo euclideo, MCD ed equazioni diofantee	169
7.1.5 Equazioni diofantee	172
7.1.6 Struttura quoiente	174
7.2 Congruenze in \mathbb{Z}	174
7.2.1 La relazione di congruenza modulo m	174
7.2.2 Equazioni congruenziali	188
7.3 L'anello dei polinomi	183
7.3.1 Definizione e terminologia essenziale	183
7.3.2 Proprietà universale	186
7.3.3 Grado di somme e prodotto di polinomi	187
7.3.4 Divisione con resto tra polinomi	189
7.3.5 Applicazioni polinomiali	192
7.3.6 Fattorizzazione	195
7.3.7 Metodi ed esempi di fattorizzazione per polinomi su un campo	197
7.4 Esercizi svolti	200
7.4.1 Aritmetica e congruenze	200
7.4.2 Polinomi	204

8 ELEMENTI DI TEORIA DEI GRAFI

8.1 Grafi e multigrafi	208
8.1.1 Isomorfismi tra grafi	211
8.1.2 Multigrafi	211
8.2 Cammini e circuiti in un grafo	213
8.3 Foreste ed alberi	213
8.3.1 Rappresentazione radiale di un albero	214
8.3.2 Sottoalberi massimali	215
8.4 Esercizi svolti	216

9 TRACCE D'ESAME

9.1 Esame del 16 gennaio 2023	218
9.2 Esame del 13 luglio 2023	222
9.3 Esame del 15 gennaio 2024	227
9.4 Esame del 16 marzo 2024	232
9.5 Esame del 22 aprile 2024	238
9.6 Esame del 15 luglio 2024	242
9.7 Esame del 10 settembre 2024	246

Indice Alfabetico

258

LOGICA RUDIMENTALE

1.1

PROPOSIZIONI LOGICHE



Ogni teoria matematica è espressa in un **linguaggio**, che è costituito da:

1. Da un **alfabeto di simboli** che possono essere messi insieme per costruire parole (stringhe di caratteri);
2. Da **regole sintattiche** che permettono di distinguere tra stringhe “composte correttamente”, chiamate **formule**, e stringhe che non sono correttamente composte.

Esempio 1.1.1

Ad esempio, la stringa “ $0 < 1$ ” rappresenta una formula mentre la stringa “ $0 <$ ” no.

Tra le formule matematiche facciamo un’ulteriore distinzione:

Definizione 1.1.1: Formula chiusa

Le formule alle quali è possibile attribuire univocamente un valore di verità, *vero* o *falso*, vengono chiamate **proposizioni** o **formule chiuse**.

Esempio 1.1.2

La formula “ $x > 1$ ” non è una proposizione in quanto non possiamo associare un valore vero o falso in quanto *dipendente* dal valore della variabile x .

1.1.1 ■ I connettivi logici

Ogni linguaggio contiene dei simboli, mediante i quali è possibile costruire periodi più complessi a partire da blocchi atomici. Anche nella logica matematica esistono dei simboli, chiamati **connettivi logici**, che permettono di costruire proposizioni più complesse a partire da proposizioni più semplici. I connettivi logici più comuni sono:

- **Negazione**: \neg ;
- **Congiunzione**: \wedge ;
- **Disgiunzione**: \vee ;
- **Disgiunzione esclusiva**: $\dot{\vee}$;
- **Equivalenza**: \iff ;
- **Implicazione**: \implies .

1.1.1.1 ■ Negazione

La negazione di una proposizione p è una proposizione che è vera quando p è falsa e viceversa. La negazione di una proposizione p viene indicata con $\neg p$. Il connettivo di negazione è **unario**, ovvero è un connettivo che agisce su una sola proposizione. Spesso,

per visualizzare i valori di verità di una proposizione, si utilizza una tabella chiamata **tabella di verità**.

La tabella di verità della negazione è la seguente:

p	$\neg p$
V	F
F	V

Tabella 1.1: Tavola di verità della negazione

1.1.1.2 ■ Congiunzione

La congiunzione di due proposizioni p e q è una proposizione che è vera quando p e q sono vere e falsa in tutti gli altri casi. La congiunzione di due proposizioni p e q viene indicata con $p \wedge q$. Il connettivo di congiunzione è **binario**, ovvero è un connettivo che agisce su due proposizioni. La tabella di verità della congiunzione è la seguente:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Tabella 1.2: Tavola di verità della congiunzione

1.1.1.3 ■ Disgiunzione

La disgiunzione di due proposizioni p e q è una proposizione che è vera quando p o q sono vere e falsa in tutti gli altri casi. La disgiunzione di due proposizioni p e q viene indicata con $p \vee q$. La tabella di verità della disgiunzione è la seguente:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Tabella 1.3: Tavola di verità della disgiunzione

1.1.1.4 ■ Disgiunzione esclusiva

La disgiunzione esclusiva di due proposizioni p e q è una proposizione che è vera quando p o q sono vere, ma non entrambe, e falsa in tutti gli altri casi. La disgiunzione esclusiva di due proposizioni p e q viene indicata con $p \dot{\vee} q$. La tabella di verità della disgiunzione esclusiva è la seguente:

p	q	$p \dot{\vee} q$
V	V	F
V	F	V
F	V	V
F	F	F

Tabella 1.4: Tavola di verità della disgiunzione esclusiva

1.1.1.5 ■ Equivalenza

L'equivalenza di due proposizioni p e q è una proposizione che è vera quando p e q hanno lo stesso valore di verità e falsa in tutti gli altri casi. L'equivalenza di due proposizioni p e q viene indicata con $p \iff q$. La tabella di verità dell'equivalenza è la seguente:

p	q	$p \iff q$
V	V	V
V	F	F
F	V	F
F	F	V

Tabella 1.5: Tavola di verità dell'equivalenza logica

Definizione 1.1.2: Proposizione logica

Una **proposizione logica** o **forma proposizionale** è una formula ottenuta dalla composizione di una o più formule mediante connettivi logici.

Per calcolare il valore di verità di una forma proposizionale possiamo avvalerci delle tabelle di verità oppure, come si vedrà più in avanti, usare alcune proprietà che permettono di arrivare al risultato in maniera più veloce. Infatti, data una forma proposizionale di k variabili è necessario costruire una tabella di 2^k righe.

Esempio 1.1.3

- Si voglia calcolare il valore di verità della forma $p \wedge (q \vee p)$, dove p e q sono proposizioni. La tabella di verità conterrà $2^2 = 4$ righe e sarà la seguente:

p	q	$q \vee p$	$p \wedge (q \vee p)$
V	V	V	V
V	F	V	V
F	V	V	F
F	F	F	F

Come si può notare, per calcolare il valore di verità della formula finale ci siamo avvalsi di una colonna intermedia.

- Si calcoli il valore di verità della forma $P \wedge (Q \vee R)$, dove P , Q e R sono proposizioni. Essendo tre le variabili proposizionali la tabella di verità avrà $2^3 = 8$ righe.

p	q	r	$q \vee r$	$p \wedge (q \vee r)$
V	V	V	V	V
V	F	V	V	V
F	V	V	V	F
F	F	V	V	F
V	V	F	V	V
V	F	F	F	F
F	V	F	V	F
F	F	F	F	F

- Un altro esempio banale di proposizioni logicamente equivalenti è dato dalla formula $P \wedge P$ e P . Si vede infatti immediatamente dalla tabella di verità:

P	$P \wedge P$	$P \iff P \wedge P$
V	V	V
F	F	V

Osservando la tavola di verità notiamo che la prima e l'ultima colonna sono uguali. Questo è dovuto al fatto che la congiunzione è un connettivo **idempotente**, ovvero che restituisce sempre il primo valore di verità quando le due proposizioni sono uguali.

Definizione 1.1.3: Tautologia

Una forma proposizionale φ che assume valore di verità vero in modo del tutto indipendente dai valori attribuiti alle variabili che appaiono in φ viene chiamata **tautologia**. Dualmente, esistono forme proposizionali φ per le quali, calcolato il valore di verità, si ottiene sempre il valore F. Queste si chiamano **contraddizioni**.

Ovviamente φ è una contraddizione se e solo se $\neg\varphi$ è una tautologia. Una forma proposizionale che non sia né una tautologia né una contraddizione si dice **contingente**. Le tautologie sono molto utili nelle dimostrazioni. Infatti, nota la tabella di verità di una determinata formula siamo in grado di sapere la tabella di verità di una formula logicamente equivalente alla prima.

Esempio 1.1.4

- La **doppia negazione** è una tautologia. Infatti, la tabella di verità è la seguente:

p	$\neg p$	$\neg(\neg p)$
V	F	V
F	V	F

La doppia negazione è molto utile per semplificare le formule proposizionali. Infatti, è possibile semplificare la formula $P \wedge \neg(\neg P)$ in $P \wedge P$ e quindi in P .

- Il **principio di non contraddizione** afferma che una proposizione non può essere vera e falsa allo stesso tempo. Questo principio può essere espresso in logica proposizionale come $\neg(p \wedge \neg p)$, ovvero la negazione della congiunzione di una proposizione e della sua negazione. La tabella di verità è la seguente:

p	$\neg p$	$p \wedge \neg p$	$\neg(p \wedge \neg p)$
V	F	F	V
F	V	F	V

Come si può notare, la formula è una tautologia. Analogamente, è possibile ottenere una tautologia simile utilizzando il connettivo di disgiunzione: $p \vee (\neg p)$. Esempi di questa proposizione nel parlato quotidiano possono essere: "In questo momento piove oppure in questo momento non piove", "Studio l'algebra oppure non studio l'algebra", ecc. Verità oggettive sotto qualsiasi punto di vista.

Proposizione 1.1.1

Siano P e Q due forme proposizionali. P e Q sono logicamente equivalenti se e solo se $(P \iff Q)$ è una tautologia.

Dimostrazione. Banale. Siano P e Q due proposizioni logicamente equivalenti, si ha allora:

P	Q	$P \iff Q$
V	V	V
F	F	V

e $P \iff Q$ risulta essere quindi una tautologia. Viceversa, sia $P \iff Q$ una tautologia. Allora, per definizione di equivalenza logica, P e Q hanno gli stessi valori logici e quindi sono logicamente equivalenti. \square

1.1.2 ■ Il connettivo condizionale

Il connettivo condizionale è un connettivo binario che associa due proposizioni p e q e restituisce una proposizione che è falsa quando p , detta "antecedente", è vera e q , detta "conseguente", è falsa, e vera in tutti gli altri casi. Il connettivo condizionale di due proposizioni p e q viene indicato con $p \implies q$. Il connettivo condizionale è anche detto **implicazione**. La tabella di verità del connettivo condizionale è mostrata nella Tabella 1.6.

p	q	$p \implies q$
V	V	V
V	F	F
F	V	V
F	F	V

Tabella 1.6: Tavola di verità del connettivo condizionale.

Esempio 1.1.5

Nella logica proposizionale, frasi come “Se piove allora il Vesuvio è alto più di mille metri sul livello del mare” hanno assolutamente senso in quanto sono delle vere e proprie formule proposizionali. Infatti, se indichiamo con P la proposizione “piove” e con Q la proposizione “il Vesuvio è alto più di mille metri sul livello del mare”, la frase precedente può essere riscritta come $P \implies Q$.

Osservazione 1.1.1

Perché le implicazioni con antecedente falso devono essere vere? Consideriamo la frase: “Per ogni numero intero x compreso tra 1 e 3 si ha che se $x > 2$ allora $x > 1$ ”. Tutti concordiamo sul fatto che questa frase sia vera. Analizziamola: essa significa che tutte le implicazioni del tipo $x > 2 \implies x > 1$ ottenute sostituendo ad x uno dei numeri 1, 2, 3 sono vere. Sono vere quindi le proposizioni:

1. Φ_1 : “ $1 > 2 \implies 1 > 1$ ”
2. Φ_2 : “ $2 > 2 \implies 2 > 1$ ”
3. Φ_3 : “ $3 > 2 \implies 3 > 1$ ”

In particolare risulta vera anche la proposizione Φ_1 , che è del tipo $F \implies V$. Questo è in accordo con la tabella di verità del connettivo condizionale (Tabella 1.6). Dunque le implicazioni con antecedente falso sono vere. Si osserva che sono vere anche le implicazioni con conseguente vero. In effetti, si può dire, sinteticamente, che una *implicazione è vera precisamente quando il suo antecedente è falso o il suo conseguente è vero*.

1.2

PROPRIETÀ DEI CONNETTIVI LOGICI



Esprimere una proprietà per un connettivo logico significa affermare che la tabella di verità di una formula è sempre uguale a quella di un'altra formula. In altre parole, significa affermare che le due formule sono logicamente equivalenti e quindi che la formula che esprime la proprietà è una tautologia.

Proposizione 1.2.1

I connettivi logici godono delle seguenti proprietà, valgono cioè le seguenti tautologie:

1. Idempotenza:

$$p \wedge p \iff p \quad (1.1)$$

$$p \vee p \iff p \quad (1.2)$$

2. Commutatività:

$$p \wedge q \iff q \wedge p \quad (1.3)$$

$$p \vee q \iff q \vee p \quad (1.4)$$

$$p \dot{\vee} q \iff q \dot{\vee} p \quad (1.5)$$

$$(p \iff q) \iff (q \iff p) \quad (1.6)$$

3. Associatività

$$(p \wedge q) \wedge r \iff p \wedge (q \wedge r) \quad (1.7)$$

$$(p \vee q) \vee r \iff p \vee (q \vee r) \quad (1.8)$$

$$((p \iff q) \iff r) \iff (p \iff (q \iff r)) \quad (1.9)$$

4. Distributività:

$$(p \wedge (q \vee r)) \iff ((p \wedge q) \vee (p \wedge r)) \quad (1.10)$$

$$(p \vee (q \wedge r)) \iff ((p \vee q) \wedge (p \vee r)) \quad (1.11)$$

Dimostrazione. Per esercizio mostriamo la dimostrazione della proprietà associativa dell'equivalenza logica (1.9). La dimostrazione delle altre proprietà è lasciata al lettore. La verifica del fatto che la proprietà in questione si tratti di una tautologia è immediata se si osserva la tabella di verità 1.7.

p	q	r	$p \iff q$	$(p \iff q) \iff r$	$p \iff (q \iff r)$
V	V	V	V	V	V
V	V	F	V	V	V
V	F	V	F	F	F
V	F	F	F	F	F
F	V	V	F	F	F
F	V	F	F	F	F
F	F	V	V	V	V
F	F	F	V	V	V

Tabella 1.7

Si noti che $((p \iff q) \iff r)$ risulta vera se e solo se esattamente uno o tutti e tre tra p , q ed r risultano vere. \square

Osservazione 1.2.1 ➤➤

Sull'associatività di \wedge e \vee , si osserva che $(p \wedge q) \wedge r$ risulta vera se e solo se sono contemporaneamente vere sia p che q che r (lo stesso vale per $r \wedge (q \wedge r)$), mentre $(p \vee q) \vee r$ è vera se e solo se è vera almeno una tra p , q ed r .

Più in generale è possibile provare che, qualunque sia l'intero positivo k le forme proposizionale in cui appaiano tutte e sole le variabili p_1, p_2, \dots, p_k , delle parentesi e, tra i connettivi solo \wedge (analogamente \vee) sono equivalenti tra loro. Per queste forme si può allora rinunciare all'uso delle parentesi e scrivere semplicemente:

$$p_1 \wedge p_2 \wedge p_3 \wedge \dots \wedge p_k$$

oppure

$$\bigwedge_{i=1}^k p_i$$

per indicare una qualunque di queste forme.

1.2.1 ■ Le leggi di De Morgan

Quando è che una proposizione della forma $p \wedge q$ è falsa? Quando (e solo quando) è falsa almeno una tra p e q . Questo è evidente dalla tavola di verità che descrive la congiunzione. Dualmente una proposizione della forma $p \vee q$ è falsa precisamente quando sia p che q sono false. Tutto questo è espresso da due tautologie molto importanti, note come **leggi di De Morgan**.

Proposizione 1.2.2 (Leggi di De Morgan)

Siano p , q due formule, valgono allora le seguenti tautologie:

$$\neg(p \wedge q) \iff (\neg p) \vee (\neg q) \quad (1.12)$$

$$\neg(p \vee q) \iff (\neg p) \wedge (\neg q) \quad (1.13)$$

Dimostrazione. Poniamo $\alpha := (\neg p) \wedge (\neg q)$, $\beta := (\neg p) \vee (\neg q)$. Abbiamo allora:

p	q	$p \wedge q$	$p \vee q$	$\neg(p \wedge q)$	$\neg(p \vee q)$	α	β
V	V	V	V	F	F	F	F
V	F	F	V	V	F	F	V
F	V	F	V	V	F	F	V
F	F	F	F	V	V	V	V

Dunque, per negare una disgiunzione si negano i due termini che stiamo disgiungendo e, contemporaneamente, si scambiano tra loro i simboli \vee e \wedge . La negazione di una congiunzione è duale. \square

1.2.2 ■ Le tautologie dell'implicazione

Proposizione 1.2.3 (Tautologia della doppia implicazione)

La congiunzione di una implicazione e della corrispondente inversa equivale alla doppia implicazione. Vale cioè la tautologia:

$$(P \iff Q) \iff ((P \implies Q) \wedge (P \Leftarrow Q)) \quad (1.14)$$

Dimostrazione. È facile convincersi osservando la seguente tabella di verità:

p	q	$p \iff q$	$p \implies q$	$p \Leftarrow q$	$(p \implies q) \wedge (p \Leftarrow q)$
V	V	V	V	V	V
V	F	F	F	V	F
F	V	F	V	F	F
F	F	V	V	V	V

che dimostra l'enunciato. \square

Osservazione 1.2.2 ➤➤

Affermare che una certa proposizione A **implica** una determinata proposizione B è equivalente a dire che A è una **condizione sufficiente** per B , ovvero che la veridicità di A è sufficiente per garantire la veridicità di B . Inoltre, affermare che A implica B , è equivalente a dire che B è una **condizione necessaria** per A , ovvero che la veridicità di B è necessaria per garantire la veridicità di A . Il connettivo \implies , a differenza degli altri connettivi binari, non è commutativo. Vale a dire che le forme $P \implies Q$ e $Q \implies P$ non sono equivalenti tra di loro.

P	Q	$P \implies Q$	$Q \implies P$
V	V	V	V
V	F	F	F
F	V	V	F
F	F	V	V

Tabella 1.8: Tavola di verità dell'implicazione inversa

Spesso si scrive " $P \Leftarrow Q$ " per " $Q \implies P$ ". Si può considerare questo simbolo " \Leftarrow " come un ulteriore connettivo binario (**implicazione inversa**), definito appunto dall'essere $p \Leftarrow q$ logicamente equivalente a $q \implies p$ come mostrato nella Tabella 1.8.

Esempio 1.2.1

Consideriamo le frasi p : "Oggi sto sciando" e q : "Oggi sono in montagna". Date queste due proposizioni possiamo considerare l'implicazione: "Se oggi sto sciando allora sono in montagna." Questa implicazione è vera, infatti lo stare in montagna è una **condizione necessaria** per poter sciare ma non una condizione sufficiente. Viceversa, lo stare sciando è una **condizione sufficiente** per dirci che si sta in montagna. Non vale però la formula $q \implies p$. Stare in montagna, infatti, non è sufficiente per affermare che si sta sciando, potrei infatti essere in montagna per fare una passeggiata o per fare escursionismo.

In generale, quando valgono contemporaneamente le formule " $(p \implies q) \wedge (p \Leftarrow q)$ " possiamo parlare di **condizioni necessarie e sufficienti**.

$P \implies Q$	$P \Leftarrow Q$	$P \iff Q$
Se p allora q	Se q allora p	p se e solo se q
p solo se q	p se q	p è condizione necessaria e sufficiente per q
p è condizione sufficiente per q	p è condizione necessaria per q	q è condizione necessaria e sufficiente per p

Tabella 1.9: Le seguenti frasi traducono la formula nell'intestazione

Proposizione 1.2.4 (Implicazione come disgiunzione)

Il connettivo condizionale può essere espresso in termini di altri connettivi. Infatti, vale la seguente tautologia:

$$(p \implies q) \iff \neg p \vee q \quad (1.15)$$

che esprime l'implicazione mediante la disgiunzione tra la negazione dell'antecedente e il conseguente.

Dimostrazione. La dimostrazione segue direttamente dalle tavole di verità di implicazione e disgiunzione:

p	q	$(\neg p) \vee q$	$p \implies q$
V	V	V	V
V	F	F	F
F	V	V	V
F	F	V	V

Una implicazione infatti è vera se e solo se il suo antecedente è falso o il suo conseguente è vero. \square

Da questa tautologia se ne può facilmente dedurre un'altra, la **legge di contrapposizione**.

Proposizione 1.2.5 (Legge di contrapposizione)

Siano p, q due proposizioni logiche, vale allora la seguente:

$$(p \implies q) \iff (\neg q \implies \neg p) \quad (1.16)$$

Dimostrazione. Il passaggio è il seguente:

$$\begin{aligned} p \implies q &\iff (\neg p) \vee q && \text{(per la tautologia precedente)} \\ &\iff q \vee (\neg p) && \text{(per la commutatività di } \vee\text{)} \\ &\iff \neg(\neg q) \vee (\neg p) && \text{(per la doppia negazione)} \\ &\iff \neg q \implies \neg p && \text{(per la tautologia precedente)} \end{aligned}$$

\square

Osservazione 1.2.3

La legge di contrapposizione sta alla base del ragionamento per assurdo. Se, negando la tesi, si riesce infatti a dimostrare un fatto che neghi l'ipotesi iniziale (un **assurdo**) si dimostra allora l'implicazione originale.

Altra tautologia importante è quella che mostra come negare una implicazione. Una implicazione, infatti, è falsa precisamente quando l'*antecedente è vera e falso il conseguente*. Quindi vale la seguente:

Proposizione 1.2.6 (Negazione dell'implicazione)

Siano p e q due formule proposizionali. Vale:

$$\neg(p \implies q) \iff p \wedge \neg q \quad (1.17)$$

Dimostrazione. La dimostrazione è immediata dalla tavola di verità dell'implicazione:

p	q	$p \implies q$	$(\neg(p \implies q))$	$p \wedge (\neg q)$
V	V	V	F	F
V	F	F	V	V
F	V	V	F	F
F	F	V	F	F

□

Un'altra tautologia di uso frequentissimo è quella della **transitività dell'implicazione**. Essa afferma che se $p \implies q$ e $q \implies r$ sono entrambe vere, allora anche $p \implies r$ è vera. In altre parole, se p è una condizione sufficiente per q e q è una condizione sufficiente per r , allora p è una condizione sufficiente per r .

Proposizione 1.2.7 (Transitività dell'implicazione)

Siano p, q, r tre formule proposizionali, vale:

$$((p \implies q) \wedge (q \implies r)) \implies (p \implies r) \quad (1.18)$$

Dimostrazione. La dimostrazione è immediata dalla tavola di verità dell'implicazione.

Posto $\alpha := (p \implies q) \wedge (q \implies r)$ e $\beta := ((p \implies q) \wedge (q \implies r)) \implies (p \implies r)$, abbiamo:

p	q	r	$p \implies q$	$q \implies r$	α	$(p \implies r)$	β
V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	V
V	F	V	F	V	F	V	V
V	F	F	F	V	F	F	V
F	V	V	V	V	V	V	V
F	V	F	V	F	F	V	V
F	F	V	V	V	V	V	V
F	F	F	V	V	V	V	V

Un modo alternativo per dimostrare la transitività dell'implicazione è il seguente: provare che la formula 1.18 non può risultare falsa in nessun caso. Perché la formula sia falsa occorre che sia vero l'antecedente $((p \implies q) \wedge (q \implies r))$ e falso il conseguente $(p \implies r)$. La prima condizione significa che sono vere $(p \implies q)$ e $(q \implies r)$ per via del connettivo \wedge , la seconda che sia vera p e falsa r .

Ora, assumendo queste condizioni, sono in particolare vere p e q (se p fosse vera e q falsa allora $p \implies q$ non sarebbe potuta essere vera). Quindi, se la nostra formula è falsa, risultano vere p e q , ma falsa r . Tuttavia, in questo caso, $q \implies r$ è falsa, mentre si era detto che, perché la formula sia falsa, $q \implies r$ deve essere vera. Questo ragionamento porta così ad una contraddizione che mostra che la formula considerata, cioè:

$$((p \implies q) \wedge (q \implies r)) \implies (p \implies r)$$

non può essere falsa in nessun caso, quindi la 1.18 è una tautologia. □

L'idea esemplificata da questa dimostrazione consiste in questo: imporre che una implicazione sia falsa fornisce immediatamente due informazioni: il valore di *verità dell'antecedente* ed il *valore di verità del conseguente*. Dunque può essere conveniente, nello studiare una implicazione, analizzare subito le conseguenze nell'ipotesi che essa sia falsa.

Dalla transitività dell'implicazione e dalla tautologia della doppia implicazione si possono dedurre molte altre tautologie che coinvolgono i connettivi \implies , \Leftarrow e \iff , come ad esempio la **transitività dell'equivalenza**.

Proposizione 1.2.8 (Transitività dell'equivalenza)

Siano p, q, r tre proposizioni, vale allora:

$$((p \iff q) \wedge (q \iff r)) \implies (p \iff r) \quad (1.19)$$

Proposizione 1.2.9 (Negazione di \iff)

Vale questa utilissima serie di tautologie, che si possono esprimere come catena di equivalenze:

$$(\neg(p \iff q)) \iff (\neg p \iff q) \quad (1.20)$$

$$\iff (p \iff \neg q) \quad (1.21)$$

$$\iff (p \dot{\vee} q) \quad (1.22)$$

Le quattro forme proposizionali sono a due a due logicamente equivalenti. Ciascuna di esse è vera quando e solo quando p e q hanno diversi valori di verità. La dimostrazione è lasciata al lettore come esercizio.

1.2.3 ■ Tautologie dello XOR

Grazie a questa proposizione è possibile dimostrare la **proprietà associativa della disgiunzione esclusiva** (Formula 1.23):

Proposizione 1.2.10 (Associatività di $\dot{\vee}$)

Siano p, q, r tre proposizioni. Allora vale la seguente tautologia:

$$((p \dot{\vee} q) \dot{\vee} r) \iff (p \dot{\vee} (q \dot{\vee} r)) \quad (1.23)$$

Dimostrazione. Consideriamo la seguente catena di equivalenze:

$$\begin{aligned} p \iff (q \iff r) &\iff \neg(\neg(p \iff (q \iff r))) && \text{(per la tautologia della doppia negazione)} \\ &\iff \neg(p \iff (\neg(q \iff r))) && \text{(per la formula 1.20)} \\ &\iff \neg(p \iff (q \dot{\vee} r)) && \text{(per la formula 1.22)} \\ &\iff p \dot{\vee} (q \dot{\vee} r) && \text{(per la formula 1.22)} \end{aligned}$$

Allo stesso modo si verifica la tautologia:

$$((p \dot{\vee} q) \dot{\vee} r) \iff ((p \iff q) \iff r) \quad (1.24)$$

Da queste due, e dall'associatività di \iff si ricava la tautologia che volevamo provare. \square

Altre due facili tautologie che riguardano la disgiunzione esclusiva sono espresse nella seguente catena di implicazioni che dimostrano l'esplicitazione del connettivo $\dot{\vee}$ in termini di altri connettivi:

Proposizione 1.2.11 (Esplicitazione del connettivo $\dot{\vee}$)

Valgono le seguenti equivalenze:

$$(p \dot{\vee} q) \iff (p \wedge \neg(q)) \vee (q \wedge \neg(p)) \quad (1.25)$$

$$\iff (p \vee q) \wedge (\neg(p \wedge q)) \quad (1.26)$$

Dimostrazione. Queste equivalenze si provano facilmente osservando che, evidentemente, sia $(p \wedge \neg(q)) \vee (q \wedge \neg(p))$ che $(p \vee q) \wedge (\neg(p \wedge q))$ sono vere se e solo se esattamente una tra le proposizioni p e q è vera. \square

Proposizione 1.2.12 (Distributività di \wedge rispetto a $\dot{\vee}$)

Siano a, b, c proposizioni logiche, vale allora:

$$a \wedge (b \dot{\vee} c) \iff (a \wedge b) \dot{\vee} (a \wedge c) \quad (1.27)$$

Dimostrazione. Per dimostrare la Formula 1.27 senza usare tavole di verità possiamo usare le tautologie algebriche degli operatori logici visti finora. Abbiamo quindi:

$$\begin{aligned} a \wedge (b \dot{\vee} c) &\iff a \wedge ((b \wedge \neg c) \dot{\vee} (\neg b \wedge c)) && \text{Per la tautologia 1.25} \\ &\iff (a \wedge (b \wedge \neg c)) \vee (a \wedge (\neg b \wedge c)) && \text{Per la distributività di } \wedge \text{ rispetto a } \vee \\ &\iff (a \wedge b \wedge \neg c) \vee (a \wedge \neg b \wedge c) && \text{Semplificando} \end{aligned}$$

Ora consideriamo l'espansione a destra della Formula 1.27 che dobbiamo dimostrare essere uguale:

$$\begin{aligned}(a \wedge b) \vee (a \wedge c) &\iff ((a \wedge b) \wedge \neg(a \wedge c)) \vee (\neg(a \wedge b) \wedge (a \wedge c)) \\&\iff ((a \wedge b) \wedge (\neg a \vee \neg c)) \vee ((\neg a \vee \neg b) \wedge (a \wedge c)) \\&\iff ((a \wedge b \wedge \neg a) \vee (a \wedge b \wedge \neg c)) \vee ((\neg a \wedge a \wedge c) \vee (\neg b \wedge a \wedge c)) \\&\iff (a \wedge b \wedge \neg c) \vee (a \wedge \neg b \wedge c)\end{aligned}$$

Notiamo ora che entrambi i lati dell'equazione sono uguali e la dimostrazione può dirsi conclusa. □

1.3

I QUANTIFICATORI



1.3.1 ■ Formule e quantificatori

Consideriamo la formula “ $x > 1$ ” del linguaggio naturale. Questa formula, pur avendo un senso compiuto, non è una **proposizione**, ovvero non è possibile determinare per essa un valore di verità. Espressioni del genere possono essere generalizzate nel modo seguente:

$$\varphi(x) : \text{“Espressione della variabile } x\text{”}$$

E così via:

$$\varphi(x_1, \dots, x_n) : \text{“Espressione delle variabili } x_1, \dots, x_n\text{”}$$

Di conseguenza, nel caso di $\varphi(x) : x > 1$ se $x = 3$ allora $\varphi(3) = 3 > 1$ che è una proposizione, in particolare vera. Da questo breve esempio possiamo estendere la nozione di verità, valutando la formula per ciascuno dei valori che possono essere *sostituiti* alla variabile x .

Definizione 1.3.1: Formula valida

Una formula che risulta vera per ogni possibile sostituzione delle variabili si dice **valida**.

La nozione di sostituzione permette di introdurre due nuovi simboli logici che svolgono un ruolo centrale nel **calcolo dei predicati**. Questi simboli sono i **quantificatori**.

Definizione 1.3.2: Quantificatore universale

Se φ è una formula ed x è una variabile allora anche “ $\forall x(\varphi)$ ” è una formula, chiamata **formula universale** e si legge “per ogni x , φ è vera”. Questa formula esprime la contemporanea affermazione di tutte le formule $\varphi(a)$ ottenute sostituendo ad x ogni possibile valore a . Il simbolo \forall prende il nome di **quantificatore universale**.

Osservazione 1.3.1 ➤➤➤

Sono equivalenti le forme: $\forall x(\varphi(x))$ e $\forall x(\varphi)$. A volte, per esplicitare la parte del quantificatore si usa racchiuderlo tra parentesi tonde: $(\forall x)(\varphi(x))$.

Esempio 1.3.1

Sia $\varphi : x > 3$ e sia l'universo del discorso ristretto all'insieme dei numeri naturali, allora scrivere “ $\forall x(\varphi(x))$ ” equivale a dire “per ogni numero naturale x , questo è maggiore di 3” che ovviamente è falso.

Osservazione 1.3.2 ➤➤➤

Il quantificatore universale può essere visto^a come una sequenza di proposizioni collegate tra di loro con un connettivo di congiunzione.

^aLa congiunzione però non può operare su un numero infinito di proposizioni mentre il quantificatore si.

Se le formule universali possono essere pensate come una sorta di congiunzione generalizzata, le **formule esistenziali**, cioè quelle del tipo “ $\exists x(\varphi)$ ” (che si legge “esiste un x tale che φ è vera”) possono essere pensate come disgiunzioni generalizzate.

Definizione 1.3.3: Quantificatore esistenziale

Se x è una variabile e $\varphi = \varphi(x)$ una formula, $\exists x(\varphi)$ esprime l'affermazione di *almeno una* tra le formule ($\varphi(a)$) ottenute sostituendo ad x ogni possibile valore a . Il simbolo \exists prende il nome di **quantificatore esistenziale**.

Oltre a \forall e \exists esistono altri quantificatori. Quello di uso più frequente è $\exists!$. Se φ è una formula ed x è una variabile, la formula “ $\exists!x(\varphi)$ ” si legge “esiste uno ed un solo x tale che φ ” ed afferma $\varphi(a)$ per uno dei possibili valori a che possono essere sostituiti ad x , negando $\varphi(b)$ per ogni b diverso da a . In modo più sintetico e più formale, se y è una variabile (diversa da x) che non appare in φ , questo quantificatore è definito dall'equivalenza:

$$\exists!x(\varphi(x)) \iff \exists x(\forall y(\varphi(y) \iff y = x)) \quad (1.28)$$

Siano φ una formula e x, y due variabili, e assumiamo che y non appaia in φ . Se chiamiamo $\psi(x, y)$ la formula

$$\varphi(y) \iff y = x$$

possiamo riscrivere l'equivalenza come:

$$\exists!x(\varphi(x)) \iff \exists x(\forall y(\psi(x, y)))$$

Vogliamo esaminare il membro a destra di questa equivalenza. Supponiamo che φ sia un predicato unario in x , quindi che $\exists x(\forall y(\psi(x, y)))$ sia una proposizione. Quando è che questa proposizione è vera? Esattamente quando esiste almeno un a per il quale sia vera la formula $\forall y(\psi(a, y))$; questo equivale a dire che è vera $\psi(a, b)$, cioè la formula $\varphi(b) \iff b = a$, per ogni possibile scelta di b .

Tra le possibili scelte per b c'è anche a ; la formula diventa in questo caso particolare $\varphi(a) \iff a = a$. Poiché $a = a$ è vera, questa equivale a $\varphi(a)$. Se invece scegliamo come b un qualsiasi oggetto diverso da a , allora $b = a$ è falsa, quindi $\varphi(b) \iff b = a$ equivale alla negazione di $\varphi(b)$.

In definitiva, abbiamo mostrato che la formula $\exists x(\forall y(\psi(x, y)))$ è vera se e solo se esiste un a per il quale è vera $\varphi(a)$ e, contemporaneamente, è falsa $\varphi(b)$ per ogni b diverso da a . Questo è precisamente quello che si vuole esprimere con il quantificatore $\exists!$.

1.3.2 ■ Occorrenze libere e vincolate

In una formula come:

$$\forall x(\dots)$$

o come

$$\exists x(\dots)$$

si dice che le *occorrenze* della variabile x all'interno dello *scope del quantificatore* (ovvero la parte della formula logica o del programma in cui il quantificatore è efficace) sono **vincolate** dal quantificatore \forall o dal quantificatore \exists .

Definizione 1.3.4: Occorrenza libera

Una variabile che non è vincolata da alcun quantificatore si dice ad **occorrenza libera**.

Esempio 1.3.2

Nella definizione appena data di occorrenze libere e vincolate si intende il fatto che ogni quantificatore può vincolare solo le occorrenze delle variabili che lo seguono immediatamente. In $\forall x(x = y)$ il quantificatore vincola solo le occorrenze della variabile x mentre le occorrenze della variabile y sono libere.

Esempio 1.3.3

Sono vincolate le occorrenze di x in $\forall x(x + 1 > x) \wedge (\exists x(x > y))$, mentre nella stessa formula è libera l'occorrenza di y .

Esempio 1.3.4

In una stessa formula possono esserci sia occorrenze libere che vincolate di una stessa variabile. Ad esempio in $(\forall x(x + 1 > x)) \vee (x = 0)$ l'ultima occorrenza di x è libera perché fuori dallo scope di ogni quantificatore.

Definizione 1.3.5: Formula chiusa

Una formula si dice **chiusa** se e solo se non contiene variabili con occorrenze libere.

Esempio 1.3.5

Formule del tipo $\exists x(x > y)$ non sono proposizioni a causa della presenza di variabili libere. Quindi non hanno un valore di verità. Per poter attribuire un valore di verità bisogna prima “quantificare” le variabili libere che vi appaiono facendo opportune modifiche.

1.3.3 ■ Sostituzioni

Per quanto riguarda le *sostituzioni* invece va detto che queste coinvolgono solo e soltanto le *occorrenze delle variabili libere presenti*.

Esempio 1.3.6

Sia “ $\varphi(x) : x > 1$ ” e consideriamo la sostituzione $\varphi(5)$ ottenuta eseguendo la sostituzione della variabile x con il simbolo 5. Si ottiene quindi la formula “ $5 > 1$ ” che ha un proprio valore di verità. Consideriamo adesso la formula “ $\psi(x) : (\forall x)(x > 1)$ ” dove è presente una occorrenza vincolata della variabile x . Provando ad eseguire la sostituzione di tutte le occorrenze della variabile x con il simbolo 5 si ottiene “ $\psi(5) : \forall 5(5 > 1)$ ” che è una formula priva di senso.

È buona norma scrivere le formule in modo che le variabili appaiano solo in forma libera o vincolata. Inoltre, cambiando il nome di una variabile vincolata, se non è presente anche in forma di occorrenza libera nella formula, allora la formula non cambia il suo valore di verità.

1.3.4 ■ Predicati

Definizione 1.3.6: Predicato

Un **predicato unario** nella variabile x è una formula che *non contiene* occorrenze libere di variabili diverse da x . Similmente, si dice che la formula φ è un **predicato binario** quando in essa appaiono al più due variabili con occorrenze libere.

Esempio 1.3.7

La formula $x = x$ è un predicato unario nella variabile x in quanto è una formula in cui occorre una sola variabile libera che è x . La formula $x = y$ è un predicato binario in quanto è una formula in cui occorrono due variabili libere che sono x e y .

1.3.5 ■ I quantificatori ristretti

Nella pratica matematica si incontrano spesso espressioni del tipo:

$$(\forall x \in \mathbb{R})(\alpha(x))$$

oppure:

$$(\exists x > 0)(\varphi)$$

in cui il quantificatore è accompagnato da una condizione che “limita” l’ambiente in cui la variabile può assumere valori. Queste formule sono abbreviazioni¹ di formule in cui i quantificatori sono usati nel metodo tradizionale. La prima formula può essere definita in questo modo:

$$(\forall x \in \mathbb{R})(\alpha(x)) : \iff \forall x(x \in \mathbb{R} \implies \alpha(x))$$

¹ Anche detto allargamento del linguaggio

Esempio 1.3.8

Quando ci si trova davanti a formule del tipo

$$\begin{aligned}\forall x \in \emptyset (x = x) \\ \forall x \in \emptyset (x \neq x)\end{aligned}$$

si stanno abbreviando formule del tipo:

$$\begin{aligned}\forall x(x \in \emptyset \implies x = x) \\ \forall x(x \in \emptyset \implies x \neq x)\end{aligned}$$

che risultano sempre vere in quanto implicazioni con antecedente falso.

Espressioni come $(\exists x \in S)(\varphi(x))$ abbreviano invece formule del tipo $\exists x(x \in S \wedge \varphi(x))$ e qui non dovrebbero esserci difficoltà: “esiste x in S tale che ...” significa proprio che “esiste x tale che x sia in S e ...”. Ovviamente, nella solita ipotesi che φ sia un predicato unario in x , questa formula è sicuramente una proposizione falsa quando $S = \emptyset$.

1.3.6 ■ Regole di manipolazione dei quantificatori

In matematica è molto comune trovare delle formule al cui interno sono presenti quantificatori annidati come segue:

$$\begin{aligned}\forall x(\forall y(\forall z(\cdots))) \\ \exists x(\exists y(\exists z(\cdots)))\end{aligned}$$

In questi casi è comodo abbreviare usando una notazione compatta del tipo:

$$\begin{aligned}\forall x, y, z(\cdots) &\text{ al posto di } \forall x(\forall y(\forall z(\cdots))) \\ \exists x, y, z(\cdots) &\text{ al posto di } \exists x(\exists y(\exists z(\cdots)))\end{aligned}$$

Le cose cambiano quando troviamo annidati sia il quantificatore esistenziale che quello universale. Le formule “ $\forall x(\exists y(\varphi))$ ” e “ $\exists y(\forall x(\varphi))$ ” non sono in generale equivalenti e non possono essere scambiate a proprio piacimento. La prima afferma che, scelto comunque un termine a , ne esiste almeno uno, b , dipendente, in generale, dalla scelta di a per il quale si abbia $\varphi(a, b)$. La seconda afferma qualcosa di più: che si ha la stessa situazione ma, questa volta, si può scegliere b indipendentemente dalla scelta di a : esiste un particolare b per il quale sia abbia $\varphi(a, b)$ per ogni possibile scelta di a . Dunque vale sempre l’implicazione:

$$\exists y(\forall x(\varphi)) \implies \forall x(\exists y(\varphi))$$

ma, in generale, non vale l’implicazione inversa.

Esempio 1.3.9

Nel linguaggio dell’aritmetica, sia $\varphi(x, y)$ la formula $x < y$. La prima delle nostre formule diventa:

$$\forall x(\exists y(x < y))$$

che afferma che per ogni numero esiste un numero più grande. Questa è una proposizione vera: se a è un numero intero, $a + 1$ è un numero intero maggiore di a , quindi $\varphi(a, a + 1)$ è vera. La seconda formula è invece:

$$\exists y(\forall x(x < y))$$

che afferma che esiste un intero (quello che andrebbe sostituito ad y) maggiore di tutti gli interi; questa è una proposizione falsa.

1.3.7 ■ Negazione dei quantificatori

Proposizione 1.3.1

Valgono le seguenti equivalenze logiche:

$$\neg(\forall x(\varphi(x))) \iff (\exists x(\neg\varphi(x))) \quad (1.29)$$

$$\neg(\exists x(\varphi(x))) \iff (\forall x(\neg\varphi(x))) \quad (1.30)$$

Dimostrazione. Lasciata al lettore come esercizio. □

Queste regole valgono in maniera analoga per i quantificatori ristretti con le dovute osservazioni:

$$\begin{aligned}\neg(\forall x \in S(\varphi(x))) &\iff \neg(\forall x(x \in S \implies \varphi(x))) \\ &\iff \exists x(\neg(x \in S \implies \varphi(x))) \\ &\iff \exists x(x \in S \wedge \neg\varphi(x))\end{aligned}$$

Analogamente:

$$\begin{aligned}\neg(\exists x \in S(\varphi(x))) &\iff \neg(\exists x(x \in S \wedge \varphi(x))) \\ &\iff \forall x(\neg(x \in S \wedge \varphi(x))) \\ &\iff \forall x(\neg(x \in S) \vee (\neg\varphi(x)))\end{aligned}$$

Proposizione 1.3.2

La negazione di $\exists!$ è data dalla seguente equivalenza:

$$\neg(\exists x(\forall y(\varphi(y) \iff x = y)) \iff \forall x(\exists y(\neg(\varphi(y) \iff x = y))) \quad (1.31)$$

Dimostrazione. Banale. □



Esercizio 1.4.1

Scrivere le tavole di verità di ciascuna delle forme proposizionali:

- “ $p \wedge p$ ”
- “ $(\neg p) \wedge q$ ”

Svolgimento.

p	p	$p \wedge p$
V	V	V
F	F	F

p	q	$\neg p$	$(\neg p) \wedge q$
V	V	F	F
V	F	F	F
F	V	V	V
F	F	V	F

Esercizio 1.4.2

Scrivere le tavole di verità delle forme proposizionali

1. “ $p \wedge (q \wedge r)$ ”
2. “ $p \wedge (q \wedge (\neg r))$ ”

Svolgimento.

p	q	r	$q \wedge r$	$p \wedge (q \wedge r)$
V	V	V	V	V
V	V	F	F	F
V	F	V	F	F
V	F	F	F	F
F	V	V	V	F
F	V	F	F	F
F	F	V	F	F
F	F	F	F	F

p	q	r	$\neg r$	$q \wedge (\neg r)$	$p \wedge (q \wedge (\neg r))$
V	V	V	F	F	F
V	V	F	V	V	V
V	F	V	F	F	F
V	F	F	V	F	F
F	V	V	F	F	F
F	V	F	V	V	F
F	F	V	F	F	F
F	F	F	V	F	F

Esercizio 1.4.3

Scrivere le tavole di verità di ciascuna delle forme proposizionali:

- $p \wedge (p \vee q)$

Svolgimento.

p	q	$p \vee q$	$p \wedge (p \vee q)$
V	V	V	V
V	F	V	V
F	V	V	F
F	F	F	F

Esercizio 1.4.4

Scrivere le tavole di verità di ciascuna delle forme proposizionali:

- $p \vee (p \wedge q)$
- $p \implies (\neg p)$
- $p \wedge (\neg q) \wedge r$

Svolgimento. Abbiamo:

p	q	$(p \wedge q)$	$p \vee (p \wedge q)$
V	V	V	V
V	F	F	V
F	V	F	F
F	F	F	F

p	$\neg p$	$(p \implies \neg p)$
V	F	F
F	V	V

p	q	r	$\neg q$	$p \wedge (\neg q) \wedge r$
V	V	V	F	F
V	V	F	F	F
V	F	V	V	V
V	F	F	V	F
F	V	V	F	F
F	V	F	F	F
F	F	V	V	F
F	F	F	V	F

Esercizio 1.4.5

Definiamo il connettivo **NAND** tra due proposizioni p e q , $p \uparrow q$ come $\neg(p \wedge q)$. Decidere se la forma proposizionale $(p \uparrow (q \uparrow r)) \iff ((p \uparrow q) \uparrow r)$ è una tautologia.

Svolgimento. È possibile dimostrare che tale formula non è una tautologia costruendo le tavole di verità. Si ha:

p	q	r	$q \uparrow r$	$p \uparrow (q \uparrow r)$
V	V	V	F	V
V	V	F	V	F
V	F	V	V	F
V	F	F	V	F
F	V	V	F	V
F	V	F	V	V
F	F	V	V	V
F	F	F	V	V

p	q	r	$p \uparrow q$	$(p \uparrow q) \uparrow r$
V	V	V	F	V
V	V	F	F	V
V	F	V	V	F
V	F	F	V	V
F	V	V	V	F
F	V	F	V	V
F	F	V	V	F
F	F	F	V	V

È possibile raggiungere lo stesso risultato ponendo $\alpha := (p \uparrow (q \uparrow r))$ e $\beta := ((p \uparrow q) \uparrow r)$ e supporre che α sia falsa. Essendo $p \uparrow q \iff \neg(p \wedge q)$ si ha che $p \uparrow q$ è falsa se sono vere entrambe le proposizioni p e q . Allora α è falsa se e solo se p e $q \uparrow r$ sono entrambe vere. Se $q \uparrow r$ è vera, allora almeno una tra q e r è falsa. Se q è falsa, allora $p \uparrow q$ è vera, dunque β è vera. Se r è falsa, allora $q \uparrow r$ è vera, dunque β è vera. In entrambi i casi β è vera, dunque $\alpha \iff \beta$ non è una tautologia. ■

Esercizio 1.4.6

Scrivere le tavole di verità di ciascuna delle forme proposizionali: “ $p \implies (p \vee q)$ ”, “ $(p \wedge q) \implies r$ ”, “ $(p \wedge q) \iff r$ ”.

Svolgimento. Possiamo costruire, per semplicità, una singola tabella per il calcolo delle tre proposizioni. Si ha quindi:

p	q	r	$p \wedge q$	$p \vee q$	$p \implies (p \vee q)$	$(p \wedge q) \implies r$	$(p \wedge q) \iff r$
V	V	V	V	V	V	V	V
V	V	F	V	V	V	F	F
V	F	V	F	V	V	V	F
V	F	F	F	V	V	V	V
F	V	V	F	V	V	V	F
F	V	F	F	V	V	V	V
F	F	V	F	F	V	V	F
F	F	F	F	F	V	V	V

Esercizio 1.4.7

Verificare se $(t \wedge (\neg v) \vee m) \iff (t \wedge (v \implies m))$.

Svolgimento. Dimostriamo costruendo la tavola di verità:

t	v	m	$t \wedge (\neg v) \vee m$	$t \wedge (v \implies m)$
V	V	V	V	V
V	V	F	F	F
V	F	V	V	V
V	F	F	V	V
F	V	V	F	F
F	V	F	F	F
F	F	V	F	F
F	F	F	F	F

Confrontando le colonne si ha l'asserto. ■

Esercizio 1.4.8

Stabilire i valori di verità delle formule e frasi (assumiamo nota la matematica elementare coinvolta): “ $(1+1=0) \wedge (0+0=0)$ ”; “ $(1+1=0) \vee (0+0=0)$ ”; “ $(1+1=0) \implies (0+0=0)$ ”; “ $\sqrt{2}$ è un numero razionale o un numero irrazionale”; “ $2^5 = 32 \implies 47 - 1 = 46$ ”.

Svolgimento.

1. “ $(1+1=0) \wedge (0+0=0)$ ” risulta vera in quanto falsa l'antecedente.
2. “ $(1+1=0) \vee (0+0=0)$ ” risulta vera;
3. “ $(1+1=0) \implies (0+0=0)$ ” risulta vera;
4. “ $\sqrt{2}$ è un numero razionale o un numero irrazionale” è vera;
5. “ $2^5 = 32 \implies 47 - 1 = 46$ ” è vera.

Esercizio 1.4.9

È molto importante saper “tradurre” espressioni del linguaggio ordinario (della lingua italiana) in linguaggio “semiformalizzato”, riconoscendo la presenza ed il ruolo dei connettivi proposizionali contenuti nelle frasi. Ad esempio, se indichiamo con α la frase “domani pioverà” e con β la frase “domani prenderò l'ombrelllo”, si può rendere con $\alpha \wedge \beta$ la frase “domani pioverà e prenderò l'ombrelllo”. Fare lo stesso con le frasi:

- Il supermercato era aperto e non ci sono entrato.
- Il supermercato era aperto ma non ci sono entrato.
- Se vedo Nicola lo saluto.
- Se domenica non piove e vado a Roma, $2 > 1$, ma se Marco mangia la pizza allora certamente fioriranno le rose.

Svolgimento.

Si ha:

- Posto α : “Il supermercato era aperto” e β : “Ci sono entrato” si ottiene: $\alpha \wedge \neg\beta$;
- Posto α : “Il supermercato era aperto” e β : “Ci sono entrato” si ottiene: $\alpha \wedge \neg\beta$;
- Posto α : “Vedo Nicola” e β : “Lo saluto” si ottiene: $\alpha \implies \beta$;
- Posto α : “Domenica piove”, β : “Vado a Roma”, γ : “ $2 > 1$ ”, δ : “Marco mangia la pizza” e ζ : “Fioriscono le rose” si ottiene: $((\neg\alpha \wedge \beta) \implies \delta) \wedge (\theta \implies \zeta)$.

Esercizio 1.4.10

Spiegare la seguente storiella: la moglie del logico chiede al marito: “Caro, stasera usciamo o restiamo a casa?”. Il marito risponde “Sì.”.

Svolgimento. Il marito ha risposto “sì” perché la frase “stasera usciamo o restiamo a casa” è una proposizione composta da una singola proposizione logica, p , congiunta dalla disunione esclusiva: $p \vee (\neg p)$ che risulta essere una tautologia. La risposta del marito non può essere quindi che affermativa. ■

Esercizio 1.4.11

Verificare la tautologia $(p \implies (q \implies r)) \iff ((p \implies q) \implies (p \implies r))$ (distributività da sinistra dell'implicazione rispetto a sé stessa).

Svolgimento. Sia $\alpha := (p \implies (q \implies r))$ e $\beta := ((p \implies q) \implies (p \implies r))$. Verifichiamo che $\alpha \iff \beta$ non può essere mai falsa. Per essere falsa devono assumere valore diverso, per ogni valore di p, q, r , le due formule. Sia quindi α falsa e β vera. Si ha quindi che sia p che $q \implies r$ hanno valore falso. Quindi q ha valore vero ed r assume valore falso. In questa situazione si ha che $p \implies q$ è vera e $p \implies r$ è falsa. Quindi β è falsa, trovando una contraddizione. Viceversa, sia α vera e β falsa. Procedendo in maniera analoga si ottiene che p e q sono vere mentre r è falsa. Allora, stando questi valori, α è falsa, contro le ipotesi iniziali e quindi α e β non assumono mai valori logicamente diversi. ■

Esercizio 1.4.12

Negare ciascuna delle frasi: "Mario corre e Maria nuota", "La bottiglia è vuota oppure tappata".

Svolgimento. Poniamo α : "Mario corre" e β : "Mario nuota". La frase "Mario corre e Mario nuota" corrisponde quindi a $\alpha \wedge \beta$. Per negare la frase si procede quindi nel seguente modo:

$$\neg(\alpha \wedge \beta) \iff \neg(\alpha) \vee \neg(\beta)$$

ovvero: "Mario non corre oppure non nuota". Analogamente, posto α : "La bottiglia è vuota" e β : "La bottiglia è tappata" si ha:

$$\neg(\alpha \vee \beta) = \neg(\alpha) \wedge \neg(\beta)$$

Ovvero: "La bottiglia non è vuota e non è tappata". ■

Esercizio 1.4.13

Negare la frase: "Alice ha i capelli biondi ricci". (Si chiede che anche la negazione inizi con "Alice ha i capelli...")

Svolgimento. La frase "Alice ha i capelli biondi ricci" cela al suo interno una congiunzione, infatti Alice ha i capelli biondi e i capelli ricci. Quindi, posto α : "Alice ha i capelli biondi" e β : "Alice ha i capelli ricci", la frase diventa $\alpha \wedge \beta$ la cui negazione è $\neg(\alpha \wedge \beta) = \neg(\alpha) \vee \neg(\beta)$, ovvero "Alice ha i capelli mori oppure ha i capelli lisci". ■

Esercizio 1.4.14

Usando le leggi di De Morgan, negare $p \wedge (\neg(q \wedge (\neg p)))$. Ciò che si chiede è scrivere una formula che sia equivalente alla negazione di quella data e che non abbia \neg come primo simbolo.

Svolgimento. Si ha:

$$\begin{aligned} \neg(p \wedge (\neg(q \wedge (\neg p)))) &\iff \neg(p \wedge (\neg(q) \vee p)) && \text{Applicando De Morgan a } \neg(q \wedge (\neg p)) \\ &\iff (\neg(p) \vee \neg(\neg(q) \vee p)) && \text{Applicando De Morgan all'intero membro} \\ &\iff (\neg(p) \vee (\neg(\neg q) \wedge \neg(p))) && \text{Applicando De Morgan a } \neg(\neg q) \vee p \\ &\iff (\neg(p) \vee (q \wedge \neg(p))) && \text{Per la doppia negazione} \\ &\iff ((\neg(p) \vee q) \wedge (\neg(p) \vee \neg(p))) && \text{Per la distributività di } \vee \text{ rispetto a } \wedge \\ &\iff ((\neg(p) \vee q) \wedge \neg(p)) && \text{Per idempotenza} \end{aligned}$$

Esercizio 1.4.15

Come per l'esercizio precedente, negare ciascuna delle due formule: " $p \wedge q \wedge r$ " e " $(p \vee q) \wedge ((p \vee r) \wedge (q \vee s))$ "

Svolgimento. Si ha:

$$\bullet \quad \neg(p \wedge q \wedge r) \iff (\neg(p) \vee \neg(q) \vee \neg(r))$$

$$\bullet \neg((p \vee q) \wedge ((p \vee r) \wedge (q \vee s))) \iff (\neg(p \vee q) \vee \neg((p \vee r) \wedge (q \vee s))) \iff ((\neg(p) \wedge \neg(q)) \vee (\neg(p \vee r) \vee \neg(q \vee s))) \iff$$

$$((\neg(p) \wedge \neg(q)) \vee ((\neg(p) \wedge \neg(r)) \vee (\neg(q) \wedge \neg(s))))$$

Esercizio 1.4.16

Negare le frasi “Se piove mi bagno”, “Se piove non mi bagno”, “Se piove, mi bagno e mi ammalo”.

Svolgimento. Poniamo per semplicità α : “Piove”, β : “Mi bagno”, δ : “Mi ammalo”. Allora:

- “Se piove mi bagno” = $\alpha \implies \beta$. E vale $\neg(\alpha \implies \beta) = \alpha \wedge \neg(\beta)$, ovvero “Piove e non mi bagno”;
- “Se piove non mi bagno” = $\alpha \implies (\neg(\beta))$, si ha:

$$\begin{aligned} \neg(\alpha \implies (\neg(\beta))) &\iff \alpha \wedge \neg(\neg(\beta)) \\ &\iff \alpha \wedge \beta \end{aligned}$$

Ovvero “Piove e mi bagno”;

- “Se piove, mi bagno e mi ammalo” = $\alpha \implies (\beta \wedge \delta)$. Si ha:

$$\begin{aligned} \neg(\alpha \implies (\beta \wedge \delta)) &\iff \alpha \wedge \neg(\beta \wedge \delta) \\ &\iff \alpha \wedge (\neg(\beta) \vee \neg(\delta)) \end{aligned}$$

ovvero: “Piove eppure o non mi bagno o non mi ammalo”.

Esercizio 1.4.17

Abbiamo dimostrato la distributività di \wedge rispetto a $\dot{\vee}$. Verificare che \vee non è distributivo rispetto a $\dot{\vee}$, vale a dire:

$$(p \vee (q \dot{\vee} r)) \iff ((p \vee q) \dot{\vee} (p \vee r))$$

non è una tautologia. Analogamente, \vee è distributivo rispetto a \iff ? Ovvero:

$$(p \vee (q \iff r)) \iff ((p \vee q) \iff (p \vee r))$$

è una tautologia?

Svolgimento. Dimostriamo che \vee non è distributivo rispetto a $\dot{\vee}$ costruendo le tavole di verità. Poniamo $\alpha : (p \vee (q \dot{\vee} r))$ e $\beta : ((p \vee q) \dot{\vee} (p \vee r))$.

p	q	r	$q \dot{\vee} r$	$p \vee q$	$p \vee r$	α	β
V	V	V	F	V	V	V	F
V	V	F	V	V	V	V	F
V	F	V	V	V	V	V	F
V	F	F	F	V	V	V	F
F	V	V	F	V	V	F	F
F	V	F	V	V	F	V	V
F	F	V	V	F	V	V	V
F	F	F	F	F	F	F	V

Esercizio 1.4.18

Negare “Se esco di casa o mi affaccio al balcone, vedo Maria e Franco”.

Svolgimento. Possiamo tradurre la frase ponendo α : “Esco di casa”, β : “Mi affaccio al balcone”, δ : “Vedo Maria”, θ : “Vedo Franco”. Quindi: $(\alpha \vee \beta) \implies (\delta \wedge \theta)$. Per negare:

$$\begin{aligned} \neg((\alpha \vee \beta) \implies (\delta \wedge \theta)) &\iff (\alpha \vee \beta) \wedge \neg(\delta \wedge \theta) \\ &\iff (\alpha \vee \beta) \wedge (\neg(\delta) \vee \neg(\theta)) \end{aligned}$$

Applicando De Morgan

Quindi una possibile proposizione che nega la formula proposta può essere: "Nonostante esca di casa o mi affacci al balcone comunque non vedo Maria o Franco".

Esercizio 1.4.19

Negare la forma proposizionale $(p \vee q) \implies (r \wedge s)$.

Svolgimento. Si ha:

$$\begin{aligned} \neg((p \vee q) \implies (r \wedge s)) \\ \iff (p \vee q) \wedge \neg(r \wedge s) \\ \iff (p \vee q) \wedge (\neg(r) \vee \neg(s)) \end{aligned}$$

Applicando De Morgan

Esercizio 1.4.20

Vero o falso? E perché? Questo è un esercizio di corretta lettura ed interpretazione di formule.

1. $(\forall x \in \mathbb{N})(x + 1 < x \implies x^2 = 1)$
2. $(\exists x \in \mathbb{N})(\forall y \in \mathbb{N}(x \leq y))$
3. $(\forall x \in \mathbb{N})(\exists y \in \mathbb{N}(x < y))$
4. $(\forall x \in \mathbb{N})(\exists y \in \mathbb{N}((x = y + 1) \implies (x < y)))$
5. $(\exists x \in \mathbb{N})(\forall y \in \mathbb{N}((x < y) \vee (y < x) \vee (y = 11)))$
6. $(\exists x \in \mathbb{N})(\forall y \in \mathbb{Z}((x \neq y) \implies (x < y)))$
7. Ogni numero reale il cui quadrato sia negativo è maggiore di 10^{327} .

Svolgimento.

1. L'espressione risulta essere una formula vera in quanto l'implicazione $(x + 1 < x \implies x^2 = 1)$ è sempre vera in quanto l'antecedente è falsa.
2. L'espressione afferma l'esistenza di un numero naturale minore od uguale a ciascun $y \in \mathbb{N}$. Tale elemento esiste (lo zero) e quindi la formula risulta vera.
3. Al contrario questa espressione risulta falsa in quanto non esiste un elemento in \mathbb{N} minore di ciascun elemento di \mathbb{N} .
4. La formula esprime l'esistenza, per ogni numero naturale $x \in \mathbb{N}$, di un y che sia il suo successore il che è sempre vero.
5. La formula risulta vera in quanto, esiste un numero naturale il quale per ogni $y \in \mathbb{N}$ è sempre vera la proposizione $(x < y) \vee (y < x) \vee (y = 11)$. Infatti, preso $x = 11$ la proposizione è vera.
6. La formula risulta falsa. Non esiste infatti un naturale per il quale, per ogni numero intero relativo, se $x \neq y$ allora $x < y$. Basta infatti considerare il seguente controsenso: sia $x = 3$ e $y = 1$ allora $x \neq y$ ma $x > y$.
7. La formula è vera in quanto l'implicazione è vera in quanto l'antecedente è falso.

Esercizio 1.4.21

Verificare (in modo diretto) la formula $\neg(\exists x \in S)(\varphi) \iff \forall(x \in S)(\neg\varphi)$.

Svolgimento. Per dimostrare in maniera diretta la formula basta considerare il caso in cui questa sia falsa.

Infatti per avere un'implicazione falsa basta che sia vera l'antecedente e falsa la formula conseguente. Negando la conseguente si ottiene

$$\neg(\neg(\exists x \in S)(\varphi)) \iff \exists x \in S(\varphi)$$

che è coerente con la formula $(\forall x \in S)(\varphi)$. Infatti se tale predicato φ valesse per ogni elemento dell'insieme S allora certamente esisterebbe almeno un elemento x in S per il quale il predicato sia verificato. Per questo motivo allora possiamo dire che la formula originale è falsa.

Esercizio 1.4.22

Si neghi ciascuna delle formule (le notazioni sono le solite):

1. $\forall x(\exists y(\varphi(x, y) \implies \psi(x, y)))$
2. $\exists x(\varphi(x) \wedge \forall y(\neg\psi(x, y)))$
3. $\forall x, y(\exists z(z \neq y \wedge \varphi(x, z)))$

Svolgimento. Si ha:

1. Si procede negando dall'esterno verso l'interno.

$$\neg \left(\forall x \left(\exists y (\varphi(x, y) \implies \psi(x, y)) \right) \right)$$

che è equivalente a:

$$\exists x \left(\neg \left(\exists y (\varphi(x, y) \implies \psi(x, y)) \right) \right)$$

Quindi si nega il quantificatore esistenziale all'interno:

$$\exists x \left(\forall y \left(\neg (\varphi(x, y) \implies \psi(x, y)) \right) \right)$$

ed infine si nega l'implicazione:

$$\exists x \left(\forall y (\varphi(x, y) \wedge (\neg \psi(x, y))) \right)$$

2. Neghiamo $\exists x (\varphi(x) \wedge \forall y (\neg \psi(x, y)))$:

$$\begin{aligned} \neg \left(\exists x (\varphi(x) \wedge \forall y (\neg \psi(x, y))) \right) &\iff \forall x \left(\neg (\varphi(x) \wedge \forall y (\neg \psi(x, y))) \right) \\ &\iff \forall x \left(\neg \varphi(x) \vee \neg (\forall y (\neg \psi(x, y))) \right) \\ &\iff \forall x \left(\neg \varphi(x) \vee \exists y (\neg (\neg \psi(x, y))) \right) \\ &\iff \forall x \left(\neg \varphi(x) \vee \exists y (\psi(x, y)) \right) \end{aligned}$$

3. Abbiamo:

$$\begin{aligned} \neg \left(\forall x, y \left(\exists z (z \neq y \wedge \varphi(x, z)) \right) \right) &\iff \exists x, y \left(\neg \left(\exists z (z \neq y \wedge \varphi(x, z)) \right) \right) \\ &\iff \exists x, y \left(\forall z \left(\neg (z \neq y \wedge \varphi(x, z)) \right) \right) \\ &\iff \exists x, y \left(\forall z \left(\neg (z \neq y) \vee \neg (\varphi(x, z)) \right) \right) \end{aligned}$$

Esercizio 1.4.23

Negare: $\exists x \in y (x = y \iff x \in y)$.

Svolgimento. Sviluppiamo la formula seguendo la definizione di quantificatore limitato:

$$\exists x \in y (x = y \iff x \in y) \iff \exists x (x \in y \wedge (x = y \iff x \in y))$$

e neghiamo:

$$\begin{aligned} \neg \left(\exists x (x \in y \wedge (x = y \iff x \in y)) \right) &\iff \forall x \left(\neg (x \in y \wedge (x = y \iff x \in y)) \right) \\ &\iff \forall x \left(\neg (x \in y) \vee \neg (x = y \iff x \in y) \right) \\ &\iff (x \notin y \vee (x \neq y \iff x \in y)) \end{aligned}$$

Esercizio 1.4.24

Negare: $\forall x \in \mathbb{N} (0 + x = 1 + x)$.

Svolgimento. Sviluppiamo la formula seguendo la definizione di quantificatore limitato:

$$\forall x(x \in \mathbb{N} \implies (0 + x = 1 + x))$$

e neghiamo:

$$\begin{aligned}\neg(\forall x(x \in \mathbb{N} \implies (0 + x = 1 + x))) &\iff \exists x(\neg(x \in \mathbb{N} \implies 0 + x = 1 + x)) \\ &\iff \exists x(x \in \mathbb{N} \wedge 0 + x \neq 1 + x)\end{aligned}$$

■

TEORIA DEGLI INSIEMI

2.1

DEFINIZIONE E RAPPRESENTAZIONE DEGLI INSIEMI



Il concetto di insieme è un concetto primitivo, ovvero non è possibile definirlo in termini di altri concetti. Un insieme è una collezione di oggetti, detti elementi, che possono essere di qualsiasi tipo. Agli albori della teoria degli insiemi si pensava che ogni insieme fosse l'**estensione di un predicato**, ovvero l'insieme di tutti gli oggetti che soddisfano una determinata proprietà.

Definizione 2.1.1: Estensione di un predicato

Sia $\varphi = \varphi(x)$ un predicato unario nella variabile x . Si indica col simbolo $E_\varphi = \{x \mid \varphi\}$ la totalità degli oggetti a che, sostituiti ad x in φ , rendono φ vera ($\varphi(a)$ è una formula vera). Questa totalità prende il nome di **estensione** di φ che può essere anche scritta mediante la formula:

$$\forall x(x \in E_\varphi \iff \varphi(x)) \quad (2.1)$$

Il tentativo di fondare l'intera teoria sull'idea che l'estensione di ogni predicato unario si potesse considerare come insieme fallì non appena si scoprì che questa assunzione portava necessariamente a delle contraddizioni. Non sempre infatti l'estensione $\{x \mid \varphi\}$ di un predicato φ è un insieme¹ come dimostrò Bertrand Russell mediante il suo omonimo paradosso. Limitando però la ricerca degli oggetti ai soli elementi di un insieme s allora sicuramente è possibile considerare l'insieme degli elementi di s che verificano quella data proprietà φ . Questo è assicurato da uno degli assiomi della teoria degli insiemi, ovvero l'**assioma di separazione**.

Assioma 2.1.1 Axioma di separazione

Dati un insieme s ed un predicato unario φ nella variabile x , la formula " $(x \in s) \wedge \varphi$ " è ancora un predicato unario e in particolare, l'estensione

$$\{x \mid (x \in s) \wedge \varphi(x)\}$$

di questo predicato è un insieme.

Per indicare questo insieme si usa, in genere, una notazione compatta: $\{x \in s \mid \varphi(x)\}$. L'insieme così ottenuto è ovviamente una parte di s .

Esempio 2.1.1

Non hanno alcun senso espressioni quali:

- $X = \{\text{multipli di due}\}$
- $Y = \{\text{numeri naturali grandi}\}$
- $Z = \{\text{Soluzioni di } x^4 - 1 = 0\}$

Nella teoria degli insiemi standard si assume abitualmente che *non esistano enti matematici che non siano insiemi*. Quindi da questo punto in poi si adotterà la convenzione secondo la quale ogni cosa sia un insieme. Espressioni come " $\forall a, b$ " intenderanno

¹Esistono proprietà perfettamente ragionevoli e ben definite tali che non esista l'insieme degli oggetti che le verificano.

quindi a e b come insiemi².

Assioma 2.1.2 Assioma di estensionalità

Dati un insieme a e un insieme b , si ha:

$$\forall a, b \quad \left(a = b \iff (\forall x(x \in a \iff x \in b)) \right) \quad (2.2)$$

Questo assioma stabilisce che gli insiemi sono completamente determinati dai loro elementi, ovvero dati un insieme a e un insieme b , si ha $a = b$ se e solo se a e b hanno esattamente gli stessi elementi. La scrittura $a \neq b$ indicherà invece la negazione dell'assioma appena visto:

$$a \neq b \iff \neg(a = b) \iff \neg(\forall x(x \in a \iff x \in b)) \iff \exists x(x \in a \vee x \in b)$$

Ovvero, due insiemi sono diversi se esiste almeno un elemento che si trova solo in uno dei due insiemi. Per esprimere la condizione di **appartenenza** si è utilizzato il simbolo “ \in ”. Per denotare che l'elemento x non è un elemento di un insieme a si usa il simbolo $x \notin a$.

Lemma 2.1.1

Siano $h = \{x | \varphi(x)\}$ e $k = \{x | \psi(x)\}$ due insiemi. L'assioma di estensionalità si può esprimere anche nella forma seguente:

$$h = k \iff \left(\forall x(\varphi(x) \iff \psi(x)) \right) \quad (2.3)$$

Esempio 2.1.2

Gli insiemi $a = \{x | x \in \mathbb{N} \wedge x > 3\}$ e $b = \{x | x \in \mathbb{N} \wedge x \geq 4\}$ sono equivalenti. Infatti:

$$\forall x \left((x \in \mathbb{N} \wedge x > 3) \iff (x \in \mathbb{N} \wedge x \geq 4) \right)$$

Consideriamo un insieme V definito ponendo $V = \{x \in \mathbb{R} / x^2 = -1\}$. Chiaramente V è perfettamente definito e rappresenta effettivamente un insieme. Poiché nessun numero reale ha quadrato negativo, l'insieme V risulta non avere alcun elemento, ovvero:

$$\nexists x \in \mathbb{R} (x \in V)$$

V prende il nome di **insieme vuoto** e sarà denotato con il simbolo \emptyset .

Lemma 2.1.2

L'insieme vuoto è unico.

Dimostrazione. Banale. □

Osserviamo che l'insieme vuoto può essere definito come l'insieme:

$$\emptyset := \{x \mid x \neq x\} \quad (2.4)$$

Osservazione 2.1.1

Risulta vera la formula:

$$(\forall x \in \emptyset)(x \neq x)$$

in quanto può essere riscritta come:

$$\forall x(x \in \emptyset \implies x \neq x)$$

e ricordiamo che ogni implicazione con antecedente falso è vera. Analogamente, la formula:

$$(\exists x \in \emptyset)(\varphi)$$

è falsa perché è possibile riscriverla come:

$$\exists x(x \in \emptyset \wedge \varphi)$$

ed, essendo $x \in \emptyset$ falsa, la congiunzione risulta falsa.

²Non avrà alcun senso *fissare* alcuna notazione secondo la quale i simboli in minuscolo rappresenterebbero elementi mentre quelli in minuscolo degli insiemi. Ciò nonostante, per questioni di leggibilità (e non di formalismo semantico), nel corso della dispensa sarà possibile trovare nomi di insieme denotati con lettere maiuscole.

Definizione 2.1.2: Singleton di un elemento

Se a è un insieme, l'insieme $\{a\}$ costituito dal solo insieme a prende il nome di **singleton** di a .

In particolare, dato l'assioma di estensionalità (Assioma 2.1.2):

$$\forall x(x \in \{a\} \iff x = a)$$

e soprattutto:

$$\forall a(a \neq \{a\})$$

Infatti l'insieme a può essere vuoto quanto contenere infiniti elementi, mentre l'insieme $\{a\}$ contiene sempre uno ed un solo elemento, ovvero l'insieme a stesso. Vale piuttosto: $\forall a(a \in \{a\})$.

2.1.1 Rappresentazione degli insiemi

Esistono diversi modi per rappresentare un insieme. Il modo più semplice è quello di elencare i suoi elementi tra parentesi graffe. Ad esempio, l'insieme $a = \{1, 2, 3\}$ è l'insieme che contiene gli elementi 1, 2 e 3. Questo metodo di rappresentazione è però limitato a insiemi finiti. Per rappresentare insiemi infiniti si usa invece la notazione detta **elenco caratteristico** che si limita a descrivere la proprietà che caratterizza gli elementi dell'insieme.

Ad esempio, l'insieme $b = \{x \in \mathbb{N} \mid x \geq 4\}$ è l'insieme dei numeri naturali maggiori o uguali a 4. Un altro modo per rappresentare un insieme è mediante i cosiddetti **diagrammi di Eulero-Venn**, che sono dei diagrammi che rappresentano gli insiemi come regioni del piano.

Esempio 2.1.3

Consideriamo l'insieme $c = \{x \in \mathbb{N} \mid x \leq 4\}$. c può essere rappresentato come mostrato in figura 2.1.

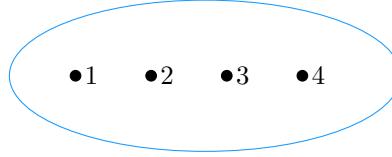


Figura 2.1: Diagramma di Eulero-Venn per l'insieme c

2.2

NOTAZIONE INSIEMISTICA



2.2.1 Sottoinsiemi e relazione di inclusione

Definizione 2.2.1: Sottoinsiemi

Siano a e b due insiemi, si dice che a è **incluso** in b se vale

$$\forall a, b(a \subseteq b \iff \forall x(x \in a \implies x \in b)) \quad (2.5)$$

In questo caso si dice anche che a è una **parte** di b o anche un **sottoinsieme**.

Osservazione 2.2.1



Una semplice conseguenza di questa definizione è che $\emptyset \subseteq \emptyset$. Infatti l'implicazione:

$$\forall x(x \in \emptyset \implies x \in \emptyset)$$

è vera in quanto la sua antecedente è falsa.

Analogamente a quanto osservato precedentemente, è vera anche la formula $\forall x(\emptyset \subseteq x)$. Infatti la condizione di inclusione richiede che ogni elemento dell'insieme vuoto appartenga anche all'insieme x ma, poiché nell'insieme vuoto non ci sono elementi, la prima proposizione dell'implicazione risulta sempre falsa e questo rende vera la condizione. Da ciò si può concludere affermando

che l'*insieme vuoto* è *sottoinsieme di tutti gli insiemi*. In maniera analoga è possibile dimostrare che $\forall x(x \subseteq x)$. Ovvero, ogni insieme è sottoinsieme di sé stesso. Dato un insieme s , indicheremo s e \emptyset come i **sottoinsiemi banali** di s .

Lemma 2.2.1

Siano $h = \{x|\varphi(x)\}$ e $k = \{x|\psi(x)\}$ due insiemi. La condizione di inclusione $h \subseteq k$ si può esprimere come:

$$(h \subseteq k) \iff \forall x(\varphi(x) \implies \psi(x)) \quad (2.6)$$

Definizione 2.2.2: Sottoinsiemi propri

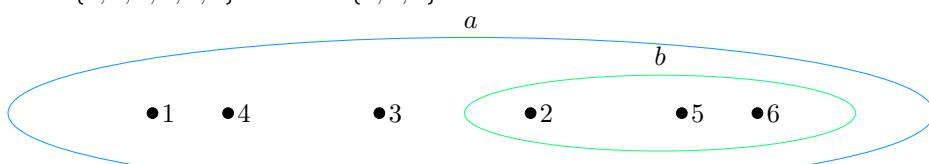
Siano a, b insiemi. Diremo che a è **incluso strettamente** in (oppure che è un **sottoinsieme proprio**) b se e soltanto se:

$$a \subseteq b \wedge a \neq b \quad (2.7)$$

Ovvero se ogni elemento di a è presente in b ma esiste almeno un elemento di b che non appartiene ad a .

Esempio 2.2.1

Si consideri l'insieme $a = \{1, 2, 3, 4, 5, 6\}$ e sia $b = \{2, 5, 6\}$.



Da come è osservabile nel diagramma di Venn, l'insieme b è un sottoinsieme proprio di a : $b \subset a$.

2.2.2 ■ L'insieme delle parti

Nella teoria degli insiemi è difficile stabilire quali insiemi esistano e quali no. Esistono, però, particolari insiemi per i quali l'esistenza è assolutamente certificata. L'**insieme delle parti** di un insieme è uno di questi insiemi.

Definizione 2.2.3: Insieme delle parti

Supponiamo che x sia un insieme. Con $\mathcal{P}(x)$ si denota l'**insieme delle parti** di x . Questo insieme è composto dall'insieme vuoto e da tutti i possibili sottoinsiemi di x :

$$\mathcal{P}(x) = \{y / y \subseteq x\} \quad (2.8)$$

Questo insieme è sicuramente non vuoto, e quindi esistente, in quanto per ogni insieme x il suo insieme delle parti conterrà sempre almeno x e l'insieme vuoto³:

$$\forall x(x \in \mathcal{P}(x) \wedge \emptyset \in \mathcal{P}(x))$$

Esempio 2.2.2

Se $a = \{1, 2, 3\}$, allora:

$$\mathcal{P}(a) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Teorema 2.2.1 (Tautologia della doppia implicazione)

Siano a, b insiemi. Vale la seguente tautologia:

$$a = b \iff ((a \subseteq b) \wedge (b \subseteq a)) \quad (2.9)$$

Dimostrazione. La tautologia della doppia implicazione assicura che:

$$x \in a \iff x \in b$$

è equivalente a:

$$(x \in a \implies x \in b) \wedge (x \in b \implies x \in a)$$

³a meno che non siano lo stesso insieme

Inoltre, dalle regole del calcolo dei predicati vale:

$$(\forall x(\phi \wedge \psi)) \iff ((\forall x(\phi)) \wedge (\forall x(\psi)))$$

Qualsiasi siano le formule ϕ e ψ . Abbiamo allora le equivalenze:

$$\begin{aligned} a = b &\iff \forall x(x \in a \iff x \in b) && \text{Per l'Assioma 2.1.2} \\ &\iff \forall x((x \in a \implies x \in b) \wedge (x \in b \implies x \in a)) && \text{Per la Proposizione 1.2.3} \\ &\iff (\forall x(x \in a \implies x \in b)) \wedge (\forall x(x \in b \implies x \in a)) \\ &\iff (a \subseteq b) \wedge (b \subseteq a) && \text{Per definizione 2.5} \end{aligned}$$

□

Osservazione 2.2.2 ➤➤

Grazie a questa tautologia, per dimostrare l'uguaglianza tra due insiemi sarà sufficiente verificare la **doppia inclusione** tra i due invece del confronto diretto degli elementi.

In maniera del tutto analoga a quanto appena visto, la tautologia della transitività (Formula 1.18) fornisce la **transitività dell'inclusione**:

Proposizione 2.2.1 (Transitività dell'inclusione)

Siano a, b, c insiemi. Se $a \subseteq b$ e $b \subseteq c$ allora $a \subseteq c$. Vale cioè:

$$(\forall a, b, c) \quad \left((a \subseteq b) \wedge (b \subseteq c) \right) \implies (a \subseteq c) \quad (2.10)$$

2.3

OPERAZIONI INSIEMISTICHE



2.3.1 ■ Intersezione

Definizione 2.3.1: Intersezione

Siano a, b insiemi. Si definisce **intersezione** tra a e b l'insieme così definito:

$$a \cap b = \{x : x \in a \wedge x \in b\} \quad (2.11)$$

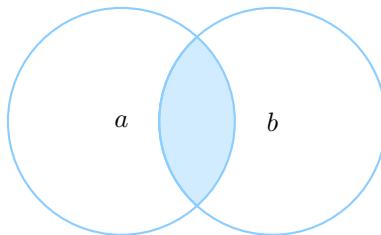


Figura 2.2: $a \cap b$

Esempio 2.3.1

- Si considerino gli insiemi $a = \{3, 4, 5, 6\}$ e $b = \{3, 4, 6, 7\}$. Si avrà:

$$a \cap b = \{3, 4, 6\}$$

- Sia $V = \{2, 4, 6, \dots\}$ l'insieme dei multipli di 2, mentre $W = \{3, 6, 9, \dots\}$ l'insieme dei multipli di 3. Allora:

$$V \cap W = \{6, 12, 18, \dots\}$$

Ossia l'insieme dei multipli di 6.

Osservazione 2.3.1



1. $a \cap b$ è contenuto, quale sottoinsieme, tanto in a che in b :

$$(a \cap b) \subseteq a \wedge (a \cap b) \subseteq b$$

2. Se due insiemi non hanno elementi comuni, se in altri termini, $a \cap b = \emptyset$, allora si dice che i due insiemi sono **disgiunti**.

2.3.2 Unione

Definizione 2.3.2: Unione

Siano a, b insiemi. Si definisce **unione** tra a e b l'insieme così definito:

$$a \cup b = \{x | x \in a \vee x \in b\} \quad (2.12)$$

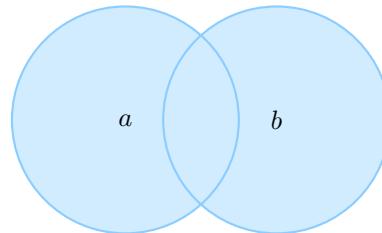


Figura 2.3: $a \cup b$

Esempio 2.3.2

Si considerino gli insiemi $a = \{3, 4, 5, 6\}$ e $b = \{3, 4, 6, 7\}$. Si avrà:

$$a \cup b = \{3, 4, 5, 6, 7\}$$

Osservazione 2.3.2



Tanto a quanto b sono sempre sottoinsiemi di $a \cup b$, ossia:

$$a \subset (a \cup b) \wedge b \subset (a \cup b)$$

Dato un insieme $a = \{x | \varphi(x)\}$ e $b = \{y | \psi(y)\}$, le operazioni insiemistiche appena viste possono essere tradotte con i connettivi logici applicati ai predicati dei relativi insiemi. Si avrà quindi:

$$a \cap b \iff \varphi \wedge \psi$$

$$a \cup b \iff \varphi \vee \psi$$

Dalle tautologie d'idempotenza, commutatività e associatività (Vedi 1.2) e le leggi distributive per \wedge e \vee si ottengono le analoghe proprietà per le operazioni di unione e intersezione tra insiemi.

Proposizione 2.3.1

Per ogni insieme a, b, c valgono le seguenti proprietà:

$$a = a \cap a, \quad a \cap b = b \cap a, \quad a \cap (b \cap c) = (a \cap b) \cap c, \quad (2.13)$$

$$a = a \cup a, \quad a \cup b = b \cup a, \quad a \cup (b \cup c) = (a \cup b) \cup c \quad (2.14)$$

che esprimono l'**idempotenza**, la **commutatività** e l'**associatività** delle operazioni di intersezione ed unione. Si hanno inoltre:

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c) \quad (2.15)$$

$$a \cup (b \cap c) = (a \cup b) \cap (a \cup c) \quad (2.16)$$

che esprimono le proprietà distributive dell'unione rispetto all'intersezione e viceversa.

2.3.3 Differenza insiemistica

Definizione 2.3.3: Differenza insiemistica

Siano a, b due insiemi. Si definisce **sottrazione** tra a e b e si indica con $a \setminus b$ l'insieme:

$$a \setminus b = \{x \in a \mid x \notin b\} \quad (2.17)$$

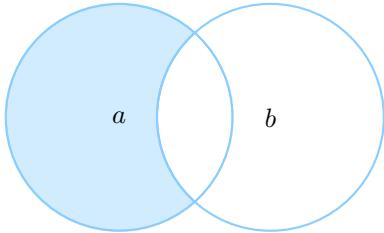


Figura 2.4: $a \setminus b$

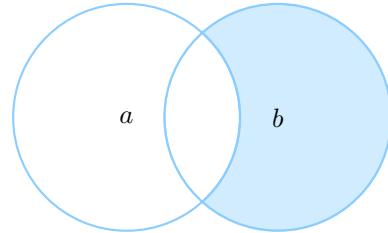


Figura 2.5: $b \setminus a$

Osservazione 2.3.3 ➤➤➤

L'insieme a contiene $a \setminus b$ come sottoinsieme:

$$a \setminus b \subset a$$

Se l'insieme a è parte di b allora:

$$b \setminus a = \{x \in b \mid x \notin a\}$$

Posto con α la condizione di appartenenza all'insieme a ($\alpha(x) \iff x \in a$), possiamo riscrivere la differenza precedente come segue:

$$b \setminus a = \{x \in b \mid \neg\alpha\}$$

Dalla tautologia della doppia implicazione si può ricavare una proprietà interessante:

$$\begin{aligned} b \setminus (b \setminus a) &= \{x \in b \mid \neg(\neg\alpha)\} \\ &= \{x \in b \mid x \in a\} \\ &= a \end{aligned} \quad (2.18)$$

L'osservazione precedente, chiaramente, non vale in generale per qualsiasi insieme a e b ma solo nel caso in cui a sia sottoinsieme di b . Infatti, posto " $\alpha = x \in a$ " e " $\beta = x \in b$ " si ha, per ogni a, b :

$$\begin{aligned} a \setminus (a \setminus b) &= \left\{x \mid \alpha \wedge (\neg(\alpha \wedge (\neg\beta)))\right\} \iff \left\{x \mid \alpha \wedge ((\neg\alpha) \vee (\neg(\neg\beta)))\right\} \\ &\iff \left\{x \mid \alpha \wedge ((\neg\alpha) \vee \beta)\right\} \\ &\iff \left\{x \mid (\alpha \wedge (\neg\alpha)) \vee (\alpha \wedge \beta)\right\} \\ &\iff \left\{x \mid \alpha \wedge \beta\right\} = a \cap b \end{aligned}$$

Dati n insiemi, un diagramma di Eulero Venn generico deve poter delimitare in maniera univoca ciascun tipo di intersezione per ogni insieme rappresentato. Ad esempio, supponendo di avere a disposizione cinque insiemi a, b, c, d ed e , il diagramma di Eulero Venn mostrato in Figura 2.6 non risulta essere un diagramma generico in quanto non sono rappresentate tutte le possibili intersezioni tra gli insiemi.

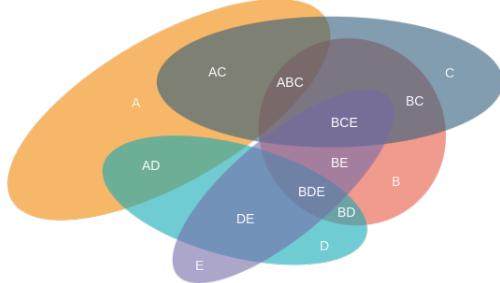


Figura 2.6

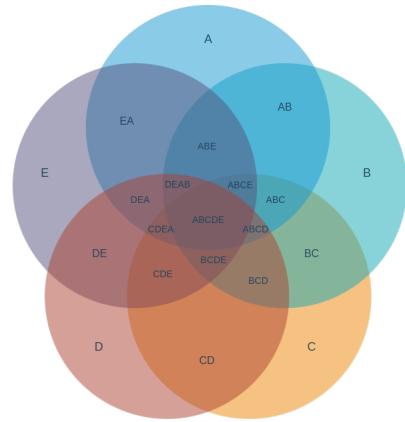


Figura 2.7

2.3.4 Le leggi di De Morgan e differenza simmetrica

Teorema 2.3.1

Siano a, b, c insiemi. Valgono allora le seguenti formule che prendono il nome di **leggi di De Morgan**:

$$a \setminus (b \cap c) = (a \setminus b) \cup (a \setminus c) \quad (2.19)$$

$$a \setminus (b \cup c) = (a \setminus b) \cap (a \setminus c) \quad (2.20)$$

Dimostrazione. Siano α, β, γ i predicati di appartenenza nella variabile x , rispettivamente: α è “ $x \in a$ ”, β è “ $x \in b$ ”, γ è “ $x \in c$ ”. Da queste definizioni segue:

$$\begin{aligned} x \in a \setminus (b \cap c) &\iff \alpha \wedge (\neg(\beta \wedge \gamma)) \\ &\iff (\alpha \wedge ((\neg\beta) \vee (\neg\gamma))) \\ &\iff ((\alpha \wedge (\neg\beta)) \vee (\alpha \wedge (\neg\gamma))) \\ &\iff x \in (a \setminus b) \cup (a \setminus c) \end{aligned}$$

Similmente si dimostra l'equazione 2.20. □

Definizione 2.3.4: Differenza simmetrica

Si definisce l'operazione insiemistica Δ di **differenza simmetrica** l'operazione corrispondente alla disgiunzione esclusiva.

Si pone dunque, per ogni insieme a e b :

$$a \Delta b := \{x \mid (x \in a) \dot{\vee} (x \in b)\} \quad (2.21)$$

La tautologia che abbiamo chiamato **esplicitazione di XOR** (Vedi Formula 1.26) implica facilmente:

$$a \Delta b = (a \setminus b) \cup (b \setminus a) = (a \cup b) \setminus (b \cap a) \quad (2.22)$$

mentre la commutatività e l'associatività di $\dot{\vee}$ e la distributività di \wedge rispetto a $\dot{\vee}$ forniscono la commutatività e l'associatività di Δ e la distributività di \cap rispetto a Δ . Per ogni insieme a, b, c abbiamo cioè:

$$a \Delta b = b \Delta a \quad (2.23)$$

$$a \Delta (b \Delta c) = (a \Delta b) \Delta c \quad (2.24)$$

$$a \cap (a \Delta c) = (a \cap b) \Delta (a \cap c) \quad (2.25)$$

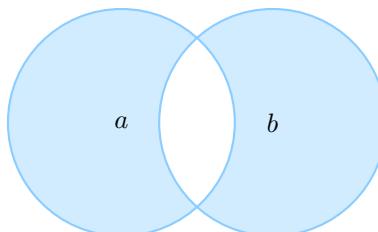


Figura 2.8: $a \Delta b$

2.3.5 ■ Operazioni unarie

Per ogni insieme s abbiamo definito l'insieme delle parti come l'insieme di tutti i sottoinsiemi di s . Dato però un numero naturale n è possibile definire un altro insieme delle parti che va sotto il nome di **insieme delle parti n -arie**.

Definizione 2.3.5: Insieme delle parti n -arie

Per ogni numero naturale $n \in \mathbb{N}$ e per ogni insieme s si ha:

$$\mathcal{P}_n(s) = \left\{ x \mid x \subseteq s \wedge x \text{ ha esattamente } n \text{ elementi} \right\} \quad (2.26)$$

Esempio 2.3.3

Dato un insieme s si ha $\mathcal{P}_0(s) = \{\emptyset\}$ e $\mathcal{P}_1(s) = \{\{x\} \mid x \in s\}$.

Definizione 2.3.6: Unione unaria

Sia a un insieme. Si definisce **unione unaria** di a e si denota col simbolo $\bigcup a$ l'insieme:

$$\bigcup a = \{x \mid \exists y \in a (x \in y)\} \quad (2.27)$$

ovvero l'*insieme degli elementi dei sottoinsiemi di a* .

Esempio 2.3.4

1. Per ogni $m \in \mathbb{N}$ si pone:

$$I_m = [0, m] = \{x \in \mathbb{R} \mid 0 \leq x \leq m\}$$

per definire un **intervallo chiuso reale** di estremi 0 ed m . Denotiamo con $a = \{I_m \mid m \in \mathbb{N}\}$ l'insieme di tutti gli intervalli siffatti. Allora l'unione unaria di a sarà:

$$\bigcup a = \{x \in \mathbb{R} \mid x \geq 0\} = \mathbb{R}^+$$

2. Sia $S = \{\{1, 5, 7\}, \{1, 5, 8, 9\}, \{2, 15, 66\}\}$, allora è:

$$\bigcup S = \{1, 2, 5, 7, 8, 9, 15, 66\}$$

Esempio 2.3.5

L'unione unaria delle parti di \mathbb{N} è \mathbb{N} stesso. Infatti, preso un qualsiasi numero naturale è possibile prendere un sottoinsieme che lo contiene:

$$\forall n \in \mathbb{N} (\exists b \in \mathcal{P}(\mathbb{N}) (n \in b))$$

Questo vuol dire allora che \mathbb{N} è un sottoinsieme dell'unione unaria dell'insieme delle sue parti:

$$\mathbb{N} \subseteq \bigcup \mathcal{P}(\mathbb{N})$$

Per la definizione di inclusione (Formula 2.5) questo vuol dire che:

$$\forall x (x \in \mathbb{N} \implies x \in \bigcup \mathcal{P}(\mathbb{N}))$$

Preso un numero $y \notin \mathbb{N}$ ci chiediamo se questo possa appartenere a $\bigcup \mathcal{P}(\mathbb{N})$. Per appartenere a tale insieme deve soddisfare alla condizione:

$$y \in \bigcup \mathbb{N} \iff (\exists b \in \mathcal{P}(\mathbb{N}) (y \in b))$$

Il che è chiaramente falso in quanto abbiamo ipotizzato che y non sia un numero naturale. Quindi possiamo dire che $\forall x (x \notin \mathbb{N} \implies x \notin \bigcup \mathcal{P}(\mathbb{N}))$. Dalla legge di contrapposizione si ha quindi:

$$\forall x (x \in \bigcup \mathcal{P}(\mathbb{N}) \implies x \in \mathbb{N})$$

Ovvero $\bigcup \mathcal{P}(\mathbb{N}) \subseteq \mathbb{N}$, e allora $\mathbb{N} = \bigcup \mathcal{P}(\mathbb{N})$ per la legge della doppia inclusione (Formula 2.9).

Definizione 2.3.7: Intersezione unaria

Sia $a \neq \emptyset$ un insieme non vuoto. Si definisce **intersezione unaria** di a e si denota col simbolo $\bigcap a$ l'insieme:

$$\bigcap a = \{x \mid \forall b \in a (x \in b)\} \quad (2.28)$$

ovvero l'insieme degli elementi che appartengono a ciascun elemento di a .

Osservazione 2.3.4



1. È importante precisare che a non possa essere l'insieme vuoto altrimenti si avrebbe una contraddizione. Infatti:

$$\bigcap \emptyset = \{x \mid \forall y \in \emptyset (x \in y)\}$$

il che rappresenterebbe l'insieme di tutti gli insiemi.

2. Sia $c = \{a, b\}$ un insieme contenente gli insiemi a e b . Quindi, per definizione di unione unaria si ha che $\bigcup c$ è l'insieme degli elementi che si trovano o in a o in b :

$$\bigcup c = \{x \mid \exists y \in c (x \in y)\} = \{x \mid x \in a \vee x \in b\} = a \cup b$$

Quindi l'unione tra due insiemi altro non è che un caso particolare dell'unione unaria applicato ad un insieme formato da due elementi. Grazie all'operazione unaria è possibile quindi effettuare unioni tra infiniti oggetti. Analogamente per l'intersezione unaria $\bigcap \{a, b\} = a \cap b$.

Proposizione 2.3.2 (Formule generalizzate di associatività, distributività e di De Morgan)

Per ogni a, b insiemi non vuoti valgono:

$$(\bigcap a) \cap (\bigcap b) = \bigcap (a \cup b) \quad (2.29)$$

$$(\bigcap a) \cup (\bigcap b) = \bigcup (a \cap b) \quad (2.30)$$

$$a \cap (\bigcup b) = \bigcup_{x \in b} (a \cap x) \quad (2.31)$$

$$a \cup (\bigcap b) = \bigcap_{x \in b} (a \cup x) \quad (2.32)$$

$$a \setminus \bigcup b = \bigcap_{x \in b} (a \setminus x) \quad (2.33)$$

$$a \setminus \bigcap b = \bigcup_{x \in b} (a \setminus x) \quad (2.34)$$

Dimostrazione. La dimostrazione di queste formule è lasciata al lettore come esercizio. □

2.4

PRODOTTO CARTESIANO DI INSIEMI



2.4.1 ■ Coppie ordinate

Definizione 2.4.1: Coppia ordinata

Siano a, b insiemi. Una **coppia ordinata** si denota col simbolo (a, b) e gode della seguente proprietà:

$$\forall a, b, c, d \quad (a, b) = (c, d) \iff (a = c \wedge b = d) \quad (2.35)$$

Proposizione 2.4.1

Per ogni a, b, c, d si ha:

$$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} \iff a = c \wedge b = d$$

Dimostrazione. (\implies) Si supponga quindi che $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Per l'assioma di estensionalità (Assioma 2.1.2) allora entrambi gli insiemi hanno gli stessi elementi. Se $a = b$ allora $\{\{a\}, \{a, b\}\} = \{\{a\}\}$ ha un solo elemento, per cui anche $\{\{c\}, \{c, d\}\}$ ha un solo elemento. Quindi $a = b = c = d$.

Sia allora $a \neq b$. Dall'ipotesi $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ segue allora $c \neq d$, per cui deve essere:

$$\begin{aligned}\{a\} &= \{c\} \implies a = c \\ \{a, b\} &= \{c, d\} \implies b = d\end{aligned}$$

(\Leftarrow) Chiaramente la condizione è sufficiente. □

Si può usare questa proposizione per dare una definizione esplicita delle coppie ordinate, ponendo:

$$\forall a, b \quad (a, b) := \{\{a\}, \{a, b\}\}$$

Questa è la cosiddetta **definizione di Kuratowski** della nozione di coppia ordinata.

2.4.2 ■ Prodotti cartesiani

Definizione 2.4.2: Prodotto cartesiano

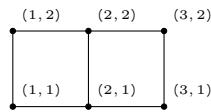
Siano a, b insiemi. Si dice **prodotto cartesiano** di a e b , e si denota col simbolo $a \times b$, l'insieme di tutte le coppie (x, y) , con x appartenente ad a e y appartenente a b .

$$a \times b = \{(x, y) \mid x \in a \wedge y \in b\} \quad (2.36)$$

Esempio 2.4.1

Ad esempio se $a = \{1, 2, 3\}$ e $b = \{1, 2\}$, allora

$$a \times b = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 2)\}$$



Definizione 2.4.3: Terna ordinata

Si definisce una **terna ordinata** (a, b, c) come una coppia ordinata in cui la prima coordinata è una coppia ordinata (a, b) e come seconda coordinata c :

$$\forall a, b, c \quad (a, b, c) = ((a, b), c) \quad (2.37)$$

Proposizione 2.4.2

Due terne ordinate (a, b, c) e (d, e, f) sono uguali se e solo se:

$$\forall a, b, c, d, e, f \quad ((a, b), c) = ((d, e), f) \iff (a = d \wedge b = e \wedge c = f) \quad (2.38)$$

Dimostrazione. L'enunciato si dimostra facilmente ponendo $(a, b) = m$ e $(d, e) = n$. In questo modo la dimostrazione si riduce alla dimostrazione già vista delle coppie ordinate (m, c) e (n, f) . □



Esercizio 2.5.1

Verificare $3 \in \{2n^2 + 1 \mid n \in \mathbb{Z}\}$.

Svolgimento. Poniamo $A = \{2n^2 + 1 \mid n \in \mathbb{Z}\}$. Per essere verificata l'appartenenza deve valere la seguente equivalenza logica

$$3 \in A \iff \exists n \in \mathbb{Z} (3 = 2n^2 + 1)$$

e procediamo sviluppando algebricamente tale relazione fino ad ottenere una relazione più semplice da valutare:

$$\begin{aligned} 3 \in A &\iff \exists n \in \mathbb{Z} (3 = 2n^2 + 1) \\ &\iff \exists n \in \mathbb{Z} (2 = 2n^2) && \text{Spostando 1 a sinistra} \\ &\iff \exists n \in \mathbb{Z} (n^2 = 1) && \text{Semplificando} \end{aligned}$$

L'ultima equivalenza è chiaramente vera in quanto, per $n = \pm 1 \in \mathbb{Z}$ si ha $n^2 = 1$. Quindi $3 \in A$. ■

Esercizio 2.5.2

Sia $A = \{\{a, b\} / a, b \in \mathbb{Z}\}$ un insieme. Verificare $\{1\} \in A$ e $\{1, 2, 3\} \in A$.

Svolgimento. Chiaramente:

$$\{1\} \in A \iff \exists a, b \in \mathbb{Z} (\{a, b\} = \{1\})$$

che risulta vera per $a = b = 1$. Infatti $\{1, 1\} = \{1\} \in A$. Al contrario, non esistono due numeri interi relativi tali che $\{a, b\} = \{1, 2, 3\}$ in quanto tale insieme contiene 3 elementi mentre $\{a, b\}$ ne può contenere al massimo due (quando $a \neq b$). Quindi $\{1, 2, 3\} \notin A$. ■

Esercizio 2.5.3

Sia $f = \{\{a, b\}, \{b, d\}\}$. Si calcolino $\bigcap f$ e $\bigcup f$.

Svolgimento. L'intersezione unaria di f è definita come l'insieme degli elementi appartenenti a ciascun elemento di f , ovvero:

$$\bigcap f = \{x / \forall y \in f (x \in y)\} = \{a, b\} \cap \{b, d\} = \{b\}$$

! Non dimenticare che $b \neq \{b\}$, nel primo caso ci si sta riferendo all'entità b mentre nel secondo al singleton dell'entità b . Sarebbe stato un errore scrivere quindi $\bigcap f = b$.

Nel caso dell'unione unaria abbiamo che:

$$\bigcup f = \{x / \exists y \in f (x \in y)\} = \{a, b\} \cup \{b, d\} = \{a, b, d\}$$

Esercizio 2.5.4

Sia A l'insieme dei numeri pari e B quello dei numeri naturali moltiplicati per 2; dire in quale relazione stanno i due insiemi.

Svolgimento. Per definizione di numero pari esprimiamo l'insieme A come:

$$\{p \in \mathbb{Z} / \exists k \in \mathbb{Z} (p = 2k)\}$$

mentre

$$B = \{m \in \mathbb{N} / \exists k \in \mathbb{N} (m = 2k)\}$$

Ovviamente vale $B \subset A$. ■

Esercizio 2.5.5

Decidere se esistono e, nel caso, descrivere esplicitamente gli insiemi:

1. $\{x \mid \forall y(x = y)\}$
2. $\{x \mid \forall y(x \neq y)\}$
3. $\{x \mid \exists y(x = y)\}$
4. $\{x \mid \exists y(x \neq y)\}$
5. $\{x \mid \forall y(y \subseteq x)\}$
6. $\{x \mid x = \{0, 1, 2\}\}$
7. $\{y \mid y = \{0, 1, 2\}\}$
8. $\{x \mid x = \{0, 1, 2, x\}\}$

Svolgimento. Si ha:

1. $\{x \mid \forall y(x = y)\} = \emptyset$. Non esiste infatti un insieme x che sia uguale a tutti gli insiemi y . Quindi non esiste nessun elemento in questo insieme. Quindi l'insieme è l'insieme vuoto.
2. $\{x \mid \forall y(x \neq y)\} = \emptyset$. Infatti non è vero che per ogni x , comunque si prenda un insieme y allora $x \neq y$ perché appunto si potrebbe scegliere x stesso al posto di y ottenendo la proposizione " $\forall x(x \neq x)$ " e poiché ogni oggetto è uguale a se stesso allora si può dire che non esistono oggetti che appartengono alla totalità descritta dalla formula e per questo motivo l'insieme descrive l'insieme vuoto.
3. Va notato che la proprietà di questo insieme è la negazione dell'insieme precedente. Per questo motivo possiamo dire che la proprietà è vera in quanto è vero che esiste almeno un insieme tale per cui sia uguale ad x (ovvero x stesso). Essendo vera questa formula allora sarebbe vero che per ogni insieme x questo appartiene all'insieme $A = \{x \mid \exists y(x = y)\}$ ma non esistendo l'insieme di tutti gli insiemi allora l'insieme in questione non esiste.
4. Analogamente come nell'esercizio precedente.
5. L'insieme $\{x \mid \forall y(y \subseteq x)\}$ rappresenta l'insieme vuoto. Infatti non esiste un insieme tale per cui, comunque si scelga un insieme y , esso sia parte di x . Per fugare ogni dubbio, per rendere evidente che questa proposizione è falsa basta trovare un controsenso: preso l'insieme x è immediato osservare che il singleton $\{x\}$ non è contenuto in x : $\forall x(\{x\} \notin x)$.
6. L'insieme $\{x \mid x = \{0, 1, 2\}\}$ esiste ed ha un solo elemento. Infatti, per l'assioma di estensionalità, l'insieme delle x tali che $x = \{0, 1, 2\}$ è il singleton di siffatto insieme x . Quindi:

$$\{x \mid x = \{0, 1, 2\}\} = \{\{0, 1, 2\}\}$$

7. Uguale all'insieme precedente.
8. $A = \{x \mid x = \{0, 1, 2, x\}\} = \emptyset$. Infatti si deve avere $\forall x(x \in A \iff \varphi)$, dove φ rappresenta il predicato " $x = \{0, 1, 2, x\}$ ". Questa condizione è falsa per ogni x in quanto nessun insieme appartiene a sé stesso e quindi l'insieme A è vuoto. ■

Esercizio 2.5.6

Dire quali delle seguenti relazioni sono vere e quali false:

1. $\{1, 3, 5, 10\} = \{3, 1, 10, 5\}$;
2. $\{a, b, d\} = \{b, d, a\}$;
3. $\{2, 5, 6\} = \{2, 7, 5\}$;
4. $\{a\} = a$;
5. $a \in \{a\}$;

Svolgimento. Si ha:

1. Vero
2. Vero
3. Falso
4. Falso
5. Vero

Esercizio 2.5.7

Sia $x = \{\{\{\emptyset\}\}\}$. Quanti elementi ha x ? Quante parti ha x ?

Svolgimento. L'insieme x ha un solo elemento, di conseguenza l'insieme delle parti avrà solo le parti banali. ■

Esercizio 2.5.8

Vero o falso?

1. $\emptyset \in \emptyset$
2. $\emptyset \subseteq \emptyset$
3. $\emptyset \subset \emptyset$
4. $\emptyset \in \mathcal{P}(\emptyset)$
5. $\emptyset \subseteq \mathcal{P}(\emptyset)$
6. $\emptyset = \{\emptyset\}$
7. $\emptyset \subseteq \{\emptyset\}$
8. $\emptyset \in \{\emptyset\}$
9. $\{1, 1, 2, 2, 2, 3, 3\}$ è una parte di $\{2, 1, 3\}$
10. $\{1, 1, 2, 2, 2, 3, 3\}$ è una parte di $\{4, 2, 1, 3\}$

Svolgimento. Si ha:

1. Falso
2. Vero
3. Falso
4. Vero
5. Vero
6. Falso
7. Vero
8. Vero
9. Vero
10. Vero.

Esercizio 2.5.9

Elencare gli elementi di $\mathcal{P}(\{0, 1, 2\})$.

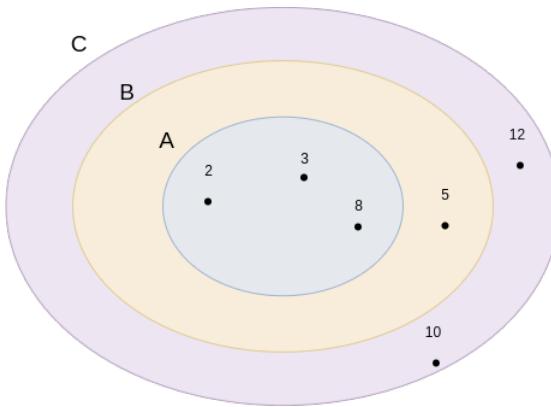
Svolgimento. Si ha $\mathcal{P}(\{0, 1, 2\}) = \{\emptyset, \{0, 1, 2\}, \{0\}, \{1\}, \{2\}, \{1, 2\}, \{0, 1\}, \{0, 2\}\}$.

Esercizio 2.5.10

Illustrare con i grafici di Eulero Venn la proprietà transitiva dell'inclusione tra i seguenti insiemi:

$$A = \{2, 3, 5\} \quad B = \{2, 3, 8, 5\} \quad C = \{3, 2, 8, 5, 10, 12\}$$

Svolgimento. Si ha:



Esercizio 2.5.11

Determinare rispetto a \mathbb{Z} gli insiemi complementari dei seguenti insiemi:

1. $\{x/x \in \mathbb{Z} \wedge x < 3\}$
2. $\{x/x \in \mathbb{Z} \wedge 2 \leq x \leq 5\}$
3. $\{x/x \in \mathbb{Z} \wedge 1 < x < 5\}$
4. $\{x/x \in \mathbb{Z} \wedge 1 \leq x \leq 2\}$
5. $\{x/x \in \mathbb{Z} \wedge x \geq 1\}$
6. $\{x/x \in \mathbb{Z} \wedge x \leq 0\}$

Svolgimento. Definiamo complemento di una parte X di un insieme non vuoto S la differenza $S \setminus X$. Abbiamo allora:

1. $\mathbb{Z} \setminus \{x/x \in \mathbb{Z} \wedge x < 3\} = \{x/x \in \mathbb{Z} \wedge x > 3\};$
2. $\mathbb{Z} \setminus \{x/x \in \mathbb{Z} \wedge 2 \leq x \leq 5\} = \{x/x \in \mathbb{Z} \wedge x < 2 \wedge x > 5\};$
3. $\mathbb{Z} \setminus \{x/x \in \mathbb{Z} \wedge 1 < x < 5\} = \{x/x \in \mathbb{Z} \wedge x \leq 1 \wedge x \geq 5\};$
4. $\mathbb{Z} \setminus \{x/x \in \mathbb{Z} \wedge 1 \leq x \leq 2\} = \{x/x \in \mathbb{Z} \wedge x < 1 \wedge x > 2\};$
5. $\mathbb{Z} \setminus \{x/x \in \mathbb{Z} \wedge x \geq 1\} = \{x/x \in \mathbb{Z} \wedge x < 1\};$
6. $\mathbb{Z} \setminus \{x/x \in \mathbb{Z} \wedge x \leq 0\} = \{x/x \in \mathbb{Z} \wedge x > 0\}.$

Esercizio 2.5.12

L'insieme \mathbb{Z} appartiene a $\mathcal{P}(\mathbb{Z})$?

Svolgimento. Sì. In ogni insieme $S \neq \emptyset$ si ha che \emptyset ed S sono parti banali e appartengono a $\mathcal{P}(S)$.

Esercizio 2.5.13

Descrivere esplicitamente gli insiemi:

1. $\{x|\forall y(x \cap y = \emptyset)\}$
2. $\{x|\exists y(x \cup y = \emptyset)\}$
3. $\{x|\forall y(x \cup y = \emptyset)\}$

Svolgimento. Si ha:

1. $\{x|\forall y(x \cap y = \emptyset)\} = \{\emptyset\}$. Infatti l'insieme rappresenta l'insieme degli insiemi che non hanno alcun elemento in comune con tutti gli insiemi. L'unico insieme a soddisfare questa proprietà è l'insieme vuoto.
2. $\{x|\exists y(x \cup y = \emptyset)\} = \{\emptyset\}$. Infatti l'insieme rappresenta l'insieme di tutti gli insiemi x per i quali esiste almeno un insieme y tale che l'unione con x sia il vuoto. L'unico insieme a soddisfare tale proprietà è l'insieme vuoto in quanto $\emptyset \cup \emptyset = \emptyset$.
3. $\{x|\forall y(x \cup y = \emptyset)\} = \emptyset$. Infatti non esiste un insieme per cui la sua unione con qualsiasi insieme sia uguale all'insieme vuoto.

Esercizio 2.5.14

Per quali coppie di insiemi a, b , si ha $a \setminus b = b \setminus a$?

Svolgimento. L'unico caso in cui $a \setminus b$ può essere uguale a $b \setminus a$ è quando $a = b$. Infatti si ha $a \setminus b = \emptyset = b \setminus a$.

Esercizio 2.5.15

Rappresentare, in diagrammi di Venn generici, i termini insiemistici $a \setminus (b \setminus c)$ e $(a \setminus b) \setminus c$. Decidere se è vera o falsa la proposizione: $(\forall a, b, c)(a \setminus (b \setminus c) = (a \setminus b) \setminus c)$. Ripetere l'esercizio per $a \cap (b \setminus c)$ e $(a \cap b) \setminus c$.

Svolgimento. L'insieme $a \setminus (b \setminus c)$ è rappresentato dal diagramma di Venn 2.9 mentre l'insieme $(a \setminus b) \setminus c$ dal diagramma 2.10.

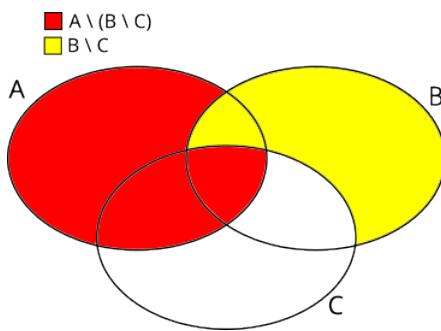


Figura 2.9

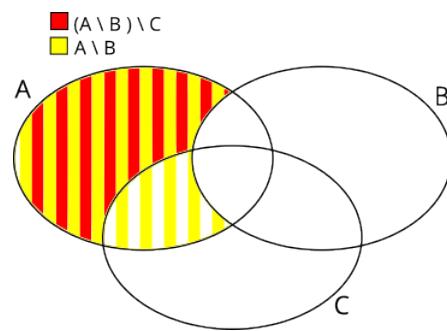


Figura 2.10

Osservando i due diagrammi possiamo concludere che la differenza simmetrica tra tre insiemi non gode della proprietà associativa. Non è vero dunque che: $\forall a, b, c (a \setminus (b \setminus c) = (a \setminus b) \setminus c)$. Analogamente, i diagrammi di Eulero Venn 2.11 e 2.12 rappresentano gli insiemi $a \cap (b \setminus c)$ e $(a \cap b) \setminus c$.

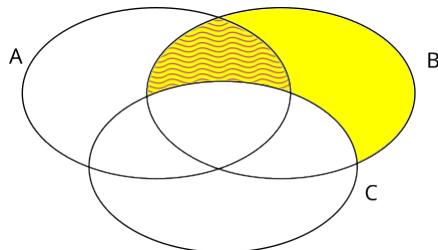


Figura 2.11

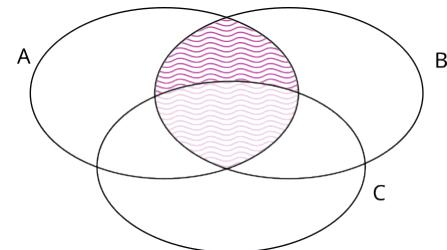


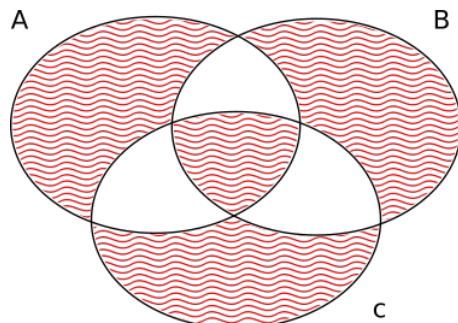
Figura 2.12

Dai due diagrammi ci si può convincere del fatto che: $\forall a, b, c (a \cap (b \setminus c) = (a \cap b) \setminus c)$. ■

Esercizio 2.5.16

Rappresentare in diagramma di Eulero Venn $(a \Delta b) \Delta c$.

Svolgimento. Si ha che $(a \setminus b) \setminus c$ è uguale al seguente diagramma di Eulero Venn:



Infatti, posto $\alpha = x \in A$, $\beta = x \in B$ e $\gamma = x \in C$ si ha:

$$x \in (a \Delta b) \Delta c \iff (\alpha \dot{\vee} \beta) \dot{\vee} \gamma$$

Che, per la tautologia 1.24 è equivalente all'implicazione:

$$(\alpha \iff \beta) \iff \gamma$$

che è vera quando vale una e una sola delle tre proprietà (come evidenziato dalle zone in verde alle estremità del diagramma) oppure valgono contemporaneamente (la parte centrale del diagramma). ■

Esercizio 2.5.17

Dimostrare che, per ogni a, b sono equivalenti tra loro:

1. $a \subseteq b$
2. $a \cap b = a$
3. $a \cup b = b$

Svolgimento. (1 \implies 2) Dire che per ogni insieme a e b si ha $a \subseteq b$ significa affermare:

$$\forall x(x \in a \implies x \in b)$$

Poiché l'intersezione tra i due insiemi è l'insieme che contiene gli elementi in comune tra i due è evidente che l'insieme formato sia a .

(1 \implies 3) Analogamente, se a è un sottoinsieme di b e l'unione è l'insieme formato da tutti gli elementi che si trovano o in a o in b allora l'unione tra i due insiemi è b stesso.

(3 \implies 1) Se $a \cup b = \{x | x \in a \vee x \in b\} = b$ può significare solo due cose. O che a è l'insieme vuoto o che a è un sottoinsieme di b . In entrambi i casi si ha $a \subseteq b$. ■

Esercizio 2.5.18

Calcolare, per un arbitrario insieme a :

1. $a \Delta a$
2. $a \Delta \emptyset$

Svolgimento. Per definizione di differenza simmetrica si ha:

$$\begin{aligned} a \Delta a &= \{x | x \in ((a \cup a) \setminus (a \cap a))\} \\ &= \{x | x \in (a \setminus a)\} \\ &= \emptyset \end{aligned}$$

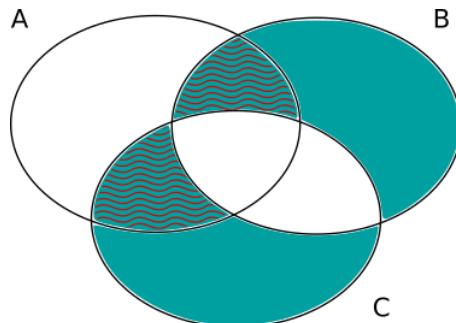
mentre nel caso della seconda formula:

$$\begin{aligned} a \Delta \emptyset &= \{x | x \in ((a \cup \emptyset) \setminus (a \cap \emptyset))\} \\ &= \{x | x \in (a \setminus \emptyset)\} \\ &= a \end{aligned}$$

Esercizio 2.5.19

Rappresentare, in un diagramma di Venn generico, il termine insiemistico $A \cap (B \Delta C)$.

Svolgimento. Si procede calcolando innanzitutto $B \Delta C$ (la zona evidenziata di grigio) e poi si calcola l'intersezione con l'insieme A . Si ottiene così il diagramma di Venn mostrato in figura:

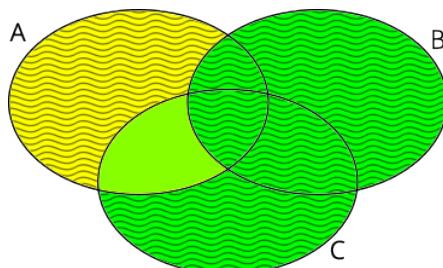


Esercizio 2.5.20

Rappresentare su un diagramma di Venn di tipo generale l'espressione insiemistica: $(A \setminus B) \Delta (B \cup C)$.

Svolgimento. Si ha:

$$(A \setminus B) \Delta (B \cup C) = ((A \setminus B) \cup (B \cup C)) \setminus ((A \setminus B) \cap (B \cup C))$$



Esercizio 2.5.21

Rappresentare, in un diagramma di Venn generico, i termini insiemistici $A \cup (B \cap C)$ e $A \cap (B \cup C)$. Decidere se vale una delle formule:

$$\forall A, B, C (A \cup (B \cap C) \subseteq A \cap (B \cup C)) \quad (2.39)$$

$$\forall A, B, C (A \cup (B \cap C) \supseteq A \cap (B \cup C)) \quad (2.40)$$

Svolgimento. Si ha $A \cup (B \cap C)$ rappresentato in figura 2.13 mentre $A \cap (B \cup C)$ è mostrato in Figura 2.14.

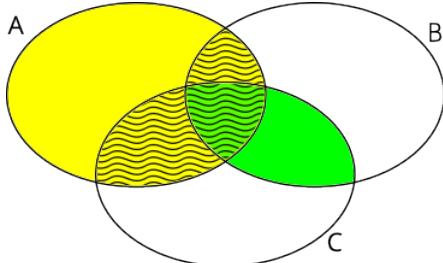


Figura 2.13: $A \cup (B \cap C)$

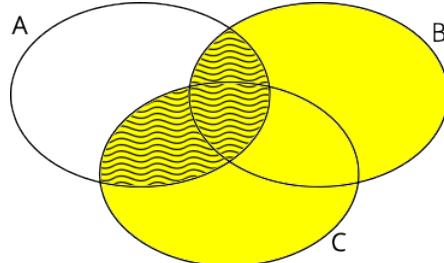


Figura 2.14: $A \cap (B \cup C)$

Osservando i diagrammi di Venn possiamo dire con certezza che $\forall A, B, C (A \cup (B \cap C) \supseteq A \cap (B \cup C))$. ■

Esercizio 2.5.22

Rappresentare con un diagramma di Eulero Venn l'insieme: $((a \Delta b) \Delta c) \Delta d$.

Svolgimento. Affermare che un qualsiasi x appartiene all'insieme $((a \Delta b) \Delta c) \Delta d$ è equivalente alla seguente catena di implicazioni:

$$\begin{aligned} \forall x (x \in ((a \Delta b) \Delta c) \Delta d) &\iff \forall x ((a \Delta b) \Delta c) \dot{\vee} (x \in d) \\ &\iff \forall x ((x \in (a \Delta b) \dot{\vee} x \in c) \dot{\vee} (x \in d)) \\ &\iff \forall x ((x \in a) \dot{\vee} (x \in b) \dot{\vee} (x \in c) \dot{\vee} (x \in d)) \end{aligned}$$

che è vera quando è vera singolarmente una delle condizioni di appartenenza oppure quando vale per tre di esse. Quindi l'insieme così ottenuto è quello evidenziato dalle strisce nel diagramma di Eulero Venn mostrato nella Figura 2.15.

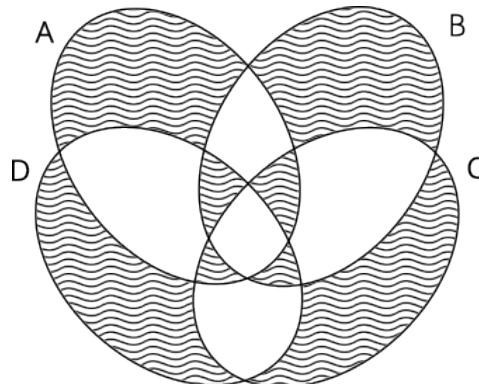


Figura 2.15

Esercizio 2.5.23

Rappresentare, in diagrammi di Venn generici, i termini insiemistici $a \cap (b \Delta c)$ e $a \cup (b \Delta c)$, confrontandoli tra loro e con $(a \cap b) \Delta (a \cap c)$ e $(a \cup b) \Delta (a \cup c)$.

Svolgimento. Si ha:

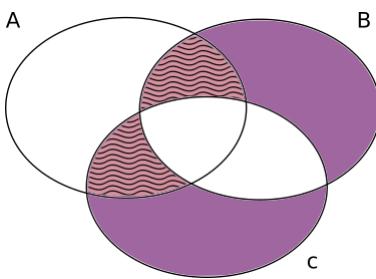


Figura 2.16: $a \cap (b \Delta c)$

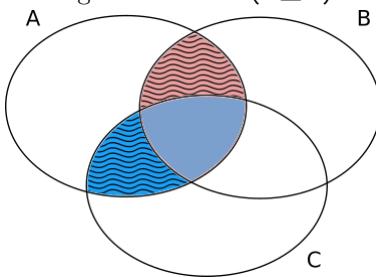


Figura 2.18: $(a \cap b) \Delta (a \cap c)$

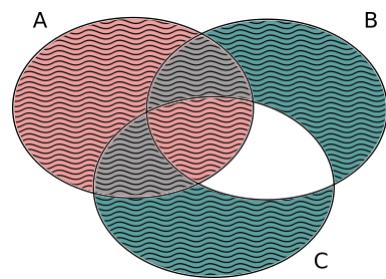


Figura 2.17: $a \cup (b \Delta c)$

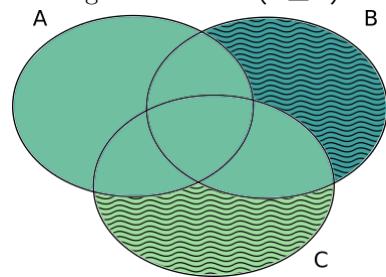


Figura 2.19: $(a \cup b) \Delta (a \cup c)$

Osservando i vari diagrammi di Venn possiamo dire con certezza che vale:

$$\begin{aligned} a \cap (b \Delta c) &= (a \cap b) \Delta (a \cap c) \\ a \cap (b \Delta c) &\subset a \cup (b \Delta c) \\ (a \cup b) \Delta (a \cup c) &\subset a \cup (b \Delta c) \end{aligned}$$

Esercizio 2.5.24

Siano a e b due insiemi. Supposto $a \subseteq b$, descrivere $a \Delta b$.

Svolgimento. Per definizione

$$a \Delta b = (a \cup b) \setminus (a \cap b) \quad (2.41)$$

Ma, essendo $a \subseteq b$, valgono le seguenti relazioni:

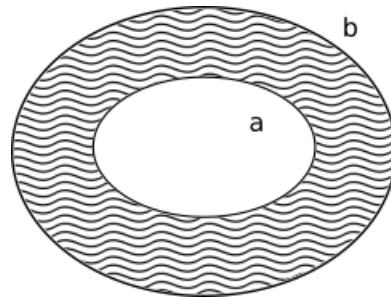
$$a \cup b = b \quad (2.42)$$

$$a \cap b = a \quad (2.43)$$

Quindi, sostituendo tali relazioni in 2.41 si ottiene:

$$\begin{aligned} a \Delta b &= (a \cup b) \setminus (a \cap b) \\ &= b \setminus a \end{aligned}$$

Ovvero il complemento di a in b come mostrato nel seguente diagramma di Venn:



Esercizio 2.5.25

Siano $A = \{n \in \mathbb{N} \mid 3 \leq n \leq 10\}$, B l'insieme dei numeri naturali pari, $C = \{1, 2, 8, 13, 1234\}$. Descrivere, elencandone gli elementi:

1. $A \setminus B$
2. $A \Delta C$
3. $B \cap C$
4. $B \Delta (B \setminus C)$.

Svolgimento. Abbiamo:

$$\begin{aligned}A \setminus B &= \{3, 5, 7, 9\} \\A \Delta C &= \{1, 2, 4, 5, 6, 7, 9, 10, 13, 1234\} \\B \cap C &= \{2, 8, 1234\} \\B \Delta (B \setminus C) &= \{2, 8, 1234\}\end{aligned}$$

! Sfrutta la proprietà della differenza simmetrica tra un insieme ed una sua parte dimostrata nell'esercizio precedente.

Esercizio 2.5.26

Calcolare:

1. $\bigcup \emptyset$
2. $\bigcup \{\emptyset\}$
3. $\bigcup \{a\}$
4. $\bigcap \{a\}$

Svolgimento. Si ha:

$$\begin{aligned}\bigcup \emptyset &= \emptyset \\ \bigcup \{\emptyset\} &= \{x \mid x \in \emptyset\} = \emptyset \\ \bigcup \{a\} &= \{x \mid x \in \{a\}\} = a \\ \bigcap \{a\} &= a\end{aligned}$$

Esercizio 2.5.27

Calcolare $\bigcap A$ e $\bigcup A$ in ciascuno dei seguenti casi:

1. A è l'insieme delle parti infinite di \mathbb{N}
2. $A = \{X \subseteq \mathbb{N} \mid 13 \notin X\}$
3. $A = \{X \subseteq \mathbb{N} \mid 13 \in X\}$
4. $A = \{\{124, n\} \mid n \in \mathbb{N}\}$
5. $A = \{[n-1, n+1] \mid n \in \mathbb{N}\}$ dove $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$

Svolgimento. Si ha:

1. $\bigcup A = \mathbb{N}$, $\bigcap A = \emptyset$. Se supponiamo infatti che esista un elemento x appartenente a tutte le parti infinite di \mathbb{N} , cioè $\bigcap A = \{x\}$. Allora $x \in \mathbb{N}$ e vale $\forall x (x \notin \mathbb{N} \setminus \{x\})$, dove $\mathbb{N} \setminus \{x\}$ è una parte infinita di \mathbb{N} e il che è assurdo.
2. $\bigcup A = \mathbb{N} \setminus \{13\}$, $\bigcap A = \emptyset$
3. $\bigcup A = \mathbb{N}$, $\bigcap A = \{13\}$
4. $\bigcup A = \mathbb{N}$, $\bigcap A = \{124\}$
5. $\bigcup A = \{x \in \mathbb{R} \mid x \geq -1\}$, $\bigcap A = \emptyset$

Esercizio 2.5.28

Vero o falso?

1. $(\{0\} \times \mathbb{N}) \cap (\{1\} \times \mathbb{N}) = \{0, 1\} \times \mathbb{N}$
2. $(\mathbb{N} \times \mathbb{N}) \cup ((\mathbb{Z} \setminus \mathbb{N}) \times (\mathbb{Z} \setminus \mathbb{N})) = \mathbb{Z} \times \mathbb{Z}$

Svolgimento. Si ha:

1. $(\{0\} \times \mathbb{N}) \cap (\{1\} \times \mathbb{N}) \neq \{0, 1\} \times \mathbb{N}$. Infatti $(\{0\} \times \mathbb{N})$ rappresenta l'insieme di tutte le coppie del tipo $(0, n)$ con $n \in \mathbb{N}$ mentre $(\{1\} \times \mathbb{N})$ quello delle coppie del tipo $(1, n)$ con $n \in \mathbb{N}$ quindi la loro intersezione è sicuramente vuota.
2. $(\mathbb{N} \times \mathbb{N}) \cup ((\mathbb{Z} \setminus \mathbb{N}) \times (\mathbb{Z} \setminus \mathbb{N})) \neq \mathbb{Z} \times \mathbb{Z}$. Infatti:

$$(\mathbb{N} \times \mathbb{N}) \cup ((\mathbb{Z} \setminus \mathbb{N}) \times (\mathbb{Z} \setminus \mathbb{N})) = \{(n, m) \mid n, m \in \mathbb{N}\} \cup \{(-n, -m) \mid n, m \in \mathbb{N}\}$$

Preso un elemento di $\mathbb{Z} \times \mathbb{Z}$, ad esempio $(1, -2)$ si vede facilmente che questo non appartiene al primo insieme.

Esercizio 2.5.29

Verificare che:

1. $A \setminus B = A \implies A \cap B = \emptyset$
2. $A \setminus B = \emptyset \implies A \subseteq B$
3. $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$

Svolgimento.

1. Supponiamo che $A \cap B \neq \emptyset$. Allora, essendo non vuoto, esiste un elemento appartenente a tale intersezione, sia esso $\bar{x} \in A \cap B$. Per definizione di intersezione si ha:

$$\bar{x} \in A \cap B \iff x \in A \wedge x \in B$$

Consideriamo adesso la differenza $A \setminus B$ definito come:

$$A \setminus B = \{x / x \in A \wedge x \notin B\}$$

ovviamente si ha che $\bar{x} \notin A \setminus B$. Per questo e per la generalità di \bar{x} possiamo affermare quindi che $A \cap B \notin A \setminus B$. Sapendo che l'intersezione tra due insiemi è sempre una parte di entrambi gli insiemi, affermare che $A \cap B \notin A \setminus B$ equivale a dire che $A \setminus B \neq A$ in quanto da tale insieme mancano sicuramente gli elementi appartenenti a $A \cap B$. Per contrapposizione si ha la tesi.

2. Supponiamo che A non sia una parte di B . Per definizione di sottoinsieme abbiamo che:

$$A \subseteq B \iff \forall x \in A (x \in B) \quad (2.44)$$

Allora, negando:

$$\begin{aligned} A \notin B &\iff \neg(\forall x (x \in A \implies x \in B)) \\ &\iff \exists x (x \in A \wedge x \notin B) && \text{Negando il quantificatore universale} \\ &\iff \exists x \in A \setminus B && \text{Per definizione di differenza} \end{aligned}$$

Quindi $A \setminus B \neq \emptyset$. Per contrapposizione si ottiene la tesi.

3. Dimostriamo innanzitutto che $A \cap (B \setminus C) \subseteq (A \cap B) \setminus (A \cap C)$. Sia $x \in A \cap (B \setminus C)$ allora x appartiene sia ad A che a $B \setminus C$, ovvero x appartiene sia ad A che a B ma non appartiene a C . Pertanto x appartiene a ciascuna delle differenze $A \setminus C$ che $B \setminus C$. Da $x \in A \setminus C$ possiamo osservare che sicuramente $x \notin A \cap C$ e vale quindi $x \in (A \cap B) \setminus (A \cap C)$, ovvero vale: $A \cap (B \setminus C) \subseteq (A \cap B) \setminus (A \cap C)$.

Viceversa, se $x \in (A \cap B) \setminus (A \cap C)$, si ha che x appartiene a $A \cap B$ e $x \notin (A \cap C)$ per cui x non appartiene ad almeno uno degli insiemi A e C . Se $x \in A \cap B$ sicuramente deve essere $x \notin C$ e allora si ha che $x \in A \wedge x \in B \wedge x \notin C$, per associatività quindi: $x \in A \cap (B \setminus C)$ e la tesi è dimostrata avendo ottenuto la doppia inclusione. ■

Esercizio 2.5.30

Si dimostri che se B è un insieme e $A \subseteq B$ allora $(B \setminus A) \cap A = \emptyset$ e $(B \setminus A) \cup A = B$.

Svolgimento. Per dimostrare che un certo insieme è vuoto conviene ragionare per assurdo, cioè supporre che non sia vuoto e dedurne una contraddizione. Ad esempio, siano $A \subseteq B$ due insiemi e supponiamo per assurdo che $(B \setminus A) \cap A \neq \emptyset$. Da $(B \setminus A) \cap A \neq \emptyset$ segue che $\exists x \in (B \setminus A) \wedge x \in A$. Ne segue che $x \notin A$ e $x \in A$ e questa è una contraddizione. Abbiamo così dimostrato che deve essere $(B \setminus A) \cap A = \emptyset$.

Mostriamo ora che se $A \subseteq B$, allora $(B \setminus A) \cup A = B$. Dato che $B \setminus A \subseteq B$ e $A \subseteq B$, abbiamo che $(B \setminus A) \cup A \subseteq B$. Per mostrare che $B \subseteq (B \setminus A) \cup A$ fissiamo $b \in B$. Allora si possono avere i due casi $b \in A$ oppure $b \notin A$. Se $b \in A$, allora $b \in (B \setminus A) \cup A$. Se invece $b \notin A$, si ha che $b \in B \setminus A$, e quindi $b \in (B \setminus A) \cup A$. In entrambi i casi si ha pertanto che $b \in (B \setminus A) \cup A$ e questo prova che $B \subseteq (B \setminus A) \cup A$. ■

Esercizio 2.5.31

Siano a e b due insiemi. Si ha $a \times b = b \times a$ se e solo se ...?

Svolgimento. Dati due insiemi a e b si ha che $a \times b = b \times a$ se e solo se $a = b$. Essendo la condizione banalmente sufficiente⁴ dimostriamo che essa è necessaria, ovvero $a \times b = b \times a \implies a = b$. Prendiamo un qualsiasi elemento $x \in a$. Se $y \in b$ allora la coppia $(x, y) \in a \times b = b \times a$. Allora x appartiene anche all'insieme b e, per la sua generalità, possiamo dire che $a \subseteq b$. Analogamente per la seconda coordinata si ha che $y \in a$ e quindi $b \subseteq a$. Per la legge della doppia inclusione allora abbiamo $a = b$. ■

⁴Si veda l'osservazione 1.2.2

Esercizio 2.5.32

Siano A e B due sottoinsiemi di I e sia B' il complementare di B rispetto a I . Verificare che $A \setminus B = A \cap B'$.

Svolgimento. Confrontando i due diagrammi di Venn si ha la verifica dell'asserto:



Si può arrivare alla stessa conclusione osservando che un elemento x appartiene all'insieme $A \setminus B$ se, e soltanto se, x appartiene ad A ma non appartiene a B . Sfruttando il fatto che A è una parte di I abbiamo sicuramente che x è un elemento appartenente anche ad I , ovvero: $\forall x \in (A \setminus B)(x \in A \wedge x \in I \wedge x \notin B)$ il che è equivalente ad affermare che $x \in A \wedge x \in B'$ e quindi si ha che $A \setminus B \subseteq A \cap B'$. Viceversa, sia $x \in A \cap B'$. Si ha ovviamente che x appartiene sia ad A che al complemento di B , ovvero $I \setminus B$. Quindi $x \in A$, $x \in I$ e $x \notin B$. Allora x appartiene ad A e non appartiene a B , ovvero $x \in A \setminus B$ e vale $A \cap B' \subseteq A \setminus B$. Dalla doppia inclusione deriva l'asserto. ■

Esercizio 2.5.33

Dimostrare che, per ogni insieme A , B :

$$A \times B = \emptyset \iff A = \emptyset \vee B = \emptyset$$

Svolgimento

\Leftarrow La condizione è ovviamente sufficiente.

\Rightarrow Ragionando per contrapposizione, si ottiene:

$$\forall A, B(A = \emptyset \vee B = \emptyset)$$

quindi:

$$\exists A, B(A \neq \emptyset \wedge B \neq \emptyset)$$

dunque:

$$\exists a \in A \wedge \exists b \in B$$

Fissati tali a, b si ottiene: $(a, b) \in A \times B \neq \emptyset$. ■

Esercizio 2.5.34

Elencare gli elementi di $\{1, 2\} \times \{1, 2, 3\}$, quelli di $\{1, 2, 3\} \times \{1, 2\}$ e quelli di $(\{1, 2\} \times \{1, 2, 3\}) \cap (\{1, 2, 3\} \times \{1, 2\})$.

Svolgimento. Si ha:

- $\{1, 2\} \times \{1, 2, 3\} = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\}$
- $\{1, 2, 3\} \times \{1, 2\} = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 2)\}$
- $\{1, 2\} \times \{1, 2, 3\} \cap (\{1, 2, 3\} \times \{1, 2\}) = \{(1, 1), (1, 2), (2, 2)\}$.

Esercizio 2.5.35

Vero o falso?

1. $(\{0\} \times \mathbb{N}) \cup (\{1\} \times \mathbb{N}) = \{0, 1\} \times \mathbb{N}$
2. $(\mathbb{N} \times \mathbb{N}) \cup (\mathbb{Z} \setminus \mathbb{N}) \times (\mathbb{Z} \setminus \mathbb{N}) = \mathbb{Z} \times \mathbb{Z}$.

Svolgimento.

1. Vero, perché $(\{0\} \times \mathbb{N}) \cup (\{1\} \times \mathbb{N})$ è l'unione tra l'insieme di tutte le coppie di prima coordinata 0 e seconda coordinata un naturale e l'insieme di tutte le coppie di prima coordinata 1 e seconda coordinata un naturale.
2. Vero, perché $\mathbb{Z} \times \mathbb{Z}$ può essere visto come l'unione tra l'insieme delle coppie (a, b) con a, b entrambi positivi e l'insieme delle coppie (c, d) con c, d entrambi negativi. ■

Un **teorema** è un enunciato della forma “Se valgono P_1, P_2, \dots, P_n allora vale anche Q ” che equivale alla formula logica: $P_1 \wedge P_2 \wedge \dots \wedge P_n \implies Q$. Le affermazioni P_1, P_2, \dots, P_n sono dette **ipotesi** mentre Q è la **tesi** del teorema. Come possiamo organizzare in modo rigoroso un ragionamento e stabilire che esso costituisce la dimostrazione di un teorema? Ci sono diverse strategie dimostrative variamente utilizzate:

- la **dimostrazione diretta** è la strategia più semplice e naturale per stabilire un teorema del tipo descritto. La dimostrazione diretta assume di trovarsi in un qualunque contesto in cui siano verificate le ipotesi e sulla base di semplici e rigorosi ragionamenti stabilisce che in tale contesto anche la tesi è verificata.
- la **dimostrazione per assurdo** consiste in una dimostrazione in cui si assume che la tesi sia falsa e da questa assunzione si deriva (utilizzando anche le ipotesi) una contraddizione, ovvero una proposizione della forma $p \wedge (\neg p)$ che asserisce che una qualche affermazione p è contemporaneamente vera e falsa. Questo prova che Q non può essere che vera in quanto il suo essere falso porterebbe a conclusioni assurde. In altre parole: si dimostra che se le premesse sono vere non è possibile che la tesi sia falsa.
- la **dimostrazione per contrapposizione** viene usata per dimostrare un teorema del tipo $p \implies q$ attraverso la dimostrazione (in modo diretto) del teorema: $\neg q \implies \neg p$. Infatti, supposto di aver stabilito la correttezza del teorema “non Q allora non P ” e di essere in un contesto in cui vale l’ipotesi P , allora, in tale contesto, anche Q deve essere vera, perché se fosse falsa (ovvero se valesse non Q) allora si avrebbe che sia P che non P sarebbero vere, contraddizione!

CORRISPONDENZE E RELAZIONI DI EQUIVALENZA

3.1

CORRISPONDENZE E RELAZIONI BINARIE



Definizione 3.1.1: Corrispondenza

Dati due insiemi a, b , una **corrispondenza** da a a b è una terna ordinata:

$$\rho = (a, b, G) \quad (3.1)$$

tale che: $G \subseteq a \times b$. L'insieme G prende il nome di **grafico** della corrispondenza ρ .

Per ogni $x \in a$ e per ogni $y \in b$ scriveremo: $x \rho y \iff (x, y) \in G$ per dire che gli elementi x e y sono in *corrispondenza* mediante ρ . In questo caso si dice che y è il **corrispondente** di x (non il contrario!). La coppia ordinata (x, y) appartiene quindi al grafico G . Con il simbolo $Corr(a, b)$ si denota l'insieme di tutte le corrispondenze tra a e b :

$$Corr(a, b) = \{(a, b, G) \mid G \subseteq a \times b\} \quad (3.2)$$

Definizione 3.1.2: Relazioni binarie

Una **relazione binaria** è una corrispondenza tra un insieme a e se stesso. Con il simbolo $Rel(a)$ si denota l'insieme di tutte le relazioni binarie in a :

$$Rel(a) = Corr(a, a) \quad (3.3)$$

Definizione 3.1.3: Diagonale

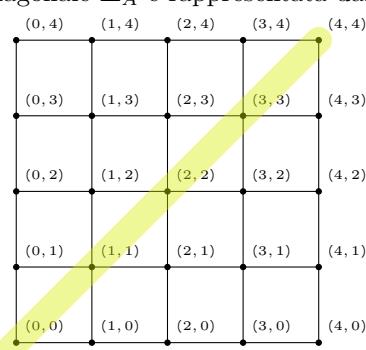
Sia a un insieme. L'insieme:

$$\Delta_a = \{(x, x) \mid x \in a\} \subset a \times a \quad (3.4)$$

prende il nome di **diagonale** di a e lo si indica col simbolo Δ_a .

Esempio 3.1.1

Si consideri l'insieme $A = \{0, 1, 2, 3, 4\}$, la diagonale Δ_A è rappresentata dall'area gialla evidenziata di seguito:



Esempio 3.1.2

Tra le relazioni binarie in un insieme s vi sono la **relazione identica** $\iota_s = (s, s, \Delta_s)$ e la **relazione totale** $\tau_s = (s, s, s \times s)$. È chiaro che nella relazione identica ogni elemento è in relazione soltanto con se stesso mentre nella relazione totale ogni elemento di s è in relazione con ciascun elemento.

3.1.1 ■ Proprietà delle relazioni binarie

Definizione 3.1.4: Relazione opposta

Sia $\rho = (s, s, G)$ una relazione binaria nell'insieme non vuoto s e si ponga $G^* = \{(y, x) \mid (x, y) \in G\}$. Allora la coppia $\rho^* = (s, s, G^*)$ è una relazione binaria in s che prende il nome di **relazione opposta** di ρ .

Sia s un insieme non vuoto. Per una relazione binaria $\rho = (s, s, G)$ in s si danno le seguenti definizioni:

- ρ si dice **riflessiva** se $\forall x \in s (x \rho x)$, cioè se il grafico G contiene la diagonale Δ_s ;
- ρ si dice **antiriflessiva** se $\forall x \in s (x \not\rho x)$, cioè se il grafico G è disgiunto dalla diagonale Δ_s ;
- ρ si dice **simmetrica** se per ogni coppia (x, y) di elementi di s tali che $x \rho y$ si ha anche $y \rho x$, cioè se ρ coincide con la sua relazione opposta ρ^* .
- ρ si dice **asimmetrica** se da $x \rho y$ e $y \rho x$ segue $x = y$.
- ρ si dice **transitiva** se qualunque siano gli elementi x, y e z di s tali che $x \rho y$ e $y \rho z$, si ha anche $x \rho z$.

3.1.2 ■ Rappresentazione delle corrispondenze

Esempio 3.1.3

Dati $A = \{0, 1, 2\}$ e $b = \{0, 4\}$ si avrà che l'insieme $A \times b$ conterrà le coppie ordinate:

$$A \times b = \{(0, 0), (0, 4), (1, 0), (1, 4), (2, 0), (2, 4)\}$$

Dunque esisteranno $2^6 = 64$ sottoinsiemi del prodotto cartesiano, ovvero 64 diverse tipologie di corrispondenze tra gli insiemi A e b . Per descrivere dunque una corrispondenza può essere comodo esprimere la **condizione di appartenenza** al grafico della corrispondenza. Ad esempio il grafico: $G = \{(x, y) \in A \times b \mid x < y\}$ esprime l'insieme:

$$G = \{(0, 4), (1, 4), (2, 4)\} \subset A \times b$$

Che descrive la seguente definizione di corrispondenza:

$$\alpha \in \text{Corr}(A, b) \quad \text{definito da} \quad \forall x \in A \ \forall y \in b \quad (x \alpha y \iff x < y)$$

Esempio 3.1.4

Oltre a rappresentare una corrispondenza mediante il proprio grafico è possibile utilizzare anche una rappresentazione grafica mediante i diagrammi di Venn oppure mediante tabelle. Si considerino gli insiemi $A = \{1, 2, 3\}$, $b = \{x, y\}$ e la corrispondenza $\rho = (A, b, \{(1, x), (1, y), (3, y)\})$. Si hanno quindi le seguenti rappresentazioni:

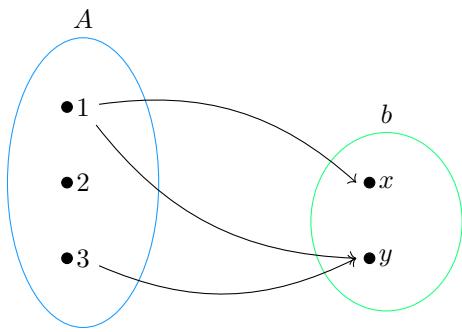


Figura 3.1: Diagrammi di Venn

	x	y
1	•	•
2		
3		•

Tabella 3.1: Rappresentazione tabellare

3.1.3 ■ Prodotto relazionale

Definizione 3.1.5: Prodotto relazionale

Siano A, B, C insiemi e $\varphi \in \text{Corr}(A, B)$, e $\psi \in \text{Corr}(B, C)$ corrispondenze. Il **prodotto relazionale** di φ per ψ , denotata con $\varphi\psi$, è la corrispondenza definita ponendo:

$$\forall a \in A, \forall c \in C \quad a \varphi\psi c \iff (\exists b \in B((a \varphi b) \wedge (b \psi c))) \quad (3.5)$$

Teorema 3.1.1 (Associatività del prodotto relazionale)

Il prodotto relazionale gode della proprietà associativa, cioè se: $\alpha \in \text{Corr}(A, B)$, $\beta \in \text{Corr}(B, C)$, $\gamma \in \text{Corr}(C, D)$ sono corrispondenze, allora vale:

$$(\alpha\beta)\gamma = \alpha(\beta\gamma) \quad (3.6)$$

Dimostrazione. Deve essere, per ogni $a \in A$ e per ogni $d \in D$:

$$\begin{aligned} a(\alpha\beta)\gamma d &\iff \exists c \in C(a \alpha b \wedge b \beta c \wedge c \gamma d) \\ &\iff \exists c \in C(\exists b \in B(a \alpha b \wedge b \beta c) \wedge c \gamma d) \\ &\iff \exists c \in C, \exists b \in B(a \alpha b \wedge b \beta c \wedge c \gamma d) \end{aligned}$$

Analogamente:

$$\begin{aligned} a\alpha(\beta\gamma)d &\iff \exists b \in B(a \alpha b \wedge b \beta c \wedge c \gamma d) \\ &\iff \exists b \in B(a \alpha b \wedge (\exists c \in C(b \beta c \wedge c \gamma d))) \\ &\iff \exists b \in B, \exists c \in C(a \alpha b \wedge b \beta c \wedge c \gamma d) \end{aligned}$$

Dato che le due condizioni sono equivalenti quindi le due corrispondenze coincidono. \square

Per ogni insieme A, B e per ogni corrispondenza $\alpha \in \text{Corr}(A, B)$ è possibile considerare i prodotti $\text{id}_A\alpha$ e αid_B :

$$A \xrightarrow{\text{id}_A} A \xrightarrow{\alpha} B \xrightarrow{\text{id}_B} B$$

E vale: $\text{id}_A\alpha = \alpha = \alpha\text{id}_B$. Infatti:

$$x \alpha b \implies (x \text{id}_A x \wedge x \alpha b) \implies x(\text{id}_A\alpha) b$$

e:

$$x(\text{id}_A\alpha) b \implies \exists y \in A(x \text{id}_A y \wedge y \alpha b) \implies x \alpha b$$

Analogamente, per ogni $x \in A$ e $b \in B$:

$$x \alpha b \implies (x \alpha b \wedge b \text{id}_B b) \implies x \alpha \text{id}_B b$$

e

$$x \alpha \text{id}_B b \implies \exists c \in B(x \alpha c \wedge c \text{id}_B b) \implies x \alpha b$$

3.2

APPLICAZIONI



Definizione 3.2.1: Applicazione

Un'**applicazione** (o *funzione* o *mappa*) di A in B è una corrispondenza $\varphi \in \text{Corr}(A, B)$ con la seguente proprietà:

$$\forall x \in A \quad (\exists! y \in B(x \varphi y)) \quad (3.7)$$

Per indicare che φ è un'applicazione di A in B scriveremo: $\varphi : A \rightarrow B$ oppure $A \xrightarrow{\varphi} B$. Per indicare che all'elemento $a \in A$ corrisponde l'unico elemento $b \in B$ scriveremo $\varphi(a) = b$ oppure $\varphi : a \mapsto b$, b è chiamata "**immagine** di a mediante φ ". L'insieme A prende il nome di **dominio** dell'applicazione mentre l'insieme B viene chiamato **codominio**.

Esempio 3.2.1

- La f assegna a ogni numero reale il suo quadrato, si abbia cioè, per ogni $x \in \mathbb{R}$ ($f(x) = x^2$). Dominio e codominio di f sono i numeri reali.
- La f associa ogni nazione la rispettiva capitale. Ora il dominio di f è l'insieme delle nazioni, e il suo codominio l'insieme delle città.

Definizione 3.2.2: Mappa

L'insieme delle funzioni dall'insieme A all'insieme B viene chiamato **mappa** e si indica col simbolo:

$$\text{Map}(A, B) = \{\varphi \mid \varphi : A \rightarrow B\}$$

Altre notazioni possibili sono quella esponenziale: B^A oppure $t(A, B)$.

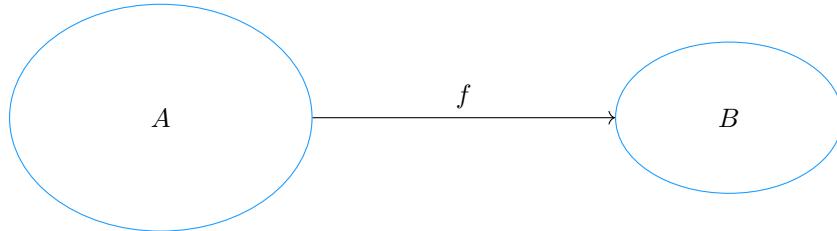


Figura 3.2: Diagramma di una mappa dall'insieme A all'insieme B

Osservazione 3.2.1 ➤➤➤

Definite le funzioni come terne ordinate si avrà, in base alla Proposizione 2.4.2, che due funzioni $f = (A, B, G_f)$ e $g = (C, D, G_g)$ si diranno equivalenti se, e soltanto se, hanno lo stesso dominio ($A = C$), lo stesso codominio ($B = D$) e lo stesso grafico ($G_f = G_g$).

Spesso per assegnare una funzione $f: A \rightarrow B$ si fornisce una "legge" ossia una qualche formula che permette di associare A ciascun elemento del dominio la sua immagine. Si faccia però attenzione al fatto che la funzione è caratterizzata soltanto dal dominio A , dal codominio B e dal grafico G e non dalla eventuale "formulazione della legge". I due esempi seguenti mostrano come una stessa "legge" può definire funzioni diverse e come, d'altra parte, "leggi" diverse possono definire una stessa funzione.

Esempio 3.2.2

- La funzione $f: \mathbb{Z} \rightarrow \mathbb{N}$ data da $f(n) = n^2$ e la funzione $g: \mathbb{N} \rightarrow \mathbb{Z}$ data da $g(n) = n^2$ sono diverse, perché non hanno lo stesso dominio e lo stesso codominio, ma, oltre a questo, hanno anche proprietà molto diverse. Usando la terminologia che definiremo in seguito, f non è iniettiva, mentre g lo è.
- Siano $A = \{0, 1, 2\}$ ed $f, g: A \rightarrow \mathbb{R}$ le funzioni definite rispettivamente da $f(x) = x - 7$ e $g(x) = x^3 - 3x^2 + 3x - 7$. Queste funzioni, per quanto espresse mediante "leggi" diverse, sono la stessa funzione, ossia $f = g$, poiché hanno lo stesso dominio, lo stesso codominio e lo stesso grafico: $G_f = G_g = \{(0, -7), (1, -6), (2, -5)\}$.

3.2.1 ■ Questione della ``buona posizione'' delle applicazioni

Soltanente si trovano notazioni del tipo: $x \in A \mapsto y \in B$ per indicare una funzione $t = (A \times B, G)$ dove: $G = \{(x, y) \mid x \in A, y \in B\}$ è il grafico della funzione. È importante saper distinguere le varie notazioni, infatti:

$\mathbb{N} \rightarrow \mathbb{Z}$ viene utilizzata per le corrispondenze tra insiemi
 $n \mapsto n + 1$ è la notazione per indicare il valore associato all'elemento n

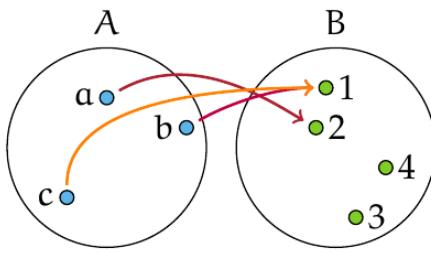
È possibile trovare anche notazioni più complicate:

$$s(x, y, z, \dots) \in A \mapsto t(x, y, z, \dots) \in B$$

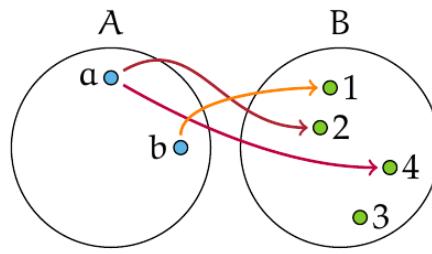
dove $s(x, y, z, \dots)$ è una espressione nelle variabili (x, y, z, \dots) . Non è sempre detto, però, che tali notazioni stiano ad indicare delle vere e proprie applicazioni "ben definite". Non sempre l'espressione $s(x, y, z, \dots)$ è *descrittiva di tutti gli elementi del dominio*, così facendo si otterrebbero elementi del dominio che non godono di corrispondente e questo non va bene secondo la definizione di applicazione. Analogamente, $t(x, y, z, \dots)$ deve associare uno ed uno solo elemento del codominio.

Esempio 3.2.3

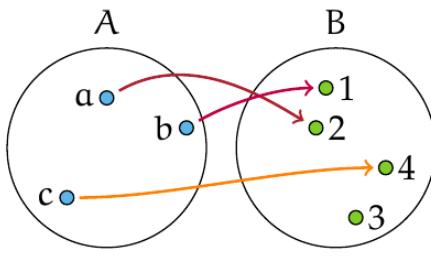
Analizziamo le corrispondenze rappresentate dai seguenti grafici:



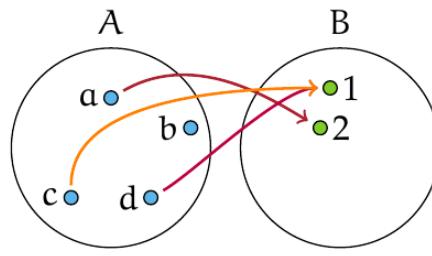
a



b



c



d

La corrispondenza di figura a rappresenta una funzione. La corrispondenza di figura b non rappresenta una funzione perché l'elemento a di A è in corrispondenza con due elementi di B , il 2 e il 4, quindi non è una corrispondenza univoca. La corrispondenza della figura c rappresenta una funzione. La corrispondenza della figura d non è una funzione perché il dominio non coincide con l'insieme A .

Esempio 3.2.4

L'applicazione: $\beta : x \in \mathbb{N} \mapsto x + 1 \in \mathbb{Z}$ è ben posta in quanto per ogni elemento $x \in \mathbb{N}$ esiste ed è unico il suo successivo definito in \mathbb{Z} .

Esempio 3.2.5

La corrispondenza $\alpha : n \in \mathbb{N} \mapsto n - 1 \in \mathbb{N}$ non è un'applicazione. Infatti l'elemento $0 \in \mathbb{N}$ non ammette precedente. Quando verifichiamo la buona posizione di una applicazione dobbiamo verificare che **tutti** i valori del dominio abbiano un corrispondente del codominio.

Esempio 3.2.6

La notazione $(a, b) \in \mathbb{R} \times \mathbb{R} \mapsto \frac{a}{b} \in \mathbb{R}$ non descrive una applicazione in quanto tutte le coppie di seconda coordinata nulla non hanno un loro corrispondente.

Esempio 3.2.7

L'applicazione $n \in \mathbb{N} \mapsto n - 1 \in \mathbb{Z}$ è un'applicazione dato che l'insieme di arrivo è quello dei numeri interi.

Esempio 3.2.8

La corrispondenza $X \in \mathcal{P}(\mathbb{Z}) \mapsto X \cap \mathbb{N} \in \mathcal{P}(\mathbb{N})$ è un'applicazione. Infatti ogni parte dell'insieme dei numeri interi, se intersecata con l'insieme dei numeri naturali, è una parte dell'insieme \mathbb{N} . Al contrario, la corrispondenza $\{x\} \in \mathcal{P}(\mathbb{Z}) \mapsto \{x\} \cap \mathbb{N} \in \mathcal{P}(\mathbb{N})$ non è un'applicazione. Infatti l'espressione $\{x\} \in \mathcal{P}(\mathbb{Z})$ non è *descrittiva* di tutti gli elementi del dominio $\mathcal{P}(\mathbb{Z})$, esistono quindi elementi che non hanno corrispondenti secondo la formula.

Esempio 3.2.9

La relazione:

$$f = (\mathbb{R} \times \mathbb{R}, G) \quad G = \{(x, y) \in \mathbb{R}^2 \mid y^2 = x\}$$

non è una funzione poiché contraddice la definizione di applicazione in quanto esistono sempre due numeri y_1, y_2 tali che $y_1^2 = y_2^2 = x$, ad esempio $(-2)^2 = 2^2 = 4$.

Esempio 3.2.10

$\{a, b\} \in \mathcal{P}(\mathbb{Z}) \mapsto a + b \in \mathbb{Z}$ **non** è una funzione poiché non tutti gli elementi del dominio hanno una propria immagine. Fissato invece, per ogni insieme A e per ogni naturale k , l'insieme:

$$\mathcal{P}_k(A) = \{X \in \mathcal{P}(A) \mid |X| = k\} \quad (3.8)$$

detto l'*insieme delle parti di A di cardinalità k*. Possiamo considerare quindi:

$$\begin{aligned} p : \{a, b\} \in \mathcal{P}_2(\mathbb{Z}) &\mapsto a + b \in \mathbb{Z} \\ q : \{a, b\} \in \mathcal{P}_2(\mathbb{Z}) &\mapsto a - b \in \mathbb{Z} \end{aligned}$$

Mentre p è una applicazione, q non lo è. Infatti elementi uguali di $\mathcal{P}_2(\mathbb{Z})$ hanno immagini distinte: ad esempio l'insieme $\{1, 2\}$ può essere riscritto anche come $\{2, 1\}$ ma

$$q(\{1, 2\}) = -1 \neq q(\{2, 1\}) = 1$$

Esempio 3.2.11

Analogamente all'esempio precedente si ha che: $(a, b) \in \mathbb{N}^2 \mapsto a - b \in \mathbb{N}$ **non** è una applicazione mentre la relazione: $(a, b) \in \mathbb{Z}^2 \mapsto a - b \in \mathbb{Z}$ lo è.

Definizione 3.2.3: Insieme immagine

Si definisce **immagine** dell'insieme A mediante l'applicazione φ l'insieme:

$$Im \varphi = \{\varphi(x) \mid x \in A\} \quad (3.9)$$

Esempio 3.2.12

Sia dato $X = \{1, 2, 3\}$ e sia $f : x \in X \mapsto \sqrt{x^2 + 3} \in \mathbb{R}$ e si voglia determinare l'insieme immagine della funzione f . In questo caso basta sostituire uno alla volta gli elementi del dominio nell'espressione di f e svolgere dei semplici passaggi algebrici:

$$\begin{aligned} f(1) &= \sqrt{1^2 + 3} = \sqrt{4} = 2 \\ f(2) &= \sqrt{2^2 + 3} = \sqrt{7} \\ f(3) &= \sqrt{3^2 + 3} = \sqrt{12} \end{aligned}$$

Esempio 3.2.13

Sia dato $X = \mathbb{R}$ e $f : x \in X \mapsto x + 1 \in \mathbb{R}$. Per determinare l'insieme immagine $Im(f)$ esplicitiamo la x in funzione della y :

$$\begin{aligned} y &= x + 1 && \text{Sposto il } +1 \text{ A sinistra e inverto il segno} \\ x &= y - 1 \end{aligned}$$

Che ha soluzione su tutto \mathbb{R} e tra l'altro coincide con il codominio della funzione, ovvero $Im(f) = cod(f) = \mathbb{R}$.

Definizione 3.2.4: Funzione costante

Siano A, B insiemi e sia $f \in Map(A, B)$. f si dice **costante** se e solo se

$$f(x) = f(y) \quad \forall x, y \in A \quad (3.10)$$

Fissato $h \in B$, l'applicazione $x \in A \mapsto h \in B$ si dice **funzione costante** h .

Esempio 3.2.14

Un esempio di applicazione costante è l'applicazione costante c_0 che associa ad ogni numero naturale l'elemento $0 \in \mathbb{N}$:

Definizione 3.2.5: Restrizione

Sia A un insieme, $f \in Map(A, B)$ e $T \subseteq A$. Possono definire una applicazione $r \in Map(T, B)$ come:

$$f|_T : x \in T \mapsto f(x) \in B \quad (3.11)$$

Questa applicazione è ben definita e si chiama **restruzione** di f a T .

Esempio 3.2.15

Sia: $\alpha : n \in \mathbb{Z} \mapsto n^2 + 1 \in \mathbb{N}$. Un esempio di restruzione si ottiene cambiando l'insieme di partenza con $\mathbb{N} \subset \mathbb{Z}$, ottenendo così l'applicazione:

$$\alpha|_{\mathbb{N}} : n \in \mathbb{N} \mapsto n^2 + 1 \in \mathbb{N}$$

Definizione 3.2.6: Prolungamento

Se $g : T \subseteq A \longrightarrow B$ è la restruzione di $f : A \longrightarrow B$, allora f viene detta **prolungamento** dell'applicazione g .

Definizione 3.2.7: Immersione

Per ogni insieme A e per ogni $T \subseteq A$, l'applicazione:

$$\iota : x \in T \mapsto x \in A \quad (3.12)$$

viene chiamata **immersione di T in A** e si denota col simbolo $\iota := T \hookrightarrow A$.

Osservazione 3.2.2



L'immersione è la *restruzione dell'applicazione identica id_A* all'insieme $T \subseteq A$. Inoltre, per ogni applicazione $f : A \longrightarrow B$ si ha:

$$f \circ \iota = f(\iota(x)) = f(x)$$

Quindi $f \circ \iota : x \in T \mapsto f(x) \in B$ è proprio $f|_T$. Quindi una restruzione si ottiene componendo una applicazione con una immersione.

Esempio 3.2.16

L'applicazione identica id_A è un'immersione di A in A :

$$id_A = A \hookrightarrow A$$

Ogni applicazione $f : A \longrightarrow B$ può essere considerata come restruzione di sé stessa rispetto all'insieme A : $f = f|_A$.

Definizione 3.2.8: Applicazione ridotta

Sia $f : A \rightarrow B$, per ogni sottoinsieme $C \subseteq B$ tale che $im f \subseteq C$, l'applicazione:

$$x \in A \mapsto f(x) \in C \quad (3.13)$$

si chiama **ridotta** di f a C e si indica col simbolo $f|_C$.

Definizione 3.2.9: Applicazione immagine

Siano a, b due insiemi ed $f : A \rightarrow B$ un'applicazione. L'applicazione:

$$\vec{f} : C \in \mathcal{P}(A) \mapsto \{f(x) \mid x \in C\} \in \mathcal{P}(B) \quad (3.14)$$

è chiamata **applicazione immagine** definita da f .

Proposizione 3.2.1

Siano A e B due insiemi e consideriamo l'applicazione $f : A \rightarrow B$. Per ogni $C \in \mathcal{P}(A)$:

$$\vec{f}(C) = Im(f|_C) = \{f(x) \mid x \in C\} \quad (3.15)$$

$$\vec{f}(A) = Im(f) \quad (3.16)$$

Ovvero:

- L'applicazione immagine di un sottoinsieme $C \subseteq A$ è l'insieme immagine della restrizione dell'applicazione f all'insieme C ;
- L'applicazione immagine del dominio coincide con l'insieme immagine dell'applicazione f .

Esempio 3.2.17

Sia $f : n \in \mathbb{Z} \mapsto |n| \in \mathbb{N}$ e sia $X = \{0, 1, -1\}$, allora $\vec{f}(X) = \{0, 1\}$.

Definizione 3.2.10: Applicazione antimimmagine

Siano A, B due insiemi ed $f : A \rightarrow B$ un'applicazione. Si definisce **applicazione antimimmagine** definita da f l'applicazione:

$$\overleftarrow{f} : C \in \mathcal{P}(B) \mapsto \{x \in A \mid f(x) \in C\} \in \mathcal{P}(A) \quad (3.17)$$

Proposizione 3.2.2

Siano A, B insiemi e sia $f : A \rightarrow B$ un'applicazione di A in B . Allora:

$$\overleftarrow{f}(B) = \{x \in A \mid f(x) \in B\} = A = \overleftarrow{f}(im f) \quad (3.18)$$

Ovvero, l'antimmagine del codominio B coincide con il dominio A che a sua volta coincide con l'antimmagine dell'insieme immagine dell'applicazione f . Ovviamente si ha anche che: $\overleftarrow{f}(\emptyset) = \emptyset$.

Esempio 3.2.18

Sia $f : n \in \mathbb{Z} \mapsto |n| \in \mathbb{N}$, allora se consideriamo il sottoinsieme $\{1, 2, 3\} \subseteq \mathbb{N}$ si ha:

$$\overleftarrow{f}(\{1, 2, 3\}) = \{-1, 1, -2, 2, -3, 3\}$$

Le proprietà seguenti saranno importanti per poter caratterizzare le applicazioni iniettive e suriettive. Siano infatti A, B due insiemi non vuoti e sia $f : A \rightarrow B$. È opportuno notare che in generale risulta:

$$\begin{aligned} \forall C \in \mathcal{P}(A) (C \neq \overleftarrow{f}(\vec{f}(C))) \\ \forall Y \in \mathcal{P}(B) (Y \neq \vec{f}(\overleftarrow{f}(Y))) \end{aligned}$$

Se C è una parte di A e $x \in C$, si ha $f(x) \in \vec{f}(C)$ e quindi $x \in \overleftarrow{f}(\vec{f}(C))$. Quindi $C \subseteq \overleftarrow{f}(\vec{f}(C))$ (l'inclusione può essere stretta come mostrato nel prossimo esempio). Sia invece Y un sottoinsieme del codominio B di f . Qualunque sia l'elemento z di $\vec{f}(\overleftarrow{f}(Y))$ risulta $z = f(x)$ con $x \in \overleftarrow{f}(Y)$. Allora $z = f(x)$ appartiene a Y e perciò $\vec{f}(\overleftarrow{f}(Y)) \subseteq Y$. In particolare $\vec{f}(\overleftarrow{f}(Y)) = Y \cap im f$.

Esempio 3.2.19

Sia $T = \{3\}$ e sia $f : n \in \mathbb{Z} \mapsto n^2 \in \mathbb{Z}$. Allora:

$$\vec{f}(\{3\}) = \{f(x) \mid x \in \{3\}\} = \{9\}$$

e

$$\overleftarrow{f}(\vec{f}(\{3\})) = \overleftarrow{f}(\{9\}) = \{n \in \mathbb{Z} \mid 9 = n^2\} = \{+3, -3\}$$

e vale $T \subset \overleftarrow{f}(\vec{f}(T))$.

3.2.2 Composizione tra applicazioni

Proposizione 3.2.3

Supponiamo di avere due applicazioni componibili come corrispondenze. Siano quindi:

$$\begin{aligned}\alpha : A &\longrightarrow B \\ \beta : B &\longrightarrow C\end{aligned}$$

due applicazioni siffatte. Allora $\alpha\beta$ è ancora un'applicazione, chiamata **applicazione composta**.

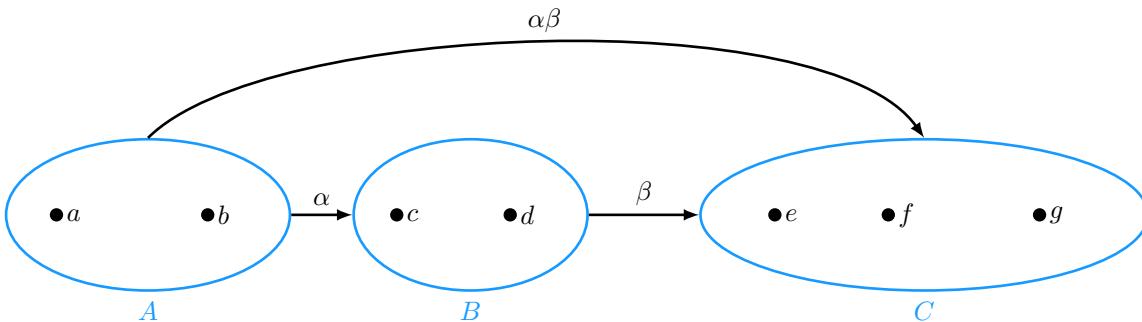


Figura 3.3: Esempio di composizione delle applicazioni $\alpha : A \rightarrow B$ e $\beta : B \rightarrow C$

Dimostrazione. Per ogni $a \in A$ possiamo considerare l'elemento $\beta(\alpha(a)) \in C$. Quindi l'elemento $a \in A$ rispetto alla corrispondenza $\alpha\beta$ ha $\beta(\alpha(a)) \in C$ come corrispondente. Bisogna dimostrare che questo è unico stando alla definizione di applicazione.

Supponiamo di avere $c \in C$ tale che sia un corrispondente rispetto a $\alpha\beta$ di $a \in A$. Ciò sta a significare che $\exists b \in B (a \alpha b \wedge b \beta c)$. Ma se $a \alpha b$ allora, per definizione di applicazione, $b = \alpha(a)$ e $c = \beta(b) = \beta(\alpha(a))$. Quindi per ogni elemento $a \in A$ esiste ed è unico il corrispondente $c \in C$ ovvero $\beta(\alpha(a))$. Ciò dimostra che $\alpha\beta$ è una applicazione. \square

Spesso si usa indicare il prodotto relazionale $\alpha\beta$ con $\beta \circ \alpha$ dove \circ indica il simbolo dell'operazione di prodotto relazionale.

La composizione tra applicazioni, così come il prodotto relazionale, non gode della proprietà commutativa. Non vale cioè, date due applicazioni $\alpha : a \rightarrow b$ e $\beta : b \rightarrow c$, $\alpha\beta = \beta\alpha$ o, equivalentemente, $\beta \circ \alpha = \alpha \circ \beta$. Infatti, continuando ad utilizzare la notazione "cerchietto", osserviamo che non esiste una applicazione del tipo $\alpha \circ \beta$ in quanto β mappa ogni elemento dell'insieme b nell'insieme c mentre α è applicata solo e soltanto sugli elementi di a e non ha senso quindi valutare l'espressione $\alpha(z)$ dove $z = g(y)$. La composizione tra applicazioni gode, però, della proprietà associativa come già osservato per le corrispondenze:

Proposizione 3.2.4

Siano $f : a \rightarrow b$, $g : b \rightarrow c$ e $h : c \rightarrow d$ tre applicazioni tra gli insiemi a, b, c, d . Vale allora:

$$f(gh) = (fg)h \quad (3.19)$$

o, equivalentemente:

$$(h \circ g) \circ f = h \circ (g \circ f) \quad (3.20)$$

Esempio 3.2.20

Sia:

$$\alpha : n \in \mathbb{Z} \mapsto n + 1 \in \mathbb{Z}$$

Allora:

$$\alpha^2 = \alpha\alpha : n \in \mathbb{Z} \mapsto \alpha(\alpha(n)) \in \mathbb{Z}$$

ovvero, per ogni $n \in \mathbb{Z}$ si ha: $\alpha(\alpha(n)) = \alpha(n + 1) = (n + 1) + 1 = n + 2$. Sia ora:

$$\beta : m \in \mathbb{Z} \mapsto \{m\} \in \mathcal{P}(\mathbb{Z})$$

un'applicazione. Allora $\alpha\beta = \beta \circ \alpha : \mathbb{Z} \longrightarrow \mathcal{P}(\mathbb{Z})$ e sarà:

$$\beta(\alpha(n)) = \beta(n + 1) = \{n + 1\}$$

Osservazione 3.2.3



Sia $s = \{x, y\}$ un insieme composto da due elementi distinti. È possibile quindi considerare le applicazioni costanti:

$$\begin{aligned} c_{s,x} : a \in s &\mapsto x \in s \\ c_{s,y} : a \in s &\mapsto y \in s \end{aligned}$$

Componendole, si ottiene:

$$\begin{aligned} c_{s,x} \circ c_{s,y} &= c_{s,x} \\ c_{s,y} \circ c_{s,x} &= c_{s,y} \end{aligned}$$

Da questo esempio si osserva inoltre che la composizione tra applicazioni non gode della proprietà commutativa. In particolare, se $|s| = 2$ allora l'insieme delle trasformazioni in s , s^s , non è abeliano.

3.3

SURIETTIVITÀ E INIETTIVITÀ



3.3.1 ■ Funzioni iniettive

Definizione 3.3.1: Applicazione iniettiva

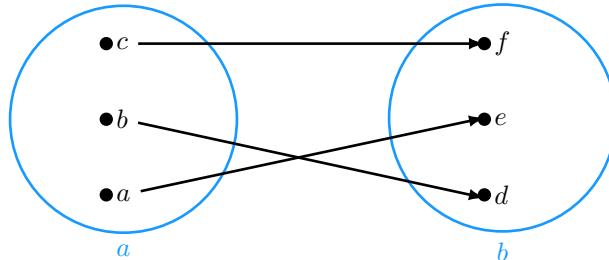
Una funzione $f : a \rightarrow b$ si dice **iniettiva** se:

$$\forall x, y \in a (x \neq y \implies f(x) \neq f(y)) \quad (3.21)$$

oppure

$$\forall x, y \in a (f(x) = f(y) \implies x = y) \quad (3.22)$$

Per farsi un'idea visivamente di cosa sia una applicazione iniettiva si può osservare il seguente diagramma:



Si può notare infatti che ogni elemento di a ha una immagine nel codominio b diversa da quella di ciascun altro elemento.

Osservazione 3.3.1



Una applicazione $f : a \rightarrow b$ non è iniettiva se e soltanto se:

$$\exists x, y \in a (x \neq y \wedge f(x) = f(y))$$

Ovvero se esistono elementi diversi di a che hanno la medesima immagine.

Esempio 3.3.1

L'applicazione id_a è iniettiva. Se infatti $id_a(x) = id_a(y)$ allora $x = y$.

Sia $t \subset a$, l'immersione $\iota : x \in t \mapsto x \in a$ è iniettiva. Infatti, se $\iota(x) = \iota(y)$ allora $x = y$.

L'applicazione $\alpha : n \in \mathbb{Z} \mapsto n^2 \in \mathbb{Z}$ non è iniettiva, infatti presi gli elementi distinti 1 e -1 si ha:

$$\alpha(-1) = \alpha(1)$$

Al contrario, l'applicazione $\beta : n \in \mathbb{N} \mapsto n^2 \in \mathbb{N}$ è iniettiva.

Osservazione 3.3.2



Se f è un'applicazione iniettiva, per ogni $t \subseteq a$ allora la restrizione di f a t :

$$f|_t : x \in t \mapsto f(x) \in b$$

è iniettiva. Infatti, presi due elementi $a, b \in t$ si ha, dall'iniettività di f

$$f(a) = f(b) \implies a = b$$

quindi vale in particolare anche per la restrizione di f a t . Quindi $f|_t$ è iniettiva.

Proposizione 3.3.1 (Caratterizzazione dell'iniettività mediante antimmagini)

Un'applicazione $f : a \rightarrow b$ è iniettiva, se e soltanto se

$$\forall y \in b \left(|\overleftarrow{f}(\{y\})| \leq 1 \right)$$

Ovvero se e soltanto se per ogni singleton sottoinsieme del suo codominio, la sua antimmagine è vuota o ha un solo elemento.

Dimostrazione. \implies Supponiamo che f sia iniettiva e prendiamo un $y \in b$. Supponiamo che non sia vera la tesi, ovvero che l'antimmagine del singleton di y non abbia al massimo un elemento. Se $|\overleftarrow{f}(\{y\})| \neq 1$ allora esistono $a, b \in a$ tali che $a \neq b \wedge a, b \in \overleftarrow{f}(\{y\})$. Ma dire che $a \in \overleftarrow{f}(\{y\})$ significa che $f(a) = y$ e $b \in \overleftarrow{f}(\{y\})$ che $f(b) = y$. Quindi $f(a) = f(b)$ con $a \neq b$ distinti e ciò va in contraddizione con la nostra ipotesi. Quindi $\overleftarrow{f}(\{y\})$ non può avere più di un elemento se f è iniettiva.

\impliedby Viceversa, se f non è iniettiva, vale:

$$\exists x, y \in a (x \neq y \wedge f(x) = f(y))$$

Quindi, fissato $a, b \in a$ tali che $a \neq b \wedge f(a) = f(b)$, ponendo $y = f(a)$, abbiamo $a \in \overleftarrow{f}(\{y\})$ e anche $b \in \overleftarrow{f}(\{y\})$. Abbiamo così trovato due elementi diversi in $\overleftarrow{f}(\{y\})$ che avrà quindi più di un elemento. Di fatto, se f non è iniettiva allora $\overleftarrow{f}(\{y\})$ avrà più di un elemento. Per contrapposizione si ottiene la tesi.

□

Proposizione 3.3.2

Siano $f : a \rightarrow b$ e $g : b \rightarrow c$ due applicazioni. Se f, g sono iniettive allora anche l'applicazione $g \circ f$ è iniettiva.

Dimostrazione. Siano $f : a \rightarrow b$ e $g : b \rightarrow c$ due funzioni iniettive. Siano $w, z \in a$ tali che $g \circ f(w) = g \circ f(z)$. Questo equivale a dire che $g(f(w)) = g(f(z))$. Essendo g iniettiva, allora $f(w) = f(z)$. Ma, essendo f iniettiva, allora $w = z$. Pertanto la funzione composta è iniettiva.

□

Proposizione 3.3.3

Siano $f : a \rightarrow b$ e $g : b \rightarrow c$ due applicazioni. Se l'applicazione composta $g \circ f$ è iniettiva allora f è iniettiva.

Dimostrazione. Siano x e x' elementi di a tali che $f(x) = f(x')$. Allora risulta:

$$(g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x')$$

e quindi $x = x'$, in quanto $g \circ f$ è iniettiva. Pertanto f è iniettiva.

□

3.3.2 ■ Funzioni suriettive

Definizione 3.3.2: Applicazioni suriettive

L'applicazione f si dice **suriettiva** se e solo se $im(f) = b$ e vale la seguente catena di implicazioni:

$$im(f) = b \iff b \subseteq Im(f) \quad (3.23)$$

$$\iff \forall y \in b(y \in Im(f)) \quad (3.24)$$

$$\iff \forall y \in b(\exists x \in a(y = f(x))) \quad (3.25)$$

Proposizione 3.3.4 (Caratterizzazione suriettività mediante le antimmagini)

Sia f una applicazione da a in b ; f è suriettiva se e soltanto se, per ogni $y \in b$:

$$\forall y \in b(\overleftarrow{f}(\{y\}) \neq \emptyset) \quad (3.26)$$

Dimostrazione. Infatti, fissato un elemento $y \in b$ si ha sicuramente $\{y\} \subseteq b$, quindi ha senso considerare l'insieme:

$$\overleftarrow{f}(\{y\}) = \{x \in a \mid f(x) \in \{y\}\} = \{x \in a \mid f(x) = y\}$$

Se la funzione $a \xrightarrow{f} b$ è suriettiva allora sicuramente l'insieme degli elementi del dominio che hanno per immagine $y \in b$ è non vuoto. Vale cioè l'implicazione:

$$\forall y \in b(y \in Im(f) \iff (\overleftarrow{f}(\{y\}) \neq \emptyset))$$

□

Osservazione 3.3.3



Quando definiamo un concetto è importante fare qualche esempio. Per considerare una applicazione suriettiva è bene tenere a mente cosa *non* è una applicazione suriettiva. Negando la definizione quindi si ottiene che una applicazione $f : a \longrightarrow b$ non è suriettiva se e soltanto se:

- $im f \neq b \iff b \not\subseteq im f$
- $\exists y \in b(\forall x \in a(y \neq f(x)))$
- $\exists y \in b \setminus im f$

Esempio 3.3.2

L'applicazione identica in un insieme a è suriettiva. Infatti $\forall a \in a(\exists a \in a(id_a(a) = a))$, ovvero a stesso.

Esempio 3.3.3

Se $t \subset a$ e consideriamo l'immersione $t \hookrightarrow a$ questa non è suriettiva in quanto esistono elementi del codominio che non sono immagine degli elementi del dominio.

Esempio 3.3.4

L'applicazione $n \in \mathbb{Z} \mapsto n^2 \in \mathbb{Z}$ non è suriettiva. Infatti non tutti i numeri interi possono essere espressi come quadrato di un numero intero relativo. Ad esempio il numero $5 \in \mathbb{Z}$.

Esempio 3.3.5

L'applicazione $n \in \mathbb{Z} \mapsto |n| \in \mathbb{Z}$ non è suriettiva. Non tutti gli interi relativi possono essere espressi come il valore assoluto di un numero intero. Se però consideriamo la ridotta di tale applicazione:

$$n \in \mathbb{Z} \mapsto |n| \in \mathbb{N}$$

questa è suriettiva in quanto ogni numero naturale rispetta tale condizione.

Esempio 3.3.6

Diamo esempi grafici di un'applicazione suriettiva (Figura 3.4) e di una non suriettiva (Figura 3.5).

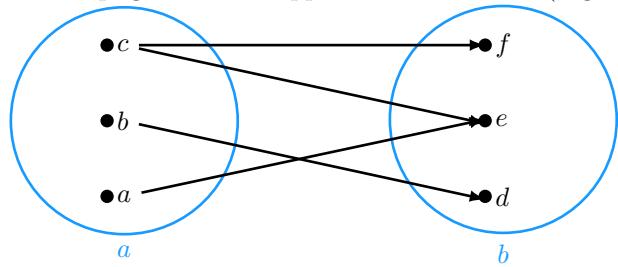


Figura 3.4

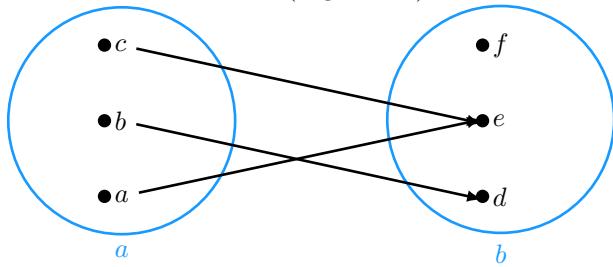


Figura 3.5

In generale, per dimostrare la suriettività di una applicazione bisogna eseguire una dimostrazione che giustifichi la validità di una delle condizioni definite in 3.23. Spesso però trovare una strategia vincente può risultare lungo e contorto. In questi casi le opzioni sono due: si procede per tentativi fino a quando non si trova un indizio sulla validità universale della condizione oppure si cerca un controesempio che dimostri che l'applicazione data non sia suriettiva.

Esempio 3.3.7

Consideriamo l'applicazione:

$$\mu : x \in \mathcal{P}(\mathbb{Z}) \mapsto x \cap \mathbb{N} \in \mathcal{P}(\mathbb{N})$$

Per dimostrare che questa applicazione sia suriettiva bisogna dimostrare che vale la condizione:

$$\forall y \in \mathcal{P}(\mathbb{N}) (\exists x \in \mathcal{P}(\mathbb{Z}) (\mu(x) = y)) \quad (3.27)$$

Non sapendo come procedere inizio considerando un elemento a piacere di $\mathcal{P}(\mathbb{N})$, ad esempio $\{3\}$. La domanda che ci si pone sarà:

“Esiste una parte di \mathbb{Z} la cui intersezione con \mathbb{N} sia uguale a $\{3\}$?”

Ovviamente sì e tale parte è $\{3\}$ stesso. Sostituendo a $\{3\}$ un qualsiasi elemento di $\mathcal{P}(\mathbb{N})$ notiamo che la risposta è sempre la stessa e quindi, generalizzando:

$$\forall y \in \mathcal{P}(\mathbb{Z}) (\mu(y) = y \cap \mathbb{N} = y \in \mathcal{P}(\mathbb{N}))$$

Proposizione 3.3.5

Siano a, b, c insiemi e $f : a \rightarrow b$, $g : b \rightarrow c$ due applicazioni. È possibile quindi considerare l'applicazione composta $g \circ f$. Allora, se f, g sono suriettive anche $g \circ f$ è suriettiva.

Dimostrazione. Se f, g sono applicazioni suriettive, per dimostrare che la loro composta è suriettiva bisogna far vedere che:

$$\forall z \in C (\exists x \in A (z = g \circ f(x)))$$

Ma sappiamo che $g \circ f(x) = g(f(x))$ e per la suriettività dell'applicazione g :

$$\forall z \in C (\exists y \in B (z = g(y)))$$

e per la suriettività di f si ha:

$$\forall z \in C (\exists y \in B (\exists x \in A (z = g(f(x)))))$$

il che dimostra la tesi. □

Proposizione 3.3.6

Se l'applicazione $g \circ f$ è suriettiva allora l'applicazione g è suriettiva.

Dimostrazione. L'obiettivo è quello di dimostrare che:

$$\forall x \in C (\exists y \in B (x = g(y)))$$

Dato che $g \circ f$ è suriettiva sappiamo che:

$$\forall x \in C (\exists x' \in A (x = g \circ f(x')))$$

Quindi preso $y = f(x') \in B$ si ha:

$$c = g(f(x'))$$

e quindi g è suriettiva. □

3.3.3 ■ Funzioni biettive

Definizione 3.3.3: Applicazione biettiva

Un'applicazione $a \xrightarrow{f} b$ si dice **biettiva** se è sia iniettiva che suriettiva.

Proposizione 3.3.7

Un'applicazione $f : a \longrightarrow b$ è biettiva

$$\iff \forall y \in b (\overleftarrow{f}(\{y\}) = 1) \quad (3.28)$$

$$\iff \forall y \in b (\exists! x \in a (f(x) = y)) \quad (3.29)$$

Corollario 3.3.1

Siano $f : a \longrightarrow b$ e $g : b \longrightarrow c$ due applicazioni. Allora:

1. Se f, g sono biettive allora $g \circ f$ è biettiva.
2. Se $g \circ f$ è biettiva allora g è suriettiva e f è iniettiva.

3.4

SEZIONI E RETRAZIONI



Definizione 3.4.1: Sezione

Sia $f : a \longrightarrow b$. Si chiama **sezione** di f un'applicazione $h : b \longrightarrow a$ tale che:

$$f \circ h = id_b \quad (3.30)$$

Teorema 3.4.1

Un'applicazione $f : a \longrightarrow b$ è suriettiva se e solo se f ha una sezione.

Dimostrazione. Supponiamo che esista una sezione $h : b \longrightarrow a$. Allora:

$$f \circ h = id_b$$

è suriettiva in quanto id_b è suriettiva. Quindi, essendo tale applicazione suriettiva si ha che f è suriettiva.

Viceversa se f è suriettiva, sappiamo che:

$$\forall y \in b (\exists x \in a (y = f(x)))$$

cioè:

$$\overleftarrow{f}(\{y\}) \neq \emptyset$$

Quindi $\forall y \in b$ scegliamo un $a_y \in \overleftarrow{f}(\{y\})$ che sicuramente esiste in quanto non vuoto. È possibile quindi considerare l'applicazione:

$$f \circ h = f(h(y)) = f(a_y) = y = id_b(y)$$

e quindi h è una sezione di f . □

Osservazione 3.4.1



Dal teorema appena dimostrato concludiamo che se una applicazione $f : a \longrightarrow b$ non è suriettiva allora non ha sezioni.

Esempio 3.4.1

L'applicazione $w : n \in \mathbb{Z} \mapsto |n| \in \mathbb{Z}$ non è suriettiva (i numeri interi negativi non possono essere espressi in termini di valore assoluto di un numero intero relativo) e quindi non ha sezioni. L'applicazione $v : n \in \mathbb{Z} \mapsto |n| \in \mathbb{N}$ è invece suriettiva e ammette sezioni. Ad esempio:

$$\sigma_1 : n \in \mathbb{N} \mapsto n \in \mathbb{Z}$$

è una sezione e vale: $v \circ \sigma_1(n) = v(\sigma_1(n)) = v(n) = |n| = n = id_{\mathbb{N}}(n)$, analogamente anche l'applicazione:

$$\sigma_2 : n \in \mathbb{N} \mapsto -n \in \mathbb{Z}$$

è una sezione e vale: $v \circ \sigma_2(n) = v(\sigma_2(n)) = v(-n) = |-n| = n = id_{\mathbb{N}}(n)$.

Definizione 3.4.2: Retrazione

Sia $f : a \rightarrow b$ un'applicazione. Si chiama **retrazione** di f un'applicazione $h : b \rightarrow a$ tale che:

$$h \circ f = id_a \quad (3.31)$$

Teorema 3.4.2

Un'applicazione $f : A \rightarrow B$ è iniettiva se e solo se $A = \emptyset$ oppure f ha una retrazione.

Dimostrazione. \Leftarrow Se f ha una retrazione allora è iniettiva, infatti, presa la retrazione $h : B \rightarrow A$:

$$h \circ f = id_A$$

con id_A biettiva, quindi f è iniettiva.

\Rightarrow Sia f iniettiva. Chiaramente, per ogni elemento $y \in im f$ si ha:

$$|\overleftarrow{f}(\{y\})| = 1$$

Allora $\exists! a_y \in a (y = f(a_y))$ Fissato $z \in a$ posso considerare l'applicazione:

$$h : y \in b \mapsto \begin{cases} a_y & \text{se } y \in im f \\ z & \text{se } y \notin im f \end{cases} \in A$$

Dimostriamo che h è una retrazione di f . Per ogni $x \in a$ si ha:

$$(h \circ f) = h(f(x)) = a_{f(x)}$$

dove $a_{f(x)}$ è l'unico elemento di a tale che $f(a_{f(x)}) = f(x)$ ovvero x stesso. Quindi $h \circ f : A \rightarrow A$ è un'applicazione che mappa ogni elemento in sé stesso. Di conseguenza $h \circ f = id_A$ ed h è una retrazione di f . □

Esempio 3.4.2

Si consideri l'insieme $s = \{1, 2, 3\}$ e sia $t = \{1, 2\} \subset s$ una parte propria di s . Dato che l'immersione $t \hookrightarrow s$ è una applicazione iniettiva allora questa applicazione ammette retrazioni. Ad esempio due possibili retrazioni di $\iota : x \in t \mapsto x \in s$ sono:

$$\rho_1 : x \in s \mapsto \begin{cases} 1 & \text{se } x = 1 \\ 2 & \text{se } x = 2 \\ 1 & \text{se } x = 3 \end{cases} \in t, \quad \rho_2 : x \in s \mapsto \begin{cases} 1 & \text{se } x = 1 \\ 2 & \text{se } x = 2 \\ 2 & \text{se } x = 3 \end{cases} \in t$$

In entrambi i casi, le restrizioni delle funzioni ρ_1 e ρ_2 a t sono le identità, in quanto mappano gli elementi di t in se stessi.

3.4.1 ■ Applicazioni inverse

Teorema 3.4.3 (Unicità dell'applicazione inversa)

Sia $f : a \rightarrow b$ un'applicazione. Se f ha una sezione σ e una retrazione ρ , allora $\sigma = \rho$ è un'inversa di f , inoltre s è l'unica sezione e l'unica retrazione di f .

Dimostrazione. Poiché σ è una sezione di f si ha: $f \circ \sigma = id_b$, poiché ρ è una retrazione di f si ha: $\rho \circ f = id_a$. Allora:

$$\begin{aligned}\sigma &= id_a \circ \sigma \\ &= (\rho \circ f) \circ \sigma \\ &= \rho \circ (f \circ \sigma) \\ &= \rho \circ id_b = \rho\end{aligned}$$

Dunque σ è sia una sezione che una retrazione di f , quindi ne è un'inversa. Se σ_1 è una qualsiasi sezione di f , applicando a σ_1 e ρ la prima parte dell'enunciato appena dimostrata, si ottiene $\sigma_1 = \rho$, quindi $\sigma_1 = \sigma$. Per lo stesso motivo, se ρ_1 è una retrazione di f si deve avere $\rho_1 = \rho$. Ciò prova l'unicità di σ come sezione e come retrazione di f . \square

Definizione 3.4.3: Applicazione inversa

Sia $f : a \rightarrow b$ un'applicazione, una applicazione $h : b \rightarrow a$ viene detta **inversa** di f se e solo se h è una sezione ed una retrazione di f .

Dato che id_b è iniettiva allora h è iniettiva, analogamente, essendo id_a suriettiva si ha che h è suriettiva. Quindi h è biettiva.

Teorema 3.4.4

Sia $f : a \rightarrow b$ un'applicazione. Sono equivalenti:

1. f è biettiva;
2. f ha una ed una sola sezione (ed una retrazione);
3. f è invertibile

Dimostrazione. Che (3) implica (2) è ovvio, che (2.) implica 3. è stato dimostrato col Teorema 3.4.3. Nel caso in cui il dominio di f non sia vuoto, l'equivalenza tra (1.) e (2) segue immediatamente da 3.4.1 e 3.4.2. Nel caso in cui il dominio sia vuoto f è invertibile se e solo se anche il codominio di f è vuoto; d'altra parte è chiaro che quest'ultima condizione è necessaria e sufficiente affinché f sia biettiva. Dunque, anche in questo caso le proposizioni sono equivalenti. \square

Corollario 3.4.1

L'inversa di una applicazione, se esiste, è unica. L'unica inversa di un'applicazione invertibile viene indicata come f^{-1} .

Corollario 3.4.2

Affermare che una applicazione $f : A \rightarrow B$ equivale a dire che:

$$\forall y \in b \left(\exists! x \in A (f(x) = y) \right) \quad (3.32)$$

3.5

PARTIZIONI E RELAZIONI DI EQUIVALENZA



3.5.1 ■ Partizioni

Definizione 3.5.1: Partizione

Sia a un insieme non vuoto. L'insieme $b = \{x \mid x \subseteq a\}$ si dice **partizione** di a se:

1. Ogni elemento di b è diverso dall'insieme vuoto: $\forall x \in b (x \neq \emptyset)$
2. L'unione degli elementi di b corrisponde ad a : $\bigcup b = a$
3. Gli elementi di b sono a due a due disgiunti: $\forall x, y \in b (x \cap y = \emptyset)$

L'insieme delle partizioni di a viene indicato con il nome $Partz(a)$.

Osservazione 3.5.1



L'unica partizione dell'insieme vuoto è l'insieme vuoto stesso.

3.5.2 ■ Relazioni di equivalenza

Definizione 3.5.2: Relazione di equivalenza

Una relazione binaria \sim in a è una **relazione di equivalenza** se e solo se verifica ciascuna delle tre proprietà:

1. **Riflessiva:** $\forall x \in a(x \sim x)$
2. **Simmetrica:** $\forall x, y \in a(x \sim y \Rightarrow y \sim x)$
3. **Transitiva:** $\forall x, y, z \in a((x \sim y \wedge y \sim z) \Rightarrow x \sim z)$

Indichiamo con $Eq(a)$ l'insieme delle relazioni di equivalenza in a .

Osservazione 3.5.2

Per ogni insieme a sono relazioni di equivalenza la relazione di uguaglianza in a e la relazione totale in a . La relazione di uguaglianza in a ha per grafico l'insieme Δ_a mentre la relazione totale ha per grafico $a \times a$.

Esempio 3.5.1

1. Sia ρ la relazione binaria in \mathbb{Z} definita da: $\forall x, y \in \mathbb{Z}(x \rho y \Leftrightarrow x + y \text{ è pari})$.

Verifichiamo che ρ è di equivalenza. Per ogni $x \in \mathbb{Z}$ il numero $x + x = 2x$ è pari, quindi $x \rho x$ e vale la proprietà riflessiva.

Per ogni $x, y \in \mathbb{Z}$ si ha: $x \rho y \Leftrightarrow x + y \text{ è pari} \Leftrightarrow y + x \text{ è pari} \Leftrightarrow y \rho x$ e vale la proprietà simmetrica. Infine, verifichiamo la proprietà transitiva. Siano $x, y, z \in \mathbb{Z}$ ed assumiamo $x \rho y$ e $y \rho z$. Allora $x + y$ e $y + z$ sono pari, quindi è pari la loro somma $x + y + y + z$ e quindi anche $x + z = (x + y) + (y + z) - 2y$, dunque $x \rho z$. Pertanto $\rho \in Eq(\mathbb{Z})$.

2. Sia σ la relazione binaria definita in $\mathcal{P}(\mathbb{Z})$ ponendo, per ogni $x, y \in \mathcal{P}(\mathbb{Z})$, $x \sigma y \Leftrightarrow x \cap \mathbb{N} = y \cap \mathbb{N}$. Per ogni $x \in \mathcal{P}(\mathbb{Z})$ si ha $x \cap \mathbb{N} = x \cap \mathbb{N}$, ovvero $x \sigma x$, quindi σ è riflessiva. Per ogni $x, y \in \mathcal{P}(\mathbb{Z})$, se $x \sigma y$ allora $y \sigma x$ e σ risulta simmetrica. Per ogni $x, y, z \in \mathcal{P}(\mathbb{Z})$, se $x \sigma y$ e $y \sigma z$, cioè $x \cap \mathbb{N} = y \cap \mathbb{N} = z \cap \mathbb{N}$ allora sicuramente $x \sigma z$ e σ risulta transitiva. Quindi $\sigma \in Eq(\mathcal{P}(\mathbb{Z}))$.

Definizione 3.5.3: Classe di equivalenza

La **classe di equivalenza** di x rispetto a \sim è l'insieme:

$$[x]_{\sim} := \{y \in a \mid y \sim x\} \quad (3.33)$$

che è ovviamente una parte di a . Osserviamo subito che, per ogni $x \in a$, $x \in [x]_{\sim}$, per la proprietà riflessiva di \sim , e $[x]_{\sim} = \{y \in a \mid x \sim y\}$, dal momento che, per la proprietà simmetrica, scelti comunque x e y in a si ha $x \sim y \Leftrightarrow y \sim x$.

Definizione 3.5.4: Rappresentante

Sia s un insieme non vuoto, e siano \mathfrak{R} una relazione di equivalenza in s e x un elemento di s . Se y è un elemento di $[x]_{\mathfrak{R}}$ allora $[y]_{\mathfrak{R}} = [x]_{\mathfrak{R}}$. Per questo motivo ogni elemento di $[x]_{\mathfrak{R}}$ si dice un **rappresentante** di $[x]_{\mathfrak{R}}$.

Lemma 3.5.1

Siano A un insieme, $\sim \in Eq(A)$ e $x, y \in A$. Allora sono equivalenti:

1. $x \sim y$
2. $x \in [y]_{\sim}$
3. $[x]_{\sim} = [y]_{\sim}$

Dimostrazione. Per definizione di classe di equivalenza, certamente (1.) \Leftrightarrow (2.). Supponiamo ora che valga (1.). Per ogni $z \in [x]_{\sim}$ si ha, sempre per la stessa definizione, $z \sim x$, quindi, per la proprietà transitiva, $z \sim y$, cioè $z \in [y]_{\sim}$. Dunque, se vale (1.), allora $[x]_{\sim} \subseteq [y]_{\sim}$. Ma, se vale (1.) si ha anche $y \sim x$, per la proprietà simmetrica, quindi, scambiando i ruoli di x e y , abbiamo anche $[y]_{\sim} \subseteq [x]_{\sim}$. Abbiamo così provato che (1.) \Rightarrow (3.). Infine, se assumiamo (3.), poiché, come sappiamo, $x \in [x]_{\sim}$ per la proprietà riflessiva, concludiamo che $x \in [y]_{\sim}$. Dunque (3.) \Rightarrow (2.). A questo punto la dimostrazione è completa. \square

Definizione 3.5.5: Insieme quoziante

Data una relazione di equivalenza \sim in un insieme a , l'insieme delle classi di equivalenza:

$$a/\sim = \{[x]_\sim \mid x \in a\} \quad (3.34)$$

di tutte le classi di equivalenza rispetto a \sim degli elementi di a prende il nome di **insieme quoziante**.

Proposizione 3.5.1

Siano A un insieme e $\sim \in Eq(A)$. Allora A/\sim è una partizione di A . Inoltre, per ogni $x \in A$, l'unica classe di equivalenza rispetto a \sim a cui x appartenga è $[x]_\sim$.

Dimostrazione. Per ogni $x \in A$, sappiamo che vale $x \in [x]_\sim$. Se $y \in A$ è tale che $x \in [y]_\sim$, allora, per il Lemma 3.5.1, $[y]_\sim = [x]_\sim$. Possiamo concludere che $[x]_\sim$ è l'unica classe di equivalenza rispetto a \sim a cui x appartenga. Abbiamo anche provato che A/\sim è un insieme di parti non vuote di A con la proprietà che ogni elemento di A appartenga ad uno ed un solo elemento di A/\sim , quindi $A \in Partz(A)$, come richiesto dalla prima parte dell'enunciato. \square

Lemma 3.5.2

Siano A un insieme, $\sim \in Eq(a)$ e $x, y \in A$, due elementi distinti. Sono allora equivalenti:

- (i) $x \sim y$
- (ii) $y \sim x$
- (iii) $x \in [y]_\sim$
- (iv) $y \in [x]_\sim$
- (v) $[x]_\sim \cap [y]_\sim \neq \emptyset$
- (vi) $[x]_\sim = [y]_\sim$

Dimostrazione. Abbiamo: Per la proprietà simmetrica delle relazioni di equivalenza sicuramente (i.) \iff (ii.). Inoltre, per il Lemma 3.5.1 si ha (i.) \iff (ii.) \iff (iii.) \iff (iv.) \iff (v.).

Se queste valgono, allora ovviamente, $[x]_\sim \cap [y]_\sim = [x]_\sim \neq \emptyset$, e quindi vale (vi.). Infine, $[x]_\sim$ e $[y]_\sim$ sono due elementi di A/\sim , che è una partizione per la Proposizione 3.5.1, quindi come segue dalla definizione di partizione, se $[x]_\sim \neq [y]_\sim$, allora $[x]_\sim \cap [y]_\sim = \emptyset$. Questo vuol dire che (vi.) \implies (v.); a questo punto la dimostrazione è completata. \square

Teorema 3.5.1 (Teorema fondamentale sulle partizioni)

Per ogni insieme A , l'applicazione:

$$\sim \in Eq(A) \mapsto A/\sim \in Partz(A)$$

è biettiva e prende il nome di **biezione canonica**.

Dimostrazione. Chiamiamo α l'applicazione $\sim \in Eq(A) \mapsto A/\sim \in Partz(A)$ considerata nell'enunciato. Innanzitutto, osserviamo che α è ben definita. Per verificare che α sia iniettiva, supponiamo che ρ e σ siano relazioni di equivalenza in A tali che $\alpha(\rho) = \alpha(\sigma)$, cioè $A/\rho = A/\sigma$, e proviamo che di conseguenza $\rho = \sigma$. Per ogni $x \in A$, si ha ovviamente $[x]_\rho \in A/\rho$, ma anche $A/\rho = A/\sigma$, quindi $[x]_\rho \in A/\sigma$, vale a dire: $[x]_\rho$ è una classe di equivalenza rispetto a σ . L'unico elemento di A/σ a cui x appartenga è $[x]_\sigma$, pertanto $[x]_\sigma = [x]_\rho$. Questo vale per ogni $x \in A$. Ora, per ogni $x, y \in A$, abbiamo:

$$\begin{aligned} x \rho y &\iff [x]_\rho = [y]_\rho \\ &\iff [x]_\sigma = [y]_\sigma \\ &\iff x \sigma y \end{aligned}$$

La conclusione è che σ e ρ coincidono. Abbiamo così provato che α è iniettiva.

Proviamo ora che α è suriettiva. Sia $\mathfrak{F} \in Partz(A)$. Definiamo un'applicazione $\pi : A \rightarrow \mathfrak{F}$ in questo modo: ad ogni $x \in A$ facciamo corrispondere quell'unico elemento di \mathfrak{F} a cui x appartiene. Sia ora \sim il nucleo di equivalenza di π , proveremo che A/\sim è proprio \mathfrak{F} . Per ogni $x \in A$ la classe $[x]_\sim$ è l'insieme degli $y \in A$ tali che $\pi(y) = \pi(x)$, e quest'ultima condizione equivale a $y \in \pi(x)$. Dunque, per ogni $x \in A$:

$$[x]_\sim = \{y \in A \mid y \in \pi(x)\} = \pi(x)$$

vale a dire: la classe di ciascun elemento di A rispetto a \sim è il blocco di \mathfrak{F} a cui quell'elemento appartiene. Quindi ogni classe appartenente a A/\sim è un elemento di \mathfrak{F} , dunque $A/\sim \subseteq \mathfrak{F}$. Viceversa, come è chiaro, per ogni $b \in \mathfrak{F}$, scelto un qualsiasi $x \in b$, abbiamo $b = \pi(x)$ per definizione di π , quindi $b = [x]_\sim \in A/\sim$ per quanto appena visto. Dunque, $\mathfrak{F} \subseteq A/\sim$, e così $\mathfrak{F} = A/\sim$. Abbiamo provato pertanto che α è suriettiva, dunque biettiva. \square

Il teorema 3.5.1 è di grande importanza: esso stabilisce che il problema di descrivere le relazioni di equivalenza in un dato insieme è essenzialmente lo stesso che quello (generalmente più facile da affrontare direttamente) dello studio delle partizioni dello stesso insieme. Per descrivere le prime basta descrivere le seconde ed usare la biezione che abbiamo chiamato α^{-1} per “tradurre” le partizioni in relazioni di equivalenza.

Esempio 3.5.2

1. Descriviamo le relazioni di equivalenza in un insieme A di tre elementi: $A = \{1, 2, 3\}$. Per farlo ci basta elencare le partizioni di A e quindi applicare il Teorema 3.5.1. Le partizioni sono in tutto cinque, le due partizioni banali e poi le tre partizioni $F_1 = \{\{1\}, \{2, 3\}\}$, $F_2 = \{\{2\}, \{1, 3\}\}$, $F_3 = \{\{3\}, \{1, 2\}\}$. Allora le relazioni di equivalenza in A saranno anch'esse cinque: le due banali (quella di uguaglianza e quella universale) e le tre relazioni di equivalenza σ_1 , σ_2 e σ_3 che corrispondono, nell'ordine, a F_1 , F_2 ed F_3 . Le rappresentiamo in tabella:

σ_1	1	2	3
1	•		
2		•	•
3		•	•

σ_2	1	2	3
1	•		•
2		•	
3	•		•

σ_3	1	2	3
1	•	•	
2	•	•	
3			•

2. Sia $a = \{n \in \mathbb{N} \mid n < 10\}$ e consideriamo la partizione $\mathcal{F} = \{\{0, 2, 4\}, \{1\}, \{3, 9\}, \{5, 6, 7, 8\}\}$. Qual è la relazione di equivalenza \sim di a che corrisponde ad \mathcal{F} ? In accordo con quanto appena stabilito, è quella descritta dalla proprietà che due arbitrari elementi di a siano in relazione se e solo se appartengono allo stesso blocco di \mathcal{F} . Il grafico può essere rappresentato mediante una tabella in cui ogni cella rappresenta un elemento di $a \times a$ ed ogni cella marcata rappresenta un elemento del grafico:

	0	1	2	3	4	5	6	7	8	9
0	•		•		•					
1		•								
2	•		•		•					
3				•						•
4	•		•		•					
5						•	•	•	•	•
6						•	•	•	•	•
7						•	•	•	•	•
8						•	•	•	•	•
9				•						•

Osservazione 3.5.3

Per ogni insieme a , ci sono tante relazioni di equivalenza quante sono le partizioni di a . In particolare risulta, per ogni insieme S , $S/\iota_S = \{\{x\} \mid x \in S\}$ e $S/\tau_S = \{S\}$. Questi due insieme prendono il nome di **partizioni banali**. Quindi, se $|a| = 2$, a ha esattamente due partizioni, che coincidono con quelle banali.

Definizione 3.5.6: Proiezione canonica

Sia \sim una relazione di equivalenza in un insieme a . Si chiama **proiezione canonica** l'applicazione:

$$\pi : x \in a \mapsto [x]_{\sim} \in a/\sim \quad (3.35)$$

È evidente dalla definizione di insieme quoziante che π è suriettiva.

Esempio 3.5.3

Consideriamo l'insieme finito di numeri interi $x = \{-5, -2, -1, 3, 4\}$ e la relazione \sim definita come:

$$a \sim b \iff "a \text{ ha lo stesso segno di } b"$$

\sim è una relazione di equivalenza in quanto riflessiva, simmetrica e transitiva. Risulta quindi:

$$[-5]_\sim = \{-5, -2, -1\}, \quad [3]_\sim = \{3, 4\}$$

L'insieme quoziante così ottenuto è: $x/\sim = \{[-5]_\sim, [3]_\sim\}$. In particolare x/\sim è una partizione di x , infatti ogni classe di equivalenza è non vuota e disgiunta da qualsiasi altra classe (numeri di segno distinto non possono essere in relazione tra di loro), inoltre vale $\bigcup x/\sim = x$. Quindi $x/\sim \in \text{Partz}(x)$.

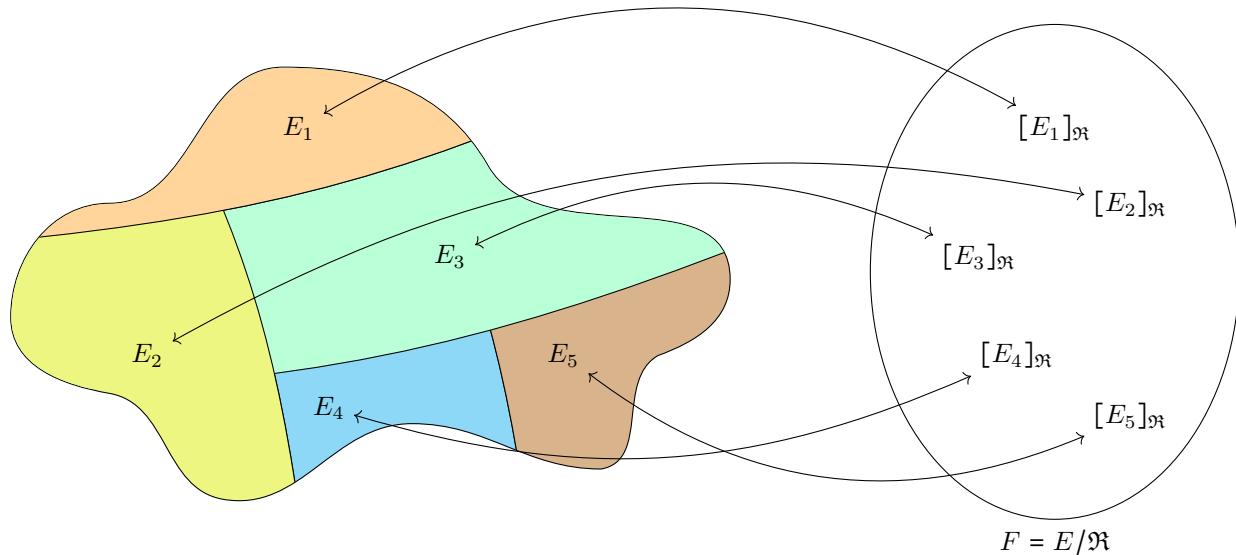


Figura 3.6: Esempio di partizione e rispettivo insieme quoziante

Definizione 3.5.7: Nucleo di equivalenza

Sia $f : a \rightarrow b$ una qualsiasi applicazione di dominio l'insieme a . Si chiama **nucleo di equivalenza** di f la relazione binaria \mathfrak{R}_f definita ponendo, per ogni $x, y \in a$:

$$x \mathfrak{R}_f y \iff f(x) = f(y) \quad (3.36)$$

L'insieme quoziante a/\mathfrak{R}_f prende il nome di **coimmagine** di f e si indica abitualmente come $\text{coim } f$:

$$\text{coim } f = a/\mathfrak{R}_f = \{\overleftarrow{f}(\{b\}) \mid b \in \text{im } f\} \quad (3.37)$$

Esempio 3.5.4

Supponiamo che A sia l'insieme dei numeri naturali minori di 10 e B sia un insieme di colori, poniamo $B = \{\text{rosso, verde, blu, marrone, giallo}\}$. Sia f un'applicazione da A a B ; dunque f associa a ciascuno dei numeri in A uno dei colori in B . Supponiamo che f sia definita in questo modo: a 1, 5 e 7 è associato il colore rosso, a 0, 3, 6 e 8 il verde, a 2 e 9 il blu e a 4 il marrone. Allora, rispetto a \mathfrak{R}_f , due elementi di A sono equivalenti se e solo se hanno lo stesso colore, e $\text{coim } f$ è costituita da quattro classi di equivalenza: quella degli elementi di colore rosso, che è l'antimmagine di $\{\text{rosso}\}$ mediante f , quella degli elementi verdi, quella degli elementi blu e quella degli elementi marroni.

Proposizione 3.5.2

Siano $f : A \rightarrow B$ un'applicazione e \mathfrak{R}_f il suo nucleo di equivalenza. Allora $\mathfrak{R}_f \in \text{Eq}(A)$.

Dimostrazione. Per ogni $x \in A$ si ha ovviamente $f(x) = f(x)$, ovvero $x \mathfrak{R}_f x$, quindi \mathfrak{R}_f è riflessiva.

Per ogni $x, y \in A$ abbiamo:

$$x \mathfrak{R}_f y \iff f(x) = f(y) \iff f(y) = f(x) \iff y \mathfrak{R}_f x$$

Quindi \mathfrak{R}_f è simmetrica.

Per ogni $x, y, z \in A$, se $x \mathfrak{R}_f y$ e $y \mathfrak{R}_f z$, cioè $f(x) = f(y)$ e $f(y) = f(z)$ allora $f(x) = f(z)$, cioè $x \mathfrak{R}_f z$; quindi \mathfrak{R}_f è transitiva. Quindi $\mathfrak{R}_f \in Eq(A)$. \square

Osservazione 3.5.4



Sia $f : a \rightarrow b$ una applicazione tra i due insiemi a e b . Valgono le seguenti caratterizzazioni interessanti:

- f è iniettiva $\iff \mathfrak{R}_f$ è la relazione identica in a ;
- f è costante $\iff \mathfrak{R}_f$ è la relazione totale in a .

Proposizione 3.5.3

Sia \sim una relazione di equivalenza. Allora \sim è il nucleo di equivalenza della proiezione canonica che definisce.

Dimostrazione. Sia $\sim \in Eq(A)$ e sia $\pi_\sim : A \rightarrow A/\sim$ la proiezione canonica. Sia ρ il nucleo di equivalenza di π_\sim . Allora, per ogni $x, y \in A$, abbiamo:

$$x \rho y \iff \pi(x) = \pi(y) \iff [x]_\sim = [y]_\sim \iff x \sim y$$

Dunque $\rho = \sim$ e l'enunciato è provato. \square

La costruzione del nucleo di equivalenza fornisce immediatamente un gran numero di esempi di relazioni di equivalenza: per ottenere una relazione di equivalenza in un insieme A basta considerare una qualsiasi applicazione che abbia A come dominio ed il nucleo di equivalenza di questa. Non solo: questa costruzione permette di verificare in modo diretto che alcune relazioni binarie sono di equivalenza. Quella dei nuclei di equivalenza non è semplicemente una costruzione che fornisce esempi di relazioni di equivalenza, ma è l'esempio più generale possibile. Infatti vale il seguente corollario:

Corollario 3.5.1

Ogni relazione di equivalenza è il nucleo di equivalenza di qualche applicazione^a.

^aNon vale il contrario perché applicazioni diverse possono avere lo stesso nucleo di equivalenza.

In maggior dettaglio, se A è un insieme e \sim è una relazione di equivalenza in A , esiste almeno un'applicazione f di dominio A tale che \sim sia il nucleo di equivalenza di f . Studiamo ora in maggior dettaglio i nuclei di equivalenza ed i corrispondenti quoienti.

Lemma 3.5.3

Siano $f : A \rightarrow B$ un'applicazione e \mathfrak{R}_f il suo nucleo di equivalenza. Allora, per ogni $x \in A$, si ha:

$$[x]_{\mathfrak{R}_f} = \overleftarrow{f}(\{f(x)\}) \quad (3.38)$$

Dimostrazione. Sia $x \in A$. Allora:

$$\begin{aligned} [x]_{\mathfrak{R}_f} &= \{y \in A \mid y \in [x]_{\mathfrak{R}_f}\} \\ &= \{y \in A \mid y \sim x\} \\ &= \{y \in A \mid f(y) = f(x)\} \end{aligned}$$

Ora, per ogni $y \in A$, la condizione $f(y) = f(x)$ è equivalente A:

$$\forall y \in A \left(f(y) \in \{f(x)\} \right)$$

cioè alla condizione che y appartenga all'antimmagine $\overleftarrow{f}(\{f(x)\})$ di $\{f(x)\}$ mediante f . Pertanto:

$$\begin{aligned} [x]_{\mathfrak{R}_f} &= \{y \in A \mid y \in \overleftarrow{f}(\{f(x)\})\} \\ &= \overleftarrow{f}(\{f(x)\}) \end{aligned}$$

\square

Teorema 3.5.2 (Teorema fondamentale di omomorfismo per insiemi)

Sia $f : A \rightarrow B$ un'applicazione e \mathfrak{R}_f il suo nucleo di equivalenza. Allora l'applicazione:

$$\alpha : b \in \text{im } f \mapsto \overleftarrow{f}(\{b\}) \in A/\mathfrak{R}_f$$

è biettiva ed ha per inversa l'applicazione:

$$\alpha^{-1} : [x]_{\mathfrak{R}_f} \in A/\mathfrak{R}_f \mapsto f(x) \in \text{im } f$$

Dimostrazione. Per il Lemma 3.5.3 la classe di equivalenza di x secondo il nucleo di equivalenza risulta l'insieme degli elementi di A che hanno la stessa immagine di x mediante f . È possibile quindi considerare l'applicazione $\alpha : \text{im } f \rightarrow A/\mathfrak{R}_f$, tale applicazione risulta:

- **Ben posta:** essendo $\text{im } f = \{f(x) \mid x \in A\}$ allora, per ogni $y \in \text{im } f$ esiste un elemento $x \in A$ tale che $y = f(x)$ e per l'osservazione precedente si ha: $\overleftarrow{f}(\{f(x)\}) = \overleftarrow{f}(\{y\}) = [x]_{\mathfrak{R}_f}$;
- **Suriettiva:** per ogni $c \in A/\mathfrak{R}_f$ esiste un elemento $x \in A$ per il quale $c = [x]_{\mathfrak{R}_f}$. Essendo $[x]_{\mathfrak{R}_f} = \overleftarrow{f}(\{f(x)\})$ e $f(x) \in \text{im } f$ allora $c = \alpha(f(x))$ sicché α risulta suriettiva.
- **Iniettiva:** siano $u, v \in \text{im } f$ tali che $\alpha(u) = \alpha(v)$. Dal momento che $u \in \text{im } f$ esiste un elemento $x \in A$ per il quale $u = f(x)$, ovvero $x \in \overleftarrow{f}(\{u\})$. Dato che $\alpha(u) = \alpha(v)$ deve essere anche $x \in \overleftarrow{f}(\{v\}) = \alpha(v)$, ovvero $v = f(x)$. Pertanto $u = f(x) = v$ e quindi α risulta iniettiva.

Quindi α risulta essere biettiva. Vogliamo infine descrivere α^{-1} . A questo scopo, sia $c \in A/\mathfrak{R}_f$. Naturalmente $c = [x]_{\mathfrak{R}_f}$ per un opportuno $x \in A$, e:

$$\begin{aligned} \alpha(f(x)) &= \overleftarrow{f}(\{f(x)\}) \\ &= [x]_{\mathfrak{R}_f} \end{aligned} \quad (\text{Per il Lemma 3.5.3})$$

Quindi:

$$\begin{aligned} f(x) &= \alpha^{-1}([x]_{\mathfrak{R}_f}) \\ &= \alpha^{-1}(c) \end{aligned}$$

In questo modo abbiamo verificato che l'inversa di α è, come richiesto dall'enunciato, l'applicazione:

$$\alpha^{-1} : [x]_{\mathfrak{R}_f} \in A/\mathfrak{R}_f \mapsto f(x) \in \text{im } f$$

□

È opportuno osservare che, qualunque sia l'applicazione $f : A \rightarrow B$, la relazione di equivalenza \mathfrak{R}_f in A è l'unica per la quale esiste l'applicazione inversa di α . La situazione descritta nel teorema appena dimostrato può essere descritta da questo diagramma:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow \pi & & \uparrow \iota \\ A/\mathfrak{R}_f & \xrightarrow{\alpha^{-1}} & \text{im } f \end{array}$$

Risulta $f = (\iota \circ \alpha^{-1} \circ \pi)$, infatti:

$$\begin{aligned} \forall x \in A((\iota \circ \alpha^{-1} \circ \pi)(x) &= \iota(\alpha^{-1}(\pi(x)))) \\ &= \iota(\alpha^{-1}([x]_{\mathfrak{R}_f})) \\ &= \iota(f(x)) \\ &= f(x) \end{aligned}$$

Siccome la proiezione canonica è suriettiva, α^{-1} è biettiva mentre l'immersione ι risulta iniettiva possiamo concludere osservando che ogni applicazione è ottenibile come composizione tra un'applicazione iniettiva e una suriettiva. Questa fattorizzazione è nota come **fattorizzazione canonica**.

Esempio 3.5.5

1. Siano $A = \{n \in \mathbb{Z} \mid -3 \leq n \leq 5\}$ e $f : n \in A \mapsto n^2 \in \mathbb{N}$. Sia poi τ il nucleo di equivalenza di f . Per descrivere il quoziente A/τ possiamo partire dalla descrizione di $im(f)$. Dovrebbe essere chiaro che $im f = \{n^2 \mid n \in A\} = \{0, 1, 4, 9, 16, 25\}$. Allora $im f$ ha sei elementi, quindi, per il teorema 3.5.2 abbiamo $|A/\tau| = 6$; in altri termini, in A ci sono esattamente sei classi di equivalenza rispetto a τ , che corrispondono ai sei elementi di $im f$. Le classi, cioè gli elementi di $A\tau$ sono dunque, sempre per lo stesso teorema: $\overleftarrow{f}(0) = \{0\}$, $\overleftarrow{f}(\{1\}) = \{\pm 1\}$, $\overleftarrow{f}(\{4\}) = \{\pm 2\}$, $\overleftarrow{f}(\{9\}) = \{\pm 3\}$, $\overleftarrow{f}(\{16\}) = \{4\}$ e $\overleftarrow{f}(\{25\}) = \{5\}$.
2. Utilizziamo lo stesso insieme A dell'esempio precedente, e studiamo il nucleo di equivalenza σ dell'applicazione $g : x \in \mathcal{P}(A) \mapsto x \cap \mathbb{N} \in \mathcal{P}(\mathbb{N})$. Iniziamo con l'identificare $im g$. Posto $B = A \cap \mathbb{N}$, per ogni $x \in \mathcal{P}(B)$ si ha evidentemente $g(x) = x \cap \mathbb{N} \subseteq B$. Viceversa, per ogni $y \in \mathcal{P}(B)$ abbiamo $y = y \cap \mathbb{N} = g(y)$, quindi $y \in im g$. Pertanto $im g = \mathcal{P}(B)$ e quindi, come mostra il Teorema 3.5.2, $|\mathcal{P}(B)/\sigma| = |im g| = |\mathcal{P}(B)| = 2^{|B|} = 32$. Come sono fatte le singole classi di equivalenza rispetto a σ ? Sempre per lo stesso teorema esse corrispondono agli elementi di $im g = \mathcal{P}(B)$, sono cioè gli insiemi $\overline{g}(\{y\})$ al variare di $y \in \mathcal{P}(B)$. Ad esempio, l'elemento $\emptyset \in \mathcal{P}(B)$ corrisponde alla classe $\overline{g}(\{\emptyset\}) = \{x \in \mathcal{P}(A) \mid g(x) = \emptyset\} = \{x \in \mathcal{P}(A) \mid x \cap \mathbb{N} = \emptyset\}$. Non è difficile vedere che questo insieme è $\mathcal{P}(A \setminus B) = \mathcal{P}(\{-3, -2, -1\})$.



3.6.1 Corrispondenze e applicazioni

Esercizio 3.6.1

Dati gli insiemi $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ dire quali dei seguenti diagrammi definiscono una funzione:

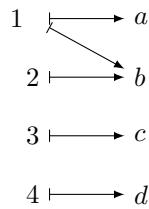


Figura 3.7: Diagramma 1

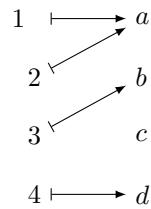


Figura 3.8: Diagramma 2

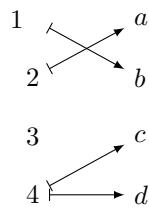


Figura 3.9: Diagramma 3

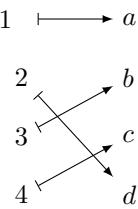


Figura 3.10: Diagramma 4

Svolgimento.

- I diagrammi 1 e 3 non descrivono una applicazione in quanto sono presenti elementi con più di una immagine (nel diagramma 1 l'elemento 1) oppure elementi del dominio cui non hanno immagine (l'elemento 3 nel diagramma 3).
- I diagrammi 2 e 4 descrivono correttamente una applicazione.

Esercizio 3.6.2

Indicato con \mathbb{R}_0^+ l'insieme dei numeri reali non negativi (cioè: $\mathbb{R}_0^+ = \{a \in \mathbb{R} | a \geq 0\}$), si stabilisca quali delle seguenti corrispondenze sono applicazioni:

- $\alpha : \mathbb{R} \rightarrow \mathbb{R}$, di grafico $\{(a, b) \in \mathbb{R} \times \mathbb{R} | a = b^2\}$
- $\beta : \mathbb{R}_0^+ \rightarrow \mathbb{R}$, di grafico $\{(a, b) \in \mathbb{R} \times \mathbb{R} | a = b^2\}$
- $\gamma : \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+$, di grafico $\{(a, b) \in \mathbb{R} \times \mathbb{R}_0^+ | a = b^2\}$

Svolgimento.

Si ha:

- La corrispondenza α non è una applicazione. Infatti all'interno del dominio \mathbb{R} non tutti gli elementi godono di immagine mediante α , ad esempio nessun numero reale negativo può essere espresso come il quadrato di un numero reale.
- La corrispondenza β non è una applicazione in quanto ogni elemento del dominio gode di immagine ma questa non è unica. Infatti, preso l'elemento $4 \in \mathbb{R}_0^+$ vale:

$$4 = (-2)^2 = 2^2$$

Quindi le coppie $(2, -2)$ e $(2, 2)$ appartengono al grafico G . Per la definizione di applicazione (Definizione 3.7) però ogni elemento del dominio deve avere una ed un'unica immagine.

- La corrispondenza γ è una applicazione in quanto ogni elemento del dominio ha un'immagine e questa è unica.

Esercizio 3.6.3

Sappiamo che esiste un'applicazione suriettiva e costante da \mathbb{N} ad un certo insieme A . Cosa possiamo dire su A ?

Svolgimento. Se esiste una funzione suriettiva e costante da \mathbb{N} ad un certo insieme A possiamo dire che A contiene un solo elemento. Infatti per essere suriettiva φ deve essere:

$$im(\varphi) = A$$

Essendo inoltre φ costante si ha che tutti gli elementi di \mathbb{N} hanno un'unica immagine $\varphi(n) = \bar{y} \in A$ che risulta l'unico elemento di A .

Esercizio 3.6.4

Quali tra queste sono applicazioni ben definite? Qui P è l'insieme delle parti non vuote di \mathbb{Z} .

1. $n \in \mathbb{N} \mapsto \frac{3n}{2} \in \mathbb{Z}$
2. $n \in \mathbb{Z} \mapsto n^2/2 \in \mathbb{Z}$
3. $X \in P \mapsto \min X \in \mathbb{Z}$
4. $X \in P \mapsto \mathbb{Z} \setminus X \in P$
5. $X \in \mathcal{P}(\mathbb{Z}) \mapsto X \cap \mathbb{N} \in \mathcal{P}(\mathbb{N})$
6. $X \in \mathcal{P}(\mathbb{Z}) \mapsto X \Delta \mathbb{N} \in \mathcal{P}(\mathbb{N})$

Svolgimento. Si ha:

1. Non è una applicazione ben definita in quanto l'elemento $1 \in \mathbb{Z}$ non ha un suo corrispondente:

$$1 \in \mathbb{Z} \mapsto 3/2 \notin \mathbb{Z}$$

2. Non è una applicazione ben definita in quanto l'elemento $1 \in \mathbb{Z}$ non ha un suo corrispondente:

$$1 \in \mathbb{Z} \mapsto 1/2 \notin \mathbb{Z}$$

3. Non è una applicazione ben definita in quanto solo le parti finite non vuote di \mathbb{Z} ammettono minimo.

4. Non è una applicazione ben definita in quanto il corrispondente di \mathbb{Z} non è in P :

$$\mathbb{Z} \in \mathbb{Z} \mapsto \mathbb{Z} \setminus \mathbb{Z} = \emptyset \notin P$$

5. È una applicazione ben definita.

6. Non è una applicazione in quanto le parti di $\mathbb{Z} \setminus \mathbb{N}$ non hanno un corrispondente nel codominio. Sia ad esempio: $Y = \{-2, -3, -4\} \in P$ si ha allora:

$$Y \Delta \mathbb{N} = (Y \cup \mathbb{N}) \setminus (Y \cap \mathbb{N}) = (Y \cup \mathbb{N}) \setminus \emptyset = (Y \cup \mathbb{N}) \notin \mathcal{P}(\mathbb{N})$$

■

Esercizio 3.6.5

Siano \mathbb{N} l'insieme dei numeri naturali e $S = \{1, 2, 3\}$. Siano poi α la relazione binaria in S definita da:

$$(\forall x, y \in S)(x \alpha y \iff x < y)$$

e β la corrispondenza da S ad \mathbb{N} di grafico:

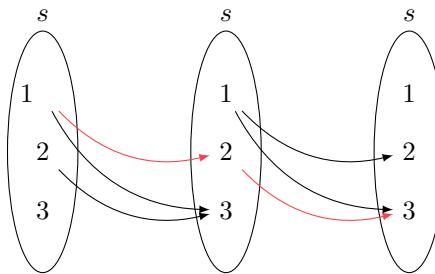
$$G = \{2\} \times \{x \in \mathbb{N} \mid x < 10\}$$

Descrivere la corrispondenza prodotto $\alpha\beta$ e la relazione binaria $\alpha^2 = \alpha\alpha$.

Svolgimento. Si ha che il grafico di $\alpha\beta$ è dato dall'insieme:

$$\{(1, 0), (1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (1, 7), (1, 8), (1, 9)\}$$

Infatti, un elemento $x \in S$ è in relazione $\alpha\beta$ con un elemento $n \in \mathbb{N}$ se e solo se esiste un elemento $b \in S$ tale che: $a \alpha b \wedge b \beta n$. L'unico elemento che soddisfa tale condizione è $2 \in S$ in quanto: $1 \alpha 2 \wedge 2 \beta n$ con n che varia da 1 a 9. Analogamente, la relazione $\alpha\alpha$ si ottiene come mostrato in figura:



L'unico collegamento che si ha tra i tre insiemi è dato dagli archi che passano attraverso il punto 2. Quindi si ha $1 \alpha\alpha 3$ e $(1, 3)$ è l'unica coppia presente nel grafico del prodotto $\alpha\alpha$.

■

Esercizio 3.6.6

Per un arbitrario insieme A , sia k l'applicazione: $x \in \mathcal{P}(A) \mapsto A \setminus x \in \mathcal{P}(A)$. Calcolare $k \circ k$.

Svolgimento. Si ha, per ogni $x \in \mathcal{P}(A)$:

$$\begin{aligned} k \circ k(x) &= k(A \setminus x) \\ &= A \setminus (A \setminus x) \\ &= x \end{aligned} \quad (\text{Per la 2.18})$$

Quindi: $k \circ k = id_{\mathcal{P}(A)}$. ■

Esercizio 3.6.7

Siano $A = \{1, 2\}$ e $B = \{1, 2, 3\}$. Scrivere due diversi prolungamenti a B dell'immersione di A in B (si richiedono, in altri termini, due applicazioni $B \rightarrow B$ che abbiano l'immersione di A in B come restrizione).

Svolgimento. Si considerino le applicazioni: $f : B \rightarrow B$ e $g : B \rightarrow B$ definite ponendo:

$$\begin{array}{ll} f(1) = 1 & g(1) = 1 \\ f(2) = 2 & g(2) = 2 \\ f(3) = 1 & g(3) = 3 \end{array}$$

Come mostrato in Figura 3.11 e 3.12:

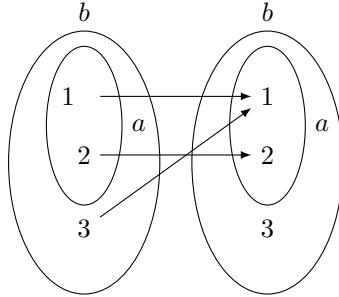


Figura 3.11: $f : B \rightarrow B$

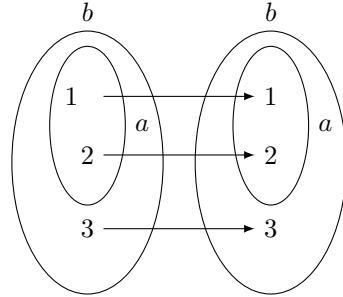


Figura 3.12: $g : B \rightarrow B$

Le applicazioni f e g sono diverse ma sono entrambe prolungamenti dell'immersione $A \hookrightarrow B$. ■

Esercizio 3.6.8

Sia $f : x \in \mathcal{P}(\mathbb{Z}) \mapsto x \cup \mathbb{N} \in \mathcal{P}(\mathbb{Z})$. Descrivere $\vec{f}(\mathcal{P}(\mathbb{N}))$.

Svolgimento. Per ogni parte $X \subseteq \mathbb{N}$ si ha $f(X) = X \cup \mathbb{N} = \mathbb{N}$ quindi $\vec{f}(\mathcal{P}(\mathbb{N})) = \mathbb{N}$. ■

Esercizio 3.6.9

Sia:

$$+ : (a, b) \in \mathbb{N} \times \mathbb{N} \mapsto a + b \in \mathbb{N}$$

la consueta operazione di addizione in \mathbb{N} . Calcolare l'anti-immagine di $\{1, 2\}$ mediante $+$.

Svolgimento. Si ha:

$$\overleftarrow{+}(\{1, 2\}) = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid + (a, b) \in \{1, 2\}\} = \{(0, 1), (1, 0), (0, 2), (2, 0), (1, 1)\}$$

Esercizio 3.6.10

Siano $f : n \in \mathbb{Z} \mapsto n^2 \in \mathbb{Z}$ e $X = \{n \in \mathbb{N} \mid n \leq 10\}$. Calcolare:

1. $\vec{f}(X)$;
2. $\vec{f}(\vec{f}(X))$;
3. $\vec{f}(\vec{f}(X))$.

Svolgimento. Si ha:

- $\vec{f}(X) = \{0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100\}$
- $\vec{f}(\vec{f}(X)) = \{0, -1, 1, -2, 2, -3, 3, -4, 4, -5, 5, -6, 6, -7, 7, -8, 8, -9, 9, -10, 10\}$
- $\vec{f}(\vec{f}(X)) = \{0, 1, 4, 9\}$

Esercizio 3.6.11

Dimostrare che se $f : A \rightarrow B$ è un'applicazione si ha $\vec{f}(\vec{f}(A)) = A$ e:

1. per ogni $Y \subseteq B$, $\vec{f}(\vec{f}(Y)) = Y \cap \text{im } f \subseteq Y$;
2. per ogni $X, Y \subseteq A$ si ha $X \subseteq Y \Rightarrow \vec{f}(X) \subseteq \vec{f}(Y)$;
3. per ogni $X, Y \subseteq B$ si ha $X \subseteq Y \Rightarrow \vec{f}(X) \subseteq \vec{f}(Y)$.

Svolgimento. Per definizione di applicazione immagine e antimmagine si ha:

$$\vec{f}(\vec{f}(A)) = \vec{f}(\text{im } f) = \{x \in A \mid f(x) \in \text{im } f\}$$

Per definizione di applicazione, ogni $x \in A$ gode di immagine mediante f quindi sicuramente vale:

$$\vec{f}(\vec{f}(A)) = A$$

1. Sia ora Y una parte del codominio B . Si ha allora che l'insieme:

$$\begin{aligned}\vec{f}(\vec{f}(Y)) &= \vec{f}(\{x \in A \mid f(x) \in Y\}) \\ &= \{y \in Y \mid \exists x \in A (y = f(x))\} \\ &= Y \cap \text{im } f\end{aligned}$$

E ovviamente vale $Y \cap \text{im } f \subseteq Y$.

2. Siano $X, Y \subseteq A$ tali che $X \subseteq Y$, cioè:

$$\forall x \in X \implies x \in Y \quad (3.39)$$

Per definizione di applicazione immagine abbiamo:

$$\begin{aligned}\vec{f}(X) &= \{f(x) \mid x \in X\} \\ \vec{f}(Y) &= \{f(x) \mid x \in Y\}\end{aligned}$$

Ma stando la 3.39, per ogni elemento $y \in \vec{f}(X) \implies y \in \vec{f}(Y)$ e quindi $\vec{f}(X) \subseteq \vec{f}(Y)$.

3. Analogamente con le antimmagini.

Esercizio 3.6.12

Tra queste applicazioni, decidere quali sono suriettive e descrivere, per esse, almeno una sezione e, se possibile, due:

1. la consueta operazione di addizione: $+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$
2. $\alpha : n \in \mathbb{N} \mapsto |n| + 1 \in \mathbb{N}^*$
3. $\beta : n \in \mathbb{N} \mapsto \begin{cases} 44 & \text{se } n = 0 \\ n - 1 & \text{se } n \neq 0 \end{cases} \in \mathbb{N}$
4. $\gamma : n \in \mathbb{N} \mapsto \begin{cases} n/2 & \text{se } n \text{ è pari} \\ n & \text{se } n \text{ è dispari} \end{cases} \in \mathbb{N}$
5. $\delta : x \in \mathcal{P}(\mathbb{Z}) \mapsto \mathbb{N} \setminus x \in \mathcal{P}(\mathbb{Z})$
6. $\epsilon : x \in A \mapsto 4 - x \in A$, qui $A = \{1, 2, 3\}$
7. $\zeta : \mathbb{N}^* \rightarrow \mathbb{N}^*$ che ad ogni numero intero positivo associa il numero delle sue cifre nella consueta rappresentazione del numero in base 10.
8. $\theta : n \in \mathbb{Z} \mapsto \begin{cases} n + 1 & \text{se } n \text{ pari} \\ n - 1 & \text{se } n \text{ dispari} \end{cases} \in \mathbb{Z}$

Svolgimento. Si ha:

1. L'addizione in $\mathbb{Z} \times \mathbb{Z}$ è suriettiva, infatti ogni numero intero relativo può essere espresso come somma di due interi relativi. Una possibile sezione di questa applicazione è l'applicazione:

$$h : n \in \mathbb{Z} \mapsto (n - 1, 1) \in \mathbb{Z} \times \mathbb{Z}$$

e infatti si ha:

$$\forall n \in \mathbb{Z} (+(h(n)) = +(n - 1, 1) = n - 1 + 1 = n = id_{\mathbb{Z}}(n))$$

2. L'applicazione α è suriettiva. Infatti, per ogni $n \in \mathbb{N}^*$ esiste sempre un numero intero relativo $x \in \mathbb{Z}$ per il quale è possibile esprimere n come la somma di $|x| + 1$. Una possibile sezione di tale applicazione è l'applicazione:

$$h : n \in \mathbb{N}^* \mapsto 1 - n \in \mathbb{Z}$$

Infatti:

$$\alpha(h(n)) = \alpha(1 - n) = |1 - n| + 1 = 1 - n + 1 = n = id_{\mathbb{N}^*}$$

Esercizio 3.6.13

Siano $f : A \rightarrow B$ e $g : B \rightarrow C$ applicazioni componibili. Verificare che:

$$im(g \circ f) \subseteq im \ g$$

e che vale:

$$im(g \circ f) = im \ g$$

se f è suriettiva.

Svolgimento. Se $c \in C$ appartiene all'insieme $im \ g \circ f$ allora:

$$c \in \{(g \circ f)(x) \mid x \in A\}$$

per la definizione di insieme immagine. Dato che $\forall z \in C (g \circ f)(x) = g(f(x))$ allora $c \in im \ g$ e quindi $im \ g \circ f \subseteq im \ g$. Se l'applicazione f fosse suriettiva si avrebbe invece che ogni elemento $g(x) \in C$ possa essere espresso come $g(f(x))$ per ogni elemento $x \in A$ e quindi appartenere ad $im \ g \circ f$ e data la doppia implicazione si ottiene l'uguaglianza. ■

Esercizio 3.6.14

Provare che se f è un'applicazione, allora f è suriettiva se e solo se \vec{f} è suriettiva.

Svolgimento Sia f suriettiva. Quindi: $im \ f = \vec{f}(A) = \{f(x) \mid x \in A\} = B$. In particolare, presa una qualsiasi parte $Y \subseteq B$ è possibile considerare l'insieme $\vec{f}(\{Y\}) \subseteq A$ che è non vuoto in quanto f è suriettiva. Vale allora:

$$\forall Y \subseteq B (\exists X \subseteq A (Y = \vec{f}(X)))$$

e questo dimostra che \vec{f} è suriettiva in quanto ogni parte di B può essere espressa come immagine secondo \vec{f} di una parte di A . Analogamente viceversa. ■

Esercizio 3.6.15

Siano date le seguenti funzioni:

1. $g : n \in \mathbb{N} \mapsto \sqrt{n} - 4 \in \mathbb{R}$
2. $h : x \in \mathbb{R} \mapsto x^3 + 5 \in \mathbb{R}$

Stabilire se sono funzioni. In caso affermativo, provare se sono iniettive, suriettive o biettive. Calcolare, dove possibile, le funzioni inverse g^{-1} e h^{-1} , e le composizioni $h \circ g$ e $g \circ h$.

Svolgimento. Si ha:

- La legge definita da h è una funzione, infatti ad ogni valore $x \in \mathbb{R}$ viene associata la sua potenza x^3 , che è ancora un numero reale, sommata al numero reale 5. Per stabilire se h è iniettiva deve valere:

$$\forall x_1, x_2 \in \mathbb{R} \quad h(x_1) = h(x_2) \implies x_1 = x_2$$

Siano $x_1, x_2 \in \mathbb{R}$ tali che $h(x_1) = h(x_2)$ e proviamo che $x_1 = x_2$. Si ha:

$$h(x_1) = h(x_2) \implies x_1^3 + 5 = x_2^3 + 5 \iff x_1^3 = x_2^3 \iff x_1 = x_2$$

Quindi h è iniettiva. Ora controlliamo se h è suriettiva, cioè:

$$\forall y \in \mathbb{R} (\exists x \in \mathbb{R} (h(x) = y))$$

Sia $y \in \mathbb{R}$ e si supponga che esista $x \in \mathbb{R}$ tale che $h(x) = y$, quindi si ha:

$$h(x) = y \iff x^3 + 5 = y \iff x^3 = y - 5 \iff x = \sqrt[3]{y - 5}$$

Osserviamo che la radice cubica del numero reale $y - 5$ è sicuramente un numero reale per ogni scelta di $y \in \mathbb{R}$, quindi h è suriettiva. Poiché h è sia iniettiva che suriettiva allora sarà invertibile ed è possibile considerare l'applicazione inversa:

$$h^{-1} : y \in \mathbb{R} \mapsto \sqrt[3]{y - 5} \in \mathbb{R}$$

la cui espressione è ottenuta sfruttando il calcolo fatto per provare la proprietà suriettiva.

- La legge definita da g è una funzione. Infatti, ad ogni numero naturale n viene associata la sua radice quadrata \sqrt{n} , che è ancora un numero reale a cui viene sottratto il numero 4. Detto ciò stabiliamo se g è iniettiva, cioè:

$$\forall n_1, n_2 \in \mathbb{N} \quad g(n_1) = g(n_2) \implies n_1 = n_2$$

Siano $n_1, n_2 \in \mathbb{N}$ tali che $g(n_1) = g(n_2)$ e proviamo che $n_1 = n_2$. Si ha:

$$g(n_1) = g(n_2) \iff \sqrt{n_1} - 4 = \sqrt{n_2} - 4 \iff \sqrt{n_1} = \sqrt{n_2} \iff n_1 = \pm n_2$$

Ma l'insieme di partenza è \mathbb{N} quindi $n_1 = \pm n_2 \iff n_1 = n_2$. Quindi g è iniettiva. Ora vogliamo controllare che g sia suriettiva, cioè:

$$\forall x \in \mathbb{R} \quad \exists n \in \mathbb{N} \quad \text{tale che} \quad g(n) = x$$

Sia $x \in \mathbb{R}$ e si supponga che esista $n \in \mathbb{N}$ tale che $g(n) = x$, quindi si ha:

$$g(n) = x \iff \sqrt{n} - 4 = x \iff \sqrt{n} = x + 4$$

Sicuramente se $x = -10$ si ottiene $\sqrt{n} = -6$, ma ciò è impossibile poiché la radice quadrata di un numero (positivo) è sempre una quantità positiva. Allora g non è suriettiva. Da ciò risulta che g non è biettiva e non ammette inversa.

Infine, ci chiediamo se sono possibili le composizioni $g \circ h$ e $h \circ g$. Ricordiamo che la composizione tra due funzioni $f \circ g$ è possibile se il dominio (insieme di partenza) della funzione f coincide con il codominio della funzione g . Nel nostro caso, notiamo che il dominio di g è \mathbb{N} e non coincide con il codominio di h che è \mathbb{R} . Pertanto non è possibile considerare $g \circ h$. D'altra parte, per quanto riguarda $h \circ g$ si ha che il dominio di h , cioè \mathbb{R} , coincide con il codominio di g , cioè \mathbb{R} . Quindi possiamo calcolare la composizione:

$$h \circ g : \mathbb{N} \longrightarrow \mathbb{R}$$

e si ha, per ogni $n \in \mathbb{N}$:

$$(h \circ g)(n) = h(\sqrt{n} - 4) = (\sqrt{n} - 4)^3 + 5$$

■

Esercizio 3.6.16

Si provi che l'applicazione:

$$\begin{aligned} f : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \times \mathbb{Z} \\ (x, y) &\mapsto (2x - y, 4x + 5y) \end{aligned}$$

è iniettiva ma non suriettiva.

Svolgimento. Siano (x, y) e (a, b) due elementi di $\mathbb{Z} \times \mathbb{Z}$ tali che:

$$f((x, y)) = f((a, b))$$

e mostriamo che $(x, y) = (a, b)$. Abbiamo che:

$$(2x - y, 4x + 5y) = (2a - b, 4a + 5b)$$

Ovvero:

$$\begin{cases} 2x - y = 2a - b \\ 4x + 5y = 4a + 5b \end{cases}$$

Sottraendo dalla seconda equazione due volte la prima si ottiene:

$$7y = 7b$$

da cui $y = b$ che risostituita nella prima equazione da $x = y$ e pertanto $(x, y) = (a, b)$. Mostriamo ora che f non è suriettiva. Osserviamo che, se lo fosse, avremmo che, preso un arbitrario elemento $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ esiste un $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ tale che $f((x, y)) = (u, v)$, ovvero:

$$\begin{cases} 2x - y = u \\ 4x + 5y = v \end{cases}$$

Ricavando la y dalla prima equazione e sostituendola nella seconda si ottiene:

$$\begin{cases} y = 2x - u \\ 14x = 5u + v \end{cases}$$

Ora l'equazione $14x = 5u + v$ è irrisolvibile in \mathbb{Z} se 14 non divide $5u + v$. Ne segue che se prendiamo (u, v) in $\mathbb{Z} \times \mathbb{Z}$ tale che $5u + v$ non è divisibile per 14 allora tale elemento non ammette antimmagine tramite f . Ad esempio $(0, 1)$ ha antimmagine vuota, quindi f non è suriettiva. ■

Esercizio 3.6.17

Trovare tutte le sezioni e tutte le retrazioni dell'applicazione

$$\{0\} \longrightarrow \{0, 1\}$$

Svolgimento. L'immersione da $\{0\} \hookrightarrow \{0, 1\}$ non è suriettiva e quindi non ammette sezioni per il [Teorema di caratterizzazione delle applicazioni suriettive](#). L'applicazione è però iniettiva e dato che $\{0\} \neq \emptyset$ allora esiste un'unica retrazione (in quanto il dominio è composto da un solo elemento) ovvero l'applicazione costante che associa ogni elemento di A a $0 \in \{0\}$. Infatti si ha:

$$\begin{aligned} \tau : x \in \{0, 1\} &\mapsto 0 \in \{0\} \\ \tau \circ \iota = \tau(\iota(0)) &= \tau(0) = 0 = id_{\{0\}}(0) \end{aligned}$$

Esercizio 3.6.18

Trovare, ove possibile, una sezione ed una retrazione di ciascuna delle applicazioni qui indicate, dove $A = \{0, 1, 2\}$, $B = \{1, 2\}$, $C = \{1, 2, 3, 4\}$:

1. $f : A \longrightarrow B$ definita da $0 \mapsto 1, 1 \mapsto 2, 2 \mapsto 1$;
2. $g : C \longrightarrow A$ definita da $1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 0, 4 \mapsto 0$;
3. $f \circ g$;
4. $h : x \in B \mapsto 2 + x \in C \setminus B$.

Svolgimento. Si ha:

1. L'applicazione f è suriettiva ma non iniettiva, quindi ammette sezioni ma non retrazioni. Ad esempio l'applicazione:

$$\sigma : \begin{cases} 1 \in B \mapsto 0 \\ 2 \in B \mapsto 1 \end{cases} \in A$$

è una sezione di f , infatti:

$$\begin{aligned} (f \circ \sigma)(1) &= f(0) = 1 \\ (f \circ \sigma)(2) &= f(1) = 2 \end{aligned}$$

2. L'applicazione g è suriettiva ma non iniettiva. Quindi ammette sezioni ma non retrazioni. Una possibile sezione di g è:

$$h : x \in A \mapsto \begin{cases} 4 & \text{se } x = 0 \\ 1 & \text{se } x = 1 \\ 2 & \text{se } x = 2 \end{cases} \in C$$

3. L'applicazione composta $f \circ g : C \rightarrow B$ è suriettiva in quanto lo sono f e g . Di conseguenza ammetterà sezioni ma non retrazioni. Quindi esiste un'applicazione $h : B \rightarrow C$ tale che $(f \circ g) \circ h = id_B$. Ad esempio $h : B \rightarrow C$ che mappa 1 in 3 e 2 in 1.
4. L'applicazione h è sia iniettiva che suriettiva quindi ammette un'unica sezione ed un'unica retrazione e queste coincidono. Ovvero esiste l'applicazione inversa: $h^{-1} : x \in C \setminus B \mapsto x - 2 \in B$. ■

Esercizio 3.6.19

Sia X un insieme non vuoto ed Y un fissato sottoinsieme di X . Si consideri $f : \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ definita ponendo:

$$A \in \mathcal{P}(X) \mapsto A \Delta Y \quad (3.40)$$

si provi che f è biettiva. Descrivere $f \circ f$.

Svolgimento. Proviamo che f è iniettiva. Siano $A_1 \neq A_2$ due parti distinte di X e, ragionando per assurdo, assumiamo che $f(A_1) = f(A_2)$. Nostro obiettivo è quello di trovare una contraddizione.

Senza perdere di generalità, possiamo supporre $A_1 \not\subseteq A_2$. Sia quindi $a \in A_1$ e $a \notin A_2$. Si possono presentare due casi: $a \notin Y$ e $a \in Y$.

- Nel primo caso, $a \in A_1 \setminus Y$, quindi $a \in A_1 \Delta Y$. Ma $A_1 \Delta Y = A_2 \Delta Y$, quindi abbiamo che $a \in A_2 \Delta Y = (A_2 \setminus Y) \cup (Y \setminus A_2)$ e, poiché $a \notin Y$, $a \in X_2 \setminus Y$ e dunque $a \in A_2$. Assurdo.
- Sia ora $a \in Y$. Poiché $a \in A_1$ segue che $a \notin A_1 \Delta Y = (A_1 \cup Y) \setminus (A_1 \cap Y)$. Allora $a \notin A_2 \Delta Y = (A_2 \cup Y) \setminus (A_2 \cap Y)$. Essendo $a \in Y$, necessariamente $a \in A_2$, altrimenti $a \in (A_2 \cup Y) \setminus (A_2 \cap Y)$. Quindi $a \in A_2$, assurdo.

Proviamo che f è suriettiva. Sia B un arbitrario elemento di $\mathcal{P}(X)$ e mostriamo che esiste un $C \in \mathcal{P}(X)$ tale che $f(C) = B$, ovvero $C \Delta Y = B$. Prendiamo $C = B \Delta Y$ e calcoliamo $f(C)$:

$$\begin{aligned} f(C) &= f(B \Delta Y) \\ &= (B \Delta Y) \Delta Y \\ &= B \Delta (Y \Delta Y) \\ &= B \Delta \emptyset \\ &= B \end{aligned}$$

Quindi f è biettiva. Dal fatto che per ogni $B \subseteq X$ si ha $f(B) = B \Delta Y$ e $f(B \Delta Y) = B$, segue che:

$$(f \circ f)(B) = f(f(B)) = f(B \Delta Y) = B$$

Quindi $f \circ f = id_{\mathcal{P}(X)}$, la funzione identità su $\mathcal{P}(X)$. ■

3.6.2 Relazioni di equivalenza e partizioni

Esercizio 3.6.20

Sia $f : A \rightarrow B$ un'applicazione e \mathfrak{R}_f il suo nucleo di equivalenza. Si dimostri che f è iniettiva se e solo se \mathfrak{R}_f coincide con la relazione identica id_A .

Svolgimento. Supponiamo che $f : A \rightarrow B$ sia un'applicazione iniettiva. Per dimostrare che le due equivalenze \mathfrak{R}_f e id_A coincidono si deve provare che per ogni $a, a' \in A$ si ha $a \mathfrak{R}_f a' \iff a id_A a'$. Se $a \mathfrak{R}_f a'$ allora $f(a) = f(a')$, da cui l'iniettività di f si ha $a = a'$, cioè $a id_A a'$. Viceversa, se $a = a'$, allora $f(a) = f(a')$ e quindi $a \mathfrak{R}_f a'$. Questo dimostra che le due relazioni coincidono.

Supponiamo ora invece che \mathfrak{R}_f coincida con la relazione d'uguaglianza id_A e dimostriamo che f è iniettiva. Se $a, a' \in A$ e $f(a) = f(a')$, allora, per come è definita \mathfrak{R}_f si ha $a \mathfrak{R}_f a'$; ma $\mathfrak{R}_f = id_A$ e quindi $a id_A a'$, cioè $a = a'$. Pertanto f è iniettiva. ■

Esercizio 3.6.21

Siano $A = \{n \in \mathbb{N} \mid n < 10\}$ e $B = \{n \in \mathbb{N} \mid n < 9\}$. Detti T l'insieme delle applicazioni da A in A ed S l'insieme delle applicazioni da B in A , sia poi $r : T \rightarrow S$ l'applicazione che associa ad ogni $f \in T$ la restrizione di f a B , cioè l'applicazione $x \in B \mapsto f(x) \in A$.

- Esprimere (non calcolare) $|T|$ ed $|S|$.
- Vero o falso? Per ogni $f \in T$:
 - f iniettiva $\implies r(f)$ è iniettiva;
 - f suriettiva $\implies r(f)$ è suriettiva;
- r è iniettiva? r è suriettiva?
- Sia ora \mathfrak{R} il nucleo di equivalenza di r , e sia h l'applicazione costante $h : x \in A \mapsto 3 \in A$. Descrivere $[h]_{\mathfrak{R}}$, calcolare $|(h)_{\mathfrak{R}}|$ e $|T/\mathfrak{R}|$.

TECNICHE DI ENUMERAZIONE

4.1

CARDINALITÀ DEGLI INSIEMI



4.1.1 ■ Il principio di inclusione-esclusione

Vogliamo contare il numero di elementi dell'unione di due o più insiemi finiti. In teoria insiemistica, per indicare il numero di elementi di un insieme finito A si usa il simbolo $|A|$, tale numero indica la **cardinalità**, ovvero il numero di elementi, dell'insieme A . Iniziamo col caso di due insiemi.

Proposizione 4.1.1

Siano A e B due insiemi finiti di cardinalità finita n e m rispettivamente, che siano disgiunti ($A \cap B = \emptyset$). Allora

$$|A \cup B| = |A| + |B| = n + m \quad (4.1)$$

La formula si generalizza al caso di k insiemi finiti A_i , $i = 1, 2, \dots, k$, con $|A_i| = n_i$, disgiunti due a due:

$$|\bigcup_{i=1}^k A_i| = \sum_{i=1}^k |A_i| = n_1 + \dots + n_k \quad (4.2)$$

Proposizione 4.1.2 (Principio di inclusione-esclusione)

Siano A e B due insiemi finiti con k elementi in comune, ossia $k = |A \cap B|$, allora:

$$|A \cup B| = |A| + |B| - |A \cap B| = n + m - k \quad (4.3)$$

Il termine correttivo $-k$ si inserisce poiché i k elementi comuni ad A e B compaiono tra gli n del primo insieme e gli m del secondo e sarebbero pertanto contati due volte in $n + m$. Tralasciamo la sua generalizzazione al caso di k insiemi poiché decisamente più complicata. La riportiamo solo per il caso $k = 3$:

$$|A_1 + A_2 + A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| - |A_1 \cap A_2 \cap A_3| \quad (4.4)$$

Esempio 4.1.1

Su 25 studenti, 15 hanno superato l'esame di Analisi, 12 quello di Programmazione e 5 hanno superato entrambi gli esami. Quanti studenti hanno superato almeno un esame? Quanti studenti hanno fallito entrambi gli esami? Sia A l'insieme degli studenti che hanno superato l'esame di Analisi: $|A| = 15$. Sia B l'insieme degli studenti che hanno superato l'esame di Programmazione, $|B| = 12$. $A \cap B$ è l'insieme degli studenti che hanno superato entrambi gli esami: $|A \cap B| = 5$. La risposta alla prima domanda è l'ordine dell'insieme $A \cup B$, dato da $15 + 12 - 5 = 22$. Non hanno superato nessuno dei due esami $25 - 22 = 3$ studenti.

Esempio 4.1.2

Sia $I = \{1, 2, \dots, 20\}$. Quanti sono i numeri di I divisibili per 2 o per 3? Sia A l'insieme dei numeri pari di I : l'ordine di A è 10. Sia B l'insieme dei multipli di 3 in I : $B = \{3, 6, 9, 12, 15, 18\}$ ha ordine 6. $A \cap B$ è l'insieme dei multipli di 6 minori di 20: $A \cap B = \{6, 12, 18\}$ ha ordine 3. I numeri di I divisibili per due o per 3 sono $10 + 6 - 3 = 13$.

Esempio 4.1.3

In un gruppo di amici tutti hanno visto almeno uno dei film x , y , z : 8 hanno visto il film x , 12 il film y e 9 il film z . Inoltre 6 hanno visto x e y , 4 hanno visto x e z , 7 hanno visto y e z e soltanto uno di essi ha assistito alle tre proiezioni. Da quante persone è formato il gruppo? Con ovvio significato delle notazioni si ha: $|X| = 8$, $|Y| = 12$, $|Z| = 9$, $|X \cap Y| = 6$, $|X \cap Z| = 4$, $|Y \cap Z| = 7$, $|X \cap Y \cap Z| = 1$. Quindi:

$$|X \cup Y \cup Z| = 8 + 12 + 9 - 4 - 7 + 1 = 13$$

4.1.2 ■ Insiemi finiti

Proposizione 4.1.3

Siano A e B insiemi non vuoti tali che $|A| = n$ e $|B| = m$. Allora il prodotto cartesiano $A \times B$ avrà precisamente nm elementi:

$$|A \times B| = nm \quad (4.5)$$

Dimostrazione. Se $A = a_1, \dots, a_n$, consideriamo gli n sottoinsiemi B_i di $A \times B$ a due a due disgiunti formati ognuno dalle m coppie aventi a_i come prima componente. Si avrà quindi:

$$|A \times B| = |B_1| + \dots + |B_n| = nm$$

□

Lemma 4.1.1

Siano A e B insiemi non vuoti tali che $|B| = m$ e $|A| = n$. Il numero di applicazioni $A \rightarrow B$ è m^n :

$$|\text{Map}(A, B)| = m^n \quad (4.6)$$

In teoria degli insiemi si denota l'insieme $\text{Map}(A, B)$ col simbolo B^A . Quindi:

$$|B^A| = |B|^{|A|} = m^n \quad (4.7)$$

Dimostrazione. Poniamo $A = \{a_1, a_2, \dots, a_n\}$. Preso un $\bar{a} \in A$ esistono m possibili scelte come sua immagine, possiamo quindi dire che un'applicazione $f : a \rightarrow B$ è univocamente determinata dalla n -pla delle immagini $(f(a_1), f(a_2), \dots, f(a_n)) \in B^n$, dove B^n è il prodotto cartesiano di B con se stessa per n volte. Sfruttando la Proposizione 4.1.3 sappiamo che $|B^n| = \underbrace{m \cdot \dots \cdot m}_{n \text{ volte}} = m^n$.

Quindi $|B^A| = |B^n| = m^n$. □

Esempio 4.1.4

Dato un alfabeto C di k caratteri, quante parole (stringhe) di lunghezza n sull'alfabeto C esistono? La domanda si traduce nella ricerca di tutte le possibili applicazioni dall'insieme $I_n = \{1, 2, 3, \dots, n\}$ all'insieme C . Infatti una stringa di lunghezza n può essere espressa nella forma:

$$[g(1) \ g(2) \ g(3) \ \dots \ g(n)]$$

con $g \in \text{Map}(I_n, C)$. Per il lemma precedente abbiamo quindi $|\text{Map}(I_n, C)| = k^n$ possibili stringhe.

Esempio 4.1.5

Sia $A = \{a_1, a_2, a_3\}$ e $B = \{b_1, b_2\}$. Abbiamo quindi che $|A| = 3$, $|B| = 2$ e $|Map(A, B)| = 2^3 = 8$. Per trovare tutte le otto applicazioni da A in B basta costruire la seguente tabella:

	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7
a_1	b_1	b_1	b_1	b_1	b_2	b_2	b_2	b_2
a_2	b_1	b_1	b_2	b_2	b_1	b_1	b_2	b_2
a_3	b_1	b_2	b_1	b_2	b_1	b_2	b_1	b_2

Tabella 4.1: Elementi di $Map(A, B)$

In questo caso troviamo due applicazioni costanti (f_0, f_7), le applicazioni $f_{1:6}$ sono suriettive mentre nessuna applicazione è iniettiva.

In generale, la presenza o meno di applicazioni iniettive in B^A dipende dalla relazione $n \leq m$. Non a caso, nel caso analizzato nell'esempio precedente, non esistevano applicazioni iniettive in quanto $|A| = 3 > 2 = |B|$. Si consideri l'insieme $A = \{a_1, a_2, \dots, a_n\}$. Una applicazione f per essere iniettiva deve associare n valori diversi a ciascun elemento di A quindi la cardinalità del suo codominio deve essere *almeno pari* a quella del dominio A .

Proposizione 4.1.4 (Condizione esistenza applicazioni iniettive)

Esistono applicazioni iniettive in B^A se e solo se:

$$|A| \leq |B| \quad (4.8)$$

nel caso, il loro numero è dato da:

$$|Inj\ Map(A, B)| = m(m-1)(m-2)\cdots(m-n+1) = m^n \quad (4.9)$$

dove m^n è chiamato **fattoriale discendente**^a.

^aNotazione introdotta da Donald Knuth. Conosciuto per essere l'autore di *The Art of Computer Programming*, è considerato il padre del campo di studio che studia in maniera rigorosa la parte algoritmica della teoria della complessità e ha dato fondamentali contributi in svariati rami dell'informatica teorica.

Dimostrazione. Consideriamo gli insiemi $A = \{a_1, \dots, a_n\}$ e $B = \{b_1, \dots, b_m\}$ per costruire una applicazione iniettiva da A in B possiamo procedere nel modo seguente. Preso $a_1 \in A$ esistono m possibili scelte in B da far mappare su a_1 :

$$a_1 \mapsto \dots m \text{ scelte possibili in } B$$

passando all'elemento a_2 non avremo più m possibili scelte bensì $m - 1$ per garantire l'iniettività dell'applicazione che stiamo costruendo:

$$a_2 \mapsto \dots m - 1 \text{ scelte possibili in } B$$

procedendo in avanti:

$$a_3 \mapsto \dots m - 2 \text{ scelte possibili in } B$$

Se $n > m$ chiaramente non sarà possibile trovare nuovi elementi distinti da mappare per ogni elemento a_i , non sarà possibile quindi costruire una applicazione iniettiva. Nel caso contrario, se $n \leq m$, anche all'elemento a_n sarà possibile mappare un elemento distinto da tutti gli altri precedentemente selezionati e in particolare:

$$a_n \mapsto \dots m - (n - 1) \text{ scelte possibili in } B$$

Dove $m - (n - 1)$ sarà sicuramente maggiore di zero in quanto $n \leq m$. Per l' i -esimo elemento di A esisteranno quindi, sotto questa condizione, $m - i + 1$ possibili scelte in B da mappare:

$$a_i \mapsto \dots m - i + 1 \text{ scelte possibili in } B$$

L'insieme delle coppie ordinate così costruite sarà quindi composto da:

$$m(m-1)(m-2)\cdots(m-n+1)$$

elementi. □

Esempio 4.1.6

Si consideri l'insieme delle lettere dell'alfabeto italiano:

$$I = \{A, B, C, D, E, F, G, H, I, L, M, N, O, P, Q, R, S, T, U, V, Z\}$$

Cercare stringhe di lunghezza 5 in cui non ci siano ripetizioni significa cercare le applicazioni iniettive dall'insieme delle posizioni $P = \{1, 2, 3, 4, 5\}$ all'insieme I . Il numero di applicazioni iniettive che possiamo costruire sarà:

$$21^5 = 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 = 2441880$$

Corollario 4.1.1

È possibile riscrivere l'equazione 4.9 in termini di fattoriale e vale:

$$|Inj\ Map(A, B)| = \frac{m!}{(m - n)!} \quad (4.10)$$

Definizione 4.1.1: Equipotenza

Due insiemi A e B si dicono **equipotenti** se e solo se:

$$|A| = |B| \quad (4.11)$$

Principio della piccionaia

Se una piccionaia ha m nicchie e n piccioni, con $n > m$, allora almeno due piccioni finiscono nella stessa nicchia.

Tradotto in termini rigorosi, il principio sostiene che, se $n > m$, nessuna funzione di A in B è iniettiva. Più in generale vale quanto segue:

Teorema 4.1.1

Dati A e B insiemi finiti. Assumiamo $|A| = n$ e $|B| = m$. Allora:

1. Esistono applicazioni iniettive da A in B se e soltanto se $n \leq m$;
2. Esistono applicazioni suriettive da A in B se e soltanto se $n \geq m$ oppure se da $B = \emptyset$ allora segue $A = \emptyset$.
3. Esistono applicazioni biettive da A in B se e soltanto se i due insiemi sono equipotenti, cioè $n = m$;

Dimostrazione. Si ha:

1. Già vista nella proposizione 4.1.4.
2. Sia $B \neq \emptyset$ e sia $m \leq n$, esiste quindi una applicazione iniettiva $f : B \rightarrow A$. In questo caso esiste sicuramente una retrazione di f , ovvero una applicazione $h : A \rightarrow B$ che è sicuramente suriettiva.

Viceversa, se esiste un'applicazione $f : A \rightarrow B$ suriettiva allora f ammette sezioni $h : B \rightarrow A$ e tale applicazione è iniettiva e vale $|A| \geq |B|$. Se B è l'insieme vuoto esistono invece due casi:

- Se $n > 0$ allora non esistono applicazioni da A in B ;
 - Se $n = 0$ allora $A = B = \emptyset$ e $B^A = Map(A, B) = \{id_{\emptyset}\}$ che risulta biettiva, e in particolare suriettiva.
3. Se esistono applicazioni biettive da $A \rightarrow B$ allora esistono applicazioni che siano iniettive e suriettive, quindi $n \leq m \wedge m \leq n \implies n = m$ e i due insiemi risultano equipotenti. Viceversa, siano A e B equipotenti. Ponendo $f(a_i) = b_i$ per ogni $i = 1, \dots, n$ si definisce una funzione biettiva di A in B .

□

Corollario 4.1.2

Siano A e B due insiemi finiti. Allora:

$$|A| \leq |B| \wedge |B| \leq |A| \implies |A| = |B| \quad (4.12)$$

Teorema 4.1.2

Siano A e B due insiemi finiti equipotenti e sia $f : A \rightarrow B$ un'applicazione. Allora sono equivalenti:

1. f è iniettiva
2. f è suriettiva
3. f è biettiva

Dimostrazione. • Consideriamo l'immagine di f , l'insieme $im\ f = \{f(x) \mid x \in A\}$. Siccome f è iniettiva, $im\ f$ ha la stessa cardinalità di A perché ad ogni elemento di A corrisponde un elemento distinto in $im\ f$. Ora, dato che A è equipotente a B , la cardinalità di A è uguale a quella di B . Quindi, la cardinalità di $im\ f$ è uguale a quella di B per transitività. Poiché $im\ f \subseteq B$ e $|im\ f| = |B|$, l'unica possibilità è che $im\ f = B$, ma ciò significa che f è suriettiva, e quindi biettiva. Quindi $(1 \implies 3)$.

- Che $(3 \implies 2)$ risulta ovvio.
- Resta da dimostrare che $(2 \implies 1)$. Supponiamo che f sia suriettiva. Allora f , per il Teorema 3.4.1, ha una sezione $g : B \rightarrow A$, ovviamente g risulta iniettiva (in quanto, per definizione di sezione, deve essere $f \circ g = id_B$ ed f risulta essere una retrazione per g). Avendo dimostrato che se f è una applicazione iniettiva tra due insiemi equipotenti allora questa risulta essere una biezione, allora g è una applicazione biettiva e quindi invertibile. Applicando i risultati del Teorema 3.4.3 f è l'unica retrazione di g e coincide con la sua inversa. Allora $f = g^{-1}$ che risulta essere biettiva. e in particolare iniettiva. Come volevasi dimostrare.

□

Corollario 4.1.3

Se $|A| = |B| = m$ allora ogni applicazione iniettiva da A a B è biettiva. In questo caso:

$$|Inj\ Map(A, B)| = \frac{|a|!}{(|a| - |b|)!} = \frac{|a|!}{0!} = m!$$

Osservazione 4.1.1 ➤➤➤

Per le conclusioni appena dimostrate, un insieme risulta infinito se esiste un'applicazione iniettiva $f : A \rightarrow A$. Inoltre, l'insieme delle permutazioni in un insieme A , $Sym(A)$, ovvero l'insieme delle applicazioni biettive $\sigma : A \longrightarrow A$ ha ben $|A|!$ elementi.

Esempio 4.1.7

Sono equipotenti l'insieme \mathbb{N} dei numeri naturali e l'insieme \mathbb{Z} dei numeri interi relativi. Consideriamo infatti la funzione:

$$h : n \in \mathbb{N} \mapsto \begin{cases} \frac{n}{2} & \text{se } n \text{ è pari} \\ -\frac{n+1}{2} & \text{se } n \text{ è dispari} \end{cases} \in \mathbb{Z}$$

Chiaramente h è iniettiva, infatti:

$$\forall a, b \in \mathbb{N} (h(a) = h(b) \implies a = b)$$

Se $h(a) = h(b)$ possiamo avere i due seguenti casi:

$$\begin{cases} \frac{a}{2} = \frac{b}{2} \implies a = b \\ -\frac{a+1}{2} = -\frac{b+1}{2} \implies a = b \end{cases}$$

Inoltre, per ogni $b \in \mathbb{Z}$ possiamo trovare un elemento $x \in \mathbb{N}$ per il quale valga $b = h(x)$:

- Se $b \in \mathbb{N}$ allora $b = h(2b)$;
- Se $b \in \mathbb{Z} \setminus \mathbb{N}$ allora $b = h(-2b - 1)$.

Ciò dimostra la suriettività di h che risulta infine biettiva. L'inversa della funzione h è:

$$h^{-1} : b \in \mathbb{Z} \mapsto \begin{cases} 2b & \text{se } b \geq 0 \\ 2b - 1 & \text{se } b < 0 \end{cases} \in \mathbb{N}$$

Quindi $|\mathbb{N}| = |\mathbb{Z}|$.

Definizione 4.1.2: Insiemi infiniti

Un insieme è **infinito** se è equipotente ad un suo sottoinsieme proprio. Un insieme è **finito** se questo non capita.

Esempio 4.1.8

L'insieme dei numeri naturali \mathbb{N} è un insieme infinito poiché la funzione “successore” $\sigma : \mathbb{N} \rightarrow \mathbb{N}$, $\sigma(n) = n + 1$ è iniettiva ma non suriettiva. Possiamo anche vedere che la funzione “doppio” $f : \mathbb{N} \rightarrow P$ (dove P è l'insieme dei numeri pari) data da $f(n) = 2n$ è biunivoca e quindi \mathbb{N} è equipotente ad una sua parte propria.

4.1.3 ■ La funzione caratteristica e la cardinalità dell'insieme delle parti

Definizione 4.1.3: Funzione caratteristica

Sia S un insieme e $T \subseteq S$ un suo sottoinsieme. L'applicazione $\chi_{T,S} \in Map(S, \{0, 1\})$, definita come:

$$\chi_{T,S} : x \in S \mapsto \begin{cases} 1 & \text{se } x \in T \\ 0 & \text{se } x \notin T \end{cases} \in \{0, 1\} \quad (4.13)$$

prende il nome di **applicazione caratteristica**^a di T in S .

^aPuò essere visto come un predicato logico che verifica l'appartenenza di un elemento x in T

Esempio 4.1.9

Sia $S = \{1, 2, 3, 4, 5, 6, 7\}$ e sia $T = \{2, 4, 7\} \in \mathcal{P}(S)$, allora $\chi_{T,S}$ è uguale a:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Si considerino le applicazioni biettive:

$$\begin{aligned} \alpha : T \in \mathcal{P}(S) &\mapsto \chi_{T,S} \in M \\ \beta : f \in Map(S, \{0, 1\}) &\mapsto \overleftarrow{f}(\{1\}) \in \mathcal{P}(S) \end{aligned}$$

allora vale il seguente teorema:

Teorema 4.1.3

Le applicazioni biettive α e β sono l'una l'inversa dell'altra.

Dimostrazione. Per comodità poniamo $M = Map(S, \{0, 1\})$. Per dimostrare l'enunciato bisogna verificare che β sia una sezione ed una retrazione di α ovvero:

$$\begin{aligned} \alpha \circ \beta &= id_M \\ \beta \circ \alpha &= id_{\mathcal{P}(S)} \end{aligned}$$

1. Si ha chiaramente che, per ogni applicazione $f \in M$:

$$\begin{aligned} \alpha(\beta(f)) &= \alpha(\overleftarrow{f}(\{1\})) \\ &= \chi_{\overleftarrow{f}(\{1\}), S} \mapsto \begin{cases} 1 & \text{se } x \in \overleftarrow{f}(\{1\}) \\ 0 & \text{se } x \notin \overleftarrow{f}(\{1\}) \end{cases} \end{aligned}$$

e si ha che, $\forall x \in S$:

$$x \in \overleftarrow{f}(\{1\}) \iff f(x) \in \{1\} \iff f(x) = 1$$

dunque, per ogni $f \in M$,

$$\chi_{\overleftarrow{f}(\{1\}), S} : x \in S \mapsto \begin{cases} 1 & \text{se } f(x) = 1 \\ 0 & \text{se } f(x) = 0 \end{cases}$$

il che è equivalente a mappare $x \in S$ su $f(x) \in \{0, 1\}$, quindi $\chi_{\overleftarrow{f}(\{1\}), S} = f$ e abbiamo $\alpha(\beta(f)) = f$, cioè $\alpha \circ \beta = id_M$.

2. Per ogni sottoinsieme T di S , si ha:

$$\beta(\alpha(T)) = \beta(\chi_{T,S}) = \overleftarrow{\chi_{T,S}}(\{1\}) = \{x \in S \mid \chi_{T,S}(x) = 1\} = T$$

Quindi $\beta \circ \alpha = id_{\mathcal{P}(S)}$ e l'enunciato è dimostrato. □

Corollario 4.1.4

Se S è un insieme finito con n elementi allora avrà esattamente 2^n parti finite. Ovvero:

$$|\mathcal{P}(S)| = |Map(S, \{0, 1\})| = 2^{|S|} = 2^n \quad (4.14)$$

Dimostrazione. Basta applicare la formula 4.6 e osservare che $|\{0, 1\}| = 2$. □

Definizione 4.1.4: Coefficiente binomiale

Dati S un insieme di n elementi e $k \in \mathbb{N}$ è possibile considerare l'insieme:

$$\mathcal{P}_k(S) = \{X \subseteq S \mid |X| = k\} \quad (4.15)$$

ovvero l'insieme delle parti di S con k elementi. Per indicare la cardinalità di $\mathcal{P}_k(S)$ si usano i **coefficienti binomiali**. Ovvero:

$$\binom{n}{k} = |\mathcal{P}_k(S)| \quad (4.16)$$

dove $\binom{n}{k}$ si legge “coefficiente binomiale di n su k ”.

Osservazione 4.1.2



Alcuni coefficienti binomiali immediati da calcolare: per ogni $n \in \mathbb{N}$ vale:

$$\binom{n}{0} = 1 = \binom{n}{n} \quad (4.17)$$

Infatti, se consideriamo un insieme finito S di cardinalità n , il numero di sottoinsiemi di cardinalità pari a zero è uno in quanto il solo insieme vuoto risulta avere tale cardinalità. Analogamente, l'unico sottoinsieme di S di cardinalità pari a quella di S risulta S stesso. Un'altra proprietà molto semplice da verificare è:

$$\binom{n}{1} = n \quad (4.18)$$

La cui dimostrazione è abbastanza banale in quanto in un insieme finito di n elementi esistono sempre n singleton.

Proposizione 4.1.5

Per ogni $n \in \mathbb{N}$ si ha:

$$\sum_{k=0}^n \binom{n}{k} = 2^n \quad (4.19)$$

Dimostrazione. Sia S un insieme tale che $|S| = n$. È chiaro che $\mathcal{P}(S)$ è unione disgiunta degli insiemi $\mathcal{P}_k(S)$ al variare dell'intero k tra 0 ed n . In altri termini $\{\mathcal{P}_k(S) \mid k \in \mathbb{N} \wedge k \leq n\}$ è una partizione di $\mathcal{P}(S)$. Pertanto $|\mathcal{P}(S)| = \sum_{k=0}^n \binom{n}{k} = 2^n$ e, per ogni scelta di k , $|\mathcal{P}_k(S)| = \binom{n}{k}$. Otteniamo così l'asserto. □

Si può pensare al coefficiente binomiale $\binom{n}{k}$ in questi termini: $\binom{n}{k}$ è il numero di modi in cui si possono scegliere k oggetti da un insieme di n oggetti (infatti scegliere k oggetti significa in sostanza scegliere una k -parte). Ora, selezionare k oggetti da un insieme di n è concettualmente equivalente a sceglierne $n - k$ da scartare. Dunque dovrebbe essere facile comprendere che il coefficiente binomiale $\binom{n}{n-k}$ coincide con $\binom{n}{k}$.

Proposizione 4.1.6

Siano $n, k \in \mathbb{N}$ e sia $k \leq n$, vale allora:

$$\binom{n}{n-k} = \binom{n}{k} \quad (4.20)$$

Dimostrazione. Consideriamo l'applicazione:

$$\xi : X \in \mathcal{P}(S) \mapsto S \setminus X \in \mathcal{P}(S)$$

che ad ogni parte di S associa il suo complemento in S . Essendo $S \setminus (S \setminus X) = X$ ovvero $\xi(\xi(S \setminus X)) = \xi^2(S \setminus X) = X$ deve essere per forza $\xi^2 = id_{\mathcal{P}(S)}$.

Per questo motivo ξ corrisponde all'inversa di se stessa e dunque risulta essere biettiva. L'immagine dell'insieme $\mathcal{P}_k(S)$ è costituita dai complementi delle parti di S con cardinalità pari a k . Tali complementi avranno cardinalità pari a $n - k$. Essendo ξ una applicazione biettiva risulterà:

$$|\mathcal{P}_k(S)| = |\xi(\mathcal{P}_k(S))| = |\mathcal{P}_{n-k}(S)|$$

da cui deriva l'asserto. \square

Proposizione 4.1.7

Sia $n, k \in \mathbb{N}$ vale allora:

$$\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k} \quad (4.21)$$

Dimostrazione. Diamo questa dimostrazione in una versione poco formalizzata ma più facile da seguire di quanto sarebbe in una stesura più rigorosa.

Supponiamo di avere un insieme S costituito da $n + 1$ palline bianche. Ovviamente $S \neq \emptyset$, perché $n + 1 > 0$, quindi possiamo selezionare una delle palline e colorarla, diciamo, di nero. Il coefficiente binomiale che vogliamo calcolare, $\binom{n+1}{k+1}$, è il numero delle $k + 1$ parti di S . Possiamo distinguere tra due tipi di $(k + 1)$ -parti di S : quelle costituite da sole palline bianche e quelle costituite dalla pallina nera e da k palline bianche. Ovviamente $\binom{n+1}{k+1}$ è la somma tra il numero delle parti del primo tipo ed il numero delle parti del secondo tipo. Quante sono le parti del primo tipo? Esse sono precisamente le $(k + 1)$ -parti dell'insieme delle palline bianche. Poiché il numero delle palline bianche è n , questo numero sarà $\binom{n}{k+1}$. Quante sono invece le parti del secondo tipo? Ciascuna di esse si ottiene aggiungendo la pallina nera del secondo tipo ad una k -parte dell'insieme delle palline bianche, e da ciò è facile dedurre che il numero delle parti del secondo tipo è uguale a quello delle k parti dell'insieme delle palline bianche, dunque $\binom{n}{k}$. Pertanto $\binom{n+1}{k+1}$, che come detto è uguale alla somma tra il numero delle parti del primo tipo ed il numero delle parti del secondo tipo, è proprio $\binom{n}{k+1} + \binom{n}{k}$, come volevasi dimostrare. \square

Questa proprietà permette di costruire i coefficienti binomiali con il cosiddetto **triangolo di Tartaglia** come mostrato in Figura 4.1.

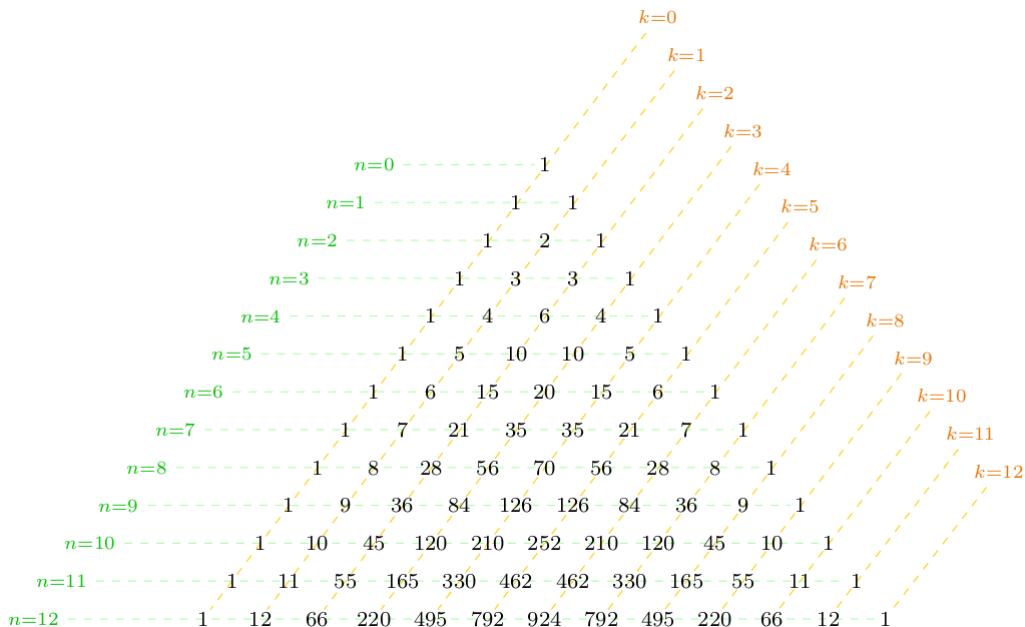


Figura 4.1: Triangolo di Tartaglia

**Proposizione 4.2.1 (Principio di induzione (Prima forma))**

Sia p un predicato unario nella variabile n e $b \in \mathbb{N}$ un numero naturale. Sia $\mathbb{N}_b = \{n \in \mathbb{N} \mid b \leq n\}$. Vale allora la seguente implicazione:

$$\left(p(b) \wedge \left(\forall n \in \mathbb{N}_b (p(n) \implies p(n+1)) \right) \right) \implies \forall n \in \mathbb{N}_b (p(n)) \quad (4.22)$$

Dimostrazione. Si veda la sezione 7.1.1. □

Teorema 4.2.1

Per ogni $n, k \in \mathbb{N}$ tali che $k \leq n$, vale allora:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad (4.23)$$

Dimostrazione. Si dimostra per induzione.

- **Passo base:** sia $n = 0$. Verifichiamo che il predicato sia vero. Se $n = 0$ allora l'unico $k \leq n$ risulta essere $k = 0$. Essendo $\binom{0}{0} = 1$ allora risulta :

$$\binom{0}{0} = \frac{0!}{0!} = 1$$

e il predicato risulta vero. In generale:

$$\binom{n}{0} = \frac{n!}{0!(n-0)!} = \frac{n!}{n!} = 1$$

- **Passo induttivo:** assumiamo vero il predicato $p(n)$, dimostriamo $p(n) \implies p(n+1)$. Si ha:

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

Se $k = 0$ abbiamo che il predicato risulta vero. Se $k \neq 0$ applichiamo la formula 4.21:

$$\begin{aligned} \binom{n+1}{k} &= \binom{n}{k} + \binom{n}{k-1} \\ &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\ &= \frac{n!}{(k-1)!(n-k)!} \left(\frac{1}{k} + \frac{1}{n-k+1} \right) \\ &= \frac{n!}{(k-1)!(n-k)!} \left(\frac{n-k+1+k}{k(n-k+1)} \right) \\ &= \frac{n!(n+1)}{k!(n-k+1)!} \\ &= \frac{(n+1)!}{k!((n+1)-k)!} \end{aligned}$$

Il che dimostra il predicato $p(n+1)$. □



Esercizio 4.3.1

Siano $X = \{1, 2, 3, 4, 5\}$ ed $Y = \{1, 2, 3\}$.

1. Quanti sono i sottoinsiemi di X che contengono l'elemento 1?
2. Quanti sono i sottoinsiemi A di X che contengono l'elemento 1 e tali che $A \cap \{2, 3\} \neq \emptyset$?
3. Quante sono le applicazioni iniettive da X a Y ?
4. Quante sono le applicazioni iniettive da Y a X ?
5. Quante sono le applicazioni suriettive da X in Y ?

Svolgimento. Abbiamo:

1. Sia Ω l'insieme di tutti i sottoinsiemi di X che contengono l'elemento 1, ovvero:

$$\Omega := \{A \subseteq X \mid 1 \in A\}$$

Allora è immediato constatare che Ω è in corrispondenza biunivoca con l'insieme delle parti $X \setminus \{1\}$, mediante l'applicazione:

$$\begin{aligned}\varphi : \Omega &\rightarrow \mathcal{P}(X \setminus \{1\}) \\ A &\mapsto A \setminus \{1\}\end{aligned}$$

Ne segue che $|\Omega| = |\mathcal{P}(X \setminus \{1\})| = 2^{|X \setminus \{1\}|} = 2^4 = 16$.

2. Indichiamo con Θ il seguente insieme:

$$\Theta := \{A \subseteq X \mid 1 \in A \wedge A \cap \{2, 3\} \neq \emptyset\}$$

Osserviamo che Θ è l'unione insiemistica di Λ e Δ , dove:

$$\begin{aligned}\Lambda &:= \{A \subseteq X \mid 1 \in A \wedge 2 \in A\} \\ \Delta &:= \{A \subseteq X \mid 1 \in A \wedge 3 \in A\}\end{aligned}$$

Pertanto $\Theta = \Lambda \cup \Delta$. Ragionando come nel punto precedente, si ha che:

$$|\Lambda| = |\Delta| = 2^3 = 8$$

Inoltre $\Lambda \cap \Delta := \{A \subseteq X \mid \{1, 2, 3\} \subseteq A\}$, quindi $|\Lambda \cap \Delta| = 2^2 = 4$. Siamo perciò in grado di calcolare con esattezza il numero di elementi di Θ tramite la 4.3:

$$|\Theta| = |\Lambda \cup \Delta| = |\Lambda| + |\Delta| - |\Lambda \cap \Delta| = 12$$

3. Essendo $|X| \geq |Y|$ non esistono applicazioni iniettive da X in Y .
4. Si ha $|Inj\ Map(Y, X)| = 5^3 = 5 \cdot 4 \cdot 3 = 60$ applicazioni iniettive.
5. Sia $S \subseteq Map(X, Y)$ l'insieme di tutte le applicazioni suriettive da X in Y . Inoltre, per ogni $y \in Y$ indichiamo con A_y il sottoinsieme di $Map(X, Y)$ definito come:

$$\begin{aligned}A_y &:= \{f \in Map(X, Y) \mid y \notin f(X)\} \\ &:= \{f \in Map(X, Y) \mid f^{-1}(\{y\}) = \emptyset\}\end{aligned}$$

Una applicazione f è suriettiva se e solo se non appartiene a nessun A_y , per ogni $y = 1, 2, 3$ abbiamo che:

$$S = Map(X, Y) \setminus (A_1 \cup A_2 \cup A_3) \quad (4.24)$$

Ne segue che:

$$\begin{aligned}|S| &= |Map(X, Y)| - |A_1 \cup A_2 \cup A_3| \\ &= 3^5 - |A_1 \cup A_2 \cup A_3|\end{aligned}$$

Osserviamo che per ogni $f \in A_1$ vale $f(X) \subseteq \{2, 3\}$, pertanto per tali funzioni l'insieme dei valori ammissibili è $\{2, 3\}$, detto in altri termini: $|A_1| = |\{2, 3\}|^{|X|} = 2^5$. Similmente per A_2 e A_3 . Ora ci si accorge subito che $A_1 \cap A_2$ contiene solo la funzione costante $c_3 : x \mapsto 3$, per ogni $x \in X$ e, similmente, $A_1 \cap A_3 = \{c_2\}$, $A_2 \cap A_3 = \{c_1\}$. In particolare $|A_1 \cap A_2| = |A_1 \cap A_3| = |A_2 \cap A_3| = 1$. Mentre $A_1 \cap A_2 \cap A_3 = \emptyset$. Applicando la 4.4 otteniamo:

$$\begin{aligned}|A_1 \cup A_2 \cup A_3| &= |A_1| + |A_2| + |A_3| + |A_1 \cap A_2 \cap A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ &= 3 \cdot 2^5 + 3 \cdot 1 - 0 \\ &= 3 \cdot (2^5 - 1) \\ &= 3 \cdot 31\end{aligned}$$

Ne segue che $|S| = 150$. ■

Esercizio 4.3.2

Siano $A = \{n \in \mathbb{N} \mid n < 8\}$ e $B = \{n \in \mathbb{N} \mid n < 10\}$. Esprimere:

1. $|A|$, $|B|$ e $|A \times B|$;
2. il numero delle applicazioni da A a B e, tra queste, il numero di quelli iniettive, il numero di quelle suriettive, il numero di quelle biettive;
3. il numero delle applicazioni da $A \times B$ a $B \times A$ e, tra queste, il numero di quelli iniettive, il numero di quelle suriettive, il numero di quelle biettive;
4. il numero delle applicazioni costanti da B ad A ;
5. il numero delle applicazioni f da B ad A tali che $f(0) = 2$;
6. il numero delle applicazioni f da B ad A tali che $\text{im } f \subseteq \{0, 1, 7\}$;
7. il numero di applicazioni iniettive f da A a B tali che $f(0) \neq 5$.

Sia X una parte di A . Supponiamo che esista un'applicazione suriettiva da X ad A . Cosa sappiamo dire su X ?

Svolgimento. Si ha:

1. $|A| = 8$, $|B| = 10$ e $|A \times B| = 80$.
2. Il numero di applicazioni da A in B è $|\text{Map}(A, B)| = 10^8$ mentre il numero di applicazioni iniettive da A in B è: $|\text{Inj Map}(A, B)| = 10^8$. Non esistono applicazioni suriettive da A in B in quanto $|A| \leq |B|$ e di conseguenza non esistono applicazioni biettive da A e B , non a caso A e B non possono essere equipotenti.
3. Si ha che $|A \times B| = |B \times A| = 80$ e i due prodotti cartesiani sono quindi equipotenti. Il numero di applicazioni è dato da: $|\text{Map}(A \times B, B \times A)| = 80^{80}$ mentre il numero di applicazioni iniettive e quindi biettive è $|\text{Inj Map}(A \times B, B \times A)| = 80!$.
4. Il numero di applicazioni costanti da B in A è dato dal numero degli elementi del codominio, ovvero 8.
5. Per trovare il numero di applicazioni f da B ad A tali che $f(0) = 2$ basta fissare tale mappa e considerare in numero di applicazioni tra il sottoinsieme $B \setminus \{0\}$ e A ovvero: $|\text{Map}(B \setminus \{0\}, A)| = 8^9 = 8^{10}/8$
6. Una funzione $f : B \rightarrow A$ tali che $\text{im } f \subseteq \{0, 1, 7\}$ può essere vista come una funzione $f : B \rightarrow \{0, 1, 7\}$ quindi il numero di applicazioni tra questi due insiemi è dato da 3^{10} .
7. Per trovare il numero di applicazioni iniettive da A in B tali che $f(0) \neq 5$ si ragiona nel modo seguente. All'elemento 0 non è possibile associare l'elemento $5 \in B$, esisteranno quindi 9 possibili scelte diverse da poter assegnare:

$$0 \mapsto \underbrace{\dots}_{9 \text{ scelte}}$$

All'elemento 1 sarà possibile assegnare $10 - 1$ scelte per ottenere una funzione iniettiva e così via:

$$\begin{aligned} 1 &\mapsto \underbrace{\dots}_{9 \text{ scelte}} \\ 2 &\mapsto \underbrace{\dots}_{8 \text{ scelte}} \\ &\vdots \\ 7 &\mapsto \underbrace{\dots}_{3 \text{ scelte}} \end{aligned}$$

Di conseguenza il numero di applicazioni iniettive tali che $f(0) \neq 5$ è dato da: $9 \cdot 9^7 = 9 \cdot 9 \cdot 8 \cdot 7 = 4536$.

Se X è una parte di A ed esiste una applicazione suriettiva da X in A allora $A = X$. Infatti, dire che esiste una applicazione suriettiva da X in A significa affermare che $|X| \geq |A|$ ma questo è possibile se e solo se $|A| = |X|$ essendo X una parte di A . ■

Esercizio 4.3.3

Utilizzando un alfabeto A di 7 caratteri, quante stringhe di lunghezza n possiamo formare se $n = 5$ e quante se $n = 12$? E, in ciascuno dei due casi, quante senza ripetizioni di caratteri?

Svolgimento. Utilizzando un alfabeto A di 7 caratteri possiamo considerare l'applicazione:

$$\lambda : I_n \longrightarrow A$$

che associa ad ogni numero $m \in I_n$ un elemento di A per costruire una stringa di lunghezza n . Dato $n = 5$ allora $|\text{Map}(I_n, A)| = 7^5$. Se $n = 12$ allora $|\text{Map}(I_n, A)| = 7^{12}$. Nel caso in cui $n = 5$ si ha: $|\text{Inj Map}(I_n, A)| = 7^5 = 2520$ mentre se $n = 12$ non esistono applicazioni iniettive. ■

Esercizio 4.3.4

Siano $S = \{0, 1, 5\}$ e $T = \{1, 2\}$. Descrivere esplicitamente tutte le applicazioni iniettive da T ad S e le applicazioni suriettive da S a T (suggerimento per la seconda parte: si fa prima a dire quali non sono suriettive). Quante sono?

Svolgimento. Dati gli insiemi $S = \{0, 1, 5\}$ e $T = \{1, 2\}$ si hanno 6 funzioni iniettive da T in S :

t_i	c_0	c_1	c_5	f_1	f_2	f_3	f_4	f_6	f_7
1	0	1	5	0	0	1	1	5	5
2	0	1	5	1	5	0	5	0	1

Le funzioni $f_{1:7}$ sono tutte iniettive. Le applicazioni suriettive da S in T sono tutte quelle non costanti. ■

Esercizio 4.3.5

Provare che se due insiemi A e B sono equipotenti, gli insiemi $(\mathcal{P}(A), \subseteq)$ e $(\mathcal{P}(B), \subseteq)$ sono isomorfi.

Numero di partizioni in un insieme finito

Indichiamo con B_{n+1} il numero di partizioni di un insieme finito con n elementi. Si dimostra che un insieme con $n+1$ elementi ammette un numero di partizioni dato da:

$$B_{n+1} = \sum_{k=0}^n \binom{n}{k} B_k \quad (4.25)$$

In altri termini, il numero di partizioni di un qualsiasi insieme finito si può calcolare mediante la successione ricorsiva $\{B_n\}_{n \in \mathbb{N}}$ detta **successione dei numeri di Bell**. I primi sette termini di tale successione sono: $B_0 = 1$, $B_1 = 1$, $B_2 = 2$, $B_3 = 5$, $B_4 = 15$, $B_5 = 52$, $B_6 = 203$.

OPERAZIONI E STRUTTURE ALGEBRICHE

5.1

GENERALITÀ SULLE OPERAZIONI



Definizione 5.1.1: Operazioni binarie

Se S è un insieme non vuoto, un'applicazione

$$\perp : S \times S \longrightarrow S$$

si chiama **operazione binaria** (ovunque definita) in S . Qualunque siano gli elementi x e y di S , l'immagine $\perp(x, y)$ della coppia x, y mediante \perp si dice **composto** di x e y , e si denota col simbolo $x \perp y$.

Esempio 5.1.1

1. In \mathbb{Z} sono operazioni binarie le operazioni di addizione, sottrazione e moltiplicazione.
2. La divisione non è un'operazione binaria in \mathbb{Z} in quanto non tutte le coppie $(m, n) \in \mathbb{Z}^2$ godono di composto. Ad esempio $(2, 4)$, infatti: $2 / 4 \notin \mathbb{Z}$.
3. Fissato un insieme A è possibile considerare l'insieme delle parti $\mathcal{P}(A)$. In $\mathcal{P}(A)$ è possibile considerare come operazioni binarie tutte le operazioni di intersezione, unione, differenza simmetrica e differenza, ecc.

Esiste un modo per rappresentare in tabella un'operazione. Supponiamo che l'insieme S sia composto da tre elementi:

$$S = \{a, b, c\}$$

Consideriamo un'operazione $\perp : S \times S \rightarrow S$ che può essere rappresentata mediante una tabella come mostrato qui di seguito:

\perp	a	b	c
a	$a \perp a$	$a \perp b$	$a \perp c$
b	$b \perp a$	$b \perp b$	$b \perp c$
c	$c \perp a$	$c \perp b$	$c \perp c$

Queste tabelle prendono il nome di **tavole di Cayley**.

5.1.1 ■ Proprietà delle operazioni

Definizione 5.1.2: Operazioni associative

Sia S un insieme non vuoto. Un'operazione $\perp : S \times S \longrightarrow S$ si dice **associativa** se risulta:

$$\forall x, y, z \in S ((x \perp y) \perp z = x \perp (y \perp z))$$

Esempio 5.1.2

Sono un esempio di operazioni associative tutte le operazioni insiemistiche come l'unione, l'intersezione, la differenza simmetrica, l'unione unaria e l'intersezione unaria.

Definizione 5.1.3: Operazioni commutative

Sia S un insieme non vuoto. Un'operazione $\perp : S \times S \rightarrow S$ si dice **commutativa** se risulta:

$$\forall x, y \in S (x \perp y = y \perp x)$$

Due elementi a, b di S tali che $a \perp b = b \perp a$ si dicono **permutabili**.

Osservazione 5.1.1



È possibile determinare la proprietà commutativa di un'operazione osservando la relativa tavola di Cayley. Infatti, un'operazione gode della proprietà commutativa se e solo se la tavola di Cayley è *simmetrica* lungo la propria diagonale.

Esempio 5.1.3

Sia $s = \{a, b\}$, è possibile quindi considerare l'insieme $\mathcal{P}(s) = \{\emptyset, \{a\}, \{b\}, s\}$ e l'operazione binaria interna $\cap : \mathcal{P}(s) \times \mathcal{P}(s) \rightarrow \mathcal{P}(s)$. Come ben sappiamo l'intersezione gode della proprietà commutativa e possiamo ben osservarlo costruendo la tavola di Cayley:

\cap	\emptyset	$\{a\}$	$\{b\}$	s
\emptyset	\emptyset	\emptyset	\emptyset	\emptyset
$\{a\}$	\emptyset	$\{a\}$	\emptyset	$\{a\}$
$\{b\}$	\emptyset	\emptyset	$\{b\}$	$\{b\}$
s	\emptyset	$\{a\}$	$\{b\}$	s

Infatti, osservando le celle dello stesso colore osserviamo che la tavola è simmetrica lungo la diagonale secondaria. Notiamo inoltre che, nonostante \cap goda anche della proprietà associativa questa non può essere osservata dalla tavola ed è necessario quindi eseguire un controllo diretto tra tutte le possibili composte.

Esempio 5.1.4

La sottrazione in \mathbb{Z} non gode della proprietà commutativa e associativa. Infatti:

$$\forall a, b \in \mathbb{Z} \quad a - b \neq b - a$$

Infatti: $3 - 2 \neq 2 - 3$. Per verificare l'associatività di una operazione è comodo verificare prima se essa gode della proprietà commutativa in quanto questa può velocizzare significativamente i calcoli. La sottrazione è associativa in \mathbb{Z} se e solo se:

$$\forall a, b, c \in \mathbb{Z} \quad ((a - (b - c)) = (a - b) - c)$$

Per procedere avanti nella dimostrazione si osserva che: $a - (b - c) = (a - b) + c$. Quindi per essere associativa l'operazione deve valere:

$$(a - b) + c = (a - b) - c$$

ma qualsiasi sia la terna, ad esempio $(0, 0, 1)$, si ha:

$$(0 - 0) + 1 \neq (0 - 0) - 1$$

Quindi l'operazione non è associativa in \mathbb{Z} .

Teorema 5.1.1 (Teorema di associatività)

Se un'operazione \star è associativa, presi n elementi, qualsiasi sia l'ordine delle operazioni, il risultato è sempre lo stesso.

Teorema 5.1.2 (Teorema di commutatività)

Se un'operazione \star è associativa e commutativa, dati n elementi, qualsiasi sia l'ordine delle operazioni e degli operandi il risultato non cambia.

Esempio 5.1.5

L'associatività e la commutatività *non sono correlate* tra di loro. Prendiamo ad esempio l'operazione binaria in \mathbb{Z} definita come:

$$\forall a, b \in \mathbb{Z} \quad a * b = (a + b)^2$$

Questa operazione è banalmente commutativa in quanto:

$$\forall a, b \in \mathbb{Z} \quad a * b = (a + b)^2 = (b + a)^2 = b * a$$

ma non è associativa. Infatti, per essere associativa dovrebbe essere:

$$\forall a, b, c \in \mathbb{Z} \quad a * (b * c) = (a * b) * c$$

ma

$$a * (b * c) = a * (b + c)^2 = (a + (b + c)^2)^2$$

e

$$(a * b) * c = c * (a * b) = (c + (a + b)^2)^2$$

sono diverse in quanto rappresentano due espressioni diverse qualunque sia la terna (a, b, c) .

Definizione 5.1.4: Operazioni distributive

Se \perp e \star sono operazioni in S , si dice che \star è **distributiva a destra** rispetto a \perp se per ogni terna x, y, z di elementi di S risulta

$$(x \perp y) \star z = (x \star z) \perp (y \star z) \quad (5.1)$$

Sarà **distributiva a sinistra** rispetto a \perp se per ogni terna $x, y, z \in S$ risulta:

$$x \star (y \perp z) = (x \star y) \perp (x \star z) \quad (5.2)$$

Quando \star è commutativa, allora le due condizioni sono equivalenti.

Esempio 5.1.6

1. In \mathbb{N} possiamo considerare le operazioni \cdot e $+$ che corrispondono alle operazioni usuali di moltiplicazioni e addizioni. Dalle proprietà dell'aritmetica sappiamo che vale la proprietà distributiva della moltiplicazione rispetto all'addizione:

$$\forall a, b, c \in \mathbb{N} (a \cdot (b + c) = a \cdot b + a \cdot c)$$

2. L'unione insiemistica è distributiva rispetto all'intersezione, e l'intersezione è distributiva rispetto all'unione. Inoltre l'intersezione è distributiva rispetto alla differenza simmetrica.

Definizione 5.1.5: Operazione opposta

Sia $* : S \times S \rightarrow S$ una operazione binaria in S . È possibile considerare l'**operazione opposta** $*^*$ definita ponendo:

$$\forall a, b \in S (a *^* b = b * a) \quad (5.3)$$

L'operazione opposta ha le stesse proprietà dell'operazione iniziale. Riferendosi alla rappresentazione grafica delle tavole di Cayley, calcolare l'operazione opposta significa ribaltare la tavola rispetto a righe e colonne.

Osservazione 5.1.2



Una operazione è commutativa se e solo se essa coincide con la propria operazione opposta.



5.2.1 ■ Semigruppi

Definizione 5.2.1: Struttura algebrica

Sia S un insieme non vuoto e siano \perp_1, \dots, \perp_n n operazioni in S . La $n+1$ -pla $(S, \perp_1, \dots, \perp_n)$ si chiama **struttura algebrica** e l'insieme S si chiama **sostegno** di tale struttura.

Definizione 5.2.2: Semigruppo

Una struttura algebrica ad una operazione interna (S, \perp) si dice **semigruppo** se l'operazione \perp è associativa. Un semigruppo (S, \perp) si dice **commutativo** o **abeliano** se l'operazione \perp è anche commutativa.

Esempio 5.2.1

1. Gli insiemi $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ con l'usuale operazione somma sono tutti semigruppi. Analogamente se invece della somma consideriamo il prodotto.
2. Sia A un insieme, sia A^A l'insieme delle funzioni $f : A \rightarrow A$ e sia \circ la composizione di funzioni. Possiamo considerare la composizione come un'operazione su A^A :

$$\circ : (f, g) \in A^A \times A^A \mapsto f \circ g \in A^A$$

Dato che \circ è associativa la struttura (A^A, \circ) è un semigruppo.

3. Consideriamo \mathbb{Z} e la funzione $- : \mathbb{Z} \times \mathbb{Z} : (a, b) \mapsto a - b$. La funzione $-$ è un'operazione, ma non è associativa. Infatti è possibile trovare almeno una terna $a, b, c \in \mathbb{Z}$ per cui $a - (b - c) \neq (a - b) - c$. Per esempio $a = 4, b = -2, c = 8$:

$$(4 - (-2)) - 8 = -2 \neq 10 = 4 - (-2 - 8)$$

Quindi l'operazione $-$ non dà su \mathbb{Z} la struttura di semigruppo.

4. Su $\mathbb{R} \times \mathbb{R}$ definiamo $(a, b) * (c, d) = (ac, ad + b)$. $(\mathbb{R} \times \mathbb{R}, *)$ è un semigruppo. Infatti:

$$\begin{aligned} \forall (a, b), (c, d), (e, f) \in \mathbb{R} \times \mathbb{R} & ((a, b) * ((c, d) * (e, f))) = (a, b) * (ce, cf + d) \\ & = (ace, acf + ad + b) \\ & = (ac, ad + b) * (e, f) \\ & = ((a, b) * (c, d)) * (e, f) \end{aligned}$$

Definizione 5.2.3: Parte stabile e operazione indotta

Sia $\perp : S \times S \longrightarrow S$ un'operazione nell'insieme non vuoto S . Una parte non vuota X di S si dice **stabile** o **chiusa** rispetto a \perp se per ogni coppia (x, y) di elementi di X anche il composto $x \perp y$ appartiene a X . In questo caso l'applicazione

$$\perp_X : (x, y) \in X \times X \longmapsto x \perp y \in X$$

è un'operazione in X , che si dice **indotta** da \perp su X .

Esempio 5.2.2

Consideriamo la struttura $(\mathbb{Z}, -)$, chiaramente $\mathbb{N} \subseteq \mathbb{Z}$ non è chiusa rispetto alla sottrazione.

Definizione 5.2.4: Sottostruttura algebrica

Sia $(S, \perp_1, \dots, \perp_n)$ una struttura algebrica, e sia X una parte non vuota di S che sia stabile rispetto a ciascuna delle operazioni \perp_1, \dots, \perp_n . La struttura algebrica $(X, \perp_1, \dots, \perp_n)$ si dice **sottostruttura** di $(S, \perp_1, \dots, \perp_n)$.

Definizione 5.2.5: Potenze in un semigruppo

Se (S, \perp) è un semigruppo, possiamo definire le **potenze** di un elemento $a \in S$ mediante l'induzione:

$$\begin{cases} a^n = a & \text{se } n=1 \\ a^{n+1} = a^n \perp a & \text{se } n \geq 1 \end{cases} \quad (5.4)$$

Proposizione 5.2.1

Sia (S, \perp) un semigruppo. Se $a \in S$ e $m, n \in \mathbb{Z}^+$, allora:

$$a^n \perp a^m = a^{n+m} \quad (5.5)$$

$$(a^n)^m = a^{nm} \quad (5.6)$$

Dimostrazione. Dimostriamo per induzione su m che $a^n \perp a^m = a^{n+m}$. Se $m = 1$, si ha $a^n \perp a^1 = a^n \perp a = a^{n+1}$ per come abbiamo definito la potenza. Supponiamo che la proprietà sia vera per un certo m , ossia che valga $a^n \perp a^m = a^{n+m}$, e dimostriamo che allora vale la proprietà anche per l'intero successivo $m + 1$, ossia che si ha $a^n \perp a^{m+1} = a^{n+m+1}$. Si hanno le uguaglianze:

$$\begin{aligned} a^n \perp a^{m+1} &= a^n \perp (a^m \perp a) && (\text{Per definizione di potenza}) \\ &= (a^n \perp a^m) \perp a && (\text{Per l'associatività di } \perp) \\ &= (a^{n+m}) \perp a && (\text{Per ipotesi induttiva}) \\ &= a^{n+m+1} && (\text{Per definizione di potenza}) \end{aligned}$$

Dimostriamo ora per induzione su m che $(a^n)^m = a^{nm}$. Per $m = 1$, $(a^n)^1 = a^n = a^{n \cdot 1}$. Supponiamo ora che sia vero che $(a^n)^m = a^{nm}$ e otteniamo la catena di uguaglianze:

$$\begin{aligned} (a^n)^{m+1} &= (a^n)^m \perp (a^n)^1 && (\text{Per definizione di potenza}) \\ &= (a^n)^m \perp a^n && (\text{Per ipotesi induttiva}) \\ &= a^{nm} \perp a^n \\ &= a^{nm+n} && (\text{Per la proprietà precedente}) \\ &= a^{n(m+1)} && (\text{Mettendo } n \text{ in evidenza}) \end{aligned}$$

□

Quando l'operazione che si considera è l'addizione tra elementi, il concetto di potenza si traduce nel concetto di *multiplo*.

Definizione 5.2.6: Multiplo

Sia $(S, +)$ un semigruppo denotato additivamente e sia $a \in S$. Qualsiasi sia $n \in \mathbb{N}^+$ si ha:

$$na = \underbrace{a + a + \dots + a}_{n \text{ volte}} \quad (5.7)$$

ed na prende il nome di **multiplo** di a .

5.2.2 I monoidi

Definizione 5.2.7: Elemento neutro

Sia (S, \perp) una struttura algebrica ad una operazione interna. Un elemento u di S si chiama **elemento neutro a sinistra** se risulta

$$\forall x \in S \quad u \perp x = x \quad (5.8)$$

Si dice invece che u è **neutro a destra** se

$$\forall x \in S \quad x \perp u = x \quad (5.9)$$

u è **elemento neutro** se è neutro sia a sinistra che a destra, cioè se risulta

$$\forall x \in S \quad x \perp u = u \perp x = x \quad (5.10)$$

La struttura (S, \perp) si dice **unitaria** se è dotata di elemento neutro e si indica con (S, \perp, u) . Quando la struttura (S, \perp) è commutativa le tre definizioni coincidono.

Definizione 5.2.8: Monoide

Sia S un insieme e \perp un'operazione su S . Si dice che (S, \perp) è un **monoide** se \perp è associativa ed esiste l'elemento neutro. In altre parole un monoide (S, \perp) è un semigruppo unitario. Spesso, per i monoidi, si usa la notazione (S, \perp, u) .

Esempio 5.2.3

1. Gli insiemi \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} con l'usuale operazione $+$ sono tutti monoidi, l'elemento neutro è sempre 0. Analogamente se invece della somma consideriamo il prodotto, abbiamo struttura di monoide per tutti gli insiemi sopra citati, con elemento neutro 1.
2. Sia $Rel(a)$ l'insieme delle relazioni binarie nell'insieme a . Allora l'insieme $(Rel(a), \cdot, id_a)$ è un monoide, anche detto **monoide delle relazioni binarie** in a . Per quanto visto nell'Osservazione 3.2.3, il monoide non è abeliano in quanto il prodotto relazionale non è una operazione commutativa.
Inoltre, poiché la composizione di due relazioni binarie risulta ancora una relazione binaria, l'insieme $Map(a, a)$ delle applicazioni sull'insieme a , detto anche **insieme delle trasformazioni** e indicato anche con $T(a)$ o anche a^a , è una parte stabile del monoide delle relazioni binarie, in particolare ne è un **sottomonoide**^a.
3. Consideriamo \mathbb{Z} e l'operazione \star definita ponendo:

$$a \star b := ab - a - b + 2$$

Verifichiamo se (\mathbb{Z}, \star) è un semigruppo. Prendo a, b, c in \mathbb{Z} :

$$\begin{aligned} a \star (b \star c) &= a \star (bc - b - c + 2) \\ &= (abc - ab - ac + 2a) - a - (bc - b - c + 2) + 2 \\ &= abc - ab - ac - bc + a + b + c \\ (a \star b) \star c &= (ab - a - b + 2) \star c \\ &= (abc - ac - bc + 2c) - (ab - a - b + 2) - c + 2 \\ &= abc - ab - ac - bc + a + b + c \end{aligned}$$

Quindi \star è associativa e (\mathbb{Z}, \star) è un semigruppo. Verifichiamo se esiste un elemento neutro e rispetto all'operazione \star . Cerchiamo $e \in \mathbb{Z}$ tale che $e \star a = a \star e = a \quad \forall a \in \mathbb{Z}$.

$$a \star e = ae - a - e + 2 = a \Rightarrow (e - 2)a + (e - 2) = 0 \Rightarrow e = 2$$

L'elemento neutro esiste ed è 2. Quindi (\mathbb{Z}, \star) è un monoide.

4. Si consideri l'operazione di elevamento a potenza nell'insieme dei numeri reali munito dell'operazione di moltiplicazione:

$$\forall (a, b) \in \mathbb{R} \quad a^b = \begin{cases} 1 & \text{se } b = 0 \\ \underbrace{a \cdot a \cdot \dots \cdot a}_{b \text{ volte}} & \text{se } b > 0 \end{cases}$$

L'elemento $1 \in \mathbb{R}$ risulta neutro a destro in quanto $\forall a \in \mathbb{R}(a^1 = a)$, ma non neutro a sinistra dato che: $\forall a \in \mathbb{R}(1^a = 1)$.

5. Si consideri l'insieme $s = \{a, b\}$ e il suo insieme delle parti $\mathcal{P}(s) = \{\emptyset, \{a\}, \{b\}, s\}$ già visto in precedenza. Chiaramente la struttura $(\mathcal{P}(s), \cap, a)$ è un monoide in quanto \cap risulta essere una operazione associativa e s risulta neutro rispetto a tale operazione. Infatti, per ogni $x \in \mathcal{P}(s)$ si ha $x \cap s = x$. La proprietà di essere elemento neutro è facilmente osservabile all'interno di una tavola di Cayley. Infatti, se un determinato elemento t è elemento neutro a sinistra, allora la sua riga corrispondente conterrà l'intestazione della colonna corrispondente. Viceversa a destra.

\cap	\emptyset	$\{a\}$	$\{b\}$	s
\emptyset	\emptyset	\emptyset	\emptyset	\emptyset
$\{a\}$	\emptyset	$\{a\}$	\emptyset	$\{a\}$
$\{b\}$	\emptyset	\emptyset	$\{b\}$	$\{b\}$
s	\emptyset	$\{a\}$	$\{b\}$	s

^aIl più importante monoide non commutativo.

Definizione 5.2.9: Alfabeto

Sia A un insieme, che chiamiamo **alfabeto**. Chiamiamo **parola nell'alfabeto** A una qualsiasi sequenza $a_1 a_2 \dots a_n$ di elementi $a_i \in A$ (ed anche la parola vuota, sequenza di 0 simboli).

Esempio 5.2.4

Sia $A = \{0, 1, 2, \dots, 15\}$. Alcune parole nell'alfabeto A sono ad esempio: "1 5 15", "4 4 4 3 4 5", "6".

Definizione 5.2.10: Insieme delle parole

Per ogni $n \geq 0$, definiamo W_n come l'insieme delle parole w nell'alfabeto A formate esattamente da n elementi di A :

$$W_n := \{w = a_1a_2\dots a_n \mid a_i \in A\} \quad (5.11)$$

Per $n = 0$, W_0 contiene un solo elemento, la **parola vuota** w_0 che non contiene nessun elemento di A . Invece $W_1 = A$. L'insieme $W_A = \bigcup_{n \in \mathbb{N}} W_n$ è l'**insieme delle parole** dell'alfabeto A .

Definiamo un'operazione su W_A : siano $w_1 = a_1a_2\dots a_n$ e $w_2 = b_1b_2\dots b_m$ due parole di W_A e sia

$$\circ := W_A \times W_A \longrightarrow W_A$$

definita ponendo:

$$w_1 \circ w_2 = a_1\dots a_n b_1\dots b_m \quad (5.12)$$

$w_1 \circ w_2$ è una parola di W_A e \circ è un'operazione, quindi (W_A, \circ) è una struttura algebrica. Chiamiamo \circ operazione di **concatenazione**.

Proposizione 5.2.2

(W_A, \circ) è un monoide.

Dimostrazione. Dobbiamo dimostrare che \circ è associativa ed esiste l'elemento neutro. Per l'associatività è sufficiente osservare che se $w_1 = a_1\dots a_n$, $w_2 = b_1\dots b_m$ e $w_3 = c_1\dots c_l$ allora

$$\begin{aligned} (w_1 \circ w_2) \circ w_3 &= (a_1a_2\dots a_n b_1b_2\dots b_m) \circ w_3 \\ &= a_1a_2\dots a_n b_1b_2\dots b_m c_1c_2\dots c_l \\ w_1 \circ (w_2 \circ w_3) &= w_1 \circ (b_1b_2\dots b_m c_1c_2\dots c_l) \\ &= a_1a_2\dots a_n b_1b_2\dots b_m c_1c_2\dots c_l \end{aligned}$$

Inoltre l'elemento neutro rispetto a \circ esiste, ed è la parola vuota w_0 . □

Osservazione 5.2.1

Banalmente \circ non è commutativo, quindi (W_A, \circ, w_0) è un esempio di monoide non commutativo.

Teorema 5.2.1 (Unicità dell'elemento neutro)

Sia (S, \perp) una struttura algebrica ad una operazione e siano u un elemento neutro a sinistra di S e u' un elemento neutro a destra di S . Risulta allora $u = u'$. Inoltre, se u è l'unico elemento neutro a sinistra in (S, \perp) e l'unico elemento neutro a destra in (S, \perp) allora sarà l'unico elemento neutro in (S, \perp) .

Dimostrazione. Poiché u è neutro a sinistra ed u' neutro a destra, si ha:

$$u' = u \perp u' = u$$

Per dimostrare che u è unico consideriamo un elemento $t \in S$ neutro a sinistra rispetto a \perp . Allora, per la prima parte della dimostrazione si ha necessariamente: $t = u'$ e dunque: $t = u$. □



Il teorema garantisce l'**unicità dell'elemento neutro** (se questo esiste) ma non nega il fatto che *possano esistere più di un elemento neutro a sinistra o a destra* (a condizione che nell'altro senso non ce ne siano).

Esempio 5.2.5

Si consideri ad esempio l'operazione:

$$*: (a, b) \in S \times S \mapsto a \in S$$

nota come **proiezione** in S della prima componente. La struttura $(S, *)$ è associativa. Infatti:

$$\forall a, b, c \in S \quad a * (b * c) = (a * b) * c$$

In $(S, *)$ vale dunque la proprietà:

$$\forall t \in S \quad (a * t) = a$$

dunque t è neutro a destra rispetto a $*$. Ogni elemento di S risulta essere quindi un elemento neutro a destra.

5.2.3 ■ Elementi simmetrizzabili

Definizione 5.2.11: Elemento simmetrico

Sia (S, \perp) una struttura algebrica dotata di elemento neutro u . Un elemento x di S si dice **simmetrizzabile a sinistra** se esiste x' in S tale che

$$x' \perp x = u \tag{5.13}$$

e l'elemento x' si chiama **simmetrico sinistro**. Analogamente, x si dice **simmetrizzabile a destra** se esiste x'' di S tale che

$$x \perp x'' = u \tag{5.14}$$

e in tal caso l'elemento x'' si chiama **simmetrico destro** di x . L'elemento x si dice **simmetrizzabile** se esiste un elemento x' di S che sia simmetrico sinistro e destro di x , cioè tale che

$$x' \perp x = x \perp x' = u \tag{5.15}$$

L'elemento x' si dice allora un **simmetrico** di x . Ovviamente, se l'elemento x è simmetrizzabile e x' è un suo simmetrico, anche x' è simmetrizzabile, e x è un simmetrico di x' .

Se (S, \perp) è un semigruppo dotato di elemento neutro e x è un elemento simmetrizzabile di S , l'unico simmetrico di x sarà denotato con x' . Se l'operazione nel semigruppo S è denotata moltiplicativamente, un elemento simmetrizzabile di S si dice **invertibile**, e il suo simmetrico si chiama **inverso** e si denota col simbolo x^{-1} . Se invece per l'operazione del semigruppo si usa la notazione additiva e x è un elemento simmetrizzabile di S , il simmetrico di x si chiama **opposto** e si denota col simbolo $-x$.

Esempio 5.2.6

In (\mathbb{Z}, \cdot) gli unici elementi ad avere simmetrico sono 1 e -1 . Infatti $1 \cdot 1 = 1 = -1 \cdot (-1)$ e si dimostra che per ogni $a \in \mathbb{Z} \setminus \{\pm 1\}$ non esiste a^{-1} tale che $a \cdot a^{-1} = 1$. In $(\mathbb{Z}, +)$ ogni elemento $n \in \mathbb{Z}$ ha simmetrico, che si indica con il simbolo $-n$.

Definizione 5.2.12: Insieme dei simmetrizzabili

Dato il monoide (S, \perp, u) , si denota con \mathcal{U} l'**insieme degli elementi simmetrizzabili** di S rispetto a \perp .

Esempio 5.2.7

Ad esempio, se consideriamo il monoide dei numeri reali con l'operazione moltiplicazione si ha:

$$\mathcal{U}(\mathbb{R}, \times, 1) = \mathbb{R} \setminus \{0\}$$

mentre: $\mathcal{U}(\mathcal{P}(A), \cup, \emptyset) = \{\emptyset\}$ e $\mathcal{U}(\mathcal{P}(A), \cap, A) = \{A\}$.

Proposizione 5.2.3

Sia (S, \perp, u) un monoide, e sia x un elemento di S per il quale esistano un simmetrico sinistro x' e un simmetrico destro x'' . Allora $x' = x''$ e quindi x è simmetrizzabile. In particolare, un elemento simmetrizzabile di S è dotato di un unico simmetrico.

Dimostrazione. Poiché l'operazione \perp è associativa, risulta:

$$x' = x' \perp u = x' \perp (x \perp x'') = (x' \perp x) \perp x'' = u \perp x'' = x''$$

il che dimostra l'enunciato. \square

Proposizione 5.2.4

Sia (S, \perp, u) un monoide, e siano x, y elementi simmetrizzabili di S . Allora $x \perp y$ è simmetrizzabile e risulta:

$$(x \perp y)' = y' \perp x' \quad (5.16)$$

Dimostrazione. Si ha:

$$(x \perp y) \perp (y' \perp x') = x \perp (y \perp y') \perp x' = x \perp u \perp x' = x \perp x' = u$$

e similmente $(y' \perp x') \perp (x \perp y) = u$. Pertanto $x \perp y$ è simmetrizzabile, e $y' \perp x'$ è il suo simmetrico. \square

Osservazione 5.2.2



Dalla Proposizione 5.2.4 segue che, se (S, \perp) è un semigruppo dotato di elemento neutro, l'insieme $\mathcal{U}(S)$ degli elementi simmetrizzabili di S è una parte stabile.

In sintesi, un elemento $x \in (S, \perp, u)$ è:

$$\begin{aligned} \text{Simmetrizzabile a sinistra} &\iff \exists x' \in S (x' \perp x = u) \\ \text{Simmetrizzabile a destra} &\iff \exists x' \in S (x \perp x' = u) \\ \text{Simmetrizzabile} &\iff \exists x' \in S (x \perp x' = x' \perp x = u) \end{aligned}$$

5.2.4 ■ Elementi cancellabili

Definizione 5.2.13: Traslazioni

Sia (S, \perp) una struttura algebrica ad una operazione interna, e sia $a \in S$. È allora possibile considerare le applicazioni:

$$\sigma_a : x \in S \mapsto a \perp x \in S \quad \text{e} \quad \delta_a : x \in S \mapsto x \perp a \in S$$

che si chiamano rispettivamente **traslazione sinistra** e **traslazione destra** di S di **ampiezza** a .

Definizione 5.2.14: Elementi cancellabili

Sia (S, \perp) una struttura algebrica ad una operazione interna. Un elemento $a \in S$ si dice **cancellabile a sinistra** se vale

$$\forall x, y \in S (a \perp x = a \perp y \Rightarrow x = y) \quad (5.17)$$

ovvero se la traslazione sinistra σ_a è una applicazione iniettiva.

Si dice che a è **cancellabile a destra** se:

$$\forall x, y \in S (x \perp a = y \perp a \Rightarrow x = y) \quad (5.18)$$

Ovvero se la traslazione destra δ_a è una funzione iniettiva. L'elemento si dice **regolare o cancellabile** se è cancellabile sia a sinistra che a destra, ovvero se entrambe le traslazioni σ_a e δ_a risultano iniettive. (S, \perp) si dice **regolare** se ogni suo elemento è regolare. In questo caso si dice anche che nella struttura algebrica (S, \perp) vale la **legge di cancellazione**.

Esempio 5.2.8

Rispetto all'operazione $+$ in \mathbb{Z} tutti gli elementi sono cancellabili. Infatti, qualsiasi elemento $a \in \mathbb{Z}$ si ha:

$$\forall x, y \in \mathbb{Z} (a + x = a + y \Rightarrow x = y)$$

Esempio 5.2.9

In (\mathbb{Z}, \cdot) tutti gli elementi sono cancellabili tranne il numero zero. Infatti un numero $a \in S$ non è cancellabile a sinistra in $(S, *)$ se e soltanto se esistono due elementi $x, y \in S$ tali che:

$$a * x = a * y \wedge x \neq y$$

e nel caso di $0 \in \mathbb{Z}$ si ha ad esempio, presi due qualsiasi elementi a, b diversi tra loro:

$$0 \cdot a = 0 = 0 \cdot b$$

Quindi 0 non è cancellabile.

Preso un insieme finito $A = \{1, 2, \dots, i, j, \dots, n\}$ è possibile interpretare la cancellabilità in una struttura (A, \perp) osservando la tavola di Cayley. Infatti, osservando la tabella 5.1 si può notare che ciascuna cella può essere vista come una traslazione sinistra dell'elemento della colonna determinata dall'elemento della riga corrispondente, oppure una traslazione destra dell'elemento della riga determinata dall'elemento della colonna corrispondente.

\perp	1	2	\dots	i	j	\dots	n
1	$1 \perp 1$	$1 \perp 2$	\dots	$1 \perp i$	$1 \perp j$	\dots	$1 \perp n$
2	$2 \perp 1$	$2 \perp 2$	\dots	$2 \perp i$	$2 \perp j$	\dots	$2 \perp n$
\vdots	\dots	\dots	\dots	\dots	\dots	\dots	\dots
i	$i \perp 1$	$i \perp 2$	\dots	$i \perp i$	$\sigma_i(j) = i \perp j = \delta_j(i)$	\dots	$i \perp n$
j	$j \perp 1$	$j \perp 2$	\dots	$j \perp i$	$j \perp j$	\dots	$j \perp n$
\vdots	\dots	\dots	\dots	\dots	\dots	\dots	\dots
n	$n \perp 1$	$n \perp 2$	\dots	$n \perp i$	$n \perp j$	\dots	$n \perp n$

Tabella 5.1

Quindi, se si notano ripetizioni sulla stessa riga, sia questa ad esempio quella dell'elemento a , vuol dire che l'applicazione σ_a non è iniettiva e che l'elemento a non è cancellabile a sinistra. Analogamente, se si notano ripetizioni sulla stessa colonna, sia questa ad esempio a , vorrà dire che l'applicazione δ_a non è iniettiva e che quindi l'elemento a non è cancellabile a destra.

Esempio 5.2.10

Sia A un insieme non vuoto e consideriamo la struttura algebrica $(\mathcal{P}(A), \setminus)$, dove con \setminus si intende la differenza insiemistica. Quali sono gli elementi cancellabili a sinistra e a destra in questa struttura? Per definizione di elemento cancellabile a sinistra, un elemento $x \in \mathcal{P}(A)$ deve soddisfare alla seguente condizione:

$$\forall a, b \in \mathcal{P}(A) (x \setminus a = x \setminus b \Rightarrow a = b)$$

È immediato osservare che la funzione:

$$x \in \mathcal{P}(A) \mapsto A \setminus x \in \mathcal{P}(A)$$

è iniettiva. Infatti, se $A \setminus x = A \setminus b$, qualsiasi siano le parti a, b di A allora deve essere per forza $a = b$. Quindi l'insieme A è cancellabile a sinistra. Analogamente, la funzione:

$$x \in \mathcal{P}(A) \mapsto x \setminus \emptyset \in \mathcal{P}(A)$$

è chiaramente iniettiva e l'insieme vuoto risulta cancellabile a destra. Come si fa a dimostrare se ce ne sono altri di elementi cancellabili? A ipoteticamente potrebbe essere infinito quindi risulta difficile verificare le proprietà di cancellabilità per ciascun elemento. Per questo motivo bisogna sfruttare le proprietà dei quantificatori. Infatti, negando ad esempio l'equazione 5.17 si ottiene che un elemento $x \in \mathcal{P}(A)$ **non è cancellabile** se e soltanto se:

$$\exists b, c \in \mathcal{P}(A) ((x \setminus b = x \setminus c) \wedge (b \neq c))$$

La prova della cancellabilità di un elemento si riduce così nella ricerca di almeno un controsenso che soddisfa la formula appena descritta. Si ha infatti, ponendo: $b = \emptyset$ e $c = A \setminus x$ si ottiene:

$$\begin{aligned} x \setminus b &= x \setminus \emptyset = x \\ x \setminus c &= x \setminus A \setminus x = x \end{aligned}$$

Ma $b \neq c$ e quindi si ha che ogni parte $x \in \mathcal{P}(A)$ non è cancellabile a sinistra.

Teorema 5.2.2 (degli elementi cancellabili)

Sia (S, \perp, u) un monoide e sia $a \in S$. Valgono allora le seguenti implicazioni:

1. Se a simmetrizzabile a sinistra rispetto a \perp allora a è cancellabile a sinistra rispetto a \perp ;
2. Se a simmetrizzabile a destra rispetto a \perp allora a è cancellabile a destra rispetto a \perp ;
3. Se a simmetrizzabile rispetto a \perp allora a è cancellabile rispetto a \perp ;

Dimostrazione. Dimostriamo la prima implicazione. Siano quindi x e y elementi di S tali che

$$a \perp x = a \perp y$$

Si ha allora:

$$\begin{aligned} x &= u \perp x && \text{Per definizione di elemento neutro} \\ &= (a' \perp a) \perp x && \text{Per definizione di elemento simmetrizzabile} \\ &= a' \perp (a \perp x) && \text{Per associatività} \\ &= a' \perp (a \perp y) && \text{Per ipotesi} \\ &= (a' \perp a) \perp y = u \perp y = y \end{aligned}$$

e quindi a è cancellabile a sinistra. Un ragionamento analogo prova che a è cancellabile a destra, e quindi cancellabile. \square

! Attenzione, non vale il contrario. Un elemento può essere cancellabile ma non simmetrizzabile. Il viceversa **vale solo nei monoidi finiti**.

Esempio 5.2.11

Nel monoide infinito $(\mathbb{Z}, \cdot, 1)$ gli unici elementi simmetrizzabili sono ± 1 ma 3 ad esempio è un elemento cancellabile.

In sintesi, un elemento $a \in (S, \perp, u)$ è:

Cancellabile a sinistra	\iff	$\forall x, y \in S(a \perp x = a \perp y \implies x = y)$
Cancellabile a destra	\iff	$\forall x, y \in S(x \perp a = y \perp a \implies x = y)$
Cancellabile	\iff	è cancellabile sia destra che a sinistra.
Simmetrizzabile	\implies	Cancellabile

5.3

GRUPPI



Definizione 5.3.1: Gruppo

Siano G un insieme e \perp un'operazione in G . Diremo che (G, \perp) è un **gruppo** se:

1. L'operazione \perp è associativa: $\forall a, b, c \in G((a \perp (b \perp c)) = (a \perp b) \perp c))$;
2. Esiste un elemento $e \in G$, detto **identità** o **elemento neutro** tale che $\forall x \in G(a \perp e = e \perp a = a)$;
3. Ogni elemento ha l'inverso, ossia $\forall a \in G(\exists b \in G(a \perp b = b \perp a = e))$.

Un gruppo (G, \perp) si dice **gruppo abeliano** se l'operazione \perp è anche commutativa, assia $\forall a, b \in A$ si ha $a \perp b = b \perp a$.

Osservazione 5.3.1



Un gruppo altro non è che *un monoide in cui ogni elemento è invertibile*.

Salvo avviso contrario, l'operazione in un gruppo sarà denotata *moltiplicativamente*. In notazione moltiplicativa, l'elemento neutro di un gruppo viene denotato col simbolo 1 e detto **unità** di G , il simmetrico di un elemento $x \in G$ è chiamato **inverso** di x e denotato col simbolo x^{-1} . In notazione additiva il simbolo per l'elemento neutro è 0 , se $(G, +)$ è un monoide commutativo, un elemento $a \in G$ è invertibile se esiste $b \in G$ tale che $a + b = 0$, in tal caso si scrive $b = -a$ (invece di $b = a^{-1}$) e $-a$ si chiama **opposto** di a .

Esempio 5.3.1

- Il semigruppo A^A delle trasformazioni $f : A \rightarrow A$ non è un gruppo se $|A| \geq 2$, poiché ad esempio le funzioni costanti non hanno inverso. Se infatti $a, b \in A$ sono due elementi diversi e indichiamo con c_a la funzione costante data da $\forall x \in A (c_a(x) = a)$, allora la composizione $c_a \circ g$ di una qualsiasi funzione $g \in T(A)$ con c_a , coincide con c_a ed è quindi diversa da id_A : si ha ad esempio $c_a(b) = a \neq id_A(b) = b$.
- Si consideri il monoide $(\mathcal{P}(A), \Delta, \emptyset)$. Si ha:

$$\forall x \in \mathcal{P}(A) (x \Delta x = \emptyset)$$

Quindi x è il simmetrico di sé stesso. Quindi, se due insiemi $a, b \in \mathcal{P}(A)$ determinano $a \Delta b = \emptyset$ allora deve essere necessariamente $a = b$. In particolare $(\mathcal{P}(A), \Delta, \emptyset)$ è un gruppo.

Osservazione 5.3.2



Se (S, \perp) è un semigruppo dotato di elemento neutro e $\mathcal{U}(S)$ è l'insieme dei suoi elementi simmetrizzabili allora (\mathcal{U}, \perp) è un gruppo, chiamato **gruppo degli invertibili**.

Definizione 5.3.2: Potenza

Sia G un gruppo e sia $g \in G$ e $n \in \mathbb{Z}$. La **potenza** n -esima g^n di g si definisce nella maniera seguente:

$$\begin{cases} \text{se } n = 0 & g^0 = 1_G \\ \text{se } n > 0 & g^n \text{ è la potenza di } g \text{ che abbiamo definito nei semigruppi} \\ \text{se } n < 0 \text{ ossia } n = -m \text{ con } m \text{ positivo} & g^n = (g^{-1})^m \end{cases} \quad (5.19)$$

Le proprietà delle potenze che abbiamo dimostrato nei semigruppi relativamente al caso degli esponenti positivi valgono nel caso dei gruppi anche per gli esponenti minori o uguali a 0 e si estendono a proprietà che riguardano gli inversi.

Proposizione 5.3.1

Sia G un gruppo, $g \in G$ e siano $n, m \in \mathbb{Z}$. Allora:

$$g^{n+m} = g^n g^m \quad (5.20)$$

$$g^{nm} = (g^n)^m \quad (5.21)$$

$$(g^m)^{-1} = g^{-m} \quad (5.22)$$

Proposizione 5.3.2

Sia G un gruppo denotato additivamente, $a \in G$ e siano $n, m \in \mathbb{Z}$. Allora:

$$(n + m)a = na + ma \quad (5.23)$$

$$(nm)a = n(ma) \quad (5.24)$$

Osservazione 5.3.3



Nel gruppo abeliano $(\mathbb{Z}, +)$ qualunque siano gli elementi m, n il multiplo di m secondo n coincide con il multiplo di n secondo m , ovvero il prodotto nm . L'**insieme dei multipli** di un elemento n è denotato con il simbolo $n\mathbb{Z}$.

5.3.1 ■ Sottogruppi di un gruppo

Definizione 5.3.3: Sottogruppo

Sia (G, \perp) un gruppo e sia H una parte stabile di G . H si dice un **sottogruppo** di G se la sottostruttura (H, \perp) è un gruppo. Se H è un sottogruppo di un gruppo G si usa indicarlo con la notazione $H \leq G$.

Esempio 5.3.2

- Qualunque sia il gruppo G , i sottoinsiemi G e $\{1\}$ sono evidentemente sottogruppi di G , chiamati **sottogruppi banali** di G . In particolare, $\{1\}$ si dice **sottogruppo identico** di G , mentre i sottogruppi di G diversi da G si dicono **sottogruppi propri** di G . È inoltre chiaro che, se H è un sottogruppo di G , i sottogruppi di H sono precisamente i sottogruppi di G contenuti in H .
- L'insieme \mathbb{Z} è un sottogruppo di $(\mathbb{Q}, +)$, mentre $\{1, -1\}$ è un sottogruppo di $(\mathbb{Q} \setminus \{0\}, \cdot)$.

Lemma 5.3.1

Sia G un gruppo, e sia H un sottogruppo di G . Allora:

- L'elemento neutro di H coincide con l'unità di G
- Se h è un elemento di H , il simmetrico di h in H coincide con l'inverso di h in G .

Dimostrazione. (1) Se u è l'elemento neutro di H , risulta $uu = u = u1$, e quindi $u = 1$ per la legge di cancellazione in G .

(2) Sia h' il simmetrico di h in H . Poiché l'elemento neutro di H è 1, si ha $h'h = 1 = h^{-1}h$ e quindi $h' = h^{-1}$. \square

Corollario 5.3.1

Sia G un gruppo. Una parte H di G è un sottogruppo se e solo se è stabile, contiene l'unità di G e l'inverso di ogni suo elemento.

Esempio 5.3.3

Consideriamo il gruppo abeliano $(\mathbb{Z}, +)$. Un suo sottogruppo è l'insieme dei multipli di n in \mathbb{Z} , ossia l'insieme $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$. Infatti, sommando due multipli di n si otterrà sempre un multiplo di n , inoltre $0 \in n\mathbb{Z}$ e vale $-n(-k) = n(-k) \in n\mathbb{Z}$.

Teorema 5.3.1 (caratterizzazione dei sottogruppi)

Sia G un gruppo. Una parte stabile non vuota H di G è un sottogruppo se e solo se per ogni coppia (x, y) di elementi di H anche il prodotto $x^{-1}y$ appartiene ad H .

Dimostrazione. Se H è un sottogruppo di G , e x e y sono elementi di H , anche x^{-1} appartiene ad H e quindi, essendo H stabile, si ha $x^{-1}y \in H$. Allo scopo di provare che la condizione dell'enunciato è anche sufficiente, sia x un elemento della parte non vuota H di G . Dall'ipotesi segue che $1 = x^{-1}x$ appartiene ad H . Allora anche $x^{-1} = x^{-1}1$ appartiene ad H . Siano infine x e y elementi di H . Risulta $xy = (x^{-1})^{-1}y$, per cui xy è in H , e H è un sottogruppo di G . \square

5.3.2 ■ Parti chiuse e generatori

Proposizione 5.3.3

Sia (S, \perp) un semigruppo e sia L un insieme di parti chiuse di S . Allora $\bigcap L$ è una parte chiusa di S .

Dimostrazione. Si ha infatti:

$$\forall x, y \in \bigcap L (\forall X \in L (x, y \in X \implies x \perp y \in X))$$

Quindi se si prendono due elementi di $\bigcap L$, anche il loro composto tramite \perp appartiene a tutti gli elementi di L , ovvero $x \perp y \in \bigcap L$. \square

Definizione 5.3.4: Sottostrutture generate

Data una struttura algebrica (s, \perp) e $t \subseteq s$ una sua parte, definiamo:

$$\langle t \rangle = \bigcap \{x \in \mathcal{P}(s) \mid t \subseteq x \wedge x \text{ è chiusa rispetto a } \perp\} \quad (5.25)$$

Ovvero l'intersezione delle sottostrutture di s che contengono t e diciamo che $\langle t \rangle$ è la **sottostruttura generata** da t .

Teorema 5.3.2 (Caratterizzazione delle sottostrutture generate da singleton)

Valgono le seguenti equivalenze:

1. Sia (S, \perp) un semigruppo e $x \in S$, la parte chiusa generata da $\{x\}$ è $\langle \{x\} \rangle = \{x^n \mid n \in \mathbb{N}^*\}$;
2. Sia (S, \perp) un monoide e $x \in S$, la parte chiusa generata da $\{x\}$ è $\langle \{x\} \rangle = \{x^n \mid n \in \mathbb{N}\}$;
3. Sia (S, \perp) un gruppo e $x \in S$, la parte chiusa generata da $\{x\}$ è $\langle \{x\} \rangle = \{x^n \mid n \in \mathbb{Z}\}$.

Osservazione 5.3.4

La ragione per cui la chiamiamo “generata” è che si può dimostrare che essa è in realtà l’insieme delle combinazioni lineari dell’insieme t . Per esempio, il sottomonoide generata da $\{2\} \subseteq (\mathbb{N}, +)$ è l’insieme di tutti i valori che si possono ottenere sommando due:

$$\langle 2 \rangle = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, \dots\}$$

5.3.3 ■ Il gruppo delle permutazioni

Definizione 5.3.5: Gruppo simmetrico

Consideriamo il monoide $(T(A), \circ, id_A)$, dove $T(A)$ è l’insieme delle trasformazioni in A . Chiaramente $(\mathcal{U}(T(A)), \circ)$ è un gruppo. I suoi elementi sono tutti e soli quelli del tipo:

$$\mathcal{U}(T(A)) = \{f \in T(A) \mid \exists g \in T(A)(f \circ g = g \circ f = id_A)\}$$

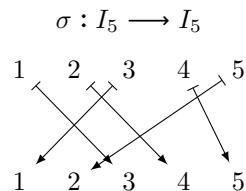
ovvero tutte le applicazioni biettive in $T(A)$, chiamate anche **permutazioni** di A . Tale gruppo è denotato col simbolo $Sym(A)$ ed è chiamato **gruppo simmetrico**:

$$Sym(A) = (\mathcal{U}(T(A)), \circ) \quad (5.26)$$

Fissiamo un numero intero positivo n . Denotiamo con I_n l’insieme dei numeri naturali $\{1, \dots, n\}$. L’insieme di tutte le permutazioni definite su I_n si denota col simbolo S_n .

Esempio 5.3.4

Consideriamo in S_5 la permutazione σ data da:



Per scrivere in modo veloce σ si usa una tabella costituita da due righe: nella prima sono elencati ordinatamente gli elementi di I_5 e al di sotto di ciascuno di essi, la seconda riga contiene le loro immagini. Otteniamo così la seguente tabella:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

Possiamo utilizzare una tabellina analoga a quella presentata nell’esempio per scrivere in modo sintetico qualsiasi permutazione. Nella prima riga elenchi gli elementi di I_n e al di sotto di ciascuno scriviamo la sua immagine:

$$\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

Esempio 5.3.5

Sia $A = \{a, b\}$ con $a \neq b$, in questo caso A^A avrà 4 elementi: $A^A = \{f \mid f : A \rightarrow A\} = \{id_A, c_a, c_b, \sigma\}$, con $\sigma : A \rightarrow A$ che mappa a in b e b in a . In questo caso l'insieme delle permutazioni di A è:

$$Sym(A) = \{id_A, \sigma\}$$

Esempio 5.3.6

Consideriamo in S_5 la permutazione σ dell'esempio 5.3.4 e la seguente permutazione τ :

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$$

Possiamo comporre σ e τ . Poiché la composizione di funzioni non è commutativa, eseguiamo entrambe le composizioni (ottenendo risultati diversi):

$$\begin{aligned} (\sigma \circ \tau)(1) &= \sigma(\tau(1)) = \sigma(1) = 3 \\ (\sigma \circ \tau)(2) &= \sigma(\tau(2)) = \sigma(3) = 1 \\ (\sigma \circ \tau)(3) &= \sigma(\tau(3)) = \sigma(4) = 5 \\ (\sigma \circ \tau)(4) &= \sigma(\tau(4)) = \sigma(5) = 2 \\ (\sigma \circ \tau)(5) &= \sigma(\tau(5)) = \sigma(2) = 4 \end{aligned}$$

Riassumendo con la scrittura tabellare:

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$$

Analogamente, possiamo calcolare $\tau \circ \sigma$, ottenendo:

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$$

Definizione 5.3.6: *K*-cicli e trasposizioni

Sia k un numero intero tale che $1 \leq k \leq n$. Si dice che una permutazione $f \in S_n$ è un ***k*-ciclo**, oppure un **ciclo di lunghezza *k*** se esistono elementi a due a due distinti $i_1, \dots, i_k \in I_n$ tali che:

$$f(i_1) = i_2, \quad f(i_2) = i_3, \quad \dots, \quad f(i_{k-1}) = i_k, \quad f(i_k) = i_1$$

e $f(j) = j$ per ogni $j \notin \{i_1, \dots, i_k\}$. In questo caso la permutazione f si denota col simbolo $(i_1 i_2 \dots i_k)$. Un ciclo di lunghezza 2 è chiamato **trasposizione**. Ovviamente l'unico ciclo di lunghezza 1 in S_n è la permutazione identica. Un ciclo si dice **non banale** se $k \geq 2$.

Esempio 5.3.7

In S_7 consideriamo la permutazione:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 1 & 3 & 6 & 5 & 7 \end{pmatrix}$$

Un elemento i si dice **fissato** dalla permutazione f quando $f(i) = i$, al contrario, se $f(i) \neq i$ si dice che i è **spostato** da f . Nel caso della permutazione α abbiamo che il primo elemento spostato è 1. Si ha così: $1 \rightarrow 2 \rightarrow 4 \rightarrow 3 \rightarrow 1$ che fornisce il 4-ciclo $\gamma_1 = (1 \ 2 \ 4 \ 3)$.

Esempio 5.3.8

In I_3 consideriamo le permutazioni:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

chiaramente α e β sono delle trasposizioni in quanto cicli di lunghezza 2: infatti α e β non fanno altro che **fissare** un elemento e scambiare di posto i restanti due. È facile osservare che: $\alpha \circ \alpha = id_{I_3} = \beta \circ \beta$. Calcolando le varie composte otteniamo:

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

che risultano essere due 3-cicli. Chiaramente $\alpha \circ \beta \neq \beta \circ \alpha$ e S_3 non risulta quindi un gruppo commutativo.

Teorema 5.3.3

Sia A un insieme non vuoto. Il gruppo simmetrico $Sym(A)$ è abeliano se e solo se A è finito e ha ordine al più 2.

Esempio 5.3.9

Se $S = \{1, 2, 3\}$ vale $S_3 = \{id_S, \alpha, \beta, \gamma, \delta, \epsilon\}$. La tavola di Cayley data calcolando la composizione delle varie permutazioni risulta:

\circ	id_S	α	β	γ	δ	ϵ
id_S	id_S	α	β	γ	δ	ϵ
α	α	β	id_S	δ	ϵ	γ
β	β	id_S	α	ϵ	γ	δ
γ	γ	ϵ	δ	id_S	β	α
δ	δ	γ	ϵ	α	id_S	β
ϵ	ϵ	δ	γ	β	α	id_S

s_i	id_S	α	β	γ	δ	ϵ
1	1	2	3	1	2	3
2	2	3	1	3	1	2
3	3	1	2	2	3	1

Osservando la tavola, vediamo che in ogni riga ed in ogni colonna ogni elemento del gruppo compare una ed una sola volta. Vale cioè la legge di cancellazione.

5.3.4 ■ Gruppi ciclici

Definizione 5.3.7: Gruppo ciclico

Sia (G, \cdot) un gruppo e a un suo elemento. Si dice **sottogruppo ciclico generato da a** e si denota con $\langle a \rangle$ il sottogruppo costituito dalle potenze di a con esponenti interi. L'elemento a è detto **generatore** di G . Diremo che G è **ciclico** se vi è un suo elemento tale che $G = \langle a \rangle$.

In notazione additiva, ossia se il gruppo è $(G, +)$ scriveremo: $G = \langle x \rangle = \{nx \mid n \in \mathbb{Z}\}$.

Osservazione 5.3.5



Poiché due qualunque potenze di uno stesso elemento di un gruppo sono permutabili, si ha anche subito che *ogni gruppo ciclico è abeliano*.

Esempio 5.3.10

- Nel gruppo delle permutazioni S_5 il sottogruppo ciclico generato dal ciclo $\sigma = (1\ 4\ 2)$ contiene 3 elementi, ed esattamente $\langle \sigma \rangle = \{1_{S_5} = \sigma^0, \sigma = \sigma^1, (1\ 2\ 4) = \sigma^2\}$. Infatti si può verificare che $\sigma^3 = 1_{S_5}$ e quindi tutte le potenze con esponenti interi positivi coincidono con uno dei tre elementi scritti. Inoltre da $\sigma^3 = 1_{S_5}$ si deduce anche che $\sigma^2 = \sigma^{-1}$ e quindi anche le potenze di σ con esponenti negativi coincidono con una delle tre potenze elencate.
- Il gruppo $(\mathbb{Z}, +)$ contiene oltre ai sottogruppi banali anche tanti altri sottogruppi ciclici. Per ogni $n \geq 0$ il sottoinsieme di \mathbb{Z} dei multipli interi di n :

$$n\mathbb{Z} := \{nt \mid t \in \mathbb{Z}\}$$

è un sottogruppo ciclico di $(\mathbb{Z}, +)$. Notiamo che $(\mathbb{Z}, +)$ stesso è un gruppo ciclico perché coincide con i sottogruppi ciclici generati da 1 e -1 :

$$(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$$

**Definizione 5.4.1: Omomorfismo**

Siano (S, \perp) e $(T, *)$ due strutture algebriche. Un'applicazione $f : S \rightarrow T$ si dice **omomorfismo** di S in T se e soltanto se:

$$\forall x, y \in S (f(x \perp y) = f(x) * f(y)) \quad (5.27)$$

Un omomorfismo di (S, \perp) in $(T, *)$ che sia iniettivo si dice **monomorfismo**; un omomorfismo suriettivo si dice **epimorfismo** mentre un omomorfismo biettivo si dice **isomorfismo**.

Esempio 5.4.1

- Si consideri la funzione $f : (\mathbb{Z}, +) \rightarrow (\mathbb{R}, \cdot)$ data da $f(a) = 2^a$. Possiamo verificare che f è un omomorfismo rispetto alle operazioni indicate. Infatti:

$$\forall a, b \in \mathbb{Z}, \quad f(a + b) = 2^{a+b} = 2^a \cdot 2^b = f(a) \cdot f(b)$$

- Sia $(S, *)$ il monoide delle parole in un alfabeto e sia $(T, \perp) = (\mathbb{N}, +)$. Un esempio di omomorfismo tra le due strutture è l'applicazione:

$$\lambda : S \rightarrow T$$

che ad ogni stringa associa la sua lunghezza. Infatti date due stringhe x, y si avrà che $\lambda(x * y)$ ovvero la lunghezza della stringa ottenuta dalla concatenazione di x e y è uguale a $\lambda(x) + \lambda(y)$, ovvero la somma delle lunghezze delle stringhe prese singolarmente.

Osservazione 5.4.1

Se esiste un isomorfismo di (S, \perp) in $(T, *)$, si dice che le strutture algebriche (S, \perp) e $(T, *)$ sono **isomorfe**^a e si usa la notazione: $(S, \perp) \simeq (T, *)$.

^aDal greco *isos*, che significa uguale, e *morfé*, che significa forma.

Proposizione 5.4.1

Siano (S, \perp) e $(T, *)$ strutture algebriche, e sia $f : S \rightarrow T$ un isomorfismo. Allora anche l'applicazione inversa $f^{-1} : T \rightarrow S$ è un isomorfismo.

Dimostrazione. Qualunque siano gli elementi z e w di T , esistono (e sono univocamente determinati) x e y in S tali che $f(x) = z$ e $f(y) = w$ e risulta:

$$\begin{aligned} f^{-1}(z * w) &= f^{-1}(f(x) * f(y)) \\ &= f^{-1}(f(x \perp y)) \\ &= x \perp y \\ &= f^{-1}(z) \perp f^{-1}(w) \end{aligned}$$

Pertanto f^{-1} è un isomorfismo di T in S . □

Gli omomorfismi risultano utilissimi da studiare in quanto **conservano le proprietà algebriche tra strutture**.

Proposizione 5.4.2

Se $f : S \rightarrow T$ è un epimorfismo tra le strutture (S, \perp) e $(T, *)$, se \perp è associativa allora $*$ è associativa. Analogamente, se \perp è commutativa allora $*$ è commutativa. Inoltre, qualsiasi sia l'elemento $x \in S$, se x è neutro, o neutro a sinistra o neutro a destra in (S, \perp) allora $f(x)$ ha la stessa proprietà in $(T, *)$. Infine, sia $x \in S$ simmetrizzabile a sinistra, sia $x' \in S$ un simmetrico sinistro allora $f(x')$ è simmetrico sinistro di $f(x)$ in $(T, *)$.

Dimostrazione. Sia \perp commutativa e $f : S \rightarrow T$ un epimorfismo. Allora, per ogni $a, b \in T$ esistono $x, y \in S$ tali che $a = f(x)$ e $b = f(y)$, quindi:

$$\begin{aligned} a \perp b &= f(x) * f(y) \\ &= f(x \perp y) \\ &= f(y \perp x) \\ &= f(y) * f(x) \\ &= b \perp a \end{aligned}$$

Sia invece \perp associativa, ed f un epimorfismo tra S e T , questo vuol dire che per ogni $x, y, z \in T$ esistono $a, b, c \in S$ tali che $a = f(x)$, $b = f(y)$ e $c = f(z)$. Dimostriamo che anche $*$ è associativa.

$$\begin{aligned} x * (y * c) &= f(a) * (f(b) * f(c)) && \text{(Per suriettività di } f\text{)} \\ &= f(a) * f(b \perp c) && \text{(Poiché } f\text{ è un epimorfismo)} \\ &= f(a \perp (b \perp c)) \\ &= f((a \perp b) \perp c) && \text{(Per associatività di } \perp\text{)} \\ &= f(a \perp c) * f(c) && \text{(Per definizione di omomorfismo)} \\ &= (f(a) * f(b)) * f(c) \\ &= (x * y) * z \end{aligned}$$

e l'operazione $*$ risulta associativa.

Sia x un elemento neutro a sinistra in (S, \perp) . Per la suriettività di f si ha: $\forall a \in T (\exists d \in S (a = f(d)))$. Quindi, preso un $a \in T$ si ha:

$$\begin{aligned} f(x) * a &= f(x) * f(d) \\ &= f(x \perp d) \\ &= f(d) \\ &= a \end{aligned}$$

e $f(x)$ risulta elemento neutro a sinistra rispetto a $*$ in T . □

Osservazione 5.4.2

Dalla proposizione appena dimostrata si ha quindi che gli epimorfismi conservano la commutatività, l'associatività, l'elemento neutro e gli elementi simmetrici. Analogamente, gli isomorfismi *conservano tutte le proprietà algebriche*, compresa la cancellabilità.

Esempio 5.4.2

Si consideri l'applicazione:

$$f : x \in (\mathcal{P}(S), \cap) \mapsto S \setminus x \in (\mathcal{P}(S), \cup)$$

f è un isomorfismo. Infatti per il primo teorema di De Morgan si ha:

$$\begin{aligned} \forall x, y \in \mathcal{P}(S) (f(x \cap y)) &= S \setminus (x \cap y) \\ &= (S \setminus x) \cup (S \setminus y) \\ &= f(x) \cup f(y) \end{aligned}$$

e quindi f è un omomorfismo. Siano $x, y \in \mathcal{P}(S)$ tali che $f(x) = f(y)$ ovvero $(S \setminus x = S \setminus y)$ e questo chiaramente avviene solo se $x = y$, quindi f è un monomorfismo. Inoltre f è suriettiva in quanto per ogni parte di S esiste il complemento rispetto ad S di tale parte.

Osservazione 5.4.3

Tutti i gruppi di due e tre elementi sono isomorfi tra di loro. È unicamente determinata quindi la tavola di Cayley per ciascuno di questi gruppi. Preso $T(\{0, 1\})$, l'insieme delle trasformazioni in $\{0, 1\}$, si ha $T(\{0, 1\}) = \{id_{\{0,1\}}, c_0, c_1, \alpha\}$,

dove c_0 e c_1 sono le applicazioni costanti mentre α è la permutazione che mappa 0 in 1 e viceversa. Le applicazioni biettive $Sym(\{0, 1\})$ sono esattamente 2 e sono $id_{\{0,1\}}$ e α ottenendo così la seguente tavola di Cayley:

\circ	$id_{\{0,1\}}$	α
$id_{\{0,1\}}$	$id_{\{0,1\}}$	α
α	α	$id_{\{0,1\}}$

Si ha quindi che ogni gruppo di due elementi è isomorfo a $Sym(\{0, 1\})$.

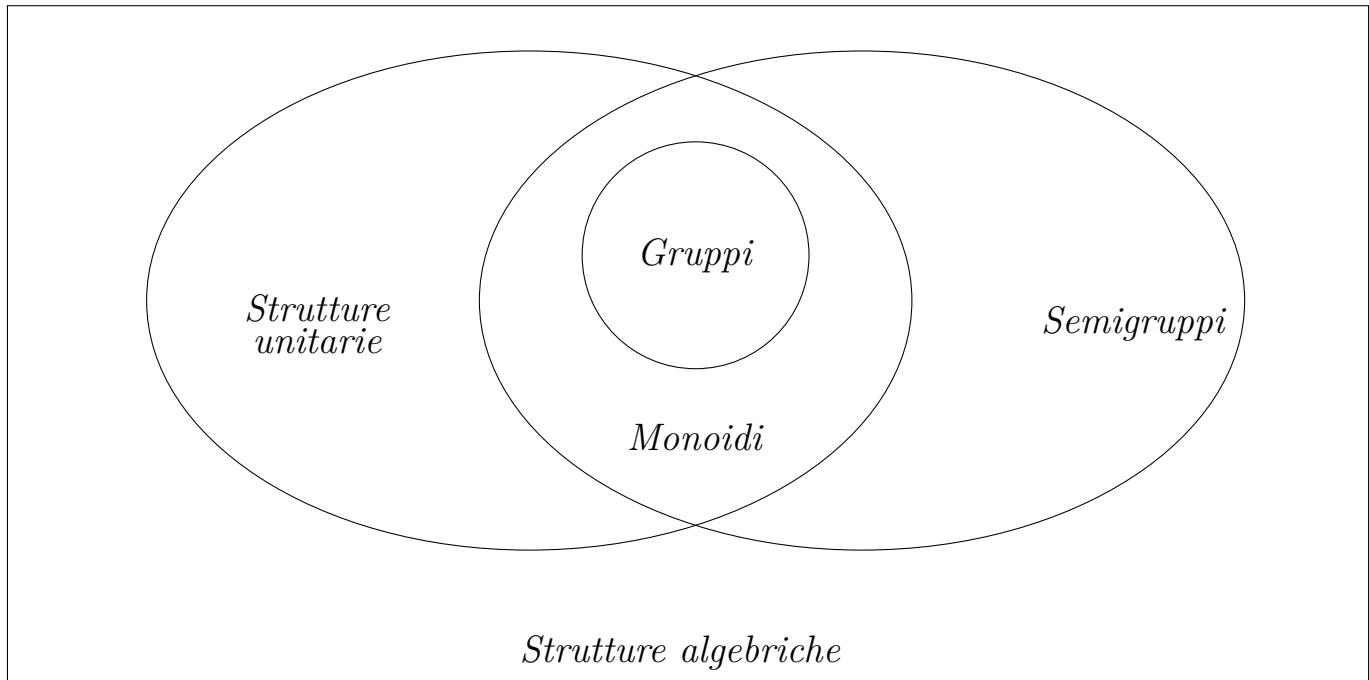


Figura 5.1: Strutture algebriche ad una singola operazione interna

! Per **gruppoide** si intende una struttura (A, \perp) dotata di una operazione interna.

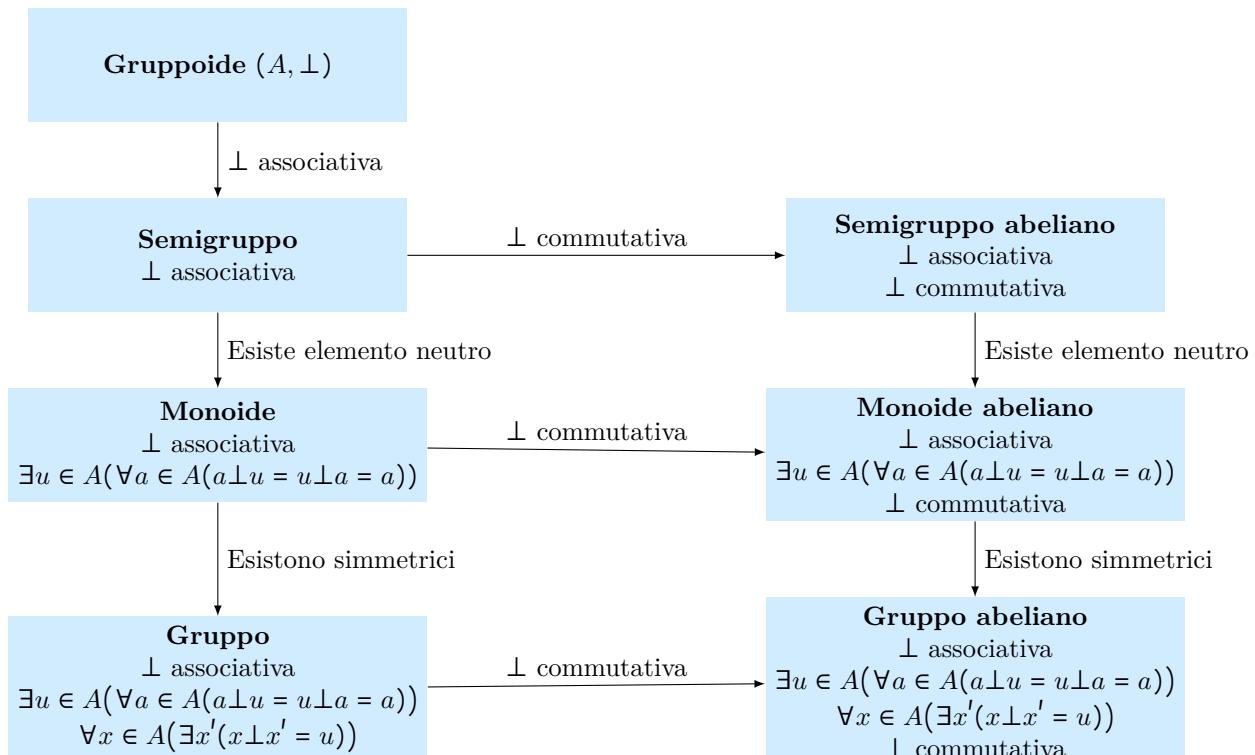


Figura 5.2: Caratterizzazione delle strutture ad una singola operazione interna



Definizione 5.5.1: Anello

Un **anello** è un insieme A dotato di due operazioni $+$, \cdot (che saranno sempre chiamate “somma” e “prodotto”), che soddisfano le seguenti proprietà:

1. $(G, +)$ è un gruppo abeliano:
 - (a) $+$ è associativa
 - (b) $+$ è commutativa
 - (c) Esiste l’elemento neutro rispetto a $+$ ed è denotato con 0_G
 - (d) Per ogni $x \in G$ esiste $-x \in G$ tale che $x + (-x) = 0_G$.
2. (G, \cdot) è un semigruppo
3. L’operazione \cdot è distributiva rispetto a $+$:

$$\forall a, b, c \in A \begin{cases} a \cdot (b + c) = ab + ac \\ (a + b)c = ac + bc \end{cases}$$

Se anche l’operazione \cdot è commutativa allora l’anello si dice **abeliano**. Se esiste l’elemento neutro per la moltiplicazione^a indicato con 1_A allora l’anello si dice **unitario**.

^aQuindi (A, \cdot) è un monoide

Esempio 5.5.1

Sono anelli, con le usuali operazioni di somma e prodotto, gli insiemi numerici $\mathbb{R}, \mathbb{Z}, \mathbb{Q}, \mathbb{C}$.

Esempio 5.5.2

Dato l’insieme $E = \{a, b, c\}$ consideriamo l’insieme delle parti $\mathcal{P}(E)$:

$$\mathcal{P}(E) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, E\}$$

Consideriamo in tale insieme le due operazioni di differenza simmetrica Δ e di intersezione \cap . È facile verificare che la struttura $(\mathcal{P}(E), \Delta, \cap)$ è un anello:

1. L’operazione Δ è associativa e commutativa;
2. Esiste l’elemento neutro rispetto a Δ , ovvero l’elemento: $\emptyset: \forall x \in \mathcal{P}(E)(a \Delta \emptyset = \emptyset \Delta a = a)$;
3. Ogni elemento $a \in \mathcal{P}(E)$ ha come simmetrico se stesso rispetto a Δ : $a \Delta a = (a \cup a) \setminus (a \cap a) = \emptyset$. Quindi $(\mathcal{P}(E), \Delta)$ è un gruppo;
4. L’operazione \cap è associativa e commutativa;
5. Esiste l’elemento neutro rispetto a \cap , ovvero E e vale: $\forall a \in \mathcal{P}(E)(a \cap E = E \cap a = a)$;
6. L’intersezione è distributiva rispetto alla differenza simmetrica:

$$\forall a, b, c \in \mathcal{P}(E)(a \cap (b \Delta c) = (a \cap b) \Delta (a \cap c))$$

Pertanto la struttura $(\mathcal{P}(E), \Delta, \cap)$ è un anello commutativo unitario. Tale anello prende il nome di **anello di Boole**.

5.5.1 ■ Regole di calcolo in un anello

Dagli assiomi che definiscono la struttura di anello, seguono di fatto molte di quelle proprietà delle operazioni che utilizziamo familiarmente nel caso di anelli numerici. Le elenchiamo nelle seguenti proposizioni: la prima riguarda la somma, e non è altro che la **legge di cancellazione**, valida in qualsiasi gruppo; la seconda riguarda il prodotto (si osservi come sia fondamentale la proprietà distributiva).

Proposizione 5.5.1

Sia A un anello. Allora, per ogni $a, b, c \in A$:

$$a + b = a + c \implies b = c \tag{5.28}$$

Dimostrazione. Siano per ogni $a, b, c \in A$, tali che $a + b = a + c$ e sia $a' \in A$ tale che $a' + a = 0_A$. Allora:

$$\begin{aligned}
 b &= 0_A + b && (\text{elemento neutro della somma}) \\
 &= (a + a') + b && (\text{elemento opposto}) \\
 &= a' + (a + b) && (\text{proprietà associativa}) \\
 &= a' + (a + c) && (\text{per ipotesi}) \\
 &= (a' + a) + c = 0_A + c = c
 \end{aligned}$$

□

Supponiamo ora che $0'_A$ sia un elemento neutro per la somma. Allora: $0'_A = 0'_A + 0_A = 0_A$. Infine, se a' e a'' sono opposti dell'elemento a , allora $a + a' = 0_A = a + a''$ e quindi, per quanto provato sopra, $a' = a''$. Se a e b sono elementi dell'anello A , si adotta la seguente notazione: $a - b = a + (-b)$. Nel caso del prodotto invece si è soliti scrivere direttamente: $a \cdot b = ab$.

Proposizione 5.5.2

Sia A un anello unitario, e siano $a, b \in A$ allora:

1. Esiste un unico elemento neutro per il prodotto
2. $a \cdot 0_A = 0_A \cdot a = 0_A$
3. $a(-b) = -(ab) = (-a)b$
4. $(-a)(-b) = ab$

Dimostrazione. (1) Siano 1_A e $1'_A$ elementi neutri per il prodotto. Allora, analogamente a quanto visto per l'addizione:

$$1'_A = 1'_A \cdot 1_A = 1_A$$

(2) Sia $c = a0_A$. Allora, applicando la proprietà distributiva:

$$\begin{aligned}
 c &= a0_A && (\text{per ipotesi}) \\
 &= a(0_A + 0_A) && (\text{idempotenza}) \\
 &= a0_A + a0_A && (\text{proprietà distributiva}) \\
 &= c + c
 \end{aligned}$$

e quindi $c = c + c - c = c - c = 0_A$. Analogamente si dimostra che $0_a a = 0_A$.

(3) Proviamo che $a(-b) = -(ab)$. Applicando la proprietà distributiva ed il punto 2:

$$a(-b) + ab = a(-b + b) = a0_A = 0_A$$

e quindi $a(-b) = -(ab)$. Analogamente si dimostra che $(-a)b = -(ab)$.

(4) Per il punto 3 si ha:

$$\begin{aligned}
 (-a)(-b) &= -a(-b) \\
 &= -(-(ab)) \\
 &= ab
 \end{aligned}$$

□

Anche per un generico anello è possibile definire l'elevazione a potenza per un numero intero. In generale, in un anello non commutativo, A non è detto che, dati $a, b \in A$ e $n \in \mathbb{N}$ valga $(ab)^n = a^n b^n$. Tuttavia, non è difficile provare che se $ab = ba$ allora si ha, per ogni $n \in \mathbb{N}$, $(ab)^n = a^n b^n$. In particolare, questa ulteriore proprietà delle potenze sussiste negli anelli abeliani, nei quali vale il seguente teorema:

Teorema 5.5.1 (del binomio di Newton)

Sia A un anello commutativo, e siano $a, b \in A$. Per ogni $n \in \mathbb{N}$:

$$(a + b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i \quad (5.29)$$

Questa formula non vale se l'anello non è commutativo. Per verificarlo basta osservare ciò che accade se si prova a calcolare $(a + b)^3$:

$$\begin{aligned}
 (a + b)^3 &= (a + b)(a + b)(a + b) \\
 &= a(a + b)(a + b) + b(a + b)(a + b) \\
 &= a(a(a + b) + b(a + b)) + b(a(a + b) + b(a + b)) \\
 &= a(aa + ab + ba + bb) + b(aa + ab + ba + bb) \\
 &= aaa + aab + aba + abb + baa + bab + bba + bbb
 \end{aligned}$$

Se l'anello fosse commutativo si potrebbero unire i fattori $(aab + aba + baa)$ come $3a^2b$ e ottenere la formula indicata dal binomio di Newton ma essendo $ab \neq ba$ questo non è possibile e tutti i fattori sono uno diverso dall'altro.

Definizione 5.5.2: Sottoanello

Un sottoinsieme non vuoto S di un anello A che sia chiuso rispetto alle due operazioni di A si dice **sottoanello** di A .

5.5.2 ■ Tipologie di anello

La nozione di cancellabilità, come quella di invertibilità, riveste una grande importanza in teoria degli anelli. In questo contesto una prima precisazione, per quanto ovvia, è necessaria: *ogni elemento di un anello è simmetrizzabile, quindi anche cancellabile, rispetto all'operazione additiva*, dunque quando si parla di elementi cancellabili o simmetrizzabili in un anello è all'operazione moltiplicativa che si fa riferimento.

Nei paragrafi precedenti abbiamo provato alcune proprietà degli anelli, che per \mathbb{Z} siamo abituati a considerare "naturali". Ora, \mathbb{Z} soddisfa anche altre proprietà, quali il fatto che il prodotto di due elementi diversi da zero è diverso da zero. Questa legge non discende dagli assiomi di anello, esistono infatti anelli in cui questa legge non vale.

Definizione 5.5.3: Divisore dello zero

Sia $(A, +, \cdot)$ un anello e sia $a \in A$. Allora:

- a è un **divisore sinistro dello zero** in A se e soltanto se esiste un elemento $b \in A$ tale che $b \neq 0_A$ e $ab = 0_A$.
- a è un **divisore destro dello zero** in A se e soltanto se esiste un elemento $b \in A$ tale che $b \neq 0_A$ e $ba = 0_A$.
- a è un **divisore dello zero** in A se e soltanto se esiste un elemento $b \in A$ tale che $b \neq 0_A$ e $ab = ba = 0_A$.

Esempio 5.5.3

Un esempio di divisori dello zero si può trovare negli anelli di matrici; ad esempio, in $(M_2(\mathbb{R}), +, \cdot)$ ovvero l'anello delle matrici quadrate di dimensione 2 con le operazioni di somma e prodotto righe per colonne si ha:

$$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Teorema 5.5.2

Per ogni elemento $a \in A$ si ha che:

- a è un divisore sinistro dello zero in A se e soltanto se a non è cancellabile a sinistra in (A, \cdot) ;
- a è un divisore destro dello zero in A se e soltanto se a non è cancellabile a destra in (A, \cdot) ;
- a è un divisore dello zero in A se e soltanto se non è cancellabile in (A, \cdot) .

Dimostrazione. Dimostriamo la prima delle equivalenze logiche, la seconda equivalenza si dimostra in maniera analoga mentre la terza discende dalla veridicità delle prime due equivalenze.

\implies) Sia a un divisore sinistro dello zero in A . Allora, per definizione, esiste un elemento $b \in A$ tale che $ab = 0_A \neq b$. Chiaramente vale: $0_A = a \cdot 0_A$ eppure l'equivalenza $ab = a0_A$ non implica che $b = 0_A$. Quindi a non è cancellabile a sinistra.

\impliedby) Se a non è cancellabile a sinistra in (A, \cdot) allora esistono u e v in A tale che $au = av$ e $u \neq v$. Per tali u e v :

$$\begin{aligned}
 au &= av \\
 au - av &= 0_A \\
 a(u - v) &= 0_A
 \end{aligned}$$

e quindi a è un divisore sinistro dello zero. □

Teorema 5.5.3

In un anello con più di un elemento, lo zero (0_A) è un divisore dello zero.

Dimostrazione. Sia $|A| > 1$ allora esiste un elemento $b \in A \setminus \{0_A\}$ per il quale $0_A = 0_A = b0_A$ e quindi 0_A risulta un divisore dello zero. Ovviamente se $|A| = 1$ le operazioni di somma e prodotto coincidono in quanto si ha $0_A = 1_A$. □

Definizione 5.5.4: Anello integro

Un anello si dice **integro** se in esso vale la legge di annullamento del prodotto.

Con la terminologia appena introdotta, possiamo riformulare questa condizione in questo modo: un anello è integro se e solo se non ha divisori propri dello zero. Per quanto appena dimostrato, ciò equivale anche a dire che nell'anello in questione ogni elemento diverso da zero è cancellabile.

Proposizione 5.5.3 (Legge di annullamento del prodotto)

Sia A un anello integro e siano $a, b \in A$ due elementi qualsiasi. Si ha allora:

$$ab = 0 \implies (a = 0 \vee b = 0) \quad (5.30)$$

Definizione 5.5.5: Dominio di integrità

Un anello si dice un **dominio di integrità** se è un anello integro commutativo unitario.

Proposizione 5.5.4 (Legge di cancellazione)

Sia A un dominio di integrità, allora per ogni $a, b \in A$ e per ogni $c \neq 0_A$ si ha:

$$ac = bc \implies a = b \quad (5.31)$$

Possiamo formularne la definizione in uno qualsiasi dei seguenti modi, tra loro equivalenti: un dominio di integrità è:

- un anello commutativo integro;
- un anello commutativo in cui vale la legge di annullamento del prodotto;
- un anello commutativo in cui ogni elemento diverso da zero è cancellabile.

Teorema 5.5.4

Un anello $(A, +, \cdot)$ è un dominio di integrità se è privo di divisori dello zero.

Dimostrazione. \implies Se l'anello è un dominio di integrità, per la Proposizione 5.5.3 vale la legge di annullamento del prodotto.

Per assurdo, sia $x \in A$ un divisore dello zero, allora:

$$\exists y \in A \setminus \{0_A\} (xy = 0)$$

e dunque, per la legge di annullamento del prodotto, deve essere $x = 0_A \vee y = 0_A$ che va contro le ipotesi che siano entrambi non nulli. Quindi A è privo di divisori dello zero.

\impliedby Se nessun elemento è divisore dello zero, allora tutti gli elementi sono cancellabili per il Teorema 5.5.2. Dunque, se consideriamo:

$$\forall x, y \in A (x \neq 0_A \wedge xy = 0_A \implies y = 0_A)$$

Quindi A è un dominio di integrità, come volevasi dimostrare. □

Definizione 5.5.6: Corpo

Un anello unitario A si dice **corpo** se ogni elemento non nullo di A è invertibile.

Definizione 5.5.7: Campo

Un **campo** è un corpo commutativo, ovvero un anello abeliano in cui ogni suo elemento non nullo è invertibile.

Proposizione 5.5.5

Ogni campo è un dominio di integrità.

Dimostrazione. Un campo è un corpo commutativo, ed un corpo è un anello unitario. Un anello commutativo unitario è dominio di integrità se e soltanto se è privo di divisori dello zero. Ogni elemento di un campo, eccetto lo zero, è invertibile, e dunque cancellabile. Un elemento cancellabile non può essere divisore dello zero, e quindi non esistono divisori dello zero. Dunque il campo è dominio di integrità. \square

Non vale il viceversa, non tutti i domini di integrità sono dei campi. Ad esempio $(\mathbb{Z}, +, \cdot)$ è un dominio di integrità ma non è un campo in quanto, ad esempio, il numero 2 non ha un inverso moltiplicativo in \mathbb{Z} . *Ogni dominio di integrità finito*, però, *risulta essere un campo*. La ragione sta nel fatto che in un dominio di integrità finito, ogni elemento non nullo deve necessariamente avere inverso moltiplicativo. Questo può essere dimostrato con un argomento di tipo combinatorio. Sia D un dominio di integrità con n elementi. Consideriamo l'elemento $a \in D$ con $a \neq 0_D$. La funzione $f : D \rightarrow D$ definita da $f(x) = ax$ è iniettiva. Infatti:

$$\forall x, y \in D (f(x) = f(y) \iff ax = ay)$$

e poiché D è un dominio di integrità, vale la legge di cancellazione, cioè: $x = y$. Essendo f una funzione iniettiva tra due insiemi equipotenti questa risulta essere anche suriettiva. Dunque deve esistere un elemento $b \in D$ tale che $ab = 1_D$ e b risulta essere a^{-1} . Questo dimostra che ogni elemento non nullo ha un inverso moltiplicativo e D è un campo.

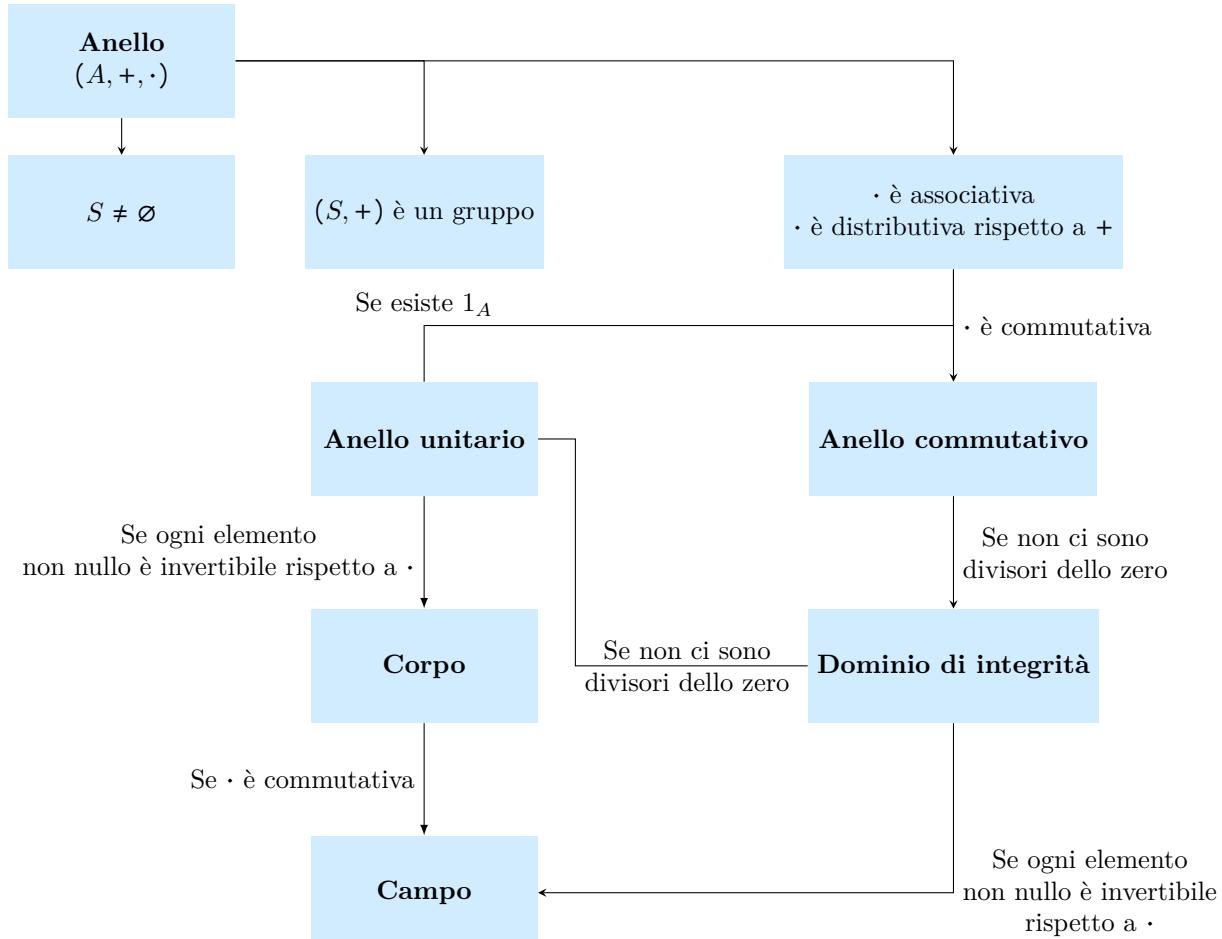


Figura 5.3: Caratterizzazione dei corpi



Esercizio 5.6.1

Sia $A = \{1, 2\}$ e consideriamo l'operazione di intersezione nell'insieme delle parti di A:

$$\cap : \mathcal{P}(A) \times \mathcal{P}(A) \longrightarrow \mathcal{P}(A)$$

Si rappresenti la relativa tavola di Cayley.

Svolgimento. Si ha:

\cap	\emptyset	{1}	{2}	A
\emptyset	\emptyset	\emptyset	\emptyset	\emptyset
{1}	\emptyset	{1}	\emptyset	{1}
{2}	\emptyset	\emptyset	{2}	{2}
A	\emptyset	{1}	{2}	A

Esercizio 5.6.2

Vero o falso? Per ogni insieme non vuoto S ed ogni operazione binaria $*$ in S, \dots

1. In S esiste sempre un elemento neutro a destra o un elemento neutro a sinistra;
2. Se $*$ è commutativa, tutti gli elementi neutri a destra in $(S, *)$ sono anche neutri a sinistra;
3. Se $*$ è commutativa, in S esiste al massimo un elemento neutro a sinistra;
4. Se a e b sono due elementi neutri a sinistra distinti in $(S, *)$, in $(S, *)$ non esistono elementi neutri a destra.

Svolgimento. Sia $(S, *)$ un'arbitraria struttura algebrica.

1. Falso. Ad esempio nell'insieme degli interi maggiori di 1 con l'operazione della moltiplicazione non esiste elemento neutro.
2. Vero. Infatti se esiste un elemento $t \in S$ neutro a destra allora $\forall x \in S (x * t = t * x = x)$ e quindi t è neutro a sinistra.
3. Vero. Infatti, posto u l'elemento neutro a sinistra, se esistesse un secondo elemento neutro a sinistra u' si avrebbe:

$$u' = u * u' = u' * u = u$$

4. Vero. Infatti se per assurdo esistesse un elemento neutro a destra, detto u''' , si avrebbe:

$$u' * u''' = u'$$

ma anche:

$$u'' * u''' = u''$$

Tuttavia, poiché u' e u'' sono elementi distinti si deve avere:

$$u' * u''' = u''' = u'' * u'''$$

ma $u'' \neq u'$.

Esercizio 5.6.3

Dato l'insieme $A = \{0, 1\}$ scrivere le tavole di Cayley di $(\mathcal{P}(A), \cup)$ e di $(\mathcal{P}(A), \Delta)$.

Svolgimento. Si ha:

\cup	\emptyset	{0}	{1}	A
\emptyset	\emptyset	{0}	{1}	A
{0}	{0}	{0}	A	A
{1}	{1}	A	{1}	A
A	A	A	A	A

Δ	\emptyset	{0}	{1}	A
\emptyset	\emptyset	{0}	{1}	A
{0}	{0}	\emptyset	A	{1}
{1}	{1}	A	\emptyset	{0}
A	A	{1}	{0}	\emptyset

Esercizio 5.6.4

Studiare le operazioni binarie qui elencate, stabilendo per ciascuna di essere se è commutativa e se è associativa, e determinando gli elementi neutri a sinistra, a destra, neutri delle strutture da esse definite:

1. $\alpha : (a, b) \in \mathbb{N} \times \mathbb{N} \mapsto a10^b \in \mathbb{N}$
2. $\beta : (a, b) \in \mathbb{Z} \times \mathbb{Z} \mapsto -ab \in \mathbb{Z}$
3. $\gamma : (a, b) \in \mathbb{Q} \times \mathbb{Q} \mapsto \frac{(a+b)}{2} \in \mathbb{Q}$
4. $\delta : (a, b) \in \mathbb{Z} \times \mathbb{Z} \mapsto 2ab \in \mathbb{Z}$
5. $\epsilon : (a, b) \in \mathbb{Q} \times \mathbb{Q} \mapsto 2ab \in \mathbb{Q}$
6. $\zeta : (a, b) \in \mathbb{Z} \times \mathbb{Z} \mapsto a + b + 2 \in \mathbb{Z}$
7. $\eta : (a, b) \in \mathbb{N} \times \mathbb{N} \mapsto a(b^{a+b} + 3ab^2) + 1 \in \mathbb{N}$
8. $\theta : (a, b) \in \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{Z}) \mapsto (a \cap \mathbb{N}) \cup b \in \mathbb{Z}$
9. $\iota : (a, b) \in \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{Z}) \mapsto a \cup b \cup \{1\} \in \mathbb{Z}$

Svolgimento. Si ha:

1. L'operazione non è commutativa. Infatti:

$$\exists a, b \in \mathbb{N} (a10^b \neq b10^a)$$

ad esempio $(0, 1)$. L'operazione non è associativa. Per essere associativa deve valere:

$$\forall a, b, c \in \mathbb{N} (a \alpha (b \alpha c) = (a \alpha b) \alpha c)$$

ovvero:

$$a \cdot 10^{b \cdot 10^c} = a \cdot 10^{b+c}$$

Scritto così è facile trovare una terna controesempio. Infatti sia $(1, 1, 2)$ si ha:

$$\begin{aligned} a \cdot 10^{b \cdot 10^c} &= 1 \cdot 10^{1 \cdot 10^2} = 10^{100} \\ a \cdot 10^{b+c} &= 1 \cdot 10^{1+2} = 1000 \end{aligned}$$

Si ha inoltre che $0 \in \mathbb{N}$ è neutro a destra rispetto ad α , infatti:

$$\forall a \in \mathbb{N} (a \alpha 0 = a10^0 = a)$$

A questo punto, per il [Teorema di unicità dell'elemento neutro](#), se esiste un elemento neutro a sinistra deve essere proprio 0 ma è evidente che 0 non è neutro a sinistra.

2. L'operazione è commutativa e associativa. Infatti:

$$\forall a, b \in \mathbb{Z} (a \beta b = -ab = -ba = b \beta a)$$

e

$$\forall a, b, c \in \mathbb{Z} (a \beta (b \beta c) = a \beta (-bc) = -(a(-bc)) = abc)$$

ma anche:

$$\forall a, b, c \in \mathbb{Z} ((a \beta b) \beta c = (-ab) \beta c = -(-ab)c = abc)$$

L'elemento -1 risulta neutro rispetto a β , infatti:

$$\forall b \in \mathbb{Z} (-1 \beta b = -(-1b) = b = -(b(-1)) = b \beta -1)$$

3. L'operazione risulta commutativa:

$$\forall a, b \in \mathbb{Q} (a \gamma b = \frac{a+b}{2} = \frac{b+a}{2} = b \gamma a)$$

ma non associativa. Infatti:

$$\forall a, b, c \in \mathbb{Q} (a \gamma (b \gamma c) = a \gamma (\frac{b+c}{2}) = \frac{a+\frac{b+c}{2}}{2} = \frac{2a+b+c}{4})$$

e

$$\forall a, b, c \in \mathbb{Q} ((a \gamma b) \gamma c = \frac{\frac{a+b}{2} + c}{2} = \frac{a+b+2c}{4})$$

presa la terna $(1, 1, 0)$ si ha:

$$\begin{aligned} \frac{2a+b+c}{4} &= \frac{2+1+0}{4} \\ &= \frac{3}{4} \end{aligned}$$

e

$$\begin{aligned}\frac{a+b+2c}{4} &= \frac{1+1+0}{4} \\ &= \frac{2}{4} = \frac{1}{2}\end{aligned}$$

Per esistere elemento neutro a destra deve esistere un elemento $t \in \mathbb{Q}$ tale che:

$$\forall a \in \mathbb{Q}(t \gamma a = a)$$

ovvero:

$$\begin{aligned}\frac{a+t}{2} &= a \\ a+t &= 2a \\ t &= 2a-a \\ t &= a\end{aligned}$$

ma non esiste $t \in \mathbb{Q}$ uguale ad ogni numero razionale. Quindi non esiste elemento neutro a destra. Analogamente a sinistra.

4. L'operazione δ è commutativa e associativa. Infatti:

$$\forall a, b \in \mathbb{Z}(a \gamma b = 2ab = 2ba = b \delta a)$$

e:

$$\begin{aligned}\forall a, b, c \in \mathbb{Z}(a \delta (b \delta c) &= a \delta (2bc) = 4abc) \\ \forall a, b, c \in \mathbb{Z}((a \delta b) \delta c &= (2ab) \delta c = 4abc)\end{aligned}$$

Non esiste elemento neutro rispetto a δ , infatti se esistesse un elemento neutro a destra $t \in \mathbb{Z}$ si deve avere:

$$\begin{aligned}a \delta t &= a \\ 2at &= a \\ t &= \frac{a}{2a} = \frac{1}{2} \notin \mathbb{Z}\end{aligned}$$

5. A differenza di δ , l'operazione ϵ è commutativa, associativa e gode di elemento neutro.

6. L'operazione è commutativa. Infatti, per ogni $a, b \in \mathbb{Z}$ si ha:

$$a \zeta b = a + b + 2 = b + a + 2 = b \zeta a$$

Per verificare l'associatività deve essere, qualsiasi siano gli elementi $a, b, c \in \mathbb{Z}$:

$$\begin{cases} a\zeta(b\zeta c) = a\zeta(b+c+2) = a+(b+c+2)+2 = a+b+c+4 \\ (a\zeta b)\zeta c = c\zeta(a\zeta b) = c+a+b+4 \end{cases}$$

quindi ζ è associativa. Per trovare l'elemento neutro partiamo dalla definizione :

$$\forall a \in \mathbb{Z}(a \zeta u = a \iff a + u + 2 = a)$$

L'elemento $-2 \in \mathbb{Z}$ è neutro quindi rispetto a ζ .

7. L'operazione non è associativa, non è commutativa e non ha elemento neutro. Davanti a formule poco maneggevoli è utile provare cercando terne che negano le proprietà cercate. Infatti data la coppia $(2, 3)$ si ha:

$$2 \eta 3 = 2(3^{2+3} + 3 \cdot 2 \cdot 3^2) + 1 = 595 \neq 205 = 3(2^{3+2} + 3 \cdot 3 \cdot 2^2) + 1 = 3 \eta 2$$

e data la terna $(0, 0, 1)$ si ha:

$$(0 \eta 0) \eta 1 = 5 \neq 1 = 0 \eta (0 \eta 1)$$

Per quanto riguarda la verifica dell'esistenza dell'elemento neutro, dalla definizione di elemento neutro a sinistra si ha che $t \in \mathbb{N}$ è neutro a sinistra rispetto a η se e solo se:

$$\forall b \in \mathbb{N}(t \eta b = b)$$

Osservando la formula dell'operazione si nota che:

$$\forall a \in \mathbb{N}(a \eta 0 = 1)$$

da cui si deduce la non esistenza di un elemento neutro. Infatti non esiste un elemento $t \in \mathbb{N}$ tale che $t \eta 0 = 0$ in quanto abbiamo visto che questo darà sempre 1 come risultato.

8. L'operazione non è commutativa, seguendo il metodo visto nell'esercizio precedente si può andare per tentativi. Preso $a = \{-1\} \subseteq \mathbb{Z}$ e $b = \{-2, 3\} \subseteq \mathbb{Z}$ si ha:

$$a \theta b = (a \cap \mathbb{N}) \cup b = (\{-1\} \cap \mathbb{N}) \cup b = \emptyset \cup \{-2, 3\} = \{-2, 3\}$$

$$b \theta a = (\{-2, 3\} \cap \mathbb{N}) \cup \{-1\} = \{3\} \cup \{-1\} = \{-1, 3\}$$

mentre per l'associatività, deve valere:

$$\forall a, b, c \in \mathcal{P}(\mathbb{Z}) (a \theta (b \theta c) = (a \theta b) \theta c)$$

Dove:

$$\begin{aligned} a \theta (b \theta c) &= a \theta ((b \cap \mathbb{N}) \cup c) \\ &= (a \cap \mathbb{N}) \cup ((b \cap \mathbb{N}) \cup c) \end{aligned}$$

e:

$$\begin{aligned} (a \theta b) \theta c &= ((a \cap \mathbb{N}) \cup b) \theta c \\ &= (((a \cap \mathbb{N}) \cup b) \cap \mathbb{N}) \cup c \\ &= ((a \cap \mathbb{N} \cap \mathbb{N}) \cup (b \cap \mathbb{N})) \cup c \\ &= (a \cap \mathbb{N} \cup (b \cap \mathbb{N})) \cup c \end{aligned} \quad \text{Applicando la distributività}$$

Quindi vale la proprietà associativa. Se un elemento $a \in \mathcal{P}(\mathbb{Z})$ è neutro a sinistra vale, per ogni $b \in \mathcal{P}(\mathbb{Z})$:

$$a \theta b = b$$

ovvero:

$$(a \cap \mathbb{N}) \cup b = b$$

Data questa condizione si ha sicuramente che:

$$(a \cap \mathbb{N} = \emptyset) \implies (a \cap \mathbb{N}) \cup b = b$$

Preso $a \subseteq \mathbb{Z} \wedge a \cap \mathbb{N} \neq \emptyset$ allora

$$a \theta \emptyset = (a \cap \mathbb{N}) \cup \emptyset = a \cap \emptyset \neq \emptyset$$

Quindi a non è neutro a sinistra in quanto esiste una scelta di $b \in \mathcal{P}(\mathbb{Z})$ che non verifica la condizione: \emptyset . Un metodo alternativo per arrivare alla stessa conclusione è quello di osservare che per valere la condizione deve essere:

$$\forall b \in \mathcal{P}(\mathbb{Z}) ((a \cap \mathbb{N}) \subseteq b)$$

quindi deve essere $a \cap \mathbb{N} = \emptyset$. In conclusione θ ha elementi neutri a sinistra e sono tutte le parti $a \in \mathbb{Z} \setminus \mathbb{N}$. Dati infiniti elementi neutri a sinistra, per il [Teorema di unicità dell'elemento neutro](#) possiamo dire che $(\mathcal{P}(\mathbb{Z}), \theta)$ non ha elementi neutri a destra.

9. L'operazione è commutativa e associativa per la commutatività e l'associatività dell'unione. Un elemento t è neutro se e solo se, per ogni $b \in \mathcal{P}(\mathbb{Z})$ si ha:

$$t \iota b = b \iota t = b$$

ovvero:

$$t \iota b = t \cup b \cup \{1\} = b$$

ma per ogni scelta di b non esiste un siffatto elemento neutro in quanto il loro composto tramite ι sarà sempre diverso da b . Per convincerci di questa affermazione consideriamo $b = \emptyset$:

$$t \iota \emptyset = t \cup \emptyset \cup \{1\} \neq \emptyset$$

Esercizio 5.6.5

Ripetere l'esercizio precedente per l'operazione $*$ definita in $\{0, 1, 2, 3\}$ da questa tavola di Cayley:

*	0	1	2	3
0	1	1	0	1
1	1	1	1	1
2	1	1	2	1
3	1	1	3	1

Svolgimento. Dall'osservazione diretta della tavola si può dire che l'operazione $*$ non è commutativa. Infatti, si ha:

$$3 * 2 = 3 \neq 1 = 2 * 3$$

L'elemento 2 è neutro a destra. Infatti

$$\forall a \in \{0, 1, 2, 3\} (a * 2 = a)$$

Per verificare l'associatività dell'operazione $*$ si procede confrontando se per ogni terna (a, b, c) vale:

$$a * (b * c) = (a * b) * c$$

Se si trova una terna per la quale non vale la condizione di associatività si può concludere dicendo che l'operazione non è associativa. Il calcolo può essere ridotto osservando che, quando $c = 2$ si ha:

$$a * (b * 2) = a * b = (a * b) * 2$$

Quindi il calcolo si riduce alle terne (a, b, c) con $c \neq 2$. Anche in questo caso non esistono terne che contraddicono la condizione e allora l'operazione è associativa. ■

Esercizio 5.6.6

Determinare gli elementi simmetrizzabili nel monoide $(\mathbb{R}, \cdot, 1)$ e, per un arbitrario insieme A , nei monoidi $(\mathcal{P}(A), \cup, \emptyset)$ e $(\mathcal{P}(A), \cap, A)$.

Svolgimento. All'interno del monoide $(\mathbb{R}, \cdot, 1)$ tutti gli elementi diversi da 0 sono simmetrizzabili. Infatti, per ogni $a \in \mathbb{R} \setminus \{0\}$ esiste un elemento a^{-1} tale che $a \cdot a^{-1} = 1$. Tale simmetrico, detto inverso, è esattamente $1/a$. $(\mathbb{R} \setminus \{0\}, \cdot, 1)$ è quindi un gruppo.

Per un determinato insieme A , nei monoidi $(\mathcal{P}(A), \cap, A)$ e $(\mathcal{P}(A), \cup, \emptyset)$ gli unici elementi simmetrizzabili sono A e \emptyset . Infatti, preso il primo monoide, l'unico elemento $a \in \mathcal{P}(A)$ per il quale esiste un elemento $t \in \mathcal{P}(A)$ tale che:

$$a \cup t = \emptyset$$

è l'insieme vuoto stesso. Infatti: $\emptyset \cup \emptyset = \emptyset$. Analogamente, in $(\mathcal{P}(A), \cap, A)$ l'unico elemento $a \in \mathcal{P}(A)$ per il quale esiste un $t \in \mathcal{P}(A)$ tale che:

$$a \cap t = A$$

è A stesso e risulta: $A \cap A = A$. ■

Esercizio 5.6.7

Sia $*$ l'operazione binaria definita in $X := \mathbb{Z} \times \mathbb{Z}$ da:

$$(\forall a, b, c, d \in \mathbb{Z}) ((a, b) * (c, d) = (ac, ad))$$

Decidere se $*$ è associativa, commutativa, se ammette elementi neutri a sinistra, se ne ammette a destra. Nel caso la richiesta abbia senso, determinare gli elementi simmetrizzabili in $(X, *)$, descrivendone i simmetrici. Che tipo di struttura (semigruppo, monoide, gruppo, commutativo o no?) è $(X, *)$?

Svolgimento. L'operazione $*$ non è commutativa. Non vale cioè:

$$\forall a, b, c, d \in \mathbb{Z} ((a, b) * (c, d) = (c, d) * (a, b))$$

Infatti:

$$\begin{aligned} (a, b) * (c, d) &= (ac, ad) \\ (c, d) * (a, b) &= (ca, cb) \end{aligned}$$

L'operazione è però associativa:

$$\forall a, b, c, d, e, f \in \mathbb{Z} \left(\left((a, b) * (c, d) \right) * (e, f) = (a, b) * \left((c, d) * (e, f) \right) \right)$$

Infatti:

$$\begin{aligned} \left((a, b) * (c, d) \right) * (e, f) &= (ac, ad) * (e, f) = (ace, acf) \\ (a, b) * \left((c, d) * (e, f) \right) &= (a, b) * (ce, cf) = (ace, acf) \end{aligned}$$

L'operazione non ha elementi neutri a destra. Infatti un tale elemento $(u, z) \in \mathbb{Z} \times \mathbb{Z}$ deve soddisfare alla proprietà, qualsiasi sia la coppia (a, b) :

$$(a, b) * (u, z) = (au, az) = (a, b) \iff u = 1 \wedge az = b$$

ma $az = b$ se e solo se $z = 1 \wedge a = b$ oppure $a = 1 \wedge z = b$ e quindi non esiste una siffatta coppia valida per tutti le coppie (a, b) . Esistono però infiniti elementi neutri a sinistra. Infatti:

$$(u, z) * (a, b) = (ua, ub) = (a, b) \iff u = 1$$

Quindi ogni coppia del tipo $(1, x) \in \mathbb{Z} \times \mathbb{Z}$ è un elemento neutro a sinistra. La struttura quindi è un semigruppo. ■

Esercizio 5.6.8

Stesse domande dell'esercizio precedente per le operazioni:

1. $\varphi : (a, b) \in \mathbb{Z} \times \mathbb{Z} \mapsto a + b - 1 \in \mathbb{Z}$
 2. $\psi : (a, b) \in \mathbb{Z} \times \mathbb{Z} \mapsto ab + 1 \in \mathbb{Z}$
 3. $\mu : ((a, b), (c, d)) \in (\mathbb{Z} \times \mathbb{Z}) \times (\mathbb{Z} \times \mathbb{Z}) \mapsto (a + bc, bd) \in (\mathbb{Z} \times \mathbb{Z})$
 4. $\tau : (X, Y) \in \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{Z}) \mapsto (X \cup Y) \cap \mathbb{N} \in \mathcal{P}(\mathbb{Z})$
 5. $\omega : (X, Y) \in \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{Z}) \mapsto (X \setminus Y) \cup \{1\} \in \mathcal{P}(\mathbb{Z})$
- al posto di $*$.

^aSuggerimento: per l'ultima operazione considerare terne (X, Y, Z) di parti di \mathbb{Z} tali che $X \subseteq Y \subseteq Z$.

Svolgimento. Si ha:

1. L'operazione φ è commutativa:

$$\forall a, b \in \mathbb{Z} (a \varphi b = b \varphi a)$$

Infatti:

$$a \varphi b = a + b - 1 = b + a - 1 = b \varphi a$$

ed è anche associativa:

$$\forall a, b, c \in \mathbb{Z} (a \varphi (b \varphi c) = (a \varphi b) \varphi c)$$

Infatti:

$$\begin{aligned} a \varphi (b \varphi c) &= a \varphi (b + c - 1) \\ &= a + (b + c - 1) - 1 \\ &= a + b + c - 2 \end{aligned}$$

analogamente, sfruttando la proprietà commutativa di φ :

$$\begin{aligned} (a \varphi b) \varphi c &= c \varphi (a \varphi b) \\ &= c + a + b - 2 \end{aligned}$$

E per la proprietà commutativa dell'addizione si ha l'associatività di φ . Un elemento $u \in \mathbb{Z}$ è neutro rispetto a φ se e solo se:

$$\forall a \in \mathbb{Z} (a \varphi u = u \varphi a = a)$$

Quindi deve essere $u = 1$. Gli elementi simmetrizzabili in (\mathbb{Z}, φ) sono tutti e soli gli elementi tali che:

$$\exists a' \in \mathbb{Z} (a \varphi a' = a' \varphi a = 1)$$

Deve essere quindi: $a + a' - 1 = 1$ ovvero $a' = 2 - a$. La struttura risulta quindi un gruppo abeliano.

2. L'operazione ψ è commutativa. Infatti:

$$\forall a, b \in \mathbb{Z} (a \psi b = b \psi a)$$

Sviluppando i calcoli:

$$\begin{aligned} a \psi b &= ab + 1 \\ b \psi a &= ba + 1 \end{aligned}$$

L'operazione però non è associativa. Calcolando le due espressioni infatti:

$$\begin{aligned} a \psi (b \psi c) &= a \psi (bc + 1) \\ &= a(bc + 1) + 1 \\ &= abc + a + 1 \end{aligned}$$

e, sfruttando la commutatività dell'operazione:

$$\begin{aligned} (a \psi b) \psi c &= c \psi (a \psi b) \\ &= cab + c + 1 \end{aligned}$$

le due formule infatti sono diverse. Presa una terna arbitraria come ad esempio $(1, 2, 3)$ si ha:

$$1 \cdot 2 \cdot 3 + 1 + 1 = 8 \neq 10 = 3 \cdot 1 \cdot 2 + 3 + 1$$

Un elemento $u \in \mathbb{Z}$ è neutro se e solo se, per ogni $a \in \mathbb{Z}$ si ha:

$$\forall a \in \mathbb{Z} (a \psi u = u \psi a = a)$$

dove

$$a \psi u = au + 1 = a \iff u = -1$$

Un elemento $x \in \mathbb{Z}$ è simmetrizzabile invece se esiste x' tale che:

$$x \psi x' = u$$

Sviluppando i calcoli si ottiene:

$$\begin{aligned} x \psi x' = -1 &\iff xx' + 1 = -1 \\ &\iff xx' = -2 \\ &\iff x' = \frac{-2}{x} \end{aligned}$$

Quindi gli unici elementi simmetrizzabili in \mathbb{Z} rispetto a ψ sono 2, -2, 1 e -1.

3. L'operazione μ non è commutativa. Infatti, per essere commutativa, per ogni scelta di $a, b, c, d \in \mathbb{Z}$ deve valere:

$$(a, b) \mu (c, d) = (c, d) \mu (a, b)$$

Ovvero:

$$(a + bc, bd) = (c + da, bd)$$

Per osservare che l'operazione μ non gode della proprietà commutativa si consideri la seguente quaterna come controesempio: $(2, 4, 3, 7)$. Infatti:

$$\begin{aligned} (2, 4) \mu (3, 7) &= (2 + 12, 28) = (14, 28) \\ (3, 7) \mu (2, 4) &= (2 + 14, 28) = (17, 28) \end{aligned}$$

L'operazione è associativa. Infatti si ha, qualsiasi siano $a, b, c, d, e, f \in \mathbb{Z}$:

$$((a, b) \mu (c, d)) \mu (e, f) = (a + bc, bd) \mu (e, f) = (a + bc + dbe, dbf)$$

e

$$(a, b) \mu ((c, d) \mu (e, f)) = (a, b) \mu (c + de, df) = (a + bc + dbe, dbf)$$

L'elemento $(0, 1) \in \mathbb{Z}$ è neutro rispetto a μ , infatti:

$$\forall (a, b) \in \mathbb{Z} \times \mathbb{Z} \quad (a, b) \mu (0, 1) = (0, 1) \mu (a, b) = (a, b)$$

Chiaramente non esistono elementi neutri diversi da $(0, 1)$, un siffatto elemento deve soddisfare alla condizione:

$$\forall (a, b) \in \mathbb{Z} \times \mathbb{Z} \quad \left(\underbrace{((a, b) \mu (x, y) = (a, b))}_{\text{neutro a destra}} \wedge \underbrace{((x, y) \mu (a, b) = (a, b))}_{\text{neutro a sinistra}} \right)$$

Prendendo la prima delle due condizioni e sviluppando si ottiene:

$$(a + bx, by) = (a, b)$$

valida se e soltanto se:

$$\begin{cases} a + bx = a \\ by = b \end{cases}$$

che ammette come unica soluzione la coppia $(0, 1)$. Escluso l'elemento neutro non esistono elementi simmetrizzabili rispetto a μ .

4. L'operazione τ è commutativa. Infatti, per ogni scelta delle parti $A, B \in \mathcal{P}(\mathbb{Z})$ si ha:

$$(A \tau B) = (A \cup B) \cap \mathbb{N} = (B \cup A) \cap \mathbb{N} = (B \tau A)$$

L'operazione τ per essere associativa deve soddisfare alla condizione:

$$\forall A, B, C \in \mathcal{P}(\mathbb{Z}) \quad (A \tau (B \tau C)) = ((A \tau B) \tau C)$$

Sviluppando i calcoli si ottiene:

$$\begin{aligned} A \tau (B \tau C) &= A \tau ((B \cup C) \cap \mathbb{N}) \\ &= \left(A \cup ((B \cup C) \cap \mathbb{N}) \right) \cap \mathbb{N} \\ &= \left(A \cup ((B \cap \mathbb{N}) \cup (C \cap \mathbb{N})) \right) \cap \mathbb{N} \\ &= (A \cap \mathbb{N}) \cup \left((B \cap \mathbb{N}) \cap \mathbb{N} \cup (C \cap \mathbb{N}) \cap \mathbb{N} \right) \\ &= (A \cap \mathbb{N}) \cup (B \cap \mathbb{N}) \cup (C \cap \mathbb{N}) \end{aligned}$$

mentre:

$$\begin{aligned} (A \tau B) \tau C &= ((A \cup B) \cap \mathbb{N}) \tau C \\ &= \left(((A \cup B) \cap \mathbb{N}) \cup C \right) \cap \mathbb{N} \\ &= \left(((A \cap \mathbb{N}) \cup (B \cap \mathbb{N})) \cup C \right) \cap \mathbb{N} \\ &= (A \cap \mathbb{N}) \cup (B \cap \mathbb{N}) \cup (C \cap \mathbb{N}) \end{aligned}$$

il che dimostra che l'operazione τ è associativa. Un elemento $U \in \mathcal{P}(\mathbb{Z})$ è neutro se per ogni elemento A di $\mathcal{P}(\mathbb{Z})$ vale:

$$A \tau A = (A \cup U) \cap \mathbb{N} = A$$

ma osservando che $(A \cup U) \cap \mathbb{N} = A \iff A \cup U \subseteq \mathbb{N} \wedge (A \cup U) = A \wedge A \subseteq \mathbb{N}$. Quindi in via definitiva la condizione non vale per tutti gli insiemi $B \in \mathcal{P}(\mathbb{Z} \setminus \mathbb{N}) \subseteq \mathcal{P}(\mathbb{Z})$. Quindi non esiste elemento neutro e non avrà senso inoltre cercare elementi simmetrizzabili.

5. L'operazione ω non è commutativa in quanto la differenza simmetrica non gode di tale proprietà:

$$\forall A, B \in \mathcal{P}(\mathbb{Z}) \quad ((X \setminus Y) \cup \{1\} \neq (Y \setminus X) \cup \{1\})$$

Per verificare la proprietà associativa deve valere, per ogni $A, B, C \in \mathcal{P}(\mathbb{Z})$:

$$A \omega (B \omega C) = (A \omega B) \omega C$$

Dove:

$$\begin{aligned} A \omega (B \omega C) &= A \omega ((B \setminus C) \cup \{1\}) \\ &= (A \setminus (B \setminus C) \cap A \setminus \{1\}) \cup \{1\} \\ &= (A \setminus (B \setminus C)) \cup \{1\} \cap A \end{aligned}$$

e:

$$\begin{aligned} (A \omega B) \omega C &= ((A \setminus B) \cup \{1\}) \omega C \\ &= (((A \setminus B) \cup \{1\}) \setminus C) \cup \{1\} \end{aligned}$$

Che rappresentano insiemi diversi. Infatti, considerati gli insiemi:

$$\begin{aligned} A &= \{-3, 4, 5\} \\ B &= \{7, -5, 3\} \\ C &= \{1, 2, 3\} \end{aligned}$$

Si ha:

$$\begin{aligned} A \omega (B \omega C) &= (A \setminus (B \setminus C)) \cup \{1\} \cap A = A \\ (A \omega B) \omega C &= (((A \setminus B) \cup \{1\}) \setminus C) \cup \{1\} = A \cup \{1\} \end{aligned}$$

Quindi ω non è associativa. Un elemento $U \in \mathcal{P}(\mathbb{Z})$ è neutro a destra se e solo se, per ogni parte di \mathbb{Z} si ha:

$$A \omega U = A$$

Ovvero:

$$(A \setminus U) \cup \{1\} = A$$

Ma:

$$\emptyset \omega U = \{1\} \neq \emptyset$$

Quindi non esiste elemento neutro a destra in $\mathcal{P}(\mathbb{Z})$ rispetto a ω . Analogamente a sinistra. ■

Esercizio 5.6.9

Sia $S = \{a, x, y\}$ un insieme di tre elementi e si consideri in S l'operazione $*$ definita in S da questa tavola di Cayley:

*	a	x	y
a	a	x	y
x	x	a	a
y	y	y	a

Dopo aver verificato che a è neutro in $(S, *)$ e aver determinato i simmetrici destri e sinistri degli elementi di S , senza fare ulteriori calcoli si decida se $(S, *, a)$ è un monoide.

Svolgimento. Una struttura algebrica, per essere un monoide deve essere associativa la sua operazione interna ed esistere l'elemento neutro. Osservando la tavola di Cayley si ha che a è elemento neutro. Osservando i simmetrici destri e sinistri degli elementi di S notiamo però che:

$$x * x = x * y = a$$

e se $*$ fosse associativa questo non dovrebbe essere possibile. Infatti in un semigruppo ogni elemento ha al più un simmetrico destro e/o sinistro. Quindi possiamo concludere dicendo che $(S, *, a)$ non è un monoide. ■

Esercizio 5.6.10

Verificare che se $*$ è un'operazione associativa, anche la sua operazione opposta è associativa.

Svolgimento. Se l'operazione $*$ è associativa allora vale, per ogni elemento $a, b, c \in S$:

$$a * (b * c) = (a * b) * c$$

L'operazione opposta $*^*$ definita ponendo:

$$a *^* b := b * a$$

sarà associativa se e solo se:

$$a *^* (b *^* c) = (a *^* b) *^* c$$

Si ha:

$$\begin{aligned} a *^* (b *^* c) &= a *^* (c * b) && \text{Applicando la definizione di } *^* \\ &= (c * a) * b && \text{Applicando la definizione di } *^* \\ &= c * (b * a) && \text{Applicando l'associatività di } * \\ &= (a *^* b) *^* c && \text{Applicando la definizione di } *^* \end{aligned}$$

E l'asserto è dimostrato. ■

Esercizio 5.6.11

Nel monoide delle parole^a su un alfabeto che contenga la lettera y , dire se sono o non sono parti chiuse: l'insieme delle parole di lunghezza (nel senso ovvio) maggiore di 55; l'insieme delle parole di lunghezza pari; l'insieme delle parole che iniziano per y ; l'insieme delle parole che finiscono per yyy ; l'insieme delle parole in cui y appare al massimo tre volte; l'insieme delle parole che se hanno lunghezza maggiore di 10 allora non hanno y tra le lettere che vi appaiono.

^aRispetto all'operazione di concatenazione

Svolgimento. Si ha:

- L'insieme delle parole di lunghezza maggiore di 55 è una parte chiusa. Infatti concatenando due o più parole di questo insieme la stringa risultante sarà sempre di lunghezza maggiore di 55 caratteri;
- L'insieme delle parole di lunghezza pari è una parte stabile;
- L'insieme delle parole che iniziano per y è una parte stabile;
- L'insieme delle parole che terminano per yyy è una parte stabile;
- L'insieme delle parole in cui y appare al massimo tre volte non è una parte stabile;
- L'insieme delle parole che se hanno lunghezza maggiore di 10 allora non hanno y tra le lettere non è una parte stabile. ■

Esercizio 5.6.12

In $D := \mathbb{Z} \times \mathbb{Z}$ si definiscano le operazioni binarie $*$ e \perp ponendo, per ogni $a, b, c, d \in \mathbb{Z}$

$$((a, b) * (c, d)) = (ac, b + d)$$

e per ogni $a, b, c, d \in \mathbb{Z}$

$$((a, b) \perp (c, d)) = (ac, b - d)$$

Studiare $(D, *)$ e (D, \perp) , decidendo che genere di strutture algebriche siano e, nel caso la domanda abbia senso, quali siano i loro elementi simmetrizzabili. Stabilire poi se $\mathbb{Z} \times \{0\}$ e $\mathbb{Z} \times \{1\}$ sono o non sono parti chiuse rispetto a $*$ o rispetto a \perp e studiare, ove esistano, le corrispondenti strutture indotte.

Svolgimento.

1. Iniziamo studiando l'operazione $*$. Per essere associativa, deve valere, *foralla*, $a, b, c, d, e, f \in \mathbb{Z}$,

$$(a, b) * ((c, d) * (e, f)) = ((a, b) * (c, d)) * (e, f)$$

Applicando la definizione di $*$:

$$\begin{aligned} (a, b) * ((c, d) * (e, f)) &= (a, b) * (ce, d + f) \\ &= (ace, b + d + f) \end{aligned}$$

e:

$$\begin{aligned} ((a, b) * (c, d)) * (e, f) &= (ac, b + d) * (e, f) \\ &= (ace, b + d + f) \end{aligned}$$

Quindi $*$ è associativa e la struttura $(D, *)$ è un semigruppo. Per verificare la commutatività verifichiamo se vale l'uguaglianza, per ogni $a, b, c, d \in \mathbb{Z}$:

$$(a, b) * (c, d) = (c, d) * (a, b)$$

la cui verifica è diretta osservando che le operazioni di addizione e moltiplicazione sono commutative:

$$(ac, b + d) = (ca, d + b)$$

Quindi $(D, *)$ è un semigruppo commutativo. Verifichiamo adesso l'esistenza dell'elemento neutro. Essendo $*$ commutativa possiamo effettuare tale ricerca componendo sia a destra che a sinistra. Una coppia di numeri interi positivi è elemento neutro rispetto ad $*$ se, per ogni $a, b \in \mathbb{Z}$:

$$(a, b) * (u, l) = (a, b)$$

Ovvero se:

$$(au, b + l) = (a, b)$$

E ciò accade se e solo se $u = 1$ e $l = 0$. Quindi la coppia $(1, 0)$ risulta essere elemento neutro rispetto a $*$ e $(D, *)$ risulta essere un monoide commutativo. Ci chiediamo ora quali coppie siano simmetrizzabili. Per definizione di elemento simmetrizzabile, una coppia (a, b) ammette simmetrico se esistono a', b' tali che $(a, b) * (a', b') = (1, 0)$. Svolgendo i calcoli si ottiene:

$$(a, b) * (a', b') = (1, 0) \iff (aa', b + b') = (1, 0) \iff \begin{cases} a' = a^{-1} \\ b' = -b \end{cases}$$

Dato che gli unici elementi di \mathbb{Z} ad ammettere inverso sono 1 e -1 mentre tutti gli elementi di \mathbb{Z} ammettono opposto possiamo concludere dicendo che gli elementi simmetrizzabili in $(D, *)$ sono tutte e sole le coppie del tipo $(1, b)$ e $(-1, b)$ con $b \in \mathbb{Z}$. Quindi, in particolare $(D, *)$ non risulta essere un gruppo. Consideriamo ora gli insiemi $\mathbb{Z} \times \{0\} = \{(a, 0) \mid a \in \mathbb{Z}\}$. Componendo due elementi di tale insieme si ottiene:

$$(a, 0) * (b, 0) = (ab, 0)$$

che è ancora un elemento di $\mathbb{Z} \times \{0\}$ e $(\mathbb{Z} \times \{0\}, *_{\mathbb{Z} \times \{0\}})$ è una parte stabile di $(D, *)$.

2. Consideriamo adesso l'operazione \perp e verifichiamo se vale la proprietà associativa. Per ogni coppia $(a, b), (c, d), (e, f)$ abbiamo:

$$((a, b) \perp (c, d)) \perp (e, f) = (ac, b - d) \perp (e, f) = (ace, b - d - f)$$

e

$$(a, b) \perp ((c, d) \perp (e, f)) = (ace, b - d + f)$$

Quindi (D, \perp) non è un semigruppo e non ha senso continuare con lo studio. ■

Esercizio 5.6.13

Sia $S = \{0, 1\}$. Elencare gli elementi di $T(S)$ e scrivere la tavola di Cayley di $T(S)$.

Svolgimento. Si ha $T(S) = \{id_S, c_0, c_1, \sigma\}$ dove σ è la trasposizione che sposta 0 in 1 e 1 in 0. Abbiamo quindi:

o	id_S	c_0	c_1	σ
id_S	id_S	c_0	c_1	σ
c_0	c_0	c_0	c_0	c_0
c_1	c_1	c_1	c_1	c_1
σ	σ	c_1	c_0	id_S

RETICOLI E ALGEBRE DI BOOLE

6.1

RELAZIONI D'ORDINE



Definizione 6.1.1: Relazione d'ordine

Sia S un insieme non vuoto. Una relazione binaria ρ in S si dice una **relazione d'ordine largo** se è:

1. **Riflessiva:** $\forall x \in S(x \rho x)$;
2. **Antisimmetrica:** $\forall x, y \in S((x \rho y \wedge y \rho x) \Rightarrow x = y)$;
3. **Transitiva:** $\forall x, y, z \in S((x \rho y) \wedge (y \rho z) \Rightarrow x \rho z)$.

Una relazione binaria ρ in S si dice una **relazione d'ordine stretto** se è :

- **Antiriflessiva:** $\forall x \in S(x \not\rho x)$.
- **Transitiva**

Osservazione 6.1.1



Chiaramente ogni relazione di ordine stretto è necessariamente antisimmetrica. Infatti, sia ρ una relazione di ordine stretto e siano $x, y \in A$ tali che $x \rho y \wedge y \rho x$. Per la proprietà transitiva deve essere $x \rho x$ ma per ipotesi ρ è antiriflessiva. Questo vuol dire che non può essere $x \rho y \wedge y \rho x$ e quindi risulta vera l'implicazione $(x \rho y \wedge y \rho x) \implies (x = y)$ in quanto l'antecedente risulta falsa.

Una relazione d'ordine in S è in genere denotata, col simbolo \leq .

Proposizione 6.1.1

Sia **OL(A)** l'insieme di tutte le relazioni di ordine largo in A e **OS(A)** l'insieme di tutte le relazioni di ordine stretto in A . Per ogni $\rho \in OL(A)$ è possibile definire $\rho_{\neq} \in Rel(A)$ in modo tale che, $\forall x, y \in A$:

$$(x \rho_{\neq} y \iff (x \rho y \wedge x \neq y)) \implies \rho_{\neq} \in OS(A)$$

Dimostrazione. Dimostriamo che la relazione ρ_{\neq} gode della proprietà antiriflessiva e transitiva:

- **Antiriflessiva:** si ha che per ogni $x \in A$ ($x \rho_{\neq} x$) poiché $x = x$ e $x \rho x$ dato che $\rho \in OL(A)$;
- **Transitività:** per ogni $x, y, z \in A$ tali che $x \rho_{\neq} y \wedge y \rho_{\neq} z$ si ha:

$$\begin{aligned}(x \rho_{\neq} y \wedge y \rho_{\neq} z) &\implies (x \rho y \wedge x \neq y) \wedge (y \rho z \wedge y \neq z) \\ &\implies x \rho z \wedge x \neq z\end{aligned}$$

Per ipotesi
Sfruttando la transitività di ρ

Proposizione 6.1.2

Per ogni $\sigma \in OS(A)$ è possibile definire $\sigma_+ \in Rel(A)$ in modo tale che, per ogni $x, y \in A$:

$$(x \sigma_+ y \iff (x \sigma y \vee x = y)) \implies \sigma_+ \in OL(A)$$

Dimostrazione. Dimostriamo che ρ_+ è riflessiva, antisimmetrica e transitiva:

- **Riflessiva:** per ogni $x \in A$ si ha $x \rho_+ x$ poiché $x = x$;
- **Antisimmetria:** negando la proprietà devono esistere $x, y \in A$ per i quali $(x \sigma_+ y \wedge y \sigma_+ x \wedge x \neq y)$ il che sarebbe equivalente a dire che $((x \sigma y \vee x = y) \wedge (y \sigma x \vee y = x) \wedge (x \neq y))$, ovvero $(x \sigma y) \wedge (y \sigma x) \wedge (x \neq y)$ il che è assurdo in quanto σ è antisimmetrica. Quindi σ_+ è antisimmetrica.
- **Transitività:** per ogni $x, y, z \in A$ tali che $x \sigma y$ e $y \sigma z$ si ha:

$$x \sigma y \wedge y \sigma z \implies (x \sigma y \vee x = y) \wedge (y \sigma z \vee y = z)$$

Nel caso in cui $x = y \wedge y = z$ si ha $x = z$, ovvero $x \sigma_+ z$. Altrimenti, da $x \sigma y \wedge y \sigma z$ segue $x \sigma z$ e, per la transitività di σ si ottiene $x \sigma_+ z$.

□

Proposizione 6.1.3

Le applicazioni $\rho \in OL(A) \mapsto \rho_+ \in OS(A)$ e $\sigma \in OS(A) \mapsto \sigma_+ \in OL(A)$ sono biettive e l'una l'inversa dell'altra.

Dimostrazione. Sia $\bar{\rho}$ la relazione duale di ρ e sia $(\bar{\rho})^\#$ il suo grafico. Definiamo:

1. ρ antiriflessiva se e soltanto se: $\Delta_A \cap \rho^\# = \emptyset$;
2. ρ antisimmetrica se e soltanto se: $\rho^\# \cap (\bar{\rho})^\# \subseteq \Delta_A$;

Inoltre, si ha $(\rho_+)^\# = \rho^\# \setminus \Delta_A$ e $(\sigma_+)^\# = \sigma^\# \cup \Delta_A$. Allora il grafico di $(\rho_+)^\#$ risulta:

$$((\rho_+)^\#)^\# = (\rho^\# \setminus \Delta_A) \cup \Delta_A = \rho^\#$$

dualmente per $(\sigma_+)^\#$

□

! La relazione identica ι_S è una relazione d'ordine in S , ed è chiaro che ι_S è l'unica relazione di equivalenza in S che sia anche una relazione d'ordine.

Osservazione 6.1.2



Qualunque sia l'insieme S , la relazione binaria ρ in $\mathcal{P}(S)$, definita ponendo:

$$x \rho y \iff x, y \in \mathcal{P}(S) \wedge x \subseteq y$$

è una relazione d'ordine in $\mathcal{P}(S)$ chiamata **relazione di inclusione** e denotata con il simbolo \subseteq .

Esempio 6.1.1

Un esempio di relazione d'ordine stretto è fornito dalla relazione binaria ρ , definita nell'insieme $\mathcal{P}(S)$ delle parti di un insieme S ponendo:

$$x \rho y \iff x \subset y$$

cioè se e soltanto se:

$$x \subseteq y \wedge x \neq y$$

Tale relazione viene denotata col simbolo \subset .

Esempio 6.1.2

Sia (\mathbb{N}, \cdot) un monoide abeliano. La relazione di divisibilità $|$ in (\mathbb{N}, \cdot) indicata da $|$ oppure da $|_{(\mathbb{N}, \cdot)}$ è definita dalla formula:

$$\forall a, b \in S (a | b \iff \exists c \in \mathbb{N} (b = ac)) \quad (6.1)$$

è una relazione di ordine parziale:

1. Per ogni $a \in \mathbb{N}$ ($a | a$), infatti $a = a \cdot 1$.
2. Per ogni scelta di $a, b \in \mathbb{N}$, se $a | b$ e $b | a$, allora $a = b$: infatti esistono $q, q' \in \mathbb{N}$ tali che $b = a \cdot q$, $a = b \cdot q'$, quindi $a = a \cdot q \cdot q'$ e $a \cdot (1 - q \cdot q') = 0$; se $a \neq 0$ deve essere $1 - q \cdot q' = 0$, per cui $q = q' = 1$ e $a = b$; se invece $a = 0$, anche $b = 0$ e dunque nuovamente $a = b$;
3. Per ogni scelta di $a, b, c \in \mathbb{N}$, se $a | b$ e $b | c$, allora $a | c$. Infatti, siano q e $q' \in \mathbb{N}$ tali che $b = a \cdot q$ e $c = b \cdot q'$ allora $c = a \cdot (q \cdot q')$.

Altri risultati importanti sulla relazione di divisibilità saranno mostrati nella sezione 7.1.3.

6.1.1 ■ Insiemi ordinati

Definizione 6.1.2: Insieme ordinato

Sia S un insieme non vuoto e sia \leq una relazione d'ordine in S . La coppia (S, \leq) si chiama **insieme ordinato** (parzialmente), e l'insieme S si dice **sostegno** di tale insieme ordinato.

Esempio 6.1.3

Sono insiemi ordinati:

$$(\mathbb{R}, \leq) \quad (\mathbb{Q}, \leq) \quad (\mathbb{Z}, \leq) \quad (\mathbb{N}, \leq)$$

dove \leq è l'ordine usuale (ad esempio definito su \mathbb{R} da $x \leq y$ se $y - x \geq 0$, ovvero se esiste $a \in \mathbb{R}$ tale che $y - x = a^2$).

Definizione 6.1.3: Relazione d'ordine totale

Se (S, \leq) è un insieme ordinato, gli elementi x e y di S si dicono **confrontabili** se risulta $x \leq y$ oppure $y \leq x$, cioè se il grafico di \leq contiene almeno una delle coppie (x, y) e (y, x) . Se due qualunque elementi di S sono confrontabili allora la relazione \leq si dice una **relazione d'ordine totale** e la coppia (S, \leq) è un **insieme totalmente ordinato**.

Esempio 6.1.4

1. $(\mathcal{P}(X), \subseteq)$ non è un insieme totalmente ordinato se X ha più di due elementi. Infatti, se a_1, a_2 sono elementi distinti di X , allora $\{a_1\}, \{a_2\} \in \mathcal{P}(X)$ e $\{a_1\} \not\subseteq \{a_2\}, \{a_2\} \not\subseteq \{a_1\}$. In questo caso diremo che $(\mathcal{P}(X), \subseteq)$ è un insieme **parzialmente ordinato**.
2. L'insieme ordinato $(\mathbb{N}, |)$ non è totalmente ordinato. Basta considerare gli elementi 2 e 3 per vedere che $2 \nmid 3$ e $3 \nmid 2$.
3. Gli insiemi $(\mathbb{R}, \leq), (\mathbb{Q}, \leq), (\mathbb{Z}, \leq)$, dove \leq è l'ordine usuale, sono totalmente ordinato.

Definizione 6.1.4: Funzioni crescenti

Se (S, ρ) e (T, σ) sono insiemi ordinati, un'applicazione $f : S \rightarrow T$ si dice **crescente** se e soltanto se:

$$\forall a, b \in S (a \rho b \implies f(a) \sigma f(b)) \quad (6.2)$$

Teorema 6.1.1 (Isomorfismi tra insiemi ordinati)

Siano (S, \leq_S) e (T, \leq_T) due insiemi ordinati. Si dice che $f : S \rightarrow T$ è un isomorfismo^a tra le strutture (S, \leq_S) e (T, \leq_T) se e soltanto se:

1. f è biettiva;
2. f è crescente da (S, \leq_S) a (T, \leq_T) : $\forall x, y \in S (x \leq_S y \implies f(x) \leq_T f(y))$;
3. f^{-1} è crescente da (T, \leq_T) a (S, \leq_S) : $\forall x, y \in T (x \leq_T y \implies f^{-1}(x) \leq_S f^{-1}(y))$.

^aDetto anche **isomorfismo d'ordine**

6.1.2 ■ Minimo, massimo, minimali e massimali

Definizione 6.1.5: Minimo e massimo di un insieme

Sia (S, \leq) un insieme ordinato, e sia X una parte non vuota di S . Un elemento \bar{x} di X si dice **minimo** di X se risulta:

$$\forall x \in X (\bar{x} \leq x)$$

L'eventuale minimo della parte non vuota X di S si denota col simbolo $\min X$. Un elemento $\bar{x} \in X$ si dice invece **massimo** se risulta:

$$\forall x \in X (x \leq \bar{x})$$

L'eventuale massimo di X si denota col simbolo $\max X$.

Definizione 6.1.6: Elementi minimali e massimali

Sia (S, \leq) un insieme ordinato. Un elemento x di S si dice **minimale** se non esiste alcun elemento y di S tale che $y < x$. Si dice invece che x è un elemento **massimale** di S se non esiste alcun elemento $y \in S$ tale che $x < y$.

Dalle definizioni segue, in particolare, che ogni elemento massimo (minimo) è anche un elemento massimale (minimale). Non sempre, però, vale il contrario. Osserviamo anche che un insieme ordinato può avere diversi elementi minimali (o massimali).

Esempio 6.1.5

1. Qualunque sia l'insieme S , nell'insieme ordinato $(\mathcal{P}(S), \subseteq)$ si ha:

$$\begin{aligned}\min \mathcal{P}(S) &= \emptyset \\ \max \mathcal{P}(S) &= S\end{aligned}$$

2. L'insieme ordinato $(\mathbb{N}, |)$ ha minimo 1, infatti $1 | n$ per ogni $n \in \mathbb{N}$, e massimo 0, infatti $n | 0$ per ogni $n \in \mathbb{N}$. Se però togliamo 0 e consideriamo $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$, l'insieme ordinato $(\mathbb{N}^*, |)$ non ha massimo.
3. Nell'insieme ordinato $(\mathbb{N} \setminus \{1\}, |)$ dei numeri naturali diversi da 1 ordinato per divisibilità, gli elementi minimali sono tutti i numeri primi (positivi).
4. Consideriamo, per un $n \in \mathbb{N}$, l'insieme $\text{Div}(n) = \{a \in \mathbb{N} \mid a | n\}$ dei divisori di n . Chiaramente in $(\text{Div}(n), |)$ si ha $\min(\text{Div}(n)) = 1$ e $\max(\text{Div}(n)) = n$.
5. Consideriamo l'insieme $\{1, 2, 3\}$ ordinato dalla divisibilità. Così:

$$1 | 2, \quad 1 | 3, \quad 2 \nmid 3, \quad 3 \nmid 2$$

Quindi 1 è minimo (minimale), mentre 2, 3 sono massimali, ma non massimi.

6. Sia $Z = \{1, 2, 3\}$ e sia $X = \{A \in \mathcal{P}(Z) \mid |A| \text{ è pari}\}$. Allora $\emptyset = \min(X)$, e dunque è l'unico elemento minimale di X , mentre $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$ sono elementi massimali di (X, \subseteq) .

Proposizione 6.1.4

Se $x \in (S, \leq)$ è il minimo allora x è l'unico minimale. (Rispettivamente con il massimo).

Dimostrazione. Supponiamo esista un elemento y' minimale in (S, \leq) allora deve valere:

$$(y' \text{ minimale in } S) \implies (y' \leq x)$$

Sappiamo però che x è il minimo in (S, \leq) , quindi per ogni elemento $y \in S$ vale sicuramente $(x \leq y)$. Allora, mettendo insieme le due proprietà varrebbero contemporaneamente:

$$((x \leq y') \wedge (y' \leq x)) \implies x = y'$$

□

Il minimo ed il massimo di un insieme, se esistono sono unici. In un insieme totalmente ordinato, *il concetto di minimo e minimale coincidono*. Analogamente con massimo e massimale.

Teorema 6.1.2

Sia (S, ρ) un insieme ordinato finito non vuoto. Allora (S, \leq) ha elementi minimali ed elementi massimali.

Dimostrazione. Supponiamo che (S, \leq) non abbia minimi. Poiché $S \neq \emptyset$ allora esiste un elemento $x_0 \in S$. Fissato tale elemento, sicuramente questo non sarà un elemento minima (in quanto abbiamo assunto che non sono presenti in S), allora esiste un elemento $x_1 \in S$ tale che $x_1 < x_0$ con x_1 non minima. Allora possiamo considerare un ulteriore elemento $x_2 \in S$ e $x_2 < x_1 < x_0$. Proseguendo in questo modo è possibile definire una successione $(x_n)_{n \in \mathbb{N}}$ di elementi di S tale che:

$$\forall i, j \in \mathbb{N} (i < j \implies x_i < x_j)$$

Quindi:

$$\forall i, j \in \mathbb{N} (i \neq j \implies x_i \neq x_j)$$

Allora, l'insieme $\{x_i \mid i \in \mathbb{N}\}$ è una parte infinita di S , il che chiaramente è assurdo in quanto S è un insieme finito. Allora S deve avere per forza degli elementi minimi. (In maniera analoga si dimostra l'esistenza degli elementi massimi). \square

6.1.3 ■ Intervalli e coperture

Definizione 6.1.7: Intervallo

Siano S un insieme, \leq una relazione d'ordine in S , $<$ la corrispondente relazione d'ordine stretto e $a, b \in S$. Definiamo gli **intervalli**:

- **Chiuso:** $[a, b] = \{x \in S \mid a \leq x \leq b\}$
- **Aperto:** $]a, b[= \{x \in S \mid a < x < b\}$
- **Semiacerto a destra:** $[a, b[= \{x \in S \mid a \leq x < b\}$
- **Semiacerto a sinistra:** $]a, b] = \{x \in S \mid a < x \leq b\}$

Definizione 6.1.8: Copertura

Sia (S, \leq) un insieme ordinato e siano $a, b \in S$ tali che $a < b$. Diciamo che b **copre** a oppure che a è coperto da b se e solo se $]a, b[= \emptyset$, ovvero se, e soltanto se:

$$a < b \wedge (\neg(\exists c \in S)(a < c < b))$$

Ovvero se non esistono elementi di S strettamente compresi tra a e b . In questo caso scriviamo $a \lessdot b$.

Lemma 6.1.1

Per ogni $a, b \in S$ sono equivalenti:

1. $a \lessdot b$;
2. $a < b \wedge \neg(\exists c \in S)(a < c < b)$;
3. a è un elemento massimale in $(\{x \in S \mid x < b\}, \leq)$;
4. b è un elemento minima in $(\{x \in S \mid a < x\}, \leq)$;

Esempio 6.1.6

1. Nell'insieme ordinato (\mathbb{N}, \leq) , $x \in \mathbb{N}$ è coperto da y se, e soltanto se $y = x + 1$. Analogamente, in (\mathbb{Z}, \leq) l'elemento 2 è coperto da 3. In generale, $\forall n \in \mathbb{Z}$, n è coperto solo da $n + 1$.
2. In (\mathbb{R}, \leq) nessun elemento copre alcun elemento di \mathbb{R} : $\forall a, b \in \mathbb{R} (\neg(a \lessdot b))$.
3. In $(\mathcal{P}(\mathbb{N}), \subseteq)$, l'elemento \emptyset è coperto da tutti e soli i singleton degli elementi di \mathbb{N} .

L'insieme $\{(x, y) \mid x, y \in S \wedge x < y\}$ è un sottoinsieme del grafico della relazione d'ordine \leq in S e in particolare è una relazione d'ordine che prende il nome di **relazione di copertura**. Se S è un insieme finito allora $<$ determina \leq . Infatti vale il seguente teorema.

Teorema 6.1.3

Sia (S, \leq) un insieme ordinato finito e siano $a, b \in S$. Allora si ha che $a \leq b$ se e soltanto se esistono n elementi $x_0, x_1, \dots, x_{n-1} \in S$ tali che:

1. $x_0 = a$
2. $x_{n-1} = b$
3. $\forall j \in \{i \in \mathbb{N} \mid i < n\} (x_j < x_{j+1})$

Dimostrazione. Abbiamo:

\Leftarrow Se esiste $n \in \mathbb{N}$ e x_0, \dots, x_{n-1} elementi di S con le proprietà richieste allora, se $n = 0$ si ha $a = x_0 = b$ e allora $a \leq b$. Se $n > 0$ si ha $a = x_0 \lessdot x_1 \lessdot \dots \lessdot x_{n-1} = b$, ovvero $a \leq b$.

⇒ Sia $a \leq b$ per ipotesi.

1. Se $a = b$ allora si ottiene la condizione richiesta ponendo $n = 0$ e $x_0 = a = b$. Infatti, per $n = 0$ l'insieme: $\{i \in \mathbb{N} \mid i < 0\}$ è vuoto, dunque $\forall j \in \{i \in \mathbb{N} \mid i < 0\} (x_j < x_{j+1})$ risulta vera in quanto l'antecedente risulta falsa.
2. Sia $(a \neq b \implies a < b)$, poniamo $x_0 = a$ e si consideri l'intervallo $X =]a, b[$. Siccome X è finito deve essere $X = \emptyset$ oppure (X, \leq) ha un elemento minimale x_1 . Se $X = \emptyset$ allora $a < b$, quindi basta porre $n = 1$ e $x_0 = a, x_1 = b$. Se invece $X \neq \emptyset$ consideriamo l'intervallo $]x_1, b[$.
 - Se $]x_1, b[= \emptyset$ allora $x_1 < b$ e quindi basta porre $n = 2$ e $x_2 = b$
 - Se $]x_1, b[\neq \emptyset$, dato che è un insieme finito possiamo scegliere un elemento minimale x_2 e considerare l'intervallo $]x_2, b[$.

Procedendo in questo modo è possibile costruire una sequenza di elementi di S tali che $a = x_0 < x_1 < \dots < x_{n-1} = b$ ottenuto ricorsivamente. Poiché S è finito e gli elementi x_i sono a due a due distinti la costruzione deve necessariamente arrestarsi. Si trova quindi $i \in \mathbb{N}$ tale che $x_i = b$. Ponendo $n - 1 = i$ si ottiene l'enunciato.

□

Da questo teorema possiamo quindi affermare che gli insiemi ordinati finiti sono *codificati* dalla loro relazione di copertura.

6.1.4 ■ Diagrammi di Hasse

Definizione 6.1.9: Diagramma di Hasse

Sia (S, \leq) un insieme ordinato finito. Rappresentiamo gli elementi di S come punti del piano, col vincolo che, se $a, b \in S$ e $a < b$, il punto che rappresenta b sia disegnato più in alto rispetto al punto che rappresenta a . Si traccia una linea tra due punti a e b se e solo se b copre a . La figura così ottenuta è un **diagramma di Hasse**.

Osservazione 6.1.3 ➤➤

Il diagramma di Hasse di un insieme totalmente ordinato finito è “banale”: non è altro che un insieme di punti uno sopra l'altro, dove un punto è collegato a quello che gli sta sopra da un segmento verticale orientato verso l'alto.



Figura 6.1: Diagramma di Hasse dell'insieme totalmente ordinato (\mathbb{N}, \leq)

Esempio 6.1.7

Si consideri l'insieme $S = \{1, 2, 3\}$ con la relazione d'ordine usuale. Il diagramma 6.2 non rappresenta un diagramma di Hasse in quanto $1 \not\leq 3$. Infatti: $]1, 3[= \{2\} \neq \emptyset$.

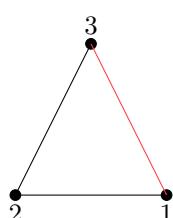


Figura 6.2

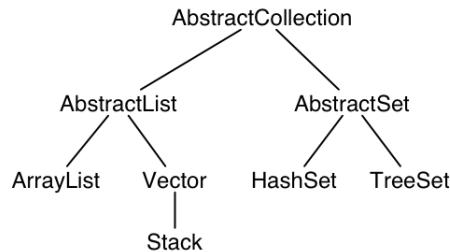
Esempio 6.1.8

Si consideri l'insieme $S = \{1, 2, 3\}$ ordinato mediante la relazione identica, o d'uguaglianza id_S . Chiaramente ogni elemento, essendo diverso da ogni altro elemento dell'insieme, sarà in relazione solo con se stesso. Il diagramma di Hasse che ne deriva prende il nome di **anticatena**:



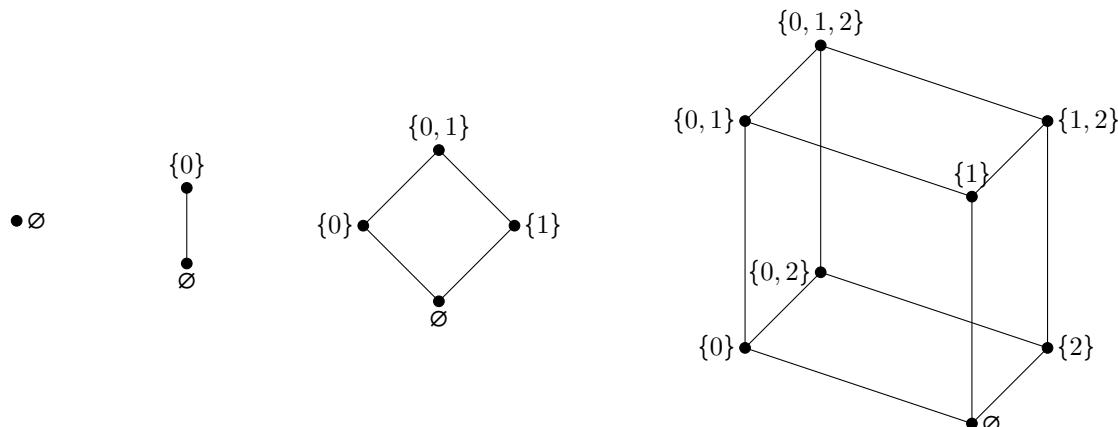
Esempio 6.1.9

Le classi in `java.util` ordinate mediante la relazione gerarchica formano un insieme parzialmente ordinato in quanto non tutte le classi sono in relazione tra di loro (ad esempio `Vector` e `HashSet`). Si ottiene il seguente diagramma delle classi che non è altro che un diagramma di Hasse dell'insieme ordinato:

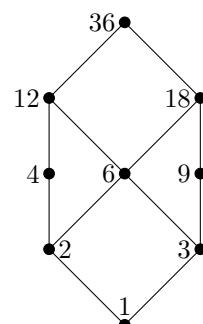


Esempio 6.1.10

1. Si consideri l'insieme ordinato $(\mathcal{P}(I_n), \subseteq)$ nel caso in cui I_n sia l'insieme vuoto, I_n abbia un solo elemento, due e tre elementi. Ricordiamo che $I_n = \{x \in \mathbb{N} \mid x \leq n\}$. Si ottengono quindi i diagrammi mostrati in Figura:



2. Consideriamo l'insieme $Div(36) = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$ ordinato secondo la divisibilità. Il suo diagramma di Hasse è:



Due insiemi si dicono **isomorfi** se hanno lo stesso diagramma di Hasse. Il duale di un diagramma di Hasse (ovvero il diagramma di Hasse della sua relazione opposta) si ottiene ruotando il grafico di 180° .

Esempio 6.1.11

Consideriamo l'insieme ordinato $(\mathbb{N}, |)$ e costruiamone il diagramma di Hasse (parziale):

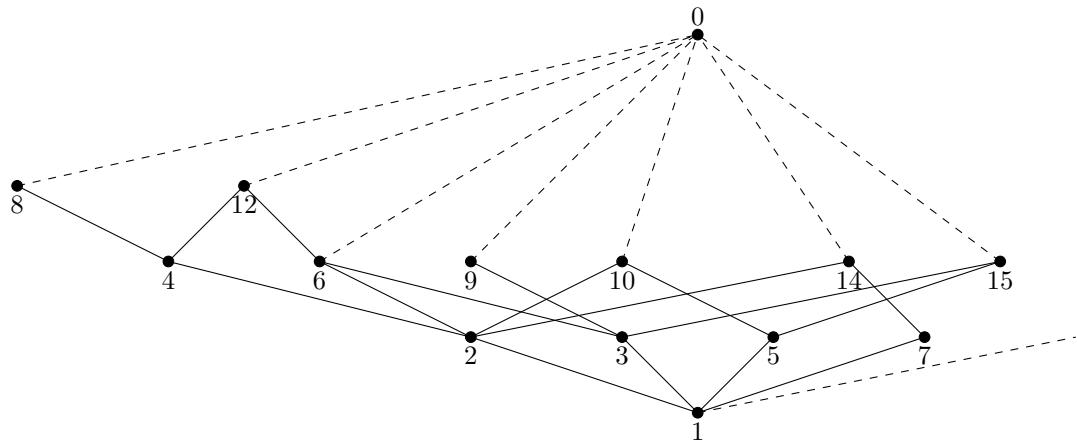


Figura 6.3: Diagramma di Hasse dell'insieme ordinato $(\mathbb{N}, |)$.

6.1.5 ■ Maggioranti, minoranti, estremo superiore ed inferiore

Definizione 6.1.10: Maggioranti e minoranti

Sia (S, \leq) un insieme ordinato, e sia X una parte non vuota di S . Un elemento $a \in S$ si dice **minorante** di X se risulta $a \leq x$ per ogni x in X . Si dice invece che a è un **maggiorante** di X se $x \leq a$ per ogni $x \in X$.

Definizione 6.1.11: Insiemi inferiormente e superiormente limitati

Una parte $X \subseteq S$ si dice **inferiormente limitata** se è dotata di minoranti, mentre X si dice **superiormente limitata** se è dotata di maggioranti.

L'insieme dei minoranti di X si denota col simbolo:

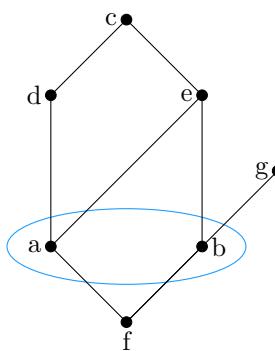
$$X_{(S, \leq)}^{\downarrow} = \{a \in S \mid \forall x \in X (a \leq x)\} \quad (6.3)$$

Mentre l'insieme dei maggioranti si denota col simbolo:

$$X_{(S, \leq)}^{\uparrow} = \{a \in S \mid \forall x \in X (x \leq a)\} \quad (6.4)$$

Esempio 6.1.12

Si consideri il seguente diagramma di Hasse:



Si ha che l'insieme dei maggioranti di $\{a, b\}$ è dato da:

$$\{a, b\}^{\uparrow} = \{c, e\}$$

mentre l'insieme dei minoranti di $\{a, b\}$ è:

$$\{a, b\}^{\downarrow} = \{f\}$$

Esempio 6.1.13

Sia $(\mathcal{P}(S), \subseteq)$ allora, per un sottoinsieme $X \subseteq S$:

$$X^\uparrow = \{Y \in \mathcal{P}(S) \mid \forall c \in \bigcup X (c \in Y)\} = \{Y \in \mathcal{P}(S) \mid \bigcup X \subseteq Y\} \quad (6.5)$$

$$X^\downarrow = \{Y \in \mathcal{P}(S) \mid \forall x \in X (Y \subseteq x)\} = \begin{cases} \{Y \in \mathcal{P}(S) \mid Y \subseteq \bigcap X\} & \text{se } X \neq \emptyset \\ \{Y \mid Y \in \mathcal{P}(S)\} = \mathcal{P}(S) & \text{se } X = \emptyset \end{cases} \quad (6.6)$$

Sia $S = \mathbb{N}$ e sia $X = \{\{1, 2\}, \{2, 3\}\}$. Allora:

$$\begin{aligned} X^\uparrow &= \{Y \in \mathcal{P}(\mathbb{N}) \mid \bigcup X \subseteq Y\} = \{Y \in \mathcal{P}(\mathbb{N}) \mid \{1, 2, 3\} \subseteq Y\} \\ X^\downarrow &= \{Y \in \mathcal{P}(\mathbb{N}) \mid Y \subseteq \bigcap X\} = \{Y \in \mathcal{P}(\mathbb{N}) \mid Y \subseteq \{2\}\} = \{\emptyset, \{2\}\} \end{aligned}$$

Definizione 6.1.12: Estremo inferiore e superiore

Sia (S, \leq) un insieme ordinato, e sia X una parte inferiormente limitata di S . Allora l'insieme dei minoranti di X è una parte non vuota di S , il cui eventuale massimo si chiama **estremo inferiore** di X e si denota col simbolo $\inf_{(S, \leq)} X$. Se invece X è una parte superiormente limitata di S , l'eventuale minimo dell'insieme dei maggioranti di X si chiama **estremo superiore** di X e si denota col simbolo $\sup_{(S, \leq)} X$:

$$\inf_{(S, \leq)} X = \max(X_{(S, \leq)}^\downarrow) \quad (6.7)$$

$$\sup_{(S, \leq)} X = \min(X_{(S, \leq)}^\uparrow) \quad (6.8)$$

Esempio 6.1.14

Sia $X = \{C \in \mathcal{P}(\{1, 2, 3, 4, 5, 6\}) \mid |C| \text{ è pari}\}$, ordinato mediante l'inclusione. Sia $A = \{\{1, 2\}, \{1, 3\}, \{2, 5\}\} \subseteq X$. Allora abbiamo $A^\downarrow = \{\emptyset\}$ e $A^\uparrow = \{\{1, 2, 3, 5\}, \{1, 2, 3, 4, 5, 6\}\}$. Dunque:

$$\begin{aligned} \inf(A) &= \max(A^\downarrow) = \emptyset \\ \sup(A) &= \min(A^\uparrow) = \{1, 2, 3, 5\} \end{aligned}$$

Osservazione 6.1.5

Se S è un insieme ordinato non costituito da un solo elemento, nell'insieme ordinato $(\mathcal{P}(S) \setminus \{\emptyset\}, \subseteq)$ gli elementi minimali sono i sottoinsiemi del tipo $\{x\}$, con $x \in S$. Similmente, è chiaro che se l'insieme ordinato S è dotato di massimo, questo è l'unico elemento massimale. D'altra parte, qualunque sia l'insieme S non costituito da un solo elemento, per ogni $x \in S$ il sottoinsieme $S \setminus \{x\}$ è un elemento massimale dell'insieme ordinato $(\mathcal{P}(S) \setminus \{S\}, \subseteq)$.

Teorema 6.1.4

Sono equivalenti le seguenti affermazioni:

1. $a \leq b$
2. $a = \min\{a, b\}$
3. $a = \inf\{a, b\}$
4. $a \in \{a, b\}^\downarrow$

Osservazione 6.1.6

Riprendiamo il Diagramma di Hasse dell'insieme ordinato $(\mathbb{N}, |)$ (Figura 6.3). Per ogni coppia (a, b) vale:

$$\inf\{a, b\} = MCD(a, b) \quad (6.9)$$

$$\sup\{a, b\} = mcm(a, b) \quad (6.10)$$

Infatti, il massimo comun divisore di a e b è il più grande numero che divide a e b , ovvero risulta essere il massimo dei minoranti secondo la relazione di divisibilità. Analogamente, il minimo comune multiplo risulta essere il minimo dell'insieme dei maggioranti (i multipli comuni di a e b per l'appunto).

Esempio 6.1.15

Sia (A, \leq) l'insieme ordinato definito dal diagramma di Hasse mostrato in Figura 6.4 e sia $B = \{c, d, e\}$:

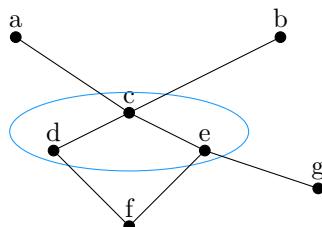


Figura 6.4

L'insieme dei maggioranti di B è:

$$B^\uparrow = \{a, b, c\}$$

e risulta $\sup B = c$ poiché $c \in B$, c è l'elemento massimo di B . L'insieme dei minoranti di B è $\{f\}$ e quindi $\inf B = f$. Poiché $f \notin B$ allora non esiste il minimo di B . Osserviamo che g non precede d e quindi non è un minorante di B .

Esempio 6.1.16

Sia (A, \leq) l'insieme ordinato definito dal diagramma di Hasse in Figura 6.5 e sia $B = \{d, e, f\}$. L'insieme dei maggioranti di B è

$$B^\uparrow = \{a, b, c\}$$

e risulta $\sup B = c$. Poiché $c \notin B$ allora il massimo di B non esiste. L'insieme dei minoranti di B è

$$B^\downarrow = \{f, h\}$$

e risulta $\inf B = f$. Poiché $f \in B$, f è l'elemento minimo di B (osserviamo che g non è un minorante di B).

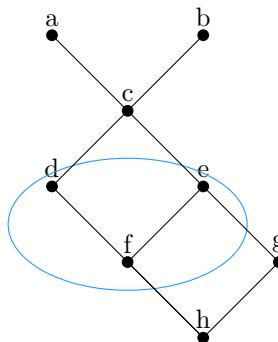


Figura 6.5

Esempio 6.1.17

Sia (A, \leq) l'insieme ordinato definito dal diagramma di Hasse in Figura 6.6 e sia $B = \{b, c, d\}$. L'insieme dei maggioranti di B è

$$B^\uparrow = \{a, b\}$$

e risulta $\sup B = b$. Poiché $b \in B$, b è il massimo di B . L'insieme dei minoranti di B è $B^\downarrow = \{e, f\}$ Poiché gli elementi e, f sono non confrontabili, $\inf B$ non esiste.

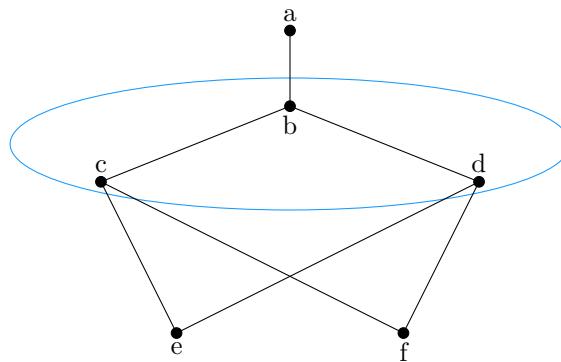


Figura 6.6



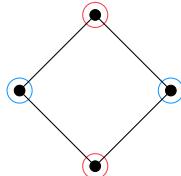
Definizione 6.2.1: Reticolo

Sia (S, \leq) un insieme parzialmente ordinato. S si dice **reticolo** se e solo se:

$$\forall a, b \in S (\exists \inf_{(S, \leq)}(\{a, b\}) \wedge \exists \sup_{(S, \leq)}(\{a, b\})) \quad (6.11)$$

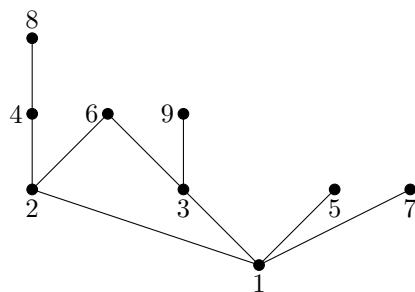
Esempio 6.2.1

- Si consideri il seguente diagramma di Hasse:



Per verificare che tale diagramma rappresenti un reticolo basterà osservare che le coppie non confrontabili (evidenziate in blu) abbiano sia un estremo superiore che un estremo inferiore (evidenziati in rosso).

- L'insieme dei numeri naturali, \mathbb{N} , ordinato mediante la divisibilità, è un reticolo.
- L'insieme $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, ordinato mediante la divisibilità, non è un reticolo. Infatti, per esempio, $\sup(\{6, 9\})$ non esiste.



- L'insieme $\text{Div}(36) = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$, ordinato mediante la divisibilità, è un reticolo.

Proposizione 6.2.1

Sia (S, \leq) un reticolo e consideriamo $a \in S$. L'elemento a è minimale in S se e soltanto se $a = \min(S, \leq)$. Dualmente per gli elementi massimali.

Dimostrazione. \Leftarrow La condizione è chiaramente sufficiente.

\Rightarrow Sia a un elemento minimale. Per ogni $b \in S$ poniamo $X = \{a, b\}$ e sia $c = \inf(X) = \max(X^\downarrow)$, allora $c \leq a$ e $c \leq b$. Tuttavia, essendo a minimale deve essere $c = a$ e quindi $a \leq b$ per ogni $b \in S$. Quindi, per definizione di minimo si ha l'asserto. □

Osservazione 6.2.1



Per ogni $a, b \in (S, \leq)$ ($a \leq b \iff a = \inf\{a, b\} \iff b = \sup\{a, b\}$). Inoltre, se $X \subseteq S$ ed esiste $x = \inf(X)$ allora, essendo l'estremo inferiore il massimo dei minoranti, vale: $X^\downarrow = \{x\}^\downarrow$.

Definizione 6.2.2: Reticolo limitato e completo

Un reticolo si dice **limitato** se ammette minimo e massimo. Un reticolo si dice **completo** se ogni sua parte non vuota è dotata di estremo inferiore e superiore. Ogni reticolo completo è anche limitato.

Osservazione 6.2.2



Un reticolo finito non vuoto è sempre limitato. Il viceversa non vale: ci sono dei reticolini infiniti che sono limitati. Ad esempio se A è un insieme infinito, $\mathcal{P}(A)$ è limitato, infatti si ha che il massimo di $\mathcal{P}(A)$ è A stesso mentre il minimo è rappresentato dall'insieme vuoto. Il reticolo (\mathbb{N}, \leq) ha minimo, il numero naturale 0, ma non ha massimo. Quindi non è un reticolo limitato.

Proposizione 6.2.2

Sia (S, ρ) un insieme ordinato e siano $X, Y \subseteq S$ delle parti finite di S . Supponiamo che esistano $x = \inf(X)$ e $y = \inf(Y)$. Allora:

$$(X \cup Y)^\downarrow = X^\downarrow \cap Y^\downarrow = \{x\}^\downarrow \cap \{y\}^\downarrow$$

Per dualità vale l'analogo per i maggioranti. Inoltre, se (S, ρ) è un reticolo esiste $a = \inf(\{x, y\}) = \max(\{x, y\}^\downarrow) = \max((X \cup Y)^\downarrow) = \inf(X \cup Y)$.

Dimostrazione. Sia $x \in (X \cup Y)^\downarrow$, valgono allora le seguenti equivalenze:

$$\begin{aligned} x \in (X \cup Y)^\downarrow &\iff \forall y \in X \cup Y (x \leq y) \\ &\iff \forall y ((y \in X \vee y \in Y) \implies (x \leq y)) \\ &\iff \forall y (y \in X \implies x \leq y) \wedge \forall y (y \in Y \implies x \leq y) \\ &\iff x \in X^\downarrow \wedge x \in Y^\downarrow \\ &\iff x \in X^\downarrow \cap Y^\downarrow \end{aligned}$$

□

Corollario 6.2.1

Sia (S, \leq) un reticolo. Ogni sua parte finita è dotata di estremo inferiore e superiore.

Dimostrazione. Consideriamo una parte finita $T = \{a_1, a_2, \dots, a_n\} \subset S$ e procediamo per induzione.

- Se $n = 1$, cioè $T = \{a_1\}$, l'estremo inferiore di T è semplicemente a_1 perché, per l'Osservazione 6.2.1 si ha $T^\downarrow = \{a_1\}^\downarrow$, allora:

$$\inf(T) = \max(T^\downarrow) = \max(\{a_1\}^\downarrow) = a_1$$

- Supponiamo che l'estremo inferiore esista per tutti i sottoinsiemi finiti di S con n elementi. Consideriamo un sottoinsieme con $n + 1$ elementi, $T = \{a_1, a_2, \dots, a_{n+1}\}$. Possiamo riscrivere T come l'unione dell'insieme $T_1 = \{a_1, \dots, a_n\}$ e $T_2 = \{a_1\}$:

$$T = T_1 \cup T_2$$

Per ipotesi induttiva esiste l'estremo inferiore di T_1 , sia esso $b = \inf(\{a_1, a_2, \dots, a_n\})$ ed, essendo T_2 un insieme di un solo elemento, risulta inoltre $\inf(T_2) = a_{n+1}$. Per la Proposizione 6.2.2 vale allora:

$$\begin{aligned} T^\downarrow &= (T_1 \cup T_2)^\downarrow \\ &= T_1^\downarrow \cap T_2^\downarrow \\ &= \{b\}^\downarrow \cap \{a_{n+1}\}^\downarrow \\ &= \{b, a_{n+1}\}^\downarrow \end{aligned}$$

Dato che S è un reticolo, l'insieme $\{b, a_{n+1}\}$ sicuramente ammette estremo inferiore, e vale quindi:

$$\inf(\{b, a_{n+1}\}) = \max(\{b, a_{n+1}\}^\downarrow) = \max(T^\downarrow) = \inf(T)$$

□

Se un insieme finito è un reticolo allora risulta essere un reticolo completo.

6.2.1 ■ Operazioni reticolari

In questa sezione vedremo che i reticoli possono essere definiti, in modo equivalente, come insiemi muniti di due operazioni che soddisfano certe proprietà. L'idea è che $(a, b) \mapsto \sup(\{a, b\})$ e $(a, b) \mapsto \inf(\{a, b\})$ sono due operazioni che possiamo denotare rispettivamente $a \vee b$ e $a \wedge b$. Viceversa, la relazione d'ordine può essere ricavata da queste operazioni, nel modo seguente:

$$\forall a, b \in S (a \rho b \iff b = a \vee b)$$

oppure:

$$\forall a, b \in S (a \rho b \iff a = a \wedge b)$$

Proposizione 6.2.3

Sia S un reticolo. Allora posto $a \vee b = \sup(\{a, b\})$ e $a \wedge b = \inf(\{a, b\})$, si ha che le operazioni su S :

$$(a, b) \mapsto a \vee b \tag{6.12}$$

$$(a, b) \mapsto a \wedge b \tag{6.13}$$

verificano le seguenti proprietà:

1. *Commutatività*: $a \vee b = b \vee a$ e $a \wedge b = b \wedge a$, per ogni $a, b \in S$;
2. *Associatività*: $a \vee (b \vee c) = (a \vee b) \vee c$ e $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ per ogni $a, b, c \in S$
3. *Assorbimento*: $a \wedge (a \vee b) = a$, $a \vee (a \wedge b) = a$, per ogni $a, b \in S$.

Dimostrazione. Evidente, la prova è lasciata al lettore come esercizio. □

Osservazione 6.2.3

Per ogni $a \in S$, a è neutro rispetto a \vee se e soltanto se, per ogni $b \in S$ si ha $b = a \vee b$. Cioè, se e soltanto se, $\forall b \in S (a \leq b)$ e cioè, $a = \min(S, \leq)$. Dualmente, un elemento a è neutro rispetto a \wedge se è il massimo di (S, \leq) . L'eventuale minimo di un reticolo si indica con il simbolo 0 mentre l'eventuale massimo si indica con il simbolo 1.

Esaminiamo ora il viceversa della precedente Proposizione.

Proposizione 6.2.4

Sia (S, \vee, \wedge) un insieme munito di due operazioni che verificano le proprietà:

1. *Commutatività*: $a \vee b = b \vee a$ e $a \wedge b = b \wedge a$, per ogni $a, b \in S$;
2. *Associatività*: $a \vee (b \vee c) = (a \vee b) \vee c$ e $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ per ogni $a, b, c \in S$
3. *Assorbimento*: $a \wedge (a \vee b) = a$, $a \vee (a \wedge b) = a$, per ogni $a, b \in S$.

Allora la relazione ρ su S definita come:

$$a \rho b \iff b = a \vee b \tag{6.14}$$

è una relazione d'ordine su S . Si ha anche:

$$a \rho b \iff a = a \wedge b \tag{6.15}$$

Inoltre, S , munito di tale relazione d'ordine, è un reticolo, e, per ogni $a, b \in S$:

$$\begin{cases} \sup(\{a, b\}) = a \vee b \\ \inf(\{a, b\}) = a \wedge b \end{cases}$$

Dimostrazione. Iniziamo con il dimostrare la 6.15. Infatti, se $a \rho b$, cioè se $b = a \vee b$, allora per l'assorbimento, $a \wedge b = a \wedge (a \vee b) = a$. Viceversa, se $a = a \wedge b$, ancora per l'assorbimento e per la commutatività, $a \vee b = (a \wedge b) \vee b = b \vee (a \wedge b) = b$.

Dimostriamo ora che ρ è una relazione d'ordine:

1. *Riflessività*: $a \rho a$, cioè $a = a \vee a$. Infatti, usando le due proprietà di assorbimento, per ogni $a, b \in S$ si ha che $a = a \vee (a \wedge (a \vee b)) = a \vee a$;
2. *Antisimmetria*: Se $a \rho b$ e $b \rho a$, cioè se $b = a \vee b$ e $a = b \vee a$, allora, per la commutatività di \vee , deve essere $a = b$;
3. *Transitività*: se $a \rho b$ e $b \rho c$, cioè se $b = a \vee b$ e $c = b \vee c$ segue che $a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = a \vee c$.

Rimane da dimostrare l'ultima asserzione. Dimostriamo che:

$$a \vee b = \sup(\{a, b\})$$

Infatti, $a \rho (a \vee b)$, perché per la 6.15, ciò è equivalente al fatto che $a \wedge (a \vee b) = a$, cosa che è verificata per l'assorbimento. Allo stesso modo, si vede che $b \rho (a \vee b)$. Quindi $a \vee b$ è un maggiorante dell'insieme $\{a, b\}$. Rimane da dimostrare che è il minimo dell'insieme dei maggioranti. Supponiamo dunque che $a \rho c$ e $b \rho c$, cioè $c = a \vee c = b \vee c$. Allora $(a \vee b) \vee c = a \vee (b \vee c) = a \vee c = c$. Dunque $(a \vee c) \rho c$ e l'asserzione è dimostrata. Il fatto che $a \wedge b = \inf(\{a, b\})$ si dimostra in modo analogo. \square

Definizione 6.2.3: Reticolo come algebra

Una struttura algebrica (S, \wedge, \vee) a due operazioni interne si dice **reticolo** se le operazioni \vee e \wedge sono associative, commutative, e inoltre per ogni coppia (a, b) di elementi di S risulta:

$$a \wedge (a \vee b) = a \quad (6.16)$$

$$a \vee (a \wedge b) = a \quad (6.17)$$

ovvero valgono le leggi di assorbimento. Se (S, \wedge, \vee) è un reticolo, le operazioni \wedge e \vee sono spesso chiamate **intersezione** e **unione** in S oppure **meet** e **join**.

Esempio 6.2.2

Sia X un qualunque insieme, e nell'insieme $\mathcal{P}(X)$ delle parti di X si considerino le operazioni:

$$\cap : (A, B) \in \mathcal{P}(X)^2 \mapsto A \cap B \in \mathcal{P}(X)$$

e:

$$\cup : (A, B) \in \mathcal{P}(X)^2 \mapsto A \cup B \in \mathcal{P}(X)$$

Allora la terna $(\mathcal{P}(X), \cap, \cup)$ è un reticolo, chiamato **reticolo delle parti** di X .

6.2.2 ■ Sottoreticolari

Definizione 6.2.4: Sottoreticolo

Sia (S, \leq) un reticolo. Una parte $T \subseteq S$ si dice un **sottoreticolo** se esso è stabile rispetto a ciascuna delle operazioni reticolari \wedge e \vee .

Proposizione 6.2.5

Gli intervalli chiusi di un reticolo sono sempre sottoreticolari.

Dimostrazione. La dimostrazione è lasciata al lettore. \square

È chiaro che un sottoreticolo è esso stesso un reticolo. Invece il viceversa non è necessariamente vero: dato un reticolo S , esso può avere sottoinsiemi che sono reticolari rispetto alle operazioni di S ma non sono sottoreticolari di S .

Esempio 6.2.3

Si consideri l'insieme $\text{Div}(12) = \{1, 2, 3, 4, 6, 12\}$. Oltre ai **sottoreticolari banali** ($\text{Div}(12)$ stesso e i sottoinsiemi con un solo elemento) abbiamo i sottoreticolari $\{1, 2, 3, 6\}$ e $\{2, 4, 6, 12\}$. Sia $T = \text{Div}(12) \setminus \{2\} = \{1, 3, 4, 6, 12\} \subset \text{Div}(12)$.

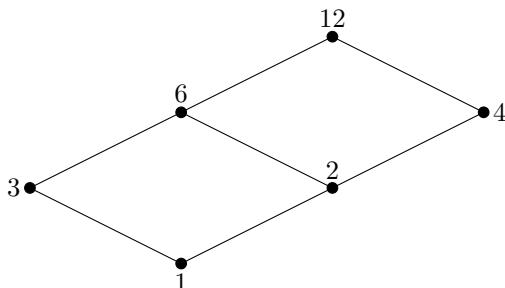


Figura 6.7: Il reticolo $(\text{Div}(12), |)$

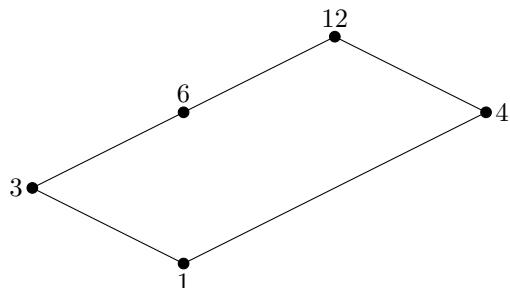


Figura 6.8: Il reticolo $(\text{Div}(12) \setminus \{2\}, |)$

Chiaramente T risulta essere un reticolo (perché per qualsiasi coppia di elementi esiste un estremo inferiore e superiore) ma non è un sottoreticolo di $(\text{Div}(12), |)$ in quanto non chiuso rispetto a \wedge , infatti:

$$6 \wedge_T 4 = \inf_{(T, |)}(\{6, 4\}) = 1 \neq 2 = \inf_{(\text{Div}(12), |)}(\{6, 4\}) = 6 \wedge_{\text{Div}(12)} 4$$

6.2.3 ■ Omomorfismi tra reticolati

Siano (S_1, \wedge, \vee) e (S_2, \wedge, \vee) reticolati. Seguendo la terminologia introdotta nella sezione 5.4 un'applicazione $f : S_1 \longrightarrow S_2$ si dice **omomorfismo** se risulta, per ogni coppia $(a, b) \in S_1$:

$$f(a \wedge b) = f(a) \wedge f(b), \quad f(a \vee b) = f(a) \vee f(b)$$

Teorema 6.2.1

Siano (S, ρ) e (T, σ) due reticolati con operazioni reticolari \wedge, \vee per S e $\overset{\circ}{\wedge}, \overset{\circ}{\vee}$ per T . Sia $f : S \rightarrow T$ una biezione. Allora f è un isomorfismo tra i due insiemi ordinati se e soltanto se f è un isomorfismo tra le strutture algebriche (S, \wedge, \vee) e $(T, \overset{\circ}{\wedge}, \overset{\circ}{\vee})$.

Dimostrazione. (\implies) Per ogni $a, b \in S$ si ha $a \wedge b = \inf_{(S, \rho)}(\{a, b\})$ e vale:

$$f(a \wedge b) = \inf_{(T, \sigma)}\{f(a), f(b)\} = f(a) \overset{\circ}{\wedge} f(b)$$

e dualmente $f(a \vee b) = f(a) \overset{\circ}{\vee} f(b)$. Quindi f risulta essere un omomorfismo tra strutture algebriche e in particolare un isomorfismo.

(\impliedby) Per ipotesi, per ogni $a, b \in S$ si ha $f(a \wedge b) = f(a) \overset{\circ}{\wedge} f(b)$. Quindi:

$$a \leq b \iff a = a \wedge b \iff a = f(a \wedge b) = f(a) \overset{\circ}{\wedge} f(b) \iff f(a) \sigma f(b)$$

ed f risulta essere un isomorfismo tra i due insiemi ordinati. □

6.2.4 ■ Dualità reticolare

Definizione 6.2.5: Relazione inversa

Siano A, B due insiemi e sia σ una corrispondenza tra A e B . Definiamo la **relazione inversa** σ^{-1} ponendo:

$$b \sigma^{-1} a \iff a \sigma b$$

Proposizione 6.2.6

Principio di dualità Se \leq è una relazione d'ordine in L , allora \leq^{-1} è ancora una relazione d'ordine. Inoltre, se (L, \leq) è un reticolo, allora (L, \leq^{-1}) è ancora un reticolo.

Definizione 6.2.6: Reticolo duale

Sia (L, \leq) un reticolo. Diciamo **reticolo duale** il reticolo (L, \leq^{-1}) .

6.2.5 ■ Reticoli distributivi e complementati

Definizione 6.2.7: Complemento

Sia (S, \leq) un reticolo limitato. Un elemento $a \in S$ si dice un **complemento** di un elemento $b \in S$ se e solo se:

$$a \wedge b = \min(S, \leq) = 0$$

e

$$a \vee b = \max(S, \leq) = 1$$

Un reticolo si dice **complementato** se ogni elemento del reticolo ammette almeno un complemento.

Esempio 6.2.4

Il reticolo delle parti di S è un reticolo complementato infatti, presi $\min\mathcal{P}(S) = \emptyset$ e $\max\mathcal{P}(S) = S$, per ogni parte X di S si ha il complemento $S \setminus X$ e vale:

$$\begin{aligned} X \wedge (S \setminus X) &= \inf\{X, S \setminus X\} = \emptyset \\ X \vee (S \setminus X) &= \sup\{X, S \setminus X\} = S \end{aligned}$$

Osserviamo inoltre che \emptyset ed S sono l'uno il complemento dell'altro ed è l'unico caso in cui due elementi a, b sono sia complementari che confrontabili.

Esempio 6.2.5

I reticolati:

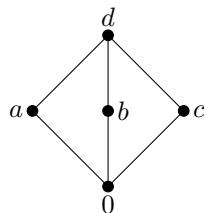


Figura 6.9

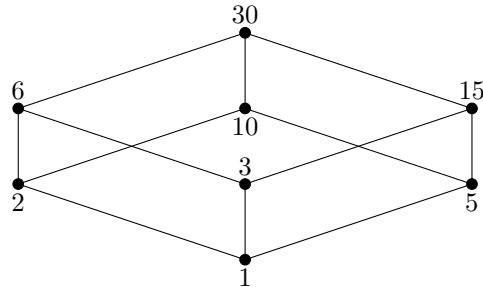


Figura 6.10

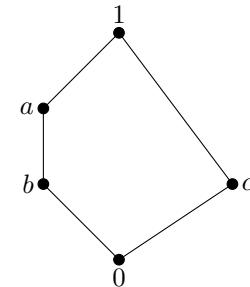


Figura 6.11

sono complementati. Nel caso del reticolo mostrato in Figura 6.9 l'elemento a ha due complementi (b e c) così come b e c hanno due complementi ciascuno. Analogamente, nel reticolo 6.11 l'elemento c ha più di un complemento: a e b sono entrambi complementi di c mentre a e b hanno entrambi un unico complemento (c). Nel caso del reticolo 6.10 ogni elemento ha un unico complemento. Notiamo inoltre che tale reticolo corrisponde all'insieme $\text{Div}(30)$ e che il complemento di ogni $k \in \text{Div}(30)$ corrisponde all'elemento $\frac{30}{k}$.

Definizione 6.2.8: Reticolo distributivo

Sia (S, \wedge, \vee) un reticolo. Allora (S, \leq) è **distributivo** se e soltanto se, per ogni $a, b, c \in S$:

$$\begin{aligned} a \vee (b \wedge c) &= (a \vee b) \wedge (a \vee c) \\ a \wedge (b \vee c) &= (a \wedge b) \vee (a \wedge c) \end{aligned}$$

ossia \wedge è distributiva rispetto a \vee e viceversa.

Esempio 6.2.6

Il reticolo delle parti di un insieme S è distributivo in quanto \cap e \cup sono distributive l'una rispetto all'altra.

Proposizione 6.2.7

Se (S, \leq) è un reticolo limitato distributivo, allora ogni $a \in S$ ammette unico complemento.

Dimostrazione. Supponiamo per assurdo che x e y siano entrambi complementi di a e sia $0 = \min S$ e $1 = \max S$. Allora:

$$\begin{aligned} a \wedge x &= 0 = a \wedge y \\ a \vee x &= 1 = a \vee y \end{aligned}$$

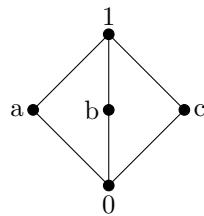
Allora:

$$x = x \wedge 1 = x \wedge (a \vee y) = (x \wedge a) \vee (x \wedge y) = 0 \vee (x \wedge y) = x \wedge y$$

Analogamente $y = y \wedge x$. Per la proprietà commutativa delle operazioni reticolari allora si ha $x = y$. \square

Esempio 6.2.7

La distributività del reticolo è una condizione necessaria per l'unicità del complemento. Si consideri il seguente reticolo:



Si ha chiaramente $\forall x (0 \leq x)$ e $\forall x (x \leq 1)$ ed inoltre i punti a, b, c non sono confrontabili tra di loro. Allora chiaramente sia b che c sono dei complementi per a ed infatti il reticolo non è distributivo:

$$a \vee (b \wedge c) = a \vee 0 = a$$

mentre:

$$(a \vee b) \wedge (a \vee c) = 1 \wedge 1 = 1$$

Inoltre, non è detto che se ogni elemento ha un unico complemento nel reticolo allora questo risulti distributivo. Non vale ovvero l'implicazione inversa.

Definizione 6.2.9: Reticolo pentagonale

Si consideri un insieme $X = \{x_1, x_2, x_3, x_4, x_5\}$ di ordine 5 e si introduca in X una relazione d'ordine ponendo $\forall x \in X (x \leq x, x_1 \leq x, x \leq x_5)$ e inoltre $x_2 \leq x_3$. Allora $\{x_2, x_4\}$ e $\{x_3, x_4\}$ sono gli unici sottoinsiemi di ordine 2 di X costituiti da elementi non confrontabili, e si ha $x_1 = \inf\{x_2, x_4\} = \inf\{x_3, x_4\}$ e $x_5 = \sup\{x_3, x_4\}$. Il reticolo (X, \wedge, \vee) associato all'insieme ordinato (X, \leq) si chiama **reticolo pentagonale**.

Definizione 6.2.10: Reticolo trirettangolo

Sia $Y = \{y_1, y_2, y_3, y_4, y_5\}$ un altro insieme di ordine 5 e si introduca in Y una relazione d'ordine \leq ponendo $y \leq y, y_1 \leq y$ e $y \leq y_5$ per ogni $y \in Y$. Allora $\{y_2, y_3\}, \{y_2, y_4\}$ e $\{y_3, y_4\}$ sono i sottoinsiemi di ordine 2 di Y costituiti da elementi non confrontabili, e si ha $y_1 = \inf\{y_2, y_3\} = \inf\{y_2, y_4\} = \inf\{y_3, y_4\}$. Il reticolo (Y, \wedge, \vee) associato all'insieme ordinato (Y, \leq) si chiama **reticolo trirettangolo**.

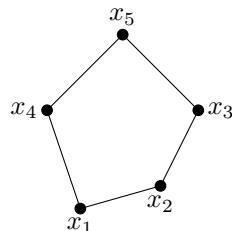


Figura 6.12: Reticolo pentagonale

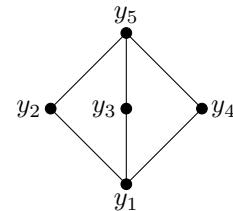


Figura 6.13: Reticolo trirettangolo

Per capire se un reticolo è distributivo, ne costruisco il diagramma di Hasse e verifico se questo contiene un sottoreticolo pentagonale o trirettangolo. Se un reticolo li contiene, eredita a sua volta le proprietà dei sottoreticolari. Infatti, un reticolo isomorfo ad un altro reticolo ha le sue stesse proprietà. Vale quindi il seguente teorema.

Teorema 6.2.2 (Criterio di Birkhoff)

Sia (S, \leq) un reticolo, allora (S, \leq) è distributivo se e soltanto se nessun sottoreticolo di (S, \leq) è isomorfo ad un reticolo pentagonale o trirettangolo.

Corollario 6.2.2

I reticolari pentagonali e trirettangolo sono i più piccoli tra i reticolari non distributivi. Ogni reticolo di ordine inferiore a 5 è distributivo.



6.3.1 ▶ Anelli booleani

Definizione 6.3.1: Anello booleano

Un anello A si dice **booleano** se A è unitario ed ogni elemento è idempotente, cioè coincide col proprio quadrato: $\forall a \in A (a = a \cdot a)$.

Esempio 6.3.1

L'anello $(\mathcal{P}(S), \Delta, \cap)$ delle parti di un insieme è un anello booleano. Infatti è unitario e dal momento che l'operazione di moltiplicazione dell'anello $\mathcal{P}(S)$ è quella di intersezione, per ogni $X \in \mathcal{P}(S)$ si ha $X^2 = X \cap X = X$.

Definizione 6.3.2: Caratteristica di un anello

Se A è unitario e indichiamo l'unità di A con 1_A , se esiste qualche intero positivo $n \in \mathbb{Z}^+$ tale che:

$$n1_A = 1_A + 1_A + \cdots + 1_A = 0_A$$

allora la **caratteristica** di A è il minimo tale intero n .

Osservazione 6.3.1



Ovviamente A ha caratteristica 1 se e soltanto se $1_A = 0_A$ e quindi $A = \{0_A\}$. Altrettanto banale è il caso in cui la caratteristica di A è due, per cui $1_A \neq 0_A$ e risulta $2 \cdot 1_A = 0_A$. Notiamo che l'anello $(\mathcal{P}(S), \Delta, \cap)$ ha questa proprietà se $S \neq \emptyset$. Infatti in questo anello l'unità è S , lo zero è \emptyset , l'addizione è la differenza simmetrica e si ha $2 \cdot S = S \Delta S = \emptyset$. Quindi l'anello $\mathcal{P}(S)$ ha caratteristica 2.

Dimostriamo ora che quanto appena visto per $(\mathcal{P}(S), \Delta, \cap)$ vale per tutti gli anelli booleani; verificando inoltre che questi anelli sono sempre commutativi.

Proposizione 6.3.1

Sia A un anello booleano, allora A è commutativo e, se $|A| > 1$ allora A ha caratteristica 2.

Dimostrazione. Per ogni $a, b \in A$ vale: $a^2 = a \cdot a = a$, $b^2 = b \cdot b = b$. Quindi:

$$\begin{aligned} (a + b)^2 &= (a + b)(a + b) \\ &= a(a + b) + b(a + b) \\ &= a^2 + ab + ba + b^2 \\ &= a + ab + ba + b \end{aligned}$$

Essendo la caratteristica di A pari a due, però, si ha che $(a + b)^2 = (a + b)$ quindi:

$$\begin{aligned} a + ab + ba + b &= a + b \\ \implies ab + ba &= 0_A \\ \implies ab &= -ba \end{aligned}$$

Nel caso in cui sia $a = b$ si ottiene che, per ogni $a \in A$ vale $a^2 = -a^2$ ovvero $a = -a$. Quindi $\forall a \in A$ si ha $2a = 0_A$. In particolare $2 \cdot 1_A = 0_A$, quindi o $1_A = 0_A$ ed $A = \{0_A\}$ oppure $|A| > 1$ e la caratteristica di A è due. Infine, per ogni a, b , sfruttando $a = -a$ per l'elemento ba si ha: $ba = -ba = ab$ ed A risulta commutativo. \square

Enunciamo ma non dimostriamo il teorema di Stone, che è il risultato fondamentale nella teoria degli anelli booleani.

Teorema 6.3.1 (di Stone)

Sia A un anello booleano, allora:

- Esiste un insieme S tale che A sia isomorfo ad un sottoanello unitario di $(\mathcal{P}(S), \Delta, \cap)$;
- Se A è finito esiste un insieme S tale che A sia isomorfo a $(\mathcal{P}(S), \Delta, \cap)$.

Osservazione 6.3.2

Tutti i sottoanelli unitari di $(\mathcal{P}(S), \Delta, \cap)$ sono booleani.

Corollario 6.3.1

Sia R un anello booleano finito. Allora:

1. Esiste $n \in \mathbb{N}$ tale che $|R| = 2^n$;
2. Se A è un anello booleano e $|A| = |R|$ allora $A \simeq R$.

Dimostrazione. Per il teorema di Stone, esiste un insieme S , ovviamente finito, tale che R sia isomorfo a $(\mathcal{P}(S), \Delta, \cap)$. Posto $n = |S|$, allora $|R| = |\mathcal{P}(S)| = 2^n$, il che giustifica la (1). Se poi A è un anello booleano, anch'esso di cardinalità 2^n , ancora per il teorema di Stone abbiamo $A \simeq (\mathcal{P}(T), \Delta, \cap)$ per un opportuno insieme T . Ma allora $|\mathcal{P}(T)| = |A|$, quindi $|\mathcal{P}(T)| = 2^n$ e deduciamo così $|T| = n$. Dunque $|T| = |S|$ e quindi $A \simeq R$. \square

6.3.2 ■ Reticoli booleani

Ricordiamo che un reticolo è un insieme ordinato non vuoto (L, \leq) tale che, per ogni $a, b \in L$ esistano l'estremo inferiore $\inf_{(L, \leq)}\{a, b\}$ e l'estremo superiore $\sup_{(L, \leq)}\{a, b\}$ di $\{a, b\}$ in (L, \leq) . Ricordiamo anche che si può, in modo equivalente, riguardare i reticoli anche come strutture algebriche.

Definizione 6.3.3: Reticolo booleano

Un reticolo si dice **booleano** se e solo se è distributivo e complementato.

Come abbiamo appena visto, un reticolo può essere visto anche come una struttura algebrica (L, \wedge, \vee) . Affinché L sia un reticolo booleano devono valere:

- le proprietà commutative per \wedge e \vee ;
- le proprietà associative per \wedge e \vee ;
- le leggi di assorbimento;
- le proprietà distributive;
- l'esistenza degli elementi neutri di \wedge e \vee (ovvero devono esistere \min e \max del reticolo);
- ogni elemento deve avere un complemento. Esiste quindi l'applicazione¹: $' : a \in L \mapsto a' \in L$.

Gli insiemi totalmente ordinati con massimo due elementi sono reticoli booleani.

6.3.3 ■ Algebre di Boole

Definizione 6.3.4: Algebra di Boole

Si definisce **algebra di Boole** una struttura algebrica $(L, \vee, \wedge, 0, 1, {}')$ tale che:

1. $(L, \vee, 0)$ e $(L, \wedge, 1)$ sono monoidi commutativi;
2. valgono le leggi di assorbimento: $\forall a, b \in L (a \vee (a \wedge b) = a = a \wedge (a \vee b))$;
3. vale la distributività di \wedge rispetto a \vee e viceversa;
4. per ogni $a \in L$ esiste il complementare a' per il quale $a \wedge a' = 0$ e $a \vee a' = 1$.

¹Che risulta ben posta in quanto il reticolo è distributivo e ogni elemento ammette un unico complemento.

Osservazione 6.3.3



Ogni reticolo booleano è un'algebra di Boole e viceversa. Infatti, la (1) e la (2) esprimono il fatto che (L, \wedge, \vee) è un reticolo limitato, con minimo 0 e massimo 1 mentre la (3) dice che questo reticolo è distributivo e la (4) garantisce che ogni elemento a di L ha un complemento a' . Possiamo dunque dire che la nozione di algebra di Boole è la versione “puramente algebrica” della nozione di reticolo booleano.

Definizione 6.3.5: Sottoalgebra di Boole

Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole. Un sottoinsieme $C \subset L$ è detto **sottoalgebra di Boole** se, per ogni $x, y \in C$:

1. $x \vee y \in C$ e $x \wedge y \in C$
2. $0 \in C$ e $1 \in C$
3. $x' \in C$

La nozione di sottoalgebra di Boole differisce da quella di sottoreticolo. Infatti, un sottoreticolo K di un reticolo booleano L deve essere chiuso rispetto alle due operazioni reticolari (quindi deve verificare la prima delle tre condizioni appena elencate), ma non contiene necessariamente il massimo o il minimo del reticolo né, tanto meno, i complementi dei suoi elementi.

Esempio 6.3.2

1. Sia $S \neq \emptyset$ un insieme. Consideriamo il reticolo booleano $(\mathcal{P}(S), \subseteq)$. Questo si struttura come algebra di Boole nella forma $(\mathcal{P}(S), \cup, \cap, \emptyset, S, \mathcal{C}_X)$ dove \mathcal{C}_X è l'applicazione “complemento” che manda ogni $X \in \mathcal{P}(S)$ in $S \setminus X$.
2. Sia $\mathbb{B} = \{0, 1\}$ dotato delle operazioni binarie \wedge e \vee e dell'operazione unaria $'$ dove:
 - (a) \vee (OR) è definita da $0 \vee 0 = 0$, $0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1$;
 - (b) \wedge (AND) è definita da $0 \wedge 0 = 0 \wedge 1 = 1 \wedge 0 = 0 \wedge 1 = 1$;
 - (c) $0' = 1$ e $1' = 0$.

Si ha che $(\mathbb{B}, \vee, \wedge, 0, 1, ')$ è un'algebra di Boole.

Il prossimo enunciato elenca alcune identità che valgono nelle algebre di Boole. La terza si esprime dicendo che l'operazione di complemento è **involutoria**, cioè coincide con l'applicazione inversa di sé stessa (e, in particolare, è biettiva); le ultime due sono le note come leggi di De Morgan per algebre di Boole.

Proposizione 6.3.2

Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole. Allora $\forall a, b \in L$ valgono:

1. $1 \vee a = 1$ e $0 \wedge a = 0$
2. $1' = 0$ e $0' = 1$
3. $(a')' = a$
4. $(a \vee b)' = a' \wedge b'$
5. $(a \wedge b)' = a' \vee b'$

Dimostrazione. La (1) e la (2) sono immediate in quanto L è un reticolo.

Per dimostrare la validità della (3) basta osservare che a' è un complemento di a e a è un complemento di a' , anche $(a')'$ è un complemento di a' ; quindi per l'unicità dei complementi nei reticoli booleani si ha $a = (a')'$.

Per la (4) basta mostrare che $(a' \wedge b')$ è un complemento di $a \vee b$, ovvero che:

$$(a \vee b) \vee (a' \wedge b') = 1$$

e:

$$(a \vee b) \wedge (a' \wedge b') = 0$$

Usando la distributività e la (1) si ottiene:

$$\begin{aligned} (a \vee b) \vee (a' \wedge b') &= (a \vee b \vee a') \wedge (a \vee b \vee b') \\ &= (1 \vee b) \wedge (a \vee 1) \\ &= 1 \wedge 1 = 1 \end{aligned}$$

e

$$\begin{aligned} (a \vee b) \wedge (a' \wedge b') &= (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') = (0 \wedge b') \vee (0 \wedge a') \\ &= 0 \vee 0 = 0 \end{aligned}$$

La numero (5) si dimostra in maniera duale. □

6.3.4 ■ Anelli booleani e algebre di Boole

Si rimanda [qui](#) alle note del docente. Argomento cardine di questa sezione è la sostanziale *equivalenza tra concetto di algebra di Boole, reticolo booleano e anello booleano* in quanto esiste una corrispondenza biunivoca fra le tre strutture, nel senso che si può costruire una struttura di reticolo booleano su ogni anello booleano e, viceversa, una struttura di anello booleano su ogni reticolo booleano, in modo che queste due costruzioni siano l'una inversa dell'altra. Grazie al Teorema di Stone, infatti, ogni anello booleano finito è isomorfo a $(\mathcal{P}(S), \Delta, \cap)$ per un opportuno insieme S (per gli anelli infiniti il teorema è un po' più debole: ogni anello booleano è isomorfo ad un sottoanello unitario di $(\mathcal{P}(S), \Delta, \cap)$, per un opportuno insieme S). Analoghi enunciati valgono per i reticolati booleani e per le algebre di Boole.

In primo luogo, partendo da un anello booleano $(R, +, \cdot)$ vogliamo definire una struttura di reticolo booleano su R . L'esempio dell'anello delle parti di un insieme può suggerirci in che modo procedere. Fissato un insieme S , infatti, $(\mathcal{P}(S), \Delta, \cap)$ è un anello booleano ma $\mathcal{P}(S)$ è anche un reticolo booleano, con operazioni reticolari \cup e \cap . La seconda operazione reticolare è proprio l'operazione di moltiplicazione nell'anello. Anche la prima operazione reticolare si può esprimere in termini delle operazioni dell'anello: per ogni $A, B \in \mathcal{P}(S)$ abbiamo infatti che:

$$A \cup B = (A \Delta B) \cup (A \cap B) = (A \Delta B) \Delta (A \cap B)$$

Inoltre, il minimo ed il massimo del reticolo sono \emptyset e S , cioè lo zero e l'unità dell'anello, e ciascun $A \in \mathcal{P}(S)$ ha come complemento, nel reticolo $(\mathcal{P}(S), \subseteq)$ l'insieme $S \setminus A = S \Delta A = 1_{\mathcal{P}(S)} \Delta A$.

Passando ora ad un arbitrario anello booleano $(R, +, \cdot, 0_R, 1_R)$ dove 0_R e 1_R sono lo zero e l'unità dell'anello, l'esempio di $\mathcal{P}(S)$ suggerisce di definire in R l'operazione binaria \vee ponendo, per ogni $a, b \in R$:

$$a \vee b := a + b + ab \quad (6.18)$$

e l'applicazione $' : a \in R \mapsto 1_R + a \in R$ da utilizzare come operazione unaria di complemento.

Proposizione 6.3.3

Con le notazioni appena fissate, $(R, \vee, \cdot, 0_R, 1_R, ')$ è un'algebra di Boole.

Dimostrazione. Dobbiamo verificare che $(R, \vee, 0_R)$ e $(R, \cdot, 1_R)$ siano monoidi commutativi, che valgano per \vee e \cdot le leggi di assorbimento e le proprietà distributive ed infine che l'applicazione $'$ verifichi la condizione richiesta dalla definizione di complemento.

Che \vee sia commutativa è evidente, ed è anche chiaro che $a \vee 0_R = a + 0_R + a0_R$ per ogni $a \in R$, quindi 0_R è neutro rispetto a \vee . Proviamo l'associatività di \vee : per ogni $a, b, c \in R$ si ha:

$$\begin{aligned} (a \vee b) \vee c &= (a + b + ab) \vee c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + ab + c + ac + bc + abc \end{aligned}$$

Si ha inoltre:

$$\begin{aligned} a \vee (b \vee c) &= (b \vee c) \vee a \\ &= b + c + a + bc + ba + ca + bca \end{aligned}$$

dunque $(a \vee b) \vee c = a \vee (b \vee c)$. È così provato che \vee è associativa. $(R, \vee, 0_R)$ è un monoide commutativo. Che lo sia anche $(R, \cdot, 1_R)$ è già noto in partenza, dal momento che R è un anello booleano.

Verifichiamo le leggi di assorbimento. Per ogni $a, b \in R$ ($a \vee (ab) = a + ab + a(ab)$). Dal momento che R è booleano, $a(ab) = a^2b = ab$ e $ab + ab = 0_R$, quindi $a \vee (ab) = a + ab + ab = a$. Inoltre $a(a \vee b) = a(a + b + ab) = a^2 + ab + a^2b = a + ab + ab = a$. Le leggi di assorbimento sono così provate. A questo punto possiamo concludere che (R, \vee, \cdot) è un reticolo limitato.

Verifichiamo ora che \cdot è distributiva rispetto a \vee . Per ogni $a, b, c \in R$ si ha $a(b \vee c) = a(b + c + bc) = ab + ac + abc$ e $(ab) \vee (ac) = ab + ac + (ab)(ac) = ab + ac + abc$. Dunque $a(b \vee c) = (ab) \vee (ac)$. Pertanto, utilizzando anche la proprietà commutativa, possiamo concludere che \cdot è distributiva rispetto a \vee .

Resta infine da dimostrare che, per ogni $a \in R$, l'immagine di a mediante l'applicazione $'$, vale a dire $a' := 1_R + a$, verifica le condizioni $a \vee (1_R + a) = 1_R$ e $aa' = 0_R$. Questo è molto facile: per ogni $a \in R$ si ha $aa' = a(1_R + a) = a + a = 0_R$ e $a \vee a' = a + a' + aa' = a + (1_R + a) + 0_R = 1_R$, come richiesto. Con questo la dimostrazione è completa. \square

Descriviamo ora la costruzione inversa: quella di un anello booleano a partire da un'algebra di Boole. Anche in questo caso ci facciamo guidare dall'esempio dell'algebra $(\mathcal{P}(S), \cup, \cap, \emptyset, S, C_X)$ delle parti di un insieme S . Delle due operazioni binarie dell'anello booleano $(\mathcal{P}(S), \Delta, \cap)$, quella di moltiplicazione, \cap , è già tra le operazioni dell'algebra di Boole. Per esprimere

l'altra, la differenza simmetrica, utilizzando le operazioni dell'algebra di Boole ci è utile osservare che se A e B sono parti di S , allora $A \setminus B = A \cap (S \setminus B) = A \cap C_X(B)$. Dunque $A \Delta B$ può essere scritta come:

$$\begin{cases} (A \setminus B) \cup (B \setminus A) = (A \cap C_X(B)) \cup (B \cap C_X(A)) \\ (A \cup B) \setminus (A \cap B) = (A \cup B) \cap (C_X(A \cap B)) \end{cases}$$

Questo esempio mostra due modi possibili per definire, in un'arbitraria algebra di Boole, un'operazione binaria di addizione + analoga alla differenza simmetrica in $\mathcal{P}(S)$.

Lemma 6.3.1

Sia $(L, \vee, \wedge, 0, 1, ')$ un'algebra di Boole. Allora, per ogni $a, b \in L$:

$$(a \wedge b') \vee (a' \wedge b) = (a \vee b) \wedge (a \wedge b)'$$

Dimostrazione. Usando la proprietà distributiva di \vee rispetto a \wedge abbiamo:

$$\begin{aligned} (a \wedge b') \vee (a' \wedge b) &= (a \vee a') \wedge (a \vee b) \wedge (b' \vee a') \wedge (b' \vee b) \\ &= 1 \wedge (a \vee b) \wedge (b' \vee a') \wedge 1 \\ &= (a \vee b) \wedge (a' \vee b') \\ &= (a \vee b) \wedge (a \wedge b)' \end{aligned}$$

avendo utilizzato, per ultimo passaggio, una delle leggi di De Morgan. □

Teorema 6.3.2 (di Stone per le algebre di Boole)

Ogni reticolo booleano finito è isomorfo al reticolo finito delle parti. Ogni algebra di Boole è isomorfa ad un'algebra di Boole delle parti finite.

Questo vuol dire, ad esempio, che se sappiamo descrivere il reticolo delle parti degli insiemi finiti, conosciamo, a meno di isomorfismi, tutti i reticolli booleani finiti. Una conseguenza del teorema di Stone è che gli anelli booleani finiti (ma lo stesso vale per i reticolli booleani finiti o per le algebre di Boole finite) hanno per cardinalità una potenza di 2, e che due anelli booleani finiti con lo stesso numero di elementi sono necessariamente isomorfi.

Sia allora $X \subseteq S$. Prendiamo la funzione caratteristica:

$$\chi_{X,S} : x \in S \mapsto \begin{cases} 0 & \text{se } x \notin X \\ 1 & \text{se } x \in X \end{cases} \in \{0, 1\}$$

e alteriamone il codominio:

$$\chi_{X,S} : x \in S \mapsto \begin{cases} \bar{0} & \text{se } x \notin X \\ \bar{1} & \text{se } x \in X \end{cases} \in \mathbb{Z}_2$$

Dimostriamo che $X \in \mathcal{P}(S) \mapsto \chi_{X,S} \in Map(S, \mathbb{Z}_2)$ è biettiva. Sia $S = \{1, 2, 3, \dots, n\}$ con $n \in \mathbb{N}^*$. Allora $Map(S, \mathbb{Z}_2)$ è l'insieme delle n -ple di elementi di \mathbb{Z}_2 . Come già osservato, possiamo scrivere ogni funzione da S in \mathbb{Z}_2 come una stringa $(s_1 s_2 \dots s_n)$. Chiamiamo \mathbb{Z}_2^n l'insieme di tali stringhe, gli elementi di $\mathcal{P}(S)$ corrispondono quindi a tali stringhe.

Sia allora $R^n = R \times \dots \times R$ il prodotto cartesiano di n copie di un anello R , ovvero l'insieme di n -ple di elementi di R . Se prendiamo due elementi e ne facciamo somma e prodotto, otteniamo:

$$\begin{aligned} a + b &= (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n) \\ a \cdot b &= (a_1 \cdot b_1, a_2 \cdot b_2, \dots, a_n \cdot b_n) \end{aligned}$$

E possiamo considerare la struttura $(R^n, +, \cdot)$ che risulta essere un anello. Se R è booleano, anche R^n è booleano. Allora anche \mathbb{Z}_2^n , per le stesse osservazioni, sarà un anello booleano rispetto alle operazioni di somma e prodotto.

Esempio 6.3.3

Sia $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$ e consideriamo le stringhe $a = (10010011)$ e $b = (01101101)$, facendo somma e prodotto, otteniamo:

$$\begin{aligned}a + b &= 11111110 = a \vee b \\a \cdot b &= 00000001 = a \wedge b\end{aligned}$$

dove \vee e \wedge sono i classici operatori logici bit a bit. Sappiamo inoltre che l'applicazione $X \in \mathcal{P}(S) \mapsto \chi_{X,S} \in \mathbb{Z}_2^8$ è biettiva. Quindi prese le parti $A = \{1, 4, 7, 8\}$ e $B = \{2, 3, 5, 6, 8\}$, codificate dalle stringhe $a = (10010011)$ e $b = (01101101)$,abbiamo:

$$\begin{aligned}a + b &= (11111110) = \{1, 2, 3, 4, 5, 6, 7\} = A \Delta B \\a \cdot b &= 00000001 = \{8\} = A \cap B\end{aligned}$$

Allora $X \in \mathcal{P}(S) \mapsto \chi_{X,S} \in \mathbb{Z}_2^n$ è un isomorfismo di anelli.

Nel caso finito, come anticipato, tutte le algebre di Boole sono isomorfe a $\mathcal{P}(S)$.

Osservazione 6.3.4



I simboli che si usano per le operazioni reticolari coincidono con i simboli usati per i connettivi logici perché è possibile definire una struttura con l'insieme di tutte le formule con i connettivi logici come operazioni, che descrivono relazioni di equivalenza. L'insieme quoziante che ne deriva è proprio un'algebra di Boole. Per questo motivo si usano gli stessi simboli e per questo motivo le algebre di Boole rivestono un ruolo importante in logica ed in informatica.



6.4.1 ■ Relazioni d'ordine e reticolì

Esercizio 6.4.1

Trovare un isomorfismo di reticolì dall'insieme di parti $\{0, 1\}$ all'insieme delle parti $\{3, 4\}$, ordinati per inclusione.

Esercizio 6.4.2

Stabilire per quali interi n nell'insieme $\{2, 14, 18, 27, 30\}$ il reticolo dei numeri naturali divisori di n (sottoreticolo di $(\mathbb{N}, |)$) è complementato.

Esercizio 6.4.3

2 ha un complemento in $(\mathbb{N}, |)$? Il reticolo $(\mathbb{N}, |)$ è complementato?

Esercizio 6.4.4

Disegnare il diagramma di Hasse di un reticolo in cui esista un elemento con sei complementi.

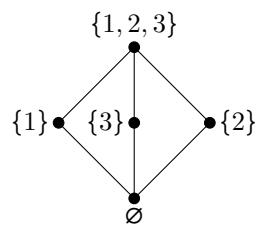
Esercizio 6.4.5

Trovare, tra i sottoinsiemi di $\mathcal{P}(\mathbb{N})$, ordinati per inclusione:

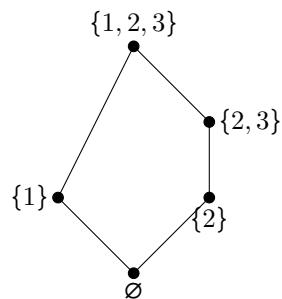
1. Un sottoinsieme di cardinalità 5 che non sia un reticolo;
2. Un sottoinsieme di cardinalità 5 che sia un reticolo trirettangolo;
3. Un sottoinsieme di cardinalità 5 che sia un reticolo pentagonale.

Svolgimento. Abbiamo:

- (i) Basterà prendere un insieme di 5 singleton. Ovviamente saranno inconfrontabili rispetto all'inclusione e quindi non costituiscono un reticolo.
- (ii) Consideriamo $A = \{\emptyset, \{0\}, \{1\}, \{2\}, \{1, 2, 3\}\}$. Si ottiene il reticolo trirettangolo:



- (iii) Consideriamo $B = \{\emptyset, \{1\}, \{2\}, \{2, 3\}, \{1, 2, 3\}\}$. Si ottiene il reticolo pentagonale:



Esercizio 6.4.6

Dimostrare in modo diretto che gli insiemi totalmente ordinati sono reticolì distributivi.

Svolgimento. Sia (S, \leq) un insieme totalmente ordinato. Ovviamente, per definizione di relazione d'ordine totale, per ogni parte $\{a, b\}$ di elementi di S esiste un minimo ed un massimo, in quanto vale $a \leq b$ oppure $b \leq a$. Ovvero, posto $a \leq b$:

$$\begin{aligned} a \wedge b &= \inf(\{a, b\}) = a \\ a \vee b &= \sup(\{a, b\}) = b \end{aligned}$$

Si determina cioè una catena. Presi quindi $a, b, c \in S$ ($a \leq b \leq c$), vale:

$$\begin{aligned} a \vee (b \wedge c) &= a \vee b = b \\ (a \vee b) \wedge (a \vee c) &= b \wedge c = b \end{aligned}$$

E vale:

$$\begin{aligned} a \wedge (b \vee c) &= a \wedge c = a \\ (a \wedge b) \vee (a \wedge c) &= a \vee a = a \end{aligned}$$

Quindi il reticolo risulta essere distributivo. ■

Esercizio 6.4.7

Sia $X = \{n \in \mathbb{N} \mid 1 \leq n \leq 10\}$. Si considerino i seguenti insiemi di parti di X :

$$\begin{aligned} A &= \{\{1, 3, 5\}, \{4, 6\}, \{1, 7, 8\}, \{9, 10\}\} \\ B &= \{\{4\}, \{5, 8\}, \{1, 2, 3\}, \{6, 7, 9, 10\}\} \end{aligned}$$

Quale tra A e B è una partizione di X ? Quale non lo è? (giustificare *entrambe* le risposte). Detta F quella tra A e B che è una partizione di X , per ogni $x \in X$ si indichi con F_x l'unico elemento di F tale che $x \in F_x$. Si consideri in X la relazione binaria Σ così definita:

$$\forall x, y \in X (x \Sigma y \iff (x = y \vee |F_x| < |F_y|))$$

- (i) Si verifichi che Σ è una relazione d'ordine in X e si dica se è totale.
- (ii) Disegnare il diagramma di Hasse di (X, Σ)
- (iii) (X, Σ) è un reticolo?
- (iv) Determinare un sottoinsieme di X di ordine 6 tale che (Y, Σ) sia un reticolo. (Y, Σ) è distributivo? È complementato?

Svolgimento. Chiaramente A non è una partizione di X in quanto risultano essere presenti parti non disgiunte ed elementi di X mancanti. Ad esempio $\{1, 3, 5\} \cap \{1, 7, 8\} = \{1\}$ e $\neg(\exists y \in A)(\{2\} \subseteq y)$. L'insieme delle parti B risulta invece essere una partizione per X in quanto ogni elemento di B è disgiunto da qualsiasi altro elemento della partizione e l'unione unaria di B coincide con X . Possiamo quindi porre $F = B$.

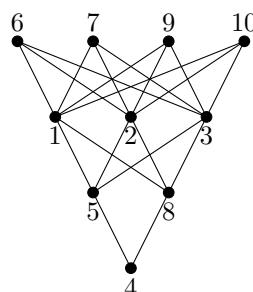
(i) Dimostriamo che $\Sigma \in OL(X)$:

- Sicuramente Σ è riflessiva in quanto per ogni $x \in X$ vale $x \Sigma x$ dato che $x = x$.
- Siano $x, y \in X$ tale che $x \Sigma y$ e $y \Sigma x$. Allora o $x = y$, per definizione della relazione Σ , oppure, da $|F_x| < |F_y|$ e $|F_y| < |F_x|$ segue $|F_x| = |F_y|$. Poiché in F non sono presenti parti equipotenti devono coincidere F_x ed F_y per avere lo stesso numero di elementi. Quindi $x, y \in F_x$. Ma essendo per ipotesi $x \Sigma y$ e $y \Sigma x$ e $|F_x| \neq |F_y|$ deve essere per forza $x = y$. Quindi Σ risulta essere antisimmetrica.
- Siano $x, y, z \in X$ tali che $x \Sigma y$ e $y \Sigma z$. Allora o è $x = y$ e $y = z$, da cui $x = z$ e quindi $x \Sigma z$, oppure $|F_x| < |F_y| < |F_z|$ da cui $|F_x| < |F_z|$ e $x \Sigma z$. Quindi Σ è transitiva e quindi una relazione d'ordine in X .

(ii) Osservando l'insieme B possiamo osservare che Σ è determinata dall'ordine stretto tra le cardinalità delle parti di B :

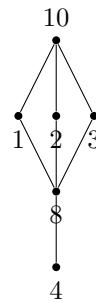
$$|\{4\}| < |\{5, 8\}| < |\{1, 2, 3\}| < |\{6, 7, 9, 10\}|$$

Due elementi nello stesso F_x sono in relazione Σ se e solo se questi coincidono. Quindi due elementi distinti risultano sempre in confrontabili in uno stesso F_x . Otteniamo quindi il seguente diagramma di Hasse:

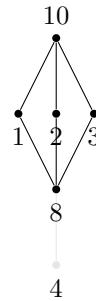


(iii) Dato che in un reticolo finito devono esistere minimo e massimo, osservando il fatto che risultano esserci 4 elementi massimali possiamo affermare che (X, Σ) non risulta essere un reticolo.

(iv) Sicuramente la parte $Y = \{4, 8, 1, 2, 3, 10\}$ risulta formare un reticolo con la relazione Σ :



(Y, Σ) non è complementato. Infatti preso l'elemento $3 \in Y$ si vede facilmente che non ha complemento.



Applicando infine il Criterio di Birkhoff osserviamo che è possibile individuare un sottoreticolo di (Y, Σ) isomorfo al reticolo trirettangolo, quindi Y non è distributivo. ■

Esercizio 6.4.8

Sia $A = \{1, 2, 3\} \times \{1, 2, 3\}$. Si consideri la relazione R definita su A come segue:

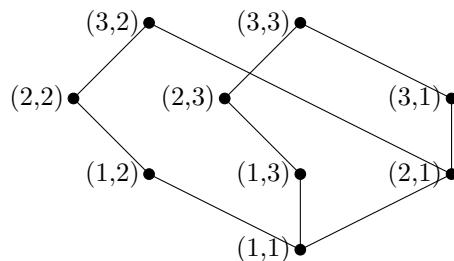
$$(a, b) R (c, d) \iff a \leq c \wedge b \mid d$$

1. Dimostrare che R è una relazione d'ordine parziale;
2. Determinare gli elementi massimali e minimali di A . Stabilire se esistono massimo e minimo;
3. Stabilire se A , munito della relazione d'ordine R , è un reticolo.

Svolgimento. Dimostriamo che R sia una relazione d'ordine:

1. Per ogni $(a, b) \in A$ si ha che $a \leq a$ e $b \mid b$, dunque $(a, b) R (a, b)$.
2. Supponiamo di avere due coppie (a, b) e (c, d) tali che $(a, b) R (c, d)$ e $(c, d) R (a, b)$. Allora deve essere $a \leq c$ e $c \leq a$ da cui $a = c$ e deve essere $b \mid d$ e $d \mid b$, da cui segue $b = d$. Allora $(a, b) = (c, d)$.
3. Se $a \leq c$ e $b \mid d$ e $c \leq e$ e $d \mid f$, allora $a \leq e$ e $b \mid f$. Quindi R risulta riflessiva, antisimmetrica e transitiva. Quindi è una relazione d'ordine parziale.

Per cercare elementi minimi o massimali ed eventuali massimi e minimi possiamo notare che la coppia $(1, 1)$ è in relazione con tutte le coppie $(a, b) \in A$ e risulta quindi un minimo. Al contrario, le coppie $(3, 2)$ e $(3, 3)$ risultano elementi massimali.



Dato che non esiste estremo superiore per la parte $\{(3, 2), (3, 3)\}$ possiamo affermare che (A, R) non è un reticolo. ■

Esercizio 6.4.9

Sull'insieme $A = \{a^n \mid a, n \in \mathbb{N}, a, n \geq 2\} \subseteq \mathbb{N}$ si definisca la relazione \leq ponendo:

$$a^n \leq b^m \iff a \mid b \wedge n \leq m$$

Si dica se \leq è una relazione d'ordine su A .

Svolgimento. Gli elementi di A non sono rappresentati univocamente da una coppia (a, n) . Ad esempio $2^4 = 4^2$. Si vede allora che la relazione proposta dall'esercizio non è ben definita: infatti da un lato risulterebbe $2^4 \leq 2^5$ (dato che $2 \mid 2$ e $4 \leq 5$) mentre anche $4^2 \not\leq 2^5$ (dato che $4 \nmid 2$). ■

Esercizio 6.4.10

Sull'insieme $A = \mathbb{N} \times \mathbb{N}$ si definisca la relazione \leq ponendo, per ogni $(a, b), (c, d) \in A$,

$$(a, b) \leq (c, d) \iff \begin{cases} a \leq c \\ a + d \leq b + c \end{cases}$$

1. Si provi che \leq è una relazione d'ordine e che non è totale;
2. Osservato che per ogni $(a, b) \in A$ si ha $(a, b) \leq (a+1, b)$, si provi che l'insieme ordinato (A, \leq) non ha né elementi massimali né minimali.
3. Posto $x = (0, 0)$ e $y = (1, 2)$ si provi che $\inf_A \{x, y\} = (0, 1)$.

Svolgimento. Si ha:

1. Proviamo che \leq è una relazione d'ordine su A :

- *Riflessività.* Per ogni $(a, b) \in A$ si ha banalmente $a \leq a$ e $a + b \leq b + a$; dunque $(a, b) \leq (a, b)$.
- *Antisimmetria.* Siano $(a, b), (c, d) \in A$ con $(a, b) \leq (c, d)$ e $(c, d) \leq (a, b)$; allora:

$$\begin{cases} a \leq c \\ a + d \leq b + c \end{cases} \quad \begin{cases} c \leq a \\ c + b \leq d + a \end{cases}$$

da cui segue subito $c = a$ e $d = (c + b) - a = a + b - a = b$.

- *Transitività.* Siano $(a, b), (c, d), (e, f) \in A$ con $(a, b) \leq (c, d)$ e $(c, d) \leq (e, f)$ allora:

$$\begin{cases} a \leq c \\ a + d \leq b + c \end{cases} \quad \begin{cases} c \leq e \\ c + f \leq d + e \end{cases}$$

da cui si ricava $a \leq e$ e:

$$\begin{aligned} a + f &= a + d - d + f \\ &\leq b + c - d + f \\ &= (c + f) - d + b \\ &\leq e + d - d + b \\ &= e + b \end{aligned}$$

Dunque $(a, b) \leq (e, f)$. Quindi (A, \leq) è un insieme ordinato. L'ordine non è totale perché, ad esempio, $(0, 0) \not\leq (1, 2)$ e $(1, 2) \not\leq (0, 0)$.

2. Sia $(a, b) \in A$. Allora, come si verifica subito dalla definizione $(a, b) \leq (a+1, b)$ e $(a, b+1) \leq (a, b)$. Questo prova che (A, \leq) non ha elementi massimali né minimali.
3. Sia $u = (a, b) \in A$. Allora $u \leq x$ se e solo se $a \leq 0$ e $a + 0 \leq b + 0$, cioè se e solo se $a = 0$; mentre $u \leq y$ se e solo se $a \leq 1$ e $a + 2 \leq b + 1$, ovvero se e solo se $a = 0, 1$ e $b \geq a + 1$. Pertanto l'insieme degli elementi minoranti di $\{x, y\}$ è:

$$\mathcal{M} = \{(0, b) \in A \mid b \geq 1\}$$

Ora, per ogni $b \geq 1$ si ha $(0, b) \leq (0, 1)$. Ne consegue che $(0, 1)$ è il massimo di \mathcal{M} e dunque è l'estremo inferiore di $\{x, y\}$. ■

Esercizio 6.4.11

Sull'insieme $A = \{(x, y) \mid x, y \in \mathbb{N} \wedge x, y \geq 2\}$ si definisca la relazione \leq ponendo:

$$(a, b) \leq (c, d) \iff (a \leq c \wedge b \mid d)$$

1. Si provi che \leq è una relazione d'ordine su A ;
2. Si determini gli eventuali massimo, minimo ed elementi massimali e minimali di (A, \leq) .
3. Sia $D = \{(x, y) \in A \mid x + y = 10\}$ si determinino, se esistono $\inf_A(D)$ e $\sup_A(D)$.

Svolgimento. Abbiamo:

1. Per dimostrare che \leq è una relazione d'ordine verifichiamo che soddisfi le proprietà riflessive, antisimmetriche e transitive:

- Per ogni coppia (a, b) deve essere $(a, b) \leq (a, b)$, infatti:

$$(a, b) \leq (a, b) \iff (a \leq a \wedge b \mid b)$$

e \leq risulta riflessiva;

- Siano (a, b) e (c, d) due coppie tali che $(a, b) \leq (c, d)$ e $(c, d) \leq (a, b)$. Abbiamo quindi:

$$(a \leq c \wedge b \mid d) \wedge (c \leq a \wedge d \mid b) \iff (a = c \wedge b = d) \iff (a, b) = (c, d)$$

per l'antisimmetria della relazione d'ordine usuale in \mathbb{N} e per le proprietà² degli elementi associati in \mathbb{N} . La relazione \leq risulta quindi antisimmetrica.

- Siano $(a, b), (c, d), (e, f)$ tre copie di A tali che $(a, b) \leq (c, d) \wedge (c, d) \leq (e, f)$. Abbiamo allora:

$$(a \leq c \wedge b \mid d) \wedge (c \leq e \wedge d \mid f)$$

Per la transitività della relazione d'ordine usuale abbiamo $a \leq e$. Inoltre, se $b \mid d$ e $d \mid f$ abbiamo:

$$\exists k \in \mathbb{N}(d = kb) \wedge \exists h \in \mathbb{N}(f = hd) \implies f = h(kb) = b(hk)$$

e quindi $b \mid f$. Allora $(a, b) \leq (e, f)$ e \leq è una relazione d'ordine.

2. Per ogni $(a, b) \in A$ osserviamo che $(a, b) \leq (a+1, b)$ quindi non ci sono elementi massimali (non esiste un elemento (\bar{a}, \bar{b}) di A tale che per ogni $(a, b) \in A$ si abbia $(a, b) \leq (\bar{a}, \bar{b})$) e dunque nemmeno massimi in (A, \leq) . Per quanto riguarda invece gli elementi minimali, consideriamo le coppie del tipo $(2, p)$ con p numero primo positivo: se $(a, b) \leq (2, p)$ allora $a \leq 2$ e $b \mid p$, da cui, poiché $a, b \geq 2$, si ha $(a, b) = (2, p)$. Quindi $(2, p)$ è un elemento minimale di (A, \leq) . Poiché esistono più elementi minimali allora non esiste il minimo.
3. Chiaramente $D = \{(2, 8), (3, 7), (4, 6), (5, 5), (6, 4), (7, 3), (8, 2)\}$. Sia $(a, b) \in A$ un elemento minorante per D allora in particolare $(a, b) \leq (2, 8)$, dunque $a = 2$ e $b \mid 8$, ma anche $(a, b) \leq (3, 7)$ da cui $b \mid 7$. Poiché $b \geq 2$, questo non è possibile. Pertanto non esistono minoranti, quindi nemmeno estremo inferiore di D . Sia ora $(a, b) \in A$ un maggiorante di D . Allora $x \leq a$ e $y \mid b$ per ogni $2 \leq x, y \in \mathbb{N}$ con $x + y = 10$. Poiché il minimo comune multiplo di 2, 3, 4, 5, 6, 7, 8 risulta essere 840, si conclude che $8 \leq a$ e $840 \mid b$. L'insieme dei maggioranti per D è dunque $\{(a, b) \in A \mid 8 \leq a, 840 \mid b\}$. Tale insieme ha un evidente minimo in (A, \leq) che è $(8, 840)$ ed è l'estremo superiore di D . ■

Esercizio 6.4.12

Sull'insieme $\mathcal{P}(\mathbb{N})$ si definisca la relazione \leq definita da:

$$\forall X, Y \in \mathcal{P}(\mathbb{N})(X \leq Y \iff X \subseteq Y \wedge Y \setminus X \text{ è finito})$$

1. Si provi che \leq è una relazione d'ordine su $\mathcal{P}(\mathbb{N})$ e si dica se è totale;
2. Si dica se l'insieme ordinato $(\mathcal{P}(\mathbb{N}), \leq)$ ha elementi minimali e/o minimi;

Svolgimento. Abbiamo:

1. Proviamo che \leq è una relazione d'ordine su $\mathcal{P}(\mathbb{N})$:

- *Riflessività.* Sia $X \in \mathcal{P}(\mathbb{N})$ allora $X \subseteq X$ e $X \setminus X = \emptyset$, quindi $X \leq X$;
- *Antisimmetria.* Siano $X, Y \in \mathcal{P}(\mathbb{N})$ con $X \leq Y$ e $Y \leq X$; allora in particolare $X \subseteq Y$ e $Y \subseteq X$, quindi $X = Y$;

²Vedi 7.1.3.

- *Transitività.* Siano $X, Y, Z \in \mathcal{P}(\mathbb{N})$ con $X \trianglelefteq Y$ e $Y \trianglelefteq Z$. Allora in particolare $X \subseteq Y$ e $Y \subseteq Z$, dunque $X \subseteq Z$. Inoltre, poiché X è contenuto in Y , $Y = X \cup (Y \setminus X)$ e analogamente $Z = Y \cup (Z \setminus Y)$ con $Y \setminus X$ e $Z \setminus Y$ finiti. Quindi:

$$Z = Y \cup (Z \setminus Y) = Z = X \cup (Y \setminus X) \cup (Z \setminus Y)$$

dunque $Z \setminus X \subseteq (Y \setminus X) \cup (Z \setminus Y)$ è finito e $X \trianglelefteq Z$. Pertanto $(\mathcal{P}(\mathbb{N}), \trianglelefteq)$ è un insieme ordinato. Chiaramente non è totale, ad esempio $\{1\} \not\trianglelefteq \{2\}$ e $\{2\} \not\trianglelefteq \{1\}$.

2. \emptyset è un elemento minimale dell'insieme ordinato ma non è minimo. Infatti se X è un sottoinsieme infinito di \mathbb{N} allora $\emptyset \not\trianglelefteq X$. Non vi sono altri elementi minimali, infatti se $0 \neq X \subseteq \mathbb{N}$ e $a \in X$ allora $X \setminus \{a\} \trianglelefteq X$. ■

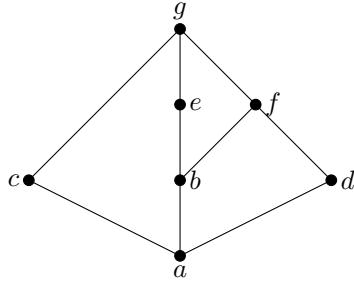
Esercizio 6.4.13

Sia $S = \{a, b, c, d, e, f, g\}$ dove $a = \emptyset$, $b = \{1\}$, $c = \{2, 3\}$, $d = \{4\}$, $e = \mathbb{N} \setminus 2\mathbb{N}$, $f = \{2^n / n \in \mathbb{N}\}$, $g = \mathbb{N}$.

1. Disegnare il diagramma di Hasse di (S, \subseteq) ;
2. Decidere se (S, \subseteq) sia un reticolo;
3. Verificare se (S, \subseteq) è distributivo, complementato o booleano;
4. (S, \subseteq) è un sottoreticolo di $(\mathcal{P}(\mathbb{N}), \subseteq)$?
5. Determinare, se esiste, un $h \in \mathcal{P}(\mathbb{N})$ tale che $(S \cup \{h\}, \subseteq)$ sia un reticolo booleano.

Svolgimento. Svolgiamo punto per punto:

1. L'idea è quella di partire dal basso, ovvero dall'insieme che sicuramente è incluso in tutti gli altri elementi di S , ossia l'elemento $a = \emptyset$. Successivamente notiamo che b, c e d sono tre elementi non confrontabili tra di loro che sicuramente includono a . Questi tre elementi faranno quindi parti del "livello" successivo. L'elemento d , essendo il singleton di 4 sicuramente è una parte di f in quanto $4 = 2^2 \in f$ mentre b , essendo il singleton di 1, ovvero un numero dispari, sicuramente è una parte di f ma anche di f in quanto $1 = 2^0 \in f$. Si ottiene così un secondo livello dato dagli elementi e ed f che sono infine parti di $\mathbb{N} = g$. Il diagramma di Hasse che si ottiene è il seguente:



2. Per definizione di reticolo deve essere:

$$\forall x, y \in S (\exists \inf_{\subseteq} \{x, y\} \wedge \exists \sup_{\subseteq} \{x, y\})$$

Poiché $\forall x, y \in S$ sono equivalenti le formule $x \subseteq y$, $x = \min\{x, y\}$ e $\inf\{x, y\}$ basterà confrontare tutte le coppie non confrontabili e stabilire se per queste esistono gli estremi inferiori e superiori. Tali coppie sono:

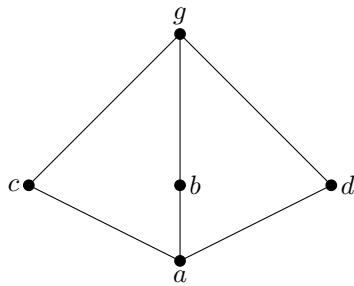
$$\{c, b\}, \quad \{c, d\}, \quad \{b, d\} \quad \{e, f\}$$

e si ha:

$$\begin{cases} \inf_{\subseteq} \{c, b\} = a \\ \sup_{\subseteq} \{c, b\} = g \end{cases} \quad \begin{cases} \inf_{\subseteq} \{c, d\} = a \\ \sup_{\subseteq} \{c, d\} = g \end{cases} \quad \begin{cases} \inf_{\subseteq} \{b, d\} = a \\ \sup_{\subseteq} \{b, d\} = f \end{cases} \quad \begin{cases} \inf_{\subseteq} \{e, f\} = b \\ \sup_{\subseteq} \{e, f\} = g \end{cases}$$

Quindi (S, \subseteq) è un reticolo.

3. Per il Criterio di Birkhoff (S, \subseteq) non è distributivo se qualche suo sottoreticolo è isomorfo al reticolo pentagonale oppure al reticolo trirettangolo. Se osserviamo il seguente sottoreticolo:



Si vede che è isomorfo al reticolo trirettangolo. Concludiamo così che (S, \subseteq) non è distributivo.

Per definizione di reticolo complementato, (S, \leq) deve essere un reticolo limitato (ovvero devono esistere minimo e massimo) ed ogni elemento del reticolo deve ammettere almeno un complemento: ovvero per ogni $x \in S$ deve esistere un $y \in S$ tale che

$$(x \wedge y = \min(S, \leq) = a) \wedge (x \vee y = \max(S, \leq) = g)$$

Chiaramente (S, \leq) è limitato e la richiesta ha senso. Se prendiamo ad esempio $g = \mathbb{N}$ e $a = \emptyset$ sono l'uno il complemento dell'altro. Presi quindi $x \in S$ tale che $x \neq g, a, c$ allora:

$$\begin{cases} \sup_{\leq}\{c, x\} = g = \mathbb{N} \\ \inf_{\leq}\{c, x\} = a = \emptyset \end{cases}$$

Quindi ogni $x \in S$ diverso da a, c, g è complementato da c (non è l'unico). In particolare c ha x come complemento. Quindi S è complementato. Per definizione di reticolo booleano, (S, \leq) deve essere sia distributivo che complementato. Poiché S non è distributivo allora non è booleano.

4. Per essere un sottoreticolo di $(\mathcal{P}(\mathbb{N}), \subseteq)$ S deve essere stabile secondo le operazioni reticolari del reticolo delle parti di \mathbb{N} ovvero \cup e \cap . Notiamo però che:

$$b \cup c = \{1\} \cup \{2, 3\} = \{1, 2, 3\} \notin S$$

Quindi S non è stabile e di conseguenza non risulta un sottoreticolo. Questa verifica può essere fatta anche osservando il diagramma di Hasse del reticolo S . Poiché le operazioni reticolari \cap e \cup mappano ogni coppia del reticolo rispettivamente nel loro estremo inferiore ed estremo inferiore, se si osservano i punti c ed e si ha:

$$\{2\} = c \cap e \neq \inf_{\leq}\{c, e\} = \emptyset$$

5. Il problema del reticolo S era la distributività. Infatti si era dimostrato al punto 3 che il reticolo S non è distributivo in quanto il sottoreticolo $(\{a, c, b, d, g\}, \leq)$ è isomorfo al reticolo trirettangolo. Essendo il reticolo trirettangolo uno dei più piccoli tra i reticoli non distributivi, aggiungendo un elemento ad S nulla cambierebbe in quanto resterebbe sempre invariato il sottoreticolo $(\{a, c, b, d, g\}, \leq)$. ■

Esercizio 6.4.14

Disegnare un diagramma di Hasse dell'insieme $\{n \in \mathbb{N} / n < 10\}$ ordinato per divisibilità in \mathbb{N} e decidere se questo insieme ordinato è un reticolo.

Esercizio 6.4.15

Per ogni $n \in \{8, 12, 18, 30, 31, 2^{10}\}$ disegnare un diagramma di Hasse dell'insieme D_n dei divisori (in (\mathbb{N}, \cdot)) di n , ordinato per divisibilità in \mathbb{N} , e decidere se $(D_n, |)$ è o non è un reticolo. Trovare tra questi insiemi ordinati, quali sono isomorfi tra loro.

Esercizio 6.4.16

Esiste in $\mathcal{P}(\mathbb{N})$ una parte infinita che sia totalmente ordinata per inclusione (cioè dall'ordinamento indotto dall'inclusione in $\mathcal{P}(\mathbb{N})$)?

Esercizio 6.4.17

In ciascuno dei seguenti insiemi, ordinati dalla relazione di inclusione, determinare gli eventuali minimali, massimali, minimo, massimo:

1. $\mathcal{P}(\mathbb{Z})$
2. $\mathcal{P}_{fin}(\mathbb{Z})$ (l'insieme delle parti finite di \mathbb{Z})
3. $\mathcal{P}(\mathbb{Z}) \setminus \mathcal{P}_{fin}(\mathbb{Z})$ (l'insieme delle parti infinite di \mathbb{Z})
4. $\mathcal{P}(\mathbb{Z}) \setminus \mathcal{P}(\mathbb{N})$

Esercizio 6.4.18

La relazione binaria τ definita in \mathbb{N} ponendo, per ogni $a, b \in \mathbb{N}$, $a\tau b$ se e solo se $ba \in \mathbb{N} \setminus \{1\}$ è d'ordine?

Esercizio 6.4.19

Sia $X = \{a, b, c, d, e, f, g, h\}$ in modo che valga $|X| = 8$. Verificare che la relazione binaria ρ in X di grafico:

$$\left\{ \begin{array}{llllll} (a, b), & (a, c), & (a, d), & (a, e), & (a, f), \\ (a, g), & (a, h), & (b, d), & (b, e), & (b, f), \\ (b, g), & (b, h), & (c, d), & (c, e), & (c, f), \\ (c, g), & (c, h), & (d, e), & (d, f), & (d, g), \\ (d, h), & (e, f), & (g, f) \end{array} \right\}$$

è un ordinamento in X e disegnarne il diagramma di Hasse. Rispetto a questo ordinamento si indichino gli eventuali minimo, massimo, elementi minimi, elementi massimali in X . Se esistono, si calcolino $\sup\{b, c, h\}$, $\inf\{b, c, h\}$, $\sup\{b, e, h\}$, $\inf\{b, e, h\}$. Quali elementi di X sono confrontabili con ogni altro elemento di X ? Infine, si stabilisca se X ordinato da ρ è un insieme totalmente ordinato, un reticolo, un reticolo completo, un reticolo distributivo, un'algebra di Boole.

Esercizio 6.4.20

Trovare un isomorfismo di reticolari dall'insieme delle parti di $\{0, 1\}$ all'insieme delle parti di $\{3, 4\}$, ordinati per inclusione.

Esercizio 6.4.21

Stabilire per quali interi n nell'insieme $\{2, 14, 18, 27, 30\}$ il reticolo dei numeri naturali divisori di n è complementato.

Esercizio 6.4.22

Trovare, tra i sottoinsiemi di $\mathcal{P}(\mathbb{N})$, ordinati per inclusione:

1. un sottoinsieme di cardinalità 5 che non sia un reticolo;
2. un sottoinsieme di cardinalità 5 che sia un reticolo trirettangolo;
3. un sottoinsieme di cardinalità 5 che sia un reticolo pentagonale.

Esercizio 6.4.23

Ogni insieme delle parti, ordinato mediante l'inclusione, è un reticolo. Infatti, dimostrare che dati $A, B \subseteq Z$, $\inf(A, B) = A \cap B$, e $\sup(A, B) = A \cup B$.

ARITMETICA E POLINOMI

7.1

ARITMETICA NELL'INSIEME DEGLI INTERI



7.1.1 ■ Il principio di buon ordinamento

Definizione 7.1.1: Relazione di buon ordine

Sia S un insieme non vuoto. Una relazione d'ordine \leq in S si dice una **relazione di buon ordine** se ogni parte non vuota di S è dotata di minimo rispetto a \leq . Se \leq è una relazione di buon ordine, la coppia (S, \leq) si dice **insieme bene ordinato**.

Lemma 7.1.1

Sia S un insieme non vuoto, e sia \leq una relazione di buon ordine in S . Allora \leq è una relazione d'ordine totale in S .

Dimostrazione. Siano x e y elementi di S . Allora la parte non vuota $\{x, y\}$ di S è dotata di minimo \bar{x} , e risulta $\bar{x} = x$ oppure $\bar{x} = y$. Quindi $x \leq y$ oppure $y \leq x$, e \leq è una relazione d'ordine totale per la generalità degli elementi x, y . \square

7.1.2 ■ Insiemi naturalmente ordinati

Definizione 7.1.2: Relazione d'ordine naturale

Una relazione d'ordine \leq in S si dice una **relazione d'ordine naturale** se ogni parte non vuota di S è dotata di minimo e, se superiormente limitata, anche di massimo rispetto a \leq .

Osservazione 7.1.1



Ovviamente ogni relazione d'ordine naturale è anche una relazione di buon ordine.

Si scelga un insieme naturalmente ordinato non superiormente limitato (\mathbb{N}, \leq) . Il Teorema sugli isomorfismi tra insiemi ordinati (Teorema 6.1.1) assicura che, se (S, \leq) è un qualunque altro insieme naturalmente ordinato non superiormente limitato esiste una applicazione biettiva e crescente $f : \mathbb{N} \rightarrow S$ sicché in particolare \mathbb{N} ed S sono equipotenti. Questa proprietà è sufficiente a rendere indifferente la scelta dell'insieme ordinato (\mathbb{N}, \leq) . Gli elementi di \mathbb{N} saranno chiamati **numeri naturali** ed \mathbb{N} è detto **insieme dei numeri naturali**. Con il simbolo \mathbb{N}^* denoteremo invece l'insieme dei numeri naturali positivi, ovvero:

$$\mathbb{N}^* = \{1, 2, 3, 4, 5, \dots\}$$

Dimostriamo quindi il principio d'induzione introdotto nella sezione 4.2.

Dimostrazione. Sia $X = \{n \in \mathbb{N}_b \mid \neg(p(n))\}$. Se $X \neq \emptyset$ allora, essendo \mathbb{N} ben ordinato esiste il minimo di (X, \leq) , sia esso m . Si ha ovviamente che $m \neq b$ in quanto $p(b)$ è vera per ipotesi. Quindi $b \notin X$ e allora $m > b$. Tuttavia $m - 1 < m = \min X$, dunque $m - 1 \notin X$ e $p(m - 1)$ risulta vera. Applicando il passo induttivo si avrebbe però:

$$p(m - 1) \implies p((m - 1) + 1) = p(m)$$

che è chiaramente una contraddizione rispetto alle ipotesi in quanto $p(m)$ risulta falsa. Quindi $X = \emptyset$ e per ogni $n \in \mathbb{N}_b$ si ha che risulta vera la proposizione $p(n)$. \square

Proposizione 7.1.1 (Principio d'induzione - Seconda Forma)

Per ogni $t \in \mathbb{N}_b$ definiamo l'insieme $M_t = \{x \in \mathbb{N}_b \mid x < t\} = [b, t[$. È valida la seguente implicazione:

$$\forall t \in \mathbb{N}_b \left(\left(\forall n \in M_t (p(n)) \implies p(t) \right) \implies \left(\forall n \in \mathbb{N}_b (p(n)) \right) \right)$$

7.1.3 ■ Divisibilità e fattorizzazione

Nella sezione 6.1.1 è stato introdotto la relazione di divisibilità. Sia qui $(M, \cdot, 1)$ un monoide commutativo. La relazione di divisibilità in M è definita come:

$$\forall a, b \in M (a | b \iff \exists c \in M (b = ac)) \quad (7.1)$$

Definizione 7.1.3: Elementi associati

Per ogni $a, b \in S$ si dice che a e b sono **associati** e si indica con la notazione $a \sim b$ se e soltanto se:

$$(a \sim b) \iff (a | b \wedge b | a) \quad (7.2)$$

Proposizione 7.1.2

Se (S, \cdot) è un semigruppo allora $|$ è una relazione transitiva.

Dimostrazione. Per ogni $x, y, z \in S$ tali che $(x | y \wedge y | z)$ esistono $c, d \in S$ per i quali $(y = xc \wedge z = yd)$, sostituendo $y = xc$ in $z = yd$ si ottiene: $z = x(cd)$ e quindi $x | z$. \square

Proposizione 7.1.3

Se (S, \cdot) è un monoide allora $|$ è riflessiva.

Dimostrazione. Preso 1_S elemento neutro in (S, \cdot) si ha che per ogni $a \in S (a = a \cdot 1_S) \implies a | a$. \square

Proposizione 7.1.4

Se (S, \cdot) è un monoide, la relazione di divisibilità $|_{(S,\cdot)}$ è una relazione d'ordine se e soltanto se è antisimmetrica. Vale cioè:

$$|_{(S,\cdot)} \in \mathbf{OL}(S) \iff \forall a, b \in S (a | b \wedge b | a \implies a = b)$$

Dimostrazione. Abbiamo:

\Leftarrow Banale

\implies Siano $a, b \in S$ tali che $a | b$ e $b | a$. Per definizione di divisibilità in S abbiamo:

$$\begin{cases} \exists c_1 \in S (b = a \cdot c_1) \\ \exists c_2 \in S (a = b \cdot c_2) \end{cases}$$

Sostituendo l'espressione di b nella seconda relazione, otteniamo:

$$\begin{aligned} a &= (a \cdot c_1) \cdot c_2 \\ &= a \cdot (c_1 \cdot c_2) \end{aligned}$$

(Applicando l'associatività di \cdot in S)

Poiché S è un monoide, esiste un elemento neutro 1_S tale che $a = a \cdot 1_S$, deve essere $(c_1 \cdot c_2) = 1_S$ e risultano essere uno l'inverso dell'altro, e in particolare cancellabili per il Teorema 5.2.2. Quindi:

$$c_1 \cdot a = c_1 \cdot b \implies a = b$$

Quindi $|_{(S,\cdot)}$ è antisimmetrica. □

Esempio 7.1.1

La relazione di divisibilità in (\mathbb{N}, \cdot) è di ordine largo; infatti $a \sim b \iff a = b$. Non è antisimmetrica in (\mathbb{Z}, \cdot) , infatti $(1 \mid -1) \wedge (-1 \mid 1)$ ma $-1 \neq 1$.

L'essere associati risulta chiaramente essere una relazione di equivalenza in quanto è:

1. **Riflessiva:** $\forall a \in M$ sicuramente $a \mid a$ in quanto esiste $1 \in M$ tale che $a = 1a$;
2. **Simmetrica:** se $a \sim b$ sicuramente $b \sim a$ per la commutatività della congiunzione;
3. **Transitiva:** se $a \sim b$ e $b \sim c$ allora sicuramente $a \sim c$.

Proposizione 7.1.5

Per ogni $a, b \in M$, siano $a \sim a'$ e $b \sim b'$. Allora:

$$a \mid b \iff a' \mid b'$$

Dimostrazione. Se $a \mid b$ allora, per ipotesi, $a' \mid a$, $a \mid b$, $b \mid b'$. Quindi $a' \mid b'$ per la transitività della relazione. Il viceversa è equivalente. □

Proposizione 7.1.6

Per ogni $a, b \in M$:

$$a \sim b \iff \text{Div}(a) = \text{Div}(b) \iff aM = bM$$

Ovvvero: due elementi sono associati se hanno gli stessi divisori e gli stessi multipli. Infatti $\text{Div}(a) = \{d \in M \mid d \mid a\}$ e $aM = \{ax \mid x \in M\} = \{m \in M \mid a \mid m\}$.

Dimostrazione. Si ha:

- \implies Per ogni $d \in \text{Div}(a)$ da $d \mid a$ e $a \mid b$ segue $d \mid b$ per transitività. Quindi $d \in \text{Div}(b)$ e $\text{Div}(a) \subseteq \text{Div}(b)$. Chiaramente vale anche l'inclusione inversa e quindi $\text{Div}(a) = \text{Div}(b)$.
- \impliedby Poiché $a \in \text{Div}(a)$, se vale $\text{Div}(a) = \text{Div}(b)$ allora $a \in \text{Div}(b)$ e $a \mid b$. Similmente $b \in \text{Div}(a)$ e $b \mid a$ quindi $a \sim b$. □

Proposizione 7.1.7

Per ogni $u \in \mathcal{U}(M)$, per ogni $a \in M$ vale: $a \sim au$.

Dimostrazione. Si ricordi che $\mathcal{U}(M)$ è l'insieme degli elementi invertibili di M . Quindi per ogni $x \in \mathcal{U}(M)$ esiste $u' \in \mathcal{U}(M)$ tale che $u \cdot u' = 1$. Ovviamente $a \mid au$ e, se consideriamo $a = (au)u'$ allora $au \mid a$. □

Proposizione 7.1.8

Se a è cancellabile in M allora:

$$[a]_\sim = \{au \mid u \in \mathcal{U}(M)\}$$

Dimostrazione. Per la proposizione precedente si ha che $\forall u \in \mathcal{U}(M)(a \sim au)$, quindi sicuramente $\{au \mid u \in \mathcal{U}(M)\} \subseteq [a]_\sim$. Per verificare l'uguaglianza basta completare la verifica della doppia inclusione: ovvero dimostrare che ogni elemento associato ad a è della forma au per un opportuno $u \in \mathcal{U}(M)$. Sia quindi $b \in M$ tale che $b \sim a$, ovvero $b \in [a]_\sim$. Chiaramente, per definizione di elemento associato $a \mid b$ e quindi esiste $u \in M$ tale che $b = au$. Vale inoltre $b \mid a$ e quindi esiste $v \in M$ tale che $a = bv$. Allora:

$$a \cdot 1_M = a = bv = (au)v = a(uv)$$

Poiché a è cancellabile per ipotesi deve essere $uv = 1_M$ e quindi $v = u^{-1}$ e $u, v \in \mathcal{U}(M)$. □

Osservazione 7.1.2

In \mathbb{N} gli elementi associati devono essere per forza uguali in quanto esiste un solo elemento invertibile.

Definizione 7.1.4: Divisori banali e propri

Per ogni elemento a in un monoide commutativo M , tra i divisori di a ci sono:

- Gli elementi associati ad a ;
- Gli elementi invertibili di M ;

Chiameremo questi elementi **divisori banali** di a . Un divisore di un elemento a si dice **proprio** se non è associato ad a .

Definizione 7.1.5: Elementi irriducibili

Un elemento si dice **irriducibile** in (M, \cdot) se e solo se $a \notin \mathcal{U}(M)$ e non ha divisori propri in M , ovvero se:

1. a non è invertibile;
2. gli unici divisori di a sono i divisori banali.

Osservazione 7.1.3

Sia $M = (\mathbb{N}^*, \cdot)$, gli elementi irriducibili di M sono detti **numeri primi**. Tali elementi ammettono come divisori solo 1 e sé stessi. L'elemento 1 non è primo in quanto risulta essere invertibile in \mathbb{N}^* .

7.1.3.1 Fattorizzazione in irriducibili

Teorema 7.1.1 (Fondamentale dell'Aritmetica)

Sia $a \in M$. Tale elemento o è esprimibile come prodotto di elementi irriducibili oppure è esso stesso irriducibile. Inoltre se $a = p_1 \cdot p_2 \cdot \dots \cdot p_t = q_1 \cdot q_2 \cdot \dots \cdot q_s$ con $t, s \in \mathbb{N}^*$ e $p_1, p_2, \dots, p_t, q_1, q_2, \dots, q_s$ elementi irriducibili, allora $s = t$ ed esiste una permutazione σ di $\{1, \dots, s\}$ tale che $p_i = \pm q_{\sigma(i)}$ per ogni $i = 1, \dots, s$.

Definizione 7.1.6: Monoide fattoriale

Un monoide commutativo (M, \cdot) si dice **fattoriale** se e solo se esso è cancellativo (ogni elemento risulta cancellabile) ed ogni elemento di $M \setminus \mathcal{U}(M)$ è prodotto di irriducibili in modo essenzialmente unico.

Definizione 7.1.7: Anello fattoriale

Un anello non nullo A si dice **fattoriale** se è un dominio di integrità unitario e se $(A \setminus \{0\}, \cdot)$ è un monoide fattoriale.^a

^aA può anche prendere il nome di **dominio a fattorizzazione unica**, spesso abbreviato in UFD, dall'inglese *Unique Factorization Domain*.

Corollario 7.1.1

Risultano essere monoidi fattoriali: $(\mathbb{N}^*, \cdot, 1)$, $(\mathbb{Z} \setminus \{0\}, \cdot, 1)$. La struttura $(\mathbb{Z}, +, \cdot)$ è un anello fattoriale.

Di questo corollario non forniremo la dimostrazione completa, bensì mostreremo che:

Lemma 7.1.2

Ogni intero diverso da 0, 1 e -1 è prodotto di primi.

Dimostrazione. Per assurdo si supponga non vuoto l'insieme:

$$X := \{n \in \mathbb{N} \mid n > 1 \wedge n \text{ non è prodotto di numeri primi}\}$$

Essendo \mathbb{N} un insieme ben ordinato allora esisterà il minimo di tale insieme X . Sia esso m : tale elemento risulta essere non primo, e poiché $m > 1$, esso avrà qualche divisore non banale; sia a uno di questi. Esisterà quindi $b \in \mathbb{N}^*$ per il quale $m = ab$,

con $1 < a < m$ e $1 < b < m$. Ne segue che $a, b \notin X$ dato che $m = \min(X)$. Quindi a, b sono prodotti di primi e allora anche m dovrà per forza esserlo. \square

Esempio 7.1.2

Un esempio di domini a fattorizzazione unica è dato dai campi, come il campo dei numeri razionali \mathbb{Q} o reali \mathbb{R} : in questo caso, tutti gli elementi non nulli sono invertibili, e quindi tutte le fattorizzazioni sono banali.

Lemma 7.1.3 (di Gauss)

Per ogni $p \in \mathbb{Z}$ vale la seguente implicazione:

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

Dimostrazione. Per il Teorema Fondamentale dell'Aritmetica possiamo scrivere a e b come prodotti di primi:

$$\begin{aligned} a &= p_1 \cdot p_2 \cdot \dots \cdot p_n \\ b &= q_1 \cdot q_2 \cdot \dots \cdot q_m \end{aligned}$$

Se per ipotesi $p \in \mathbb{P}$, dove \mathbb{P} è l'insieme dei numeri primi, e $p \mid ab$ allora esiste $c \in \mathbb{Z}$ per il quale $ab = pc$ e anche c risulta essere primo o prodotto di primi. Sia $c = m_1 \cdot m_2 \cdot \dots \cdot m_t$ allora:

$$\underbrace{(p_1 \cdot p_2 \cdot \dots \cdot p_n)}_a \underbrace{(q_1 \cdot q_2 \cdot \dots \cdot q_m)}_b = p \underbrace{(m_1 \cdot m_2 \cdot \dots \cdot m_t)}_c$$

Per l'unicità della scrittura deve essere quindi $p = p_i$ oppure $p = q_j$ per opportuni indici i, j . \square

Proposizione 7.1.9

In \mathbb{N}^* sia $a = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot \dots \cdot P_T^{\alpha_t}$, dove $t \in \mathbb{N}^*$, per ogni $i \in \{1, \dots, t\}$ si ha $P_i \in \mathbb{P}$ e $\alpha_i \in \mathbb{N}$. Inoltre per ogni $i \neq j$ si ha $P_i \neq P_j$. I divisori di a in \mathbb{N}^* sono tutti e soli i numeri della forma $P_1^{\lambda_1} \cdot \dots \cdot P_t^{\lambda_t}$ dove per ogni $i \in \{1, \dots, t\}$ si ha $\alpha_i \geq \lambda_i$. Questi divisori sono esattamente $(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \dots \cdot (\alpha_t + 1)$.

Esempio 7.1.3

Si consideri il numero 12 e la sua scomposizione in fattori primi:

$$12 = 2^2 \cdot 3^1$$

Si avrà che il numero di divisori di 12 è pari a $(2+1)(1+1) = 3 \cdot 2 = 6$. Infatti $|Div(12)| = 6$ ed è possibile esprimere tale insieme nella seguente forma:

$$Div(12) = \{2^{\lambda_1} \cdot 3^{\lambda_2} \mid \lambda_1 \in \{0, 1, 2\} \wedge \lambda_2 \in \{0, 1\}\}$$

Risultano elementi di $Div(12)$ quindi i numeri ottenuti calcolando le varie espressioni:

$$\begin{array}{ll} 2^0 \cdot 3^0 = 1 & 2^0 \cdot 3^1 = 3 \\ 2^1 \cdot 3^0 = 2 & 2^1 \cdot 3^1 = 6 \\ 2^2 \cdot 3^0 = 4 & 2^2 \cdot 3^1 = 12 \end{array}$$

Lemma 7.1.4

Siano R un anello commutativo unitario e $a, b, c \in R$. Allora:

$$(a \mid b \wedge a \mid c) \implies (\forall u, v \in R)(a \mid bu + cv) \quad (7.3)$$

Dimostrazione. Se $a \mid b$ e $a \mid c$ esistono $\beta, \delta \in R$ tale che $b = a\beta$ e $c = a\delta$. Siano ora $u, v \in R$ e consideriamo la combinazione lineare $bu + cv$. Abbiamo allora:

$$\begin{aligned} bu + cv &= (a\beta)v + (a\delta)u \\ &= a(\beta v) + a(\delta u) \\ &= a(\beta v + \delta u) \end{aligned}$$

Che risulta essere multiplo di a . Allora $a \mid (bu + cv)$ per ogni $u, v \in R$. Quindi se due elementi sono multipli di a , tutte le combinazioni lineari tra i due elementi sono multipli di a . \square

7.1.4 ■ Algoritmo euclideo, MCD ed equazioni diofantee

Se a e b sono numeri interi, si dice che a divide b , in simboli $a \mid b$, se e solo se esiste $c \in \mathbb{Z}$ tale che $b = ac$. Si può subito notare che:

- 1 e -1 sono gli unici interi che dividono ogni intero;
- 0 è l'unico intero che sia diviso da ogni intero;
- $\forall a, b \in \mathbb{Z} (a \mid b \iff -a \mid b \iff a \mid -b \iff -a \mid -b)$.

L'insieme dei divisori (in \mathbb{Z}) di un intero n si indica come $D(n)$. Dunque, per ogni $n \in \mathbb{Z}$:

$$D(n) := \{a \in \mathbb{Z} \mid a \mid n\} \quad (7.4)$$

Definizione 7.1.8: Massimo comun divisore

Siano $a, b \in \mathbb{Z}$. Un numero d si dice **massimo comune divisore** di a e b se:

- $d \mid a$ e $d \mid b$
- $\forall c \in \mathbb{Z} ((c \mid a \wedge c \mid b) \implies c \mid d)$

Dunque, un massimo comun divisore tra a e b è un divisore comune ad a e b che sia diviso da ogni altro divisore comune di a e b .

Definizione 7.1.9: Minimo comune multiplo

Siano a e b numeri naturali non nulli. Un numero naturale m si dice **minimo comune multiplo** di a e b se m è multiplo comune di a e b e inoltre divide ogni altro multiplo comune di a e b .

Il massimo comun divisore non negativo tra due interi a e b viene spesso indicato con il simbolo $MCD(a, b)$. Se una coppia (a, b) di elementi di un semigruppo commutativo regolare unitario M è dotata di massimo comun divisore e di minimo comune multiplo, questi non sono necessariamente unici. Si ha però:

- Se d è un massimo comun divisore tra due interi a e b , allora d e $-d$ sono gli unici massimi comuni divisori tra a e b . Dunque, calcolare un MCD tra due interi equivale a calcolarli tutti.
- Per ogni $a, b \in \mathbb{Z}$, i divisori comuni ad a e b sono tutti e soli i divisori comuni ad $|a|$ e $|b|$; quindi i massimi comuni divisori tra a e b sono tutti e soli i massimi comuni divisori tra $|a|$ e $|b|$.

Il calcolo dei massimi comuni divisori tra 0 ed un arbitrario intero è immediato, come segue da queste altre due osservazioni:

- Se a e b sono interi e $a \mid b$ allora a è un massimo comun divisore tra a e b .
- Per ogni $a \in \mathbb{Z}$, si ha che a è un massimo comun divisore tra a e 0.

Osservazione 7.1.4

Siano $a, b \in \mathbb{N}^*$ con $a = p_1^{\alpha_1} \cdot \dots \cdot p_t^{\alpha_t}$ e $b = p_1^{\beta_1} \cdot \dots \cdot p_t^{\beta_t}$, i divisori comuni sono i numeri della forma $p_1^{\lambda_1} \cdot \dots \cdot p_t^{\lambda_t}$ dove per ogni $i \in \{1, \dots, t\}$ si ha $\lambda_i \leq \min\{\alpha_i, \beta_i\} = \delta_i$. Allora presi gli esponenti δ_i così individuati, il massimo comun divisore di a e b è:

$$d = p_1^{\delta_1} \cdot \dots \cdot p_t^{\delta_t}$$

Analogamente, scelto $u_i = \max\{\alpha_i, \beta_i\}$ il numero:

$$m = p_1^{u_1} \cdot \dots \cdot p_t^{u_t}$$

risulta essere il minimo comune multiplo.

Il metodo di calcolo di un massimo comun divisore tra due interi a e b appena ricordato è molto rapido ed efficace nel caso in cui a e b siano numeri di valore assoluto sufficientemente piccolo da renderne semplice la scomposizione in fattori primi. Quando si ha a che fare con numeri più grandi questo metodo risulta invece spesso impraticabile, dal momento che non sono noti metodi che permettano di scomporre in tempi ragionevolmente brevi numeri interi arbitrari; anzi, il calcolo dei fattori primi di un intero può rivelarsi di estrema complessità computazionale. Per questo è molto importante disporre di un metodo alternativo, quello fornito dall'algoritmo euclideo, che ora illustreremo e che si dimostra essere invece molto efficiente.

Teorema 7.1.2 (della divisione con resto)

Siano n ed m numeri interi relativi con $m \neq 0$. Allora esistono e sono univocamente determinati dei numeri interi q ed r tali che:

$$n = mq + r \wedge 0 \leq r < |m| \quad (7.5)$$

In tal caso q ed r prendono il nome di **quoziente** e **resto** della divisione euclidea mentre n e m sono chiamati rispettivamente **dividendo** e **divisore**.

Dimostrazione. Dividiamo la dimostrazione in due parti:

Esistenza Dimostriamo innanzitutto l'esistenza dei numeri interi q ed r . Si supponga $n \geq 0$ e si proceda per induzione su n . Se $n = 0$ si ha:

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

e basta quindi porre $q = r = 0$. Sia $n > 0$ e si assuma l'asserto vero per tutti i numeri interi non negativi minori di n . Se $n < |m|$, risulta $n = (m \cdot 0) + n$ ed è sufficiente porre $q = 0$ ed $r = n$. Sia quindi $n \geq |m|$. Allora, portando $|m|$ a sinistra si ottiene:

$$0 \leq n - |m| < n$$

e, per ipotesi induttiva, esistono q_1 e r_1 tali che $n - |m| = mq_1 + r_1$ con $0 \leq r_1 < |m|$. Quindi:

$$n = |m| + mq_1 + r_1$$

Se $m > 0$ si ha:

$$n = m(q_1 + 1) + r_1$$

e basta porre $q = (q_1 + 1)$ e $r = r_1$. Se invece $m < 0$ risulta:

$$n = m(q_1 - 1) + r_1$$

e quindi si può scegliere $q = q_1 - 1$ e $r = r_1$.

Se $n < 0$ è sufficiente ragionare a partire dal fatto che $-n$ è positivo e che, per la prima parte della dimostrazione, esistono q' ed r' tali che $-n = mq' + r'$.

Unicità Siano q_1, q_2, r_1, r_2 numeri interi relativi tali che:

$$n = mq_1 + r_1 = mq_2 + r_2$$

con

$$\begin{aligned} 0 \leq r_1 &< |m| \\ 0 \leq r_2 &< |m| \end{aligned}$$

Per fissare le idee supponiamo $r_1 \leq r_2$, ovvero $r_2 - r_1 \geq 0$. Allora risulta:

$$m(q_1 - q_2) = r_2 - r_1$$

e quindi:

$$|m| \cdot |q_1 - q_2| = |r_2 - r_1| = r_2 - r_1 \leq r_2 < |m|$$

Pertanto $|q_1 - q_2| < 1$, e allora $|q_1 - q_2| = 0$ e $q_1 = q_2$. Quindi $r_2 - r_1 = 0$ e perciò $r_2 = r_1$ il che completa la dimostrazione del Teorema. \square

Lemma 7.1.5

Siano $a, b, q, r \in \mathbb{Z}$ tali che q ed r siano il quoziente ed il resto della divisione euclidea di a e b . Allora i divisori comuni ad a e b sono tutti e soli i divisori comuni di b ed r . In particolare, i massimi comuni divisori tra a e b sono precisamente i massimi comuni divisori tra b ed r .

Dimostrazione. Sia c un divisore comune a b ed r . Poiché a è combinazione lineare di b ed r , allora $c \mid a$ per il lemma precedente. Dunque c è un divisore comune dia e b . Abbiamo provato così l'inclusione:

$$D(b) \cap D(r) \subseteq D(a) \cap D(b)$$

Per provare l'inclusione opposta, osserviamo che $r = a - bq$ è combinazione lineare di a e b , quindi, come per il passaggio precedente, ogni divisore comune ad a e b divide r ed è così un divisore comune a b ed r . Abbiamo così dimostrato l'uguaglianza $D(a) \cap D(b) = D(b) \cap D(r)$. \square

7.1.4.1 L'algoritmo euclideo delle divisioni successive

Di seguito mostreremo un approccio costruttivo per la ricerca di un massimo comune divisore tra due numeri, tale metodo prende il nome di **algoritmo euclideo delle divisioni successive**.

Supponiamo di voler calcolare un massimo comun divisore tra due interi a e b . Come visto sopra possiamo supporre che essi siano entrambi positivi. Possiamo ovviamente anche supporre $a \geq b$, infatti se $a < b$ basta scambiare tra loro a e b , dal momento che $MCD(a, b) = MCD(b, a)$. Come sappiamo, per il Teorema 7.1.2, si può effettuare la divisione euclidea di a per b .

Esistono dunque (e sono univocamente determinati) due numeri naturali q ed r tali che $a = bq + r$ ed $0 \leq r < b$. Il Lemma 7.1.5 mostra che vale l'uguaglianza $MCD(a, b) = MCD(b, r)$. Possiamo quindi tradurre il problema originale con un problema simile: quello del calcolo del massimo comun divisore tra b ed r .

Il vantaggio di questa riformulazione consiste in questo, che se consideriamo la “grandezza” dei due numeri a e b come misura della difficoltà del nostro problema (nel senso che è, probabilmente, più facile calcolare un massimo comun divisore tra due numeri più piccoli piuttosto che tra due numeri più grandi), allora l'aver sostituito la coppia (b, r) alla coppia (a, b) ha semplificato il problema, perché $b < a$ e $r < b$.

È possibile che si abbia $r = 0$. In questo caso, $b \mid a$ e quindi b è un massimo comun divisore tra a e b . Se invece $r > 0$, possiamo ripetere per b ed r il procedimento effettuato per a e b . Dividendo b per r otteniamo:

$$b = rq_1 + r_1, r_1 < r$$

dove, ancora $q_1, r_1 \in \mathbb{N}$ e i massimi comuni divisori tra r e r_1 sono i massimi comuni divisori tra b ed r , quindi tra a e b . Se $r_1 = 0$ (cioè se $r \mid b$) allora r è un massimo comun divisore tra a e b . In caso contrario possiamo effettuare un'altra divisione, quella tra r ed r_1 , ottenendo $q_2, r_2 \in \mathbb{N}$ tali che:

$$r = r_1 q_2 + r_2, r_2 < r_1$$

se $r_2 = 0$ allora r_1 è il massimo comun divisore cercato, altrimenti si proseguirà dividendo r_1 per r_2 .

Dovrebbe essere a questo punto chiaro il procedimento: ad ogni passo si verifica se il resto r_t dell'ultima divisione effettuata: $r_{t-2} = r_{t-1}q_t + r_t$, è nullo; in questo caso il penultimo resto r_{t-1} (vale a dire, l'ultimo resto diverso da 0, o, ancora, l'ultimo divisore) è il massimo comun divisore positivo tra a e b , se invece $r_t \neq 0$ si effettua un'altra divisione, tra il divisore r_{t-1} ed il resto r_t della divisione precedente.

È ancora da chiarire un solo punto, cioè se questo procedimento *termina*, ovvero se, iterando questo procedimento, si perviene ad una divisione con resto 0. La risposta è *affermativa*. Infatti, la sequenza dei resti ottenuti nelle successive divisioni è strettamente decrescente:

$$b > r > r_1 > r_2 > r_3 > \dots \geq 0$$

e una sequenza strettamente decrescente di numeri naturali minori di b può avere al più b termini, dal momento che l'insieme $\{n \in \mathbb{N} \mid b \geq n\}$ ha b elementi. Dunque $r_t = 0$ per qualche $t < b$. Pertanto l'algoritmo termina, fornendo un massimo comun divisore tra a e b , dopo al più b divisioni (ad essere pedanti, si dovrebbe specificare che, affinché tutto ciò che è stato appena scritto abbia senso in ogni caso, si devono sottintendere le posizioni $r_0 := r$ e $r_{-1} := b$).

Algoritmo delle divisioni successive

In sintesi, per trovare il massimo comun divisore di due numeri si procede nel modo seguente:

1. Si divide il maggiore dei due numeri per il minore;
2. Se il resto della divisione è zero allora il massimo comun divisore è il divisore;
3. Se il resto della divisione è diverso da zero allora si divide il divisore per tale resto:
 - (a) Se il nuovo resto è zero allora il massimo comun divisore è il primo resto;
 - (b) Se il nuovo resto è diverso da zero si divide il primo resto per il secondo resto e si continua così fino ad ottenere per resto zero. Il massimo comun divisore cercato sarà il resto della penultima divisione effettuata.

Esempio 7.1.4

Si calcoli il massimo comun divisore tra 182 e 104. Normalmente si imposta il calcolo utilizzando una tabella come quella che segue:

a	=	b	.	q	+	r
182	=	104	.	1	+	78
104	=	78	.	1	+	26
78	=	26	.	3	+	0

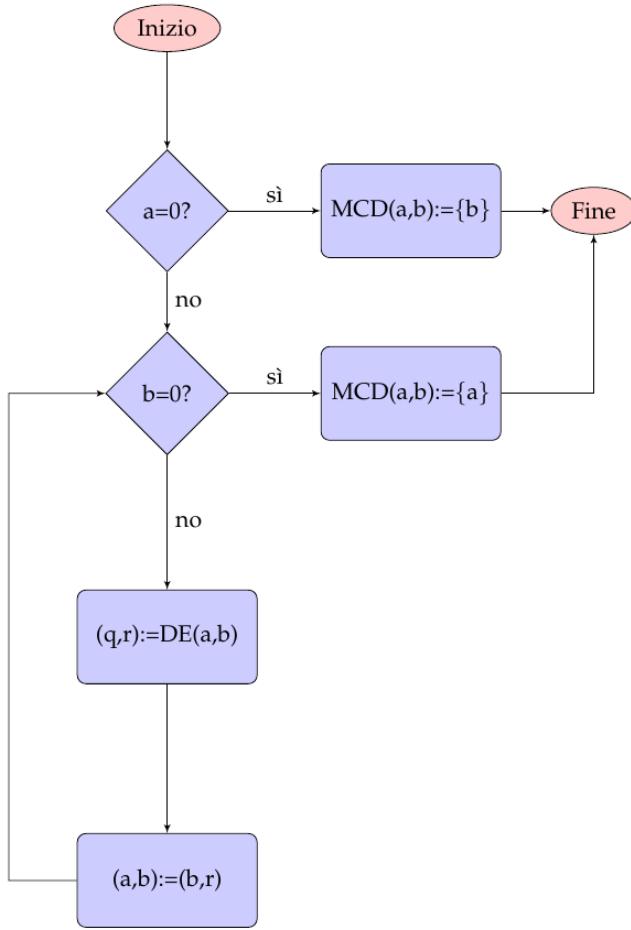


Figura 7.1: Algoritmo euclideo delle divisioni successive

7.1.5 ■ Equazioni diofantee

Oltre al calcolo dei massimi comuni divisori, l'algoritmo euclideo permette di risolvere un altro importante problema.

Definizione 7.1.10: Equazione diofantea

Un'equazione diofantea è un'equazione in cui appaiano solo indeterminate e numeri interi che si intenda risolvere in \mathbb{Z} , cioè per la quale siano ammesse come soluzioni solo numeri interi.

Ci occupiamo qui di un particolare tipo di equazione diofantea: quella cosiddetta lineare a due indeterminate, cioè una equazione diofantea della forma:

$$ax + by = c \quad (7.6)$$

dove $a, b, c \in \mathbb{Z}$. Risolvere l'equazione 7.6 significa trovare le coppie di interi (u, v) tali che rendano vera l'uguaglianza se sostituiti a x e y , cioè tali che $au + bv = c$. La 7.6 può anche non ammettere soluzioni. Ad esempio, l'equazione $0x + 0y = 1$ non ammette ovviamente soluzioni. Facendo uso della terminologia introdotta sopra, è chiaro che 7.6 ammette soluzioni (interne) se e solo se c è combinazione lineare di a e b a coefficienti in \mathbb{Z} . Ciò permette di dimostrare la prima importante osservazione su questo genere di equazioni.

Teorema 7.1.3 (di Bezout)

Sono equivalenti le seguenti affermazioni:

1. Siano a, b numeri interi relativi non nulli. Allora esiste un massimo comune divisore d di a e b e risulta $d = au + bv$ per opportuni interi u, v .
2. Siano $a, b \in \mathbb{Z}$ e sia $d = MCD(a, b)$. Allora l'insieme $\{\alpha a + \beta b \mid \alpha, \beta \in \mathbb{Z}\}$ delle combinazioni lineari di a e b a coefficienti in \mathbb{Z} coincide con l'insieme $d\mathbb{Z} = \{dk \mid k \in \mathbb{Z}\}$ dei multipli di d in \mathbb{Z} .
3. Preso $d = MCD(a, b)$, l'equazione diofantea $ax + by = c$ ha soluzioni se e solo se $d \mid c$.
4. Due numeri interi a, b si dicono coprimi se e solo se 1 è combinazione lineare a e b .

Dimostrazione. 1. Ovvio, mediante l'algoritmo delle divisioni successive è possibile ricavare un'espressione di d come combinazione lineare $au + bv$.

2. Dal punto precedente sappiamo che $d = au + bv$. Quindi $d \in \{\alpha a + \beta b \mid \alpha, \beta \in \mathbb{Z}\}$. Moltiplicando d per un qualunque $k \in \mathbb{Z}$ si ottiene quindi:

$$kd = a(\alpha k) + b(\beta k) \in \{\alpha a + \beta b \mid \alpha, \beta \in \mathbb{Z}\}$$

Quindi $d\mathbb{Z} \subseteq \{\alpha a + \beta b \mid \alpha, \beta \in \mathbb{Z}\}$. Analogamente abbiamo visto che una combinazione lineare di a e b è esprimibile come multiplo di d , quindi vale anche l'inclusione inversa e i due insiemi coincidono,

3. Supponiamo che l'equazione abbia soluzioni. Allora esistono $u, v \in \mathbb{Z}$ tali che $au + bv = c$, dunque c è combinazione lineare di a e b a coefficienti in \mathbb{Z} , e quindi, per il punto precedente, è un multiplo di $d = MCD(a, b)$. Per definizione di multiplo ovviamente sappiamo che d divide c . Dunque, se supponiamo che d non divida c dobbiamo trarre la conclusione che la nostra equazione non abbia soluzioni.
4. Non ha bisogno di dimostrazioni, è una definizione.

□

Lemma 7.1.6 (di Euclide)

Siano $a, b \in \mathbb{Z}$ coprimi. Se c è un numero intero tale che $a \mid bc$ allora $a \mid c$.

Dimostrazione. Per il teorema di Bezout esistono $u, v \in \mathbb{Z}$ tali che $1 = au + bv$. D'altra parte a divide bc quindi $bc = ah$ per un opportuno numero intero h . Pertanto:

$$\begin{aligned} c &= c(au + bv) \\ &= cau + cbv \\ &= cau + ahv \\ &= a(cu + hv) \end{aligned}$$

e quindi a divide c .

□

Esempio 7.1.5

Supponiamo di voler trovare soluzioni dell'equazione diofantea $74x + 22y = 10$. In questo caso è evidente che $MCD(74, 22) = 2$ e poiché $2 \mid 10$ siamo certi che l'equazione ammette soluzioni. Eseguendo le divisioni successive si ottiene:

$$\begin{aligned} 74 &= 3 \cdot 22 + 8 \\ 22 &= 2 \cdot 8 + 6 \\ 8 &= 1 \cdot 6 + 2 \\ 6 &= 3 \cdot 2 \end{aligned}$$

fino ad ottenere 2 come ultimo resto non nullo. A questo punto possiamo esprimere i resti:

$$\begin{aligned} 8 &= 74 - 3 \cdot 22 \\ 6 &= 22 - 2 \cdot 8 \\ 2 &= 8 - 1 \cdot 6 \end{aligned}$$

e scrivere 2 come combinazione lineare di 74 e 22:

$$\begin{aligned} 2 &= 8 - 6 \\ &= 8 - (22 - 2 \cdot 8) && \text{(Sostituendo 6)} \\ &= 8 - 22 + 2 \cdot 8 \\ &= 8(1 + 2) - 22 && \text{(Raccogliendo i coefficienti di 8)} \\ &= 3 \cdot 8 - 22 \\ &= 3 \cdot (74 - 3 \cdot 22) - 22 && \text{(Sostituendo 8)} \\ &= 3 \cdot 74 - 9 \cdot 22 - 22 \\ &= 3 \cdot 74 - 10 \cdot 22 \\ &= 3 \cdot 74 + (-10) \cdot 22 \end{aligned}$$

Abbiamo così trovato che 2 è esprimibile come combinazione lineare $\alpha 74 + \beta 22$ con $\alpha = 3$ e $\beta = -10$. La coppia $(3, -10)$ è soluzione dell'equazione diofantea $74x + 22y = 2$. Moltiplicando per 5 si ottiene $75(15) + 22(-50) = 10$, dunque la coppia $(15, -50)$ è la soluzione dell'equazione diofantea $74x + 22y = 10$.

7.1.6 ■ Struttura quoziante

Siano S un insieme non vuoto, e $\perp : S \times S \rightarrow S$ un'operazione in S .

Definizione 7.1.11: Compatibilità

Una relazione di equivalenza $\mathfrak{R} \in Eq(S)$ si dice **compatibile a sinistra** con \perp se:

$$\forall x_1, x_2 \in S \left((x_1 \mathfrak{R} x_2) \implies \left(\forall a \in S (a \perp x_1 \mathfrak{R} a \perp x_2) \right) \right)$$

Analogamente, \mathfrak{R} si dice **compatibile a destra** con l'operazione \perp se:

$$\forall x_1, x_2 \in S \left((x_1 \mathfrak{R} x_2) \implies \left(\forall a \in S (x_1 \perp a \mathfrak{R} x_2 \perp a) \right) \right)$$

Definizione 7.1.12: Congruenza

Sia (S, \perp) una struttura algebrica. Una relazione di equivalenza \mathfrak{R} in S si dice una **congruenza** in (S, \perp) se qualunque siano gli elementi x_1, x_2, y_1, y_2 di S tali che $x_1 \mathfrak{R} x_2$ e $y_1 \mathfrak{R} y_2$, risulta anche:

$$x_1 \perp y_1 \mathfrak{R} x_2 \perp y_2$$

Pertanto, quando \mathfrak{R} è una congruenza in (S, \perp) , e solo allora, è possibile considerare l'applicazione:

$$\perp_{\mathfrak{R}} : ([x]_{\mathfrak{R}}, [y]_{\mathfrak{R}}) \mapsto [x \perp y]_{\mathfrak{R}} \in S/\mathfrak{R}$$

Tale applicazione è un'operazione nell'insieme quoziante S/\mathfrak{R} , chiamata **operazione quoziante** di \perp rispetto a \mathfrak{R} . La struttura $(S/\mathfrak{R}, \perp_{\mathfrak{R}})$ viene chiamata **struttura quoziante**.

Proposizione 7.1.10

Siano S un insieme non vuoto, $\perp : S \times S \rightarrow S$ un'operazione in S e \mathfrak{R} una congruenza in (S, \perp) . Si ha:

- Se \perp è associativa, allora anche $\perp_{\mathfrak{R}}$ è associativa;
- Se \perp è commutativa, allora anche $\perp_{\mathfrak{R}}$ è commutativa;
- Se u è un elemento neutro in (S, \perp) allora $[u]_{\mathfrak{R}}$ è elemento neutro in $(S/\mathfrak{R}, \perp_{\mathfrak{R}})$.
- Se x è un elemento simmetrizzabile di (S, \perp) e x' è un suo simmetrico, allora $[x]_{\mathfrak{R}}$ è un elemento simmetrizzabile di $(S/\mathfrak{R}, \perp_{\mathfrak{R}})$ e $[x']_{\mathfrak{R}}$ è un suo simmetrico.

Osservazione 7.1.5

Una relazione di equivalenza \mathfrak{R} è una congruenza in $(S, \perp_1, \dots, \perp_n)$ se e soltanto se è compatibile con tutte le operazioni \perp_i per ogni $i \in \{1, \dots, n\}$.

7.2

CONGRUENZE IN \mathbb{Z}



7.2.1 ■ La relazione di congruenza modulo m

Sia m un numero intero relativo, e sia \equiv_m la relazione binaria definita in \mathbb{Z} ponendo:

$$\forall a, b \in \mathbb{Z} (a \equiv_m b \iff m \mid (a - b)) \quad (7.7)$$

ovvero se e solo se a e b sono numeri interi relativi tali che la differenza $(a - b)$ è multiplo di m , ovvero esiste $n \in \mathbb{Z}$ tale che $a - b = nm$.

Qualunque sia $a \in \mathbb{Z}$ risulta $a - a = 0 = 0 \cdot m$, e quindi $a \equiv_m a$ e la relazione \equiv_m risulta riflessiva. Siano a, b numeri interi tali che $a \equiv_m b$. Allora risulta $a - b = km$ con $k \in \mathbb{Z}$, e quindi $b - a = -(a - b) = (-k)m$, sicché $b \equiv_m a$ e la relazione \equiv_m è anche simmetrica. Siano infine a, b, c numeri interi tali che $a \equiv_m b$ e $b \equiv_m c$. Allora esistono $h, k \in \mathbb{Z}$ tali che $a - b = hm$ e $b - c = km$, sicché:

$$a - c = (a - b) + (b - c) = hm + km = (h + k)m$$

e quindi $a \equiv_m c$, e \equiv_m è transitiva. Pertanto \equiv_m è una relazione di equivalenza in \mathbb{Z} . Se $a, b \in \mathbb{Z}$ sono due interi tali che $a \equiv_m b$ è possibile trovare usata la notazione $a \equiv b \pmod{m}$.

Se a è un numero intero relativo, la classe di equivalenza di a rispetto alla relazione \equiv_m si chiama “**classe di congruenza** di a modulo m ” e si denota col simbolo $[a]_m$. Un numero intero b appartiene ad $[a]_m$ se e solo se $b \equiv_m a$, e quindi e se solo se $b - a = km$ per qualche $k \in \mathbb{Z}$. Pertanto:

$$[a]_m = \{a + km \mid k \in \mathbb{Z}\}$$

e in particolare:

$$[0]_m = \{km \mid k \in \mathbb{Z}\} = m\mathbb{Z}$$

dove $m\mathbb{Z}$ è l'insieme dei multipli di m . L'insieme quoziante \mathbb{Z}/\equiv_m di \mathbb{Z} rispetto alla relazione di equivalenza \equiv_m si denota col simbolo \mathbb{Z}_m , e si chiama **insieme delle classi di interi modulo m** .

Osservazione 7.2.1

Poiché in \mathbb{Z} l'unico multiplo di 0 è 0, si ha subito che la relazione \equiv_0 coincide con la relazione identica. D'altra parte ogni numero intero è divisibile per 1, sicché la relazione \equiv_1 è la relazione totale, e quindi $|\mathbb{Z}_1| = 1$. È inoltre chiaro che per ogni intero relativo m la relazione \equiv_m e la relazione \equiv_{-m} coincidono. Queste considerazioni consentono di limitare la nostra analisi al caso degli $m > 1$.

Esempio 7.2.1

Si consideri in \mathbb{Z} la relazione di equivalenza \equiv_2 . Due numeri interi $a, b \in \mathbb{Z}$ sono in relazione tra di loro se e solo se:

$$a \equiv_2 b \iff 2 \mid (a - b) \iff \exists k \in \mathbb{Z} ((a - b) = 2k)$$

ovvero se e soltanto se $(a - b)$ risulta un numero pari. Chiaramente la differenza tra due numeri interi è pari se e soltanto se a e b hanno la *stessa parità* (entrambi pari oppure entrambi dispari). Infatti sia per assurdo a un numero dispari e b un numero pari della forma $2t$ per un opportuno $t \in \mathbb{Z}$. Essendo $a - b$ un numero pari esso sarà sicuramente della forma $2k$ per un qualche intero k . Essendo a un numero dispari questo può essere scritto nella forma $2n + 1$ e si ha:

$$(a - b) = (2n + 1) - 2t = 2n + 1 - 2t = 2(n - t) + 1$$

e $(a - b)$ risulterebbe un numero dispari, contro le nostre ipotesi.

Esempio 7.2.2

Dati due numeri interi x e y , diciamo che $x \equiv_3 y$ se $(x - y)$ è multiplo di tre. Si vede subito che 0 è congruo a tutti i multipli di tre. 1 è congruo a tutti i numeri del tipo $\{\dots, -5, -2, 1, 4, 7, 10, \dots\} = \{1 + 3k \mid k \in \mathbb{Z}\}$. 2 è congruo a tutti i numeri del tipo $\{\dots, -4, -1, 2, 5, 8, 11, \dots\} = \{2 + 3k \mid k \in \mathbb{Z}\}$. Quindi nella partizione definita dalla congruenza modulo 3 ci sono tre classi di congruenza: $[0]_3, [1]_3, [2]_3$.

Proposizione 7.2.1

Sia $m > 1$ un numero intero. Qualunque sia il numero intero relativo a risulta $a \equiv_m r$ dove r è il resto della divisione euclidea di a per m .

Dimostrazione. Denotato con q il quoziante della divisione euclidea di a per m , si ha $a = mq + r$, con $0 \leq r < |m|$, per cui $(a - r) = mq$ e quindi $a \equiv_m r$. \square

Teorema 7.2.1

Sia $m > 1$ un numero intero. Allora \mathbb{Z}_m è un insieme finito di ordine m e risulta:

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$$

Corollario 7.2.1

Sia $m > 1$ un numero intero, per ogni $a, b \in \mathbb{Z}$:

$$a \equiv_m b \iff \text{hanno lo stesso resto nella divisione euclidea per } m$$

Osservazione 7.2.2

Si ha $m = 1 \cdot m + 0$ e quindi $m \equiv_m 0$. Ovvero $[m]_m = [0]_m$.

Per i risultati appena ottenuti possiamo vedere l'insieme quoziante \mathbb{Z}_m come l'insieme delle **classi di resto modulo m** .

Proposizione 7.2.2

Le relazioni di congruenza sono compatibili con l'addizione. Dati i numeri interi $a, a', b, b' \in \mathbb{Z}$:

$$(a \equiv_m a' \wedge b \equiv_m b') \implies (a + b \equiv_m a' + b') \quad (7.8)$$

Dimostrazione. Da $a \equiv_m a'$ e $b \equiv_m b'$ segue :

$$\begin{cases} a - a' = km \\ b - b' = hm \end{cases}$$

per opportuni interi $h, k \in \mathbb{Z}$. Sommando membro a membro si ha:

$$a - a' + (b - b') = km + hm \iff a + b - (a' + b') = (h + k)m$$

Quindi $a + b \equiv_m a' + b'$. □

Proposizione 7.2.3

Le relazioni di congruenza sono compatibili con la moltiplicazione. Dati i numeri interi $a, a', b, b' \in \mathbb{Z}$, vale:

$$(a \equiv_m a' \wedge b \equiv_m b') \implies (a \cdot b \equiv_m a' \cdot b') \quad (7.9)$$

Dimostrazione. È lasciata al lettore come esercizio. □

Da queste due proposizioni segue che:

Teorema 7.2.2

Qualunque sia il numero intero relativo m , la relazione di equivalenza \equiv_m è una congruenza nella struttura algebrica $(\mathbb{Z}, +, \cdot)$.

È opportuno osservare che le uniche congruenze nella struttura algebrica $(\mathbb{Z}, +, \cdot)$ sono le congruenze modulo m , al variare di $m \in \mathbb{Z}$. Questo teorema permette di introdurre nell'insieme \mathbb{Z}_m delle classi di resto le operazioni quoziante dell'addizione e della moltiplicazione in \mathbb{Z} . Tali operazioni, denotate ancora con i simboli $+$ e \cdot , sono definite ponendo:

$$\begin{cases} [a]_m + [b]_m = [a + b]_m \\ [a]_m \cdot [b]_m = [ab]_m \end{cases}$$

Tali operazioni sono associative e commutative, la classe $[0]_m$ è elemento neutro in \mathbb{Z}_m rispetto all'addizione, mentre $[1]_m$ è elemento neutro rispetto alla moltiplicazione. Inoltre, per ogni numero intero relativo a , la classe $[a]_m$ è dotata di opposto in \mathbb{Z}_m e risulta $-[a]_m = [-a]_m$. Infine, qualunque siano i numeri interi relativi $a, b, c \in \mathbb{Z}$ risulta:

$$\begin{aligned} ([a]_m + [b]_m)[c]_m &= [a + b]_m[c]_m \\ &= [(a + b)c]_m \\ &= [ac + bc]_m \\ &= [ac]_m + [bc]_m \\ &= [a]_m[c]_m + [b]_m[c]_m \end{aligned}$$

sicché in \mathbb{Z}_m la moltiplicazione è distributiva rispetto all'addizione. La struttura $(\mathbb{Z}_m, +, \cdot)$ risulta quindi un anello. Osserviamo che in \mathbb{Z}_m non vale in generale la legge di annullamento del prodotto, ovvero esistono dei quozienti in cui sono presenti divisori dello zero.

Esempio 7.2.3

Ad esempio in \mathbb{Z}_6 gli elementi $[2]_6, [3]_6$ e $[4]_6$ risultano essere divisori dello zero:

$$[2]_6 \cdot [3]_6 = [6]_6 = [0]_6 = [12]_6 = [4]_6 \cdot [3]_6$$

e \mathbb{Z}_6 non risulta essere un anello integro, in particolare un dominio di integrità.

Teorema 7.2.3

Sia $m > 1$ un numero intero relativo. Allora in \mathbb{Z}_m vale la legge di annullamento del prodotto se e solo se m è primo.

Proposizione 7.2.4

Siano $a \in \mathbb{Z}$, $n \in \mathbb{N}^*$. $[a]_m$ è invertibile in \mathbb{Z}_m se, e solo se, a ed m sono coprimi.

Dimostrazione. Abbiamo:

⇒ Se $[a]_m$ è invertibile, esiste $[b]_m$ tale che:

$$[a]_m \cdot [b]_m = [ab]_m = [1]_m$$

Quindi:

$$m \mid (1 - ab) \iff \exists h \in \mathbb{Z} (1 - ab = hm)$$

Da $1 = ab + hm$ e dal Teorema di Bezout segue che a ed m sono coprimi.

⇐ Viceversa, supposti a ed m coprimi tra di loro, essendo $(a, m) = 1$ esistono α, β tali che $1 = \alpha a + \beta m$.

Da $\alpha a - 1 = -\beta m$ segue allora $\alpha a \equiv_m 1$ per cui $[\alpha a]_m = [\alpha]_m[a]_m$ e $[\alpha]_m$ è l'inverso di $[a]_m$.

□

Corollario 7.2.2

Siano $a \in \mathbb{Z}$, $n \in \mathbb{N}^*$ e sia $[a]_m \neq [0]_m$. Allora $[a]_m$ è un divisore dello zero in \mathbb{Z}_m se, e solo se, a ed m non sono coprimi.

Dimostrazione. Si ha:

⇒ Se $[a]_m$ è un divisore dello zero risulta non regolare e quindi non invertibile. Per la proposizione precedente allora a ed m non sono coprimi.

⇐ Viceversa, se $d = (a, m)$ risulta $1 < d < m$ ed esistono a_1, m_1 tali che $a = a_1 d$ ed $m = m_1 d$. Dall'essere $1 < n_1 < n$ segue $[m_1]_m \neq [0]_m$ e $[a]_m[m_1]_m = [a_1 dm_1]_m = [a_1]_m[m]_m = [a_1][0]_m = [0]_m$, per cui $[a]_m$ è un divisore dello zero.

□

Corollario 7.2.3

Siano $a \in \mathbb{Z}$ ed $m \in \mathbb{N}^*$ sia $[a]_m \neq [0]_m$. Allora $[a]_m$ è invertibile se e solo se non è un divisore dello 0.

Teorema 7.2.4 (Caratterizzazione anello degli interi modulo m)

Sia $m > 1$ un intero. Allora le seguenti affermazioni sono equivalenti:

1. l'anello \mathbb{Z}_m è un campo;
2. L'anello \mathbb{Z}_m è un dominio di integrità;
3. m è un numero primo.

Dimostrazione. Le condizioni (1) e (2) sono equivalenti per il Corollario precedente. Per dimostrare l'equivalenza di (1) e (3) si osservi che, se m è primo, tutti gli interi $1, \dots, m-1$ sono coprimi con m e quindi tutte le classi $[1]_m, [2]_m, \dots, [m-1]_m$ sono invertibili. Viceversa, supposto che \mathbb{Z}_m sia un campo, se m non fosse primo esisterebbe un divisore m_1 di m tale che $1 < m_1 < m$. Allora risulterebbe $[m_1]_m \neq [0]_m$ ed $[m_1]_m$ non invertibile, essendo $(m, m_1) = m_1 > 1$. Dall'assurdo segue che m è necessariamente primo. □

Corollario 7.2.4

Gli elementi non nulli di \mathbb{Z}_m sono tutti invertibili se e solo se m è primo.

7.2.1.1 ■ Periodo di un elemento

Il concetto di classe di resto ha a che fare con la nozione di periodo di un elemento in un gruppo. Ricordiamo che, se un gruppo G è denotato con la notazione additiva, allora il concetto di potenza coincide con il concetto di multiplo. Quindi si dice che G è ciclico se esiste $a \in G$ tale che $G = \langle a \rangle = \{na/n \in \mathbb{Z}\}$.

Lemma 7.2.1

Sia $G = \langle x \rangle$ un gruppo ciclico. Allora G è finito se e solo se esiste un numero intero positivo m tale che $x^m = 1$.

Dimostrazione. Se G è finito, esistono dei numeri interi positivi h e k tali che $x^h = x^k$. Supposto, per fissare le idee, $h > k$, si ha $m = h - k > 0$ e $x^m = x^{h-k} = x^h(x^k)^{-1} = 1$. Reciprocamente, esiste un numero intero positivo m tale che $x^m = 1$. Qualunque sia il numero intero relativo n , si ha per il teorema della divisione euclidea: $n = mq + r$, con q ed r numeri interi relativi tali che $0 \leq r < m$. Allora $x^n = x^{mq+r} = (x^m)^q x^r = x^r$. Per cui $G = \{x^0, x^1, \dots, x^{m-1}\}$ è finito. \square

Teorema 7.2.5 (Teorema ponte)

Sia $G = \langle x \rangle$ un gruppo ciclico finito di ordine m . Allora $G = \{x^0, x^1, \dots, x^{m-1}\}$ ed m è minimo intero positivo tale che $x^m = 1$.

Definizione 7.2.1: Elemento periodico

Sia G un gruppo. Un elemento $x \in G$ si dice **periodico** se il sottogruppo $\langle x \rangle$ è finito. In questo caso l'ordine di $\langle x \rangle$ si chiama **periodo** di x e si denota con il simbolo $o(x)$. Un gruppo G si dice **periodico** se ogni suo elemento è periodico.

Osservazione 7.2.3



Un elemento x di G è periodico se e solo se esiste $m \in \mathbb{Z}$ tale che $x^m = 1_G$ se G è denotato moltiplicativamente. Nel caso in cui G è denotato additivamente allora $x \in G$ è periodico se $mx = 0_G$.

Lemma 7.2.2

Sia (G, \cdot) un gruppo e $x \in G$ un elemento periodico di periodo n . Allora:

$$\forall a \in \mathbb{Z} (x^a = x^{\text{rest}(a,n)})$$

dove $\text{rest}(a,n)$ è il resto della divisione euclidea di a per n .

Dimostrazione. Sia $r = \text{rest}(a,n)$ allora esiste un $k \in \mathbb{Z}$ tale che $a = kn + r$. Allora:

$$\begin{aligned} x^a &= x^{kn+r} \\ &= (x^n)^k \cdot x^r \\ &= 1_G \cdot x^r = x^r \end{aligned}$$

e l'asserto è dimostrato. \square

Proposizione 7.2.5

Sia (G, \cdot) un gruppo e $x \in G$ un elemento periodico di periodo n . Allora:

$$\forall a, b \in \mathbb{Z} (x^a = x^b \iff a \equiv_n b \iff \text{rest}(a,n) = \text{rest}(b,n))$$

Dimostrazione. \Leftarrow Se $a \equiv_m b$ allora $m \mid (a - b)$. Ovvvero $(a - b) = qm$ per un opportuno $q \in \mathbb{Z}$. Allora $a = qm + b$ e risulta:

$$x^a = x^{qm+b} = (x^m)^q \cdot x^b = (1_G) \cdot x^b = x^b$$

\Rightarrow Se $x^a = x^b$ allora $x^{a-b} = 1_G = x^0$ e quindi vale $a \equiv_m b$. \square

Definizione 7.2.2: Funzione di Eulero

La funzione φ di Eulero è l'applicazione di \mathbb{N}^* in sè definita ponendo, per ogni $n \in \mathbb{N}^*$:

$$\varphi(n) = |\{a \in \mathbb{N}^* \mid a \leq n \wedge MCD(a, n) = 1\}| \quad (7.10)$$

ovvero il numeri degli interi positivi minori di n e primi con n .

Esempio 7.2.4

Ad esempio, poiché tra gli interi positivi 1, 2, 3, 4, 5, 6 ad essere coprimi con 6 sono solo 1 e 5 si ha $\varphi(6) = 2$.

La funzione di Eulero esprime la cardinalità del gruppo degli invertibili dei quozienti di \mathbb{Z} . Infatti, per ogni $n \in \mathbb{N}^*$, sappiamo che gli elementi dell'anello \mathbb{Z}_n corrispondono precisamente ai numeri interi positivi tali che $a \leq n$, nel senso che:

$$\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{N}^* \wedge a \leq n\}$$

e se a e b sono interi positivi minori o uguali a n si ha $[a]_n = [b]_n$ se e solo se $a = b$. Sappiamo inoltre che, con queste stesse notazioni, $[a]_n$ è invertibile in \mathbb{Z}_n se e solo se a ed n sono coprimi. Dunque:

$$\mathcal{U}(\mathbb{Z}_n) = \{[a]_n \mid a \in \mathbb{N}^* \wedge a \leq n \wedge MCD(a, n) = 1\}$$

ovvero:

$$|\mathcal{U}(\mathbb{Z}_n)| = \varphi(n)$$

Esempio 7.2.5

Il gruppo composto dall'insieme finito $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$ insieme all'operazione di addizione è un gruppo ciclico in quanto esiste un elemento generatore in grado di generare tutti gli elementi di \mathbb{Z}_4 . Infatti, preso $[1]_4$ si ha:

$$\begin{aligned} ([1]_4)^1 &= 1 \cdot [1]_4 = [1 \cdot 1]_4 = [1]_4 \\ ([1]_4)^2 &= 2 \cdot [1]_4 = [2 \cdot 1]_4 = [2]_4 \\ ([1]_4)^3 &= 3 \cdot [1]_4 = [3 \cdot 1]_4 = [3]_4 \\ ([1]_4)^4 &= 4 \cdot [1]_4 = [4 \cdot 1]_4 = [4]_4 = [0]_4 \end{aligned}$$

Il periodo dell'elemento $[1]_4$ è uguale a quattro, infatti, il sottogruppo generato da $[1]_4$, ovvero l'insieme $\langle [1]_4 \rangle = \{n[1]_4 / n \in \mathbb{Z}\} = \{[0]_4, [1]_4, [2]_4, [3]_4\}$ coincide con l'insieme \mathbb{Z}_4 . L'elemento $[2]_4$ non è un generatore perché i suoi multipli (potenze) non generano tutti gli altri elementi dell'insieme \mathbb{Z}_4 :

$$\langle [2]_4 \rangle = \{[0]_4, [2]_4\}$$

Il periodo dell'elemento $[2]_4$ è 2 perché il numero intero più piccolo k tale che $2^k = 0_{\mathbb{Z}_4}$ è $k = 2$. Infatti:

$$([2]_4)^2 = [2]_4 + [2]_4 = [4]_4 = [0]_4$$

Anche l'elemento $[3]_4$ è un generatore del gruppo ciclico in quanto il sottogruppo $\langle [3]_4 \rangle$ coincide con \mathbb{Z}_4 :

$$\langle [3]_4 \rangle = \{[0]_4, [2]_4, [3]_4\}$$

Il periodo di $[3]_4$ risulta quindi uguale a quattro perché sono necessarie quattro ripetizioni dell'operazione per avere l'elemento neutro $([3]_4)^4 = [0]_4$. Quindi \mathbb{Z}_4 ha due generatori ($[1]_4$ e $[3]_4$) e vale:

$$\langle [1]_4 \rangle = \langle [3]_4 \rangle = \mathbb{Z}_4$$

notiamo inoltre che 1 e 3 sono coprimi con 4 e vale $\varphi(4) = 2$. Infatti, il numero di generatori distinti di un gruppo ciclico di ordine m coincide con il numero di interi positivi strettamente minori di m e coprimi con m , ovvero $\varphi(m)$.

A conclusione di questa trattazione sulle proprietà dei gruppi ciclici vogliamo mostrare che, a meno di isomorfismi, *gli unici gruppi ciclici finiti*, ovvero i gruppi per i quali esiste un elemento x tale che $x^m = 1$, sono i gruppi additivi $(\mathbb{Z}_m, +)$. Infatti, considerato un gruppo ciclico finito G e l'applicazione $f : n \in \mathbb{Z} \rightarrow x^n \in G$, poiché $G = \{x^n / n \in \mathbb{Z}\}$ si ha che f è suriettiva. Qualunque siano gli elementi $m, n \in \mathbb{Z}$ si ha inoltre:

$$f(m+n) = x^{m+n} = x^m \cdot x^n = f(m) \cdot f(n)$$

ed f risulta essere un epimorfismo. Dal Teorema di omomorfismo segue allora che G è isomorfo a $\mathbb{Z}/\mathfrak{R}_f$ dove \mathfrak{R}_f è nucleo di equivalenza di f . Se $|G| = m$ si ha \mathfrak{R}_f è equivalente¹ a \equiv_m e G è isomorfo a \mathbb{Z}_m .

Corollario 7.2.5

L'anello $(\mathbb{Z}_m, +, \cdot)$ ha caratteristica pari ad m .

Dimostrazione. Per ogni $a \in \mathbb{Z}$:

$$[a]_m = [0]_m \iff a \equiv_m 0 \iff m \mid (a - 0) \iff m \mid a \iff a = km$$

ed m risulta essere la caratteristica dell'anello \mathbb{Z}_m . □

7.2.2 ■ Equazioni congruenziali

Nel paragrafo precedente è stata data una condizione necessaria e sufficiente affinché una classe $[a]_m \neq [0]_m$ sia invertibile. In questa sezione si vedrà come è possibile determinare $[a]_m^{-1}$ quando $[a]_m$ è invertibile².

Si ricordi che un elemento $[a]_m$ è invertibile in \mathbb{Z}_m quando esiste $[c]_m \in \mathbb{Z}_m$ tale che: $[a]_m[c]_m = [ac]_m = [1]_m$ ovvero se esiste $c \in \mathbb{Z}$ tale che $ac \equiv_m 1$. In generale vale la seguente definizione:

Definizione 7.2.3: Equazioni congruenziali

Siano $a, b, m \in \mathbb{Z}$ e sia $m > 1$. L'espressione $ax \equiv_m b$ si dice **equazione congruenziale** di termini a e b modulo m . Un numero intero relativo c si dice **soluzione** dell'equazione congruenziale $ax \equiv_m b$ se risulta $ac \equiv_m b$. Ciò equivale a richiedere che sia $[a]_m[c]_m = [b]_m$.

Osservazione 7.2.4

Un elemento $[a]_m \in \mathbb{Z}_m$ è invertibile se, e solo se, l'equazione congruenziale $ax \equiv_m 1$ ammette una soluzione.

Proposizione 7.2.6 (Criterio di compatibilità)

Siano $a, b, m \in \mathbb{N}^*$, $d = MCD(a, m)$. L'equazione congruenziale $ax \equiv_m b$ ha soluzione se, e solo se, d divide b .

Dimostrazione. Dimostriamo le due implicazioni:

- ⇒ Se c è una soluzione dell'equazione congruenziale allora $\exists k \in \mathbb{Z}$ tale che $ac - b = km$. Allora da $d \mid a$ e $d \mid m$ segue $d \mid ac - km = b$.
- ⇐ Viceversa, si supponga d divisore di b : esiste $h \in \mathbb{Z}$ tale che $b = dh$. Essendo inoltre d un massimo comune divisore tra a ed m , esistono degli interi r ed s tali che $d = ra + sm$. Da ciò segue $b = hd = h(ra + sm)$. In particolare, da $hra - b = -hsm$ segue che hr è una soluzione dell'equazione congruenziale. □

Proposizione 7.2.7

Siano $a, b \in \mathbb{Z}$, $m \in \mathbb{N}^*$, t un divisore comune di a, b, m . Allora le soluzioni dell'equazione congruenziale $ax \equiv_m b$ sono tutte e sole quelle dell'equazione congruenziale:

$$\frac{a}{t}x \equiv_{\frac{m}{t}} \frac{b}{t}$$

Dimostrazione. È sufficiente osservare che, se c è un intero, allora:

$$m = t \cdot \frac{m}{t} \mid ac - b = t \cdot \frac{a}{t} \cdot c - t \cdot \frac{b}{t} \iff \frac{m}{t} \mid \frac{a}{t} \cdot c - \frac{b}{t}$$

¹ Si tenga sempre a mente che f è una applicazione che associa ogni intero n alla potenza $x^n \in G$. Se G è un gruppo ciclico denotato additivamente allora f è definita ponendo $n \mapsto nx$.

²Ovvero quando a ed m sono coprimi.

Corollario 7.2.6

Una congruenza compatibile $ax \equiv_m b$ ammette esattamente $d = MCD(a, m)$ soluzioni non congruenti modulo m date da:

$$x_0 + k \frac{m}{d} \quad (7.11)$$

dove x_0 è una soluzione della congruenza e $0 \leq k < d$.

Osservazione 7.2.5

Se $MCD(a, m) = 1$ allora la congruenza lineare ha un'unica soluzione.

Proposizione 7.2.8

Sia c una soluzione dell'equazione congruenziale $ax \equiv_m 1$. Allora, se b è un intero, cb è soluzione dell'equazione congruenziale $ax \equiv_m b$.

Dimostrazione. Basta osservare che, se m divide $ac - 1$, divide anche $(ac - 1)b = acb - b$. \square

Proposizione 7.2.9

Si consideri l'equazione congruenziale $ax \equiv_m b$ e siano a ed m primi tra loro. Allora l'equazione ha soluzioni, che costituiscono una classe di resto modulo m .

Dimostrazione. Poiché $1 = MCD(a, m)$ divide b l'equazione ha soluzioni. Indicata con c una di tali soluzioni, verifichiamo che l'insieme X di tutte e sole le soluzioni dell'equazione coincide con $[c]_m$. Sia $y \in X$ una soluzione, da $ac \equiv_m b$ e $ay \equiv_m b$ segue:

$$ac \equiv_m ay \implies m \mid ac - ay = a(c - y)$$

Ciò implica, essendo inoltre m ed a primi tra loro, che m divide $c - y$, per cui $y \in [c]_m$. Viceversa, se $y \in [c]_m$, risulta $[c]_m = [y]_m$ e quindi $[a]_m[y]_m = [a]_m[c]_m = [b]_m$ come si voleva. \square

Tecniche di semplificazione

Data l'equazione congruenziale:

$$ax \equiv_m c \quad (7.12)$$

dove $a, c, m \in \mathbb{Z}$ e $m \neq 0$:

1. Se $a' \in [a]_m$ e $c' \in [c]_m$, l'equazione congruenziale

$$a'x \equiv_m c'$$

è equivalente alla 7.12.

2. Per ogni $k \in \mathbb{Z}$, se $k \neq 0$, l'equazione congruenziale

$$akx \equiv_{mk} ck$$

è equivalente alla 7.12.

3. Per ogni $t \in \mathbb{Z}$, se t è coprimo con m , l'equazione congruenziale

$$atx \equiv_m ct$$

è equivalente a 7.12.

7.2.2.1 Esempi di equazioni congruenziali e loro soluzioni

Esempio 7.2.6

L'equazione $324x \equiv_{508} 127$ non ha soluzioni in quanto $MCD(324, 508) \nmid 127$.

Esempio 7.2.7

L'equazione $120x \equiv_m 128$ ha soluzioni (4 è MCD tra 120 e 164 e divide 128). Troviamole.

Dividiamo tutto per 4: l'equazione diventa $30x \equiv_{41} 32$ che risulta essere una equazione congruenziale ridotta ai minimi termini in quanto 30 e 41 risultano essere coprimi. Eseguiamo l'algoritmo euclideo per risolvere l'equazione diofantea $1 = 30x + 41y$ si ottiene:

$$\begin{aligned} 41 &= (1)30 + 11 \\ 30 &= (2)11 + 8 \\ 11 &= (1)8 + 3 \\ 8 &= (2)3 + 2 \\ 3 &= (1)2 + 1 \\ 2 &= (2)1 + 0 \end{aligned}$$

Ricaviamo quindi le seguenti relazioni:

$$\begin{aligned} 11 &= (1)41 + (-1)30 \\ 8 &= (1)30 + (-2)11 \\ 3 &= (1)11 + (-1)8 \\ 2 &= (1)8 + (-2)3 \\ 1 &= (1)3 + (-1)2 \end{aligned}$$

Dalle quali possiamo eseguire il seguente calcolo per ottenere una combinazione lineare di 30 e 41 che dia 1 come risultato:

$$\begin{aligned} 1 &= (1)3 + (-1)2 \\ &= (1)3 + (-1)(8 + (-2)3) \\ &= (-1)8 + (3)3 \\ &= (-1)8 + (3)(11 + (-1)8) \\ &= (3)11 + (-4)8 \\ &= (3)11 + (-4)(30 + (-2)11) \\ &= (-4)30 + (11)11 \\ &= (-4)30 + (11)(41 + (-1)30) \\ &= (11)41 + (-15)30 \end{aligned}$$

Pertanto, $1 = (11) \cdot 41 + (-15) \cdot 30$. Più significativamente: abbiamo scoperto che vale $(-15)30 \equiv_{41} 1$, cioè che l'inverso di $[30]_{41}$ in \mathbb{Z}_{41} è $[-15]_{41}$. A questo punto sappiamo che l'unica classe in \mathbb{Z}_{41} che, moltiplicata per $[30]_{41}$ dia $[32]_{41}$ è $([30]_{41})^{-1}[32]_{41} = [-15]_{41}[32]_{41} = [(-15)(32)]_{41}$. Questa classe è l'insieme delle soluzioni, in \mathbb{Z} , dell'equazione congruenziale originaria.

Esempio 7.2.8

L'equazione $4x \equiv_{10} 8$ ha ovviamente 2 come soluzione in \mathbb{Z} . L'insieme di tutte le soluzioni non è $[2]_{10}$ ma $[2]_5$, perché in forma ridotta l'equazione diventa $2x \equiv_5 4$, notare: 2 e 5 sono coprimi. Si può osservare che, ad esempio, $7 \in [2]_5 \setminus [2]_{10}$, quindi $[2]_5$ è strettamente contenuto in $[2]_{10}$; è facile anche verificare che $[2]_5$ è l'unione disgiunta di $[2]_{10}$ e $[7]_{10}$, quindi, l'equazione data, vista come equazione in Z_{10} : $[4]_{10}X = [8]_{10}$ ha esattamente due soluzioni: $[2]_{10}$ e $[7]_{10}$.

Esempio 7.2.9

L'equazione $45x \equiv_{47} 476$ si risolve immediatamente senza bisogno di calcoli: evidentemente $45 \equiv_{47} -2$ e $476 \equiv_{47} 6$, quindi l'equazione è equivalente a (nel senso che ha le stesse soluzioni di) $-2x \equiv_{47} 6$, ovvero (dividendo -2 e 6 per -2, che è invertibile modulo 47) a $x \equiv_{47} -3$, che è già risolta: l'insieme delle soluzioni è $[-3]_{47}$.

Esempio 7.2.10

L'equazione $32x - 4 \equiv_{18} 8$ non è altro che un modo diverso di scrivere $32x \equiv_{18} 12$. Per semplificarla possiamo dividere tutto per 2 (MCD tra 32 e 18), ottenendo $16x \equiv_9 6$. Da questa, siccome 2 è coprimo con 9, quindi invertibile modulo 9, dividendo 16 e 6 per 2 ricaviamo l'equazione equivalente $8x \equiv_9 3$; ma $8 \equiv_9 -1$, quindi possiamo riscrivere questa come $-x \equiv_9 3$, ovvero $x \equiv_9 -3$, e l'equazione originaria è risolta. In alternativa: da $32x \equiv_{18} 12$ passiamo a $-4x \equiv_{18} 12$, perché $-4 \equiv_{18} 32$, quindi, dividendo tutto per 2, a $-2x \equiv_9 6$; possiamo ancora dividere -2 per 2, o direttamente per -2, perché, di nuovo, 2 e -2 sono invertibili modulo 9, per ottenere ancora $x \equiv_9 -3$ e così l'insieme $[-3]_9$ di tutte le soluzioni.

Esempio 7.2.11

1. Un esempio simile: $14x \equiv_{111} 21$ ha le stesse soluzioni di $2x \equiv_{111} 3$; qui bisogna fare attenzione al fatto che 7, per il quale abbiamo diviso 14 e 21, e 111 sono coprimi. Come facciamo a saperlo? Be', $111 \equiv_7 111 - 70 = 40$, siccome 42 è multiplo di 7 certamente non lo è 40 (infatti $40 \equiv_7 2$), quindi 7 non divide 111; poiché 7 è primo questo garantisce che 7 e 111 sono coprimi. A questo punto dobbiamo risolvere $2x \equiv_{111} 3$. Possiamo farlo usando l'algoritmo euclideo, oppure osservando che, siccome 3 è dispari come 111, allora $3 + 111$ è pari, ne ricaviamo l'intero $(3 + 111)/2 = 114/2 = 57$, allora $2 \cdot 57 = 3 + 111 \equiv_{57} 3$ e così vediamo che 57 è soluzione dell'equazione. Dal momento che l'equazione è ridotta (2 e 111 sono coprimi), l'insieme delle soluzioni è $[57]_{111}$.
2. Si consideri l'equazione congruenziale:

$$ax \equiv_m b \quad (7.13)$$

Caso A: Risoluzione dell'equazione congruenziale del tipo: $ax \equiv_m 1$ con $MCD(a, m) = 1$.

Essendo $1 = MCD(a, m)$ è possibile determinare, mediante l'algoritmo di Euclide delle divisioni successive, degli interi α e β tali che risulti $\alpha a + \beta m = 1$. L'intero α risulta essere una soluzione dell'equazione e $[\alpha]_m$ coincide con l'insieme delle soluzioni dell'equazione.

Caso B: Risoluzione della generica equazione congruenziale $ax \equiv_m b$.

- Verificare che $d = MCD(a, m)$ divida b ; infatti, questa è condizione necessaria affinché l'equazione ammetta soluzioni. Se d divide b si può continuare;
- Posto $\bar{a} = \frac{a}{d}$, $\bar{b} = \frac{b}{d}$ e $\bar{m} = \frac{m}{d}$, si considera l'equazione

$$\bar{a}\bar{x} \equiv_{\bar{m}} \bar{b}$$

che ammette tutte e sole le soluzioni dell'equazione originale ed è tale che $MCD(\bar{a}, \bar{m}) = 1$.

- (c) Determinare una soluzione c dell'equazione congruenziale $\bar{a}\bar{x} \equiv_{\bar{m}} 1$ mediante il metodo illustrato nel Caso A.
3. Si dica se l'equazione congruenziale $20x \equiv_{34} 4$ ammette soluzioni; in caso di risposta affermativa, determinare l'insieme di tutte le soluzioni.

Risoluzione

- Si calcola il massimo comun divisore tra 20 e 34. In tal caso si ha $MCD(20, 34) = 2$ ed, essendo $2 \mid 4$, si ha che l'equazione ammette soluzioni che coincidono con quelle dell'equazione $10x \equiv_{17} 2$.
- Si studia l'equazione $10x \equiv_{17} 1$. Mediante l'algoritmo di Euclide si determinano gli interi h, k tali che $1 = 10h + 17k$. In questo caso $h = -5$ e $k = 3$. Quindi:

$$1 = (3)17 + (-5)10 \implies 2 = (6)17 + (-10)10$$

Quindi $[-10]_{17}$ è soluzione dell'equazione $10x \equiv_{17} 2$. Chiaramente $[-10]_{17} = [7]_{17}$.

7.3

L'ANELLO DEI POLINOMI



7.3.1 Definizione e terminologia essenziale

Definizione 7.3.1: Polinomio

Sia A un anello commutativo unitario ed indichiamo con 0 l'elemento neutro in A rispetto all'operazione di addizione. Una funzione $f : \mathbb{N} \rightarrow A$ si dice **successione di elementi di A** e si denota con $(a_n)_{n \in \mathbb{N}}$.

Una successione $(a_n)_{n \in \mathbb{N}}$ di elementi di A si dice **polinomio a coefficienti in A** se è *definitivamente nulla*, ovvero se:

$$\exists k \in \mathbb{N} ((\forall n \geq k)(a_n = 0)) \quad (7.14)$$

L'insieme di tutti i polinomi a coefficienti in A si denota con il simbolo $A[x]$.

Esempio 7.3.1

Sia $f : \mathbb{N} \rightarrow A$ la successione che associa ogni numero naturale all'elemento neutro in A . Chiaramente tale successione è un polinomio definitivamente nullo in quanto per ogni $n \geq 0$ si ha $a_n = 0$. Tale polinomio prende il nome di **polinomio nullo** ed è denotato anche col simbolo 0_A .

Definizione 7.3.2: Grado di un polinomio

Se $f \in A[x] \setminus \{0_A\}$ e $(a_i)_{i \in \mathbb{N}}$ è la successione dei coefficienti di f allora l'insieme $S_f = \{i \in \mathbb{N} \mid a_i \neq 0_A\}$ è finito e quindi, essendo un sottoinsieme finito non vuoto di \mathbb{N} , ha massimo; questo massimo è chiamato **grado** del polinomio f , denotato col simbolo $\deg(f)$ (o anche con altri simboli, tra i quali $\deg(f)$, $\deg f$ e $\delta(f)$).

Definizione 7.3.3: Coefficiente direttore e polinomi monici

Il coefficiente $a_{\deg(f)}$ di posto $\deg(f)$ si chiama **coefficiente direttore** di f e si indica con $cd(f)$. Un polinomio f è detto **monico** se e solo se il suo coefficiente direttore è 1_A . Il coefficiente di posto $i = 0$ viene invece chiamato **termine noto**.

Osservazione 7.3.1

In $(\mathbb{Z}, +, \cdot)$ consideriamo la successione: $\{a_1 = 0; a_2 = 3; a_4 = 0, a_5 = 1, a_6 = 0, \dots \forall n \geq 6 (a_n = 0)\}$. Tale successione risulta essere una successione di elementi di \mathbb{Z} definitivamente nulla in quanto esiste $k \in \mathbb{Z}$ ($k = 6$) per il quale ogni $n \geq k$ i termini a_n sono nulli. Il grado di tale polinomio può essere visto anche come:

$$\min_{k \in \mathbb{N}} \{k \in \mathbb{N} \mid (\forall n \geq k)(a_n = 0)\}$$

ovvero il minimo indice k per il quale la successione è definitivamente nulla. Quindi $\deg(f) = 5$ mentre $a_{\deg(f)} = 1$. Il polinomio ha grado 5 ed in particolare è monico in quanto il suo coefficiente direttore è pari a 1.

Il polinomio nullo risulta avere coefficiente direttore pari a 0_A mentre, per convenzione, si pone $\deg(0_A) = -\infty$ per indicare il fatto che il grado del polinomio nullo è il più piccolo di ogni altro polinomio.

Due polinomi $(a_n)_{n \in \mathbb{N}}$ e $(b_n)_{n \in \mathbb{N}}$ sono *uguali* se $a_n = b_n$ per ogni $n \in \mathbb{N}$. All'interno di $A[x]$ possiamo considerare le operazioni:

$$+ : ((a_n)_{n \in \mathbb{N}}, (b_n)_{n \in \mathbb{N}}) \in A[x] \times A[x] \mapsto (a_n + b_n)_{n \in \mathbb{N}} \quad (7.15)$$

$$\cdot : ((a_n)_{n \in \mathbb{N}}, (b_n)_{n \in \mathbb{N}}) \in A[x] \times A[x] \mapsto \left(\sum_{i+j=n} a_i \cdot b_j \right)_{n \in \mathbb{N}} \quad (7.16)$$

Esempio 7.3.2

Sia $A = \mathbb{Z}$ e si considerino i polinomi $a_n = \{1, 2, 0, \dots\}$ e $b_n = \{2, 0, \dots\}$. Si ha:

$$a_n + b_n = \{1+2, 2+0, \dots\} = \{3, 2, 0, \dots\}$$

mentre il prodotto:

$$\begin{aligned} a_n \cdot b_n &= \{a_0 b_0 = 1 \cdot 2 = 2, \\ &\quad a_0 b_1 + a_1 b_0 = 0 + 4 = 4, \\ &\quad a_1 b_1 + a_0 b_2 + a_2 b_0 = 0\} = \{2, 4, 0, \dots\} \end{aligned}$$

Proposizione 7.3.1

La struttura $(A[x], +, \cdot)$ è un anello commutativo con unità il polinomio $(1, 0, 0, \dots)$.

Dimostrazione. Chiaramente l'operazione di addizione risulta commutativa ed associativa e $(A[x], +)$ risulta un semigruppo commutativo. Inoltre, poiché A risulta un anello, per ogni elemento $a \in A$ esiste l'opposto rispetto all'operazione di somma ed è dunque possibile definire la successione opposta $(-a_n)_{n \in \mathbb{N}}$ e $(A[x], +)$ risulta quindi un gruppo abeliano.

L'elemento neutro rispetto all'operazione di addizione è il polinomio nullo 0_A e l'elemento neutro rispetto all'operazione di moltiplicazione è il polinomio costante 1_A . Inoltre, l'operazione di moltiplicazione risulta commutativa e associativa e $(A[x], \cdot)$ risulta un semigruppo commutativo. Infine, l'operazione di moltiplicazione risulta distributiva rispetto all'operazione di addizione e $(A[x], +, \cdot)$ risulta un anello commutativo con unità. \square

Definizione 7.3.4: Polinomio costante

Sia $(a_n)_{n \in \mathbb{N}}$ un polinomio a coefficienti in A . Tale polinomio si dice **costante** se e solo se per ogni $n \in \mathbb{N}^*$ risulta $a_n = 0_A$. In tal caso il polinomio costante si denota con il simbolo a_0 . Un polinomio è costante se:

$$\exists a \in A ((a_n)_{n \in \mathbb{N}} = (a, 0, 0, \dots))$$

Osservazione 7.3.2

Il polinomio nullo è un polinomio costante.

Consideriamo l'applicazione: $\varphi : a \in A \mapsto (a, 0, 0, \dots) \in A[x]$.

Proposizione 7.3.2

φ è un omomorfismo tra gli anelli $(A, +, \cdot)$ e $(A[x], +, \cdot)$. In particolare φ è un monomorfismo.

Dimostrazione. Per ogni $a, b \in A$ si ha:

$$\begin{aligned} \varphi(a+b) &= (a+b, 0, 0, \dots) \\ &= (a, 0, 0, \dots) + (b, 0, 0, 0) \\ &= \varphi(a) + \varphi(b) \end{aligned} \quad \text{Per la definizione di somma in } A[x]$$

Analogamente, per ogni $a, b \in A$:

$$\begin{aligned} \varphi(a \cdot b) &= (ab, 0, 0, \dots) \\ &= (a, 0, 0, 0, \dots) \cdot (b, 0, 0, 0, \dots) \\ &= \varphi(a) \cdot \varphi(b) \end{aligned} \quad \text{Per la definizione di prodotto in } A[x]$$

Dimostriamo ora che φ è iniettiva. Per ogni $a, b \in A$:

$$\varphi(a) = \varphi(b) \iff (a, 0, 0, 0, \dots) = (b, 0, 0, 0, \dots) \iff a = b$$

E l'asserto è dimostrato. \square

Per il teorema di omomorfismo, A è isomorfo all'insieme $im(\varphi) = \{(a, 0, 0, \dots) \mid a \in A\}$. Identifichiamo quindi A con l'insieme dei polinomi costanti ed è lecito definire ogni elemento $a \in A$ come il polinomio costante che ha per termine noto il termine a .

Poniamo $x = (0, 1, 0, \dots)$ e consideriamo il prodotto x^2 :

$$\begin{aligned} x^2 &= x \cdot x \\ &= (0, 1, 0, 0, \dots) \cdot (0, 1, 0, 0, \dots) \\ &= (0, 0, 1, 0, \dots) \end{aligned} \quad \text{Applicando la definizione di prodotto}$$

Supponendo che:

$$x^{n-1} = (\underbrace{0, \dots, 0}_{n-1 \text{ zeri}}, 1, 0, \dots)$$

si dimostra per induzione che:

$$\begin{aligned} x^n &= x^{n-1} \cdot x \\ &= (\underbrace{0, \dots, 0}_{n \text{ zeri}}, 1, 0, \dots) \cdot (0, 1, 0, \dots) \\ &= (\underbrace{0, \dots, 0}_{n \text{ zeri}}, 1, 0, 0, \dots) \end{aligned}$$

Allora quando consideriamo ax^n si ottiene:

$$(a, 0, 0, \dots) \cdot (\underbrace{0, \dots, 0}_{n \text{ zeri}}, 1, 0, 0, \dots) = (\underbrace{0, \dots, 0}_{n \text{ zeri}}, a, 0, \dots)$$

Supposto $f \in A[x]$ di grado m , ovvero:

$$f = (a_0, a_1, \dots, a_m, 0, \dots)$$

allora f , per come abbiamo definito la somma e per quanto appena visto per i polinomi del tipo ax^n , si può scrivere come:

$$f = a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m \quad (7.17)$$

che risulta la classica rappresentazione dei polinomi.

7.3.2 Proprietà universale

La proprietà più importante degli anelli di polinomi è la seguente:

Proposizione 7.3.3 (Proprietà universale per anelli di polinomi ad una indeterminata)

Sia $A[x]$ un anello di polinomi nell'indeterminata x sull'anello commutativo unitario A . Si fissino un anello commutativo unitario B ed un omomorfismo: $\theta : A \rightarrow B$ di anelli unitari e $b \in B$. Allora esiste uno ed un solo omomorfismo: $\theta^* : A[x] \rightarrow B$ di anelli unitari tale che $\theta^*(x) = b$ e θ sia la restrizione di θ^* ad A .

In altre parole, fissato un omomorfismo $\theta : A \rightarrow B$, esiste ed è unico l'omomorfismo:

$$\theta^* : \sum_{i=0}^n a_i x^i \in A[x] \mapsto \sum_{i=0}^n \theta(a_i) b^i \in B \quad (7.18)$$

che rende commutativo il diagramma a sinistra (l'omomorfismo $A \hookrightarrow A[x]$ è l'immersione di A in $A[x]$) come mostrato nel diagramma a destra:

$$\begin{array}{ccc} A & \xrightarrow{\theta} & B \\ & \searrow & \nearrow \\ & A[x] & \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{\theta} & B \\ & \searrow & \nearrow \theta^* \\ & A[x] & x \mapsto b \end{array}$$

Vediamo alcune importanti applicazioni della proprietà universale:

- Unicità dell'anello dei polinomi, a meno di isomorfismi.* Supponiamo che $A[x]$ e $A[y]$ siano due anelli di polinomi ad una indeterminata sullo stesso anello (commutativo unitario) A , con indeterminate, rispettivamente x e y . Applichiamo la proprietà universale scegliendo come θ l'immersione $A \hookrightarrow A[y]$ e, come b , l'elemento y . Otteniamo così un unico omomorfismo $\alpha : A[x] \rightarrow A[y]$ tale che $\alpha(x) = y$ e la restrizione di α ad A sia l'immersione, cioè $\alpha(a) = a$ per ogni $a \in A$. Poiché anche $A[y]$ è un anello di polinomi, possiamo ripetere la stessa costruzione scambiando i ruoli di $A[x]$ e $A[y]$.

$$\begin{array}{ccc} A & \xleftarrow{\quad} & A[y] \\ & \searrow & \nearrow \\ & A[x] & x \xrightarrow{\alpha} b \end{array} \qquad \begin{array}{ccc} A & \xleftarrow{\quad} & A[x] \\ & \searrow & \nearrow \\ & A[y] & x \xrightarrow{\beta} b \end{array}$$

Ottenendo un omomorfismo $\beta : A[y] \rightarrow A[x]$ tale che $\beta(y) = x$ e $\beta(a) = a$ per ogni $a \in A$. È facile verificare che α e β sono l'uno l'inverso dell'altro. Infatti, per ogni elemento $f = \sum_{i=0}^n a_i x^i$ di $A[x]$ si ha:

$$\beta(\alpha(f)) = \beta\left(\sum_{i=0}^n a_i y^i\right) = \sum_{i=0}^n a_i x^i = f$$

e, similmente:

$$\alpha(\beta(g)) = \alpha\left(\sum_{i=0}^n b_i x^i\right) = \sum_{i=0}^n b_i y^i = g$$

per ogni $g \in A[y]$. Ciò prova che α è un isomorfismo.

Dunque, assegnati due anelli di polinomi ad una indeterminata su A esiste un isomorfismo tra questi due anelli di polinomi che manda l'indeterminata del primo nell'indeterminata del secondo e manda in se stesso ogni elemento di A . Con le notazioni appena usate, questo isomorfismo è l'applicazione:

$$\alpha : \sum_{i=0}^n a_i x^i \in A[x] \mapsto \sum_{i=0}^n a_i y^i \in A[y]$$

osserviamo esplicitamente che essa manda ogni polinomio f di $A[x]$ nel polinomio di $A[y]$ che ha la stessa successione dei coefficienti di f . Possiamo dunque dire, in modo un poco approssimativo ma efficace, che due anelli di polinomi sullo stesso anello commutativo unitario A possono solo differire per il nome dell'indeterminata; in questo senso, a meno di isomorfismi, ne esiste solo uno.

- Omomorfismo di sostituzione.* L'applicazione più frequente della proprietà universale si ha per il caso in cui $B = A$ e θ è l'applicazione identica di A . In questo caso la proprietà ci dice che per ogni $c \in A$ esiste uno ed un solo omomorfismo di anelli unitari $A[x] \rightarrow A$ che manda ogni elemento di A in sé e x in c :

$$\begin{array}{ccc} A & \xrightarrow{id_A} & A \\ & \searrow & \nearrow \\ & A[x] & x \mapsto c \end{array}$$

È facile descrivere esplicitamente questo omomorfismo. Per ogni $f = \sum_{i=0}^n a_i x^i \in A[x]$ poniamo $f(c) = \sum_{i=0}^n a_i c^i$. L'omomorfismo di cui stiamo parlando è allora l'applicazione:

$$f \in A[x] \mapsto f(c) \in A$$

che chiamiamo **omomorfismo di sostituzione**.

- Per ogni intero positivo m , sia $\epsilon_m : n \in \mathbb{Z} \mapsto [n]_m \in \mathbb{Z}_m$, la proiezione canonica $\mathbb{Z} \twoheadrightarrow \mathbb{Z}_m$ (il simbolo di freccia a doppia punta ci ricorda il fatto che ϵ_m è un omomorfismo suriettivo). Componendo questa con l'immersione $\iota_m : \mathbb{Z}_m \hookrightarrow \mathbb{Z}_m[x]$ otteniamo l'omomorfismo di anelli unitari $\iota_m \circ \epsilon_m = \epsilon_m \iota_m : n \in \mathbb{Z} \mapsto [n]_m \in \mathbb{Z}_m[x]$. La proprietà universale fornisce l'omomorfismo $\overline{\epsilon_m}$ qui descritto:

$$\begin{array}{ccccc} \mathbb{Z} & \xrightarrow{\epsilon_m} & \mathbb{Z}_m & \xleftarrow{\iota_m} & \mathbb{Z}_m[x] \\ & \searrow & & & \nearrow \\ & & \mathbb{Z}[x] & \xrightarrow{x \xrightarrow{\overline{\epsilon_m}} x} & \end{array}$$

Più esplicitamente, l'immagine mediante $\overline{\epsilon_m}$ di $f = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ è il polinomio $f_m = \sum_{i=0}^n [a_i]_m x^i$. f_m è detto **polinomio f riguardato come polinomio a coefficienti in \mathbb{Z}_m** .

7.3.3 ■ Grado di somme e prodotto di polinomi

Siano, ancora, A un anello commutativo unitario, e siano $f, g \in A[x]$, con successioni dei coefficienti, rispettivamente, $(a_n)_{n \in \mathbb{N}}$ e $(b_n)_{n \in \mathbb{N}}$. Supponiamo anche $f \neq 0_A \neq g$ e poniamo $n = \deg(f)$, $m = \deg(g)$. Grazie alla notazione introdotta (Formula 7.17) possiamo ridefinire le operazioni di addizione e moltiplicazione di polinomi in $A[x]$.

Proposizione 7.3.4

Siano $f, g \in A[x]$ e sia $m = \deg(f)$ ed $n = \deg(g)$. Allora, posto $M = \max\{m, n\}$ si ha:

$$f + g = \sum_{i=0}^M (a_i + b_i)x^i \quad (7.19)$$

$$f \cdot g = \sum_{i=0}^{m+n} (\sum_{j=0}^i a_j \cdot b_{i-j})x^i \quad (7.20)$$

Dimostrazione. Consideriamo la somma $f + g$:

$$\begin{aligned} f + g &= (a_0 + a_1 x + \dots + a_m x^m) + (b_0 + b_1 x + \dots + b_n x^n) \\ &= a_0 + b_0 + a_1 x + b_1 x + \dots + a_M x^M + b_M x^M \\ &= a_0 + b_0 + (a_1 + b_1)x + \dots + (a_M + b_M)x^M \\ &= \sum_{i=0}^M (a_i + b_i)x^i \end{aligned}$$

Applicando la distributività di \cdot rispetto a $+$

Per quanto riguarda il prodotto, invece:

$$\begin{aligned} f \cdot g &= (a_0 + a_1 x + \dots + a_m x^m) \cdot (b_0 + b_1 x + \dots + b_n x^n) \\ &= a_0 \cdot (b_0 + b_1 x + \dots + b_n x^n) + a_1 x \cdot (b_0 + b_1 x + \dots + b_n x^n) + \dots + a_m x^m \cdot (b_0 + b_1 x + \dots + b_n x^n) \\ &= a_0 b_0 + a_0 b_1 x + \dots + a_0 b_n x^m + a_1 b_0 x + a_1 b_1 x^2 + \dots + a_m b_0 x^m + \dots + a_m b_1 x^{m+1} + \dots + a_m b_n x^{m+n} \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (b_0 a_2 + a_0 b_2 + a_1 b_1)x^2 + \dots + (a_m b_n)x^{m+n} \\ &= \sum_{i=0}^{m+n} (\sum_{j=0}^i a_j \cdot b_{i-j})x^i \end{aligned}$$

Come volevasi dimostrare. □

Cosa possiamo dire sul grado di questi tre polinomi? Consideriamo in primo luogo il polinomio $f + g$. Nella sua espressione non compaiono potenze di x con esponente superiore ad M , quindi certamente $\deg(f + g) \leq M$, e $\deg(f + g) = M$ se, e solo se, il coefficiente di posto M in $f + g$ (cioè $a_M + b_M$) è diverso da zero. Distinguiamo tre casi:

1. Se $n < m$ allora $M = m$ e $a_m = 0_A$, quindi $a_M + b_M = b_M \neq 0_A$. In questo caso, dunque, $\deg(f + g) = m = M$. Inoltre $cd(f + g) = b_m = cd(g)$.
2. Similmente, se $n > m$, vediamo che $f + g$ ha grado n e coefficiente direttore $a_n = cd(f)$.
3. Se $n = m$ bisogna fare una distinzione ulteriore:

(a) Se $a_n + b_n \neq 0_A$ abbiamo $\deg(f + g) = n = M$ e $cd(f + g) = a_n + b_n$

(b) Se $a_n + b_n = 0_A$ (cioè $a_n = -b_n$) allora certamente $\deg(f + g) < n$

Proposizione 7.3.5

Se A è un anello commutativo unitario e $f, g \in A[x] \setminus 0_A$, allora:

$$\deg(f + g) = \max\{\deg(f), \deg(g)\} \quad (7.21)$$

a meno che $\deg(f) = \deg(g)$ e $cd(f) = -cd(g)$. In questo secondo caso:

$$\deg(f + g) < \deg(f) = \deg(g) \quad (7.22)$$

Proposizione 7.3.6

Se A è un anello commutativo unitario e $f, g \in A[x] \setminus \{0_A\}$, allora:

$$\deg(f - g) = \max\{\deg(f), \deg(g)\} \quad (7.23)$$

a meno che $\deg(f) = \deg(g)$ e $cd(f) = cd(g)$. In questo secondo caso:

$$\deg(f - g) < \deg(f) = \deg(g) \quad (7.24)$$

Esempio 7.3.3

Se $f = 3x^2 + x + 1$ e $g = 2x^2 + x + 2$ sono polinomi a coefficienti interi (con $\deg(f) = \deg(g) = 2$) allora:

$$f - g = x^2 - 1$$

ha anch'esso grado due. Se invece $g = 3x^2 + x + 2$ allora $\deg(f) = \deg(g)$ e $cd(f) = cd(g)$ e quindi:

$$f - g = -1$$

ha grado zero.

Passiamo ora a considerare il grado di fg . Il ragionamento è simile: poiché nell'espressione di fg non appaiono potenze di x con esponente superiore a $n + m$ certamente $\deg(fg) \leq n + m$ e vale $\deg(fg) = n + m$ se, e solo se, $a_n b_n \neq 0$.

Proposizione 7.3.7

Se A è un anello commutativo unitario e $f, g \in A[x] \setminus \{0_A\}$, posto $a = cd(f)$ e $b = cd(g)$ si ha:

$$ab \neq 0_A \implies cd(fg) = ab \wedge \deg(fg) = \deg(f) + \deg(g) \quad (7.25)$$

$$ab = 0_A \implies \deg(fg) < \deg(f) + \deg(g) \quad (7.26)$$

Se vale la 7.25 si dice che per i polinomi f e g vale la **regola di addizione dei gradi**. Ovviamente questa regola vale sempre nel caso in cui uno dei due polinomi sia il polinomio nullo. Alcune importanti conseguenze di tale regola sono le seguenti:

Corollario 7.3.1

Sia A un anello commutativo unitario e sia $f \in A[x]$. Se $cd(f)$ è cancellabile in A allora f è cancellabile in $A[x]$ e, per ogni $g \in A[x]$, si ha $\deg(fg) = \deg(f) + \deg(g)$.

Dimostrazione. Sia $g \in A[x] \setminus \{0_A\}$ e siano $a = cd(f)$ e $b = cd(g)$. Poiché a è cancellabile in A , quindi non un divisore dello zero, e $b \neq 0_A$ allora $ab \neq 0_A$. Per quanto osservato in precedenza vale allora la 7.25 e sicuramente $fg \neq 0_A$. Quindi f non è un divisore dello zero e quindi è cancellabile. \square

Proposizione 7.3.8

Sia A un anello commutativo unitario. Sono equivalenti:

1. A è un dominio di integrità;
2. Per ogni coppia di polinomi in $A[x]$ vale la regola di addizione dei gradi;
3. $A[x]$ è un dominio di integrità.

Inoltre, se A è un dominio di integrità allora $\mathcal{U}(A[x]) = \mathcal{U}(A)$.

Dimostrazione. (1) \implies (2) Per ogni polinomio $f \in A[x]$ distinguiamo due casi:

1. $f \neq 0_A$: allora $cd(f)$ è non nullo e quindi cancellabile in A in quanto dominio di integrità ed è possibile applicare il Corollario precedente.

2. Se $f = 0_A$ vale sempre la regola di addizione dei gradi.

Ovviamente (2) \implies (3) in quanto se vale la regola di addizione dei gradi allora $\forall f, g \in A[x] (fg \neq 0_A)$ e allora vale la legge di annullamento del prodotto in $A[x]$ che quindi risulta un dominio di integrità.

(3) \implies (1) banale: se $A[x]$ è un dominio di integrità e $a, b \in A \setminus \{0_A\}$ allora $ab \neq 0_A$ perché altrimenti a sarebbe un divisore dello zero in $A[x]$.

Resta da provare solo che $\mathcal{U}(A[x]) = \mathcal{U}(A)$ se valgono le condizioni (1), (2) e (3).

Se $a \in \mathcal{U}(A)$ e b è l'inverso di a in A , allora $ab = 1_A = 1_{A[x]}$, quindi b è anche l'inverso di a in $A[x]$, dunque $a \in \mathcal{U}(A[x])$. Pertanto $\mathcal{U}(A) \subseteq \mathcal{U}(A[x])$.

Nell'ipotesi che A sia un dominio di integrità sia, viceversa, $f \in \mathcal{U}(A[x])$ e sia g l'inverso di f in $A[x]$. Allora $fg = 1_A$ e, ovviamente, $f \neq 0_A \neq g$. Poiché in $A[x]$ vale la regola di addizione dei gradi, $\deg(f) + \deg(g) = \deg(fg) = \deg(1_A) = 0_A$. Dunque, $\deg(f)$ e $\deg(g)$ sono due numeri naturali la cui somma è 0; di conseguenza $\deg(f) = \deg(g) = 0$. Ciò mostra che $f \in A$ e $g \in A$, quindi sia f che il suo inverso sono elementi di A , dunque $f \in \mathcal{U}(A)$.

Abbiamo così provato anche l'inclusione inversa. □

Esempio 7.3.4

Vediamo così che la regola di addizione dei gradi non vale per polinomi su anelli che non siano domini di integrità, ed è importante osservare che per tali anelli può non valere neanche la conclusione finale dell'ultima proposizione appena dimostrata: non è detto che i polinomi invertibili siano costanti. Consideriamo l'anello $A = (\mathbb{Z}_4, +, \cdot)$ e il polinomio di grado 1 a coefficienti in A :

$$f = [1]_4 + [2]_4x$$

Calcolando il prodotto $f \cdot f$ si ottiene:

$$\begin{aligned} f \cdot f &= ([1]_4 + [2]_4x) \cdot ([1]_4 + [2]_4x) \\ &= [1]_4 + [2]_4x + [2]_4x + [4]_4x \\ &= [1]_4 + [8]_4x \\ &= [1]_4 \end{aligned}$$

Ottenendo così un polinomio costante (di grado zero). In particolare osserviamo che f risulta invertibile e coincide con il proprio inverso. In questo caso notiamo che non vale la regola di addizione dei gradi in quanto, ricordando il Teorema di caratterizzazione dell'anello degli interi modulo m (Teorema 7.2.4), \mathbb{Z}_4 non risulta essere un dominio di integrità in quanto 4 non è primo. Notiamo infatti che il coefficiente direttore di f , $[2]_4$, è un divisore dello zero.

Proposizione 7.3.9 (Condizione di non invertibilità)

Sia $f \in A[x]$. Se f è cancellabile e $\deg(f) > 0$, allora f non è invertibile.

Dimostrazione. Per assurdo, sia f invertibile e sia $g = f^{-1}$ un suo inverso. Allora per la 7.25:

$$\deg(f) + \deg(g) = \deg(fg) = \deg(1) = 0 \implies \deg(f) = 0$$

il che è assurdo. □

Esempio 7.3.5

I polinomi monici di grado maggiore di zero non sono mai invertibili. Qualunque sia l'anello commutativo unitario non nullo A , l'indeterminata x non è mai invertibile in $A[x]$. Infatti, se x fosse invertibile, detto g il suo inverso, avremmo $1_A = xg$ e quindi $\deg(xg) = 0$ ma, valendo la 7.25, si ha $\deg(xg) = \deg(x) + \deg(g) = 1 + \deg(g)$, in contraddizione con quanto appena detto. Di conseguenza, qualsiasi sia l'anello commutativo unitario non nullo A , in $A[x]$ esistono elementi non invertibili e diversi dallo zero, quindi $A[x]$ non è un campo.

7.3.4 ■ Divisione con resto tra polinomi

Se f e g sono due polinomi su un anello commutativo unitario A , con $g \neq 0_A$, diciamo che in $A[x]$ è possibile effettuare la divisione di f (il dividendo) per g (il divisore) se e solo se esistono $q, r \in A[x]$ tali che $f = gq + r$ e $\deg(r) < \deg(g)$.

Un'osservazione banale è che se, nella situazione appena descritta, $\deg(f) < \deg(g)$ allora è sicuramente possibile effettuare la divisione di f per g : basta porre $q = 0$ e $r = f$.

Teorema 7.3.1 (della divisione lunga)

Siano A un anello commutativo e $f, g \in A[x]$. Supponiamo che $cd(g) \in U(A)$. Allora esiste una ed una sola coppia $(q, r) \in A[x] \times A[x]$ tale che $f = gq + r$ e $\deg(r) < \deg(g)$.

Dimostrazione. Iniziamo a provare l'esistenza di (q, r) . Come appena osservato, se $\deg(f) < \deg(g)$ una coppia con le proprietà richieste si ottiene ponendo $q = 0$ e $r = f$. Possiamo allora supporre $n = \deg(f)$, $m = \deg(g)$ e sia $n \geq m$. osserviamo che l'ipotesi su $cd(g)$ garantisce che $cd(g) \neq 0_A$ e quindi $n, m \in \mathbb{N}$.

Ragioniamo per induzione su n , quindi supponiamo che, per ogni $h \in A[x]$ tale che $\deg(h) < n$, sia possibile effettuare la divisione di h per g . Siano $a = cd(f)$ e $b = cd(g)$. Consideriamo il polinomio:

$$k := (ab^{-1}x^{n-m})g$$

È chiaro che per k e g vale la regola di addizione dei gradi in quanto il prodotto dei coefficienti direttori di questi due polinomi è

$$(ab^{-1})cd(g) = ab^{-1} \cdot b = a \neq 0_A$$

Dunque vale la regola di addizione dei gradi e risulta:

$$\deg(k) = \deg(ab^{-1}x^{n-m}) + \deg(g) = (n - m) + m = n = \deg(f)$$

e

$$cd(k) = a = cd(f)$$

Allora f e k hanno lo stesso grado e lo stesso coefficiente direttore.

Considerato il polinomio $f_1 := f - k$ sappiamo per certo che $\deg(f_1) < n$. L'ipotesi induttiva garantisce che è possibile effettuare la divisione di f_1 per g , dunque esistono $q_1, r_1 \in A[x]$ tali che:

$$f_1 = gq_1 + r_1$$

con:

$$\deg(r_1) < \deg(g)$$

Ora, $f_1 = f - k$, quindi $f = f_1 + k$, si ha allora:

$$\begin{aligned} f &= f_1 + k \\ &= f_1 + (ab^{-1}x^{n-m})g \\ &= (gq_1 + r_1) + (ab^{-1}x^{n-m})g \\ &= (ab^{-1}x^{n-m} + q_1)g + r_1 \\ &\simeq qg + r \end{aligned}$$

dove $q = ab^{-1}x^{n-m} + q_1$, $r = r_1$ e vale $\deg(r) = \deg(r_1) < \deg(g)$.

Dobbiamo ora verificarne l'unicità. Siano (q, r) e (\bar{q}, \bar{r}) due coppie di polinomi con le proprietà richieste. Dunque:

$$f = gq + r = g\bar{q} + \bar{r}$$

, inoltre $\deg(r), \deg(\bar{r}) < m$. Da:

$$gq + r = g\bar{q} + \bar{r} \implies g(q - \bar{q}) = \bar{r} - r$$

E quindi $\deg(\bar{r} - r) < m$. D'altra parte, poiché $cd(g)$ è invertibile, quindi cancellabile, vale per g e $q - \bar{q}$ la regola di addizione dei gradi, dunque:

$$\deg(g(q - \bar{q})) = m + \deg(q - \bar{q})$$

Abbiamo così

$$m + \deg(q - \bar{q}) = \deg(\bar{r} - r) < m$$

Di conseguenza $\deg(q - \bar{q}) < 0$ e quindi, essendo tali dei naturali deve essere per forza $q - \bar{q} = 0_A$, ovvero $\bar{q} = q$ e, quindi, poiché:

$$\bar{r} - r = g(q - \bar{q}) = 0_A$$

si ha $r = \bar{r}$. L'unicità è così dimostrata. □

Esempio 7.3.6

In $\mathbb{Q}[x]$ consideriamo i polinomi $f = 3x^5 + 3x^3 + x^2 - 1$ e $g = 2x^3 + x + 3$ e procediamo a dividere f per g . Poniamo quindi $n = \deg(f) = 5$, $m = \deg(g) = 3$, $a = cd(f) = 3$ e $b = cd(g) = 2$.

Abbiamo $ab^{-1}x^{n-m} = (3/2)x^2$, quindi:

$$\begin{aligned} k &= (ab^{-1}x^{n-m}) \cdot g \\ &= ((\frac{3}{2})x^2) \cdot (2x^3 + x + 3) \\ &= 3x^5 + (\frac{3}{2})x^3 + (\frac{9}{2})x^2 \end{aligned}$$

Seguendo la procedura descritta nella dimostrazione del teorema calcoliamo $h = f - k$. Se si avesse $\deg(h) < m$ allora la divisione terminerebbe: h sarebbe il resto, mentre il quoziente $ab^{-1}x^{n-m}$:

$$\begin{aligned} h &= (3x^5 + 3x^3 + x^2 - 1) - (3x^5 + (\frac{3}{2})x^3 + (\frac{9}{2})x^2) \\ &= 3x^5 + 3x^3 + x^2 - 1 - 3x^5 - (\frac{3}{2})x^3 - (\frac{9}{2})x^2 \\ &= (\frac{3}{2})x^3 - (\frac{7}{2})x^2 - 1 \end{aligned}$$

quindi $\deg(h) \geq m$ e la divisione va continuata, ripetendo la procedura dopo aver sostituito h ad f . Posto $a = cd(h)$ e $n_1 = \deg(h)$ calcoliamo $a_1 b^{-1} x^{n_1-m}$ (che scriviamo come secondo addendo del quoziente) e poi $k_1 = a_1 b^{-1} x^{n_1-m} g$ e $h_1 = h - k_1$. Nel nostro caso abbiamo $a_1 = 3/2$ e $n_1 = 3$, otteniamo dunque $k_1 = (3/2)x^3 + (3/4)x + (9/4)$ e $h_1 = -(7/2)x^2 - (3/4)x - 13/4$. Poiché $\deg(h)_1 < m$ la divisione termina: h_1 è il resto, il quoziente è la somma $q = ab^{-1}x^{n-m} + a_1 b^{-1} x^{n_1-m}$. Di seguito è mostrato come il procedimento descritto altro non è che la classica divisione in colonna.

$$\begin{array}{r} f \\ \hline g \\ \hline q \\ \hline r \end{array}$$

$$\begin{array}{r} 3x^5 + 3x^3 + x^2 - 1 \\ \hline (2x^3 + x + 3) \\ \hline \end{array}$$

$$\begin{array}{r} 3x^5 + (3/2)x^3 + (9/2)x^2 \\ \hline (3/2)x^3 - (7/2)x^2 \\ \hline (3/2)x^3 + (3/4)x + 9/4 \\ \hline -(7/2)x^2 - (3/4)x - 13/4 \\ \hline \end{array}$$

$$k_1 = a_1 b^{-1} x^{n_1-m}$$

$$r = h_1 = h - k_1$$

Un caso molto importante è quello dei polinomi a coefficienti in un campo. Infatti, se A è un campo e $0_A \neq g \in A[x]$ allora $cd(g)$ è invertibile, come ogni elemento non nullo di A . Dunque, in questo caso, l'ipotesi $cd(g) \in U(A)$ del teorema appena dimostrato può essere sostituita da $g \neq 0_A$. Il fatto che ogni polinomio a coefficienti in un campo non sullo sia divisibile ci permette di eseguire l'algoritmo euclideo delle divisioni successive.

Esempio 7.3.7

Per quanto appena detto, se F è un campo, è sempre possibile dividere un polinomio $f \in F[x]$ per un polinomio $g \in F[x] \setminus \{0_F\}$. Ad esempio, se $F = \mathbb{Z}_7[x]$, vediamo come si divide il polinomio $\bar{2}x^2 + \bar{3}x + \bar{4}$ per il polinomio $\bar{3}x + \bar{4}$. Un primo modo è quello di effettuare la divisione come se fosse in $\mathbb{Q}[x]$:

$$\begin{array}{r} 2x^2 + 3x + 4 \\ - 2x^2 - \frac{8}{3}x \\ \hline \frac{1}{3}x + 4 \\ - \frac{1}{3}x - \frac{4}{9} \\ \hline \frac{32}{9} \end{array}$$

Quindi:

$$\bar{2}x^2 + \bar{3}x + \bar{4} = (\bar{3}x + \bar{4}) \left(\frac{\bar{2}}{3}x + \frac{\bar{1}}{9} \right) + \frac{\bar{32}}{9}$$

Ma cosa sono $\frac{\bar{2}}{3}$, $\frac{\bar{1}}{9}$ e $\frac{\bar{32}}{9}$? In \mathbb{Z}_7 si ha che $\bar{3} \cdot \bar{5} = \bar{15} = \bar{1}$, quindi $\bar{3}^{-1} = \bar{5}$. Dunque $\frac{\bar{2}}{3} = \bar{10} = \bar{3}$. Similmente $\bar{9}^{-1} = \bar{4}$, quindi $\frac{\bar{1}}{9} = \bar{4}$ e $\frac{\bar{32}}{9} = \bar{32} \cdot \bar{4} = \bar{128} = \bar{1}$. Dunque:

$$\bar{2}x^2 + \bar{3}x + \bar{4} = (\bar{3}x + \bar{4})(\bar{3}x + \bar{4}) + \bar{1}$$

7.3.5 ■ Applicazioni polinomiali

Sia $f \in A[x]$, dove A è un anello polinomiale. Se $f = \sum_{i=0}^n a_i x^i$ e $c \in A$ si ha:

$$f(c) = \sum_{i=0}^n a_i c^i$$

Definizione 7.3.5: Applicazione polinomiale

L'applicazione:

$$\tilde{f} : c \in A \mapsto f(c) \in A \quad (7.27)$$

che prende il nome di **applicazione polinomiale** determinata da f in A .

Osservazione 7.3.3



A differenza dell'omomorfismo di sostituzione questa applicazione non è, in generale, un omomorfismo. osserviamo che se $f \in A$ allora $f(c) = f$ per ogni $c \in A$, quindi l'applicazione \tilde{f} è costante. È per questo motivo che gli elementi di A vengono chiamati polinomi costanti.

Definizione 7.3.6: Radice

L'elemento $c \in A$ è una **radice** di f se e solo se $f(c) = 0_A$.

Lemma 7.3.1

Siano A un anello commutativo unitario e $f, g \in A[x]$. Allora:

1. se, in $A[x]$, f divide g , ogni radice di f in A è radice di g .
2. se A è un dominio di integrità, allora le radici di fg in A sono tutti e soli gli elementi di A che sono radici di f o di g .

Dimostrazione. 1. Se $f |_{A[x]} g$ esiste $h \in A[x]$ tale che $g = fh$. Allora applicando l'omomorfismo di sostituzione definito da g , abbiamo:

$$g(c) = f(c)h(c) = 0_A h(c) = 0_A$$

dunque c è radice di g .

2. Per la (1), gli elementi di A che sono radici di f o g sono radici anche di fg , multiplo di entrambi. Viceversa, se c è radice di A di fg , allora:

$$0_A = (fg)(c) = f(c)g(c)$$

Poiché $A[x]$ è un dominio di integrità, questo implica che uno tra $f(c)$ e $g(c)$ è 0_A , quindi c è radice di uno tra f e g .

□

Teorema 7.3.2 (del resto)

Sia A un anello commutativo unitario e siano $f \in A[x]$ e $c \in A$. Allora $f(c)$ è il resto della divisione di f per $x - c$.

Dimostrazione. La prima cosa da osservare è che si può certamente effettuare la divisione di f per $x - c$, perché quest'ultimo polinomio è monico, quindi il suo coefficiente direttore è invertibile. Effettuata questa divisione, otteniamo $q, r \in A[x]$ tali che $f = (x - c)q + r$ e si ha $\deg(r) < \deg(x - c) = 1$. Quest'ultima condizione equivale a dire che r è un polinomio costante. Applichiamo l'omomorfismo di sostituzione:

$$f(c) = ((x - c)q + r)(c) = (c - c)q(c) + r(c) = 0_A q(c) + r = r$$

È così provato che $f(c) = r$.

□

Teorema 7.3.3 (di Ruffini)

Sia A un anello commutativo unitario e siano $f \in A[x]$ e $c \in A$. Allora c è radice di f se e solo se $(x - c)$ divide f in $A[x]$, ovvero se e solo se il resto della divisione di f per $(x - c)$ è zero.

Dimostrazione. Per il teorema del resto, c è radice di f se e solo se il resto della divisione di f per $x - c$ è zero, cioè se e solo se $x - c$ divide f . \square

Esempio 7.3.8

Dato il polinomio $f(x) = x^3 - 2x^2 - 5x + 10$ abbiamo che $f(2) = 0$ e $f(\sqrt{5})$. Per il teorema di Ruffini, abbiamo che $x - 2$ e $x - \sqrt{5}$ dividono $f(x)$. Abbiamo infatti:

$$x^3 - 2x^2 - 5x + 10 = (x - 2)(x^2 - 5) = (x - 2)(x - \sqrt{5})(x + \sqrt{5})$$

Corollario 7.3.2

Sia A un anello commutativo unitario e siano $f, g \in A[x]$ e $c \in A$. Supponiamo che f e g abbiano in $A[x]$ un massimo comun divisore d . Allora le radici comuni a f e g in A sono tutte e sole le radici di d in A :

$$\{c \in A \mid f(c) = 0_A = g(c)\} = \{c \in A \mid d(c) = 0_A\} \quad (7.28)$$

Teorema 7.3.4 (di Ruffini generalizzato)

Sia A un dominio di integrità unitario e siano $f \in A[x]$, $n \in \mathbb{N}^*$ e $c_1, c_2, \dots, c_n \in A$ degli elementi a due a due distinti. Allora si ha che ciascuno degli elementi c_i è radice di f se e solo se:

$$\prod_{i=1}^n (x - c_i) \mid_{A[x]} f$$

Dimostrazione. \Leftarrow Ovvio. Se $\prod_{i=1}^n (x - c_i)$ divide f allora ciascuno degli elementi c_i è radice di f , in quanto $x - c_i$ divide f .

\Rightarrow Si procede per induzione su n . Supponiamo che gli elementi c_i per ogni $i \in \{1, 2, \dots, n\}$ siano radici di f . Se $n = 1$ allora $x - c_1$ divide f per il teorema di Ruffini. Supponiamo allora $n > 1$ e, come ipotesi di induzione, che l'enunciato valga per insiemi di $n - 1$ elementi distinti di A ed arbitrari polinomi in $A[x]$.

Poiché $f(c_n) = 0_A$, per il teorema di Ruffini esiste $q \in A[x]$ tale che $f = (x - c_n)q$. Sia ora i un intero tale che $1 \leq i < n$. Poiché c_i è radice di f e A è un dominio di integrità, segue che c_i è radice di uno tra $x - c_n$ e q (vedi Lemma 7.3.1). Dunque ciascuno degli elementi c_1, c_2, \dots, c_{n-1} è radice di q . Possiamo allora applicare l'ipotesi di induzione e concludere che:

$$\prod_{i=1}^{n-1} (x - c_i) \mid_{A[x]} q$$

quindi esiste $h \in A[x]$ tale che:

$$q = h \prod_{i=1}^{n-1} (x - c_i)$$

Allora:

$$\begin{aligned} f &= q \cdot (x - c_n) \\ &= \left(h \cdot \prod_{i=1}^{n-1} (x - c_i) \right) \cdot (x - c_n) \\ &= h \prod_{i=1}^n (x - c_i) \end{aligned}$$

Pertanto $\prod_{i=1}^n (x - c_i)$ divide f in $A[x]$ e la dimostrazione è così completa. \square

Il teorema di Ruffini generalizzato ha due importantissime conseguenze. La prima è una **limitazione al numero di radici che un polinomio non nullo su un dominio di integrità può avere**.

Teorema 7.3.5

Sia A un dominio di integrità unitario e sia $0_A \neq f \in A[x]$. Allora il numero delle radici di f in A non supera $\deg(f)$.

Dimostrazione. Se f ha esattamente n radici, siano esse c_1, c_2, \dots, c_n allora f è multiplo di g :

$$g := \prod_{i=1}^n (x - c_i)$$

Quindi $f = gq$ per un opportuno $q \in A[x]$. Essendo $f \neq 0_A$ si ha anche $q \neq 0_A$. Ma $\deg(g) = n$ e per g e q vale la regola di addizione dei gradi. Quindi $\deg(f) = \deg(g) + \deg(q) = n + \deg(q) \geq n$, ovvero $n \leq \deg(f)$. \square

Osservazione 7.3.4



Sia per il teorema di Ruffini generalizzato che per il Teorema 7.3.5 è essenziale l'ipotesi che l'anello sia un dominio di integrità. Sia $f = \bar{2}x \in \mathbb{Z}_6[x]$. Sia $\bar{0}$ che $\bar{3}$ sono radici del polinomio, quindi f ha più radici di quanto sia il suo grado, che è 1. Inoltre, come imposto dal teorema di Ruffini sia $x = x - \bar{0}$ che $x - \bar{3}$ dividono f . Infatti:

$$f = x \cdot \bar{2} = (x - \bar{3}) \cdot \bar{2}$$

Ma osserviamo che $x(x - \bar{3})$ non divide f , quindi la conclusione di Ruffini generalizzato non vale per f .

L'altra conseguenza del teorema di Ruffini generalizzato riguarda le applicazioni polinomiali e ci dice che, nel caso dei domini di integrità infiniti, ogni polinomio è identificato univocamente dalla sua applicazione polinomiale.

Proposizione 7.3.10

Principio di identità dei polinomi Sia A un dominio di integrità infinito. Allora, per ogni $f, g \in A[x]$ si ha:

$$\tilde{f} = \tilde{g} \iff f = g$$

Dimostrazione. Ovviamente $\tilde{f} = \tilde{g}$ se $f = g$. Supponiamo, viceversa, $\tilde{f} = \tilde{g}$. Allora $f(c) = g(c)$ per ogni $c \in A$. Sia $h = f - g$. Allora, per ogni $c \in A$ abbiamo $h(c) = (f - g)(c) = f(c) - g(c) = 0_A$, vale a dire: ogni elemento di A è radice di h . Dunque h ha un numero infinito di radici. Ma il Corollario precedente assicura che, se $h \neq 0_A$, allora il numero delle radici di h non supera $\deg(h)$, quindi è finito. Di conseguenza deve essere $h = 0_A$, ovvero $f = g$. \square

È a causa del principio di identità dei polinomi che in alcuni casi vengono identificati i polinomi con le applicazioni polinomiali. Ad esempio, nei corsi di analisi matematica si definiscono i polinomi come particolari funzioni da \mathbb{R} a \mathbb{R} , quelle che per noi sono le applicazioni polinomiali definite dai polinomi in $\mathbb{R}[x]$. Questo è lecito perché, essendo \mathbb{R} un campo (quindi un dominio di integrità infinito), il principio di identità dei polinomi assicura che i polinomi in $\mathbb{R}[x]$ corrispondono esattamente alle loro applicazioni polinomiali (in corsi di analisi più avanzati i polinomi sono definiti con riferimento al campo complesso, anziché a quello reale; il discorso è analogo: anche per il campo complesso vale il principio di identità dei polinomi). D'altra parte, non è lecito identificare polinomi ed applicazioni polinomiali in contesti in cui non valga il principio di identità dei polinomi, cioè quando l'anello A considerato sia finito oppure non sia integro.

Nel caso degli anelli finiti è certo che il principio di identità dei polinomi non può valere. Infatti, se A è un anello commutativo unitario finito, il numero delle applicazioni da A ad A , e quindi il numero delle applicazioni polinomiali in A , è finito, mentre $A[x]$ è comunque infinito. Dunque, in questo caso, è impossibile che ci sia una corrispondenza biunivoca tra polinomi e applicazioni polinomiali (cioè che il principio di identità dei polinomi afferma è che, se A è un dominio di integrità infinito, l'applicazione $f \in A[x] \mapsto \tilde{f} \in \text{Map}(A, A)$ è iniettiva; ciò è impossibile nel caso che stiamo considerando ora, in cui il dominio $A[x]$ è infinito ma il codominio $\text{Map}(A, A)$ è finito).

Esempio 7.3.9

Consideriamo il polinomio $f = x^3 - x \in \mathbb{Z}_3[x]$. Si ha:

$$\begin{aligned}\bar{f}([0]_3) &= \bar{0}^3 - \bar{0} = \bar{0} \\ \bar{f}([1]_3) &= \bar{1}^3 - \bar{1} = \bar{0} \\ \bar{f}([2]_3) &= \bar{2}^3 - \bar{2} = \bar{8} - \bar{2} = \bar{6} = \bar{0}\end{aligned}$$

Quindi $\bar{f} = \bar{0}$ ma $f \neq 0$.

7.3.6 ■ Fattorizzazione

Ricordiamo che un monoide commutativo cancellativo (cioè ad elementi tutti cancellabili) si dice **fattoriale** se e solo se ogni suo elemento non invertibile è prodotto di elementi irriducibili e tali decomposizioni in irriducibili sono essenzialmente uniche.

Teorema 7.3.6

Se A è un anello fattoriale allora $A[x]$ è fattoriale.

Sono certamente fattoriali i campi ed è fattoriale, per il Teorema Fondamentale dell'Aritmetica, l'anello \mathbb{Z} degli interi. Quindi è fattoriale $\mathbb{Z}[x]$ e, per ogni campo K , anche $K[x]$. Dunque, sia per i polinomi a coefficienti in \mathbb{Z} che per quelli a coefficienti in un campo vale un teorema di fattorizzazione essenzialmente unica in prodotto di polinomi irriducibili: *ogni polinomio non invertibile e non nullo è prodotto di polinomi irriducibili e tale fattorizzazione è unica a meno dell'ordine dei fattori e della sostituzione di alcuni fattori con polinomi associati*.

Se K è un campo, si ha:

$$\mathcal{U}(K[x]) = \mathcal{U}(K) = K \setminus \{0_K\}$$

Quindi l'insieme di tutti i polinomi associati ad un $f \in K[x] \setminus \{0_K\}$ è:

$$\{uf \mid u \in K \setminus \{0_K\}\}$$

Se $a = cd(f)$, si ha $cd(uf) = ua$ per ogni $u \in K \setminus \{0_K\}$. Allora, qualunque sia $k \in K \setminus \{0_K\}$, il polinomio f ha esattamente un associato con coefficiente direttore k , precisamente $(ka^{-1})f$. Infatti, per ogni $u \in K \setminus \{0_K\}$ abbiamo che $cd(uf) = ua = k$ se, e solo se, $c = ka^{-1}$.

Proposizione 7.3.11

Sia K un campo. In ogni classe di elementi associati di polinomi non nulli in $K[x]$ esiste uno ed un solo polinomio monico che prende il nome di **rappresentante monico**.

Esempio 7.3.10

In $\mathbb{Q}[x]$ il polinomio monico associato a $f = 3x^2 + x - 6$ è:

$$(\frac{1}{3})f = x^2 + \frac{1}{3}x - 2$$

ma anche:

$$-6x^2 - 2x + 12$$

e infiniti altri polinomi della forma uf , dove $0 \neq u \in \mathbb{Q}$.

Proposizione 7.3.12

Sia K un campo. Allora ogni polinomio non nullo in $K[x]$ è prodotto di un elemento di K e di polinomi monici irriducibili in $K[x]$. Tale fattorizzazione è unica a meno dell'ordine dei fattori.

Dimostrazione. L'unicità della fattorizzazione segue dal fatto che $K[x]$ è fattoriale e dal fatto che ogni classe di polinomi associati non nullo contiene un solo rappresentante monico. L'esistenza della decomposizione è ovvia nel caso dei polinomi costanti, va provata per polinomi non costanti. Sia, allora $f \in K[x] \setminus K$. Sia $f = p_1 p_2 \cdots p_n$ una fattorizzazione di f in prodotto di polinomi irriducibili. Per ogni $i \in \{1, 2, \dots, n\}$ sia $a_i = cd(p_i)$; allora $p_i = a_i q_i$, dove $q_i = a_i^{-1} p_i$ è associato a p_i (quindi è irriducibile) ed è monico. Posto $a = a_1 a_2 \cdots a_n$ abbiamo $f = a q_1 q_2 \cdots q_n$. Questa è la decomposizione cercata. \square

Osservazione 7.3.5

Nell'ipotesi che A sia fattoriale, una delle conseguenze del fatto che $A[x]$ è fattoriale è che, nota una fattorizzazione in prodotto di irriducibili di un polinomio f , è facile determinare l'insieme dei divisori di f . Posto infatti $f = p_1^{\lambda_1} \cdot p_2^{\lambda_2} \cdots p_n^{\lambda_n}$, dove i p_i sono polinomi irriducibili e per ogni $i \neq j$ p_i e p_j non sono associati, l'**insieme dei divisori** di f è dato da tutti i polinomi della forma:

$$p_1^{\sigma_1} \cdot p_2^{\sigma_2} \cdots p_n^{\sigma_n}$$

ed i loro associati, dove, per ogni i , $\sigma_i \in \mathbb{N}$ e $\sigma_i \leq \lambda_i$.

Quindi, ogni polinomio non nullo di grado diverso da zero a coefficienti su un campo K (ciò vale a dire: ogni elemento non zero e non invertibile di $K[x]$) si fattorizza in modo essenzialmente unico come prodotto di polinomi irriducibili. Poiché ogni classe di polinomi irriducibili associati contiene uno ed un solo polinomio monico, possiamo concludere che, se K è un campo, allora ogni polinomio $f \in K[x] \setminus K$ si scrive in modo unico (a meno dell'ordine dei fattori) come:

$$f = a_n f_1 f_2 \dots f_k$$

dove a_n è il coefficiente direttore di f e f_1, f_2, \dots, f_k sono polinomi monici irriducibili in $K[x]$. Ci vogliamo ora occupare di descrivere, per quanto possibile, la proprietà di essere o meno **irriducibile** per un polinomio a coefficienti in un campo. Vedremo in che modo questo proprietà è collegata alla presenza di radici.

Esempio 7.3.11

In $\mathbb{Q}[x]$, $x^2 - 1$ ammette la fattorizzazione:

$$x^2 - 1 = (x - 1)(x + 1)$$

In realtà $x^2 - 1$ ammette altre decomposizioni, come $(\frac{1}{2}x - \frac{1}{2}) \cdot (2x + 2)$. Tuttavia $x + 1$ e $2x + 2$ sono associati, differiscono cioè per un fattore invertibile. Allo stesso modo $x - 1$ e $\frac{1}{2}x - \frac{1}{2}$ sono associati. Quindi sostanzialmente le due decomposizioni sono la stessa.

Proposizione 7.3.13 (Criterio di irriducibilità)

Siano K un campo e $f \in K[x]$. Se $n = \deg(f)$ allora f è irriducibile in $K[x]$ se e solo se $n > 0$ e vale una delle due proprietà equivalenti:

1. non esistono $g, h \in K[x]$ tali che $f = gh$ e sia g che h abbiano grado minore di n ;
2. non esistono $g, h \in K[x]$ tali che $f = gh$ e sia g che h abbiano grado maggiore di 0 .

Dimostrazione. Ricordiamo che f è irriducibile se e solo se, in $K[x]$, non è invertibile e non ha divisori se non quelli banali. Possiamo subito osservare che i polinomi costanti non sono irriducibili. Infatti i polinomi costanti non nulli sono invertibili, mentre il polinomio nullo ha tutti gli elementi di $K[x] \setminus K$ come divisori non banali. Abbiamo così che l'asserto è corretto nel caso in cui f sia costante: f non è irriducibile e non è vero che $n = \deg(f) > 0$, quindi la condizione all'enunciato non è soddisfatta.

Possiamo allora assumere $f \notin K$, cioè: $n > 0$. Supponiamo dunque $n > 0$. osserviamo che, se $g, h \in K[x]$ e $f = gh$, per la regola di addizione dei gradi (che vale perché K è un campo) si ha:

$$n = \deg(f) = \deg(g) + \deg(h)$$

Quindi $\deg(g) < n$ e $\deg(h) < n$ che è equivalente alla condizione $(\deg(g) > 0 \wedge \deg(h) > 0)$, vale a dire che la (1) e la (2) sono equivalenti.

Se f è irriducibile, scelti comunque $g, h \in K[x]$ tali che $f = gh$, allora g è un divisore di f , quindi un divisore banale perché f è irriducibile. Allora o g è invertibile, nel qual caso $g \in K \setminus \{0_K\}$ e $\deg(g) = 0$, oppure g è associato ad f , nel qual caso $\deg(g) = \deg(f) = n$. Ciò mostra che, se f è irriducibile, sono verificate (1) e (2).

Se invece f non è irriducibile, f ha un divisore non banale g , allora $g \neq 0_K$ e g non è invertibile, quindi $\deg(g) > 0$ ed esiste $h \in K[x]$ tale che $f = gh$. Ovviamente $h \neq 0_K$ e h non è invertibile perché g non è associato ad f , quindi abbiamo anche $\deg(h) > 0$. In questo caso, dunque, non vale (2) e quindi neanche (1). \square

Osservazione 7.3.6



Un'ovvia conseguenza di questa caratterizzazione è che *i polinomi di primo grado a coefficienti in un campo K sono certamente irriducibili in $K[x]$* , dal momento che i prodotti tra polinomi di grado minore di 1 sono certamente costanti.

Proposizione 7.3.14

Sia K un campo e sia $f \in K[x]$. Allora f ha radici in K se e solo se ha almeno un divisore di primo grado in $K[x]$.

Proposizione 7.3.15

Sia A un dominio di integrità unitario e sia $f \in A[x]$. Se $\deg(f) > 1$ e f ha radici in A , allora f è riducibile in $A[x]$.

Proposizione 7.3.16

Siano K un campo e f un polinomio in $K[x]$ di grado 2 o 3. Allora f è irriducibile in $K[x]$ se e solo se è privo di radici in K .

Possiamo schematizzare come segue le informazioni ottenute sulle proprietà di un polinomio a coefficienti in un campo di essere o meno irriducibile ed di avere o meno radici. Se K è un campo e $0_K \neq f \in K[x]$, posto $\deg(f) = n$ si ha:

$n = 0$	\implies	f è invertibile e privo di radici
$n = 1$	\implies	f è irriducibile ed ha una radice
$n \in \{2, 3\}$	\implies	f irriducibile $\iff f$ non ha radici
$n > 3$	\implies	f irriducibile $\implies f$ non ha radici

Tabella 7.1: Irriducibilità di un polinomio in un campo

7.3.7 ■ Metodi ed esempi di fattorizzazione per polinomi su un campo

Supponiamo di voler fattorizzare un polinomio (in un fissato anello di polinomi) in prodotto di polinomi irriducibili. Per farlo abbiamo bisogno:

- di saper trovare divisori non banali del polinomio dato, se ne esistono;
- di saper riconoscere quali tra questi divisori sono irriducibili.

Limitiamoci al caso dei polinomi su un campo. Usando la tabella nella sezione precedente, sappiamo, in linea di massima, rispondere al secondo punto nel caso di divisori di grado minore di quattro. I polinomi di grado uno sono sempre irriducibili, quelli di grado due o tre lo sono se e solo se sono privi di radici. In due casi notevoli queste informazioni sono addirittura più di quanto non sia necessario. Infatti valgono questi teoremi (che non dimostriamo) per polinomi in $\mathbb{R}[x]$.

Teorema 7.3.7

Ogni polinomio irriducibile in $\mathbb{R}[x]$ ha grado minore di 3.

Dunque, i polinomi irriducibili in $\mathbb{R}[x]$ sono precisamente quelli di grado 1 e quelli di grado 2 privi di radici. Come è noto dalle scuole superiori, un polinomio $ax^2 + bx + c \in \mathbb{R}[x]$ di grado 2 ha radici in \mathbb{R} se e solo se $b^2 - 4ac \geq 0$.

Teorema 7.3.8 (di Bolzano)

Ogni polinomio di grado dispari in $\mathbb{R}[x]$ ha qualche radice in \mathbb{R} .

La situazione è molto più complessa (ed interessante) nel caso di polinomi in $\mathbb{Q}[x]$. Lo studio dei polinomi in $\mathbb{Q}[x]$ si può ridurre al caso dei polinomi a coefficienti interi. Ricordiamo che $\mathbb{Z}[x]$ è un dominio di integrità, così come $\mathbb{Q}[x]$, ma gli unici elementi invertibili di $\mathbb{Z}[x]$ sono ± 1 , cioè gli stessi di \mathbb{Z} . Inoltre i polinomi di $\mathbb{Z}[x]$ che dividono un intero $a_0 \neq 0$ devono avere grado zero, cioè solo a loro volta interi. Dunque:

- a_0 ha gli stessi divisori in $\mathbb{Z}[x]$ e \mathbb{Z} ;
- in particolare a_0 è invertibile in $\mathbb{Z}[x]$ se e solo se è invertibile in \mathbb{Z} , cioè se e solo se è ± 1 ;
- per $a_0 \neq \pm 1$, a_0 ha le stesse decomposizioni in prodotto di fattori irriducibili in $\mathbb{Z}[x]$ e in \mathbb{Z} .

Definizione 7.3.7: Polinomio primitivo

Sia $f(x)$ un polinomio a coefficienti interi. Si dice che $f(x)$ è primitivo se il massimo comun divisore dei suoi coefficienti è 1. Un polinomio monico intero è primitivo.

Teorema 7.3.9

Ogni polinomio $f \in \mathbb{Q}[x]$ è associato, in $\mathbb{Q}[x]$ ad un polinomio $\bar{f} \in \mathbb{Z}[x]$.

Esempio 7.3.12

Ad ogni polinomio $b(x) \in \mathbb{Q}[x]$ è associato un polinomio primitivo $a(x) \in \mathbb{Z}[x]$ ottenuto moltiplicando $b(x)$ per il minimo comune multiplo dei suoi coefficienti e successivamente dividendo il polinomio così ottenuto per il massimo comun divisore dei coefficienti. Ad esempio, il polinomio $f(x) = \frac{1}{2}x^2 + \frac{3}{4}x + \frac{1}{3}$ è associato al polinomio primitivo $g(x) = \frac{12}{2}x^2 + \frac{12 \cdot 3}{4}x + \frac{12}{3} = 6x^2 + 9x + 4$.

Ora, polinomi tra loro associati hanno esattamente le stesse proprietà rispetto alla fattorizzazione.

Proposizione 7.3.17 (Criterio di Eisenstein)

Sia $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in \mathbb{Z}[x]$. Se esiste un primo $p \in \mathbb{P}$ tale che:

1. p divide a_0, a_1, \dots, a_{n-1}
2. p non divide a_n
3. p^2 non divide a_0

allora f è irriducibile in $\mathbb{Q}[x]$.

Osservazione 7.3.7



Per ogni intero positivo n e per ogni primo p , il polinomio $x^n - p$ è irriducibile in $\mathbb{Q}[x]$ e dunque in $\mathbb{Q}[x]$ ci sono polinomi irriducibili di ogni grado.

Teorema 7.3.10 (delle radici razionali)

Sia $f = a_nx^n + a_{n-1}x^{n-1} + \dots + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$, un polinomio a coefficienti interi con $a_n \neq 0$. Allora ogni soluzione razionale di f (ogni radice in \mathbb{Q}) si scrive come frazione u/v , dove u e v sono interi coprimi e u è un divisore del termine noto a_0 e v è un divisore del coefficiente direttore a_n .

Dimostrazione. Ogni numero razionale si può scrivere come frazione ridotta, quindi nella forma u/v , dove u e v sono interi coprimi e $v \neq 0$. Se una tale frazione u/v è radice di f allora:

$$0 = a_0v^n + a_1uv^{n-1} + a_2u^2v^{n-2} + \dots + a_{n-2}u^{n-2}v^2 + a_{n-1}u^{n-1}v + a_nu^n = 0$$

Ora, escluso (per il momento) il primo, tutti gli addendi a primo membro sono multipli di u . Poiché la loro somma vale 0, il primo addendo a_0v^n è l'opposto della somma dei rimanenti. Quindi anch'esso è un multiplo di u . Dunque u divide a_0v^n . Ma u è coprimo con v , quindi con v^n , dunque u divide a_0 . In modo analogo v divide a_n . \square

Osservazione 7.3.8



Ogni polinomio in $\mathbb{Q}[x]$ è associato (in $\mathbb{Q}[x]$) ad un polinomio in $\mathbb{Z}[x]$, che avrà le stesse radici razionali.

Quindi, per cercare le radici razionali di un polinomio in $\mathbb{Q}[x]$ possiamo cercare le radici razionali del suo associato in $\mathbb{Z}[x]$. Questo è un vantaggio perché, come abbiamo visto, la ricerca delle radici razionali di un polinomio in $\mathbb{Z}[x]$ è semplificata dal criterio di Eisenstein e dalla proposizione 7.3.10.

Volendo ricercare le radici razionali di un polinomio $f \in \mathbb{Q}[x]$ possiamo quindi procedere come segue:

1. Sostituiamo il polinomio con un suo associato a coefficienti interi;
2. Si considera il coefficiente direttore a_n ed il termine noto a_0 del polinomio;
3. Le radici razionali del polinomio sono le frazioni della forma u/v con u e v interi coprimi tali che u divida a_0 e v divida a_n .

È chiaro che (escluso il caso, banalmente semplificabile, in cui $a_0 = 0$) esiste solo un numero finito di tali frazioni, possiamo allora verificare per ciascuna di esse se è o meno radice del polinomio.

Esempio 7.3.13

Consideriamo il polinomio $f = x^4 - 4x^2 + (3/2)x + 3 \in \mathbb{Q}[x]$. Un suo associato a coefficienti interi è:

$$2f = 2x^4 - 8x^2 + 3x + 6$$

con coefficiente direttore 2 e termine noto 6. Le frazioni della forma $\frac{u}{v}$ con u e v interi coprimi tali che u divida 6 e v divida 2 sono: $1 = \frac{1}{1}, \frac{1}{2}, 2, 3, \frac{3}{2}, 6$ e i loro opposti.

Per cercare tutte le radici razionali di f non dobbiamo fare altro che *controllare quali di questi dodici numeri sono radici di f in $\mathbb{Q}[x]$* . Nel nostro caso la verifica diretta mostra che solo -2 è radice. Concludiamo che -2 è l'unica radice in $\mathbb{Q}[x]$.

Possiamo proseguire lo studio di questo polinomio cercando di fattorizzarlo in prodotto di irriducibili. Usiamo il Teorema di Ruffini; dividendo f per $x + 2$ (cioè $(x - (-2))$) otteniamo:

$$f = (x + 2)(x^3 - 2x^2 + 3/2)$$

Il secondo fattore f_1 di questo prodotto è associato a $2f_1 = 2x^3 - 4x^2 + 3$. Sfruttando la proposizione 7.3.10 concluderemmo che le radici di f_1 sono da cercare tra le frazioni ridotte della forma u/v dove $u, v \in \mathbb{Z}$, u divide 3 e v divide 2.

In realtà non è necessario esaminare tutte queste frazioni perché ogni radice di f_1 è anche radice di f e di tutte queste frazioni, tranne -2 , sappiamo che non sono radici di f , quindi nemmeno di f_1 . Dobbiamo esaminare solo -2 , si ha:

$$f_1(-2) = (-2)^3 - 2(-2)^2 + 3/2 \neq 0$$

quindi -2 non è radice di f_1 . Pertanto f_1 non ha radici in \mathbb{Q} ; poiché $\deg(f_1) = 3$ concludiamo che f_1 è irriducibile in $\mathbb{Q}[x]$. Dunque una fattorizzazione (l'unica a meno dell'ordine) di f in prodotto di irriducibili monici in $\mathbb{Q}[x]$ è:

$$f = (x + 2)(x^3 - 2x^2 + 3/2)$$



Quando la cardinalità del campo finito F è piccola il metodo più efficace per la ricerca delle radici di un polinomio $f \in F[x]$ è spesso la verifica diretta eseguita per ogni elemento, vale a dire il calcolo di $f(c)$ per ogni elemento c del campo.



7.4.1 Aritmetica e congruenze

Esercizio 7.4.1

Determinare il più grande numero naturale $k < 100$ per cui ammette soluzione l'equazione diofantea $8x + 12y = k$ e risolverla.

Svolgimento. Sappiamo che una equazione diofantea è risolubile se il massimo comune divisore tra i due coefficienti delle incognite divide il termine noto.

In questo caso $MCD(8, 12) = 4$ e il più grande numero naturale, minore di 100 e multiplo di 4 è 96. L'equazione diofantea diventa quindi:

$$8x + 12y = 96$$

Per il Teorema di Bezout possiamo esprimere 4 come combinazione lineare di 8 e 12 e abbiamo:

$$4 = 8 \cdot -1 + 12 \cdot 1$$

Quindi la coppia $(-1, 1)$ è soluzione dell'equazione diofantea $8x + 12y = 4$. Essendo $96 = 4 \cdot 24$, moltiplicando la coppia $(-1, 1)$ per 24 si ottiene la coppia $(-24, 24)$ che è la soluzione ricercata. ■

Esercizio 7.4.2

Determinare l'insieme $X = \{n \in \mathbb{Z} / 16(1-n) \equiv_{36} 12n + a\}$ per almeno un $a \in \{6, 7, 8, 9\}$.

Svolgimento. Per come è stato definito l'insieme X possiamo dare una descrizione di tale insieme più estesa, ovvero:

$$\begin{aligned} X = \{n \in \mathbb{Z} / 16(1-n) \equiv_{36} 12n + 6\} \cup \{n \in \mathbb{Z} / 16(1-n) \equiv_{36} 12n + 7\} \\ \cup \{n \in \mathbb{Z} / 16(1-n) \equiv_{36} 12n + 8\} \\ \cup \{n \in \mathbb{Z} / 16(1-n) \equiv_{36} 12n + 9\} \end{aligned}$$

L'insieme X è costituito quindi dagli interi che sono soluzione delle quattro equazioni congruenziali. L'equazione congruenziale generica è:

$$16(1-n) \equiv_{36} 12n + a \quad (7.29)$$

con $a \in \{6, 7, 8, 9\}$. Risolvere l'equazione 7.29 significa ricercare i numeri interi tali che:

$$\begin{aligned} 36 \mid 16(1-n) - (12n + a) &\iff \exists k \in \mathbb{Z} (16(1-n) - (12n + a) = k \cdot 36) \\ &\iff \exists k \in \mathbb{Z} (16 - 16n - 12n - a = k \cdot 36) \\ &\iff \exists k \in \mathbb{Z} (16 - 28n - a = k \cdot 36) \\ &\iff \exists k \in \mathbb{Z} ((16 - a) - 28n = k \cdot 36) \end{aligned}$$

Svolgendo l'espressione algebrica

La ricerca delle soluzioni si riduce quindi alla risoluzione delle quattro equazioni congruenziali:

$$28n \equiv_{36} 16 - 6 \iff 28n \equiv_{36} 10 \quad (7.30)$$

$$28n \equiv_{36} 16 - 7 \iff 28n \equiv_{36} 9 \quad (7.31)$$

$$28n \equiv_{36} 16 - 8 \iff 28n \equiv_{36} 8 \quad (7.32)$$

$$28n \equiv_{36} 16 - 9 \iff 28n \equiv_{36} 7 \quad (7.33)$$

Procediamo quindi con la risoluzione della prima equazione. Il massimo comun divisore tra 28 e 36 è 4 e $4 \nmid 10$, quindi la prima soluzione non ammette soluzioni per $a = 6$. Analogamente per $a = 7$ e $a = 9$. Procediamo con l'equazione 7.32 in quanto $(28, 36) \mid 8$. Dividendo l'equazione per il massimo comune divisore si ottiene l'equazione congruenziale equivalente:

$$7n \equiv_9 2$$

Infatti sappiamo che le soluzioni di $28n \equiv_{36} 8$ sono tutte e sole quelle di $\frac{28}{4}n \equiv_{\frac{36}{4}} \frac{8}{4}$, ovvero $7n \equiv_9 2$, in quanto 4 risulta essere un divisore comune di 28, 36 e 8. Il vantaggio di tale semplificazione è dato dal fatto che $[7]_9$ è invertibile in \mathbb{Z}_9 in quanto $(7, 9) = 1$, ovvero 7 e 9 sono coprimi. Sfruttando il [Teorema di Bezout](#) possiamo quindi trovare un inverso di 7 in \mathbb{Z}_9 . Esistono infatti due interi u, v tali che: $1 = 7u + 9v$. Chiaramente $1 = 28 - 27 = 7 \cdot 4 - 9 \cdot 3$ e quindi $7 \cdot 4 - 1 = 9 \cdot (-3)$. Abbiamo così dimostrato che la coppia $(4, -3)$ è una soluzione dell'equazione diofantea $1 = 7u + 9v$. Moltiplicando per 2 si ottiene $2 = 7 \cdot 8 + 9 \cdot (-6) = 56 - 54$ e si ha: $7 \cdot 8 - 2 = 9 \cdot (-6)$, ovvero $9 \mid 7 \cdot 8 - 2$, cioè $7 \cdot 8 \equiv_9 2$. Quindi $n = 8$ è una soluzione dell'equazione $7n \equiv_9 2$, che è equivalente a dire che la classe di resto $[8]_9$ è una soluzione di tale equazione.

Concludiamo quindi dicendo che $X = \{n \in \mathbb{Z} / \exists k \in \mathbb{Z} (n = 9k + 8)\}$. ■

Esercizio 7.4.3

Verificare che l'insieme \mathbb{Z}_3 munito dell'operazione di addizione è un gruppo commutativo.

Svolgimento. Per dimostrare che $(\mathbb{Z}_3, +)$ sia un gruppo commutativo dobbiamo dimostra che $(\mathbb{Z}_3, +)$ risulta essere un monoide commutativo e che per ogni elemento di tale struttura esista l'opposto. Come sappiamo $(\mathbb{Z}_3, +)$ risulta essere una struttura algebrica definita dall'operazione indotta dalla relazione \equiv_3 nella struttura $(\mathbb{Z}, +)$. Dai risultati³ dimostrati per le congruenze sappiamo che $+_{\equiv_3}$ conserva l'associatività e la commutatività. Quindi $(\mathbb{Z}_3, +)$ è un semigruppo commutativo. Inoltre, preso $0 \in \mathbb{Z}$ elemento neutro in $(\mathbb{Z}, +)$ si ha che $[0]_3$ risulta essere l'elemento neutro in $(\mathbb{Z}_3, +)$ che risulta quindi un monoide commutativo. Se $-a \in \mathbb{Z}$ è l'opposto di $a \in \mathbb{Z}$ secondo l'operazione $+$ allora $[-a]_3 = [a]_3$ è l'opposto dell'elemento $[a]_3 \in \mathbb{Z}_3$ e $(\mathbb{Z}_3, +)$ è quindi un gruppo abeliano. ■

Esercizio 7.4.4

Si determinino le soluzioni della congruenza: $324x \equiv_{508} 127$.

Svolgimento. L'equazione $324x \equiv_{508} 127$ non ha soluzioni. Infatti, calcolato $MCD(324, 508) = 2$ si osserva che $2 \nmid 127$. ■

Esercizio 7.4.5

Si determinino le soluzioni della congruenza $3x \equiv_8 5$.

Svolgimento. Sappiamo che la congruenza ammette soluzioni intere poiché il massimo comun divisore tra 3 ed 8 è 1 che divide 5. Per determinare una soluzione scrivo 1 come combinazione lineare di tre ed otto, risolvo cioè l'equazione diofantea:

$$3x + 8y = 1$$

Chiaramente, dalla divisione euclidea abbiamo:

$$\begin{cases} 8 = 3 \cdot 2 + 2 \\ 3 = 2 \cdot 1 + 1 \end{cases} \implies \begin{cases} 2 = 8 - 3 \cdot 2 \\ 1 = 3 - 2 \end{cases}$$

Quindi:

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (8 - 3 \cdot 2) \\ &= 3 + 3 \cdot 2 - 8 \\ &= 3 \cdot 3 - 8 \\ &= 3 \cdot 3 + (-1) \cdot 8 \end{aligned}$$

Moltiplicando per 5 abbiamo che:

$$5 = 15 \cdot 3 + (-5) \cdot 8$$

e quindi $3 \cdot 15 \equiv_8 5$, ovvero ogni intero congruo a 15 (e cioè congruo a 7) modulo 8 è soluzione della congruenza. Dalla teoria sappiamo poi che l'insieme di tutte le soluzioni è costituito dagli interi congrui (modulo 8) a:

$$x_0 + t \cdot \frac{8}{(3, 8)} = 7 + 8t$$

al variare di $0 \leq t < (3, 8) = 1$. Pertanto solo per $t = 0$ si hanno soluzioni e queste sono dunque tutti e soli gli interi congrui a 7 modulo 8, ovvero la classe di resto $[7]_8$. ■

Esercizio 7.4.6

Trovare le soluzioni dell'equazione congruenziale $87x \equiv_{12} 27$.

Svolgimento. Applicando l'algoritmo euclideo delle divisioni successive abbiamo che:

$$\begin{aligned} 87 &= 7 \cdot 12 + 3 \\ 12 &= 4 \cdot 3 + 0 \end{aligned}$$

Pertanto $MCD(87, 12) = 3$ e $3 \mid 27$. Quindi la congruenza ammette tre soluzioni. Risolviamo l'equazione diofantea

$$87x + 12y = 27$$

³Vedi 7.1.6

Chiaramente $27 = 3 \cdot 9$, quindi:

$$\begin{aligned} 27 &= 9 \cdot 3 \\ &= 9 \cdot (87 - 7 \cdot 12) \\ &= 9 \cdot 87 - 63 \cdot 12 \\ &= 9 \cdot 87 + (-63) \cdot 12 \end{aligned}$$

Dunque 9 è soluzione e tale è anche ogni intero congruo a 9 modulo 12. Le altre eventuali soluzioni, modulo 12 sono date da:

$$9 + t \cdot \frac{12}{(87, 12)} = 9 + t \cdot 4$$

con $0 \leq t < 3$ e pertanto le soluzioni modulo 12 della congruenza di partenza sono:

$$\begin{cases} 9 + 0 \cdot 4 = 9 \implies [9]_{12} \\ 9 + 1 \cdot 4 = 13 \implies [13]_{12} = [1]_{12} \\ 9 + 2 \cdot 4 = 17 \implies [17]_{12} = [5]_{12} \end{cases}$$

Esercizio 7.4.7

Trovare le soluzioni dell'equazione congruenziale $87x + 32 \equiv_{100} x + 4$.

Svolgimento. Affermare che $87x + 32 \equiv_{100} x + 4$ è equivalente a dire:

$$\begin{aligned} 100 \mid 87x + 32 - (x + 4) &\iff 100 \mid 87x + 32 - x - 4 \\ &\iff 100 \mid 86x + 28 \\ &\iff 100 \mid 86x - (-28) \\ &\iff 86x \equiv_{100} -28 \end{aligned}$$

Calcolando il massimo comune divisore tra 86 e 100 troviamo $(86, 100) = 2$ e $2 \mid -28$. Dividendo tutti i termini per 2 otteniamo l'equazione congruenziale equivalente:

$$43x \equiv_{50} -14$$

dove $MCD(43, 50) = 1$. Per il [Teorema di Bezout](#) esistono due interi relativi tali che:

$$43u + 50v = 1$$

e vale $43 \cdot 7 + 50 \cdot (-6) = 301 - 300 = 1$, quindi la coppia $(7, -6)$ è soluzione di tale equazione diofantea. Moltiplicando tutto per -14 si ottiene la coppia $(-98, 84)$ ovvero:

$$\begin{aligned} 43 \cdot (-98) + 50 \cdot 84 = -14 &\iff 43 \cdot (-98) + 14 = -50 \cdot 84 \\ &\iff 43 \cdot (-98) - (-14) = 50 \cdot (-84) \\ &\iff 50 \mid 43 \cdot (-98) - (-14) \\ &\iff 43 \cdot (-98) \equiv_{50} -14 \end{aligned}$$

Quindi $x = -98$ è la soluzione cercata, ovvero tutti gli interi appartenenti alla classe di resto $[98]_{100} = [48]_{50}$.

Esercizio 7.4.8

Determinare le soluzioni delle congruenze:

1. $7x \equiv_{24} 28$;
2. $7x \equiv_{24} 27$;
3. $8x \equiv_{28} 8$.

Svolgimento.

1. Dato che $MCD(7, 24) = 1$ e $1 \mid 28$ abbiamo che l'equazione è compatibile e ammette un'unica soluzione. Applichiamo il [Teorema di Bezout](#) che afferma che esistono due interi relativi u, v tali che:

$$7u + 24v = 1$$

Chiaramente $49 - 48 = 7 \cdot 7 + 24(-2) = 1$ ottenendo così la coppia $(7, -2)$. Moltiplicando tutto per 28 si ottiene la coppia $(196, -56)$ che soddisfa l'equazione diofantea:

$$7 \cdot 196 + 24(-56) = 28$$

Il che è equivalente a dire che:

$$7 \cdot 196 - 28 = 24 \cdot 56 \iff 24 \mid 7 \cdot 196 - 28 \iff 7 \cdot 196 \equiv_{24} 28$$

Trovando così $x = 196$.

2. In maniera del tutto analoga all'esercizio precedente abbiamo che la coppia $(7, -2)$ è soluzione dell'equazione diofantea $7u + 24v = 1$. Moltiplicando per 27 otteniamo la coppia $(189, -54)$. Quindi $x = 189$ è soluzione dell'equazione congruenziale.
3. In questo caso abbiamo che il massimo comune divisore tra 8 e 28 è 4 e 4 divide 8. Risolviamo l'equazione diofantea:

$$\begin{aligned} 8u + 28v = 4 &\iff \frac{8}{2}u + \frac{28}{2}v = \frac{4}{2} \\ &\iff 4u + 14v = 2 \end{aligned}$$

Chiaramente $4 \cdot 4 + 14 \cdot (-1) = 16 - 14 = 2$ e la coppia $(4, -1)$ è soluzione dell'equazione $8u + 28v = 4$. Moltiplicando per due otteniamo la coppia $(8, -2)$ e si ha che $x = 8$ è una prima soluzione dell'equazione. Abbiamo quindi che le soluzioni sono esprimibili mediante la relazione:

$$8 + t \frac{28}{4} = 8 + t \cdot 7$$

Con $0 \leq t < 4$, ovvero:

$$\begin{cases} 8 + 0 = [8]_{28} \\ 8 + 7 = [15]_{28} \\ 8 + 14 = [22]_{28} \\ 8 + 21 = [29]_{28} \end{cases}$$

Notiamo inoltre che riducendo l'equazione congruenziale all'equazione equivalente $2x \equiv_7 1$ ottenuta dividendo ciascun termine per 4, le quattro classi di resto ottenute si riducono alla singola soluzione $[1]_7$. ■

Esercizio 7.4.9

È vero che ogni soluzione intera della congruenza $14x \equiv_{24} 2$ è anche soluzione dell'equazione $7x \equiv_{12} 1$? È vero il viceversa? Spiegare bene. Determinare tutte le soluzioni intere della congruenza $14x \equiv_{24} 0$.

Esercizio 7.4.10

Dire quali delle seguenti congruenze sono equivalenti fra loro (spiegare bene la risposta):

- $15x \equiv_4 6$
- $15x \equiv_4 10$
- $19x \equiv_4 10$
- $5x \equiv_4 2$

Esercizio 7.4.11

Usando l'algoritmo euclideo esteso, trovare tutte le soluzioni delle equazioni diofantee:

1. $14x + 6y = 1$
2. $15x + 6y = 4$
3. $140x + 60y = 20$

Esercizio 7.4.12

In \mathbb{Z}_{48} si determini, ove possibile, l'inverso di: $[7]_{48}, [9]_{48}, [11]_{48}, [-13]_{48}, [47]_{48}$. Capire perché c'è davvero bisogno di far calcoli in una sola occasione.

Esercizio 7.4.13

Si determinino tutti gli interi u tali che $20(u - 1) \equiv_{28} 4(u - 2)$ e gli interi v tali che $20(v - 1) \equiv_{28} 4v - 2$.

Esercizio 7.4.14

Sia $(M, *)$ un monoide commutativo. Provare che la relazione “essere elementi associati” in M è compatibile con $*$.

Esercizio 7.4.15

Assegnato un arbitrario insieme a , nel monoide $(\mathcal{P}(a), \cap, a)$ descrivere gli elementi associati ad un arbitrario elemento x .

Esercizio 7.4.16

Quali sono gli elementi irriducibili nel monoide $(\mathbb{N}, +, 0)$? $(\mathbb{N}, +, 0)$ è un monoide fattoriale?

Esercizio 7.4.17

Assegnato un insieme finito S , quali sono gli elementi irriducibili in $(\mathcal{P}(S), \cup, \emptyset)$? $(\mathcal{P}(S), \cup, \emptyset)$ è un monoide fattoriale?

Esercizio 7.4.18

Utilizzando l'algoritmo euclideo trovare in \mathbb{Z} un MDC d tra 125 e 57 e poi scrivere d come combinazione lineare tra questi due numeri. Ripetere l'esercizio partendo da 125 e 55 (e, volendo, farlo ancora, usando altre coppie di numeri interi scelti a caso).

Esercizio 7.4.19

Nel granducato di Strampalia non circolano monete e la valuta locale, il tallero strampalese, viene emesso solo in due tagli: la banconota da 15 talleri e quella da 33 talleri. Usando il teorema di Bézout, spiegare quali pagamenti in talleri strampalesi possono essere effettuati in contanti (è ammessa la possibilità di pagare ricevendo un resto).

7.4.2 ■ Polinomi

! Negli esercizi che seguono, per ogni intero a il simbolo \bar{a} rappresenta le classi di resto di a nel modulo indicato dal contesto. Saranno quindi equivalenti le scritture $[a]_n$ e \bar{a} .

Esercizio 7.4.20

Fattorizzare in $\mathbb{Q}[x]$ il polinomio: $f(x) = x^6 - 5x^5 + 8x^4 - x^3 - 15x^2 + 24x - 12$.

Svolgimento. Dato che i divisori del termine noto sono 1,2,3,4,6,12 e l'unico divisore del termine di testa è 1, le possibili radici razionali di $f(x)$ sono:

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$$

Iniziamo a testare e calcoliamo:

$$f(1) = 1 - 5 + 8 - 1 - 15 + 24 - 12 = 0$$

Quindi $x - 1$ è un fattore di $f(x)$ pertanto si divide $f(x)$ per $x - 1$ e si ottiene:

$$\begin{array}{r} x^6 - 5x^5 + 8x^4 - x^3 - 15x^2 + 24x - 12 \\ - x^6 + x^5 \\ \hline - 4x^5 + 8x^4 \\ 4x^5 - 4x^4 \\ \hline 4x^4 - x^3 \\ - 4x^4 + 4x^3 \\ \hline 3x^3 - 15x^2 \\ - 3x^3 + 3x^2 \\ \hline - 12x^2 + 24x \\ 12x^2 - 12x \\ \hline 12x - 12 \\ - 12x + 12 \\ \hline 0 \end{array} = (x - 1)(x^5 - 4x^4 + 4x^3 + 3x^2 - 12x + 12)$$

Quindi:

$$x^6 - 5x^5 + 8x^4 - x^3 - 15x^2 + 24x - 12 = (x^5 - 4x^4 + 4x^3 + 3x^2 - 12x + 12)(x - 1)$$

Ripartiamo cercando di fattorizzare:

$$g(x) = x^5 - 4x^4 + 4x^3 + 3x^2 - 12x + 12$$

Dato che il termine noto e quello di testa non sono cambiati, dobbiamo testare tutte le candidate radici. Notiamo che:

$$\begin{aligned} g(1) &\neq 0 \\ g(-1) &\neq 0 \\ g(2) &= 32 - 4 \cdot 16 + 4 \cdot 8 + 3 \cdot 4 - 12 \cdot 2 = 0 \end{aligned}$$

Quindi $x - 2$ è un fattore di $g(x)$. Eseguendo la divisione otteniamo:

$$\begin{array}{r}
 x^5 - 4x^4 + 4x^3 + 3x^2 - 12x + 12 = (x-2)(x^4 - 2x^3 + 3x - 6) \\
 \underline{-x^5 + 2x^4} \\
 \hline
 -2x^4 + 4x^3 \\
 \underline{2x^4 - 4x^3} \\
 \hline
 3x^2 - 12x \\
 \underline{-3x^2 + 6x} \\
 \hline
 -6x + 12 \\
 \underline{6x - 12} \\
 \hline
 0
 \end{array}$$

Quindi:

$$\begin{aligned}
 x^6 - 5x^5 + 8x^4 - x^3 - 15x^2 + 24x - 12 &= (x^5 - 4x^4 + 4x^3 + 3x^2 - 12x + 12)(x-1) \\
 &= (x^4 - 2x^3 + 3x - 6)(x-2)(x-1)
 \end{aligned}$$

Poniamo $h(x) = x^4 - 2x^3 + 3x - 6$ e cerchiamo di fattorizzarlo. Il termine noto è cambiato, adesso è 6, quindi possiamo evitare le radici candidate ± 12 . Possiamo evitare anche le candidate radici ± 1 che, non essendo radici di $g(x)$, non possono esserlo di $h(x)$. Dobbiamo testare tutte le altre radici candidate. Notiamo che, nuovamente $h(2) = 0$, quindi $x-2$ è un fattore di $h(x)$ ed essendo anche un fattore di $g(x)$ e $f(x)$ ha molteplicità almeno 2. Dividiamo $h(x)$ per $x-2$:

$$\begin{array}{r}
 x^4 - 2x^3 + 3x - 6 = (x-2)(x^3 + 3) \\
 \underline{-x^4 + 2x^3} \\
 \hline
 3x - 6 \\
 \underline{-3x + 6} \\
 \hline
 0
 \end{array}$$

ottenendo:

$$\begin{aligned}
 x^6 - 5x^5 + 8x^4 - x^3 - 15x^2 + 24x - 12 &= (x^5 - 4x^4 + 4x^3 + 3x^2 - 12x + 12)(x-1) \\
 &= (x^4 - 2x^3 + 3x - 6)(x-2)(x-1) \\
 &= (x^3 + 3)(x-2)(x-2)(x-1)
 \end{aligned}$$

Chiaramente $x^3 + 3$ è possibile scriverlo come $x^3 - (-3)$ che risulta essere irriducibile su \mathbb{Q} . Otteniamo così la fattorizzazione:

$$f(x) = (x^3 + 3)(x-2)^2(x-1)$$

Esercizio 7.4.21

Sia $f(x) = 2x^5 - 15x^4 + 6x^3 - 3x + 12$. Dire se $f(x)$ è irriducibile su \mathbb{Q} .

Svolgimento. Chiaramente preso $p = 3$ abbiamo che:

- 3 divide 12,3,6 e -15;
- 3 non divide 2;
- 3^2 non divide 12.

Quindi, applicando il Criterio di Eisenstein, si ha che $f(x)$ è irriducibile su \mathbb{Q} per $p = 3$.

Esercizio 7.4.22

Scrivere tutti i polinomi monici irriducibili di secondo grado di $\mathbb{Z}_3[x]$.

Svolgimento. Un polinomio monico di secondo grado è della forma:

$$x^2 + ax + b$$

Poiché $f(x)$ è di secondo grado, dalla Tabella 7.1 si ha che $f(x)$ è irriducibile se e solo se non ha radici in \mathbb{Z}_3 , quindi si ha:

$$\begin{cases} b \not\equiv_3 0 \\ 1 + a + b \not\equiv_3 0 \\ 1 + 2a + b \not\equiv_3 0 \end{cases}$$

Dunque $b \equiv_3 1$ o $b \equiv_3 2$. Se $b \equiv_3 1$ si ha, per la seconda relazione, $a + 2 \not\equiv_3 0$ e quindi $a \not\equiv_3 1$. D'altra parte, per la terza relazione, si ha $2a + 2 \not\equiv_3 0$ e quindi $a \not\equiv_3 2$. In conclusione, se $b \equiv_3 1$ deve essere $a \equiv_3 0$. Se $b \equiv_3 2$ si ha $a \not\equiv_3 0$ per la seconda relazione e $2a \not\equiv_3 0$ per la terza relazione. Dunque $a \equiv_3 0$ oppure $a \equiv_3 2$. I polinomi monici irriducibili di secondo grado di \mathbb{Z}_3 sono quindi:

$$x^2 + 1, \quad x^2 + x + 2, \quad x^2 + 2x + 2$$

Esercizio 7.4.23

Si dica se il polinomio $f(x) = x^3 + 6x^2 + 7$ è irriducibile su \mathbb{Q} , su \mathbb{R} e su \mathbb{Z}_3 .

Svolgimento. Tutti i polinomi a coefficienti reali di grado superiore a 3 sono riducibili in \mathbb{R} quindi possiamo dire con certezza che $f(x)$ non è irriducibile su \mathbb{R} . $f(x)$ è irriducibile su \mathbb{Q} non avendo radici razionali (ed essendo di grado 3) : infatti le radici razionali del polinomio sono le frazioni della forma u/v con u e v interi coprimi tali che u divida a_0 e v divida a_n , ovvero $\frac{7}{1} = 7$ e $f(7) \neq 0$. $f(x)$ è riducibile in \mathbb{Z}_3 in quanto $f(\bar{2}) = \bar{0}$. ■

Esercizio 7.4.24

È possibile che due polinomi distinti $f(x)$ e $g(x)$ a coefficienti in \mathbb{Q} , monici ed irriducibili abbiano una radice comune?

Svolgimento. Sia α la radice comune di $f(x)$ e $g(x)$. Poiché $f(x)$ è monico e irriducibile coincide necessariamente con il polinomio $x - \alpha$. Allo stesso modo $g(x)$ e quindi $f(x) = g(x)$. ■

Esercizio 7.4.25

Si consideri l'anello dei polinomi a coefficienti in \mathbb{Z}_{22} :

1. Cosa significa essere associato ad un polinomio $f \in \mathbb{Z}_{22}[x]$?
2. Sia $S = \{g \in \mathbb{Z}_{22}[x] \mid \exists u \in \mathcal{U}(\mathbb{Z}_{22}[x])(g = fu)\}$, ovvero l'insieme dei polinomi associati ad f in $\mathbb{Z}_{22}[x]$. Determinare per quali $f \in \mathbb{Z}_{22}[x]$ l'insieme $(S, +) \leq (\mathbb{Z}_{22}[x], +)$.

Esercizio 7.4.26

Indicare il numero di divisori monici in $\mathbb{Z}_7[x]$ che possiede il polinomio:

$$f = x^3 - x^2 + \bar{4}x + \bar{3} \in \mathbb{Z}_7[x]$$

Quanti divisori (monici e non) sono irriducibili?

Esercizio 7.4.27

Sia $S = \{f \in \mathbb{Z}_5[x] \mid \deg(f) = 4 \wedge (f(\bar{1}) = \bar{0})\}$. Quanti elementi possiede S ? S è una parte chiusa di $(\mathbb{Z}_5, +)$?

Esercizio 7.4.28

Verificare che l'insieme dei polinomi $\mathbb{Z}[x]$ forma un gruppo rispetto all'ordinaria operazione di addizione di polinomi. Non formano invece un gruppo rispetto all'ordinaria operazione di moltiplicazione di polinomi.

Esercizio 7.4.29

Si costruisca, se possibile, un polinomio di grado 300 in $\mathbb{Q}[x]$ le cui radici in \mathbb{Q} siano tutti e soli gli interi n tali che $-100 \leq n \leq 100$.

Esercizio 7.4.30

Per ogni primo positivo p , sia f_p il polinomio $\bar{3}x^4 + \bar{2}x^3 + \bar{2}x^2 + x + \bar{2} \in \mathbb{Z}_p[x]$. Determinare:

1. I primi positivi p tali che f_p abbia $\bar{1}$ come radice;
2. I primi positivi p tali che f_p sia divisibile per $x - \bar{1}$.

Esercizio 7.4.31

Decidere quanti sono i polinomi monici di grado 6 in $\mathbb{Z}_{11}[x]$ che abbiano (almeno) $\bar{1}$ e $\bar{2}$ come radici.

Esercizio 7.4.32

In \mathbb{Z}_3 , e con riferimento a polinomi in $\mathbb{Z}_3[x]$:

1. Trovare tutte le radici del polinomio $x^2 - x + \bar{1} \in \mathbb{Z}_3[x]$,
2. Quelle del polinomio $x^{50} + x^{35} + \bar{1}$
3. Quelle del polinomio $(x + \bar{1})^5((x - \bar{1})^7 + \bar{1})$

Esercizio 7.4.33

Determinare il massimo comun divisore monico in $\mathbb{Q}[x]$ per ciascuna delle seguenti coppie di polinomi:

1. $x^{10} + 1$ e $x^7 + 1$;
2. $x^{10} - 1$ e $x^7 - 1$;
3. $x^4 - x - 2$ e $3x^2 + 6x^2 - 3$;
4. $2x^4 + 3x^3 - 2x - 3$ e $2x^6 + 3x^5 + 2x^3 + 3x^2 - 2x - 3$;

Esercizio 7.4.34

Determinare, se esistono, polinomi u e v in $\mathbb{Q}[x]$ tali che:

1. $(x^{10} + 1)u + (x^7 + 1)v = 1$
2. $(x^{10} + 1)u + (x^7 + 1)v = x$
3. $(x^{10} - 1)u + (x^7 - 1)v = 1$
4. $(x^{10} - 1)u + (x^7 - 1)v = 2x - 2$
5. $(x^5 + 2)u + (x^4 - 1)v = 3$

Esercizio 7.4.35

Determinare tutte le radici in \mathbb{Z}_{12} del polinomio $x^2 - 1 \in \mathbb{Z}_{12}[x]$. Se il loro numero non sembra sorprendente o si è studiato troppo poco oppure piuttosto bene. Rifletterci sopra.

ELEMENTI DI TEORIA DEI GRAFI

8.1

GRAFI E MULTIGRAFI



Definizione 8.1.1: Grafo

Si dice **grafo non orientato** una coppia $G = (V, R)$ dove V è un insieme non vuoto ed R è una relazione binaria su V che gode delle proprietà:

- Antiriflessiva: $\forall u \in V ((u, u) \notin R^\#)$
- Simmetrica: $\forall u, v \in V ((u, v) \in R^\# \implies (v, u) \in R^\#)$

Dove $R^\#$ è il grafico della relazione R . Gli elementi di V sono detti **vertici** del grafo; due vertici u, v tali che $(u, v) \in R^\#$ determinano un **lato** o **arco** di G che denotiamo con $\{u, v\}$. Un grafo si può rappresentare in modo del tutto equivalente come una struttura (V, L) dove L è l'insieme dei lati:

$$L = \{\{x, y\} \in \mathcal{P}(V) \mid (x, y) \in R^\#\} \subseteq \mathcal{P}_2(V) \quad (8.1)$$

Esempio 8.1.1

Consideriamo il grafo $G = (V, L)$ con cinque vertici v_1, v_2, v_3, v_4, v_5 e quattro lati:

$$l_1 = \{v_1, v_2\}, \quad l_2 = \{v_2, v_3\}, \quad l_3 = \{v_3, v_4\}, \quad l_4 = \{v_2, v_4\}$$

Allora G ha la seguente rappresentazione:

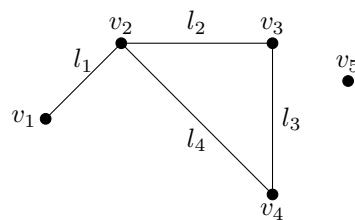


Figura 8.1: Esempio di grafo non orientato

Definizione 8.1.2: Adiacenza

Due vertici $u, u' \in V$ si dicono **adiacenti** se $\{u, u'\} \in L$. Diremo allora che il lato $l = \{u, u'\}$ **collega** u e u' .

Osservazione 8.1.1



Possiamo dunque intendere un grafo come una sorta di carta geografica in cui i vertici rappresentano i centri abitati e i lati le strade che li congiungono. La proprietà antiriflessiva ci dice che non ci sono strade che, partendo da un paese, vi ritornano senza tappe intermedie; la proprietà simmetrica che ogni strada si percorre a doppio senso.

Se aboliamo le proprietà antiriflessiva e simmetrica, e quindi ammettiamo che esistano strade che partono e arrivano allo stesso vertice, e che ogni strada tra due vertici sia a senso unico, otteniamo il concetto di **grafo orientato** (o **grafo diretto**, o **disgrafo**).

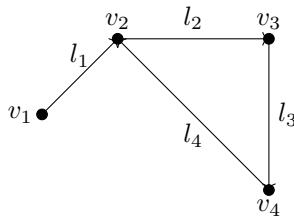


Figura 8.2: Esempio di grafo orientato

Definizione 8.1.3: Incidenza

Due lati $l, l' \in L$ si dicono **incidenti** nel vertice v o **consecutivi** se $\{v\} = l \cap l'$, cioè se v è l'unico estremo comune di l ed l' .

Esempio 8.1.2

Osservando il grado in Figura 8.1 abbiamo che i lati l_1 e l_2 sono incidenti in v_2 .

Definizione 8.1.4: Vertici isolati

Un vertice si dice **isolato** se non ci sono lati di L incidenti in v .

Esempio 8.1.3

Il vertice v_5 del grafo in Figura 8.1 è isolato.

Definizione 8.1.5: Grafo finito

Un grafo si dice **finito** se tale è l'insieme V dei suoi vertici.

Esempio 8.1.4

Il grafo in Figura 8.1 è finito.

Definizione 8.1.6: Grado

Il **grado** di un vertice v è il numero di lati incidenti in v . Lo indichiamo con $\deg(v)$. Un vertice isolato ha grado zero. Un vertice $v \in V$ si dice **pari** o **dispari** a seconda che $\deg(v)$ sia pari o dispari. Un grafo avente tutti i vertici dello stesso grado d si dice **regolare** di grado d .

Esempio 8.1.5

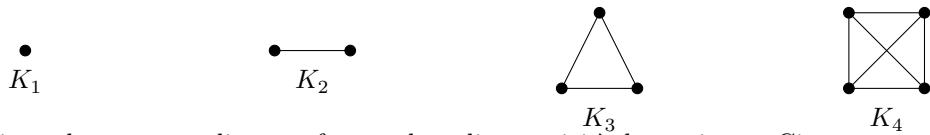
Nel grafo in Figura 8.1 il vertice v_2 ha grado 3 e si scriverà $\deg(v_2) = 3$ e risulta essere un vertice dispari.

Definizione 8.1.7: Grafo completo

Il grafo $G = (V, L)$ si dice **completo** se tutti i suoi vertici sono a due a due adiacenti, cioè, se per ogni scelta di $u, v \in V$ con $u \neq v$ $\{u, v\} \in L$.

Esempio 8.1.6

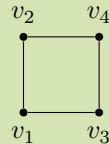
Proponiamo alcuni esempi di grafi completi, rispettivamente con 1, 2, 3, 4 vertici. Li denotiamo, nell'ordine, K_1 , K_2 , K_3 , K_4 .



Per ogni intero positivo n la struttura di un grafo completo di n vertici è determinata. Ci sono appunto n vertici e ogni coppia di vertici distinti è collegata da un lato. In genere, per ogni intero positivo n , l'“unico” grafo completo con n vertici è indicato con K_n . Si noti poi, che ogni grafo G è sottografo di un opportuno grafo completo.

Osservazione 8.1.2 ➤➤➤

Ovviamente ogni grafo completo risulta un grafo regolare ma non vale il viceversa. Si consideri il seguente grafo regolare di grado 2:



Chiaramente non è completo in quanto non esiste un lato che collega v_2 e v_3 e v_1 con v_4 .

Proposizione 8.1.1

Un grafo $G = (V, L)$ è completo se, e solo se, $L = \mathcal{P}_2(V)$. Ovvero se per ogni intero positivo n , il grafo K_n ha esattamente:

$$|\mathcal{P}_2(V)| = \binom{n}{2} = \frac{n(n-1)}{2}$$

lati.

Dimostrazione. \implies Se $G = (V, L)$ è un grafo completo allora tutti i vertici sono in relazione R tra di loro, ciò significa che R è totale e che per ogni $u, v \in V$ esiste un lato $l = \{u, v\} \in L$. Si ha allora $L = \mathcal{P}_2(V)$ e vale:

$$\begin{aligned} |L| &= |\mathcal{P}_2(V)| = \binom{n}{2} \\ &= \frac{n!}{2 \cdot (n-2)!} \\ &= \frac{n(n-1)!}{2 \cdot (n-2)(n-3)!} \\ &= \frac{n(n-1)(n-2) \dots 1}{2(n-2)(n-2)(n-4) \dots 1} \\ &= \frac{n(n-1)}{2} \end{aligned}$$

\Leftarrow Ovvio per le osservazioni fatte in precedenza. □

Corollario 8.1.1

Un grafo $G = (V, L)$ con n vertici ha al più $\binom{n}{2}$ lati, che risulta essere un *limite superiore* al numero possibile di vertici in un grafo finito.

Definizione 8.1.8: Grafo planare

Un grafo $G = (V, L)$ si dice **planare** se può essere rappresentato senza che i lati si intersechino tra loro.

Esempio 8.1.7

Si ha che il grafo mostrato a sinistra è planare mentre quello a destra non lo è:



8.1.1 ■ Isomorfismi tra grafi

Definizione 8.1.9: Isomorfismo

Due grafi $G_1 = (V_1, L_1)$, $G_2 = (V_2, L_2)$ si dicono **isomorfi** se esiste una biiezione $f : V_1 \rightarrow V_2$ tale che, per ogni scelta di $u, v \in V_1$ si ha:

$$\{u, v\} \in L_1 \iff \{f(u), f(v)\} \in L_2$$

ed f si dice **isomorfismo** di G_1 su G_2 .

Osservazione 8.1.3



Chiaramente, se un diagramma rappresenta un grafo G , lo stesso diagramma rappresenta ogni grafo isomorfo a G .

Definizione 8.1.10: Sottografo

Se $G = (V, L)$ è un grafo, V' è un sottoinsieme di V ed L' è un sottoinsieme di L tale che per ogni lato $l = \{u, v\} \in L'$ i suoi estremi u, v stanno in V' , allora $G' = (V', L')$ è un grafo, detto **sottografo** di G .

8.1.2 ■ Multigrafi

Definizione 8.1.11: Multigrafo

Un **multigrafo semplice** è una terna (V, L, φ) in cui:

- V è un insieme non vuoto di vertici;
- L è un insieme di lati;
- φ è una funzione da L in $\mathcal{P}_2(V)$ detta **funzione di incidenza**.

Osservazione 8.1.4

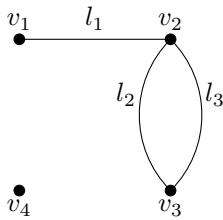


I grafi non sono altro che multigrafi in cui φ risulta iniettiva.

Infatti rispetto alla nozione di grafo, abbiamo l'ovvia complicazione tecnica che due vertici distinti u e v possono essere collegati da più di un lato; la notazione $\{u, v\}$ non basta allora a identificare tutti i lati tra u e v , e si deve ricorrere alla funzione di incidenza φ per chiarire la situazione. Infatti l'applicazione φ associa ad ogni lato $l \in L$ l'insieme $\{u, v\}$ dei suoi estremi. In un multigrafo non si richiede che φ sia iniettiva, e quindi φ può associare la stessa coppia di estremi a più lati distinti: si parla allora di lati **multipli** tra gli stessi estremi.

Esempio 8.1.8

Si consideri il multigrafo $G = (V, L, \varphi)$ dove $V = \{v_1, v_2, v_3, v_4\}$, $L = \{l_1, l_2, l_3\}$, $\varphi(l_1) = \{v_1, v_2\}$, $\varphi(l_2) = \varphi(l_3) = \{v_2, v_3\}$. I lati multipli sono l_2 ed l_3 . Si ha quindi la seguente rappresentazione grafica:



Osservazione 8.1.5

La nozione di isomorfismo ha il suo opportuno adattamento tra i multigrafi. Due multigrafi $G_1 = (V_1, L_1, \varphi)$ e $G_2 = (V_2, L_2, \psi)$ si dicono **isomorfi** se esistono due biezioni: $f : V_1 \rightarrow V_2$ e $g : V_2 \rightarrow V_1$ tali che, per ogni scelta di $l \in L_1$ e $u, v \in V_1$ si ha:

$$\varphi(l) = \{u, v\} \iff \psi(g(l)) = \{f(u), f(v)\}$$

Teorema 8.1.1

Sia $G = (V, L, \varphi)$ un multigrafo finito. Allora:

$$\sum_{v \in V} \deg(v) = 2|L|$$

Dimostrazione. Sia $S = \{(v, l) \in V \times L \mid v \text{ è un estremo di } l\}$. Rappresentiamo S mediante una tabella in cui poniamo delle crocette se, e solo se, v_i è un estremo di l_j :

	l_1	l_2	l_3	\dots	l_r
v_1	×			×	
v_2		×			
v_3	×		×		×
\vdots			×	×	
v_r		×			×

Dato che ogni lato ha sempre due estremi, ogni colonna avrà sempre due crocette. Quindi per ogni lato del multigrafo corrispondono due elementi dell'insieme S : $|S| = 2L$. Analogamente, contando per righe, il numero di crocette presente su ogni riga denoterà il numero di lati incidenti sul vertice corrispondente alla riga, ovvero il grado del vertice. Quindi possiamo dire con certezza che $S = \sum_{v \in V} \deg(v)$ concludendo così la dimostrazione. \square

Osservazione 8.1.6

Come conseguenza del teorema, i vertici pari di un multigrafo possono essere di un numero arbitrario mentre quelli dispari devono essere in numero pari. Infatti, denotato con V_p e V_d gli insiemi dei vertici pari e dispari di V si ha:

$$\sum_{v \in V} \deg(v) = \sum_{v \in V_p} \deg(v) + \sum_{v \in V_d} \deg(v)$$

Ovviamente, $\sum_{v \in V_p} \deg(v)$ è pari, pertanto anche $\sum_{v \in V_d} \deg(v) = \sum_{v \in V} \deg(v) - \sum_{v \in V_p} \deg(v)$ è un numero pari, perché differenza di numeri pari. Ma $\sum_{v \in V_d} \deg(v)$ è la somma di addendi dispari, e dunque è pari se e solo se il numero dei suoi addendi, e cioè dei vertici dispari, è pari.

**Definizione 8.2.1: Cammino**

Siano $G = (V, L)$ un grafo, $u, w \in V$. Si dice **cammino** di G tra u e w una sequenza finita $\alpha = (l_1, l_2, \dots, l_m)$ di lati di L a due a due distinti tali che, per ogni $i < m$, l_{i+1} è consecutivo ad l_i . Se un cammino passa per tutti i lati del grafo allora verrà chiamato **cammino euleriano**.

Definizione 8.2.2: Circuito

Un **circuito** o **ciclo** è un cammino da un vertice a se stesso. Se un cammino passa per ogni lato di un multigrafo una ed una sola volta allora viene chiamato **circuito euleriano**. Un grafo che contiene un ciclo è detto **ciclico**.

Definizione 8.2.3: Grafo connesso

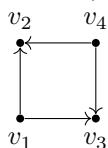
Un grafo $G = (V, L)$ si dice **connesso** se per ogni coppia di vertici distinti $u, v \in V$ esiste un cammino tra u e v .

Teorema 8.2.1 (di Eulero)

Sia G un multigrafo finito senza vertici isolati. Allora G ha un circuito euleriano se e solo se G è connesso e tutti i suoi vertici sono pari.

Esempio 8.2.1

Si osservi il seguente grafo orientato finito, senza vertici isolati, in cui ogni vertice ha grado pari:



È evidente che tale grafo non è connesso in quanto non esiste un cammino tra i vertici v_1 e v_4 . Di conseguenza si può osservare che non esiste un circuito euleriano per nessuno dei quattro vertici.

Corollario 8.2.1

Sia G un multigrafo finito privo di vertici isolati. Il multigrafo G ha un cammino euleriano se e solo se è connesso ha zero o due vertici dispari.

Osservazione 8.2.1

La relazione di connessione, o di *raggiungibilità*, è una relazione di equivalenza in quanto risulta essere riflessiva, simmetrica e transitiva. Per questo motivo possiamo considerare l'insieme quoziante di V rispetto a tale equivalenza. Gli elementi di tale quoziante vengono chiamati **componenti connesse** e sono formati da vertici connessi e dai lati che formano i cammini che li connettono.

**Definizione 8.3.1: Foresta ed alberi**

Chiamiamo **foresta** un grafo senza circuiti (**grafo aciclico**), e **albero** un grafo connesso senza circuiti (**grafo aciclico connesso**).

Il collegamento tra i due nomi (alberi e foreste) è chiaro: infatti, la assenza di circuiti si trasmette ovviamente ai sottografi, ed è dunque facile osservare che le componenti connesse di una foresta sono, appunto, alberi.

Teorema 8.3.1

Un grafo finito $G = (V, L)$ è una foresta se, e solo se, per ogni coppia di vertici (a, b) con $a \neq b$ esiste al più un cammino.

Un grafo finito è un albero se, per tale coppia esiste esattamente un cammino.

Dimostrazione. Siano $a, b \in V$. Siccome G è connesso, c'è almeno un cammino tra a e b . Ammettiamo che ce ne siano due, α e α' rispettivamente. Se α e α' non hanno lati comuni, il cammino che segue α da a a b e poi da b ad a lungo α' è un circuito di G e questo è assurdo. Anche nel caso in cui α e α' abbiano un lato in comune si costruisce un circuito in G e si cade dunque in contraddizione. Quindi esiste un unico cammino lungo tale grafo connesso che risulta quindi essere un albero. \square

8.3.1 ■ Rappresentazione radiale di un albero

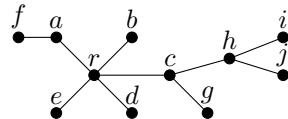
È possibile rappresentare un albero $G = (V, L)$ selezionandone un vertice, che chiameremo **radice** e disponendo poi gli altri punti di V nelle ramificazioni che si dipartono dalla radice. Tale rappresentazione prende il nome di **rappresentazione radiale** di G .

Osservazione 8.3.1

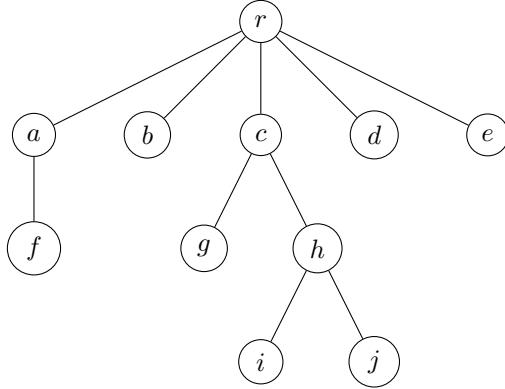
Una foresta finita è necessariamente un grafo planare.

Esempio 8.3.1

Si consideri la seguente rappresentazione generica del grafo G :



Selezionato il vertice r come radice dell'albero, si ottiene la seguente rappresentazione radiale:



Definizione 8.3.2: Foglia

Se un albero ha almeno due vertici in rappresentazione radiale, chiameremo **foglie** i vertici a distanza massima dalla radice. Tali vertici avranno grado pari ad uno in quanto esiste un solo lato incidente su tali vertici, ovvero il lato proveniente dal vertice "padre".

Lemma 8.3.1

Sia $T = (V, L)$ un albero e sia $v \in V$ tale che $\deg(v) = 1$. Si ha che v è una foglia. Sia $l \in L$ tale che v è un estremo di l . Allora $T' = (V \setminus \{v\}, L \setminus \{l\})$ è ancora un albero.

Dimostrazione. Per ogni $a, b \in T'$ si ha sicuramente che $a \neq v$ e $b \neq v$ e quindi il cammino tra a e b non è l perché ogni vertice che non sia un estremo di un cammino ha sempre grado maggiore o uguale a due. \square

Proposizione 8.3.1

Se $G = (V, L)$ è un albero finito con n vertici allora G ha esattamente $n - 1$ lati. Vale cioè la seguente uguaglianza:

$$|G| = |L| + 1$$

Dimostrazione. Sia $G = (V, L)$ un albero finito. Sappiamo che G è privo di circuiti, dobbiamo provare che, se G ha n vertici, allora G ha $n - 1$ lati. Si procede per induzione su n . Il caso $n = 1$ è banale: un albero con 1 solo vertice non ha né lati né circuiti. Assumiamo ora la tesi vera per n e proviamola per $n + 1$. Sia quindi $G = (V, L)$ un albero con $n + 1 \geq 2$ vertici. Per il lemma precedente G ha almeno una foglia (in realtà almeno due foglie), cioè almeno un vertice v di grado 1. Questo significa che in G c'è un unico lato l che ha estremo v . Se eliminiamo dall'albero G il vertice v e il lato l otteniamo un grafo G_0 che è ancora connesso e privo di circuiti, dunque è un albero. Ma G_0 ha n vertici, quindi per l'ipotesi induttiva G_0 ha $n - 1$ lati. Di conseguenza G ha n lati: gli $n - 1$ di G_0 più 1. \square

8.3.2 ■ Sottoalberi massimali

Definizione 8.3.3: Sottografo massimale

Sia $G = (V, L, \varphi)$ un multigrafo finito. Un **sottoalbero massimale** di G è un sottografo G con insieme di vertici V che sia un albero.

Si dimostra facilmente che se elimino un lato da un circuito i vertici $v \in V$ restano ancora tutti connessi. Infatti:

Proposizione 8.3.2

Sia $G = (V, L, \varphi)$ un multigrafo connesso. Sia $l_0 \in L$ tale che l faccia parte di un circuito in G . Allora il sottografo $G' = (V, L', \varphi')$ con $L' = L \setminus \{l_0\}$ è ancora connesso.

Dimostrazione. Siano $a, b \in G$. Se a, b sono connessi da un circuito, allora esistono almeno due cammini diversi da a a b siano essi ν e μ . Se l_0 si trova nel cammino ν allora a e b sono connessi da μ in G' , o viceversa. \square

Teorema 8.3.2 (Teorema conclusivo)

Sia $G = (V, L, \varphi)$ un multigrafo finito con esattamente k componenti connesse. Allora:

1. Se G è connesso allora $|L| \geq |V| - 1$
2. $|L| \geq |V| - k$
3. $|L| = |V| - k$ se, e solo se, G è una foresta
4. Sono equivalenti:
 - (a) G è un albero
 - (b) G è connesso e $|V| = |L| + 1$
 - (c) G è una foresta e $|V| = |L| + 1$

Dimostrazione. 1. Se G è connesso allora G ha un sottoalbero massimale (V, L') con $L' \subseteq L$. Allora $|V| = |L'| + 1$, quindi $|L'| = |V| - 1$ e dato che $|L'| \leq |L| \implies |L| \geq |V| - 1$, ovvero vale $|V| = |L| + 1 \iff |L| = |L'| \iff L = L'$.

2. Siano $(V_1, L_1, \varphi_1), (V_2, L_2, \varphi_2), \dots, (V_k, L_k, \varphi_k)$ le componenti connesse di G , per ogni $i \in \{1, \dots, k\}$ si ha $|L_i| \geq |V_i| - 1$ per la (1). Allora, essendo: $|L| = \sum_{i=1}^k |L_i|$, $|V| = \sum_{i=1}^k |V_i|$ e $\sum_{i=1}^k -1 = -k$ si ha: $|L| \geq |V| - k$.

3. Se per ogni $i \in \{1, \dots, k\}$ $|L_i| = |V_i| - 1$ allora $|L| = |V| - k$ per la (2), inoltre $G_i = (V_i, L_i)$ è un albero. Quindi G è una foresta.

4. (b) \implies (a) per la (1). Mentre (a) \implies (b) è stato già dimostrato.

(a) \implies (c): se G è un albero, allora G è anche una foresta. Inoltre, per la (3) si ha $|V| = |L| + k$, dove k sono le componenti connesse in G . Essendo G un albero deve essere $k = 1$.

(c) \implies (a): per la (3) G è una foresta con $k = 1$ componenti connesse, quindi G è un albero. \square

**Esercizio 8.4.1**

Vero o falso? Le foreste finite sono grafi planari.

Esercizio 8.4.2

Dimostrare che se due grafi G e G' sono isomorfi, anche il grafo complementare di G ed il grafo complementare di G' sono isomorfi tra loro.

Esercizio 8.4.3

Un grafo G ha 7 lati e 8 vertici, sette dei quali hanno grado 1. Qual è il grado dell'ottavo vertice? Disegnare un grafo con queste proprietà. Esistono due siffatti grafi tra loro non isomorfi? Un tale grafo è un albero? Esistono grafi con 7 lati e 8 vertici che non siano alberi?

Esercizio 8.4.4

Esiste un grafo con cinque lati e almeno tre vertici di grado 4?

Esercizio 8.4.5

Un grafo连通的 G ha 9 vertici. Di questi, almeno 6 sono pari. Questi dati sono sufficienti per stabilire se G ha cammini euleriani?

Esercizio 8.4.6

Si considerino i grafi $G = (V, L)$ che verificano la proprietà Φ : “ $|V| = 6 = |L|$ ed esistono in G (almeno) un vertice di grado 4 ed (almeno) tre vertici di grado 2”.

1. Se un grafo G verifica Φ , quali possono essere i gradi dei suoi vertici?
2. Disegnare, se possibile, un grafo che verifichi Φ ;
3. Disegnare, a meno di isomorfismi, tutti i grafi che verificano Φ .

Esercizio 8.4.7

Stabilire per quali interi positivi n il grafo completo su n vertici abbia cammini euleriani e per quali abbia circuiti euleriani.

TRACCE D'ESAME



**CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II E III)
16 GENNAIO 2023**

Svolgere i seguenti esercizi,

—————→ ***giustificando pienamente tutte le risposte.*** ←————

Sui fogli consegnati vanno indicati: **nome, cognome, matricola, gruppo di appartenenza.**

Non è necessario consegnare la traccia.

Esercizio 1. Dimostrare la tautologia della negazione dell'implicazione e utilizzarla per negare la formula $\exists x(\forall y(f(x, y) \rightarrow g(x, y)))$.

Esercizio 2. Siano $A = \{n \in \mathbb{N} \mid n < 10\}$ e $B = \{n \in \mathbb{N} \mid n < 9\}$. Detti T l'insieme delle applicazioni da A ad A ed S l'insieme delle applicazioni da B ad A , sia poi $r: T \rightarrow S$ l'applicazione che ad ogni $f \in T$ associa la restrizione di f a B , cioè l'applicazione $x \in B \mapsto f(x) \in A$.

- (i) Esprimere (non calcolare) $|T|$ ed $|S|$.
- (ii) Vero o falso? Per ogni $f \in T$:
 - (a) f è iniettiva $\Rightarrow r(f)$ è iniettiva;
 - (b) f è suriettiva $\Rightarrow r(f)$ è suriettiva.
- (iii) r è iniettiva? r è suriettiva?

Sia ora \mathcal{R} il nucleo di equivalenza di r , e sia h l'applicazione costante $x \in A \mapsto 3 \in A$.

- (iv) Descrivere $[h]_{\mathcal{R}}$, calcolare $|[h]_{\mathcal{R}}|$ e $|T/\mathcal{R}|$.

Esercizio 3. Si consideri la relazione d'ordine ρ in \mathbb{Z} definita da: per ogni $a, b \in \mathbb{Z}$

$$a \rho b \iff (a = b \vee \text{rest}(a, 9) \text{ è un divisore proprio di } \text{rest}(b, 9)).^1$$

- (i) Determinare gli eventuali minimo, massimo, elementi minimali, elementi massimali in (\mathbb{Z}, ρ) ;
- (ii) sempre in (\mathbb{Z}, ρ) , determinare l'insieme dei minoranti di $\{127, 721\}$ e stabilire quindi se esiste $\inf \{127, 721\}$;
- (iii) (\mathbb{Z}, ρ) è un reticolo?
- (iv) Determinare una catena (cioè un sottoinsieme totalmente ordinato) massimale (rispetto all'inclusione) in (\mathbb{Z}, ρ) .
- (v) Posto $L = \{-90, -15, -3, 7, 15, 94, 100\}$, disegnare un diagramma di Hasse di (L, ρ) . Questo insieme ordinato è un reticolo? Nel caso lo sia, è complementato? È distributivo?

Esercizio 4. Sia $*$ l'operazione binaria in \mathbb{Z}_{16} definita da: $\forall a, b \in \mathbb{Z}_{16}(a * b = \overline{3}ab)$.

- (i) Che tipo di struttura risulta essere $(\mathbb{Z}_{16}, *)$? Determinarne l'eventuale elemento neutro e, se le domande hanno senso, gli elementi simmetrizzabili ed il simmetrico di $\overline{1}$.
- (ii) Sia $H = \{\overline{7}, \overline{11}\} \subseteq \mathbb{Z}_{16}$. Decidere se H è una parte chiusa in $(\mathbb{Z}_{16}, *)$ e, se lo è, descrivere la struttura $(H, *)$.
- (iii) Dando per noto che $(\mathbb{Z}_{16}, +, *)$ è un anello (dove $+$ è l'ordinaria addizione in \mathbb{Z}_{16}), determinare i suoi divisori dello zero.

Esercizio 5. Dare la definizione di circuito euleriano e determinare tutti e soli i numeri interi positivi n tali che il grafo completo K_n su n vertici possieda circuiti euleriani.

Esercizio 6. Sia $f = 5x^4 + 10x^2 + 4x + 2 \in \mathbb{Z}[x]$ e, per ogni $n \in \mathbb{N}$, sia $f_n = \overline{5}x^4 + \overline{10}x^2 + \overline{4}x + \overline{2} \in \mathbb{Z}_n[x]$.

- (i) Stabilire se f è irriducibile in $\mathbb{Q}[x]$ e se f_1 è irriducibile in $\mathbb{Z}_1[x]$.
- (ii) Trovare il polinomio monico associato a f_5 in $\mathbb{Z}_5[x]$ e, se possibile, il polinomio monico associato a f_{32} in $\mathbb{Z}_{32}[x]$.
- (iii) Per quali numeri naturali $n < 10$ il polinomio f_n è cancellabile in $\mathbb{Z}_n[x]$?

¹per ogni intero a , $\text{rest}(a, 9)$ significa $a \bmod 9$, ovvero $a \% 9$.

Esercizio 1

La tautologia della negazione dell'implicazione afferma che sono equivalenti le seguenti proposizioni:

$$\neg(\alpha \implies \beta) \iff (\alpha \wedge \neg\beta)$$

Infatti, sfruttando la tautologia dell'implicazione come disgiunzione abbiamo:

$$\begin{aligned} \neg(\alpha \implies \beta) &\iff \neg(\neg\alpha \vee \beta) \\ &\iff \neg(\neg\alpha) \wedge \neg\beta && \text{(Applicando la legge di De Morgan)} \\ &\iff \alpha \wedge \neg(\beta) \end{aligned}$$

Sfruttando questa tautologia allora abbiamo:

$$\neg\left(\exists x\left(\forall y(f(x,y) \implies g(x,y))\right)\right) \iff \forall x\left(\exists y(f(x,y) \wedge \neg g(x,y))\right)$$

Esercizio 2

$$(i) |T| = |A|^{|A|} \text{ e } |S| = |A|^{|B|};$$

- (ii) (a) Sia f iniettiva e supponiamo che $r(f)$ non sia iniettiva. Allora esistono $x, y \in B$ tali che $r(f)(x) = r(f)(y)$ e $x \neq y$. Ma, per definizione di restrizione, $r(f)(x) = f(x)$ e $r(f)(y) = f(y)$, quindi esistono $x, y \in A$ tali che $f(x) = f(y)$, il che va contro l'ipotesi che f sia iniettiva. Quindi $r(f)$ non può non essere iniettiva se f è iniettiva e l'implicazione risulta vera.
- (b) Analogamente, sia f suriettiva e supponiamo $r(f)$ non suriettiva. Ciò implica che esiste un $x \in A$ tale che $\overleftarrow{r(f)}(\{x\}) = \emptyset$, ovvero non esiste $y \in B$ (e quindi di A) tale che $r(f)(y) = f(y) = x$. Quindi f non risulterebbe suriettiva, contro le nostre ipotesi. Quindi, come nel punto precedente, si ha la veridicità dell'implicazione.
- (iii) Essendo $|T| \geq |S|$ non possono esistere applicazioni iniettive da T in S , quindi r in particolare non può essere iniettiva. Infatti possono esistere applicazioni distinte da A in A che ammettono la stessa restrizione. Al contrario, per ogni restrizione è possibile costruire un prolungamento, per cui r risulta essere una applicazione suriettiva.

(iv) Abbiamo:

$$\begin{aligned} [h]_{\mathfrak{R}} &= \{f \in T \mid r(f) = r(h)\} \\ &= \{f \in T \mid \forall x \in B(r(f)(x) = 3)\} \end{aligned}$$

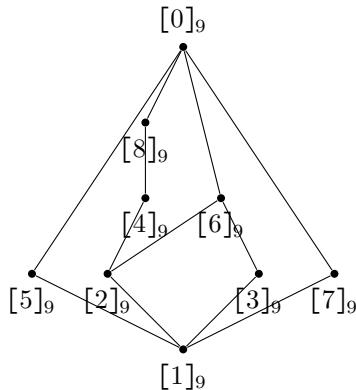
Quindi in $[h]_{\mathfrak{R}}$ sono presenti le funzioni f_i costruite ponendo:

$$f_i : x \in A \mapsto \begin{cases} 3 & \iff x \in B \\ i & \iff x \in A \setminus B = \{10\} \end{cases}$$

con i che varia in $\{1, \dots, 10\}$, per $i = 3$ otteniamo proprio h . Quindi $|[h]_{\mathfrak{R}}| = 10$. Per il Teorema 3.5.2 abbiamo che $|T/\mathfrak{R}| = |\text{im } r| = |S|$ in quanto abbiamo detto che r è suriettiva.

Esercizio 3

- (i) Consideriamo la relazione di divisibilità in \mathbb{Z}_9 , otteniamo il seguente diagramma di Hasse:



Portandoci su (\mathbb{Z}, ρ) osserviamo che ogni classe di resto contiene infiniti interi:

$$[n]_9 = \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}(z = 9k + n)\}$$

Dal diagramma di Hasse disegnato si osserva che gli interi appartenenti alla classe di 1 modulo 9 risultano essere minimi in (\mathbb{Z}, ρ) . Analogamente, gli interi appartenenti alla classe di 0 modulo 9 (i multipli di 9) risultano essere massimali in (\mathbb{Z}, ρ) . Poiché due elementi appartenenti alla stessa classe sono in relazione ρ se e solo se essi coincidono abbiamo che due elementi distinti nella stessa classe di resto risultano essere inconfrontabili e quindi non esiste un minimo ed un massimo in (\mathbb{Z}, ρ) .

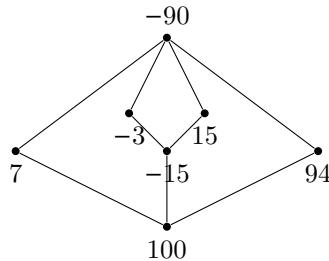
- (ii) Osserviamo che sia $127 \in [1]_9$ che $721 \in [1]_9$ ¹. Quindi i due elementi sono inconfrontabili, essendo $[1]_9$ il minimo in $(\mathbb{Z}_9, |)$ non esistono minoranti di $\{127, 721\}$ mentre esistono infiniti interi, a due a due inconfrontabili, maggioranti di $\{127, 721\}$, quindi non esiste neanche un estremo superiore.
- (iii) Per i motivi esposti al punto precedente (\mathbb{Z}, ρ) non risulta essere un reticolo.
- (iv) Osservando il diagramma di Hasse di $(\mathbb{Z}_9, |)$ osserviamo che è possibile individuare una catena massimale considerando le classi $[1]_9, [2]_9, [4]_9, [8]_9, [0]_9$. Spostandoci in (\mathbb{Z}, ρ) e prendendo un singolo elemento di ciascuna classe si ottiene un sottoinsieme massimale (rispetto all'inclusione). Ad esempio:

$$\{10, 11, 13, 17, 18\}$$

- (v) Abbiamo:

- $-90 \in [0]_9$
- $-15 \in [3]_9$
- $-3 \in [6]_9$
- $7 \in [7]_9$
- $15 \in [6]_9$
- $94 \in [4]_9$
- $100 \in [1]_9$

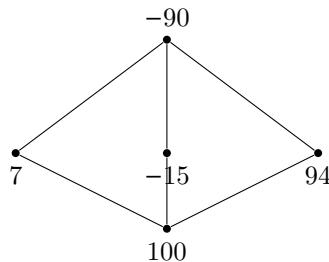
Otteniamo così il seguente diagramma di Hasse:



Tale insieme ordinato è un reticolo complementato, ma non è distributivo in quanto il sottoreticolo:

$$(\{100, 7, -15, 94, -90\}, \rho)$$

è isomorfo al reticolo trirettangolo:



Esercizio 4

- (i) L'operazione $*$ risulta essere associativa e commutativa. Infatti:

$$\forall x, y \in \mathbb{Z}_{16} (x * y = 3xy = 3yx = y * x)$$

Inoltre, presi $a, b, c \in \mathbb{Z}_{16}$ abbiamo:

$$\begin{aligned} a * (b * c) &= a * (3bc) = 3a(3bc) = 9abc \\ (a * b) * c &= (3ab) * c = 3(3ab)c = 9abc \end{aligned}$$

¹Basta applicare i criteri di divisibilità.

Un elemento $t \in \mathbb{Z}_{16}$ è neutro in $(\mathbb{Z}_{16}, *)$ se e solo se, per ogni $a \in \mathbb{Z}_{16}$ risulta:

$$\begin{aligned} a * t = t * a = 3ta = a &\iff 3t \equiv_{16} 1 \\ &\iff t = \overline{11} \end{aligned}$$

Quindi $t = \overline{11}$ è il neutro del monoide $(\mathbb{Z}_{16}, *)$. Un elemento $a \in \mathbb{Z}_{16}$ ammette simmetrico se e solo se esiste un $a' \in \mathbb{Z}_{16}$ tale che $a * a' = 11$, ovvero:

$$3aa' \equiv_{16} 11 \iff aa' \equiv_{16} 9 \quad (\text{Moltiplicando per } 11 \text{ inverso di } 3)$$

Tale equazione ammette soluzione se e solo se $(a, 16) \mid 9$. I divisori di 16 minori di 9 sono 1, 2, 4, 8 e solo divide 9. Possiamo concludere che se $a \in \{1, 3, 5, 7, 9\}$ allora $(a, 16) = 1 \mid 9$. Troviamo l'inverso di $x = \overline{1}$:

$$\begin{aligned} x * x' \equiv_{16} 11 &\iff 3x' \equiv_{16} 11 \\ &\iff x' \equiv_{16} 9 \end{aligned}$$

(ii) Risulta $7 * 7 = 3 \cdot 49 = 3 \cdot 1 = 3 \notin H$, quindi H non è stabile in $(\mathbb{Z}_{16}, *)$

(iii) Un elemento $a \in \mathbb{Z}_{16}$ è divisore dello zero in $(\mathbb{Z}_{16}, +, *)$ se esiste un elemento $b \in \mathbb{Z}_{16} \setminus \{\overline{0}\}$ tale che $a * b = \overline{0}$. Abbiamo:

$$a * b = 3ab = \overline{0}$$

Essendo 3 coprimo con 16 abbiamo che tale elemento è simmetrizzabile e quindi cancellabile, per rendere il prodotto nullo abbiamo quindi bisogno che $ab = \overline{0}$. Tale richiesta si traduce quindi nella ricerca dei divisori dello zero in (\mathbb{Z}_{16}, \cdot) i quali sono tutti e soli gli elementi non invertibili, cioè $\mathbb{Z}_{16} \setminus \mathcal{U}(\mathbb{Z}_{16}) = \{0, 2, 4, 6, 8, 10, 12, 14\}$.

Esercizio 5

Un circuito euleriano in un grafo è un percorso chiuso che attraversa ciascun arco del grafo esattamente una volta. Perché un grafo possa ammettere un circuito euleriano, deve soddisfare due condizioni:

- Tutti i vertici devono avere grado pari
- Il grafo deve essere connesso

Un grafo completo K_n è un grafo in cui ogni coppia di vertici è connessa da un arco, quindi in particolare è un grafo connesso. Per un grafo completo, il grado di ogni vertice è n , poiché ogni vertice è collegato a tutti gli altri $n-1$ vertici. Quindi se $n-1$ deve essere pari ciò significa che n è un numero dispari. Quindi ogni grafo completo con un numero dispari di vertici ammette circuiti euleriani.

Esercizio 6

(i) Applicando il Criterio di Eisenstein con $p = 2$ abbiamo che 2 divide i coefficienti a_0, \dots, a_3 , 2 non divide $a_4 = 4$ e $p^2 = 4$ non divide 2. Quindi il polinomio f è irriducibile in \mathbb{Q} e di conseguenza, essendo associato al polinomio $f_1 \in \mathbb{Z}_1[x] = \mathbb{Z}[x]$, è irriducibile anche in $\mathbb{Z}[x]$.

(ii) Risulta $f_5 = 4x + 2$. Per trovare un polinomio monico associato risolviamo l'equazione $4x \equiv 51$ che ha soluzione per $x = 4$, quindi moltiplicando f_5 per 4 otteniamo:

$$\begin{aligned} 4 \cdot f_5 &= 4 \cdot (4x + 2) \\ &= 16x + 8 \\ &= x + 3 \end{aligned}$$

Analogamente, per f_{32} risolviamo l'equazione $5x \equiv_{32} 1$ ottenendo $x = 13$. Moltiplichiamo quindi f_{32} per $x = \overline{13}$:

$$\begin{aligned} 13 \cdot f_{32} &= 13 \cdot (5x^4 + 10x^2 + 4x + 2) \\ &= x^4 + 2x^2 + 20x + 26 \end{aligned}$$

(iii) Un polinomio è cancellabile se e solo se $cd(f)$ è cancellabile nell'anello dei coefficienti. In questo caso, essendo $cd(f) = 5$ un numero primo abbiamo che per ogni intero non nullo $n < 10$ 5 è coprimo con n e quindi simmetrizzabile, quindi cancellabile.



**CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II E III)
13 LUGLIO 2023**

Svolgere i seguenti esercizi,

—————→ ***giustificando pienamente tutte le risposte.*** ←————

Sui fogli consegnati vanno indicati: **nome, cognome, matricola, gruppo di appartenenza.**

Non è necessario consegnare la traccia.

Esercizio 1. Determinare, laddove possibile, verità o falsità delle seguenti formule o frasi.

- (i) $\emptyset \in \{\{\emptyset\}\}$.
- (ii) $|\mathbb{N}| = \{\mathbb{N}\}$.
- (iii) $\{1, 2, 3\} = \{3!\} \rightarrow \emptyset \in \emptyset$.^(†)
- (iv) $\{(1, 1), (2, 1)\}$ è il grafico di un'applicazione da $\{1, 2\}$ a \mathbb{N} .

Esercizio 2. Sia $S = \mathbb{N} \cap [0]_3$ e sia $\chi = \chi_{\mathbb{N}, S}$ la funzione caratteristica di S in \mathbb{N} . Si consideri poi la seguente operazione binaria $*$ definita su \mathbb{N} :

$$*: (a, b) \in \mathbb{N} \times \mathbb{N} \mapsto a^{\chi(a)} \cdot b^{\chi(b)} \in \mathbb{N}.$$

- (i) $*$ è un'operazione commutativa? È associativa?
- (ii) Trovare tutti gli elementi neutri a destra o a sinistra in $(\mathbb{N}, *)$.
- (iii) Siano $T = \mathbb{N} \cap [0]_2$ e $U = \mathbb{N} \cap [2]_3$. Dire quali tra S , T e U sono parti stabili (ovvero: chiuse) di $(\mathbb{N}, *)$. Quali di queste parti stabili costituiscono un semigruppo?

Esercizio 3. Per ciascuna delle seguenti relazioni binarie definite in \mathbb{N} dire se essa è o non è d'ordine e, nel caso lo sia, determinare gli eventuali minimo, massimo, elementi minimali ed elementi massimali nell'insieme ordinato da essa definito, decidere se questo è un reticolo ed infine disegnare il diagramma di Hasse di $S := \{1, 20, 40, 400, 10000\}$ ordinato dall'ordinamento indotto.

- (i) α definita da: $\forall a, b \in \mathbb{N} (a \alpha b \iff a = b)$;
- (ii) β definita da: $\forall a, b \in \mathbb{N} (a \beta b \iff (a = b \vee (a|b \wedge a < 10b)))$;
- (iii) γ definita da: $\forall a, b \in \mathbb{N} (a \gamma b \iff (a = b \vee (a|b \wedge a > 10b)))$;
- (iv) δ definita da: $\forall a, b \in \mathbb{N} (a \delta b \iff (a = b \text{ oppure } a \text{ non divide } b))$.

Esercizio 4. Disegnare, se possibile, un grafo connesso $G = (V, L)$ tale che $|V| = 16$ e $|L| = 10$, oppure spiegare perché un tale grafo non esiste.

Esercizio 5. Determinare l'insieme A dei numeri interi n tali che $111n$ sia congruo a 11 o a 12 modulo 126. Quanti elementi ha $\{a \in A \mid 0 < a \leq 84\}$?

Esercizio 6. Per ogni $n \in \mathbb{Z}$, sia \bar{n} la classe di resto di n modulo 5.

- (i) Sia S l'insieme dei polinomi $f \in \mathbb{Z}_5$ di grado 4 tali che $f(\bar{1}) = \bar{0}$. Quanti elementi possiede S ?
- (ii) S è una parte chiusa di $(\mathbb{Z}_5[x], +)$? Nel caso, $(S, +)$ è un gruppo abeliano (ovvero commutativo)? Sia $\varphi: f \in S \mapsto f(\bar{1}) \in \mathbb{Z}_5$ la restrizione ad S dell'omomorfismo di sostituzione relativo a $\bar{1}$ e sia \sim_φ il nucleo di equivalenza di φ .
- (iii) φ è iniettiva? È suriettiva?
- (iv) Quanti elementi possiede S/\sim_φ ?

^(†)qui ' \rightarrow ' indica il connettivo di implicazione.

Esercizio 1

Abbiamo:

- (i) **Falso.** L'insieme vuoto non è un elemento del singleton del singleton dell'insieme vuoto ma è tutt'al più una sua parte.
- (ii) **Falso.** Non ha senso confrontare un numero cardinale con un insieme. Il simbolo $|\mathbb{N}|$ indica infatti la cardinalità di \mathbb{N} , ovvero il numero dei suoi elementi, che è quantificabile col simbolo \aleph . Il simbolo $\{\mathbb{N}\}$ indica invece il singleton dell'insieme dei numeri naturali.
- (iii) **Vera.** Notiamo infatti che l'antecedente risulta essere una proposizione falsa in quanto l'insieme dei tre elementi $\{1, 2, 3\}$ non è uguale all'insieme $\{3!\} = \{6\}$. L'implicazione risulta quindi essere vera in quanto l'antecedente è falsa.
- (iv) **Vera.** Una applicazione $f : \{1, 2\} \rightarrow \mathbb{N}$ è un'applicazione per la quale $\forall x \in \{1, 2\}$ esiste un $n \in \mathbb{N}$ tale che $n = f(x)$. Il grafico $\{(1, 1), (2, 1)\}$ descrive in particolare l'applicazione costante c_1 che associa l'elemento 1 ad ogni elemento dell'insieme $\{1, 2\}$.

Esercizio 2

L'insieme $S = \mathbb{N} \cap [0]_3$ è l'insieme dei multipli di 3, ovvero:

$$S = \mathbb{N} \cap [0]_3 = \{n \in \mathbb{N} \mid \exists k \in \mathbb{N} (n = 3k)\} = 3\mathbb{N}$$

L'applicazione caratteristica $\chi_{\mathbb{N}, S}$ restituisce 1 se $n \in 3\mathbb{N}$, 0 altrimenti. In particolare, $\forall n \in \mathbb{N}$:

$$n^{\chi(a)} = \begin{cases} a^1 & \iff a \in 3\mathbb{N} \\ a^0 & \iff a \notin 3\mathbb{N} \end{cases} \quad (9.1)$$

- (i) L'operazione $*$ è banalmente commutativa in quanto lo è la moltiplicazione ordinaria in \mathbb{N} . Per verificare l'associatività bisogna verificare che per ogni terna numerica (a, b, c) di elementi di \mathbb{N} risulti:

$$(a * b) * c = a * (b * c)$$

Sviluppando il membro a sinistra otteniamo:

$$\begin{aligned} (a * b) * c &= (a^{\chi(a)} \cdot b^{\chi(b)}) * c \\ &= (a^{\chi(a)} \cdot b^{\chi(b)})^{\chi(a^{\chi(a)} \cdot b^{\chi(b)})} \cdot c^{\chi(c)} \end{aligned} \quad (9.2)$$

Mentre, sviluppando il membro a destra:

$$\begin{aligned} a * (b * c) &= (b * c) * a \\ &= (b^{\chi(b)} \cdot c^{\chi(c)})^{\chi(b^{\chi(b)} \cdot c^{\chi(c)})} \cdot a^{\chi(a)} \end{aligned} \quad (\text{Applicando la commutatività di } *) \quad (9.3)$$

La verifica dell'uguaglianza di 9.2 con 9.3 deve essere fatta per casi:

- (a) Supponiamo il caso in cui $a, b, c \in 3\mathbb{N}$, in questo caso, applicando quanto osservato in 9.1 otteniamo:

$$\begin{aligned} (a * b) * c &= (a^{\chi(a)} \cdot b^{\chi(b)})^{\chi(a^{\chi(a)} \cdot b^{\chi(b)})} \cdot c^{\chi(c)} \\ &= (a \cdot b) \cdot c = (ab)c \end{aligned} \quad (\text{Osservando che } ab \in 3\mathbb{N})$$

e analogamente:

$$\begin{aligned} a * (b * c) &= (b^{\chi(b)} \cdot c^{\chi(c)})^{\chi(b^{\chi(b)} \cdot c^{\chi(c)})} \cdot a^{\chi(a)} \\ &= (b \cdot c) \cdot a = a(bc) \end{aligned}$$

- (b) Siano ora $a, b, c \notin 3\mathbb{N}$. Allora:

$$\begin{aligned} (a * b) * c &= (1 \cdot 1)^0 \cdot 1 = 1 \\ (a * b) * c &= (1 \cdot 1)^0 \cdot 1 = 1 \end{aligned}$$

- (c) Sia uno tra a, b, c non appartenente a $3\mathbb{N}$. Senza perdere di generalità, sia esso c . Abbiamo quindi:

$$\begin{aligned} (a * b) * c &= (a \cdot b)^1 \cdot 1 = ab \\ a * (b * c) &= a(b \cdot 1)^1 = ab \end{aligned}$$

(d) Siano due elementi non appartenenti a $3\mathbb{N}$, siano essi b, c , allora:

$$\begin{aligned}(a * b) * c &= (a \cdot 1)^1 = a \\ a * (b * c) &= a \cdot (1 \cdot 1)^0 = a\end{aligned}$$

In ogni caso il membro a destra e a sinistra coincidono e quindi $*$ risulta associativa.

(ii) Per esistere elemento neutro rispetto all'operazione $*$ deve esistere un $t \in \mathbb{N}$ tale che, per ogni $n \in \mathbb{N}$, garantisca che $n * t = t * n = n$. Un tale t non può esistere in quanto:

$$\begin{aligned}\forall n \in \mathbb{N} (n * t = n &\iff n^{\chi(n)} \cdot t^{\chi(t)} = n \\ &\iff n^{\chi(n)} = n \wedge t^{\chi(t)} = 1 \\ &\iff (n \in 3\mathbb{N}) \wedge (t \notin 3\mathbb{N}))\end{aligned}$$

Dato che non può esistere un tale t che sia neutro per ogni naturale possiamo concludere affermando la sua non esistenza.

(iii) Abbiamo $T = 2\mathbb{N}$ e $U = \{n \in \mathbb{N} \mid \exists k \in \mathbb{N} (n = 3k+2)\}$. Una parte $X \subseteq \mathbb{N}$ si dice stabile se, e solo se, per ogni $(a, b) \in X \times X$ si abbia $a * b \in X$.

- Presi ad esempio $a = 14$ e $b = 16$ elementi di T abbiamo:

$$\begin{aligned}14 * 16 &= 14^{\chi(14)} \cdot 16^{\chi(16)} \\ &= 14^0 \cdot 16^0 = 1 \notin T\end{aligned}$$

Quindi T non è stabile.

- Presi $a = 5$ e $b = 7$ elementi di U , abbiamo:

$$\begin{aligned}5 * 7 &= 5^{\chi(5)} \cdot 7^{\chi(7)} \\ &= 1 \notin U\end{aligned}$$

Quindi U non è stabile.

- Presi due elementi $a, b \in S$ abbiamo:

$$\begin{aligned}a * b &= a^{\chi(a)} \cdot b^{\chi(b)} \\ &= a \cdot b \in S\end{aligned}$$

Quindi il semigruppo $(S, *)$ risulta stabile rispetto a $*$.

Esercizio 3

(i) La relazione α coincide con la relazione identica $id_{\mathbb{N}}$ che è una relazione d'ordine. In (\mathbb{N}, α) tutti i numeri sono sia minimi che massimali. Non esistono minimo e massimo. Non potendo definire, per ogni coppia di elementi (n, m) l'infimo ed il supremo della parte $\{a, b\}$ l'insieme ordinato non costituisce un reticolo. Presa la parte $S = \{1, 20, 40, 400, 10000\}$ abbiamo il seguente diagramma di Hasse:



(ii) Per verificare che $\beta \in OL(\mathbb{N})$ verifichiamo che essa sia riflessiva, antisimmetrica e transitiva:

- (a) Chiaramente $\forall a \in \mathbb{N}$ risulta $a \beta a$ in quanto $a = a$ e questo è sufficiente per garantire la corrispondenza di un numero con se stesso.
- (b) Siano $a, b \in \mathbb{N}$ tali che $a \beta b$ e $b \beta a$:

$$\begin{cases} a \beta b & \iff a = b \vee (a | b \wedge a < 10b) \\ b \beta a & \iff b = a \vee (b | a \wedge b < 10a) \end{cases} \quad (9.4)$$

Nel caso gli elementi coincidano l'antisimmetria di β è una conseguenza triviale. Se $a | b \wedge a < 10b$ e $b | a \wedge b < 10a$ allora, in particolare, gli elementi risultano essere elementi associati in \mathbb{N} e quindi devono coincidere per forza.

- (c) Siano $a, b, c \in \mathbb{N}$ elementi tali che $a \beta b$ e $b \beta c$. Allora, se $a = b$ e $b = c$ allora $a = c$ e quindi $a \beta c$. Altrimenti, se $a | b \wedge a < 10b$ e $b | c \wedge b < 10c$ allora possiamo scrivere $b = ka$ per un opportuno $k \in \mathbb{N}$ e $c = mb = m(ka) = a(km)$. Quindi $a | c$ e inoltre possiamo eseguire la maggiorazione $a < 10b < 100c$. Quindi vale sicuramente $a < 10c$ e $a \beta c$. Quindi $\beta \in OL(\mathbb{N})$.

L'elemento 1 risulta essere il minimo in (\mathbb{N}, β) in quanto, $\forall n \in \mathbb{N}$, $1 \beta n$. Dato che per ogni a, b esiste sempre un elemento $n \in \mathbb{N}$ tale che $n \cdot a > b$, possiamo dire che in (\mathbb{N}, β) non esistono elementi massimali e dunque un massimo. L'insieme ordinato risulta essere un reticolo in quanto per ogni parte $\{a, b\}$ possiamo trovare l'infimo ed il supremo che è dato dal massimo comun divisore e dal minimo comune multiplo di (a, b) . In particolare (S, β) risulta essere un insieme totalmente ordinato. Si ottiene quindi la catena:



- (iii) La relazione γ coincide con la relazione α in quanto osserviamo che la proposizione $(a \mid b \wedge a > 10b)$ risulta sempre falsa. Infatti un divisore non può essere maggiore di un multiplo dell'elemento che divide. Resta però la condizione di uguaglianza la quale, come visto nel primo punto, risulta essere una relazione d'ordine.
- (iv) La relazione δ non risulta essere una relazione d'ordine in \mathbb{N} in quanto non soddisfa la proprietà antisimmetrica. Infatti presi $a, b \in \mathbb{N}$ tali che $a \nmid b$ e $b \nmid a$, ovvero $a \delta b$ e $b \delta a$, ciò non implica che sia necessariamente $a = b$. Ad esempio abbiamo $2 \delta 5$ e $5 \delta 2$ in quanto $2 \nmid 5$ e $5 \nmid 2$ ma $2 \neq 5$.

Esercizio 4

Un grafo si dice connesso se per ogni coppia di vertici esiste un cammino. Se il numero di vertici è pari a 16 ciò significa che devono esistere almeno 15 lati. Per questo motivo non è possibile disegnare un grafo connesso con 16 vertici e 10 lati.

Esercizio 5

Calcoliamo il Massimo Comun Divisore tra 111 e 126.

$$111 = 3 \cdot 37$$

$$126 = 2 \cdot 3^2 \cdot 7$$

L'equazione $111n \equiv_{126} 11$ non ammette soluzioni in quanto $MCD(111, 126) = 3$ non divide 11, mentre $111n \equiv_{126} 12$ risulta essere una equazione compatibile. Dividendo tutti i termini per 3 si ottiene l'equazione equivalente ridotta:

$$\frac{111}{3}n \equiv_{\frac{126}{3}} \frac{12}{3} \Rightarrow 37n \equiv_{42} 4$$

E vale $MCD(37, 42) = 1$. Cerchiamo una combinazione lineare $37u + 42v = 1$. Applicando l'algoritmo delle divisioni successive si ottiene:

$$42 = 37 \cdot 1 + 5$$

$$37 = 5 \cdot 7 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

Da queste relazioni otteniamo:

$$5 = 42 - 37 \quad (9.5)$$

$$2 = 37 - 5 \cdot 7 \quad (9.6)$$

$$1 = 5 + (-2)2 \quad (9.7)$$

Possiamo dunque esprimere 1 come:

$$\begin{aligned} 1 &= 5 - 4 \\ &= (42 - 37) + (-2)(37 - 35) \\ &= 42 - 37 + (-2)37 + (14)5 \\ &= 42 + (-3)37 + (14)(42 + (-1)37) \\ &= 42 + (-3)37 + (14)42 + (-14)37 \\ &= (15)42 + (-17)37 \end{aligned}$$

Moltiplicando tale combinazione lineare per 4 si ottiene:

$$4 = (60)42 + (-68)37$$

Quindi $u = [-68]_{42} = [16]_{42}$ è soluzione dell'equazione. L'insieme $A = \{[16]_{42}\}$ e vale $\{a \in A \mid 0 \leq a \leq 84\} = \{16, 58\}$.

Esercizio 6

- (i) L'insieme S è costituito dai polinomi $f \in \mathbb{Z}_5$ di grado 4 tali che $f(\bar{1}) = 0$. Un polinomio di grado 4 in $\mathbb{Z}_5[x]$ può essere scritto come:

$$a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

Con $a_4 \neq \bar{0}$, altrimenti non sarebbe un polinomio di quarto grado. Imporre che $f(\bar{1}) = 0$ è equivalente a dire che:

$$a_4 + a_3 + a_2 + a_1 + a_0 = 0$$

La domanda della conta degli elementi di S può essere rivista come il conteggio di tutte le possibili combinazioni degli elementi a_i con $i \in \mathbb{Z}_5$ tali che $\sum_{i=0}^4 a_i = 0$ e tale che $a_4 \neq \bar{0}$. Per ciascuno di questi casi, stiamo essenzialmente chiedendo in quanti modi possiamo scegliere 4 numeri da $\{0, 1, 2, 3, 4\}$ la cui somma sia un valore specifico. Abbiamo quindi:

- Se $a_4 = 1$, deve essere $a_3 + a_2 + a_1 + a_0 = 4$;
- Se $a_4 = 2$, deve essere $a_3 + a_2 + a_1 + a_0 = 3$;
- Se $a_4 = 3$, deve essere $a_3 + a_2 + a_1 + a_0 = 2$;
- Se $a_4 = 4$, deve essere $a_3 + a_2 + a_1 + a_0 = 1$.

Per ogni caso, il numero di combinazioni con ripetizione di 4 elementi presi dall'insieme \mathbb{Z}_5 che diano somma k con $k \in \{4, 3, 2, 1\}$ è dato da:

$$\begin{aligned} \sum_{k=1}^4 \binom{4+k-1}{i} &= \binom{4+1-1}{1} + \binom{4+2-1}{2} + \binom{4+3-1}{3} + \binom{4+4-1}{4} \\ &= 4 + 10 + 20 + 35 \\ &= 69 \end{aligned}$$

- (ii) $(S, +)$ è una parte chiusa. Infatti, presi due polinomi $s, q \in S$ allora $s + q$ calcolato in $\bar{1}$ è equivalente a $s(1) + q(1) = 0$. $(S, +)$ non risulta essere abeliano in quanto il polinomio nullo non è un polinomio di grado 4.
- (iii) Osserviamo che per ogni $f \in S$ ($\varphi(f) = f(\bar{1}) = \bar{0}$), e φ risulta essere una applicazione costante. Quindi φ non è iniettiva e non è suriettiva.
- (iv) Essendo costante φ il suo nucleo di equivalenza coincide con la relazione totale in S . Quindi $S / \sim_\varphi = S / \tau_S = \{S\}$, ed esiste un'unica classe di equivalenza.



**CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II E III)
15 GENNAIO 2024**

Svolgere i seguenti esercizi,

—————→ ***giustificando pienamente tutte le risposte.*** ←————

Sui fogli consegnati vanno indicati: **nome, cognome, matricola, gruppo di appartenenza.**
Non è necessario consegnare la traccia.

Esercizio 1. Scrivere una negazione della formula $\exists y \left(\forall x ((\varphi(x) \wedge \psi(y)) \rightarrow (\psi(y) \rightarrow \theta(x))) \right)$ in cui non appaia il connettivo di implicazione (qui φ , ψ e θ sono predicati unari).

Esercizio 2. Dare una definizione di partizione di un insieme ed enunciare il teorema fondamentale su partizioni e relazioni d'equivalenza. Fornire una partizione di \mathbb{Z} di cardinalità 2^{10} .

Esercizio 3. Determinare i numeri naturali n tali che $2^n < n!$. (Suggerimento: può essere utile fare uso del principio di induzione). Per quali insiemi finiti a si ha $|\mathcal{P}(a)| < |\text{Sym}(a)|$?

Esercizio 4. Si consideri l'operazione $*$: $(a, b) \in \mathbb{Z}_{10} \times \mathbb{Z}_{10} \mapsto \bar{6}a + b \in \mathbb{Z}_{10}$.

- (i) Decidere se $*$ è associativa, se è commutativa, se $(\mathbb{Z}_{10}, *)$ ha elementi neutri a sinistra o a destra e, nel caso la domanda abbia senso, quali suoi elementi sono simmetrizzabili. Che tipo di struttura algebrica è $(\mathbb{Z}_{10}, *)$?
- (ii) Siano $P = \{\bar{2}a \mid a \in \mathbb{Z}_{10}\}$ e $D = \mathbb{Z}_{10} \setminus P$. Per ciascuno di P e D decidere se è una parte chiusa rispetto a $*$ e, nel caso, rispondere, per la corrispondente struttura indotta, alle stesse domande poste al punto precedente per $(\mathbb{Z}_{10}, *)$.

Esercizio 5.

- (i) Stabilire quali tra $[2027]_{2024}$, $[1024]_{2024}$, $[-2]_{2024}$ e $[10001!]_{2024}$ sono invertibili in \mathbb{Z}_{2024} e quali sono divisori dello zero.
- (ii) Calcolare, utilizzando l'algoritmo euclideo, il massimo comun divisore positivo tra 209 e 165 e trovare quindi tutte le soluzioni delle equazioni congruenziali $209x \equiv_{165} 14$ e $165x \equiv_{209} 44$.

Esercizio 6. Siano F l'insieme delle parti finite non vuote di \mathbb{N} e f l'applicazione $x \in F \mapsto \min x + \max x \in \mathbb{N}$.

- (i) Spiegare perché f è ben definita come applicazione;
- (ii) determinare $\overleftarrow{f}(\{2\})$ e $|\overleftarrow{f}(\{2\})|$;
- (iii) f è iniettiva, suriettiva, biettiva?
- (iv) Detto σ il nucleo di equivalenza di f , determinare $[\{2\}]_\sigma$.

Sia ora τ la relazione d'ordine in F definita da:

$$\forall x, y \in F \quad (x \tau y \iff (x = y \vee f(x) \text{ è un divisore proprio di } f(y))).$$

- (v) Determinare in (F, τ) eventuali elementi minimali, massimali, minimo, massimo. (F, τ) è un reticolo?
- (vi) Posto $M = \{\{1\}, \{2\}, \{2, 3, 4\}, \{1, 3, 5, 7\}, \{5, 6, 7\}, \{9\}, \{10, 11, 15, 60, 62\}\}$, disegnare un diagramma di Hasse di (M, τ) , verificare se questo è un reticolo e, nel caso, se è distributivo, complementato, booleano.
- (vii) Determinare in (M, τ) una catena massimale C ed un sottoreticolo booleano massimale B .

Esercizio 7. Per ogni primo positivo p , si consideri il polinomio $f_p = (\bar{4}x^3 + x^2 - \bar{2}x - \bar{4})(x + \bar{1}) \in \mathbb{Z}_p[x]$.

- (i) Determinare l'insieme X dei primi p tali che il resto della divisione tra f_p e $x - \bar{2}$ sia $\bar{0}$.
- (ii) Posto $p = \max X$, decomporre f_p in prodotto di polinomi irriducibili in $\mathbb{Z}_p[x]$.
- (iii) f_p ha un divisore irriducibile monico di grado 2? In caso di risposta affermativa, dire quanti ne ha ed esibirne almeno uno.

Esercizio 1

Applicando la Proposizione 1.3.1 si ottiene:

$$\begin{aligned}\neg\left(\exists y\left(\forall x\left((\varphi(x) \wedge \psi(y)) \implies (\psi(y) \implies \theta(x))\right)\right)\right) &\iff \forall y\left(\neg\left(\forall x\left((\varphi(x) \wedge \psi(y)) \implies (\psi(y) \implies \theta(x))\right)\right)\right) \\ &\iff \forall y\left(\exists x\left(\neg(\varphi(x) \wedge \psi(y)) \implies (\psi(y) \implies \theta(x))\right)\right)\end{aligned}$$

Poniamo $\alpha := \varphi(x) \wedge \psi(y)$ e $\beta := \psi(y) \implies \theta(x)$ e vale, per la Proposizione 1.2.6:

$$\begin{aligned}\neg(\alpha \implies \beta) &\iff \alpha \wedge \neg(\beta) \\ &\iff (\varphi(x) \wedge \psi(y)) \wedge \neg(\psi(y) \implies \theta(x)) \\ &\iff (\varphi(x) \wedge \psi(y)) \wedge (\psi(y) \wedge \neg(\theta(x))) \\ &\iff \varphi(x) \wedge \psi(y) \wedge \psi(y) \wedge \neg(\theta(x)) \\ &\iff \varphi(x) \wedge \psi(y) \wedge \neg(\theta(x))\end{aligned}$$

Sostituiamo quindi la formula ottenuta:

$$\forall y\left(\exists x\left(\varphi(x) \wedge \psi(y) \wedge \neg(\theta(x))\right)\right)$$

Esercizio 2

Una partizione di un insieme X è un insieme \mathcal{F} di non vuote di X tale insieme, a due a due disgiunte, la cui unione unaria è tutto X , ovvero $\bigcup \mathcal{F} = X$. Il Teorema fondamentale su partizioni e relazioni di equivalenza afferma che esiste una corrispondenza biunivoca tra l'insieme delle partizioni di un insieme A e l'insieme delle equivalenze $Eq(A)$, cioè ogni partizione è un insieme quoziante e viceversa. Una partizione di \mathbb{Z} di cardinalità 2^{10} è dato dall'insieme quoziante di \mathbb{Z} rispetto alla congruenza modulo 2^{10} .

Esercizio 3

Per induzione si dimostra che per ogni $n \geq 4$ ($2^n < n!$). Infatti:

- Se $n = 0$ abbiamo $2^0 = 1 = 0!$;
- Se $n = 1$ abbiamo $2^1 = 2 > 1 = 1!$;
- Se $n = 2$ abbiamo $2^2 = 4 > 2 = 2!$;
- Se $n = 3$ abbiamo $2^3 = 8 > 6 = 3!$;
- Se $n = 4$ abbiamo $2^4 = 16 < 24 = 4!$;

Sia quindi $n > 4$ e supponiamo l'asserto vero. Dimostriamo quindi che $2^{n+1} < (n+1)!$. Si ha:

$$2^{n+1} = 2^n \cdot 2$$

e

$$(n+1)! = (n+1)n!$$

Dato che per ipotesi induttiva $2^n < n!$ e, dato che $n > 4$, sicuramente $2 < n+1$, quindi è lecito eseguire la maggiorazione:

$$2^{n+1} = 2^n \cdot 2 < n!(n+1) = (n+1)!$$

Per quanto appena visto possiamo affermare che $|\mathcal{P}(a)| < |Sym(a)|$ per tutti gli insiemi con almeno 4 elementi.

Esercizio 4

- (i) Per ogni terna di elementi $a, b, c \in \mathbb{Z}_{10}$:

$$\begin{aligned}a * (b * c) &= a * (6b + c) \\ &= 6a + 6b + c\end{aligned}$$

e:

$$\begin{aligned}(a * b) * c &= (6a + b) * c \\&= 6(6a + b) + c \\&= 36a + 6b + c \\&= 6a + 6b + c\end{aligned}$$

Quindi $*$ è associativa. Siano $a, b \in \mathbb{Z}_{10}$:

$$a * b = 6a + b \neq 6b + a = b * a$$

Infatti, presi $a = 1$ e $b = 0$ abbiamo $a * b = 6$ e $b * a = 1$. Quindi $*$ non è commutativa. Cerchiamo un eventuale neutro a sinistra. Un siffatto elemento, composto a sinistra con qualunque elemento di \mathbb{Z}_{10} deve restituire l'elemento stesso. Ossia:

$$\begin{aligned}\forall x \in \mathbb{Z}_{10} (t * x = x &\iff 6t + x = x \\&\iff 6t = 0)\end{aligned}$$

Gli unici $t \in \mathbb{Z}_{10}$ che sono soluzioni di tale equazione risultano essere $t = \bar{5}$ e $t = \bar{0}$. Questi sono gli unici possibili elementi che possono essere neutri a destra. Osserviamo però che, preso un $a \in \mathbb{Z}_{10}$:

$$\begin{aligned}a * 0 = 6a + 0 = a &\iff 5a \equiv_{10} 0 \\&\iff a = 6 \vee a = 0\end{aligned}$$

e:

$$\begin{aligned}a * 5 = 6a + 5 = a &\iff 5a \equiv_{10} 5 \\&\iff a = \bar{9} \vee a = \bar{1} \vee a = \bar{3} \vee a = \bar{5} \vee a = \bar{7}\end{aligned}$$

Quindi non risultano essere neutri per tutti gli elementi di \mathbb{Z}_{10} .

(ii) Abbiamo $P = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ e $D = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}\}$. Siano n, m due elementi di \mathbb{Z}_{10} e consideriamo i rispettivi elementi $2n$ e $2m$ in P . Allora:

$$2n * 2m = 12n + 2m = 2(6n + 3m) \in P$$

Analogamente, un elemento di D è scrivibile come $2n + 1$ e abbiamo:

$$\begin{aligned}(2n + 1) * (2m + 1) &= 12n + 6 + 2m + 1 \\&= 2(6n + m + 3) + 1 \in D\end{aligned}$$

Quindi sia P che D sono parti chiuse rispetto a $*$. Per le conclusioni del punto precedente $\bar{0}$ non è neutro a destra in P e $\bar{5}$ non è neutro a destra in D , quindi $(P, *)$ e $(D, *)$ sono semigruppi abeliani.

Esercizio 5

(i) Abbiamo:

- $[2027]_{2024} = [3]_{2024}$. Poiché $(3, 2024) = 1$ abbiamo che è un elemento invertibile in \mathbb{Z}_{2024} ;
- $[1024]_{2024}$ è un divisore dello zero in quanto è sicuramente non coprimo con 2024 essendo entrambi numeri divisibili per due.
- Analogamente $[-2]_{2024} = [2022]_{2024}$ è un divisore dello zero.
- $[10001!]_{2024} = [0]_{2024}$ in quanto 2024 è uno dei fattori di $10001!$, quindi è un divisore dello zero.

(ii) Applicando l'algoritmo delle divisioni successive troviamo:

$$\begin{aligned}209 &= 165 \cdot 1 + 44 \\165 &= 44 \cdot 3 + 33 \\44 &= 33 \cdot 1 + 11 \\33 &= 11 \cdot 3 + 0\end{aligned}$$

Quindi $(209, 165) = 11$. Dato che $11 \nmid 14$ possiamo dire che $209x \equiv_{165} 14$ non ammette soluzioni. Al contrario è ovvio che $11 \mid 44$, quindi possiamo trovare delle soluzioni per l'equazione $165x \equiv_{209} 44$, dividendo tutti i termini per 11 otteniamo l'equazione congruenziale equivalente:

$$15x \equiv_{19} 4$$

Cerchiamo una combinazione lineare $15x + 19y = 4$. Mediante l'algoritmo di Euclide abbiamo:

$$\begin{aligned} 19 &= 15 \cdot 1 + 4 \\ 15 &= 4 \cdot 3 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

Quindi $(15, 19) = 1$. Otteniamo in particolare:

$$4 = 19 + 15 \cdot (-1)$$

Quindi $\overline{-1} = \overline{18}$ è soluzione dell'equazione congruenziale.

Esercizio 6

(i) Poiché (\mathbb{N}, \leq) è un insieme naturalmente ordinato ogni parte finita non vuota di \mathbb{N} risulta dotata di minimo e massimo sicché è possibile sempre eseguire la somma tra questi due valori. Quindi f è ben posta.

(ii) Abbiamo:

$$\begin{aligned} \overleftarrow{f}(\{2\}) &= \{x \in F \mid f(x) = 2\} \\ &= \{x \in F \mid \min(x) + \max(x) = 2\} \\ &= \{\{0, 2\}, \{1\}, \{0, 1, 2\}\} \end{aligned}$$

Quindi $|\overleftarrow{f}(\{2\})| = 3$.

(iii) L'applicazione f non è iniettiva in quanto, per esserlo, dato il Teorema 3.4.2, sarebbe dovuto essere $\forall n \in \mathbb{N} (|\overleftarrow{f}(\{n\})| \leq 1)$ ma ciò chiaramente non è vero in quanto nel punto precedente è stato trovato un controsenso.

L'applicazione è suriettiva in quanto, per ogni $n \in \mathbb{N}$ è possibile trovare una parte $x \in F$ tale che $\min(x) + \max(x) = n$. Ad esempio $x = \{1, n - 1\}$.

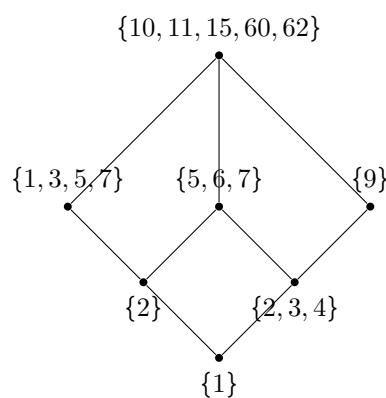
Non essendo iniettiva la funzione non può essere biettiva.

(iv) Abbiamo:

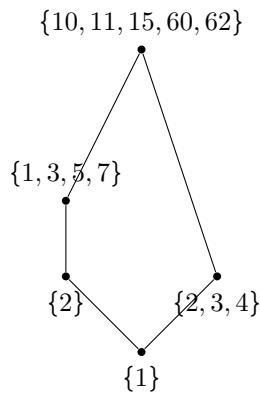
$$\begin{aligned} [\{2\}]_\sigma &= \overleftarrow{f}(\{f(\{2\})\}) \\ &= \overleftarrow{f}(\{4\}) \\ &= \{\{0, 4\}, \{0, 1, 2, 3, 4\}, \{1, 2, 3\}, \{1, 3\}\} \end{aligned}$$

(v) Per le proprietà indotte dalla relazione di divisibilità su \mathbb{N} sappiamo che $\{0, 1\} = \overleftarrow{f}(\{1\})$ divide ogni altro $f(y)$ con $y \in F$ risultando quindi il minimo di (F, τ) . Poiché, per ogni $n \in \mathbb{N} (n \mid 0)$ abbiamo che $\{0\} \in F$ è il massimo di (F, τ) . La struttura non risulta, però, essere un reticolo in quanto non è possibile determinare, per ogni coppia di elementi incontrabili un estremo inferiore ed un estremo superiore in quanto non è possibile determinare un "massimo comune divisore" oppure un "minimo comune multiplo" tra più parti che condividono la stessa immagine secondo l'applicazione f .

(vi) Abbiamo:



Chiaramente (M, τ) è un reticolo ma non è né distributivo, né complementato. Infatti è facilmente osservabile il fatto che non esiste alcun complemento per l'elemento $\{5, 6, 7\}$. Inoltre non è distributivo in quanto il sottoreticolo:



Risulta essere isomorfo al reticolo pentagonale. Non essendo distributivo chiaramente non può essere booleano.

- (vii) Una catena massimale C può essere ottenuta dalla parte $\{\{1\}, \{2, 3, 4\}, \{9\}, \{10, 11, 15, 60, 62\}\}$. Un sottoreticolo booleano massimale invece dai quattro elementi: $\{\{1, \{2\}, \{2, 3, 4\}, \{5, 6, 7\}\}\}$.

Esercizio 7

Iniziamo osservando che $\forall p \in \mathbb{P}$ la struttura $(\mathbb{Z}_p, +, \cdot)$ risulta essere un campo.

- (i) Se il resto della divisione tra f_p e il polinomio $(x - \bar{2})$ è zero, per il Teorema di Ruffini 7.3.3, $\bar{2}$ è radice di f_p , cioè $f_p(\bar{2}) = \bar{0}$. Calcoliamo quindi $f_p(\bar{2})$ e calcoliamo per quali $p \in \mathbb{P}$ si annulla:

$$\begin{aligned} (\bar{4}(\bar{2}^3) + (\bar{2}^2) - \bar{2}(\bar{2}) - 4)(\bar{2} + \bar{1}) &= (\bar{4} \cdot \bar{8} + \bar{4} - \bar{4} - \bar{4}) \cdot (\bar{3}) \\ &= (\bar{3}\bar{2} + \bar{4} - \bar{8}) \cdot \bar{3} \\ &= \bar{2}\bar{8} \cdot \bar{3} \\ &= \bar{8}\bar{4} \end{aligned}$$

Scomponiamo allora 84 in fattori primi:

$$84 = 2^2 \cdot 7 \cdot 3$$

Da questa scomposizione possiamo concludere dicendo che, essendo 84 multiplo dei primi 2, 7 e 3, avremo che $\bar{8}\bar{4} = \bar{0}$ in \mathbb{Z}_2 , \mathbb{Z}_3 e \mathbb{Z}_7 . Quindi $X = \{2, 3, 7\}$.

- (ii) Poniamo $p = 7 = \max X$. Decomponiamo f_7 in prodotto di primi irriducibili. Sappiamo che $\bar{2}$ è radice di f_7 , che risulta allora divisibile per $x - \bar{2}$. Notiamo che f_7 è definito come prodotto tra due polinomi, uno di grado 3 e uno di grado 1. Chiaramente $\bar{2}$ non è radice di $(x + \bar{1})$, per il Lemma 7.3.1 abbiamo quindi che $(x - \bar{2})$ divide $(4x^3 + x^2 - \bar{2}x - \bar{4})$:

$$\begin{array}{r} 4x^3 + x^2 - 2x - 4 \\ - 4x^3 + 8x^2 \\ \hline 9x^2 - 2x \\ - 9x^2 + 18x \\ \hline 16x - 4 \\ - 16x + 32 \\ \hline 28 \end{array} \quad \left| \begin{array}{l} x - 2 \\ 4x^2 + 9x + 16 \end{array} \right.$$

Dove $\bar{2}\bar{8}_7 = \bar{0}_7$ e $\bar{4}x^2 + \bar{9}x + \bar{16} = \bar{4}x^2 + \bar{2}x + \bar{2}$. Il polinomio g_1 così ottenuto risulta essere un polinomio di secondo grado, che sarà irriducibile e solo se non ammette radici. Mediante un controllo diretto si vede facilmente che $g_1(\bar{5}) = 0$. Eseguiamo quindi la divisione di g_1 per $(x - \bar{5})$:

$$\begin{array}{r} 4x^2 + 2x + 2 \\ - 4x^2 + 20x \\ \hline 22x + 2 \\ - 22x + 110 \\ \hline 112 \end{array} \quad \left| \begin{array}{l} x - 5 \\ 4x + 22 \end{array} \right.$$

Con $\bar{1}\bar{1}\bar{2} = \bar{0}$ e $\bar{2}\bar{2} = \bar{1}$. Otteniamo quindi la seguente fattorizzazione:

$$f_7 = (\bar{4}x + \bar{1})(x - \bar{2})(x - \bar{5})(x + \bar{1})$$

- (iii) Dalla fattorizzazione ottenuta osserviamo che f_7 non ha alcun divisore monico irriducibile di grado 2.



**CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II E III)
16 MARZO 2024**

Svolgere i seguenti esercizi,

—————→ ***giustificando pienamente tutte le risposte.*** ←————

Sui fogli consegnati vanno indicati: **nome, cognome, matricola, gruppo di appartenenza.**

Non è necessario consegnare la traccia.

Esercizio 1. La forma proposizionale $((p \Rightarrow r) \iff (s \vee \neg q)) \Rightarrow ((s \wedge q) \Rightarrow (s \vee q))$ è una tautologia?

Esercizio 2. Sia $f: (a, b) \in \mathbb{Z} \times \mathbb{Z} \mapsto 30a + b \in \mathbb{Z}$.

- (i) f è iniettiva? È suriettiva?
- (ii) Posto $T = \{n \in \mathbb{N} \mid 60 \leq n \leq 70\}$, determinare l'insieme S delle coppie in $(a, b) \in \mathbb{N} \times T$ tali che l'elemento $[f(a, b)]_{45}$ sia invertibile in \mathbb{Z}_{45} .
- (iii) Scelto $(a, b) \in S$ in modo che $a+b$ abbia il minimo valore possibile, si calcoli l'inverso di $[f(a, b)]_{45}$ in \mathbb{Z}_{45} .

Esercizio 3. Nel prodotto cartesiano $\mathbb{Z}_4 \times \mathbb{Z}_6$ si considerino le operazioni di addizione e moltiplicazione usuali componenti per componente. Rispetto a tali operazioni, che indichiamo ancora con $+$ e \cdot , $R := \mathbb{Z}_4 \times \mathbb{Z}_6$ risulta essere un anello commutativo unitario. Determinare:

- (i) $|R|$;
- (ii) lo zero 0_R , l'unità 1_R , gli elementi invertibili, i divisori dello zero e gli elementi idempotenti di R ;
- (iii) le radici in R del polinomio $x^2 - x \in R[x]$;
- (iv) la caratteristica di R (cioè il minimo $n \in \mathbb{N}^*$ tale che $n1_R = 0_R$).
- (v) R è un dominio di integrità?
- (vi) La parte $M = \mathbb{Z}_4 \times \{[0]_6, [3]_6\}$, è chiusa rispetto alle operazioni di addizione e moltiplicazione in R ? Nel caso lo sia, che tipo di struttura risulta essere $(M, +, \cdot)$?
- (vii) Se M è chiusa rispetto a \cdot , (a) (M, \cdot) ha elemento neutro? (b) Che tipo di struttura è (M, \cdot) ?

Esercizio 4. Sia ρ la relazione binaria definita in \mathbb{N} da: $\forall a, b \in \mathbb{N} (a \rho b \iff b - a \in 2a\mathbb{N})$. (Qui, come altrove, $2a\mathbb{N} = \{2ak \mid k \in \mathbb{N}\}$). Decidere se ρ è una relazione d'ordine. Se lo è:

- (i) determinare i minoranti di $\{12\}$ in (\mathbb{N}, ρ) ;
- (ii) determinare gli elementi minimali, massimali, minimo, massimo in (\mathbb{N}, ρ) ;
- (iii) decidere se (\mathbb{N}, ρ) è un reticolo;
- (iv) decidere se l'applicazione identica di \mathbb{N} è crescente da (\mathbb{N}, ρ) a $(\mathbb{N}, |)$ e se è un isomorfismo tra questi due insiemi ordinati;
- (v) posto $S = \{1, 3, 5, 9, 21, 45, 75, 105^2\}$, disegnare un diagramma di Hasse di (S, ρ) e stabilire se (S, ρ) è un reticolo, un reticolo distributivo, un reticolo complementato.

Esercizio 5. Dare la definizione di relazione binaria.

- (i) Sia $a = \{n \in \mathbb{N} \mid n \leq 7\}$. Determinare tutte le relazioni di equivalenza ρ in a tali che $0 \rho 7$, $(1, 4)$ appartenga al grafico di ρ , $\{3, 4, 7\} \subseteq [2]_\rho$ e $3 \rho 1 \Rightarrow 5 \rho 0$.
- (ii) Presentare, se possibile, due distinte partizioni p_1 e p_2 di a tali che $p_1 = a/\sim_1$ e $p_2 = a/\sim_2$ per due delle relazioni di equivalenza, \sim_1 e \sim_2 , trovate al punto (i).

Esercizio 6. Sia $f = (x^2 - \bar{5})g \in \mathbb{Z}_{11}[x]$, dove $g = x^5 + \bar{4}x^2 - x + \bar{7}$. Dopo aver calcolato $g(\bar{1})$ e $g(-\bar{1})$, dando per noto che non esistono numeri interi n tali che $n^3 + n \equiv_{11} 7$, scrivere f come prodotto di polinomi irriducibili in $\mathbb{Z}_{11}[x]$.

- (i) È possibile scrivere f come prodotto di sei polinomi (in $\mathbb{Z}_{11}[x]$) non costanti?
- (ii) È possibile scrivere f come prodotto di polinomi irriducibili (in $\mathbb{Z}_{11}[x]$) non monici tutti con lo stesso coefficiente direttore?

Esercizio 1

Poniamo:

$$\begin{aligned}\alpha &:= (p \implies r) \iff (s \vee \neg q) \\ \beta &:= (s \wedge q) \implies (s \vee q)\end{aligned}$$

Per verificare allora che $\alpha \implies \beta$ sia una tautologia proviamo che questa non può risultare mai falsa. Per risultare falsa deve essere vera α e falsa β . Se β risultasse falsa avremmo che $(s \wedge q)$ debba risultare vera mentre $(s \vee q)$ falsa. Però, se $(s \wedge q)$ è vera, lo saranno sia s che q , quindi $(s \vee q)$ in particolare non potrebbe risultare falsa. Da questo controsenso possiamo concludere che $\alpha \implies \beta$ è una tautologia. ■

Esercizio 2

- (i) La funzione non è iniettiva. Infatti prese le coppie $(1, 0)$ e $(-1, 60)$ otteniamo:

$$f((1, 0)) = 30 \cdot 1 + 0 = 30 = 30 \cdot -1 + 60 = f((-1, 60))$$

- (ii) La funzione è suriettiva, infatti per ogni $z \in \mathbb{Z}$ abbiamo che $z = f(0, z)$. Quindi, per ogni numero intero $z \in \mathbb{Z}$ esiste una coppia $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ tale che $f((a, b)) = z$.

- (iii) Un elemento $[f(a, b)]_{45} \in \mathbb{Z}_{45}$ risulta essere invertibile se e solo se $MCD(f(a, b), 45) = 1$. Ovvero se non esiste alcun divisore comune diverso da 1 tra di loro.

Per avere che un numero intero della forma $30a + b$ sia coprimo con 45 sarà necessario assicurarsi che questo non condivida alcun fattore primo con 45, cioè non essere divisibile né per 3 né per 5, in quanto $45 = 3^2 \cdot 5$. Essendo $30 = 3 \cdot 5 \cdot 2$, un intero della forma $30a$ avrà sempre divisorì in comune con 45, quindi sarà sufficiente imporre a b di non annullare i contributi di 3 e 5 in a . Ovvero imponendo che b non sia divisibile per 3 e 5.

Possiamo quindi descrivere S come l'insieme delle coppie (a, b) con $a \in \mathbb{N}$ e $b \in \{61, 62, 64, 67, 68\}$.

- (iv) Presa la coppia $(0, 61)$ procediamo a calcolare l'inverso di $[61]_{45} = [16]_{45}$. Cerchiamo dunque un elemento $x \in \mathbb{Z}_{45}$ tale che $16x \equiv_{45} 1$. Procediamo utilizzando l'algoritmo delle divisioni successive:

$$\begin{aligned}45 &= 16 \cdot 2 + 13 \\ 16 &= 13 \cdot 1 + 3 \\ 13 &= 3 \cdot 4 + 1 \\ 3 &= 1 \cdot 3 + 0\end{aligned}$$

Si ottiene quindi:

$$\begin{aligned}1 &= 13 + (-4)3 \\ &= (45 + (-2)16) + (-4)(16 + (-1)13) \\ &= 45 + (-6)16 + (4)45 + (-8)16 \\ &= (5)45 + (-14)16\end{aligned}$$

Da cui possiamo vedere che $x = [-14]_{45} = [31]_{45}$ è la soluzione cercata.

Esercizio 3

- (i) $|R| = |\mathbb{Z}_4| \times |\mathbb{Z}_6| = 4 \cdot 6 = 24$.

- (ii) Si ha $0_R = (0, 0)$ e $1_R = (1, 1)$. Infatti, per ogni coppia $(a, b) \in R$ si ha:

$$\begin{aligned}(a, b) + (0, 0) &= (a + 0, b + 0) = (a, b) \\ (a, b) \cdot (1, 1) &= (1 \cdot a, 1 \cdot b) = (a, b)\end{aligned}$$

Un elemento $(a, b) \in R$ è invertibile se esiste un elemento (a', b') tale che:

$$(a, b) \cdot (a', b') = (a \cdot a', b \cdot b') = (1, 1)$$

La ricerca di tali coppie in R può essere ridotta quindi alla ricerca degli elementi invertibili in \mathbb{Z}_4 e \mathbb{Z}_6 . Per la Proposizione 7.2.4 sappiamo che in \mathbb{Z}_4 risultano essere invertibili gli elementi $\bar{1}$ e $\bar{3}$ mentre in \mathbb{Z}_6 sono invertibili gli elementi $\bar{5}$ e $\bar{1}$. Otteniamo così le seguenti 4 coppie di elementi invertibili:

$$\mathcal{U}(R, \cdot) = \{(1, 1), (1, 5), (3, 1), (3, 5)\}$$

Facendo un ragionamento analogo otteniamo che in \mathbb{Z}_4 risultano essere divisori dello zero gli elementi $\bar{0}$ e $\bar{2}$ mentre sono divisori dello zero in \mathbb{Z}_6 gli elementi $\bar{0}, \bar{2}, \bar{3}, \bar{4}$. Le coppie di R che risultano essere divisori dello zero sono quindi:

$$\{(0,0), (0,2), (0,3), (0,4), (2,0), (2,2), (2,3), (2,4)\}$$

Un elemento $(a,b) \in R$ è idempotente se, e soltanto se, $(a,b) \cdot (a,b) = (a,b)$. In altre parole deve essere:

$$\begin{cases} a^2 \equiv_4 a \\ b^2 \equiv_6 b \end{cases}$$

L'equazione $a^2 \equiv a \pmod{4}$ è equivalente all'equazione $a^2 \equiv a \pmod{2}$ che è sua volta equivalente a $a(a-1) \equiv 0 \pmod{2}$ che ha soluzioni solo per $a = 0, a = 1$ per la legge di annullamento del prodotto. Seguendo un ragionamento analogo, l'equazione $b^2 \equiv b \pmod{6}$ è risolta da $b \in \{0, 1, 3, 4\}$. Otteniamo quindi che le coppie:

$$(0,0), (0,1), (0,3), (0,4), (1,0), (1,1), (1,3), (1,4)$$

risultano essere idempotenti in R .

(iii) Un elemento di R è radice del polinomio $x^2 - x$ se e soltanto se:

$$\begin{aligned} (a,b) \cdot (a,b) - (a,b) &= (0,0) \iff (a^2 - a, b^2 - b) = (0,0) \\ &\iff \begin{cases} a^2 = a \\ b^2 = b \end{cases} \end{aligned}$$

Quindi tutte le coppie di elementi idempotenti in R trovate nel punto precedente sono radici di tale polinomio.

(iv) Risulta $mcm(4,6) = 12$ e vale $12 \cdot 1_R = 12 \cdot (1,1) = (12,12) = (0,0) = 0_R$, quindi la caratteristica di R è 12.

(v) R non è un dominio di integrità in quanto sono presenti divisori dello zero.

(vi) Siano $(a,b), (c,d) \in M$ e consideriamo le composte $(a,b) + (c,d) = (a+c, b+d)$ e $(a,b) \cdot (c,d) = (ac, bd)$. Per verificare la stabilità di M deve essere $b+d \in \{[0]_6, [3]_6\}$ e $bd \in \{[0]_6, [3]_6\}$, che risulta banalmente vero. $(M, +, \cdot)$ risulta quindi essere un anello commutativo.

(vii) $(M, +, \cdot)$ è un anello unitario in quanto la coppia $(1,3) \in M$ risulta essere un elemento neutro rispetto alla moltiplicazione, quindi (M, \cdot) è un monoide.

Esercizio 4

La relazione ρ è una relazione d'ordine. Infatti:

- È riflessiva: $\forall a \in \mathbb{N}(a \rho a \iff (a-a) = 0 = 2a \cdot 0 \in 2a\mathbb{N})$;
- È antisimmetrica: siano $a, b \in \mathbb{N}$ tali che $a \rho b$ e $b \rho a$. Allora vale, per opportuni $k, m \in \mathbb{N}$:

$$\begin{cases} b-a = 2ak \\ a-b = 2bm \end{cases} \implies \begin{cases} b = 2ak+a = a(2k+1) \\ a = 2bm+b = b(2m+1) \end{cases}$$

Sostituendo la seconda equazione nella prima si ottiene:

$$a = (a(2m+1)(2k+1))$$

Per cui deve essere $(2m+1)(2k+1) = 1$ che risulta vera se e solo se $m = k = 0$, allora sostituendo tali valori nelle prime equazioni si ottiene $b-a = 0 \iff b = a$.

- È transitiva: siano $a, b, c \in \mathbb{N}$ tali che $a \rho b$ e $b \rho c$. Quindi $b-a \in 2a\mathbb{N}$ e $c-b \in 2b\mathbb{N}$. Dimostriamo che $c-a \in 2a\mathbb{N}$. Ripetendo un ragionamento analogo a quanto visto per dimostrare l'antisimmetria della relazione ρ , abbiamo che $b = a(2k+1)$ e $c = b(2m+1)$ per un opportuni $k, m \in \mathbb{N}$. Sostituendo l'equazione di b nella seconda si ottiene:

$$\begin{aligned} c &= b(2m+1) \\ &= (a(2k+1))(2m+1) \end{aligned}$$

Calcoliamo quindi la differenza $c-a$:

$$\begin{aligned} c-a &= (a(2k+1))(2m+1) - a \\ &= a((2k+1)(2m+1) - 1) \\ &= a(4km + 2k + 2m + 1 - 1) \\ &= a(2(km + k + m)) \\ &= a \cdot 2\nu \in 2a\mathbb{N} \end{aligned} \quad (\text{Ponendo } km + k + m = \nu)$$

Il che dimostra la transitività della relazione ρ .

(i) L'insieme dei minoranti di $\{12\}$ è definito come:

$$\{12\}^\downarrow = \{n \in \mathbb{N} \mid n \rho 12\}$$

Un naturale $n \in \mathbb{N}$ “precede” 12 se e solo se:

$$\begin{aligned} n \rho 12 &\iff 12 - n \in 2n\mathbb{N} \\ &\iff \exists k \in \mathbb{N}(12 - n = 2nk) \\ &\iff \exists k \in \mathbb{N}(12 = n + 2nk) \\ &\iff \exists k \in \mathbb{N}(12 = n(2k + 1)) \end{aligned}$$

Quindi se, e solo se $n \mid 12$ e $12/n$ è dispari. I divisori di 12 sono $\{1, 2, 3, 4, 6, 12\}$, eseguendo dei rapidi calcoli otteniamo che per $n = 4$ si ottiene $12/4 = 3$ e per $n = 12$ si ha $12/12 = 1$. Quindi:

$$\{12\}^\downarrow = \{4, 12\}$$

(ii) Un elemento $a \in \mathbb{N}$ è minimale se e solo se non esiste un naturale $b \in \mathbb{N}$ tale che sia $b \neq a$ e $b \rho a$. Ossia:

$$\begin{aligned} a \text{ minimale in } \mathbb{N} &\iff \neg(\exists b \in \mathbb{N}(b \rho a \wedge b \neq a)) \\ &\iff \neg(\exists b \in \mathbb{N}(a - b \in 2b\mathbb{N} \wedge b \neq a)) \\ &\iff \neg(\exists b \in \mathbb{N}(b \mid a \wedge \exists k \in \mathbb{N}(\frac{a}{b} = (2k + 1)) \wedge b \neq a)) \end{aligned}$$

Chiaramente 1 risulta minimale in \mathbb{N} , così come il 2. Ogni numero dispari è preceduto da almeno 1 e non può appartenere quindi all'insieme dei minimali. Infatti, preso un numero dispari della forma $m = (2k + 1)$ abbiamo che $1 \mid m$ e $\frac{m}{1} = 2k + 1$. Restano da analizzare quindi solo i numeri pari, ovvero gli elementi dell'insieme $2\mathbb{N} = \{2t \mid t \in \mathbb{N}\}$. Se t è dispari abbiamo che il numero $n = 2t$ può essere scritto come $2 \cdot (2k + 1)$ ed è chiaro che $(2k + 1) \rho n$. Sia t pari, in questo caso n risulta essere una potenza del 2 che può essere scritta come 2^k . Gli unici divisori propri di 2^k saranno le potenze del tipo 2^j con $j < k$ e $\frac{2^k}{2^j} = 2^{k-j}$ che risulta essere pari. Possiamo affermare quindi che, se n è una potenza del due, non esistono naturali m , diversi da n stesso, che dividano n e tali che $\frac{n}{m}$ sia dispari. Quindi l'insieme elementi minimali di (\mathbb{N}, ρ) è rappresentato da tutte le potenze del 2. Avendo infiniti minimali non esiste il minimo in (\mathbb{N}, ρ) .

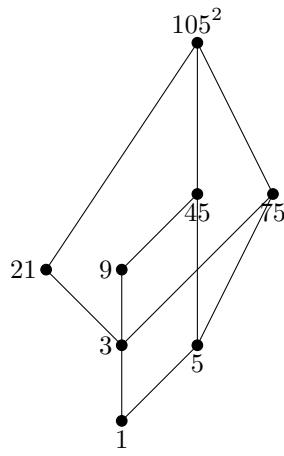
Dato che ogni numero è “coperto” da un suo multiplo, non esistono elementi massimali in \mathbb{N} , e di conseguenza neanche massimi.

- (iii) Considerata una qualsiasi coppia di elementi $\{2^i, 2^j\}$ con $i, j \in \mathbb{N}$ osserviamo che non esiste estremo inferiore in (\mathbb{N}, ρ) il quale non risulta essere quindi un reticolo.
- (iv) Sia $f : (\mathbb{N}, \rho) \rightarrow (\mathbb{N}, |)$ l'applicazione identica. Chiaramente questa risulta crescente per come è definita la relazione ρ . Infatti, presi $a, b \in \mathbb{N}$:

$$\begin{aligned} a \rho b &\iff b - a \in 2a\mathbb{N} \\ &\iff \exists k \in \mathbb{N}(b = 2ak + a) \\ &\iff \exists k \in \mathbb{N}(b = a(2k + 1)) \\ &\iff a \mid b \\ &\iff f(a) \mid f(b) \end{aligned}$$

L'applicazione identica è biettiva, crescente, ma non lo è l'applicazione inversa f^{-1} . Infatti, presi due elementi $a, b \in \mathbb{N}$ tali che $a \mid b$, non è detto che b sia esprimibile necessariamente come prodotto di a per un numero dispari, condizione necessaria affinché $a \rho b$. Ad esempio presa la coppia $(4, 8)$ vale $4 \mid 8$ eppure $4 \not\rho 8$ in quanto $8 - 4 \notin 2 \cdot 4\mathbb{N} = 8\mathbb{N}$. Quindi f non risulta essere un isomorfismo.

(v) Si ha:



(S, ρ) è un reticolo.

Esercizio 5

Una relazione binaria è una terna $\rho = (A, A, G)$ dove A è un insieme e $G \subseteq A \times A$.

(i) Preso $a = \{1, 2, 3, 4, 5, 6, 7\}$ consideriamo tutte le relazioni $\sim = (A, A, G)$ dove:

$$\{(0, 7), (1, 4), (2, 3), (2, 4), (2, 7)\} \subseteq G$$

Inoltre, se la coppia $(3, 1)$ appartiene al grafico allora anche la coppia $(5, 0) \in G$. Per la proprietà transitiva sappiamo che $(1 \sim 4) \wedge (4 \sim 2)$, quindi $(1, 2) \in G$. Analogamente, da $(0 \sim 7) \wedge (7 \sim 2) \implies (0 \sim 2)$. Infine, essendo $(3 \sim 2) \wedge (2 \sim 0) \implies (3 \sim 0) \implies (5 \sim 0)$. La parte $[2]_\sim = \{0, 1, 2, 3, 4, 5, 7\}$ risulta quindi un'unica classe di equivalenza, dalla quale resta escluso l'elemento 6. Possiamo considerare quindi due casi, e di conseguenza due relazioni di equivalenza:

- (a) Se 6 è in relazione con un elemento di $[2]_\sim$ allora $\sim_1 = \tau_A$ è la relazione totale.
- (b) Se 6 non è in relazione con alcun elemento di $[2]_\sim$ allora sarà in relazione \sim_2 solo con sé stesso.

(ii) Per il Teorema 3.5.1 esiste una applicazione biunivoca tra l'insieme $Eq(a)$ e $Partz(a)$. Si ottengono le due partizioni:

- $A/\{\sim_1\} = A/\{\tau_A\} = \{A\}$
- $A/\sim_2 = \{[2]_\sim, [6]_\sim\}$ dove $[6]_\sim = \{6\}$.

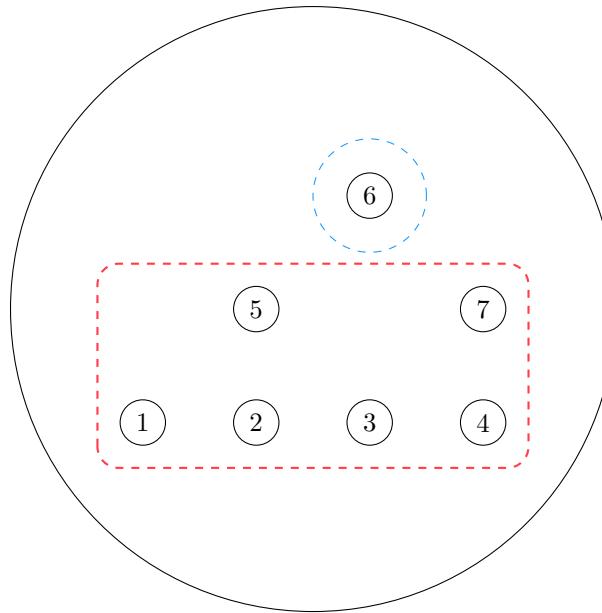


Figura 9.1: Partizione determinata dalla relazione \sim_2

Esercizio 6

Partiamo con l'osservare che $(\mathbb{Z}_{11}[x])$ è un campo. Il polinomio $(x^2 - 5)$ può essere scritto come:

$$(x^2 - 5) = (x + 4)(x - 4) = (x - 7)(x + 7)$$

In quanto $4^2 = \overline{16}_{11} = \overline{5}_{11}$ e anche $\overline{7}^2 = \overline{49}_{11} = \overline{5}_{11}$. Procediamo ora a calcolare $g(1)$ e $g(-1)$:

$$\begin{aligned} g(1) &= (\overline{1})^5 + 4(\overline{1})^2 - \overline{1} + \overline{7} = \overline{11} = \overline{0} \\ g(-1) &= (-\overline{1})^5 + 4(-\overline{1})^2 + \overline{1} + \overline{7} = \overline{11} = \overline{0} \end{aligned}$$

Quindi $(x - 1) |_{\mathbb{Z}_{11}} g$ e $(x + 1) |_{\mathbb{Z}_{11}} g$. Procediamo quindi a fattorizzare il polinomio g eseguendo la divisione lunga:

$$\begin{array}{r} x^5 + 4x^2 - x + 7 \\ \hline -x^5 + x^4 \\ \hline x^4 \\ -x^4 + x^3 \\ \hline x^3 + 4x^2 \\ -x^3 + x^2 \\ \hline 5x^2 - x \\ -5x^2 + 5x \\ \hline 4x + 7 \\ -4x + 4 \\ \hline 11 \end{array}$$

Dato che $\overline{11} = \overline{0}$ abbiamo ottenuto un divisore $g_1 = x^4 + x^3 + x^2 + 5x + 4$ che sarà divisibile per $x = -1$. Infatti, essendo $g(x) = g_1 \cdot (x - 1)$, deve valere:

$$\begin{aligned} g(-1) &= g_1(-1) \cdot (-1 - 1) \\ &= g_1(-1) \cdot (-2) = \overline{0} \\ \iff g_1(-1) &= 0 \\ \iff (x + 1) &|_{\mathbb{Z}_{11}} g_1 \end{aligned}$$

Possiamo quindi eseguire la divisione:

$$\begin{array}{r} x^4 + x^3 + x^2 + 5x + 4 \\ \hline -x^4 - x^3 \\ \hline x^2 + 5x \\ -x^2 - x \\ \hline 4x + 4 \\ -4x - 4 \\ \hline 0 \end{array}$$

Verifichiamo che g_3 sia irriducibile. Se non lo fosse dovrebbe esistere una $x \in \mathbb{Z}_{11}$ tale che $x^3 + x + 4 \equiv_{11} 0$, in particolare deve essere $x^3 + x = 7$, il quale sommato a 4, annullerebbe il polinomio. Dato che non esiste un intero $n \in \mathbb{Z}$ tale che $n^3 + n \equiv_{11} 7$, abbiamo che $g_2 = x^3 + x + 4$ è irriducibile. Otteniamo quindi la fattorizzazione:

$$f = (x + 4)(x - 4)(x^3 + x + 4)(x + 1)(x - 1)$$

- (i) Il polinomio f non è esprimibile come prodotto di sei polinomi non costanti.
- (ii) Il polinomio f non è esprimibile come prodotto di polinomi irriducibili non monici con tutti lo stesso coefficiente direttore in quanto qualsiasi coefficiente $a \neq 1$, moltiplicato ai fattori di f , restituirebbe un polinomio $a \cdot f$ diverso da f stesso.



**CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II E III)
22 APRILE 2024**

Svolgere i seguenti esercizi,

—————→ ***giustificando pienamente tutte le risposte.*** ←————

Sui fogli consegnati vanno indicati: **nome, cognome, matricola, gruppo di appartenenza.**

Non è necessario consegnare la traccia.

Esercizio 1. (i) Enunciare il teorema fondamentale sulle relazioni di equivalenza e le partizioni.

Posto $T = \{13, 24, 202, 1104, 110211\}$,

(ii) determinare il numero delle partizioni di T aventi ordine (cardinalità) 2.

(iii) Se α è la relazione di equivalenza definita in T da: per ogni $a, b \in T$,

$a \alpha b \longleftrightarrow$ la somma delle cifre di $a^{(\ddagger)}$ è uguale alla somma delle cifre di b ,
descrivere esplicitamente le classi di equivalenza di α e l'insieme quoziante T/α .

Esercizio 2. Si consideri l'applicazione $f: (a, b) \in \mathbb{N} \times \mathbb{N}^* \mapsto a^b \in \mathbb{N}$.

(i) Determinare $\vec{f}(\mathbb{N} \times \mathbb{N}^*)$, $\vec{f}(\emptyset)$, $\vec{f}(\emptyset)$, $\vec{f}(\{1\})$, $\vec{f}(\{5\})$.

(ii) Verificare se f è iniettiva, suriettiva, biettiva.

(iii) Dare la definizione di reticolo (come insieme ordinato).

Si consideri la relazione d'ordine τ definita in $\mathbb{N} \times \mathbb{N}^*$ da: $\forall a, c \in \mathbb{N} \ \forall b, d \in \mathbb{N}^*$

$(a, b) \tau (c, d) \longleftrightarrow ((a, b) = (c, d) \vee f((a, b)) \text{ è un divisore proprio di } f((c, d)))$.

(iv) Determinare in $(\mathbb{N} \times \mathbb{N}^*, \tau)$ eventuali minimo, massimo, elementi minimali, elementi massimali e verificare se $(\mathbb{N} \times \mathbb{N}^*, \tau)$ è o meno un reticolo.

Sia $M = \{(4, 1), (2, 2), (2, 3), (6, 2), (4, 2), (12, 2)\}$.

(v) Disegnare un diagramma di Hasse di (M, τ) .

(vi) Stabilire se (M, τ) è un reticolo. Se lo è decidere se è distributivo, complementato, booleano. Se non lo è determinare una coppia $(a, b) \in M$ tale che $(M \setminus \{(a, b)\}, \tau)$ sia un reticolo e decidere se questo è distributivo, complementato, booleano.

Esercizio 3. Sia $*$ l'operazione binaria definita in \mathbb{Z}_6 ponendo, per ogni $a, b \in \mathbb{Z}_6$, $a * b = \bar{3}a + \bar{4}b$.

(i) Dopo aver dato la definizione di semigruppo, verificare che $(\mathbb{Z}_6, *)$ è un semigruppo.

(ii) $(\mathbb{Z}_6, *)$ è un monoide? È commutativo?

(iii) Verificare che, in $(\mathbb{Z}_6, *)$, $\{\bar{0}, \bar{3}\}$ è una parte stabile (cioè chiusa).

Esercizio 4. Sia ρ la relazione binaria in \mathbb{Z} definita da: per ogni $a, b \in \mathbb{Z}$, $a \rho b \leftrightarrow a + b$ è dispari.

(i) Verificare che (\mathbb{Z}, ρ) definisce un grafo.

(ii) Determinare un sottoinsieme S di \mathbb{Z} tale che $|S| = 5$ e (S, ρ) definisca un albero.

Esercizio 5. Vero o falso (e perché)?

(i) In $\mathbb{Z}_{13}[x]$, un polinomio f ammette $\bar{3}$ e $\bar{5}$ come radici se e solo se f è multiplo di $x^2 - \bar{8}x + \bar{2}$.

(ii) Il polinomio $x^2 - \bar{8}x + \bar{2} \in \mathbb{Z}_{13}[x]$ è irriducibile in $\mathbb{Z}_{13}[x]$.

(iii) Il polinomio $x^2 - \bar{8}x + \bar{2} \in \mathbb{Z}_3[x]$ è irriducibile in $\mathbb{Z}_3[x]$.

(iv) Per ogni primo p , il polinomio $x^2 - \bar{8}x + \bar{2} \in \mathbb{Z}_p[x]$ è irriducibile in $\mathbb{Z}_p[x]$.

(v) Per ogni primo p , il polinomio $x^2 - \bar{8}x + \bar{2} \in \mathbb{Z}_p[x]$ è riducibile in $\mathbb{Z}_p[x]$.

(vi) Il polinomi $g = \bar{3}x^2 - \bar{11}x + \bar{6}$ e $\ell = \bar{7}x^2 + \bar{9}x - \bar{12}$ sono associati in $\mathbb{Z}_{13}[x]$ (utilizzare un'opportuna equazione congruenziale per verificarlo).

Esercizio 6. Se φ, θ e δ sono variabili proposizionali, stabilire se una, entrambe o nessuna delle seguenti è una tautologia:

(i) $(\varphi \wedge \neg(\neg\theta \vee \neg\delta)) \longleftrightarrow (\varphi \wedge \theta \wedge \delta)$;

(ii) $(\varphi \wedge \neg(\neg\theta \vee \neg\delta)) \longleftrightarrow (\varphi \wedge (\theta \vee \delta))$.

^(\ddagger)le cifre sono intese in base 10. In modo esplicito: la ‘somma delle cifre’ di a è $\sum_{i=0}^h c_i$, dove $a = \sum_{i=0}^h c_i 10^i$ per un opportuno $h \in \mathbb{N}$ e numeri naturali c_0, c_1, \dots, c_h minori di 10.

Esercizio 1

- (i) Il Teorema fondamentale su partizioni e relazioni di equivalenza afferma che esiste una corrispondenza biunivoca tra l'insieme delle partizioni di un insieme A e l'insieme delle equivalenze $Eq(A)$, cioè ogni partizione è un insieme quoziante e viceversa.
- (ii) Un insieme \mathcal{F} per essere una partizione con due elementi deve essere costituita da due parti disgiunte di T , F_3 e F_2 , tali che $|F_1| = 3$ e $|F_2| = 2$, oppure da F_1 ed F_4 con $|F_1| = 1$ ed $|F_4| = 4$. Il numero di parti di T con tre elementi è dato da:

$$\binom{5}{3} = \frac{5!}{3!2!} = 10$$

Fissati tre elementi di T a costituire una parte restano solo due elementi “liberi” per poter costituire F_2 , esistono quindi $10 \cdot 1$ possibili combinazioni tra F_2 ed F_3 per costruire una partizione di T con cardinalità 2. Il numero di parti con 4 elementi è invece dato da:

$$\binom{5}{4} = \frac{5!}{4!} = 5$$

Fissati quattro elementi di T a costituire una parte F_4 resta una sola opzione per costruire una parte di un singolo elemento. Quindi il numero totale di partizioni di cardinalità 2 è 15.

- (iii) Abbiamo:

- $1 + 3 = 4$
- $2 + 4 = 6$
- $2 + 0 + 2 = 4$
- $1 + 1 + 0 + 4 = 6$
- $1 + 1 + 0 + 2 + 1 + 1 = 6$

Quindi $T/\alpha = \{\{13, 202\}, \{24, 1104, 110211\}\}$.

Esercizio 2

- (i) Si ha:

- $\vec{f}(\mathbb{N} \times \mathbb{N}^*) = \mathbb{N}$
- $\vec{f}(\emptyset) = \emptyset$
- $\overleftarrow{f}(\emptyset) = \emptyset$
- $\overleftarrow{f}(\{1\}) = \{(1, n) \mid n \in \mathbb{N}^*\}$
- $\overleftarrow{f}(\{5\}) = \{(5, 1)\}$

- (ii) L'applicazione f non è iniettiva in quanto $f((0, 1)) = f((0, 2)) = 0$ ma $(0, 2) \neq (0, 1)$. La funzione è suriettiva in quanto per ogni $n \in \mathbb{N}$ possiamo individuare una coppia $(a, b) \in \mathbb{N} \times \mathbb{N}^*$ tale che $f((a, b)) = n$, infatti $f((n, 1)) = n^1 = n$. L'applicazione, non essendo iniettiva, non è biettiva.

- (iii) Un insieme ordinato (S, \leq) è un reticolo se, e soltanto se, per ogni parte $\{a, b\} \subseteq S$ esiste estremo inferiore ed estremo superiore.

- (iv) Il minimo di $(\mathbb{N} \times \mathbb{N}^*)$ è dato dalla coppia $(1, 1)$ in quanto, in \mathbb{N} , $f((1, 1)) = 1$ divide ogni altro naturale. Poiché non esiste alcuna coppia la cui immagine secondo f sia nulla, non esiste massimo e, avendo escluso tale valore, non esistono valori massimali in quanto ogni naturale non nullo è divisore dei suoi multipli. La struttura $(\mathbb{N} \times \mathbb{N}^*, \tau)$ non è un reticolo in quanto, prese ad esempio le coppie $\{(1, 2), (2, 1)\}$, abbiamo:

$$\{(1, 2), (2, 1)\}^\dagger = \{(2, 2), (4, 1)\}$$

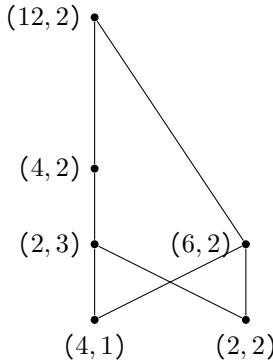
e non esiste un minimo di tale insieme, ossia non esiste un estremo superiore.

- (v) Essendo:

- $f((4, 1)) = 4^1 = 4$
- $f((2, 2)) = 2^2 = 4$

- $f((2, 3)) = 2^3 = 8$
- $f((6, 2)) = 6^2 = 36$
- $f((4, 2)) = 4^2 = 16$
- $f((12, 2)) = 12^2 = 144$

Abbiamo:



(vi) (M, τ) non è un reticolo in quanto non esiste un minimo. Eliminando la coppia $(2, 2)$ otteniamo un reticolo distributivo, complementato, e quindi booleano.

Esercizio 3

(i) Un semigruppo è una struttura (S, \perp) in cui \perp è associativa. $(\mathbb{Z}_6, *)$ è un semigruppo in quanto, per ogni terna di elementi $a, b, c \in \mathbb{Z}_6$ abbiamo:

$$\begin{aligned} a * (b * c) &= a * (3b + 4c) \\ &= 3a + 4(3b + 4c) \\ &= 3a + 12b + 16c \\ &= 3a + 4c \end{aligned}$$

e:

$$\begin{aligned} (a * b) * c &= (3a + 4b) * c \\ &= 3(3a + 4b) + 4c \\ &= 9a + 12b + 4c \\ &= 3a + 4c \end{aligned}$$

(ii) L'operazione non è commutativa, presi $a = 1$ e $b = 0$ si ha ad esempio $a * b = 1 \neq 4 = b * a$.

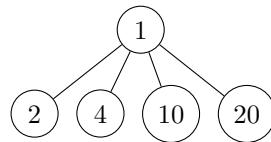
(iii) Si ha: $0 * 0 = 0$, $0 * 3 = \overline{12} = \overline{0}$, $3 * 0 = \overline{9} = \overline{3}$, $3 * 3 = 3$. Quindi $\{0, 3\}$ è stabile.

Esercizio 4

1. Essendo ρ una relazione binaria antiriflessiva e simmetrica la coppia (\mathbb{Z}, ρ) risulta essere un grafo.
2. Un albero è un grafo connesso senza circuiti. Consideriamo l'insieme $S = \{1, 2, 4, 10, 20\}$ e l'insieme dei lati:

$$L = \{(1, 2), (1, 4), (1, 10), (1, 20)\}$$

Si ottiene così il seguente albero:



Esercizio 5

(i) Siano $\overline{3}$ e $\overline{5}$ radici di f . Ciò significa che, per il teorema di Ruffini generalizzato, $(x - 3)(x - 5)$ divide f . Sviluppando $(x - 3)(x - 5)$ otteniamo il polinomio $(x^2 - 8x + 2)$, quindi f è un multiplo di $(x^2 - 8x + 2)$. Analogamente, se f è un multiplo di $(x^2 - 8x + 2)$, essendo \mathbb{Z}_{13} , le sue radici sono tutte e sole le radici dei suoi multipli. Quindi l'equivalenza è vera.

- (ii) Il polinomio $(x^2 - 8x + 2)$ non è irriducibile in quanto ammette due radici e può essere decomposto in $(x - 3)(x - 5)$;
- (iii) Il polinomio $(x^2 - 8x + 2) \in \mathbb{Z}_3$ è irriducibile in quanto non ammette radici in \mathbb{Z}_3 .
- (iv) Falso.
- (v) Falso.

- (vi) Vero, per trovare un fattore moltiplicativo che moltiplicato al coefficiente direttore di g ci dia il coefficiente direttore di l risolviamo l'equazione congruenziale $7x \equiv_{13} 3$ ottenendo $x = \bar{6}$ come risultato. Moltiplicando il polinomio l per la costante 6 otteniamo così il polinomio g :

$$\begin{aligned} 6 \cdot (7x^2 + 9x - 12) &= 42x^2 + 63x - 72 \\ &= 3x^2 - 11x + 6 \end{aligned}$$

Saremmo potuti arrivare allo stesso risultato risolvendo l'equazione congruenziale $3x \equiv_{13} 7$ che ha per soluzione $x = 11$, infatti:

$$\begin{aligned} 11 \cdot (3x^2 - 11x + 6) &= 11 \cdot (3x^2 + 3x + 6) \\ &= 33x^2 + 22x + 66 \\ &= 7x^2 + 9x - 12 \end{aligned}$$

Esercizio 6

- (i) Vero per De Morgan
- (ii) Falso



**CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II E III)
15 LUGLIO 2024**

Svolgere i seguenti esercizi,

—————→ ***giustificando pienamente tutte le risposte.*** ←————

Sui fogli consegnati vanno indicati: **nome, cognome, matricola, gruppo di appartenenza.**

Non è necessario consegnare la traccia.

Esercizio 1. Sia $A = \mathcal{P}_2(\mathbb{Z})$ l'insieme delle parti di \mathbb{Z} di cardinalità 2. Sia σ la relazione d'ordine definita da: $\forall a, b \in A$

$$a \sigma b \iff (a = b \vee \forall x \in a (\forall y \in b (x \text{ divide } y))).$$

Sia $B = \{\{0, 12\}, \{0, 16\}, \{1, 2\}, \{2, 4\}, \{2, 8\}, \{4, 6\}\}$

- (i) Disegnare un diagramma di Hasse di (B, σ) . Stabilire se (B, σ) è un reticolo e, nel caso, se è distributivo, complementato, booleano.
- (ii) Determinare un sottoinsieme C di B della cardinalità massima possibile tale che (C, σ) sia un reticolo complementato.
- (iii) Determinare in (A, σ) i minoranti di $\{\{1, 4\}\}$ e, se esistono, $\inf \{\{1, 4\}, \{1, 6\}\}$ e $\sup \{\{1, 4\}, \{1, 6\}\}$.
- (iv) Determinare, se ne esistono, gli elementi minimali, massimali, minimo, massimo in (A, σ) .
- (v) Esiste $a \in A$ tale che $(B \cup \{a\}, \sigma)$ sia un reticolo?

Esercizio 2. Stabilire per quali $c \in \{1, 3, 20, 24, 55, 60\}$ l'equazione congruenziale $470x \equiv_{350} 3c$ ha soluzioni in \mathbb{Z} e, per ciascun tale c , fornire l'insieme delle soluzioni.

Esercizio 3. Sia S un insieme tale che $|S| = 13$ e sia h un suo elemento. Indicare (ma non calcolare): (a) il numero delle parti di S di cardinalità 8; (b) il numero delle parti di S di cardinalità 18; (c) il numero delle parti T di S tali che $|T| = 7$ e $h \in T$; (d) il numero delle relazioni binarie in S .

Esercizio 4. Per ciascuno degli insiemi \mathbb{Z} , \mathbb{Z}_6 e \mathbb{Z}_3 si consideri l'operazione binaria (che indichiamo sempre con lo stesso simbolo) $*$ definita da: per ogni a, b appartenenti all'insieme, $a * b = 3a + b$. Che tipo di strutture algebriche (semigruppi, monoidi, gruppi; commutativi o no?) sono $(\mathbb{Z}, *)$, $(\mathbb{Z}_6, *)$ e $(\mathbb{Z}_3, *)$? In ciascuna di esse determinare gli eventuali elementi neutri a sinistra o a destra.

Esercizio 5. Siano $S = \mathbb{N} \setminus \{0, 1\}$ ed $f: S \rightarrow S$ l'applicazione che ad ogni $n \in S$ associa la somma $\sum_{n \geq p \in \mathbb{P}} p$ dei numeri interi primi minori o uguali a n (ad esempio, $f(4) = 2 + 3 = 5$). Sia poi \mathfrak{R} il nucleo di equivalenza di f .

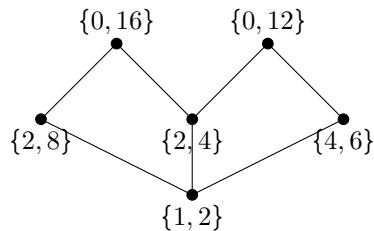
- (i) Determinare $\overleftarrow{f}(\{10\})$ e $\overleftarrow{f}(\{11\})$.
- (ii) f è iniettiva? f è suriettiva? f è biettiva?
- (iii) Elencare gli elementi di $[8]_{\mathfrak{R}}$.
- (iv) $|S/\mathfrak{R}|$ è finito o infinito?
- (v) Esiste $a \in S$ tale che $a \notin [a]_{\mathfrak{R}}$?
- (vi) Posto $T = \{n \in S \mid 10 \leq n \leq 20\}$, detta \mathfrak{R}_T la relazione di equivalenza indotta da \mathfrak{R} su T , descrivere esplicitamente le classi appartenenti a T/\mathfrak{R}_T , elencandone gli elementi. Quanto vale $|T/\mathfrak{R}_T|$?

Esercizio 6.

- (i) Quali tra queste affermazioni sono vere, e quali no, per tutte le possibili scelte di un anello commutativo unitario A , di $f \in A[x]$ e di due elementi distinti a e b di A :
 - (a) se a e b sono radici di f , allora $(x - a)$ e $(x - b)$ dividono f in $A[x]$;
 - (b) se a e b sono radici di f , allora $(x - a)(x - b)$ divide f in $A[x]$;
 - (c) se A è un campo e a e b sono radici di f , allora $(x - a)(x - b)$ divide f in $A[x]$.
- (ii) Esistono un anello commutativo unitario A ed un polinomio di grado 2 in $A[x]$ tali che f abbia infinite radici in A ?
- (iii) Sia $f \in \mathbb{Z}_{13}[x]$. Supponiamo $f = pqr$ dove p, q ed r sono polinomi irriducibili in $\mathbb{Z}_{13}[x]$, p e q hanno grado 1 e r ha grado 4. Allora, in $\mathbb{Z}_{13}[x]$,
 - (a) quanti divisori monici di grado 3 ha f ?
 - (b) quanti divisori monici di grado 2 ha f ?
 - (c) assumendo p e q non associati tra loro, quanti divisori, monici o non monici, di grado 5 ha f ?

Esercizio 1

- (i) Notiamo che $\forall x \in \mathbb{Z}(x \mid 0)$, e che $\forall x \in \mathbb{N}(1 \mid x)$. Sono incontrastabili le parti $\{2, 4\} \not\sim \{2, 8\}$ in quanto $4 \nmid 2$; $\{2, 4\} \not\sim \{4, 6\}$ poiché $4 \nmid 6$; $\{2, 8\} \not\sim \{4, 6\}$ poiché $8 \nmid 4 \wedge 8 \nmid 6$. La parte $\{1, 2\}$ precede ogni altro elemento di B . Sono incontrastabili le parti $\{0, 12\}$ e $\{0, 16\}$ in quanto $12 \nmid 16$. Vale $\{2, 4\} \sigma \{0, 16\}$, $\{2, 4\} \sigma \{0, 12\}$, $\{4, 6\} \sigma \{0, 12\}$. Si ottiene così il seguente diagramma di Hasse:



(S, σ) non è quindi un reticolo in quanto possiamo vedere che esistono in (B, σ) due elementi massimali.

- (ii) Preso $C = \{\{1, 2\}, \{2, 8\}, \{2, 4\}, \{0, 16\}\}$ di cardinalità 4 abbiamo che $0 = \min(C, \sigma) = \{1, 2\}$ e $1 = \max(C, \sigma) = \{0, 16\}$ e per ogni $x \in C(\exists y \in C(x \vee y = 1 \wedge x \wedge y = 0))$, ovvero (C, σ) è complementato.
- (iii) Abbiamo $\{\{1, 4\}\}^\perp = \{\{1, -1\}, \{1, 4\}\}$. Inoltre: $\{1, 4\} \wedge \{1, 6\} = \{1, -1\}$ mentre $\{1, 4\} \vee \{1, 6\} = \{0, 12\}$.
- (iv) Il minimo di (A, σ) è rappresentato dalla parte $\{1, -1\}$. Esistono poi infiniti elementi massimali che sono le parti del tipo $\{0, a\}$, con $a \in \mathbb{Z} \setminus \{0\}$. Una parte $\{0, a\}$, infatti, non può essere seguita da alcun elemento di A in quanto 0 non divide nessun elemento di \mathbb{Z} .
- (v) Dato che una parte del tipo $a = \{0, x\}$ è massimale in (A, σ) non è possibile inserire un elemento a tale che $(B \cup \{a\}, \sigma)$ possa diventare un reticolo.

Esercizio 2

Controlliamo per quali valori di $c \in \{1, 3, 20, 24, 55, 60\}$ l'equazione $470x \equiv_{350} 3c$ ammette soluzioni. Chiaramente deve essere $d = MCD(470, 350) \mid 3c$. Ovvero $d = 10 \mid 3c$. Vera solo per $c = 20$ e $c = 60$. Abbiamo allora:

- Sia $c = 20$, allora l'equazione diventa: $470x \equiv_{350} 60$. Dividendo tutto per 10 si ottiene l'equazione equivalente $47x \equiv 356$. È possibile scrivere $1 = MCD(47, 35)$ come combinazione lineare $1 = 47 \cdot (3) + 35 \cdot (-4)$. Moltiplicando tutto per 6 abbiamo: $6 = 47 \cdot (18) + 35 \cdot (-24)$. Quindi $x = [18]_{35}$ è una soluzione dell'equazione. Ovvero, l'insieme dei numeri interi $\{n \in \mathbb{Z} \mid n = 35k + 18\}$.
- Sia $c = 60$. L'equazione diventa: $470x \equiv_{350} 180$. Dividendo per 10 otteniamo: $47x \equiv_{35} 18$. Moltiplicando nuovamente $1 = 47 \cdot (3) + 35 \cdot (-4)$ per 18 si ha che $x = [54]_{35} = [19]_{35} = \{n \in \mathbb{Z} \mid n = 35k + 19\}$.

Esercizio 3

- (i) Il numero di 8-parti di S è dato dal calcolo del coefficiente binomiale di 13 su 8:

$$\begin{aligned}
 \binom{13}{8} &= \frac{13!}{8!(13-8)!} \\
 &= \frac{13!}{8! \cdot 5!} \\
 &= \frac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{(8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1)(5 \cdot 4 \cdot 3 \cdot 2 \cdot 1)} \\
 &= \frac{\cancel{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}}{\cancel{(8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1)}(5 \cdot 4 \cdot 3 \cdot 2 \cdot 1)} = \\
 &= \frac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} \\
 &= 1287
 \end{aligned}$$

- (ii) Non esistono parti di S di cardinalità 18.

- (iii) Fissato h in T restano da essere selezionati altri 6 elementi dall'insieme S che contiene ora $13 - 1$ elementi disponibili. Il

numero di parti di $S \setminus \{h\}$ di sei elementi è dato da:

$$\binom{12}{6} = \frac{12!}{6!(6!)} = 924$$

(iv) Una relazione binaria in S è una delle qualsiasi parti di $S \times S$, che è noto avere 13^2 elementi, ovvero 169 elementi.

Esercizio 4

Osserviamo che $*$ non è associativa in \mathbb{Z} . Infatti, presa la terna $(1, 2, 1)$ osserviamo che $(1 * 2) * 1 = 3 + 6 + 1 = 10$ mentre $1 * (2 * 1) = 9 + 6 + 1 = 16$. Possiamo quindi affermare che $(\mathbb{Z}, *)$ è un gruppoide. Stesso discorso in \mathbb{Z}_6 in quanto:

$$\forall a, b, c \in \mathbb{Z}_6 (a * (b * c) = a * (3b + c) = 3a + 9b + 3c = 3a + 3b + 3c)$$

mentre:

$$\forall a, b, c \in \mathbb{Z}_6 ((a * b) * c) = (3a + b) * c = 9a + 3b + c = 3a + 3b + c$$

Che in generale non coincidono. Al contrario, in \mathbb{Z}_3 abbiamo che:

$$\begin{aligned} (a * b) * c &= (3a + b) * c = b * c = 3b + c = c \\ a * (b * c) &= a * (3b + c) = a * c = 3a + c = c \end{aligned}$$

Quindi $(\mathbb{Z}_3, *)$ risulta essere un semigruppo. Verifichiamo quindi la commutatività in \mathbb{Z}_3 :

$$\forall a, b \in \mathbb{Z}_3 (a * b \stackrel{?}{=} b * a)$$

Abbiamo:

$$\begin{aligned} a * b &= 3a + b = b \\ b * a &= 3b + a = a \end{aligned}$$

Quindi $*$ non è commutativa. Studiamo l'eventuale esistenza di elementi neutri a sinistra o a destra. Un elemento t è neutro a sinistra se:

$$\begin{aligned} \forall x \in \mathbb{Z}_3 (t * x \equiv_3 x) &\iff \forall x \in \mathbb{Z}_3 (3t + x \equiv_3 x) \\ \forall x \in \mathbb{Z}_3 (3t \equiv_3 0) \end{aligned}$$

Trovando quindi che tutti gli elementi di \mathbb{Z}_3 risultano essere elementi neutri a sinistra. Verifichiamo l'esistenza di elementi neutri a destra. Un elemento è neutro a destra se:

$$\begin{aligned} \forall x \in \mathbb{Z}_3 (x * t \equiv_3 x) &\iff \forall x \in \mathbb{Z}_3 (3x + t \equiv_3 x) \\ \forall x \in \mathbb{Z}_3 (t \equiv_3 x) \end{aligned}$$

Dato che t , per essere neutro a destra, deve coincidere con l'elemento x col quale vogliamo comporlo per ottenere x stesso, possiamo concludere dicendo che non esiste un elemento neutro a destra. Dato che un monoide è una struttura dotata di un elemento neutro a destra e a sinistra possiamo dire che $(\mathbb{Z}_3, *)$ non è un monoide.

Esercizio 5

(i) Abbiamo:

$$\begin{aligned} \overleftarrow{f}(\{10\}) &= \{n \in S \mid f(n) = 10\} \\ &= \{n \in S \mid \sum_{p \geq n} p = 10\} \\ &= \{n \in S \mid 2 + 3 + 5 = 10 = f(n)\} \\ &= \{5, 6\} \end{aligned}$$

Analogamente:

$$\begin{aligned} \overleftarrow{f}(\{11\}) &= \{n \in S \mid f(n) = 11\} \\ &= \{n \in S \mid \sum_{p \geq n} p = 11\} = \emptyset \end{aligned}$$

Infatti nella successione delle somme $f(n)$ abbiamo:

$$\Sigma_n = (f(n))_{n \in S} = \{2, 5, 10, 17, 28, \dots\} \quad (9.8)$$

Ogni termine della successione può essere ottenuto dalla formula ricorsiva $f(n) = f(n - 1) + p_n$.

(ii) Poiché $\overleftarrow{f}(\{10\}) \geq 1$ possiamo dire che l'applicazione non è iniettiva. Analogamente, essendo $\overleftarrow{f}(\{11\}) = \emptyset$, possiamo dire che f non è suriettiva, e quindi biettiva.

(iii) Si ha:

$$[8]_{\mathfrak{R}} = \overleftarrow{f}(\{f(8)\}) = \overleftarrow{f}(\{17\}) = \{7, 8, 9, 10\}$$

(iv) Osserviamo che S/\mathfrak{R} è l'insieme delle classi di equivalenza $[n]_{\mathfrak{R}}$, ovvero partizione composta dalle parti:

$$\{\overleftarrow{f}(\{f(n)\}) \mid n \in S\} = \{\overleftarrow{f}(\{\Sigma_n\}) \mid n \in S\}$$

Dato che la successione $(\Sigma_n)_{n \in S}$ risulta essere infinita abbiamo che S/\mathfrak{R} è infinito.

(v) Abbiamo che T/\mathfrak{R}_T è composto dalle classi:

- $[10]_{\mathfrak{R}_T} = \overleftarrow{f}(\{f(10)\}) = \overleftarrow{f}(\{17\}) = \{10\}$
- $[11]_{\mathfrak{R}_T} = \overleftarrow{f}(\{f(11)\}) = \overleftarrow{f}(\{28\}) = \{11, 12\}$
- $[13]_{\mathfrak{R}_T} = \overleftarrow{f}(\{f(13)\}) = \overleftarrow{f}(\{41\}) = \{13, 14, 15, 16\}$
- $[17]_{\mathfrak{R}_T} = \overleftarrow{f}(\{f(17)\}) = \overleftarrow{f}(\{58\}) = \{17, 18\}$
- $[19]_{\mathfrak{R}_T} = \overleftarrow{f}(\{f(19)\}) = \overleftarrow{f}(\{77\}) = \{19, 20\}$

E vale $|T/\mathfrak{R}_T| = 5$.

Esercizio 6

(i) Si ha:

- (1) Vero.
- (2) Falso.
- (3) Vero.

(ii) Consideriamo l'anello booleano $(\mathbb{Z}_2, +, \cdot)$. Chiaramente, essendo ogni suo elemento idempotente, il polinomio $x^2 + x = 0$ ammette infinite radici date dalla classe di equivalenza $\bar{0}_2$.

(iii) Abbiamo:

- (a) f non ha divisori monici di grado 3;
- (b) f ha un solo divisore monico di grado 2 che è il polinomio upq associato al polinomio pq .
- (c) Un divisore di grado 5 può essere ottenuto eseguendo il prodotto tra pr o qr . Tali polinomi avranno un polinomio monico associato. Moltiplicando un divisore monico per un elemento non nullo di \mathbb{Z}_{13} otteniamo un divisore non monico, e ci sono 12 possibili moltiplicatori (elementi di \mathbb{Z}_{13}). Si ottengono quindi 24 polinomi di grado 5, monici e non monici, che dividono f .



**CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II E III)
10 SETTEMBRE 2024**

Svolgere i seguenti esercizi,

—————→ ***giustificando pienamente tutte le risposte.*** ←————

Sui fogli consegnati vanno indicati: **nome, cognome, matricola, gruppo di appartenenza.**

Non è necessario consegnare la traccia.

Esercizio 1. Decidere se la forma proposizionale $(p \Rightarrow (q \Rightarrow r)) \Leftrightarrow ((p \Rightarrow q) \Rightarrow r)$ è una tautologia.

Esercizio 2. Si consideri l'operazione binaria $*$: $(a, b) \in \mathbb{Z}_{12} \times \mathbb{Z}_{12} \mapsto a + \bar{b} \in \mathbb{Z}_{12}$.

- (i) Che tipo di struttura (semigruppo, commutativo o meno, monoide, gruppo) è $(\mathbb{Z}_{12}, *)$?
- (ii) Determinare gli insiemi D degli elementi neutri a destra e S degli elementi neutri a sinistra in $(\mathbb{Z}_{12}, *)$. $D \cup S$ è una parte stabile in $(\mathbb{Z}_{12}, *)$?
- (iii) Sia $T = \{\overline{3n} \mid n \in \mathbb{Z}\}$. T è una parte stabile in $(\mathbb{Z}_{12}, *)$? Se lo è, che tipo di struttura (semigruppo, commutativo o meno, monoide, gruppo) è $(T, *)$?
- (iv) Risolvere, determinando tutte le soluzioni in $(\mathbb{Z}_{12}, *)$, le equazioni: (a): $\bar{7} * x = \bar{1}$; (b): $\bar{5} * x = \bar{1}$.

Esercizio 3. Consideriamo la funzione:^(†)

$$\varphi: a_0 + a_1x + \cdots + a_{\deg f}x^{\deg f} \in \mathbb{Z}[x] \setminus \{0\} \longmapsto \prod_{i=0}^{\deg f} a_i \in \mathbb{Z}.$$

- (i) φ è suriettiva? È iniettiva?
- (ii) Descrivere $\overline{\varphi}(\{1, x^5 + 1\})$, $\overline{\varphi}(\{3\})$ e $\overline{\varphi}(\{2, 4\})$. Quanti polinomi irriducibili (in $\mathbb{Q}[x]$) di grado 1 contiene $\overline{\varphi}(\{3\})$?
- (iii) Sia \sim_φ il nucleo di equivalenza di φ . Se ha senso la domanda, determinare se ogni singolo elemento di $\mathbb{Z}[x]/\sim_\varphi$ è infinito.
- (iv) Dopo aver dato la definizione di polinomio associato ad un polinomio dato in un generico anello di polinomi $A[x]$, dimostrare che ad ogni elemento di $\mathbb{Z}[x]/\sim_\varphi$ appartengono almeno due polinomi (distinti) tra loro associati.

Esercizio 4. Per ogni insieme X di numeri interi, sia ρ_X la relazione binaria in X definita da:

$$\forall a, b \in X \ (a \rho_X b \iff a|7b).$$

Siano $A = \{0, 1, 2, 8, 14, 49, 88\}$ e $B = \{0, 1, 2, -3, 11, 132, 330, 49\}$ (nota bene: $132 = 2 \cdot 66$).

- (i) Spiegare perché una tra ρ_A e ρ_B è una relazione d'ordine e l'altra non lo è.

Detto S quello tra A e B tale che ρ_S sia una relazione d'ordine, e posto $\rho = \rho_S$,

- (ii) disegnare un diagramma di Hasse di (S, ρ) ;
- (iii) determinare, se esistono, $\inf_{(S, \rho)}(\{2, 49\})$ e $\sup_{(S, \rho)}(\{2, 49\})$;
- (iv) stabilire se (S, ρ) è un reticolo e, nel caso se è distributivo o complementato.

Esercizio 5. Spiegare perché, per ogni insieme non vuoto $V \subseteq \mathbb{N}^* \setminus \{1\}$ ^(‡), è ben definito il grafo (semplice) G_V su V in cui, per ogni $a, b \in V$, a e b sono adiacenti se e solo se a e b sono tra loro coprimi.

- (i) Cosa cambia se si assume, invece $V = \mathbb{N}^*$?
- (ii) Se $V = \mathbb{N}^* \setminus \{1\}$, G_V è connesso?
- (iii) Esiste $V \subseteq \mathbb{N}^* \setminus \{1\}$ tale che V non sia connesso?
- (iv) Se $V = \{2, 3, 4, 5, 6, 7, 8, 9\}$, G_V ha cammini euleriani?

^(†) $\deg f$ indica il grado del polinomio f .

^(‡) $\mathbb{N}^* := \mathbb{N} \setminus \{0\}$

Esercizio 1

Costruiamo la tavola di verità:

p	q	r	$p \Rightarrow q$	$q \Rightarrow r$	$p \Rightarrow (q \Rightarrow r)$	$(p \Rightarrow q) \Rightarrow r$
V	V	V	V	V	V	V
V	V	F	V	F	F	F
V	F	V	F	V	V	V
V	F	F	F	V	V	V
F	V	V	V	V	V	V
F	V	F	V	F	V	F
F	F	V	V	V	V	V
F	F	F	V	V	V	F

Le ultime due colonne non sono equivalenti e quindi possiamo affermare che non vale la proprietà associativa per l'implicazione.

Esercizio 2

(i) L'operazione $*$ è associativa. Presi infatti tre elementi $a, b, c \in \mathbb{Z}_{12}$ abbiamo:

$$\begin{aligned}
 a * (b * c) &= a * (b + 9c) \\
 &= a + 9(b + 9c) \\
 &= a + 9b + 81c \\
 &= a + 9b + 9c \quad (\text{In quanto } \overline{81} \equiv_{12} \overline{9})
 \end{aligned}$$

$$(a * b) * c = (a + 9b) * c = a + 9b + 9c$$

L'operazione $*$ non è commutativa, infatti presi $a = \overline{0}$ e $b = \overline{1}$ abbiamo $\overline{0} * \overline{1} = \overline{0}$ e $\overline{1} * \overline{0} = \overline{1}$. Un eventuale elemento neutro a sinistra t deve rendere vera l'uguaglianza $t * a = a$ per ogni $a \in \mathbb{Z}_{12}$, ossia:

$$\begin{aligned}
 t * a = a &\iff t + 9a = a \\
 &\iff t = -8a
 \end{aligned}$$

Quindi, dovendo t dipendere da a , possiamo concludere che non esiste un siffatto elemento neutro a sinistra. Cerchiamo ora un elemento neutro a destra. Sempre per definizione di elemento neutro a destra, per ogni $a \in \mathbb{Z}_{12}$ ($a * t = a$):

$$\begin{aligned}
 a * t = a &\iff a + 9t = a \\
 &\iff 9t = 0 \\
 &\iff t = \overline{0} \vee t = \overline{4} \vee t = \overline{8}
 \end{aligned}$$

Non esistendo un t che sia neutro sia a sinistra che a destra possiamo affermare che $(\mathbb{Z}_{12}, *)$ è un semigruppo.

(ii) Abbiamo $D = \{\overline{0}, \overline{4}, \overline{8}\}$, $S = \emptyset$. Quindi $D \cup S = D$. Verifichiamo se $D = \{\overline{4n} \mid n \in \mathbb{Z}\}$ è stabile. Siano $x = 4n$, $y = 4m \in D$, vale allora:

$$\begin{aligned}
 4n * 4m &= 4n + 9 \cdot 4m \\
 &= 4n + 36m \\
 &= 4n
 \end{aligned}$$

Quindi D è stabile.

(iii) Abbiamo $T = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$. Ogni $x \in T$ è esprimibile come $3n$ per un opportuno intero n . Siano $x = 3n$, $y = 3m \in T$, vale allora:

$$\begin{aligned}
 3n * 3m &= 3n + 9 \cdot 3m \\
 &= 3n + 27m \\
 &= 3n + 3m \\
 &= 3(n + m)
 \end{aligned}$$

Quindi T è stabile. L'operazione $*$ in T è commutativa e $\bar{0}$ risulta elemento neutro. Inoltre, per ogni $x \in T$ esiste un simmetrico x' tale che $x * x' = 0$. Infatti, posto $x = 3n$ e $x' = 3m$:

$$\begin{aligned} x * x' = 0 &\iff 3n * 3m = 0 \\ &\iff 3n + 3m = 0 \\ &\iff 3m = -3n \\ &\iff 3m = -3n + 12 \\ &\iff 3m = -3(n - 12) \\ &\iff 3m = 3(4 - n) \end{aligned}$$

Quindi $x' \in T$ e $(T, *)$ è un gruppo abeliano.

(iv) Risolviamo:

$$\begin{aligned} \bar{7} * x \equiv_{12} 1 &\iff 7 + 9x \equiv_{12} 1 \\ &\iff 9x \equiv_{12} -6 \\ &\iff 9x \equiv_{12} 6 \end{aligned}$$

Calcoliamo $(9, 12) = 3$, poiché $3 \mid 6$ abbiamo tre soluzioni non congruenti. Riduciamo l'equazione congruenziale:

$$3x \equiv_4 2$$

Dove $(3, 4) = 1$ e ovviamente $1 = 4 + 3(-1)$. Moltiplicando tale combinazione lineare otteniamo $2 = 4(2) + 3(-2)$. Quindi $x = -2 = 2$ è soluzione di tale equazione. Ritornando al modulo 12, abbiamo le tre soluzioni:

$$x = 2 + k \frac{12}{3} = 2 + 4k$$

con $0 \leq k < 3$. Sia ora:

$$\begin{aligned} 5 * x \equiv_{12} 1 &\iff 5 + 9x \equiv_{12} 1 \\ &\iff 9x \equiv_{12} -4 \\ &\iff 9x \equiv_{12} 8 \end{aligned}$$

Calcoliamo $(9, 12) = 3$, e 3 non divide 8, quindi non esistono soluzioni.

Esercizio 3

(i) La funzione φ è suriettiva. Infatti, ogni intero $n \in \mathbb{Z}$ è immagine di almeno un polinomio. Preso lo 0 ad esempio sappiamo che qualunque polinomio non completo f ha come immagine $\varphi(f) = 0$. Inoltre, preso un qualsiasi $n \in \mathbb{Z}$, questo ammette una fattorizzazione in primi $n = p_0^{\alpha_0} \cdots p_n^{\alpha_n}$ dal quale possiamo ottenere il polinomio:

$$f = p_0^{\alpha_0} + p_1^{\alpha_1}x + \cdots + p_n^{\alpha_n}x^n$$

Ed ovviamente $\varphi(f) = n$. Ovviamente stando in \mathbb{Z} , la fattorizzazione di un intero non è unica. Ad esempio $24 = (3)(2^3) = (-3)(-2)^3$ ottenendo così i due polinomi distinti, ma associati:

$$\begin{aligned} f_1 &= 3x^3 + 2x^2 + 2x + 2 \\ f_2 &= -3x^3 - 2x^2 - 2x - 2 \end{aligned}$$

e vale $\varphi(f_1) = \varphi(f_2) = 24$.

(ii) Abbiamo:

- $\vec{\varphi}(\{1, x^5 + 1\}) = \{\varphi(1), \varphi(x^5 + 0x^4 + 0x^3 + 0x^2 + 0x + 0)\} = \{1, 0\}$.
- $\overleftarrow{\varphi}(\{3\})$ è l'insieme $\{3x + 1, -3x - 1, 3, f_{n,3}\}$ dove $f_{n,3}$ è un polinomio di grado n tale che $\prod_{i=0}^{n-1} a_i = 1$ e $a_n = 3$, al variare di $n \in \mathbb{Z}$;
- $\overleftarrow{\varphi}(\{2, 4\})$ è l'insieme $\{2x + 1, -2x - 1, 2, f_{n,2}\}$ dove $f_{n,2}$ è un polinomio $\{a_n\}_{n \in \mathbb{N}}$ tale che $\prod_{i=0}^{n-1} a_i = 1$ e $a_n = 2$, unito all'insieme dei polinomi $\{4, 4x + 1, 2x + 2, -2x - 2, f_{n,4}\}$ dove $f_{n,4}$ è un polinomio $\{a_n\}_{n \in \mathbb{N}}$ e $\prod_{i=0}^{n-1} a_i = 1$ e $a_n = 4$.

In $\mathbb{Q}[x]$ il polinomio $x + 3$ ed il suo associato $(-x - 3)$ risultano essere polinomi irriducibili di primo grado appartenenti a $\overleftarrow{\varphi}(\{3\})$, così come il polinomio $(-3x - 1)$ e $(3x + 1)$.

- (iii) Per quanto osservato nei punti precedenti è ovvio che ogni classe di equivalenza $[f]_{\mathfrak{R}_\varphi}$ risulta essere infinita in quanto è sempre possibile costruire un polinomio g tale che $\varphi(g) = \varphi(f)$ sommando un termine con coefficiente 1.
- (iv) Due polinomi f e g di $A[x]$ si dicono associati se e solo se $f \mid g \wedge g \mid f$. Sempre per i punti precedenti abbiamo visto che, poiché in \mathbb{Z} non è unica la fattorizzazione, è sempre possibile costruire due polinomi associati appartenenti alla stessa classe di equivalenza.

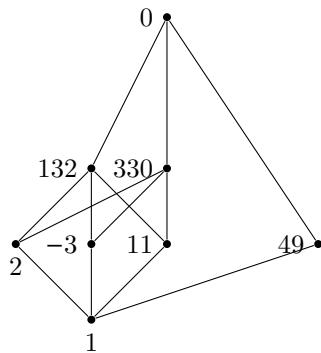
Esercizio 4

(i) La relazione ρ_A non è una relazione d'ordine in quanto $2 \rho_A 14 \wedge 14 \rho_A 2$ ma $2 \neq 14$.

(ii) Posto $\rho = \rho_B$ abbiamo:

- Ogni elemento è in relazione con 0
- L'elemento 2 è in relazione con 132, 330, 0
- L'elemento -3 è in relazione con 132, 330, 0
- L'elemento 11 è in relazione con 132, 330, 0
- L'elemento 49 è in relazione 0
- L'elemento 132 è in relazione con 0
- L'elemento 330 è in relazione 0

Quindi:



(iii) Abbiamo che $2 \wedge 49 = 1$ mentre $2 \vee 49 = 0$.

(iv) (B, ρ) è un reticolo complementato non distributivo in quanto possiamo osservare l'esistenza di un sottoreticolo isomorfo al reticolo pentagonale.

Esercizio 5

Un grafo semplice è un grafo non orientato. Una coppia $G = (V, R)$ è un grafo se e solo se V è un insieme non vuoto ed R risulta essere una relazione binaria in V tale che R sia antiriflessiva e simmetrica. Nel caso in esame la relazione in $V \subseteq \mathbb{N}^* \setminus \{1\}$ risulta essere antiriflessiva in quanto $\forall a \in V ((a, a) = a)$ e inoltre se $(a, b) = 1$ allora anche $(b, a) = 1$.

(i) Se $V = \mathbb{N}^*$ la relazione R non risulta essere antiriflessiva in quanto 1 è coprimo con se stesso.

(ii) Ogni numero non è adiacente con i suoi multipli. Preso un multiplo m di elemento $a \in \mathbb{N}^* \setminus \{1\}$ tale multiplo risulterà essere coprimo con un elemento b , coprimo con a , a meno che m non sia multiplo del minimo comune multiplo tra a e b , quindi possiamo essere. In generale, presa una fattorizzazione di m , tale numero sarà coprimo con ogni primo non appartenente alla sua fattorizzazione e tale primo sarà coprimo con ogni primo della fattorizzazione di m , quindi è sempre possibile trovare un percorso tra un numero e l'altro. Quindi G_V è connesso.

(iii) Sia $V = \{2, 3, 4, 12\}$, chiaramente 12 è un vertice isolato e quindi V non risulta essere connesso.

(iv) V non ha circuiti euleriani in quanto $\deg(5)$ non è pari.

INDICE ALFABETICO

A

Alfabeto	103
Algoritmo	
Delle divisioni successive	171
Euclideo	169
Anello	117
fattoriale	167
integro	120
Applicazione	57
Antimmagine	62
Costante	60
Immagine	61
Ridotta	61
Assioma	
Estensionalità	33
Separazione	32

B

Bertrand Russell	32
Bezout	172
Binomio di Newton	118

C

Cammino	213
Euleriano	213
Campo	121
Cayley	98
Circuito	213
Euleriano	213
Classe di equivalenza	71
Coefficiente binomiale	92
Commutatività	99
Condizione	
Necessaria	14
Sufficiente	14
Congruenza	174
Connettivi	8
Congiunzione	9
Disgiunzione	9
Disgiunzione esclusiva	9
EquivALENZA	9
Implicazione	11
Negazione	8

Contrapposizione	15
Coppia ordinata	41
Corpo	120
Corrispondente	55
Corrispondenza	55

D

De Morgan	13
Diagonale	55
Differenza	38

Distributività	100
----------------------	-----

Divisore	
banale	167
dello zero	119
proprio	167

Dominio	
a fattorizzazione unica	167
di integrità	120

E

Elemento	
Cancellabile	106
irriducibile	167
Neutro	102
Periodico	178
Simmetrico	105
Epimorfismo	114

Equazione	
Diofantea	172
Equazioni	
Congruenziali	180
Equipotenza	89
Euclide	173

F

Fattorizzazione canonica	76
Formula	
chiusa	20
Formula chiusa	8
Funzione caratteristica	91
Funzione di Eulero	179

G

Gauss	168
Grafico	55
Grafo	208
Gruppo simmetrico	111
Gruppoide	116

I

Immersione	61
Induzione	94
Insieme delle parti	35
Insieme quoziente	72
Intersezione	36
Isomorfismo	114

L

Legge	
di cancellazione	120

M

Massimo Comun Divisore	169
Matrice	119

Minimo Comune Multiplo	169
Monoide	102
Fattoriale	167
Monomorfismo	114
Multiplo	102

N

Nucleo di equivalenza	74
Numero di Bell	97

O

Occorrenza	
Libera	19
Vincolata	19
Omomorfismo	114
Operazione	
Binaria	98
Opposta	100
Operazione opposta	100

P

Parte stabile	101
Partizione	70
Periodo	177
Predicato	20
Estensione di	32
unario	20
Prodotto cartesiano	42
Proiezione canonica	73
Prolungamento	61
Proposizione	10

Q

Quantificatore	18
Esistenziale	19

Ristretto	20
Universale	18

R

Rappresentante	71
Relazione binaria	55
Relazione d'ordine	133
Relazione di equivalenza	71
Relazione opposta	56
Restrizione	61

S

Semigruppi	101
Singleton	34
Sostituzione	20
Sottoanello	119
Sottoinsieme	34
Banale	35
Proprio	35
Sottostruttura	101
Struttura	
Quoziente	174
Struttura algebrica	101

T

Tautologia	10
Terna ordinata	42
TFA	167
Traslazione	106

U

Unione	37
--------------	----

V

Venn	34
------------	----