

# Algebra

A.A. 2020-2021

Docente: A. Leone

Dispense tratte dal corso di Informatica a cura dello studente **S. Cerrone**

<b>0. Elementi di logica matematica .....</b>	<b>4</b>
0.1 Proposizioni (formule chiuse) e valori di verità .....	4
0.2 I connettivi logici principali .....	4
0.3 Tautologie .....	4
0.4 Quantificatore universale; quantificatore esistenziale .....	5
<b>1. Elementi di teoria degli insiemi .....</b>	<b>6</b>
1.1 L'insieme delle parti di un insieme $S$ .....	7
1.2 Intersezione, unione, differenza, differenza simmetrica .....	7
1.3 Prodotto cartesiano di insiemi .....	7
1.4 Operazione binaria in un insieme $S$ .....	7
1.5 Strutture algebriche principali e loro proprietà .....	8
1.6 Unione o intersezione di una famiglia di insiemi .....	9
1.7 Corrispondenze tra insiemi .....	9
1.8 Applicazioni tra insiemi .....	10
1.9 Applicazioni iniettive, suriettive, biettive .....	10
1.10 Applicazioni invertibili e loro caratterizzazione .....	10
1.11 Applicazioni composte .....	11
1.12 Proprietà caratterizzanti delle applicazioni biettive .....	12
1.13 Relazioni Binarie .....	12
1.14 Relazioni di equivalenza .....	13
1.15 Teorema fondamentale sulle relazioni di equivalenza e le partizioni .....	14
<b>2. Elementi di calcolo combinatorio .....</b>	<b>15</b>
2.1 Insiemi equipotenti .....	15
2.2 insiemi finiti e loro ordine .....	15
2.3 Coefficienti binomiali .....	16
2.4 Ordine di $\mathcal{P}S$ e principio di induzione .....	17
<b>3. Strutture Algebriche .....</b>	<b>18</b>
3.1 Operazioni su un insieme .....	18
3.2 Elementi invertibili e gruppi .....	18
3.3 Elementi non cancellabili (o regolari) .....	19
3.4 Parti chiuse in una struttura .....	19
3.5 Monoide delle parole nell'alfabeto $A$ .....	20
3.6 Sottostrutture .....	21
3.7 Potenze e multipli di un elemento .....	21
3.8 Proprietà delle potenze e dei multipli .....	22
3.9 Isomorfismo di strutture algebriche .....	22
3.10 Anelli .....	22
3.11 Divisori dello zero per un anello .....	23
3.12 Elementi invertibili in un anello unitario, campi e dominio di integrità .....	24
3.13 Sottoanello di un anello .....	24
3.14 Anelli isomorfi .....	24
3.15 Relazioni d'ordine .....	25
3.16 Diagramma di Hasse .....	26
3.17 Minimo e massimo in un insieme ordinato .....	26
3.18 Elementi minimali ed elementi massimali in un insieme ordinato .....	27
3.19 Minoranti e maggioranti .....	27
3.20 Estremo inferiore ed estremo superiore di un sottoinsieme $X$ di $S$ .....	28

<b>4. L'anello <math>\mathbb{Z}</math></b>	<b>29</b>
4.1 Elementi di aritmetica in $\mathbb{Z}$	29
4.2 Teorema fondamentale dell'aritmetica	30
4.3 Congruenze in $\mathbb{Z}$ , l'insieme delle classi resto, equazioni congruenziali	30
4.4 Massimo comun divisore e minimo comune multiplo per una coppia di interi	33
4.5 Determinazione di MCD e mcm attraverso la decomposizione in numeri primi	33
4.6 Teorema di Euclide delle divisioni successive	34
4.7 Teorema di Bezout e interi coprimi	34
4.8 L'anello degli interi modulo $m$ (anello delle classi resto)	35
4.9 Altre proposizioni sulle congruenze	36
4.10 Equazioni congruenziali	37
<b>5. Polinomi</b>	<b>40</b>
5.1 L'anello dei polinomi	40
5.2 Grado di un polinomio	40
5.3 Proposizioni sull'anello dei polinomi	41
5.4 L'anello dei polinomi a coefficienti in un campo	41
5.5 Funzione polinomiale	42
5.6 Teorema di Ruffini e sue conseguenze	43
5.7 Polinomi irriducibili	43
5.8 Teorema di fattorizzazione nell'anello dei polinomi a coefficienti in un campo	44
5.9 Criteri di irriducibilità in $\mathbb{R}x, \mathbb{Q}x$	44
<b>6. Teoria dei reticoli</b>	<b>46</b>
6.1 Reticoli	46
6.2 Reticoli come strutture algebriche a due operazioni	46
6.3 Reticoli distributivi	47
6.4 Sottoreticoli e Teorema di Birkoff	47
6.5 Reticoli limitati	48
6.6 Reticoli complementati	48
6.7 Reticoli Booleani e Teorema di Stone	49
6.8 Algebra di Boole e anelli booleani	49
6.9 Esercizi sui reticoli: Cheat	50
<b>7. Elementi di teoria dei grafi</b>	<b>51</b>
7.1 Grafi (semplici non orientati)	51
7.2 Isomorfismi tra grafi e sottografi	51
7.3 Grado di un vertice e numero dei lati in un grafo finito	51
7.4 Cammini e grafi connessi	52
7.5 Foreste e Alberi	52
7.6 Teoremi di caratterizzazione degli alberi (solo enunciati)	52

## 0. Elementi di logica matematica

Il linguaggio, in questo caso, serve per comunicare una qualunque teoria matematica. È costituito da due elementi: simboli propri del linguaggio (es. variabili, costanti, operazioni, relazioni etc...) e regole sintattiche che dicono quali stringhe di simboli abbiano senso. Quest'ultime verranno chiamate formule.

### 0.1 Proposizioni (formule chiuse) e valori di verità

Le proposizioni sono formule ben formate per le quali ha senso dire se sono vere o false. Quando parto da due formule chiuse (una formula è chiusa se non compaiono variabili libere), la risultante è sempre una formula chiusa, la quale, quindi, è sempre possibile definire se sia vera o falsa. Questo vero e falso prende il nome di valore di verità, rappresentabile nelle tabelle di verità come quella in figura.

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

Una proposizione formata da una ed una sola proposizione si dice atomica, mentre, prende il nome di proposizione composta una proposizione formata da due o più proposizioni atomiche.

### 0.2 I connettivi logici principali

Tra i simboli logici appaiono di regola i seguenti (alcuni) connettivi proposizionali:

- **Negazione**  $\neg$  NOT  
Connettivo unario che rappresenta la negazione della proposizione. (es. se  $p$  è vera allora  $\neg p$  è falsa)
- **Disgiunzione**  $\vee$  OR  
Date due proposizioni  $p$  e  $q$  la disgiunzione  $p \vee q$  è falsa se e solo se entrambe le proposizioni sono false, in tutti i restanti casi sarà vera. (es. se  $p$  è falsa e  $q$  è vera allora  $p \vee q$  è vera)
- **Congiunzione**  $\wedge$  AND  
Date due proposizioni  $p$  e  $q$  la congiunzione  $p \wedge q$  è vera se e solo se entrambe le proposizioni sono vere.
- **Doppia implicazione** o equivalenza  $\Leftrightarrow$   
Se  $p$  e  $q$  sono proposizioni,  $p \Leftrightarrow q$  (che viene letta come “ $p$  se e solo se  $q$ ”, oppure “ $p$  equivale a  $q$ ”) è vera se  $p$  e  $q$  hanno lo stesso valore di verità, falsa altrimenti.
- **Implicazione**  $\Rightarrow$   
La formula  $p \Rightarrow q$  (dove  $p$  e  $q$  sono proposizioni) è vera sempre tranne che nel caso in cui  $p$  (che si chiama antecedente dell'implicazione) è vero e  $q$  (che si chiama conseguente dell'implicazione) è falso. Sinteticamente, possiamo dire che una implicazione è vera precisamente quando il suo antecedente è falso o il suo conseguente è vero. Praticamente  $p$  è condizione sufficiente per  $q$ , mentre  $q$  è condizione necessaria per  $p$ . I modi più comuni per leggere l'implicazione sono: “se  $p$  allora  $q$ ”, “ $p$  implica  $q$ ”.

Al fine di rendere più chiari i precedenti concetti si riportano di seguito le varie tabelle di verità:

negazione		disgiunzione		congiunzione		equivalenza		implicazione					
$p$	$\neg p$	$p$	$q$	$p \vee q$	$p$	$q$	$p \wedge q$	$p$	$q$	$p \Leftrightarrow q$	$p$	$q$	$p \Rightarrow q$
V	F	V	V	V	V	V	V	V	V	V	V	V	V
V	F	V	F	V	V	F	F	V	F	F	V	F	F
F	V	F	V	V	F	V	F	F	V	F	F	V	V
		F	F	F	F	F	F	F	F	V	F	F	V

### 0.3 Tautologie

Consideriamo una forma proposizionale  $\varphi$  formata da due o più variabili, se attribuiamo un valore di verità (Vero o Falso) a ciascuna delle variabili in  $\varphi$  possiamo calcolare il valore di verità di  $\varphi$  in funzione di quelli attribuiti alle sue variabili. Si dice che  $\varphi$  è una tautologia se e solo se il valore di verità di  $\varphi$  così calcolato è Vero, indipendentemente dai valori attribuiti alle variabili che appaiono in  $\varphi$ . In altri termini,  $\varphi$  è una tautologia se e solo se, nella tavola di verità che la descrive, la colonna intestata da  $\varphi$  contiene esclusivamente Vero. Alcuni esempi banali di tautologie sono le forme “ $p \Rightarrow p$ ” e “ $p \Leftrightarrow p$ ”.

Proprietà dei connettivi date attraverso tautologie. Siano  $p, q, r$  proposizioni:

- **Proprietà di idempotenza**

1)  $p \Leftrightarrow p \vee p$

2)  $p \Leftrightarrow p \wedge p$

NON VALE  $p \Leftrightarrow (p \Leftrightarrow p)$

A volte conviene sostituire  $p$  con  $p \vee p$  o  $p \wedge p$  e viceversa.

- **Proprietà commutativa**

3)  $p \vee q \Leftrightarrow q \vee p$

4)  $p \wedge q \Leftrightarrow q \wedge p$

5)  $(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p)$  non vale per  $(p \Rightarrow q) \Leftrightarrow (q \Rightarrow p)$

- **Proprietà associativa**

6)  $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$

7)  $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$

8)  $((p \Leftrightarrow q) \Leftrightarrow r) \Leftrightarrow (p \Leftrightarrow (q \Leftrightarrow r))$  non vale per il connettivo  $\Rightarrow$

- **Distributività di  $\vee$  rispetto  $\wedge$**

9)  $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

- **Distributività di  $\wedge$  rispetto  $\vee$**

10)  $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$

- **Relazioni di De Morgan**

11)  $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$

12)  $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$

Tautologie legate all'implicazione, siano  $p, q, r$  proposizioni. Allora:

- **Implicazione come disgiunzione**

$(p \Rightarrow q) \Leftrightarrow \neg p \vee q$

- **Legge di contrapposizione**

$(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$

- **Negazione dell'implicazione**

$\neg(p \Rightarrow q) \Leftrightarrow (p \wedge \neg q)$

- **Transitività dell'implicazione**

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

**Metodi della doppia implicazione:**

1) Se  $p$  e  $q$  sono proposizioni allora la seguente è una tautologia:  $(p \Leftrightarrow q) \Leftrightarrow (p \Rightarrow q) \wedge (q \Rightarrow p)$ .

Quindi per dimostrare che due proposizioni sono equivalenti basta verificare le due implicazioni.

2) Negazione di " $p \Leftrightarrow q$ ":

○  $\neg(p \Leftrightarrow q) \Leftrightarrow ((p \wedge \neg q) \vee (\neg p \wedge q))$

○  $\neg(p \Leftrightarrow q) \Leftrightarrow (\neg p \Leftrightarrow q)$

○  $\neg(p \Leftrightarrow q) \Leftrightarrow (p \Leftrightarrow \neg q)$

**ESERCIZIO:** scrivere le tabelle di verità delle precedenti proprietà e verificarne la validità.

## 0.4 Quantificatore universale; quantificatore esistenziale

Il **quantificatore universale** indica che tutti gli elementi dell'insieme che stiamo considerando possiedono una determinata caratteristica. Si indica con  $\forall$  e si legge "per ogni".

Il **quantificatore esistenziale** indica che almeno un elemento dell'insieme che stiamo considerando possiede una specifica caratteristica. Si usa  $\exists$  per dire che esiste, mentre se è anche unico usiamo  $\exists!$ , rispettivamente si leggono "esiste" ed "esiste un unico".

Una variabile  $x$  si dice vincolata se è introdotta da un quantificatore, altrimenti è una variabile libera.

# 1. Elementi di teoria degli insiemi

Si dirà **insieme** una collezione qualunque di oggetti. Generalmente gli insiemi li chiameremo con lettere maiuscole e gli oggetti degli insiemi con lettere minuscole. Gli insiemi possono essere descritti per elencazione  $A = \{1, 2, 3\}$  (l'ordine e le ripetizioni non sono rilevanti) o per proprietà caratteristica  $A = \{x|x \in \mathbb{Q}\}$ , oppure tramite i diagrammi di Eulero Venn. Preso un oggetto qualunque, se non è possibile dire che esso appartiene o non appartiene ad  $A$  allora  $A$  non è un insieme. Se indichiamo con  $\varphi$  una proprietà, allora l'insieme  $A = \{x|\varphi(x)\}$  è costituito dagli oggetti per cui  $\varphi$  è viva. Se  $S$  è un insieme, qualunque sia la proprietà  $\varphi$ ,  $A = \{x \in S|\varphi(x)\}$  è sempre un insieme.

Simboli insiemistica	Come si legge	Funzionalità
$\emptyset$	Insieme vuoto	Indica un insieme privo di elementi
$\mathbb{N}$	Insieme dei numeri naturali	Indica l'insieme dei numeri naturali
$\mathbb{Z}$	Insieme dei numeri interi relativi	Indica l'insieme dei numeri interi relativi
$\mathbb{Q}$	Insieme dei numeri razionali	Indica l'insieme dei numeri razionali relativi
$\mathbb{R}$	Insieme dei numeri reali	Indica l'insieme dei numeri reali
$\mathbb{C}$	Insieme dei numeri complessi	Indica l'insieme dei numeri complessi
$\in$	Appartiene	Specifica che un elemento appartiene ad un insieme
$\notin$	Non appartiene	Specifica che un elemento non appartiene ad un insieme
$  $	Cardinalità	Rappresenta la cardinalità di un insieme
$\cup$	Unione	Indica l'unione tra insiemi
$\cap$	Intersezione	Denota l'intersezione tra insiemi
$\subset$	Sottoinsieme proprio di	Specifica che un insieme è un sottoinsieme proprio di un altro insieme
$\subseteq$	Sottoinsieme di	Indica che un insieme è sottoinsieme di un altro insieme e che, eventualmente, i due insiemi possono coincidere
$\supset$	Contiene	Specifica che un insieme contiene un altro insieme
$\supseteq$	Contiene impropriamente	Specifica che un insieme contiene un altro insieme e che, eventualmente, i due insiemi possono coincidere
$\setminus$	Meno	Denota la differenza tra insiemi
$\Delta$	Differenza simmetrica	Indica la differenza simmetrica tra insiemi
$\times$	Prodotto cartesiano	Rappresenta il prodotto cartesiano tra insiemi
$\bar{A}$	Complementare dell'insieme A	Denota l'insieme complementare di un insieme rispetto al suo insieme universo U
$P(A)$	Insieme delle parti di A	Indica l'insieme delle parti di un dato insieme A

Concetti fondamentali:

- **Inclusione tra insiemi  $\subseteq$ :**  
Siano  $A, B$  insiemi. Diremo che  $B$  è incluso o contenuto in ( oppure sottoinsieme di)  $A$ . Se ogni elemento di  $B$  è anche elemento di  $A$ .
- **Proprietà transitiva dell'inclusione:**  
Siano  $A, B, C$ . Se  $A \subseteq B$  e  $B \subseteq C$  allora  $A \subseteq C$ .  
Dimostrazione: Sia  $a \in A$  allora  $a \in B$  essendo  $A \subseteq B$ , allo stesso modo  $a \in C$  essendo  $B \subseteq C$  e di conseguenza  $A \subseteq C$  essendo  $a$  elemento di  $A$
- **Uguaglianza tra insiemi  $=$ :**  
Siano  $A, B$  insiemi. Diremo che  $A = B$  se sono formati dagli stessi oggetti. Quindi ogni elemento di  $A$  appartiene a  $B$  ed ogni elemento di  $B$  appartiene ad  $A$  ovvero  $A \subseteq B$  e  $B \subseteq A$
- **Inclusione stretta  $\subset$ :**  
Siano  $A, B$  insiemi. Diremo che  $B$  è incluso strettamente in (o sottoinsieme proprio di)  $A$  se e soltanto se  $B \subseteq A$  e  $B \neq A$ .
- **Singleton di un elemento:**  
Se  $a$  è un elemento, l'insieme  $\{a\}$  costituito dal solo  $a$  prende il nome di singleton di  $a$ .

## 1.1 L'insieme delle parti di un insieme $S$

Supponiamo che  $S$  sia l'insieme, con  $\mathcal{P}(S) = \{X | X \subseteq S\}$  (l'insieme dei sottoinsiemi di  $S$ ); indichiamo l'insieme delle parti di  $S$ . È un insieme composto sempre dall'insieme vuoto e poi da tutti i possibili sottoinsiemi.

Esempio:  $S = \{a, 2, \&\}$  allora  $\mathcal{P}(S) = \{\emptyset, \{a\}, \{2\}, \{\&\}, \{a, 2\}, \{a, \&\}, \{2, \&\}, \{a, 2, \&\}\}$ .

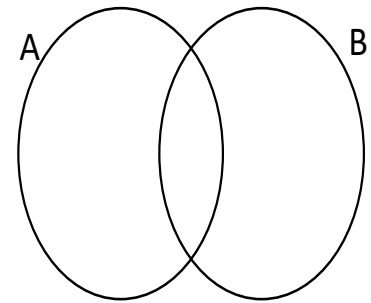
È possibile determinare il numero di oggetti di  $\mathcal{P}(S)$  dalla formula  $|\mathcal{P}(S)| = 2^n$ , dove  $n$  è il numero di oggetti dell'insieme  $S$ . La dimostrazione è evidente per il principio di induzione (trattata successivamente).

## 1.2 Intersezione, unione, differenza, differenza simmetrica

Siano  $A, B$  due insiemi rappresentati come in figura, definiamo l'insieme  $A \cap B$  ( $A$  intersezione  $B$ ) che rappresenta gli oggetti che stanno sia in  $A$  che in  $B$ .  $A \cap B = \{x | x \in A \wedge x \in B\}$ .

$A \cup B$  ( $A$  unione  $B$ ) che rappresenta tutto l'insieme, ovvero:  $A \cup B = \{x | x \in A \vee x \in B\}$  (o inclusivo).

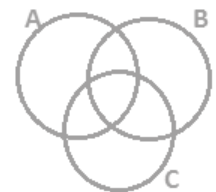
$A \setminus B$  ( $A$  meno  $B$ ) rappresenta la differenza tra insiemi, in particolare  $A \setminus B = \{x | x \in A \wedge x \notin B\}$ . A differenza delle precedenti definizioni qui l'ordine è importante, poiché  $A \setminus B \neq B \setminus A$ .



$A \Delta B$  ( $A$  delta  $B$ ) rappresenta la differenza simmetrica e si legge  $A$  unione disgiunta  $B$  o differenza simmetrica tra  $A$  e  $B$ . Questo insieme è costituito dagli oggetti che appartengono esclusivamente ad  $A$  ed esclusivamente a  $B$ , ovvero:  $A \Delta B = \{x | (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$ .

Evidentemente se  $A, B$  appartengono a  $\mathcal{P}(S)$  allora tutti i precedenti insiemi descritti (intersezione, unione, differenza, differenza simmetrica) appartengono ancora a  $\mathcal{P}(S)$ . Per operazioni tra più insiemi è utile la rappresentazione tramite i diagrammi di Eulero Venn.

Esercizio: verificare tramite i diagrammi di Eulero Venn come siano fatti l'insieme  $A \cap (B \Delta C)$  e l'insieme  $(A \cap B) \Delta (A \cap C)$ . Consiglio: disegnare gli insiemi in modo più generale possibile, come nella figura a destra. Soluzione: I due insiemi saranno uguali.



## 1.3 Prodotto cartesiano di insiemi

Dati degli oggetti  $a$  e  $b$  si definisce coppia ordinata di prima coordinata  $a$  e seconda coordinata  $b$  l'oggetto  $(a, b)$ , a differenza degli insiemi qui l'ordine è rilevante; dunque, due coppie saranno uguali solo se hanno coordinate uguali:  $(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d$ . Questo concetto si può estendere ad una terna, etc...

Dati due insiemi  $A$  e  $B$ , si dice **prodotto cartesiano** di  $A, B$  l'insieme di tutte le coppie che posso costruire con la prima coordinata in  $A$  e la seconda in  $B$ :  $A \times B = \{(a, b) | a \in A \wedge b \in B\}$ . Nota:  $A \times B \neq B \times A$ .

## 1.4 Operazione binaria in un insieme $S$

Siano  $A, B \neq \emptyset$  due insiemi, un'applicazione (o funzione)  $f$  di  $A$  in  $B$  fa corrispondere ad ogni elemento di  $A$  uno ed un solo elemento di  $B$ , in simboli  $f: a \in A \rightarrow f(a) \in B$

Si dice **operazione** definita in  $S$  ogni applicazione  $f$  che va dal prodotto cartesiano  $S \times S$  in  $S$ :  $f: S \times S \rightarrow S$

Se in un insieme  $S$  è definita una operazione  $*$ , la coppia  $(S, *)$  si dice **struttura algebrica**.

Sia  $*$  una operazione definita in  $S$ :

- \* si dice **commutativa** se per ogni  $a, b \in S$  risulta  $a * b = b * a$
- \* si dice **associativa** se comunque presi  $a, b, c \in S$  risulta  $a * (b * c) = (a * b) * c$
- \* ha **elemento neutro**  $\varepsilon \in S$  se comunque si considera  $a \in S$  avrò  $a * \varepsilon = a = \varepsilon * a$

## 1.5 Strutture algebriche principali e loro proprietà

**Struttura algebrica  $(\mathcal{P}(S), \cup)$ :** l'unione è il tipo di operazione  $\cup: (A, B) \in \mathcal{P}(S) \times \mathcal{P}(S) \rightarrow A \cup B \in \mathcal{P}(S)$  quindi, essendo la definizione di unione  $A \cup B = \{x | x \in A \vee x \in B\}$ , un elemento non appartiene ad  $A \cup B$  se (applicando le formule di De Morgan)  $x \notin A \wedge x \notin B$ .

Siano  $A, B, C$  elementi di  $\mathcal{P}(S)$  si hanno le seguenti proprietà:

- Commutativa:  $A \cup B = B \cup A$
- Associativa:  $(A \cup B) \cup C = A \cup (B \cup C)$
- Gode di elemento neutro, rappresentato dall'insieme vuoto  $\emptyset$ , infatti  $\forall X \in \mathcal{P}(S), X \cup \emptyset = X$
- Idempotenza:  $A \cup A = A$
- $A \cup B$  ha le seguenti proprietà che lo caratterizzano:
  - $A, B \subseteq A \cup B$
  - Se  $T \in \mathcal{P}(S)$  contiene  $A$  e  $B$  allora contiene anche  $A \cup B$

**Struttura algebrica  $(\mathcal{P}(S), \cap)$ :** l'intersezione è un'operazione in  $\mathcal{P}(S)$  che agisce nel modo seguente  $\cap: (X, Y) \in \mathcal{P}(S) \times \mathcal{P}(S) \rightarrow X \cap Y \in \mathcal{P}(S)$ . Ricordando che  $x \in X \cap Y \Leftrightarrow x \in X \wedge x \in Y$  la sua negazione diventa  $x \notin X \cap Y$  se e solo se  $x \notin X \vee x \notin Y$ . Sia  $A, B, C \in \mathcal{P}(S)$  si hanno le seguenti proprietà:

- Commutativa:  $A \cap B = B \cap A$
- Associativa:  $(A \cap B) \cap C = A \cap (B \cap C)$
- Gode di elemento neutro, rappresentato dall'insieme  $S$ , infatti  $\forall X \in \mathcal{P}(S), X \cap S = X$
- Idempotenza:  $A \cap A = A$
- $A \cap B = A \Leftrightarrow A \subseteq B$

Concetto di distributività per due operazioni: Sia  $(S, *, \perp)$  una struttura algebrica a due operazioni,  $*$  si dice distributiva a destra rispetto a  $\perp$  se e solo se considerati  $a, b, c \in S$  risulta  $(a \perp b) * c = (a * c) \perp (b * c)$ , mentre  $*$  si dice distributiva a sinistra rispetto a  $\perp$  se presi  $a, b, c \in S$  risulta  $a * (b \perp c) = (a * c) \perp (b * c)$ . Di conseguenza  $*$  si dirà distributiva rispetto a  $\perp$  se è distributiva sia a destra che a sinistra. Se l'operazione  $*$  è commutativa, per dimostrare la sua distributività basta verificare che lo sia solo a sinistra o solo a destra.

**Struttura algebrica  $(\mathcal{P}(S), \cup, \cap)$ :** Siano  $A, B, C \in \mathcal{P}(S)$  valgono le seguenti proprietà:

- Distributività di  $\cup$  rispetto  $\cap$ :  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$   
Essendo l'unione una operazione che gode della commutatività verifichiamo solamente che sia distributiva rispetto l'intersezione a sinistra:  $A \cup (B \cap C) = \{x | x \in A \vee x \in B \cap C\} = \{x | x \in A \vee (x \in B \wedge x \in C)\}$ ; posto  $p = x \in A, q = x \in B, r = x \in C$  avremo una proposizione nella forma  $p \vee (q \wedge r)$ , che per la distributività di  $\vee$  rispetto a  $\wedge$  sarà  $(p \vee q) \wedge (p \vee r)$  ovvero  $\{x | (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)\} = \{x | x \in A \cup B \wedge x \in A \cup C\} = (A \cup B) \cap (A \cup C)$ .
- Distributività di  $\cap$  rispetto  $\cup$ :  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

**ESERCIZIO:** dimostrare questa proprietà con i diagrammi di Eulero Venn

Connettivo XOR: rappresentato dal simbolo  $\dot{\vee}$  ci permette di costruire a partire dalle proposizioni  $p, q$ , la proposizione  $p \dot{\vee} q$  ( $p$  XOR  $q$ ) che è vera solo quando  $p \neq q$ , ovvero equivale logicamente a  $\neg(p \Leftrightarrow q)$ . Di conseguenza  $p \dot{\vee} q \Leftrightarrow \neg(p \Leftrightarrow q)$  è una tautologia; così come  $p \dot{\vee} q \Leftrightarrow (p \wedge \neg q)$ . Il connettivo XOR gode della proprietà associativa:  $(p \dot{\vee} q) \dot{\vee} r \Leftrightarrow p \dot{\vee} (q \dot{\vee} r)$

**Struttura algebrica  $(\mathcal{P}(S), \Delta)$ :**  $A \Delta B = \{x | (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$  si può anche scrivere grazie al connettivo XOR come  $A \Delta B = \{x | x \in A \dot{\vee} x \in B\}$ . La differenza simmetrica gode delle seguenti proprietà, siano  $A, B, C \in \mathcal{P}(S)$ :

- Commutativa:  $A \Delta B = B \Delta A$
- Associativa:  $(A \Delta B) \Delta C = A \Delta (B \Delta C)$  (che si dimostra facilmente grazie all'ausilio del connettivo XOR)
- Gode di elemento neutro, rappresentato da  $\emptyset$ , infatti  $A \Delta \emptyset = A = \emptyset \Delta A$
- $A \Delta A = \emptyset$



Distributività di  $\cap$  rispetto a  $\Delta$ :  $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$  cosa che non vale per l'unione.

**Struttura algebrica**  $(\mathcal{P}(S), \setminus)$ :  $\forall A, B \in \mathcal{P}(S), A \setminus B = \{x | x \in A \wedge x \notin B\}$ ; siano  $A, B \in \mathcal{P}(S)$  la struttura ha le seguenti proprietà:

- $A \setminus A = \emptyset$
- $A \setminus \emptyset = A$
- $\emptyset \setminus A = \emptyset$  } (così ho dimostrato anche la non commutatività)
- $A \setminus (A \setminus A) = A$
- $(A \setminus A) \setminus A = \emptyset$  } (non associativa)
- Se  $S \neq \emptyset$  non esiste elemento neutro per  $\mathcal{P}(S)$ , infatti  $S \setminus \emptyset = S \neq \emptyset \setminus S = \emptyset$
- $A = (A \setminus B) \cup (A \cap B)$  mentre  $(A \setminus B) \cap (A \cap B) = \emptyset$
- La differenza  $S \setminus A$  è detta complemento (insiemistico) di  $A$  in  $S$  che ha in sé le seguenti proprietà:
  - $S = A \cup (S \setminus A)$  (insieme più grande possibile)
  - $A \cap (S \setminus A) = \emptyset$  (insieme più piccolo possibile)
- $S \setminus A$  è il sottoinsieme di  $S$  che unito ad  $A$  ci dà tutto  $S$  e intersecato ad  $A$  non ha elementi in comune.
- La differenza  $S \setminus A$  è distributiva a destra rispetto a intersezione e unione, ma non è distributiva a sinistra rispetto unione e intersezione; valgono infatti le seguenti uguaglianze (**Leggi di De Morgan**):  $\forall A, B, C \in \mathcal{P}(S)$ :

$$1) A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$$

**ESERCIZIO:** Dimostrare l'uguaglianza con Eulero Venn o con il metodo usato in seguito.

$$2) A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$$

**Dimostrazione:**  $(A \setminus B) \cup (A \setminus C) = \{x | x \in (A \setminus B) \vee x \in (A \setminus C)\} = \{x | (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C)\} = \{x | x \in A \wedge (x \notin B \vee x \notin C)\} = \{x | x \in A \wedge \neg(x \in B \wedge x \in C)\} = \{x | x \in A \wedge x \notin (B \cap C)\} = A \setminus (B \cap C)$

## 1.6 Unione o intersezione di una famiglia di insiemi

Siano  $A_1, A_2, A_3, A_4$  quattro insiemi, l'insieme  $A_1 \cup A_2 \cup A_3 \cup A_4 = \{x | x \in A_1 \vee x \in A_2 \vee x \in A_3 \vee x \in A_4\}$  (che è possibile scrivere senza usare le parentesi poiché vale la proprietà associativa sia per  $\cup$  che per  $\vee$ ) può essere scritto come  $\{x | \exists i \in \{1, 2, 3, 4\}: x \in A_i\}$ . Similmente, l'intersezione dei quattro insiemi sarà l'insieme  $A_1 \cap A_2 \cap A_3 \cap A_4 = \{x | x \in A_1 \wedge x \in A_2 \wedge x \in A_3 \wedge x \in A_4\} = \{x | \forall i \in \{1, 2, 3, 4\}: x \in A_i\}$ . Questi concetti possono essere estesi ad infiniti elementi prendendo come insieme  $I = \{1, 2, 3, 4\}$  tutto  $\mathbb{N}$ , quindi definiremo un insieme che  $\forall n \in \mathbb{N} = I$  sia  $A_n = \{x \in \mathbb{N}: x \geq n\}$  (il concetto vale per qualsiasi insieme, non solo  $\mathbb{N}$ ). Definiamo quindi l'unione degli  $A_i$  per  $x \in I$  e l'intersezione degli  $A_i$  per  $x \in I$ , rispettivamente, con i simboli:

$$\bigcup_{i \in I} A_i = \{x | \exists x \in I (x \in A_i)\}; \quad \bigcap_{i \in I} A_i = \{x | x \in I (x \in A_i)\}$$

**Esempio con  $I = \mathcal{P}(S)$ :**  $\forall X \in \mathcal{P}(S)$  poniamo  $A_X = \{Y \in \mathcal{P}(S) | Y \supseteq X\}$  avremo che:

$$\bigcup_{X \in \mathcal{P}(S)} A_X = \mathcal{P}(S), \text{ mentre, } \bigcap_{X \in \mathcal{P}(S)} A_X = S$$

Definiamo una famiglia di insiemi l'insieme  $((A_i))_{i \in I} = \mathcal{F}$ . Sia  $\mathcal{F}$  un insieme di insiemi (gli oggetti di  $\mathcal{F}$  sono insiemi) possiamo definirne l'unione e l'intersezione di tutti gli elementi di  $\mathcal{F}$ : l'unione degli  $x$  per gli  $X \in \mathcal{F}$  si definisce come  $\bigcup_{X \in \mathcal{F}} X = \{x | \exists X \in \mathcal{F} (x \in X)\}$  mentre l'intersezione degli  $x$  per  $X \in \mathcal{F}$  sarà  $\bigcap_{X \in \mathcal{F}} X = \{x | \forall X \in \mathcal{F} (x \in X)\}$ .

## 1.7 Corrispondenze tra insiemi

Se  $A, B$  sono insiemi, si dice corrispondenza di  $A$  in  $B$  una terna  $(A, B, \rho)$  dove  $\rho \subseteq A \times B$ . Di conseguenza  $\forall a \in A, \forall b \in B$  se la coppia  $(a, b) \in \rho$  definisco  $a \rho b$  la coppia  $(a, b)$  scelta fra le coppie di  $\rho$  e dirò che  $a$  e  $b$  sono in corrispondenza mediante  $\rho$ . È possibile descrivere  $\rho$  dando una condizione necessarie e sufficiente affinché  $a$  sia in relazione con  $b$  come ad esempio:  $\forall a \in A, \forall b \in B, a \rho b \Leftrightarrow a \geq b$ .

## 1.8 Applicazioni tra insiemi

Una corrispondenza  $\rho$  di  $A$  in  $B$  si dirà una **applicazione di  $A$  in  $B$**  se e solo se  $\forall a \in A, \exists! b \in B (a\rho b)$ , questo significa che ogni elemento di  $A$  ha uno ed un solo corrispondente in  $B$ .  $b$  si dirà **immagine** di  $a$  (secondo  $\rho$ ) e si scrive  $b = \rho(a)$ . Se  $\rho$  è una applicazione di  $A$  in  $B$  si scrive  $\rho: a \in A \rightarrow \rho(a) \in B$  ( $\rho$  è l'applicazione che ad  $a \in A$  associa  $\rho(a) \in B$ ) o semplicemente  $\rho: A \rightarrow B$ .  $A$  è detto **dominio** di  $\rho$ ,  $B$  **codominio** di  $\rho$ , mentre  $\rho(\subseteq A \times B)$  è detto **grafico** dell'applicazione.

- **Applicazioni uguali:** siano  $(A, B, \rho)$  e  $(\bar{A}, \bar{B}, \bar{\rho})$  applicazioni. Queste sono uguali se hanno uguali dominio, codominio e grafico, ovvero se  $A = \bar{A}, B = \bar{B}, \rho = \bar{\rho}$ .
- **Identità di  $A$ :** sia  $A$  un insieme non vuoto, si dirà identità di  $A$  l'applicazione  $i_A: a \in A \rightarrow a \in A$ .
- **Immersione di  $A$  in  $B$ :** siano  $A, B \neq \emptyset$  con  $A \subseteq B$ , definisco immersione di  $A$  in  $B$  la seguente applicazione  $j_{A,B}: a \in A \rightarrow a \in B$ .
- **Applicazioni costanti:** siano  $A, B \neq \emptyset$  con  $\bar{b} \in B$  consideriamo l'applicazione  $f_{\bar{b}}: a \in A \rightarrow \bar{b} \in B$ , essa è detta applicazione costante poiché associa ogni elemento di  $a$  a  $\bar{b}$ , quindi un'applicazione  $f$  sarà costante se e solo se  $\forall x, y \in A, f(x) = f(y)$ .
- Consideriamo un'applicazione  $f: A \rightarrow B$  ed un sottoinsieme  $X \subseteq A$ ; definisco l'insieme delle immagini  $f(X)$  con  $x \in X$  come  $\vec{f}(X) = \{f(x) | x \in X\}$  che è detto **immagine** di  $X$ .
- Sia  $f: A \rightarrow B$  un'applicazione,  $\forall Y \subseteq B$  definisco  $\tilde{f}(Y) = \{x \in A | f(x) \in Y\} \subseteq A$ , questo insieme  $\tilde{f}(Y)$  è conosciuto come **controimmagine** di  $Y$ , oppure **antimmagine** di  $Y$  o ancora **immagine immersa** di  $Y$ .
- Con  $f: A \rightarrow B$  definiamo queste due applicazioni:
  - $\vec{f}: X \in \mathcal{P}(A) \rightarrow \vec{f}(X) \in \mathcal{P}(B)$  quindi sarà un'applicazione da  $\mathcal{P}(A)$  a  $\mathcal{P}(B)$
  - $\tilde{f}: Y \in \mathcal{P}(B) \rightarrow \tilde{f}(Y) \in \mathcal{P}(A)$  quindi sarà un'applicazione da  $\mathcal{P}(B)$  a  $\mathcal{P}(A)$
- Sia  $f: A \rightarrow B$  definiamo l'antimmagine di un singleton come  $\tilde{f}(\{b\}) = \{x \in A | f(x) = b\}$

## 1.9 Applicazioni iniettive, suriettive, biettive

Sia  $f: A \rightarrow B$  un'applicazione, essa è **suriettiva** per definizione se ogni elemento del codominio è immagine di qualche elemento del dominio, ovvero, in simboli:  $f$  è **suriettiva**  $\stackrel{def}{\Leftrightarrow} \forall b \in B, \exists a \in A (f(a) = b)$ . Quindi  $\tilde{f}(\{b\}) \neq \emptyset$ . Negando la suriettività avremo che  $f$  non è suriettiva  $\Leftrightarrow \exists b \in B | \forall a \in A (f(a) \neq b)$ . Quindi  $\exists b \in B (\tilde{f}(\{b\}) = \emptyset)$ . DUE ERRORI COMUNI: considerare l'insieme ristretto del codominio, ad esempio  $f: x \in \mathbb{Z} \rightarrow x^2 \in \mathbb{N}$  non si considera solo gli  $x^2 \in \mathbb{N}$  ma tutti gli  $x \in \mathbb{N}$ , quindi l'esempio non è suriettivo poiché  $\tilde{f}(\{5\}) = \emptyset$ ; l'altro errore è scambiare dominio e codominio, quindi scrivere  $f(b) = a$ .

Sia  $f: A \rightarrow B$ ,  $f$  è **iniettiva**  $\Leftrightarrow \forall x, y \in A (x \neq y \Rightarrow f(x) \neq f(y))$ , ovvero un'applicazione è iniettiva se elementi diversi hanno sempre immagini diverse, quindi se hanno immagini uguali sono lo stesso elemento, di conseguenza la definizione  $f$  **iniettiva**  $\Leftrightarrow \forall x, y \in A (f(x) = f(y) \Rightarrow x = y)$  è equivalente, così come è equivalente la definizione della controimmagine:  $f$  **iniet.**  $\Leftrightarrow \forall b \in B, \tilde{f}(\{b\})$  *contiene al più un elemento*.  $f: A \rightarrow B$  non è iniettiva  $\Leftrightarrow \exists x, y \in A (x \neq y \wedge f(x) = f(y))$ .

$f: A \rightarrow B$  si dice **biettiva** se e solo se  $f$  è sia suriettiva che iniettiva. Di conseguenza avremo  $f$  **biettiva**  $\Leftrightarrow \forall b \in B, \tilde{f}(\{b\})$  *ha uno ed un solo elemento*, e questo equivale a dire che  $\forall b \in B, \exists! a \in A (f(a) = b)$ .

## 1.10 Applicazioni invertibili e loro caratterizzazione

Sia  $f: A \rightarrow B$  biettiva,  $\forall b \in B, \exists! a_b \in A (f(a) = b)$  allora ha senso definire l'applicazione inversa come segue  $f^{-1}: b \in B \rightarrow a_b \in A$ . Quindi  $f^{-1}$  è detta **inversa** di  $f$ .

La condizione necessarie e sufficiente affinché una funzione sia invertibile, e dunque sia possibile individuare la corrispondenza inversa a quella che essa definisce, è che sia una funzione biettiva.

### 1.11 Applicazioni composte

Siano  $f: A \rightarrow B, g: B \rightarrow C$  due applicazioni dove il codominio di  $f$  sia uguale al dominio di  $g$ , allora si può definire un'applicazione che va dal dominio di  $f$  ( $\text{dom } f = A$ ) al codominio di  $g$  ( $\text{cod } g = C$ ).

Si dice **composta** di  $f$  e  $g$  e si denota con il simbolo  $g \circ f$  ( $g$  composto  $f$ ) la seguente applicazione:  $g \circ f: a \in A \rightarrow g(f(a)) \in C$ . Con  $f: A \rightarrow B$  e  $g: B \rightarrow C$ .

Proposizione 1: Siano  $f: A \rightarrow B, g: B \rightarrow C, h: C \rightarrow D$  applicazioni, allora posso definire le seguenti composte:

- $g \circ f: A \rightarrow C$
  - $h \circ g: B \rightarrow D$
  - $h \circ (g \circ f): A \rightarrow D$
  - $(h \circ g) \circ f: A \rightarrow D$
- Queste due composte sono uguali, quindi posso scrivere  $h \circ g \circ f$

Nota che questa anche se simile non è considerata proprietà associativa poiché gli oggetti sono diversi, però possiamo considerare applicazioni definiti in un insieme a valori nell'insieme (quindi da  $S$  ad  $S$ ). Se  $A, B$  sono insiemi, con  $B^A$  indico l'insieme di tutte le applicazioni  $f: A \rightarrow B$  di dominio  $A$  e codominio  $B$ . Se  $X$  è un insieme,  $X^X = \{f | f: X \rightarrow X \text{ è un'applicazione}\}$ . Di conseguenza se  $f, g \in X$  sono due applicazioni,  $f: X \rightarrow X, g: X \rightarrow X$  allora  $g \circ f: X \rightarrow X$  ed anche  $f \circ g: X \rightarrow X$ , questa composizione di applicazioni si può riguardare come operazioni nell'insieme  $X^X$ . Sia  $\circ: (f, g) \in X^X \times X^X \rightarrow f \circ g \in X^X$  un'operazione in  $X^X$ , definisco quindi la struttura  $(X^X, \circ)$  che è un semigrupp (vedi capitolo 2.1), quindi ora si può parlare di associatività.

Proposizione 2: Siano  $f: A \rightarrow B, g: B \rightarrow C$  applicazioni, allora valgono le seguenti proprietà:

- $f, g$  iniettive  $\Rightarrow g \circ f$  iniettiva  
Una applicazione è iniettiva quando immagini di elementi diversi sono diverse, ora supposte  $f$  e  $g$  iniettive si ha che  $g \circ f$  è iniettiva  $\Leftrightarrow \forall x, y \in A (x \neq y \Rightarrow (g \circ f)(x) \neq (g \circ f)(y))$ , ricordiamo inoltre che  $(g \circ f)(x) = g(f(x))$ . Sappiamo che su  $A$  agisce la funzione  $f$  quindi per l'iniettività di  $f$  si ha che per  $x \neq y \Rightarrow f(x) \neq f(y)$ , a questo punto questi elementi sono elementi di  $B$  distinti, e su questi due elementi agisce la funzione  $g$  che è anch'essa iniettiva; dunque,  $f(x) \neq f(y) \Rightarrow g(f(x)) \neq g(f(y))$  e quindi abbiamo dimostrato che  $x \neq y \Rightarrow (g \circ f)(x) \neq (g \circ f)(y)$
- $f, g$  suriettive  $\Rightarrow g \circ f$  suriettiva  
Dimostrazione non richiesta
- $f, g$  biettive  $\Rightarrow g \circ f$  biettiva  
Conseguenza delle precedenti, poiché  $g \circ f$  è sia iniettiva che suriettiva.

**N.B.:** non valgono le implicazioni inverse.

Esempio:  $f: x \in \mathbb{N} \rightarrow x \in \mathbb{Z}$  è iniettiva e non suriettiva mentre  $g: x \in \mathbb{Z} \rightarrow |x| \in \mathbb{N}$  non è iniettiva ma è suriettiva, avremo dunque  $g \circ f: \mathbb{N} \rightarrow \mathbb{N}$  con  $g(f(x)) = g(x) = |x|$  che è semplicemente  $x$ , poiché  $x \in \mathbb{N}$ , e dunque  $g \circ f$  rappresenta l'identità di  $\mathbb{N}$  che è biettiva (abbiamo dunque un controesempio per tutte e tre le implicazioni).

Proposizione 3: Siano  $f: A \rightarrow B$  una applicazione allora  $i_B \circ f = f \circ i_A = f$

Dimostriamo che  $f \circ i_A = f$  (si lascia  $i_B \circ f = f$  come esercizio), per dimostrare che due applicazioni sono uguali bisogna dimostrare che hanno uguale dominio e codominio e agiscono allo stesso modo, infatti si ha che  $f \circ i_A: A \rightarrow B$ , prendiamo a questo punto  $a \in A$  ed avremo che  $(f \circ i_A)(a) = f(i_A(a))$ , ma  $i_A(a) = a$  e quindi  $(f \circ i_A)(a) = f(a)$ .

La conseguenza di questa proposizione è il seguente corollario: l'identità di  $X$  è elemento neutro in  $(X^X, \circ)$

## 1.12 Proprietà caratterizzanti delle applicazioni biettive

Si ricorda che  $f: A \rightarrow B$  è biettiva  $\Leftrightarrow \forall b \in B, \exists! a_b \in A (f(a) = b)$ . Inoltre, l'inversa  $f^{-1}: B \rightarrow A$  con  $f^{-1}(b) = a_b$ . Poiché  $f^{-1}$  ed  $f$  si scambiano tra loro dominio e codominio è possibile fare entrambe le composte, quindi  $f^{-1} \circ f: A \rightarrow A$  e, invece,  $f \circ f^{-1}: B \rightarrow B$ .

**Proposizione 1:** Sia  $f: A \rightarrow B$  una applicazione biettiva e  $f^{-1}: B \rightarrow A$  la sua inversa. Allora  $f^{-1} \circ f$  è proprio l'identità di  $A$  mentre  $f \circ f^{-1}$  è l'identità di  $B$ .

**Dimostrazione:** caso  $f^{-1} \circ f = i_A$ : si ha semplicemente  $(f^{-1} \circ f)(a) = f^{-1}(\underbrace{f(a)}_b) = a = i_A(a)$ , simile è il caso  $f \circ f^{-1}: B \rightarrow B$ , infatti  $(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a_b) = b = i_B(b)$ .

Se  $f: X \rightarrow X$  è biettiva succede che  $f^{-1} \circ f = f \circ f^{-1} = i_X$  che è l'elemento neutro del monoide  $(X^X, \circ)$ , ne consegue che  $f$  è allora invertibile in  $(X^X, \circ)$ .

**Proposizione 2:** Sia  $f: A \rightarrow B$  una applicazione allora sono equivalenti le seguenti proprietà:

- 1)  $f$  è biettiva
- 2)  $\exists g: B \rightarrow A (g \circ f = i_A \wedge f \circ g = i_B)$

Condizione necessarie e sufficiente per la biettività è  $g$  verifica le stesse proprietà di  $f^{-1}$

**Dimostrazione:** verrà chiesta solo  $1 \Rightarrow 2$ : basta scegliere  $g = f^{-1}$  e descrivere la precedente proposizione. In particolare:  $g$  risulta essere proprio uguale ad  $f^{-1}$  e come conseguenza di questo teorema anche  $f^{-1}$  è biettiva (l'inversa di una applicazione biettiva è anch'essa biettiva).

$\mathcal{U}(X^X) = \{f \in X^X | f \text{ è invertibile su } (X^X, \circ)\}$ , prima abbiamo mostrato che se  $f$  è biettiva allora  $f$  è invertibile ( $f: X \rightarrow X$  biettiva  $\Rightarrow f \in \mathcal{U}(X^X)$ ). Viceversa, sia  $f \in \mathcal{U}(X^X)$  allora  $\exists g \in X^X (g \circ f = f \circ g = i_X)$ ; per la proposizione 2  $f$  è allora biettiva, a questo punto possiamo dire che  $\mathcal{U}(X^X) = \{f \in X^X | f \text{ è biettiva}\}$ . Quindi nel monoide  $(X^X, \circ)$  gli elementi invertibili sono applicazioni biettive.

## 1.13 Relazioni Binarie

Se  $A$  è un insieme non vuoto si dice **relazione binaria** in  $A$  una corrispondenza tra  $A$  e  $A$ . Un esempio di relazione binaria è l'insieme  $\mathbb{Z}$ , dove (ricordiamo che la corrispondenza è la terna  $(\mathbb{Z}, \mathbb{Z}, \rho)$ )  $\rho_1$  è la relazione che  $\forall a, b \in \mathbb{Z} (a \rho_1 b \Leftrightarrow a^2 = b^2)$  mentre un'altra relazione  $\rho_2$  è  $\forall a, b \in \mathbb{Z} (a \rho_2 b \Leftrightarrow a + b \text{ è dispari})$ ; altro esempio è l'insieme  $\mathcal{P}(S)$  con  $\forall X, Y \in \mathcal{P}(S) (X \rho_3 Y \Leftrightarrow X \subseteq Y)$  oppure  $\forall X, Y \in \mathcal{P}(S) (X \rho_4 Y \Leftrightarrow X \cap Y = \emptyset)$ .

Elenchiamo alcune definizioni:

- Se  $\rho$  è una relazione binaria  $A$ , useremo il simbolo  $(A, \rho)$  (inutile ripetere  $A$ )
- Sia  $\rho$  una relazione binaria in  $A$ ,  $\rho$  è **riflessiva**  $\Leftrightarrow \forall a \in A (a \rho a)$  (ogni elemento è in relazione con sé stesso)
- Sia  $\rho$  una relazione binaria in  $A$ ,  $\rho$  è **antiriflessiva**  $\Leftrightarrow \forall a \in A (a \not\rho a)$  (si noti che non è la negazione della precedente, poiché si richiede che tutti gli elementi non siano in relazione con sé stessi)
- Sia  $\rho$  una relazione binaria in  $A$ ,  $\rho$  è **simmetrica**  $\Leftrightarrow \forall x, y \in A (x \rho y \Rightarrow y \rho x)$
- Sia  $\rho$  una relazione binaria in  $A$ ,  $\rho$  è **antisimmetrica**  $\Leftrightarrow \forall x, y \in A (x \rho y \wedge y \rho x \Rightarrow x = y)$
- Sia  $\rho$  una relazione binaria in  $A$ ,  $\rho$  è **transitiva**  $\Leftrightarrow \forall x, y, z \in A (x \rho y \wedge y \rho z \Rightarrow x \rho z)$

**Esercizio:** Delle precedenti relazioni descritte  $\rho_1, \rho_2, \rho_3, \rho_4$  verificare la correttezza della seguente tabella

	Riflessiva	Antiriflessiva	Simmetrica	Antisimmetrica	Transitiva
$\rho_1$	SI	NO	SI	NO	SI
$\rho_2$	NO	SI	SI	NO	NO
$\rho_3$	SI	NO	NO	SI	SI
$\rho_4$	NO	NO	SI	NO	NO

Ad esempio  $\forall a \in \mathbb{Z} (a \rho_1 a \Leftrightarrow a^2 = a^2)$  è vero,  $\forall X \in \mathcal{P}(S) (X \rho_4 X \Leftrightarrow X \cap X = \emptyset)$  è vero solo per  $X = \emptyset$

Una relazione binaria in  $A$  si dice di **ordine (largo)** in  $A$  se e solo se  $\rho$  è riflessiva, antisimmetrica e transitiva. Quindi nei nostri esempi la relazione  $\rho_3$  (l'inclusione) è di ordine in  $\mathcal{P}(S)$ .

$\rho$  si dice un **grafo** se  $\rho$  è antiriflessiva e simmetrica, la relazione  $\rho_2$  è un esempio di grafo.

### 1.14 Relazioni di equivalenza

Una relazione binaria  $\rho$  definita in un insieme  $A$  si dice di **equivalenza** se e solo se verifica le seguenti tre proprietà:

1.  $\rho$  è **riflessiva**:  $\forall a \in A (a \rho a)$
2.  $\rho$  è **simmetrica**:  $\forall a, b \in A (a \rho b \Rightarrow b \rho a)$
3.  $\rho$  è **transitiva**:  $\forall a, b, c \in A (a \rho b \wedge b \rho c \Rightarrow a \rho c)$

Relazioni di equivalenza banali:

- **Relazione di uguaglianza**:  $\forall a, b \in A (a \rho b \Leftrightarrow a = b)$ , praticamente ogni elemento è in relazione con sé stesso; quindi, prendiamo il numero minimo di coppie possibili.
- **Relazione totale**:  $\forall a, b \in A (a \rho b)$ , mettiamo in relazione tutti gli elementi di  $A$ , quindi  $\rho = A \times A$ .

Sia  $f: A \rightarrow B$  una applicazione. Definiamo in  $A$  (dominio) questa relazione binaria  $\rho: \forall a, b \in A (a \rho b \Leftrightarrow f(a) = f(b))$  (quindi sono in relazione solo se hanno la stessa immagine). Questa relazione si indica con il simbolo  $\rho_f$  oppure con  $\mathcal{R}_f$  ed è una relazione di equivalenza binaria detta **nucleo di equivalenza di  $f$** .

Sia  $\rho$  una relazione di equivalenza in  $A$ . Si dice **classe di equivalenza** di un elemento  $a \in A$  l'insieme  $[a]_\rho = \{x \in A: x \rho a\}$  (classe di equivalenza di  $a$ ). L'insieme di tutte le classi di equivalenza si chiama **insieme quoziente** (di  $A$  rispetto a  $\rho$ ) e si denota con  $A/\rho = \{[a]_\rho | a \in A\}$ .

Proposizione: Siano  $A$  un insieme non vuoto e  $\rho$  una relazione di equivalenza in  $A$ . Allora:

- i.  $\forall a \in A, [a]_\rho \neq \emptyset$   
Dim.:  $[a]_\rho = \{x \in A | a \rho x\}$  per la proprietà della riflessività  $a \in [a]_\rho$  e quindi  $[a]_\rho \neq \emptyset$
- ii.  $\forall a, b \in A, [a]_\rho = [b]_\rho \Leftrightarrow a \rho b \Leftrightarrow a \in [b]_\rho$   
Dim.: dimostriamo la prima equivalenza, cominciamo con  $[a]_\rho = [b]_\rho \Rightarrow a \rho b$ :  $a$  e  $b$  costituiscono la stessa classe quindi so che  $b \in [b]_\rho \wedge [b]_\rho = [a]_\rho \Rightarrow b \in [a]_\rho = \{x \in A | a \rho x\} \Rightarrow a \rho b$ . Dimostriamo ora che  $[a]_\rho = [b]_\rho \Leftarrow a \rho b$ : quindi bisogna verificare che  $[a]_\rho \subseteq [b]_\rho \wedge [b]_\rho \subseteq [a]_\rho$ , prendiamo un  $x \in [a]_\rho \Rightarrow x \rho a$ , ma per ipotesi so che  $a \rho b$  quindi per la transitività se  $x \rho a \wedge a \rho b \Rightarrow x \rho b \Rightarrow x \in [b]_\rho$ . Analogamente si dimostra che preso un generico elemento di  $b$  risulta che esso è contenuto in  $[a]_\rho$  e quindi  $[b]_\rho \subseteq [a]_\rho \wedge [a]_\rho \subseteq [b]_\rho \Rightarrow [a]_\rho = [b]_\rho$ . L'equivalenza  $a \rho b \Leftrightarrow a \in [b]_\rho$  deriva semplicemente dalla definizione di classe di equivalenza.
- iii.  $\forall a, b \in A, [a]_\rho \neq [b]_\rho \Leftrightarrow [a]_\rho \cap [b]_\rho = \emptyset$   
Dim.: Supponiamo che  $[a]_\rho \neq [b]_\rho$  e dimostriamo che queste classi non hanno elementi in comune (implicazione  $\Rightarrow$ ), sia per assurdo  $c \in [a]_\rho \cap [b]_\rho$ , quindi  $c \in [a]_\rho \Rightarrow [c]_\rho = [a]_\rho$  per la proprietà ii; ma è anche vero che  $c \in [b]_\rho \Rightarrow [c]_\rho = [b]_\rho$  e cioè significa che anche  $[a]_\rho = [b]_\rho$  ed è assurdo, poiché per ipotesi ho  $[a]_\rho \neq [b]_\rho$ . Viceversa (implicazione  $\Leftarrow$ ), sempre per assurdo sia  $[a]_\rho = [b]_\rho$  quindi essendo uguali posso scrivere  $[a]_\rho \cap [a]_\rho = [a]_\rho$  che per la proprietà i questa classe è sempre diversa dal vuoto ma per ipotesi  $[a]_\rho \cap [b]_\rho = \emptyset$ .

Sia  $A$  un insieme non vuoto. Un insieme  $\mathcal{F}$  di parti di  $A$  ( $\mathcal{F} \subseteq \mathcal{P}(A)$ ) si dice una **partizione di  $A$**  se e solo se:

1.  $\forall X \in \mathcal{F}, X \neq \emptyset$
2.  $\forall X, Y \in \mathcal{F} (X \neq Y \Rightarrow X \cap Y = \emptyset)$
3.  $\bigcup_{X \in \mathcal{F}} X = A$

Esempio: Sia  $A = \{1, 2, 3, 4, 5\}$  l'insieme  $\mathcal{F} = \{\{1, 2\}, \{1\}, \{3, 4, 5\}\}$  non è una partizione di  $A$  poiché non viene rispettata la seconda condizione, infatti  $\{1, 2\} \cap \{1\} = \{1\} \neq \emptyset$ .

Esercizi: In  $\mathbb{Z} \times \mathbb{Z}$ ,  $\forall (x, y), (z, t) \in \mathbb{Z} \times \mathbb{Z}$ . Calcolare, se possibile, le classi  $[(1,1)]$  e  $[(2,1)]$  delle seguenti relazioni:  $(x, y)\rho_1(z, t) \Leftrightarrow |xy| = |zt|$  e  $(x, y)\rho_2(z, t) \Leftrightarrow x + y = z + t$ .

Sia l'insieme  $S = \{1, 2, 3\}$  definiamo in  $\mathcal{P}(S)$  le seguenti relazioni  $\forall X, Y \in \mathcal{P}(S)$   $X\rho_3 Y \Leftrightarrow |X| = |Y|$  e  $X\rho_4 Y \Leftrightarrow X \cap Y \neq \emptyset$ . Calcolare, quando possibile, tutte le classi di equivalenza e quindi l'insieme quoziente.

### 1.15 Teorema fondamentale sulle relazioni di equivalenza e le partizioni

Teorema: Sia  $A$  un insieme non vuoto. Allora

- 1) Se  $\rho$  è una relazione di equivalenza in  $A$ , l'insieme quoziente  $A/\rho$  è una partizione di  $A$ ,
- 2) Se  $\mathcal{F}$  è una partizione di  $A$ , la relazione  $\rho_{\mathcal{F}}$  così definita in  $A$   $\forall x, y \in A$   $x\rho_{\mathcal{F}} y \Leftrightarrow \exists X \in \mathcal{F} \{x, y\} \subseteq X$  è una relazione di equivalenza in  $A$  e risulta  $A/\rho_{\mathcal{F}} = \mathcal{F}$

Dimostrazione: 1)  $A/\rho_{\mathcal{F}}$  è una partizione di  $A$ : bisogna mostrare che ogni elemento dell'insieme è diverso dal vuoto; quindi,  $\forall [a] \in A/\rho_{\mathcal{F}}, [a] \neq \emptyset$  che è banalmente verificata poiché contiene almeno  $a$  stesso. La seconda proprietà da verificare è  $\forall [a], [b] \in A/\rho_{\mathcal{F}} ([a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset)$  che abbiamo già dimostrato poiché due classi di equivalenza sono uguali se e solo se sono in relazione, quando sono diverse e quindi non sono in relazione hanno intersezione vuota (vedi proposizione iii del capitolo precedente). Rimane da dimostrare l'ultima proprietà, ovvero  $\bigcup_{a \in A} [a] = A$ ; ma essendo  $\bigcup_{a \in A} [a] \subseteq A$  poiché tutti gli  $[a] \subseteq A$  quindi resta da provare che  $A \subseteq \bigcup_{a \in A} [a]$ : sia  $b \in A \Rightarrow b \in [b] \Rightarrow b \in \bigcup_{a \in A} [a]$ , questo è valido per tutti gli elementi di  $A$  che sono sempre disgiunti e quindi  $\bigcup_{a \in A} [a] = A$ . La dimostrazione della 2 non verrà svolta.

Sia  $E$  l'insieme di tutte le relazioni di equivalenza in  $A$  e sia  $F$  l'insieme di tutte le partizioni di  $A$  è possibile costruire, per il teorema fondamentale, due applicazioni:  $f: \rho \in E \rightarrow A/\rho \in F$  e  $g: \mathcal{F} \in F \rightarrow \rho_{\mathcal{F}} \in E$ . Inoltre, è dimostrabile che  $g \circ f = \text{id}_E$  e  $f \circ g = \text{id}_F$  e quindi  $f$  e  $g$  sono biettive e ( $g = f^{-1}$ ). Essendo poi  $E$  e  $F$  equipotenti, se  $E$  è finito risulta  $|E| = |F|$ .

Esercizio: determinare le relazioni di equivalenza sull'insieme  $A = \{1, 2, 3\}$  (risulta facile contare le partizioni).

## 2. Elementi di calcolo combinatorio

Partendo da insiemi finiti in cui è noto l'ordine, grazie al calcolo combinatorio si possono costruire altri insiemi con un ordine calcolabile (se si conosce l'insieme finito di partenza).

### 2.1 Insiemi equipotenti

Due insiemi  $A$  e  $B$  si dicono **equipotenti** se  $A = B = \emptyset$  oppure se esiste  $f: A \rightarrow B$  biettiva (sono legati da una applicazione biettiva).

Se  $A$  e  $B$  sono equipotenti, scriveremo  $A \sim B$ . Valgono le seguenti proprietà:

1. Per ogni insieme  $A$ :  $A \sim A$
2.  $A \sim B \Rightarrow B \sim A$  (l'inversa di una funzione biettiva è anch'essa biettiva)
3.  $A \sim B \wedge B \sim C \Rightarrow A \sim C$  (basta fare la composta)

### 2.2 insiemi finiti e loro ordine

Un insieme  $A$  si dice **finito** se  $A = \emptyset$  oppure  $\exists(!)n \in \mathbb{N}^*$  ( $\exists(!)$  = se esiste allora è unico) tale che  $A$  è equipotente ad  $I_n = \{1, 2, \dots, n\}$ . In tal caso l'**ordine** di  $A$  sarà  $n$  e scriveremo  $|A| = n$ , ovviamente  $|\emptyset| = 0$ . Se  $A$  è finito e  $B$  è equipotente ad  $A$  allora  $|B| = |A|$ . Un insieme si dice **infinito** se non è finito.

Proposizione 1: Sia  $A$  un insieme non vuoto finito ed  $f: A \rightarrow A$  allora sono equivalenti le seguenti proprietà:

1.  $f$  è iniettiva
2.  $f$  è suriettiva
3.  $f$  è biettiva

Nel caso in cui ho un applicazione da un insieme finito in sé, l'iniettività basta a dimostrare che l'applicazione è anche suriettiva e di conseguenza biettiva. Analogamente se  $A$  è suriettiva allora sarà anche iniettiva e quindi biettiva.

Di conseguenza per dimostrare che un applicazione  $f: A \rightarrow A$  è biettiva basta dimostrare che  $f$  è iniettiva oppure suriettiva. Questa proposizione vale non solo per  $f: A \rightarrow A$  ma anche  $f: A \rightarrow B$  con  $A \sim B$  (finiti).

Proposizione 2: Sia  $A$  un insieme non vuoto finito e  $B \subset A$ . Allora  $B$  è finito e  $|B| < |A|$  (più precisamente  $A$  e  $B$  non sono equipotenti)

Questa proposizione non vale per gli insiemi infiniti infatti un insieme infinito è tale se è equipotente ad una sua parte propria, ne fa da esempio l'Albergo di Hilbert: ho un albergo con numero di camere infinito e per "liberare" una camera mi basta spostare i clienti nella stanza successiva ( $f: n \in \mathbb{N}^* \rightarrow n + 1 \in \mathbb{N}^*$ ). Questo potrebbe far pensare che gli insiemi infiniti siano tutti equipotenti come  $\mathbb{Z} \sim \mathbb{Q}$  ma si ha che  $\mathbb{Q} \not\sim \mathbb{R}$ .

Se  $A$  è infinito e  $f: A \rightarrow A$  non vale la proposizione 1, consideriamo ad esempio  $A = \mathbb{N}$  e consideriamo l'applicazione  $F: a \in \mathbb{N} \rightarrow a + 1 \in \mathbb{N}$ , questa applicazione è ovviamente iniettiva, quindi se fosse finito sarebbe anche suriettiva e biettiva per la proposizione 1; ma  $f$  non è suriettiva infatti  $\tilde{f}(\{0\}) = \emptyset$ . Altro esempio è dato dalla funzione  $f: a \in \mathbb{N} \rightarrow \begin{cases} 0 & \text{se } a = 0 \\ a - 1 & \text{se } a > 0 \end{cases} \in \mathbb{N}$ , quest'applicazione è suriettiva ma non iniettiva infatti avremo  $\tilde{f}(\{0\}) = \{0, 1\}$ .

Proposizione 3: Siano  $A$  e  $B$  insiemi finiti e disgiunti (che non abbiano elementi in comune). Allora  $A \cup B$  è finito e  $|A \cup B| = |A| + |B|$

Corollario 4: Siano  $A$  e  $B$  insiemi finiti allora  $|A| = |A \setminus B| + |A \cap B|$

Proposizione 5: Siano  $A$  e  $B$  insiemi finiti allora  $|A \cup B| = |A| + |B| - |A \cap B|$

Dimostrazione:  $|A \cup B| = |A \setminus B| + |A \cap B| + |B \setminus A| = |A| - |A \cap B| + |A \cap B| + |B \setminus A| = |A| + |B| - |A \cap B|$

Proposizione 6: Se  $A_1, \dots, A_n$  sono  $n$  insiemi finiti e a due a due disgiunti  $|A_1 \cup \dots \cup A_n| = |A_1| + \dots + |A_n|$



**Proposizione 7:** Siano  $A$  e  $B$  insiemi finiti allora  $A \times B$  è finito e  $|A \times B| = |A| \cdot |B|$

**Dimostrazione:** Se uno dei due è vuoto  $A \times B$  è vuoto e quindi avrà ordine zero. Supponiamo ora  $|A| = n$ , allora  $A \times B = \{(a, b) | a \in A \wedge b \in B\}$ , quindi se  $A = \{a_1, \dots, a_n\}$  allora  $A \times B = \{a_1\} \times B \cup \dots \cup \{a_n\} \times B$ , questi insiemi sono disgiunti poiché una coppia è uguale solo se entrambe le coordinate sono uguali, dunque  $\forall i = 1, \dots, n$  ho che  $\{a_i\} \times B$  è finito e  $|\{a_i\} \times B| = |B|$  e quindi per la proposizione precedente ottengo che  $|A \times B| = n|B|$  ovvero il numero che si ottiene sommando l'ordine di  $B$  a se stesso  $n$  volte ( $n = |A|$ )

**Proposizione 8:** Siano  $A_1, \dots, A_n$   $n$  insiemi finiti allora  $A_1 \times \dots \times A_n$  è finito e  $|A_1 \times \dots \times A_n| = |A_1| \cdot \dots \cdot |A_n|$

Se  $A$  e  $B$  sono insiemi non vuoti, l'insieme  $\{f | f: A \rightarrow B \text{ è una applicazione}\}$  si denota con il simbolo  $B^A$

**Proposizione 9:** Se  $A$  e  $B$  sono insiemi finiti e non vuoti  $B^A$  è finito e risulta  $|B^A| = |B|^{|A|}$  (quindi il numero delle applicazioni sono l'ordine di  $B$  elevato all'ordine di  $A$ )

**Dimostrazione:** Sia  $f: A \rightarrow B$  una applicazione allora  $f$  determina in modo univoco una  $n$ -upla di elementi di  $B$ , supponiamo che  $|A| = n$  quindi posso pensare  $A = \{a_1, a_2, \dots, a_n\}$  di conseguenza  $f$  è nota se conosco  $f(a_1), f(a_2), \dots, f(a_n)$ , quest'ultime appartengono a  $B$ , allora considero la  $n$ -upla  $(f(a_1), f(a_2), \dots, f(a_n))$  che appartiene al prodotto cartesiano di  $B$ ,  $n$  volte, ovvero a  $B^n$ . In questo modo ad ogni applicazione ho associato una  $n$ -upla di elementi di  $B$ , viceversa se parto dalla  $n$ -upla  $(b_1, b_2, \dots, b_n) \in B^n$ , posto  $f(a_i) = b_i$   $\forall i = 1, \dots, n$  avrò che questa  $f \in B^A$  e se costruisco  $(f(a_1), f(a_2), \dots, f(a_n))$  ottengo proprio  $(b_1, b_2, \dots, b_n)$  e tutte le applicazioni si possono dedurre da una forma del genere quindi le applicazioni da  $A$  a  $B$  sono tante quante sono le  $n$ -uple in  $B^n$ ; a questo punto posso scrivere una funzione  $g: B^A \rightarrow B^n$  ed essendo questa  $g$  biettiva gli insiemi saranno equipotenti, ovvero  $|B^A| = |B^n| = \underbrace{|B| \cdot \dots \cdot |B|}_{n \text{ volte}} = |B|^n = |B|^{|A|}$

**Proposizione 10:** Siano  $A$  e  $B$  insiemi finiti non vuoti  $|A| = n$  e  $|B| = m$  allora il numero delle applicazioni iniettive di  $A$  in  $B$  è 0 se  $n > m$ , è  $m(m-1) \cdot m(m-2) \cdot \dots \cdot m(m-n)$  (ovvero  $\frac{m!}{(m-n)!}$ ) se  $n \leq m$

**Dimostrazione:** Se voglio costruire una applicazione iniettiva  $f$  da  $A = \{a_1, \dots, a_n\}$  a  $B$  ho bisogno che  $n \leq m$  dopodiché  $f(a_1) \in B$  e può variare in  $n$  modi,  $f(a_2) \in B \setminus \{f(a_1)\}$  può variare in  $n-1$  modi e così via... Avremo dunque che  $(f(a_1), \dots, f(a_n)) \in B \times (B \setminus \{f(a_1)\}) \times \dots \times (B \setminus \{f(a_1), \dots, f(a_{n-1})\})$ , e quindi l'ordine di questo prodotto cartesiano è  $|B| \cdot |B \setminus \{f(a_1)\}| \cdot \dots \cdot |B \setminus \{f(a_1), \dots, f(a_{n-1})\}|$  ovvero l'enunciato

Se  $A = B$  e  $|A| = n = |B|$  l'insieme delle applicazioni iniettive da  $A$  ad  $A$  coincide con l'insieme delle applicazioni biettive (nonché suriettive) da  $A$  ad  $A$

**Proposizione 11:** Se  $A$  è un insieme non vuoto di ordine  $n$ , l'insieme delle applicazioni biettive di  $A$  in  $A$  ha ordine  $n!$

**Dimostrazione:** Se  $f: A \rightarrow A$ , con  $A$  finito allora  $f$  è biettiva se e soltanto se  $f$  è iniettiva e di conseguenza possiamo usare la proposizione 10:  $\frac{n!}{(n-n)!} = \frac{n!}{0!} = \frac{n!}{1} = n!$

**Corollario 12:** Se  $A$  è un insieme finito non vuoto di ordine  $n$  il gruppo delle permutazioni  $S_A$  ha ordine  $n!$

Il numero delle applicazioni di  $A$  in  $B$  ( $B^A$ ) se  $|A| = n$  e  $|B| = m$  è  $m^n$  (proposizione 9) e questo è anche il **numero delle disposizioni di  $m$  elementi su  $n$  posti con ripetizioni**. Invece il numero di disposizioni senza ripetizioni di  $m$  elementi su  $n$  posti è 0 se  $n > m$  mentre  $\frac{m!}{(m-n)!}$  se  $n \leq m$  (proposizione 10)

## 2.3 Coefficienti binomiali

Sia  $n > 0$  e sia  $k | 0 \leq k \leq n$ . Allora si definisce il **coefficiente binomiale**  $\binom{n}{k}$  nel modo seguente:

$$\binom{n}{k} = \frac{n!}{k! (n-k)!}$$



**Teorema:** Sia  $A$  un insieme non vuoto di ordine  $n$  e sia  $k$  un intero tale che  $0 \leq k \leq n$  allora il numero dei sottoinsiemi di  $A$  di ordine  $k$  è  $\binom{n}{k}$

Applicazioni di questo teorema:

- Quanti sono i sottoinsiemi di  $\{1,2,3,4\}$  di ordine 3?  $\binom{4}{3} = \frac{4!}{3!(4-3)!} = \frac{4 \cdot 3!}{3! \cdot 1!} = 4$
- Quanti sono i sottoinsiemi di ordine 1 (i singleton) di  $\{1,2,3,4\}$ ? 4, si deduce che  $\binom{n}{k} = \binom{n}{n-k}$

## 2.4 Ordine di $\mathcal{P}(S)$ e principio di induzione

**Prima forma del principio di induzione:**  $\forall n \geq n_0$ , sia data una proposizione  $P(n)$  e dimostriamo che valgano le seguenti condizioni: **1)**  $P(n_0)$  è vera **2)**  $\forall n > n_0 (P(n-1) \Rightarrow P(n))$ . Allora  $\forall n \geq n_0 (P(n) \text{ è vera})$

$n_0$  può essere sostituito nell'enunciato da qualunque  $n \in \mathbb{Z}$ , in genere il valore minimo  $n_0$  è detto **base di induzione** mentre, dato  $n > (n_0)$ ,  $P(n-1)$  vera si dice **ipotesi di induzione**, infine, l'implicazione  $P(n-1) \Rightarrow P(n)$  è il **passo di induzione**.

Esercizio: dimostrare con il principio di induzione che la somma dei primi  $n$  numeri positivi è  $\frac{n(n+1)}{2}$ ,  $n \geq 1$

**Teorema (ordine  $\mathcal{P}(S)$ ):** Sia  $S$  un insieme finito di ordine  $n$ . Allora l'insieme  $\mathcal{P}(S)$  ha ordine  $2^n = 2^{|S|}$

**Dimostrazione:** Si ragiona per induzione su  $n$  con la prima forma del principio di induzione. La base di induzione è  $n = 0$ , quindi se  $|S| = 0 \Rightarrow S = \emptyset$ , di conseguenza  $\mathcal{P}(\emptyset) = \{\emptyset\} \Rightarrow |\mathcal{P}(\emptyset)| = 1 = 2^0 = 2^{|S|}$  ciò significa che  $P(n_0)$  è vera. A questo punto supponiamola vera per  $P(n-1)$  e ciò significa che se  $T$  è un insieme di ordine  $n-1$ ,  $|\mathcal{P}(T)| = 2^{n-1}$  (ipotesi di induzione). Sia  $|S| = n$  che per ipotesi è maggiore di zero  $\Rightarrow S \neq \emptyset$ . Sia  $s \in S$ ,  $\forall X \in \mathcal{P}(S)$  sono possibili solo due casi (che si escludono a vicenda), o  $a \notin X$ , oppure  $a \in X$ , chiamiamo  $A = \{X \in \mathcal{P}(S) | a \notin X\}$  e  $B = \{X \in \mathcal{P}(S) | a \in X\}$ , ne segue  $\mathcal{P}(S) = A \cup B$  e  $A \cap B = \emptyset$ , ciò significa che l'insieme finito  $\mathcal{P}(S)$  è unione di due insiemi finiti disgiunti e quindi  $|\mathcal{P}(S)| = |A| + |B|$ , ora bisogna dimostrare che  $|A| = |B| = 2^{n-1}$  così da far risultare che  $|\mathcal{P}(S)| = 2^{n-1} + 2^{n-1} = 2(2^{n-1}) = 2^n$ . L'insieme  $A$  è per definizione composto dagli insiemi che non contengono  $a$ , questi sottoinsiemi devono quindi essere contenuti in  $S \setminus \{a\}$ , a questo punto possiamo riscrivere  $A = \{X \in \mathcal{P}(S) | X \subseteq S \setminus \{a\}\}$  che è semplicemente un altro modo per descrivere l'insieme  $\mathcal{P}(S \setminus \{a\})$ , quindi  $|S \setminus \{a\}| = n-1$  e per ipotesi di induzione risulterà  $|A| = |\mathcal{P}(S \setminus \{a\})| = 2^{|S \setminus \{a\}|} = 2^{n-1}$ . Passiamo ora a dimostrare che  $A$  e  $B$  sono equipotenti (esiste  $f: A \rightarrow B$  biettiva) e quindi hanno lo stesso ordine: sia  $f: X \in A \rightarrow X \cup \{a\} \in B$  la nostra applicazione, per dimostrare che è biettiva costruiamo la sua inversa, prendiamo  $g: X \in B \rightarrow X \setminus \{a\} \in A$  e facciamo  $g \circ f: X \in A \rightarrow X \in A$  che è quindi l'identità di  $A$ , allo stesso modo  $f \circ g: B \rightarrow B$  ovvero  $\text{id}_B$  che per la caratterizzazione delle applicazioni biettive significa che  $g = f^{-1}$  e quindi  $f$  è biettiva e  $|A| = |B|$ . CVD

**Seconda forma del principio di induzione:**  $\forall n \geq n_0$ , sia data una proposizione  $P(n)$  e dimostriamo che valgano le seguenti condizioni: **1)**  $P(n_0)$  è vera **2)**  $\forall n > n_0 ((\forall h(n_0 \leq h < n)) \Rightarrow P(h))$ . Allora  $\forall n \geq n_0 (P(n) \text{ è vera})$

Mentre nella prima forma si suppone che sia vera per  $n-1$  nella seconda forma supponiamo che sia vera anche per i precedenti (da  $n-1$  a  $n_0$ ). La seconda forma la utilizzeremo nel [capitolo 3.16](#).

### 3. Strutture Algebriche

Una struttura algebrica è un insieme non vuoto su cui sono definite una o più operazioni interne.

Se  $S$  è un insieme e  $*$  un'operazione in  $S$  la coppia  $(S, *)$  è detta struttura algebrica ad una operazione, la terna  $(S, *, \perp)$  sarà una struttura algebrica a due operazioni e così via...

#### 3.1 Operazioni su un insieme

Sia  $S$  un insieme non vuoto, si dice operazione (binaria interna) definita in  $S$  un'applicazione  $f: S \times S \rightarrow S$ . Generalmente si denota  $f$  con un simbolo  $(+, -, *, \backslash, \dots)$  e si pone l'immagine della coppia  $(a, b) = a + b$  (oppure  $-, *, \backslash, \dots$ ). Se si sceglie il simbolo  $+$  si dice che si usa la notazione additiva, notazione moltiplicativa nel caso del simbolo  $\cdot$ .

Sia  $(S, *)$  una struttura algebrica:

$*$  è commutativa  $\Leftrightarrow (\forall x, y \in S (x * y = y * x))$

$*$  non è commutativa  $\Leftrightarrow (\exists x, y \in S (x * y \neq y * x))$

$*$  è associativa  $\Leftrightarrow (\forall a, b, c \in S ((a * b) * c = a * (b * c)))$

$*$  non è associativa  $\Leftrightarrow (\exists a, b, c \in S ((a * b) * c \neq a * (b * c)))$

Ammette elemento neutro a destra  $\Leftrightarrow (\exists \varepsilon \in S (\forall a \in S, a * \varepsilon = a))$

Ammette elemento neutro a sinistra  $\Leftrightarrow (\exists \varepsilon \in S (\forall a \in S, \varepsilon * a = a))$

$\varepsilon$  è identità (elemento neutro) di  $S$   $\Leftrightarrow \varepsilon$  è neutro a destra ed a sinistra,  $\forall a \in S, a * \varepsilon = \varepsilon * a = a$

Terminologie varie:

- $(S, *)$  si dice **semigrupp** se  $*$  è associativa.
- $(S, *)$  si dice **monoide** se è un semigrupp dotato di elemento neutro
- $(S, *)$  si dice **monoide commutativo** se è un monoide dotato di proprietà commutativa.

**ESERCIZIO:** definire il tipo di struttura algebrica (es. semigrupp) e l'eventuale elemento neutro delle strutture algebriche viste nel [capitolo 1.5](#). Alcune soluzioni si possono trovare nel capitolo successivo.

Osservazioni su una struttura  $(S, *)$ :

- Sia  $\varepsilon_1$  neutro a sinistra e  $\varepsilon_2$  neutro a destra allora  $\varepsilon_1 = \varepsilon_2$  per definizione, infatti  $\varepsilon_1 = \varepsilon_1 * \varepsilon_2 = \varepsilon_2$
- Se  $\varepsilon$  è elemento neutro, allora  $\varepsilon$  è neutro a destra ed a sinistra, in particolare,  $\varepsilon$  è l'unico elemento neutro a sinistra ed è l'unico elemento neutro a destra.
- In una struttura commutativa basta cercare solo un elemento neutro (a destra o sinistra) per dimostrare che sia identità di  $S$ , se la struttura non è commutativa si cerca prima l'esistenza di elementi neutri (possono essere uno, più di uno o nessuno) e poi dell'elemento (unico o inesistente) neutro di sinistra. Se a destra abbiamo più di un elemento neutro o nessun elemento neutro allora nemmeno a sinistra c'è elemento neutro, mentre nel caso di un unico elemento neutro a destra allora può esistere o non esistere elemento neutro a sinistra.
- In un monoide l'elemento neutro è sempre invertibile e coincide con il suo inverso.

#### 3.2 Elementi invertibili e gruppi

Sia  $(A, *)$  una struttura algebrica dotata di elemento neutro  $\varepsilon$ , un elemento  $a \in A$  si dice invertibile o simmetrizzabile se  $\exists a^{-1} \in A (a * a^{-1} = a^{-1} * a = \varepsilon)$ .


Si dice **gruppo** un monoide in cui tutti gli elementi sono simmetrizzabili (o invertibili).

Esempi con le strutture note:

- $(P(S), \cup)$  è un monoide con il  $\emptyset$  come identità; ed esso è l'unico elemento invertibile infatti sia  $X$  invertibile allora  $\exists Y \in P(S) | X \cup Y = Y \cup X = \emptyset \Rightarrow X = Y = \emptyset$

- $(P(S), \cap)$  è un monoide ed ha come elemento neutro  $S$  ed esso (come sopra) è anche l'unico elemento simmetrizzabile. Sia  $X$  invertibile allora  $\exists Y \in P(S) | X \cap Y (= Y \cap X) = S \Rightarrow X = S$
- $(P(S), \Delta)$  è un gruppo dove ogni elemento  $X \in P(S)$  è simmetrizzabile, infatti, sapendo che l'elemento neutro è il  $\emptyset$ ,  $\forall X \in P(S), \exists Y \in P(S) (X \Delta Y = Y \Delta X = \emptyset)$  questo  $Y$  non solo esiste ma è proprio  $X$ , il gruppo  $(P(S), \Delta)$  ha la proprietà che ogni elemento è anche suo simmetrico:  $X \Delta X = \emptyset$

Una struttura algebrica  $(S, *)$  si dice **gruppo abeliano** se e solo se possiede le seguenti proprietà:

- $*$  è associativa
  - Gode di elemento neutro  $\varepsilon$
  - Tutti gli elementi di  $S$  sono simmetrizzabili
  - $*$  è commutativa
- 

### 3.3 Elementi non cancellabili (o regolari)

Sia  $(S, \cdot)$  una struttura algebrica, se  $a \in S$  allora:

- $a$  è cancellabile (o regolare) a sinistra  $\Leftrightarrow \forall (b, c) \in S \times S (a \cdot b = a \cdot c \Rightarrow b = c)$
- $a$  è cancellabile (o regolare) a destra  $\Leftrightarrow \forall (b, c) \in S \times S (b \cdot a = c \cdot a \Rightarrow b = c)$

$a$  si dice **cancellabile** (o regolare) se è cancellabile sia a destra che a sinistra.

**Proposizione 1:** Se  $(S, \cdot)$  è un monoide, ogni elemento invertibile è sempre cancellabile.

**Dimostrazione:** Sia  $a \in S$  invertibile, e sia  $a^{-1}$  il suo inverso, se  $a$  è cancellabile a sinistra avremo che  $\forall (b, c) \in S \times S, a \cdot b = a \cdot c \Rightarrow b = c$ , possiamo dimostrarlo per la proprietà transitiva dell'implicazione, infatti  $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac) \Rightarrow (a^{-1}a)b = (a^{-1}a)c \Rightarrow 1_S b = 1_S c$  dove  $1_S$  è l'elemento neutro di  $S$ , allo stesso modo si procede per dimostrare la cancellabilità a destra.

Generalmente non vale il viceversa, ovvero se un elemento è cancellabile non è detto che sia invertibile.

**Proposizione 2:** Se  $(S, \cdot)$  è un gruppo, ogni  $a \in S$  è invertibile, quindi tutti gli elementi sono cancellabili.

**ESERCIZIO:** determinare gli elementi cancellabili nella struttura  $(\mathbb{Z}, *)$  dove l'operazione  $*$  è così definita  $a * b = a + b + ab, \forall (a, b \in \mathbb{Z})$ , studiarne anche la commutatività e l'associatività.

### 3.4 Parti chiuse in una struttura

**Proprietà:** Sia  $(S, *)$  una struttura algebrica ed  $H \subseteq S, H \neq \emptyset$  ( $H$  una parte non vuota di  $S$ ) allora  $H$  si dice chiusa rispetto a  $*$   $\Leftrightarrow \forall x, y \in H (x * y \in H)$ .

Praticamente sappiamo già che presi  $a, b \in S$  l'elemento  $a * b$  appartiene anch'esso ad  $S$ , mentre presi  $a, b \in H$ , con  $H$  sottoinsieme di  $S$ , l'elemento  $a * b \in S$  sicuramente, ma non è detto che appartenga ad  $H$ , quando succede che  $a * b$  è ancora in  $H$ , l'insieme  $H$  si dice una parte chiusa rispetto all'operazione  $*$ .

**Esempi:**  $\mathbb{N}$  è chiusa in  $(\mathbb{Z}, \cdot)$ , per dimostrarlo bisogna verificare che  $\forall x, y \in \mathbb{N}, x \cdot y \in \mathbb{N}$  (si verifica banalmente per le proprietà dei numeri naturali. Se si volesse dimostrare, che  $\mathbb{N}$  non è chiusa in  $(\mathbb{Z}, \cdot)$  bisogna verificare che  $\exists x, y \in \mathbb{N} (x \cdot y \notin \mathbb{N})$ .

$\mathbb{N}^-$  non è chiusa in  $(\mathbb{Z}, \cdot)$  infatti, poiché  $\mathbb{N}^- = \{-x | x \in \mathbb{N}\}$  il prodotto di elementi negativi è positivo:  $-3 \cdot -2 \in \mathbb{N}^- \wedge (-3)(-2) = 6 \notin \mathbb{N}^-$ .

Siano  $T, S$  insiemi e sia  $T \subseteq S$  e quindi  $\mathcal{P}(T) \subseteq \mathcal{P}(S)$  diamo le seguenti risposte:

- **$\mathcal{P}(T)$  è chiusa rispetto a  $\cup$ ?**  
Sì, essendo l'unione di due elementi di  $\mathcal{P}(T)$  ancora un elemento di  $\mathcal{P}(T)$
- **$\mathcal{P}(T)$  è chiusa rispetto a  $\cap$ ?**  
L'intersezione di due parti di  $T$  è ancora una parte di  $T$
- **$\mathcal{P}(T)$  è chiusa rispetto a  $\Delta$ ?**  
La differenza simmetrica di due elementi di  $\mathcal{P}(T)$  appartiene ancora a  $\mathcal{P}(T)$

Un esempio importante di parte chiusa è l'insieme degli elementi invertibili in un monoide. Sia il seguente insieme  $\mathcal{U}(S) = \{x \in S \mid x \text{ è invertibile in } S\}$ , detto l'insieme degli elementi invertibili di  $S$  (Units di  $S$ ), si ha che  $\mathcal{U}(S)$  è una parte chiusa di  $S$ . Innanzitutto, si ha che  $\mathcal{U}(S) \neq \emptyset$ , poiché l'elemento neutro  $1_S \in \mathcal{U}(S)$ . Inoltre, per definizione, si ha che  $\mathcal{U}(S)$  è chiusa  $\Leftrightarrow \forall x, y \in \mathcal{U}(S), xy \in \mathcal{U}(S)$ , quindi, per dimostrare che è chiusa, bisogna verificare che se  $x, y$  sono invertibili allora anche  $xy$  è invertibile: abbiamo  $x, y \in \mathcal{U}(S)$ , quindi  $\exists x^{-1} \in S (xx^{-1} = x^{-1}x = 1_S)$  e  $\exists y^{-1} \in S (yy^{-1} = y^{-1}y = 1_S)$ ; costruiamo adesso un  $h$  tale  $(xy)h = 1_S$ : abbiamo  $(xy)h \Rightarrow yh = x^{-1} \Rightarrow h = y^{-1}x^{-1}$  (nota bene che  $y^{-1}$  va a sinistra e non a destra di  $x^{-1}$  poiché non sapendo di avere la commutatività moltiplico direttamente a sinistra entrambi i membri); per l'associatività si ha  $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x1_Sx^{-1} = xx^{-1} = 1$ . Analogamente si ha che  $(y^{-1}x^{-1})(xy) = 1$  e quindi abbiamo così dimostrato che  $xy$  è invertibile ed il suo inverso è  $y^{-1}x^{-1}$  ed appartiene dunque a  $\mathcal{U}(S)$ .

**Definizione:** Sia  $(S, *)$  una struttura algebrica ed  $H$  una parte chiusa di  $(S, *)$  ( $S$  rispetto  $*$ ) allora se consideriamo l'operazione  $\odot: (x, y) \in H \times H \rightarrow x * y \in H$ ; questa operazione si continua a denotare con lo stesso simbolo  $*$ , per abuso di notazione (poiché dal punto di vista pratico il composto è lo stesso anche se sono operazioni diverse) e si può parlare della struttura  $(H, \odot)$  come una struttura algebrica che si dice **struttura algebrica indotta** su  $H$ .

Ad esempio,  $\mathbb{N}$  è stabile rispetto alla somma in  $(\mathbb{Z}, +)$  quindi  $(\mathbb{N}, +)$  è la struttura indotta rispetto la somma. Quando si ha una parte chiusa in una struttura si può considerare la sua struttura indotta.

Ricordiamo che data una struttura  $(S, \cdot)$  e dato un elemento  $a \in S$  allora  $a$  è cancellabile a sinistra se e soltanto se  $\forall b, c \in S (ab = ac \Rightarrow b = c)$ . Sia  $H = \{x \in S \mid x \text{ è cancellabile a sinistra}\}$  e supposto  $H \neq \emptyset$  allora  $H$  è chiusa rispetto a  $\cdot$ . Siano, infatti,  $x, y \in H$  cancellabili a sinistra e siano  $b, c \in S$ , per dimostrare che  $xy$  sia cancellabile a sinistra basta dimostrare che se  $(xy)b = (xy)c \Rightarrow b = c$ : essendo  $S$  un semigruppino ho la proprietà associativa e quindi è lecito scrivere  $x(yb) = x(yc)$ , ma essendo  $x$  cancellabile a sinistra allora  $yb = yc$  che, essendo anche  $y$  cancellabile, risulta  $b = c$ .

Se  $(S, \cdot)$  è un monoide, si può definire l'insieme  $\mathcal{U}(S) = \{a \in S \mid a \text{ è invertibile in } S\}$ , questo  $\mathcal{U}(S) \neq \emptyset$  essendo  $1_S \in \mathcal{U}(S)$ , essendo  $\mathcal{U}(S)$  chiusa rispetto a  $\cdot$  si può considerare la struttura indotta  $(\mathcal{U}(S), \cdot)$  che si dimostra essere un gruppo. Per dimostrare che  $(\mathcal{U}(S), \cdot)$  bisogna vedere che  $\cdot$  sia associativa, e lo è poiché se è associativa in un insieme lo sarà in tutte le sue parte chiuse;  $\mathcal{U}(S)$  ha elemento neutro ed è proprio  $1_S$ ; infine, l'ultima ipotesi,  $\forall a \in \mathcal{U}(S), \exists a^{-1} \in \mathcal{U}(S)$  e il loro prodotto, proprio per definizione di inverso, è  $aa^{-1} = a^{-1}a = 1_S$ ; quindi  $(\mathcal{U}(S), \cdot)$  è un gruppo. Prendiamo ad esempio la struttura  $(X^X, \circ)$  con l'insieme  $X^X = \{f \mid f: X \rightarrow X \text{ è una applicazione}\}$ , sia  $\mathcal{U}(X^X) = \{f \in X^X \mid f \text{ è biettiva}\}$  allora  $(\mathcal{U}(X^X), \circ)$  è un gruppo detto **gruppo delle permutazioni di  $X$** , questo importante gruppo si denota con il simbolo  $S_X$ .

### 3.5 Monoide delle parole nell'alfabeto $A$

Supponiamo che  $A$  sia un insieme non vuoto, si dice una parola nell'alfabeto  $A$  una sequenza finita di simboli  $a_1 \dots a_n \in A$ . Esempio: Una parola per l'insieme  $A = \{a, 1, b\}$  è la sequenza finita  $a11ba$ , al momento non è definito nessun prodotto, è una semplice sequenza di simboli.

Il numero  $n$  di caratteri che appaiono in una parola è detta **lunghezza della parola** e per convenzione si indica con  $w_0$  si indica una parola priva di oggetti, ovvero la **parola vuota** ed ha lunghezza 0.

$\forall n \in \mathbb{N}$  indichiamo con  $\mathcal{W}_n$  l'insieme delle parole di lunghezza  $n$  nell'alfabeto  $A$ . Mentre,  $\mathcal{W}_A = \bigcup_{n \in \mathbb{N}} \mathcal{W}_n$  e quindi rappresenta l'insieme di tutte le parole in  $A$ .

Definiamo il prodotto  $*$  per  $\mathcal{W}_A$  nel seguente modo detto **giusta apposizione**:  $(a_1 a_2 \dots a_n) * (b_1 b_2 \dots b_m) = a_1 a_2 \dots a_n b_1 b_2 \dots b_m$  che è ancora una sequenza finita di simboli di lunghezza  $n + m$ . Di conseguenza  $\forall v \in \mathcal{W}_n$  risulta  $v * w_0 = v$ , quindi  $w_0$  è elemento neutro per l'insieme  $A$ .

È chiaro che l'operazione  $*$  gode della associatività e quindi la struttura algebrica  $(\mathcal{W}_A, *)$  è un monoide ( $w_0$  elemento neutro), detto il monoide delle parole su  $A$ .

### 3.6 Sottostrutture

Abbiamo visto che quando una parte è chiusa si può considerare la sua struttura indotta, se si sta in una struttura algebrica con una certa proprietà si è interessati alle sottostrutture che mantengono quella proprietà, ad esempio se sono in un semigruppone sono interessati alle strutture che sono ancora semigruppone, queste strutture vengono chiamate sottostrutture. Diamo le seguenti definizioni:

- Sia  $(S, \cdot)$  un semigruppone, una parte  $H \neq \emptyset$  di  $S$  si dice **sottosemigruppone** di  $S$  se  $H$  è chiusa rispetto al prodotto e la struttura  $(H, \cdot)$  è a sua volta un semigruppone.

Si osserva che se  $H$  è chiusa in un semigruppone è sicuramente un sottosemigruppone.

- Sia  $(S, \cdot)$  un monoide con unità  $1_S$  (elemento neutro rispetto l'operazione), una parte  $H \neq \emptyset$  di  $S$  si dice **sottomonoide** di  $S$  se  $H$  è chiusa rispetto al prodotto e la struttura  $(H, \cdot)$  è a sua volta un monoide e che l'unità di  $H$  sia la stessa di  $S$  ( $1_H = 1_S$ ).

Esempio:  $(\mathcal{P}(S), \cup)$  è un monodie con unità  $\emptyset$  e sia  $T \subseteq S$ ,  $\mathcal{P}(T)$  è chiuso rispetto a  $\cup$  e quindi  $(\mathcal{P}(T), \cup)$  è un semigruppone con elemento neutro  $\emptyset$  e quindi posso dire che  $\mathcal{P}(T)$  è un sottomonoide di  $(\mathcal{P}(S), \cup)$ . Di contro, se ho il monoide  $(\mathcal{P}(S), \cap)$  con elemento neutro  $S$  e prendo un  $T \subset S$  avrò che  $\mathcal{P}(T)$  è chiuso rispetto a  $\cap$  ma la struttura  $(\mathcal{P}(T), \cap)$  ha elemento neutro  $T \neq S$  quindi anche se monoide,  $\mathcal{P}(T)$  non è un sottomonoide di  $(\mathcal{P}(S), \cap)$ .

- Sia  $(S, \cdot)$  un gruppo (un monoide con tutti gli elementi invertibili), una parte  $H \neq \emptyset$  di  $S$  si dice **sottogruppone** di  $S$  se  $H$  è chiusa rispetto al prodotto e la struttura  $(H, \cdot)$  è composto dall'unità  $1_S \in H$  e se  $\forall x \in H, x^{-1} \in H$  (quindi  $(H, \cdot)$  è un sottomonoide con gli inversi contenuti in  $H$ ).

Esempio:  $(\mathbb{Z}, +)$  è un gruppo,  $\mathbb{N}$  è un sottogruppone di  $\mathbb{Z}$ ? La risposta è no poiché gli opposti non appartengono all'insieme  $\mathbb{Z}$ . Prendiamo ora l'insieme  $2\mathbb{Z} = \{2z | z \in \mathbb{Z}\}$  (l'insieme dei multipli di due, detto anche l'insieme dei numeri pari), esso è un sottogruppone di  $\mathbb{Z}$ , infatti  $2\mathbb{Z}$  è chiuso rispetto alla somma poiché  $\forall 2x, 2y \in 2\mathbb{Z}$  la loro somma  $2x + 2y = 2(x + y) \in 2\mathbb{Z}$ ; inoltre l'elemento neutro è lo stesso di  $\mathbb{Z}$  e  $\forall 2x \in 2\mathbb{Z}$  l'opposto (ovvero l'inverso in notazione additiva)  $-2x = 2(-x) \in 2\mathbb{Z}$ .

Le sottostrutture sono utili poiché una determinata proprietà che esiste per una struttura  $S$  sicuramente esisterà anche per le sue sottostrutture, invece, se una struttura  $S$  non gode di una determinata proprietà una sua sottostruttura (privato di alcuni elementi) potrebbe godere di quella proprietà.

Qualunque sottogruppone di  $\mathbb{Z}$  è del tipo  $m\mathbb{Z} = \{mz | z \in \mathbb{Z}\}$ . Più precisamente,  $\forall m \in \mathbb{Z}$ , l'insieme dei multipli di  $\mathbb{Z}$ , ovvero  $m\mathbb{Z}$ , è un sottogruppone di  $(\mathbb{Z}, +)$ . Si dimostra inoltre la seguente definizione:  **$H$  è un sottogruppone di  $(\mathbb{Z}, +) \Leftrightarrow \exists m \in \mathbb{Z} (H = m\mathbb{Z})$** . Abbiamo già dimostrato che se  $H = m\mathbb{Z}$  è un sottogruppone di  $\mathbb{Z}$  (si dimostra alla stessa maniera dell'esempio visto precedentemente con l'insieme  $2\mathbb{Z}$ ), non verrà trattata l'altra implicazione; ma è importante sapere che tutti i sottogrupponi di  $\mathbb{Z}$  sono del tipo  $m\mathbb{Z}$ .

### 3.7 Potenze e multipli di un elemento

Quando si usa la nozione moltiplicativa si parla di **potenze** in  $(S, \cdot)$ , mentre in notazione additiva si parla di **multipli** in  $(S, +)$  ma fondamentalmente il concetto è lo stesso:

- Sia  $a \in S, \forall n \in \mathbb{N}^*$  si definisce  $a^n$  (potenza di base  $a$  ed esponente  $n$ ) il prodotto di  $a \cdot a \cdot \dots \cdot a$  ( $n$  volte), si scrive anche  $a^n = (a^{n-1}) \cdot a$
- Sia  $a \in S, \forall n \in \mathbb{N}^*$  si definisce  $na$  (multiplo di  $a$  secondo  $n$ ) la somma di  $a + a + \dots + a$  ( $n$  volte).

Per qualunque tipo di operazione posso operare in questo modo e si utilizza il simbolo di potenza, ad esempio se sono nella struttura  $(\mathcal{P}(S), \Delta)$  posso scrivere  $X^2$  per definire  $X\Delta X = \emptyset$ .

Le precedenti definizioni valgono per  $n > 0$ , infatti per  $n = 0$  bisogna aggiungere l'ipotesi che  $(S, \cdot)$  sia un monoide, più precisamente, se  $(S, \cdot)$  è unitario e  $1_S$  è la sua unità definiamo  $a^0 = 1_S$ .

Allo stesso modo se  $(S, +)$  ha elemento neutro  $0_S$  definiamo  $0a = 0_S$ .

Ulteriori ipotesi vanno fatte per  $n < 0$ , supponiamo  $(S, \cdot)$  e  $a$  invertibile, quindi  $\exists a^{-1}$ ; a questo punto definiamo  $a^n = (a^{-1})^n = (a^{-1}) \cdot \dots \cdot (a^{-1})$   $n$  volte. Analogamente per i multipli supponiamo che  $(S, +)$  abbia neutro e che  $a$  sia dotato di opposto e definiamo  $na = (-n)(-a) = (-a) + \dots + (-a)$   $n$  volte.

### 3.8 Proprietà delle potenze e dei multipli

$\forall a, b \in S$  e  $\forall n, m \in \mathbb{Z}$  valgono le seguenti proprietà (quando la scrittura ha senso)

- per la struttura  $(S, \cdot)$ :
  1.  $(a^n)^m = a^{nm}$
  2.  $a^n \cdot a^m = a^{n+m}$
  3. Se  $ab = ba$ ,  $(ab)^n = a^n \cdot b^n$
- per la struttura  $(S, +)$ :
  1.  $m(na) = (mn)(a)$
  2.  $na + ma = (n + m)a$
  3. Se  $a + b = b + a$ ,  $n(a + b) = na + nb$

Per le proprietà 3 si richiede che la struttura debba essere un semigruppato poiché  $a$  e  $b$  devono commutare.

### 3.9 Isomorfismo di strutture algebriche

Due strutture sono isomorfe se hanno la stessa struttura a meno del nome degli oggetti ed eventualmente il simbolo dell'operazione. Formalmente, due strutture sono isomorfe quando c'è una applicazione biettiva tra i due insiemi.

Siano  $(S, *)$  e  $(T, \blacksquare)$  due strutture algebriche,  $S$  e  $T$  si dicono **isomorfe** se esiste  $f: S \rightarrow T$  biettiva e tale che  $\forall x, y \in S$   $(f(x * y) = f(x) \blacksquare f(y))$ .

Per definizione un isomorfismo è una applicazione biettiva che verifica la proprietà  $f(x * y) = f(x) \blacksquare f(y)$  e due strutture sono isomorfe se esiste un isomorfismo tra  $S$  e  $T$ . In particolare, tutte le strutture isomorfe ad una determinata struttura avranno le sue stesse proprietà. Di conseguenza se  $1_S$  è elemento neutro di  $S$  allora l'elemento neutro di  $T$  sarà semplicemente  $f(1_S)$ .

Esempio di struttura isomorfa: sia la struttura  $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$  dove  $\forall (a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$  definiamo  $(a, b) + (c, d) = (a + c, b + d)$  mentre  $(a, b) \cdot (c, d) = (ac, bd)$ , consideriamo l'insieme  $\mathbb{Z} \times \{0\} = \{(a, 0) | a \in \mathbb{Z}\}$  e questa parte si dimostra essere chiusa rispetto a  $\cdot$  e rispetto a  $+$ , infatti  $\forall (a, 0), (b, 0) \in \mathbb{Z} \times \{0\} = T$  si ha  $(a, 0) + (b, 0) = (a + b, 0) \in T$  e  $(a, 0) \cdot (b, 0) = (ab, 0) \in T$ . Chiediamoci ora se  $(T, +)$  è isomorfo a  $(\mathbb{Z}, +)$ : prendiamo la funzione  $f: n \in \mathbb{Z} \rightarrow (n, 0) \in T$  e consideriamo  $f(n + m) = (n + m, 0) = (n, 0) + (m, 0) = f(n) + f(m)$ , quindi si mantiene l'operazione e di conseguenza le strutture sono isomorfe. Si esegua come esercizio questo procedimento per l'operatore  $\cdot$ .

Più in generale, se  $(S, *)$  e  $(T, \blacksquare)$  sono strutture algebriche si dice **omomorfismo** di  $S$  in  $T$  una applicazione  $f: S \rightarrow T$  (non viene richiesta la biettività) tale che  $\forall x, y \in S$   $(f(x * y) = f(x) \blacksquare f(y))$  (proprietà di conservare le operazioni).

### 3.10 Anelli

Sia  $(A, +, \cdot)$  una struttura algebrica a due operazioni,  $A$  si dice un **anello** se e solo se:

1.  $(A, +)$  è un gruppo abeliano
  - a. Somma associativa
  - b. Dotato di elemento neutro
  - c. Ogni elemento è dotato di opposto
  - d. Sia commutativo
2.  $(A, \cdot)$  è un semigruppato
  - a. Prodotto associativo
3.  $\cdot$  è distributivo rispetto a  $+$  (a destra e a sinistra)

Un anello  $(A, +, \cdot)$  si dice **commutativo** se il prodotto è commutativo; si dice anello **unitario** se  $(A, \cdot)$  ha elemento neutro



Esempi:  $(\mathbb{Z}, +, \cdot)$  è un anello commutativo unitario;  $(\mathbb{Q}, +, \cdot)$  e  $(\mathbb{R}, +, \cdot)$  sono anelli commutativi unitari,  $(\mathbb{N}, +, \cdot)$  non è un anello ( $(\mathbb{N}, +)$  non è un gruppo),  $(\mathcal{P}(S), \Delta, \cap)$  è un anello commutativo unitario. Sia  $S \neq \emptyset$   $(\mathcal{P}(S), \cup, \cap)$  non è un anello (né  $(\mathcal{P}(S), \cup)$ , né  $(\mathcal{P}(S), \cap)$  sono gruppi)

Esercizio: Definiamo in  $\mathbb{Z} \times \mathbb{Z}$  le seguenti operazioni:  $\forall (a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}: (a, b) + (c, d) = (a + c, b + d)$  e  $(a, b) \cdot (c, d) = (ac, bd)$ . Sapendo che  $(\mathbb{Z}, +, \cdot)$  è un anello commutativo unitario dimostrare che  $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$  sia un anello commutativo unitario.

### Proprietà di un anello:

- In un anello  $(A, +, \cdot)$  ogni elemento  $a \in A$  è invertibile rispetto alla somma; quindi, ogni  $a \in A$  è cancellabile rispetto a  $+$ .

- Regole di calcolo per un anello.

Siano  $A$  un anello,  $0_A$  l'elemento neutro di  $(A, +)$  e  $a, b \in A$ . Allora:

1.  $a \cdot 0_A = 0_A \cdot a = 0_A$

Dim.:  $a \cdot 0_A = a(0_A + 0_A) = a0_A + a0_A$  ma essendo anche  $a0_A = a0_A + 0_A$  risulta dunque  $a0_A + a0_A = a0_A + 0_A$  e cancellando  $a0_A$  risulta  $a \cdot 0_A = 0_A$ , si dimostri come esercizio il caso analogo  $0_A \cdot a = 0_A$ .

2.  $(-a)b = a(-b) = -ab$  (il meno si legge come "opposto di")

Dim.: dimostriamo  $a(-b) = -ab$ , il caso analogo  $(-a)b = -ab$  si lascia come esercizio. Scriviamo:  $a(-b) + ab = a(-b + b) = a0_A = 0_A$ , abbiamo così dimostrato che l'opposto di  $ab$ , è  $a(-b)$ , ma essendo un gruppo ogni elemento è cancellabile rispetto alla somma e quindi si ha anche  $-ab + ab = 0_A$ , poiché l'opposto è unico deve essere  $a(-b) = -ab$ .

- NON è vero che dato un anello si ha sempre che se  $ab = 0_A$  allora o  $a = 0_A$  oppure  $b = 0_A$

Esempio: in  $\mathbb{Z}$  si ha che  $ab = 0 \Leftrightarrow a = 0 \vee b = 0$ , ma prendiamo l'anello  $(\mathcal{P}(S), \Delta, \cap)$  dove  $X \in \mathcal{P}(S) | \emptyset \subset X \subset S$  e vediamo se  $X \cap Y = \emptyset$  (che rappresenta praticamente  $X \cdot Y = 0$ ),  $X$  è diverso dal vuoto essendo per ipotesi  $\emptyset \subset X$ , inoltre  $X \subset S$  ci dice che  $Y = S \setminus X \neq \emptyset$ .

- Se  $(A, +, \cdot)$  è un anello posso definire in  $A \times A$  le seguenti operazioni:  $\forall (a, b), (c, d) \in A \times A$   $(a, b) + (c, d) = (a + c, b + d)$  e  $(a, b) \cdot (c, d) = (ac, bd)$ . L'anello così costruito (perché è sempre un anello) si definisce **anello prodotto** e sarà commutativo e/o unitario se  $(A, +, \cdot)$  è commutativo/unitario.

### 3.11 Divisori dello zero per un anello

Sia  $(A, +, \cdot)$  e sia  $a \in A \setminus \{0\}$  (ovvero  $a \neq 0$ ), si dice divisore dello zero sinistro se e solo se,  $\exists b \in A \setminus \{0\}$  tale che  $ab = 0$ .

Sia  $(A, +, \cdot)$  e sia  $a \in A \setminus \{0\}$ , si dice divisore dello zero destro se e solo se,  $\exists b \in A \setminus \{0\}$  tale che  $ab = 0$ .

Se  $A$  è commutativo,  $a \in A$  è divisore dello zero sinistro se e solo se, è divisore dello zero destro. Si parla di divisore dello zero. Inoltre,  $A$  possiede divisore dello zero destro se e solo se, ha divisore dello zero sinistro. Per definizione 0 non è divisore dello zero quindi in  $\mathbb{Z}$  non ci sono divisori dello zero poiché  $\forall a, b \in \mathbb{Z}$  si ha  $ab = 0 \Leftrightarrow a = 0 \vee b = 0$ .

### Elementi di $(A, +, \cdot)$ cancellabili rispetto al prodotto ( $A \neq \{0\}$ )

- $0_A$  non è cancellabile poiché abbiamo visto che  $\forall a \in A, 0_A \cdot a = 0_A = 0_A \cdot a$  e quindi se  $0_A$  fosse cancellabile allora tutti gli elementi di  $A$  sarebbero uguali a zero, ma  $A \neq \{0\}$ .

- Anche i divisori dello zero non sono cancellabili, infatti se  $a \in A \setminus \{0\}$  è divisore dello zero sinistro,  $a$  non è cancellabile a sinistra poiché  $\exists b \in A \setminus \{0\} (ab = 0)$  ma quindi poiché ho  $ab = 0 \wedge 0 = 0$  se  $a$  fosse cancellabile dovrei avere  $ab = a0 \Leftrightarrow b = 0$  ma  $b \neq 0$  per ipotesi.

**Proposizione:** Sia  $A$  un anello e sia  $a \in A \setminus \{0\}$ . Allora  $a$  è divisore dello zero sinistro (rispettivamente destro) se e solo se,  $a$  non è cancellabile a sinistra (rispettivamente a destra).

**Dimostrazione:** Se  $a$  è divisore dello zero sinistro allora  $a$  non è cancellabile a sinistra (come osservato precedentemente). Sia  $a \in A \setminus \{0\}$  non cancellabile a sinistra, essendo per definizione  $a$  cancellabile a sinistra  $\Leftrightarrow \forall b, c \in A (ab = ac \Rightarrow b = c)$  la sua negazione è:  $a$  non è cancellabile a sinistra  $\Leftrightarrow \exists b, c \in A (ab = ac \wedge b \neq c)$ . Si ha a questo punto  $ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b - c) = 0$  ma poiché  $b \neq c$  questo implica che  $b - c \neq 0$ , ma allora  $a$  è divisore dello zero sinistro.

Un anello  $A$  si dice **intero** se  $A$  è privo di divisori dello zero. Se  $A$  è intero  $\forall a, b \in A \quad ab = 0 \Leftrightarrow a = 0 \vee b = 0$ , in questo caso si dice che in  $A$  vale la **legge di annullamento del prodotto**. Si osserva che in un anello  $A$  vale la legge di annullamento del prodotto se e solo se  $A \setminus \{0\}$  è chiusa rispetto al prodotto (un altro modo per descrivere la legge di annullamento del prodotto).

### 3.12 Elementi invertibili in un anello unitario, campi e dominio di integrità

Sia  $A$  un anello unitario e sia  $1_A$  l'unità di  $(A, \cdot)$ , un elemento  $a \in A$  si dice **invertibile** se e solo se  $a$  è invertibile rispetto al prodotto. Sarebbe, praticamente,  $\mathcal{U}((A, \cdot))$  dove  $\exists a' \in A | aa' = a'a = 1_A$ .

Se  $A \neq 0$ ,  $0$  non è mai invertibile. Se  $A$  è un anello unitario non nullo succede solo che  $0 \neq 1_A$ .

Un anello non nullo unitario in cui sono invertibili tutti gli elementi di  $A \setminus \{0\}$  si dice un **corpo**. Se un corpo è pure commutativo si dice campo. Quindi un **campo** è un corpo commutativo, ovvero un anello commutativo unitario non nullo in cui tutti gli elementi non nulli sono invertibili.

Esempi:  $(\mathbb{Q}, +, \cdot)$  è un campo,  $(\mathbb{Z}, +, \cdot)$  non è un campo,  $(\mathbb{R}, +, \cdot)$  è un campo.

Se  $a \in A$  ed  $a$  è invertibile allora sicuramente  $a$  è cancellabile e quindi  $a$  non è divisore dello zero.

Se  $A$  è un campo,  $\forall a \in A \setminus \{0\} \Rightarrow a$  è invertibile  $\Rightarrow a$  non è divisore dello zero. Quindi ogni campo (corpo) è un anello intero, in generale  $a$  cancellabile non implica  $a$  invertibile (ad esempio nell'anello  $\mathbb{Z}$  tutti gli elementi non nulli sono cancellabili ma solo  $1$  e  $-1$  sono invertibili).

Un anello  $A$  si dice un **dominio di integrità** se  $A$  è un anello commutativo unitario privo di divisori dello zero. Ogni campo è un dominio di integrità ma ogni dominio di integrità non è detto che sia un campo.

### 3.13 Sottoanello di un anello

Sia  $(A, +, \cdot)$  un anello e sia  $H$  una parte non vuota di  $A$ .  $H$  si dice sottoanello di  $A$  se e solo se:

1.  $H$  è chiusa rispetto a  $+$  e  $\cdot$  ( $\forall x, y \in H, x + y \in H \wedge xy \in H$ )
2.  $(H, +, \cdot)$  è un anello:
  - 1)  $(H, +)$  è un gruppo abeliano ( $H$  è sottogruppo di  $(A, +)$ )  
(si riduce a verificare che lo zero stia in  $H$  e che gli opposti elementi di  $H$  siano ancora in  $H$ , poiché le altre proprietà sono verificate essendo che  $H$  è chiusa rispetto a  $+$  e  $\cdot$ )
  - 2)  $(H, \cdot)$  è un semigruppato (è sempre così non c'è bisogno di verificarlo)
  - 3)  $\cdot$  è distributivo rispetto a  $+$  (sempre verificata)
3. Se  $A$  è un anello unitario,  $H$  è un anello unitario con la stessa unità di  $A$

Sottoanelli di  $(\mathbb{Z}, +, \cdot)$ : Se  $H$  è un sottoanello di  $\mathbb{Z}$ ,  $H$  sarà un sottogruppo di  $(\mathbb{Z}, +) \Rightarrow \exists m \in \mathbb{Z} | H = m\mathbb{Z}$ . Se  $H$  è sottoanello unitario di  $\mathbb{Z}$  unitario,  $1$  deve appartenere ad  $H \Rightarrow m = \pm 1 \Rightarrow H = \mathbb{Z}$ . Di conseguenza il gruppo  $(m\mathbb{Z}, +, \cdot)$  è sempre un anello e l'unico anello unitario di  $\mathbb{Z}$  è  $\mathbb{Z}$  stesso.

Sottoanelli banali di  $A$  saranno semplicemente  $A$  e  $\{0_A\}$ , quest'ultimo è detto sottoanello nullo.

### 3.14 Anelli isomorfi

Siano  $(A, +, \cdot)$  e  $(B, \oplus, *)$  anelli.  $A$  e  $B$  si dicono **isomorfi** se esiste una applicazione  $f: A \rightarrow B$  biettiva e tale che  $\forall x, y \in A$  si ha  $f(x + y) = f(x) \oplus f(y)$  e  $f(xy) = f(x) * f(y)$ . Anelli isomorfi condividono le proprietà.



### 3.15 Relazioni d'ordine

Sia  $A$  un insieme non vuoto,  $\rho (\subseteq A \times A)$  una relazione binaria in  $A$ .  $\rho$  si dice una **relazione d'ordine** in  $A$  se e solo se verifica tre proprietà:

1.  $\rho$  è riflessiva:  $\forall a \in A, a \rho a$
2.  $\rho$  è antisimmetrica:  $\forall a, b \in A (a \rho b \wedge b \rho a \Rightarrow a = b)$
3.  $\rho$  è transitiva:  $\forall a, b, c \in A (a \rho b \wedge b \rho c \Rightarrow a \rho c)$

Le relazioni d'ordine notevoli a cui si fa spesso riferimento sono le seguenti:

- Relazione di ordine usuale in  $\mathbb{Z}$ :  $\forall a, b \in \mathbb{Z}, a \leq b \Leftrightarrow \exists n \in \mathbb{N} | a + n = b$   
Dimostrare per esercizio che verifica le proprietà di relazione d'ordine
- L'inclusione in  $\mathcal{P}(S)$ :  $\forall X, Y \in \mathcal{P}(S) X \rho Y \Leftrightarrow X \subseteq Y$ 
  1. Ogni  $X$  è contenuto in se stesso quindi c'è la riflessività
  2. Se  $X \subseteq Y \wedge Y \subseteq X$ , per definizione,  $X = Y$
  3.  $X \subseteq Y \wedge Y \subseteq Z \Rightarrow X \subseteq Z$  (dimostrata nel [capitolo 1.](#))
- La divisibilità in  $\mathbb{N}$ :  $\forall a, b \in \mathbb{N} a \rho b \Leftrightarrow a|b \Leftrightarrow \exists c \in \mathbb{N} | b = ac$  ([capitolo 4.1](#))
  1.  $\forall a|a$  ( $a = a \cdot 1$ )
  2.  $\forall a, b \in \mathbb{N} a|b \wedge b|a \Rightarrow a = b$  (la proprietà  $\forall a, b \in \mathbb{Z}, a|b \wedge b|a \Leftrightarrow a = \pm b$  dimostrata in  $\mathbb{Z}$  nel capitolo successivo vale in  $\mathbb{N}$  solo per i numeri positivi, dunque  $a = b$ )
  3.  $a|b \wedge b|c \Rightarrow a|c$  (dimostrata successivamente)

Se  $\rho$  è una relazione d'ordine in  $A$ , la coppia  $(A, \rho)$  si dice **insieme ordinato**. Ovviamente  $\rho$  viene sostituito con il simbolo della relazione, quindi, le precedenti relazioni d'ordine saranno, rispettivamente, le seguenti coppie ordinate:  $(\mathbb{Z}, \leq)$ ,  $(\mathcal{P}(S), \subseteq)$  e  $(\mathbb{N}, |)$ .

In generale se  $\rho$  è di ordine in  $A$ ,  $\rho$  viene sostituita dal simbolo  $\leq$ .  $a \leq b$  ( $a$  minore o uguale a  $b$ ), mentre si usa  $a < b$  ( $a$  strettamente minore di  $b$ )  $\Leftrightarrow a \leq b \wedge a \neq b$ , analogamente  $A \subset B \Leftrightarrow A \subseteq B \wedge A \neq B$ . Entrambe le relazioni sono relazioni d'ordine,  $\leq$  si dice di ordine **largo** mentre  $<$  si dice di ordine **stretto**.

Se  $\leq$  è una relazione di ordine in  $A$ :  $\forall a, b \in A$  scriverà  $a \geq b$  ( $a$  maggiore o uguale di  $b$ )  $\Leftrightarrow b \leq a$ .

Se  $(A, \leq)$  è un **insieme ordinato** e  $B \subseteq A$ , la relazione  $\sigma$  così definita in  $B$ :  $\forall x, y \in B x \sigma y \Leftrightarrow x \leq y$  è di ordine in  $B$  e per  $\sigma$  si usa ancora il simbolo  $\leq$ .  $\sigma$  si dice **relazione di ordine indotta in  $B$** .

Sia  $(A, \leq)$  un insieme ordinato e siano  $a, b \in A$ .  $a$  e  $b$  si dicono **confrontabili** se e solo se  $a \leq b \vee b \leq a$ .

Un insieme  $A$  si dirà **totalmente ordinato** se tutti gli elementi di  $A$  sono a due a due confrontabili.

Ad esempio, per le relazioni notevoli viste prima  $(\mathbb{Z}, \leq)$  è totalmente ordinato, mentre  $(\mathcal{P}(S), \subseteq)$  con  $S$  insieme di almeno due elementi si ha che per  $x, y \in S, x \neq y$  gli insiemi  $\{x\}$  e  $\{y\}$  non sono confrontabili e quindi  $(\mathcal{P}(S), \subseteq)$  non è totalmente ordinato. Anche  $(\mathbb{N}, |)$  non è totalmente ordinato poiché,  $4 \nmid 5 \wedge 5 \nmid 4$ .

Una relazione d'ordine  $\leq$  in  $A$  è **totale** se e solo se  $\forall x, y \in A (x \leq y \vee y \leq x)$ . Di conseguenza, una relazione d'ordine  $\leq$  in  $A$  **non** è **totale** se e solo se  $\exists x, y \in A | x \not\leq y \wedge y \not\leq x$  (quindi per dire che una relazione non è totale basta trovare due elementi non confrontabili)

Sia  $f: A \rightarrow B$  una applicazione e sia  $\leq$  una relazione di ordine in  $B$ . È possibile definire in  $A$  una relazione  $\Sigma_f$  (che risulta di ordine) nel modo seguente:  $\forall x, y \in A | x \Sigma_f y \Leftrightarrow x = y \vee f(x) < f(y)$ .

Dimostriamo a questo punto che la relazione  $\Sigma_f$  è di ordine (gli esercizi che chiedono di provare che la relazione sia di ordine si svolgono in maniera analoga):  $\Sigma_f$  è riflessiva,  $\forall x \in A, x \Sigma_f x$  perché  $x = x$ . La seconda proprietà da dimostrare è che  $\Sigma_f$  sia antisimmetrica. Se  $(A, \leq)$  è ordinato, e  $a, b \in A$ , non può essere vero che  $a < b \wedge b < a$ , di conseguenza  $a \leq b \wedge b \leq a \Leftrightarrow a = b$  quindi  $\Sigma_f$  è antisimmetrica poiché supponendo, per assurdo,  $x \neq y$ , l'ipotesi diventa  $f(x) < f(y) \wedge f(y) < f(x)$  e ciò è impossibile per l'osservazione fatta precedentemente, quindi si avrà che  $x \Sigma_f y \wedge y \Sigma_f x \Rightarrow x = y$  (antisimmetria). Resta ora da provare che  $\Sigma_f$  è

transitiva, ovvero  $\forall x, y, z \in A (x \Sigma_f y \wedge y \Sigma_f z \Rightarrow x \Sigma_f z)$ . Nel caso in cui sia  $x = y$  possiamo sostituire  $y$  nella precedente relazione con  $x$  ed è banale quindi che  $x \Sigma_f z$ , allo stesso modo si procede nel caso  $y = z$  (quando si ha l'uguaglianza la tesi coincide con l'ipotesi). Rimane il caso  $x \neq y$  e  $y \neq z$ , dunque, la mia ipotesi diverrà  $f(x) < f(y) \wedge f(y) < f(z) \Rightarrow f(x) < f(z)$ , dunque anche  $x$  e  $z$  sono in relazione, C.V.D.

**Osservazione:** Se  $f$  non iniettiva  $\Rightarrow \Sigma_f$  non totale (il viceversa non sussiste) ( $f$  non iniettiva  $\Rightarrow \exists x, y \in A \mid x \neq y \wedge f(x) = f(y) \Rightarrow x$  non è in relazione con  $y$  e  $y$  non è in relazione con  $x \Rightarrow \Sigma_f$  non è totale).

Esempio: Sia  $f: (x, y) \in \mathbb{N} \times \mathbb{N} \rightarrow xy \in \mathbb{N}$ , sappiamo che  $\mathbb{N}$  è un insieme ordinato ed ha due relazioni d'ordine, ovvero la relazione d'ordine usuale  $(\mathbb{N}, \leq)$  e la relazione d'ordine  $(\mathbb{N}, \mid)$ . Prendiamo la prima e chiamiamola  $\Sigma_f$  in  $\mathbb{N} \times \mathbb{N}$ , abbiamo  $\forall (x, y), (z, t) \in \mathbb{N} \times \mathbb{N}, (x, y) \Sigma_f (z, t) \Leftrightarrow (x, y) = (z, t) \vee xy < zt$ ; se io ho la coppia  $(0, 0)$ , sarà  $(0, 0) \Sigma_f (x, y) \Leftrightarrow (0, 0) = (x, y) \vee 0 < xy$ . Il secondo tipo era la relazione  $(\mathbb{N}, \mid)$ , cioè  $\forall (x, y), (z, t) \in \mathbb{N} \times \mathbb{N}, (x, y) \bar{\Sigma}_f (z, t) \Leftrightarrow (x, y) = (z, t) \vee (xy \mid zt \wedge xy \neq zt)$ , ad esempio, chiediamoci se la coppia  $(3, 2) \bar{\Sigma}_f (6, 4)$ , la risposta è sì, poiché  $3 \cdot 2 \mid 6 \cdot 4$ ;  $(3, 2) \bar{\Sigma}_f (6, 1)$ ? No, poiché le immagini sono uguali.

Siano  $(S, \leq)$  e  $(T, \leq^*)$  insiemi ordinati. Una applicazione  $f: S \rightarrow T$  si dice un **isomorfismo** se e solo se:

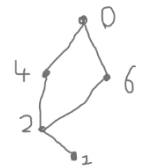
- 1)  $f$  è biettiva
- 2)  $\forall x, y \in S (x \leq y \Leftrightarrow f(x) \leq^* f(y))$

### 3.16 Diagramma di Hasse

Il diagramma di Hasse è un metodo grafico utile per capire come gli elementi di un insieme ordinato si dispongono gli uni con gli altri. Il diagramma di Hasse si disegna in maniera molto intuitiva.

Sia  $(X, \leq)$  un insieme ordinato finito, per disegnare un diagramma di Hasse seguono tre regole:

1. Ogni elemento di  $X$  si rappresenta con un punto
2. Se  $x < y$  il punto  $x$  si disegna più in basso rispetto al punto  $y$
3. Se  $x < y \wedge \nexists z \in X \mid x < z < y$ , i punti  $x$  e  $y$  si uniscono con un segmento



A destra un esempio con l'insieme  $X = \{0, 1, 2, 4, 6\}$  ordinato con la divisibilità, quindi  $(X, \mid)$

Un insieme finito totalmente ordinato viene definito **catena** per la forma rappresentata dal diagramma di Hasse, ad esempio l'insieme  $X = \{0, 1, 2, 4, 6\}$  con la relazione  $(X, \leq)$ .

### 3.17 Minimo e massimo in un insieme ordinato

Sia  $(S, \leq)$  un insieme ordinato, un elemento  $a \in S$  si dice **minimo** di  $S$  se e solo se  $\forall x \in S (a \leq x)$ , rispettivamente, un elemento  $a \in S$  si dice **massimo** di  $S$  se e solo se  $\forall x \in S (x \leq a)$ .

Il minimo (rispettivamente massimo), se esiste, è **unico**. Supponiamo che due elementi  $a, b$  siano minimi di  $S$ , avremo che  $\forall x \in S (a \leq x) \Rightarrow a \leq b$ , analogamente,  $\forall x \in S (b \leq x) \Rightarrow b \leq a$  e quindi per la proprietà di antisimmetria si avrà  $a = b$ . Denoteremo  $a = \min S$  (rispettivamente, per il massimo,  $a = \max S$ ).

Esempi: Sia  $(\mathbb{Z}, \leq)$  (ordine usuale) si ha che non esiste né minimo e né massimo. Sia, invece,  $(\mathbb{N}, \leq)$  (ordine usuale) avremo  $\exists \min \mathbb{N} = 0, \nexists \max \mathbb{N}$ . Prendiamo ora, la relazione  $(\mathbb{N}, \mid)$ , avremo  $\min \mathbb{N} = 1$  e  $\max \mathbb{N} = 0$ . Sia  $(\mathcal{P}(S), \subseteq)$ , abbiamo  $\min \mathcal{P}(S) = \emptyset$ , mentre,  $\max \mathcal{P}(S) = S$ .

Un insieme  $(S, \leq)$  si dice **bene ordinato** (o di buon ordine) se e solo se  $\forall X \subseteq S (X \neq \emptyset \Rightarrow \exists \min X)$ .

Un insieme  $(S, \leq)$  totalmente ordinato non implica che sia bene ordinato (ne fa da esempio l'insieme  $(\mathbb{Z}, \leq)$ ), ma qualunque insieme ben ordinato è sempre totalmente ordinato (poiché esiste il minimo per ogni sottoinsieme ne segue che  $\min\{x, y\} = x \Rightarrow x \leq y$  mentre  $\min\{x, y\} = y \Rightarrow y \leq x$  e di conseguenza la proprietà di insieme totalmente ordinato è sempre rispettata:  $\forall x, y \in S (x \leq y \vee y \leq x)$ ).

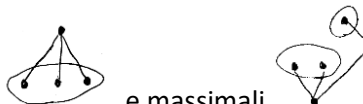
Prendiamo adesso  $(A, \Sigma_f)$ , la proprietà effettiva che richiediamo per il minimo è che sia strettamente minore degli altri elementi, essendo sempre minore di sé stesso per la riflessività. Si ricorda che  $f: A \rightarrow B, \forall x, y \in A$

$x \Sigma_f y \Leftrightarrow x = y \vee f(x) < f(y)$ . Di conseguenza se  $a = \min A \Rightarrow \forall x \in A \setminus \{a\}, a \Sigma_f x \Rightarrow f(a) < f(x)$  (chiaramente la stessa cosa vale per il massimo:  $a = \max A \Rightarrow \forall x \in A \setminus \{a\}, a \Sigma_f x \Rightarrow f(x) < f(a)$ ).

Esempi: Sia  $f: (x, y) \in \mathbb{N} \times \mathbb{N} \rightarrow x + y \in \mathbb{N}$ . Prendiamo in considerazione  $(\mathbb{N} \times \mathbb{N}, \Sigma_f)$ , avremo  $(a, b) = \min(\mathbb{N} \times \mathbb{N}) \Leftrightarrow \forall (c, d) \neq (a, b), a + b < c + d$ , il minimo così definito è la coppia  $(0, 0) = \min(\mathbb{N} \times \mathbb{N})$ . Se invece, prendiamo l'applicazione  $f: (x, y) \in \mathbb{N} \times \mathbb{N} \rightarrow xy \in \mathbb{N}$  e prendiamo l'insieme  $(\mathbb{N} \times \mathbb{N}, \Sigma_f)$  risulterà  $(a, b) = \min(\mathbb{N} \times \mathbb{N}) \Leftrightarrow \forall (c, d) \neq (a, b), ab < cd$ , è evidente che prendendo le due coppie  $(0, 1)$  e  $(1, 0)$  si avrà  $ab \not< cd$  e quindi questi elementi non sono minimo (hanno immagine minima, ma ciò è diverso).  
 $f: n \in \mathbb{N} \rightarrow \{n\} \in \mathcal{P}(\mathbb{N})$  con la relazione di inclusione.  $f$  è iniettiva, vediamo se la relazione  $\Sigma_f$  è totale o no.  $\forall n, m \in \mathbb{N}, n \Sigma_f m \Leftrightarrow n = m \vee \{n\} \subset \{m\}$ , evidentemente l'ultima equazione non sarà mai rispettata, quindi diventa, praticamente una relazione di uguaglianza:  $\forall n, m \in \mathbb{N}, n \Sigma_f m \Leftrightarrow n = m$  e quindi non è totale.

### 3.18 Elementi minimali ed elementi massimali in un insieme ordinato

Sia  $(S, \leq)$  un insieme ordinato.  $a \in S$  è **minimale** in  $S \Leftrightarrow \nexists x \in S | x < a \Leftrightarrow \forall x \in S (x \leq a \Rightarrow x = a)$ , analogamente,  $a \in A$  è **massimale** in  $S \Leftrightarrow \nexists x \in S | a < x \Leftrightarrow \forall x \in S (a \leq x \Rightarrow a = x)$ .



Nei diagrammi di Hasse si notato subito: Minimali e massimali

Ad esempio, in  $(\mathcal{P}(S) \setminus \emptyset, \subseteq)$  i minimali sono tutti e soli i singleton, si osservi che i minimali possono essere infiniti, a differenza del minimo che è unico, ovviamente lo stesso vale per i massimali.

Se  $a = \min S$ ,  $a$  è anche minimale in  $S$ . Inoltre,  $a$  è l'unico minimale di  $S$ , infatti, se  $b$  è diverso da  $a$ , e  $b$  è minimale in  $S$ ,  $a \leq b \wedge a \neq b \Rightarrow a < b \Rightarrow b$  non è minimale (stesso vale per il massimo e il massimale).

$a$  unico minimale  $\nRightarrow a$  minimo, eccetto per un caso. Sia  $a \in S$ ,  $a = \min S \Leftrightarrow \forall x \in S | a \leq x$ , mentre  $a$  è minimale in  $S \Leftrightarrow \forall x \in S$  confrontabile con  $a$ ,  $a \leq x$ , di conseguenza nel caso in cui  $(S, \leq)$  è totalmente ordinato se  $a$  è minimale  $\Rightarrow a$  sarà confrontabile con tutti, e quindi  $a$  risulta essere anche minimo in  $S$ .

Se  $(S, \leq)$  è finito,  $S$  ha sempre massimali e minimali, cosa che non succede con insiemi infiniti.

Esercizi: Trovare nei seguenti insiemi ordinati minimo, minimali, massimo, massimali:  $(\mathbb{N} \setminus \{0\}, |)$ ,  $(\mathbb{N} \setminus \{1\}, |)$  e  $(X, \sigma)$  dove  $X = \{1, 0, -1\}$  e  $(a, b) \sigma (c, d) \Leftrightarrow (a, b) = (c, d) \vee ab < cd$  (fare diagramma di Hasse di  $X$ ).

### 3.19 Minoranti e maggioranti

Sia  $(S, \leq)$  un insieme ordinato, e sia  $X \subseteq S$ .  $a \in S$  si dice un **minorante** di  $X$  se e solo se  $\forall x \in X (a \leq x)$ .

Sia  $(S, \leq)$  un insieme ordinato, e sia  $X \subseteq S$ .  $a \in S$  si dice un **maggiorante** di  $X$  se e solo se  $\forall x \in X (x \leq a)$ .

Osservazione: è praticamente la stessa definizione di minimo e massimo, l'unica differenza è che il minorante, o maggiorante, non deve essere contenuto per forza nell'insieme  $X$ . Quindi,  $a = \min X \Rightarrow a$  è un minorante di  $X$ , mentre, se  $a$  è un minorante di  $X \wedge a \in X \Rightarrow a = \min X$ .

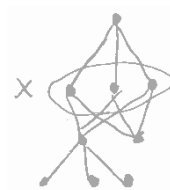
Esempi: Sia  $(\mathbb{N}, \leq)$  e  $X = \{2, 3\} \in \mathbb{N}$ , abbiamo che  $2 = \min X$  e  $3 = \max X$  mentre i minoranti sono  $0, 1, 2$ ; invece, i maggioranti sono  $a \in \mathbb{N} | a \geq 3$ . Sia ora  $(\mathbb{N}, |)$ , i minoranti di  $X$  sono: nel caso in cui appartenga ad  $X$  allora è il minimo di  $X$ , ed in questo caso non c'è; vediamo ora il caso in cui il minorante non appartenga ad  $X$ ,  $a | 2 \wedge a | 3$  ( $a \neq 2, 3$ ), in questo caso l'unico minorante è  $a = 1$ . I maggioranti di  $\{2, 3\}$ : Caso 1: non c'è massimo quindi non ci sono maggioranti. Caso 2:  $a \notin X, 2 | a \wedge 3 | a$ , quindi sono tutti e soli i multipli di 6. Mettiamoci in  $\mathbb{N} \times \mathbb{N}$ ,  $(a, b) \sigma (c, d) \Leftrightarrow (a, b) = (c, d) \vee ab < cd$ , sia  $X = \{(a, b) \in \mathbb{N} \times \mathbb{N} | a = 0 \vee b = 0\}$  è evidente che  $X$  non ha né minimo né massimo, quindi, dobbiamo cercare un minorante fuori dall'insieme  $X$ . I minoranti di  $X$  sono  $(a, b) \in \mathbb{N} \times \mathbb{N} | ab < 0$  ed è evidente che non esistono; mentre i maggioranti sono tutti e soli  $(a, b) \in \mathbb{N} \times \mathbb{N} | ab < 0$  e quindi l'insieme  $\mathbb{N} \times \mathbb{N} \setminus X$ .

### 3.20 Estremo inferiore ed estremo superiore di un sottoinsieme $X$ di $S$

Sia  $(S, \leq)$  un insieme ordinato e sia  $X \subseteq S$ . Si dice **estremo inferiore** di  $X$ , e si scrive  $\inf X$ , il massimo, se esiste, dell'insieme dei minoranti di  $X$ .

Sia  $(S, \leq)$  un insieme ordinato e sia  $X \subseteq S$ . Si dice **estremo superiore** di  $X$ , e si scrive  $\sup X$ , il minimo, se esiste, dell'insieme dei maggioranti di  $X$ .

Quando cerchiamo l'estremo superiore andiamo a scegliere prima gli elementi più grandi, nel diagramma di Hasse a destra il nostro maggiorante sarà il punto in alto fuori dall'insieme, esso è anche l'unico dei maggioranti e quindi sarà il nostro estremo superiore. I minoranti sono anche ben evidenti, ma in questo caso non c'è un massimo tra i minoranti e quindi non si ha estremo inferiore.



In simboli, è estremo inferiore e superiore se gode di due proprietà. Sia  $z \in S$ :

$$z = \inf X \Leftrightarrow \begin{array}{l} 1) \forall x \in X, z \leq x \\ 2) \forall t \in S (\forall x \in X, (t \leq x)) \Rightarrow t \leq z \end{array} \quad z = \sup X \Leftrightarrow \begin{array}{l} 1) \forall x \in X, x \leq z \\ 2) \forall t \in S (\forall x \in X, (x \leq t)) \Rightarrow z \leq t \end{array}$$

Esempio: Sia  $X = S$  ( $S = X$  come sottoinsieme di  $S$ ). Si ha che  $a$  è minorante di  $X \Leftrightarrow a$  è il minimo di  $S$ , allo stesso modo,  $a = \inf S \Leftrightarrow a = \min S$ . Da questo esempio si può dedurre che i concetti di estremo inferiore e superiore ha senso usarli per sottoinsiemi contenuti in  $S$ , altrimenti si parla di minimo (o massimo). Di conseguenza un insieme che ha minimo ha sempre estremo inferiore: Se  $a = \min X, a = \inf X$  (ed anche: Se  $a = \max X, a = \sup X$ ) e si dimostra semplicemente verificando la proprietà di estremo inferiore, ovvero 1)  $\forall x \in X, a \leq x$ , che è vera per la definizione di  $a = \min S$ ; 2)  $\forall t \in S (\forall x \in X, (t \leq x)) \Rightarrow t \leq a$  che è anche vera poiché se prendo un  $t$  che ha la proprietà di essere il più piccolo di tutti gli elementi di  $X = S$  allora è più piccolo anche di  $a$ , essendo  $a \in X$ . Viceversa,  $\inf X = \min X \Leftrightarrow \inf X \in X$ .

## 4. L'anello $\mathbb{Z}$

$(\mathbb{Z}, +, \cdot)$  è un dominio di integrità non nullo ossia un anello commutativo unitario privo di divisori dello zero.

### 4.1 Elementi di aritmetica in $\mathbb{Z}$

Sia  $A$  un dominio di integrità non nullo, definiamo in  $A$  la seguente relazione binaria:  $\forall a, b \in A, a|b \Leftrightarrow \exists c \in A \mid b = ac$ , questa relazione prende il nome di **divisibilità**, scriveremo  $a|b \Leftrightarrow a \mid b$  ( $a$  divide, oppure  $a$  è divisore di  $b$ ) ovvero  $a|b \Leftrightarrow \exists c \in A \mid b = ac$ , quindi se  $a$  è un divisore di  $b$  allora  $b$  è un multiplo di  $a$ .

Indichiamo l'**insieme dei divisori** di  $a$  con il simbolo  $D(a) = \{x \in A \mid x \text{ divide } a\}$ ,  $\forall a \in A$ , ad esempio  $D(0) = \mathbb{Z}$  poiché ogni  $x$  moltiplicato per zero fa zero.  $\forall a \in A$  sia  $M(a)$  l'insieme dei multipli di  $a$ ;  $b$  è un multiplo di  $a \Leftrightarrow a|b \Leftrightarrow \exists c \in A \mid b = ca$ .  $M(a) = \{ax \mid x \in A\}$ ; prendiamo ad esempio l'insieme  $M(2) = \{2z \mid z \in \mathbb{Z}\}$  che rappresenta l'insieme dei multipli di due, ovvero l'insieme dei numeri pari  $2\mathbb{Z}$ , quindi si ha che  $x \in \mathbb{Z}$  è pari  $\Leftrightarrow 2|x$ .

Osserviamo che  $\forall u \in \mathcal{U}(A)$  (l'insieme degli elementi invertibili rispetto al prodotto) possiamo scrivere  $a = u(u^{-1}a) \Rightarrow u|a$  ma è anche vero che  $a = u^{-1}(ua) \Rightarrow ua|a$  questo significa che tra i divisori diversi di un elemento diverso da zero ci sono sempre due tipi di divisori: gli elementi invertibili e il prodotto tra  $a$  ed un elemento invertibile. Un elemento  $b \in A$  si dice **associato** ad  $a$  (associato di  $a$ ) se  $\exists u \in \mathcal{U}(A) \mid b = ua$ . Quindi Ogni  $a \in A \setminus \{0\}$  ammette sempre come divisori gli elementi invertibili e i suoi associati, questi divisori si dicono **divisori banali** di  $a$ . In  $\mathbb{Z}$  quindi gli elementi invertibili di  $\mathbb{Z}$  sono  $\mathcal{U}(\mathbb{Z}) = \{+1, -1\}$  di conseguenza i divisori banali di  $a \in \mathbb{Z} \setminus \{0\}$  sono  $1, -1, a, -a$ .

#### Proprietà della divisibilità in $\mathbb{Z}$

1.  $\forall a \in \mathbb{Z}, \pm 1|a$

2.  $\forall a \in \mathbb{Z}, \pm a|a$

3.  $\forall a, b \in \mathbb{Z}, a|b \wedge b|a \Leftrightarrow a = \pm b$

Dim.:  $\Rightarrow$ : supponiamo quindi  $a|b \wedge b|a$ ; se  $a = 0 \vee b = 0$  risulta  $a = b = 0$  poiché  $x|0 \Rightarrow x = 0$ . Sia allora  $a \neq 0 \wedge b \neq 0$ , quindi  $a|b \Rightarrow \exists c \in \mathbb{Z} \mid b = ac$ , e  $b|a \Rightarrow \exists d \in \mathbb{Z} \mid a = bd$ . Sappiamo che  $a = a1$  ma abbiamo anche  $a = bd = (ac)d$  quindi  $a(cd) = a1$ ; essendo il mio anello integro  $a$  è cancellabile e quindi  $1 = cd \Rightarrow d = c^{-1} \Rightarrow c = d = 1 \vee c = d = -1$  e quindi  $b = ac = a1$  o  $a(-1)$

4.  $\forall a, b \in \mathbb{Z} \setminus \{0\}, a|b \Rightarrow \pm a \mid \pm b$  (la divisibilità vale a meno di elementi associati)

Mostriamo che  $a|b \Rightarrow -a \mid -b$ , gli altri casi sono analoghi: sappiamo che  $b = ac$  ma possiamo scrivere anche  $-b = -ac = (-a)c \Rightarrow -a \mid -b$ . Verifichiamo anche che  $a|b \Rightarrow -a|b$ : so che  $b = ac = (-1)(-1)ac = (-a)(-c) \Rightarrow -a|b$ . Osservazione:  $\forall m \in \mathbb{Z}, m\mathbb{Z} = (-m)\mathbb{Z}$

5.  $a|1 \Leftrightarrow a \in \mathcal{U}(\mathbb{Z}) = \{+1, -1\} \Leftrightarrow a = \pm 1$

6.  $\forall a, b, c \in \mathbb{Z} (a|b \wedge b|c \Rightarrow a|c)$  (vale la proprietà transitiva)

Dim.:  $a|b \wedge b|c \Rightarrow (\exists x \in \mathbb{Z} (b = xa)) \wedge (\exists y \in \mathbb{Z} (c = yb))$  partiamo da  $c = yb = y(xa) = (yx)a$  ma essendo  $yx \in \mathbb{Z}$  per definizione posso dire che  $a|c$

7.  $\forall a, b, c \in \mathbb{Z} (a|b \wedge a|c \Rightarrow a|b \pm c)$

Dim.: dimostriamo che  $a|b \wedge a|c \Rightarrow a|b + c$  (l'altro caso è valido per la proprietà 4):  $a|b \Leftrightarrow \exists x \in \mathbb{Z} \mid b = ax$ , analogamente,  $a|c \Leftrightarrow \exists y \in \mathbb{Z} \mid c = ay$  e quindi  $b + c = ax + ay = a(x + y)$ , ma essendo  $x + y \in \mathbb{Z}$  si ha che  $a|b + c$

8.  $\forall a, b, c \in \mathbb{Z} (a|b \wedge a|b + c \Rightarrow a|c)$

Dim.: conseguenza della 7:  $a|b \wedge a|b + c \Rightarrow a|(b + c) - b = c$

La proprietà 8 si sfrutta molto per vedere come sono fatti i multipli di un elemento. Esempio: se  $x \in \mathbb{N}$ , e  $a$  è l'ultima cifra di  $x$  (es.  $x = 224 = 220 + 4$ ) posso scrivere  $x = 10 \cdot t + a$ , quindi supponendo di dover studiare i numeri divisibili per due, poiché so che  $2|10$  per capire che  $2|x$  basta controllare che  $2|a$ .

$\forall x \in \mathbb{Z}$ , definiamo il **valore assoluto** di  $x$  e lo denotiamo  $|x|$  il numero naturale  $|x| = \begin{matrix} x & \text{se } x \in \mathbb{N} \\ -x & \text{se } x \notin \mathbb{N} \end{matrix}$

Sia  $a \in \mathbb{Z} \setminus \{0\}$  ( $a \neq 0$ ) si dice **numero primo** se e solo se

- 1)  $a \neq \pm 1$  ( $a$  non deve essere invertibile)
- 2)  $a$  ammette solo i divisori banali  $D(a) = \{1, -1, a, -a\}$

La definizione precedente fa riferimento ai divisori dei numeri primi, la successiva fa riferimento a come il numero primo divide un prodotto.

Definizione: Sia  $n \in \mathbb{Z} \setminus \{0\}$  numero primo  $\Leftrightarrow$  **1)**  $n \neq \pm 1$  **2)**  $\forall a, b \in \mathbb{Z} (n|ab \Rightarrow n|a \vee n|b)$

(tutte le volte che un numero primo divide un prodotto divide anche uno dei fattori) Esempio:  $7|ab$  e visto che è primo allora si ha che  $7|a \vee 7|b$  mentre 6 non è primo quindi  $6 \nmid 2 \cdot 3$  ma non è vero che  $6 \nmid 2 \vee 6 \nmid 3$

**Teorema di Euclide:** esistono infiniti numeri primi.

## 4.2 Teorema fondamentale dell'aritmetica

Teorema: Sia  $n \in \mathbb{Z} \setminus \{0, 1, -1\}$ . Allora  $n$  è primo oppure  $n$  è prodotto di numeri primi. Inoltre, tale fattorizzazione è "essenzialmente unica", ovvero: se  $n = p_1 \cdot \dots \cdot p_k = q_1 \cdot \dots \cdot q_h$  ( $p_i$  e  $q_j$  sono primi) allora  $k = h$  e inoltre è possibile ordinare i fattori in modo che  $\forall i \in \{1, \dots, h\} (p_i = \pm q_i)$  (oppure  $|p_i| = |q_i|$ ).

Dimostrazione: L'unicità non verrà dimostrata, ci limiteremo a dimostrare solo l'esistenza della fattorizzazione per numeri naturali, ovvero che  $\forall b \geq 2, n$  è primo o è prodotto di primi. Di conseguenza la nostra base di induzione sarà  $n_0 = 2$ , essendo 2 numero primo  $P(2)$  è vera e quindi la base di induzione è banalmente verificata. Sia ora  $n > 0$  e si suppone l'asserto vero per ogni  $h$  tale che  $(2 \leq h < n)$ ; e ciò significa che  $\forall h | 2 \leq h < n, h$  è primo o prodotto di numeri primi (ipotesi di induzione). Voglio dimostrare che  $P(n)$  è vera; quindi, che  $n$  è primo o prodotto di primi, nel caso  $n$  sia primo è banalmente dimostrato (come per il caso base). Supponiamo  $n$  non primo, poiché  $n \neq \pm 1$ , se  $n$  non è primo ammette un divisore non banale che possiamo scrivere positivo. Sia  $n_1$  un divisore non banale di  $n$  positivo. So che  $n_1$  divide  $n$ , quindi  $n_1|n \Rightarrow \exists n_2 \in \mathbb{N} | n = n_1 n_2$ . Dimostriamo che  $\forall i = 1, 2 (2 \leq n_i < n)$ , in questo modo potrò applicare a  $n_1$  e  $n_2$  l'ipotesi di induzione:  $n_1$  è un divisore positivo non banale di  $n$  quindi  $1 < n_1 < n \Leftrightarrow 2 \leq n_1 < n$  abbiamo così dimostrato la prima limitazione, resta ora da dimostrare che anche  $n_2$  non è banale, ovvero  $n_2 \neq n \wedge n_2 \neq 1$ ; se  $n_2 = n$  avremo  $n = n_1 n_2 = n_1 n \Rightarrow n_1 = 1$  e ciò è assurdo, si arriva ad un assurdo anche per  $n_2 = 1$  infatti  $n = n_1 n_2 = n_1 1 \Rightarrow n_1 = n$  e quindi anche  $n_2$  essendo un fattore non banale risulta verificata la condizione  $\forall i = 1, 2 (2 \leq n_i < n)$ . Allora  $n_1$  ed  $n_2$  verificano l'ipotesi di induzione e quindi posso scrivere  $n = p_1 \cdot \dots \cdot p_k, n_2 = q_1 \cdot \dots \cdot q_h$  dove  $k, h \geq 1$  e  $p_i$  e  $q_j$  sono primi, ma essendo  $n = n_1 \cdot n_2$  la tesi  $n = p_1 \cdot \dots \cdot p_k \cdot q_1 \cdot \dots \cdot q_h$  ( $p_i$  e  $q_j$  primi) risulta dimostrata e quindi  $P(n)$  è vera.

Prendiamo  $n \geq 2$ , sappiamo che si può scrivere come prodotto di numeri primi, posso far comparire ogni  $p_i$  una sola volta come base di una potenza, ad esempio  $n = 2 \cdot 2 \cdot 3 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = 2^2 \cdot 3^2 \cdot 5^2$ , quindi si ha che  $\forall n \in \mathbb{N} \setminus \{0, 1\} n = p_1^{\alpha_1} \cdot \dots \cdot p_t^{\alpha_t}$  con  $p_i$  primi e  $\alpha_i > 0$ , e se  $i \neq j \Rightarrow p_i \neq p_j \forall i, j \in \{1, \dots, t\}$ .

A questo punto ha senso definire la seguente applicazione:  $f: n \in \mathbb{N} \setminus \{0, 1\} \rightarrow \alpha_1 + \dots + \alpha_t \in \mathbb{N}^*$ ; ovviamente è una applicazione non iniettiva, esempio  $n = 2^2 \cdot 3^5 \rightarrow 2 + 5 = 7, m = 7^2 \cdot 5^5 \rightarrow 7$ , inoltre,  $f(n) = 1 \Leftrightarrow n = p$  primo.  $f$  è suriettiva se  $\forall a \in \mathbb{N}^*, \exists n \in \mathbb{N} \setminus \{0, 1\} | f(n) = a$  ( $n$  è prodotto di  $a$  primi), quindi essendo  $f(2^2) = f(2 \cdot 2) = 2, f(2^3) = 3, \dots$  di conseguenza  $\forall a \in \mathbb{N}^*, a = f(2^a)$  e quindi è vero che  $f$  è suriettiva.

Esercizio: Studiare iniettività e suriettività di  $g: n \in \mathbb{N} \rightarrow \alpha_1 \cdot \alpha_2 \cdot \dots \cdot \alpha_t \in \mathbb{N}^*$  e  $h: n \in \mathbb{N} \rightarrow t \in \mathbb{N}^*$  e poi studiare rispetto a  $\mathcal{R}_g$  e  $\mathcal{R}_h$  il nucleo di equivalenza la classe di  $[6]_{\mathcal{R}_h}$  e di  $[4]_{\mathcal{R}_g}$ .

## 4.3 Congruenze in $\mathbb{Z}$ , l'insieme delle classi resto, equazioni congruenziali.

Sia  $A$  un dominio d'integrità non nullo. Definiamo in  $A \setminus \{0\}$  la seguente relazione  $\rho: \forall a, b \in A \setminus \{0\} a \rho b \Leftrightarrow a$  è associato a  $b$ .  $\rho$  è di **equivalenza**, infatti  $\rho$  è **riflessiva** poiché  $\forall a \in A, a$  è associato ad  $a$  ( $a = 1a$ ), e  $\rho$  è **simmetrica**:  $\forall a, b \in A \setminus \{0\} a \rho b \Rightarrow b \rho a$  quindi  $a$  associato a  $b \Rightarrow b$  associato ad  $a$ , il che risulta vero



poiché  $apb \Rightarrow \exists u \in \mathcal{U}(A): a = bu \Rightarrow au^{-1} = buu^{-1} = b$  e quindi  $b = au^{-1} \Rightarrow b$  associato ad  $a \Rightarrow bpa$ . Resta da provare che  $\rho$  è transitiva, ovvero  $\forall a, b, c \in A \setminus \{0\} \quad apb \wedge bpc \Rightarrow apc: a = bu \wedge b = cv \ (u, v \in \mathcal{U}(A)) \Rightarrow a = bu = (cv)u = c(vu)$  ed essendo  $vu \in \mathcal{U}(A)$  risulta  $apc$ .

L'essere associato ripartisce, a meno dello zero, in classi di equivalenza:  $[a]_\rho = \{b \in A \setminus \{0\} | bpa\} = \{au | u \in \mathcal{U}(A)\}$

Per definire una operazione su un insieme quoziente  $A/\rho$  devo definire una applicazione del seguente tipo  $f: A/\rho \times A/\rho \rightarrow A/\rho$ ; questo poiché non è sempre detto che un insieme quoziente mi dia una applicazione ben posta, ad esempio  $f: A/\rho \rightarrow \mathbb{Z}$ , definiamo  $f([a]_\rho) = a + 1$ , questa applicazione ha immagine che dipende dal rappresentante ma che varia al variare del rappresentante, essendo  $[a] = [-a]$ .

**Definizione congruenza in  $\mathbb{Z}$ :**  $\forall m \in \mathbb{Z}$ , definiamo in  $\mathbb{Z}$  la seguente relazione:  $a(m\mathbb{Z})b \Leftrightarrow m|a - b \Leftrightarrow \exists h \in \mathbb{Z} \ |a - b = mh$  (questa è una prima definizione che verrà aggiornata in seguito)

**Teorema (Proprietà della divisione in  $\mathbb{Z}$ ):**  $\forall (a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}, \exists! (q, r) \mid a = bq + r \wedge (0 \leq r < |b|)$  ( $q$  ed  $r$  sono detti rispettivamente il quoziente ed il resto della divisione di  $a$  per  $b$ ) (il fatto che  $r$  sia piccolo ( $0 \leq r < |b|$ ) rende la coppia  $(q, r)$  unica).

**Dimostrazione:** Dimosteremo solo l'esistenza di  $(q, r)$  per  $(a, b) \in \mathbb{N} \times \mathbb{N} \setminus \{0\}$  e quindi che per ogni  $(a, b) \in \mathbb{N} \times \mathbb{N} \setminus \{0\}$  esiste  $(q, r) \in \mathbb{N} \times \mathbb{N}$  tale che  $a = bq + r \wedge (0 \leq r < b)$  (non tratteremo l'unicità). Si ragionerà per induzione (II forma), ma prima il caso banale in cui  $a < b$ , esso sarà  $0 \leq a < b$  e quindi  $r = a$  e  $q = 0$ , ovvero  $a = 0b + a$ . Sia ora  $a > b$ , la base di induzione è  $n = 0$ , per ipotesi se  $a = 0$  allora  $b \neq 0$  e quindi  $a < b$  e troviamo il caso risolto in precedenza, supponiamo ora  $a > 0$ ; per ipotesi di induzione supponiamo la proprietà vera per ogni  $h$  tale che  $0 \leq h < b$ , quindi esisteranno una coppia  $(q_h, r_h) \in \mathbb{N} \times \mathbb{N}$  tale che  $h = bq_h + r_h \wedge 0 \leq r_h < b$ ; abbiamo già risolto il caso  $a < b$ . Allora sia  $a \geq b$  consideriamo  $a - b$  e verifichiamo che  $0 \leq a - b < b$ ;  $0 \leq a - b \Leftrightarrow b \leq a$  che è proprio la nostra supposizione, e poiché  $b > 0$  risulta vero anche che  $a - b < b$ . Questo verifica che  $0 \leq a - b < b$  si trova in uno di quei valore per cui ho supposto vera l'ipotesi di induzione. Allora per  $a - b, \exists (q_1, r_1) \in \mathbb{N} \times \mathbb{N} \mid a - b = bq_1 + r_1 \wedge 0 \leq r_1 < b$  e sommando ad entrambi i fattori  $b$  si ha  $a = b + bq_1 + r_1 = b(1 + q_1) + r_1$ , di conseguenza  $q = 1 + q_1$  ed  $r = r_1$  che sono quoziente e resto della divisione di  $a$  per  $b$ .

Se  $a < 0$  non so dividere  $a$  per  $b$  ma essendo  $-a > 0$  posso fare  $-a = bq + r$  (con  $0 \leq r < |b|$ ) e quindi  $a = -bq - r = b(-q) - r$ , a questo punto se  $r = 0$  non ho problemi essendo  $a = b(-q) + 0$  ma se il resto  $r > 0$  avrei  $-r < 0$  il che contrasta la definizione. Ma se scriviamo  $a = b(-q) - r = b(-q) - |b| + |b| - r = b(-q \pm 1) + (|b| - r)$  e questo  $|b| - r$  verifica la condizione  $0 < |b| - r < |b|$  e sarà il nostro resto.

**Esempio:**  $a = 18, b = 7 \Rightarrow 18 = 7 \cdot 2 + 4$  quindi  $q = 2$  e  $r = 4$ ; invece per  $a = 18, b = -7$  avremo che  $18 = (-7) \cdot (-2) + 4$  con  $q = -2$  e  $r = 4$ . Mentre  $a = -18, b = 7$  dividiamo 18 per 7 e cambiamo segno:  $-18 = -7 \cdot 2 - 4 = 7(-2) - 4 \Rightarrow 18 = 7(-2) - 7 + 7 - 4$  di conseguenza  $-18 = 7 \underbrace{(-2 - 1)}_q + \underbrace{(7 - 4)}_r$

**Esercizio:** applicare la regola della divisione per  $a = \pm 22$  e  $b = \pm 5$  e anche per  $a = \pm 40$  e  $b = \pm 6$

Se  $q$  ed  $r$  sono quoziente e resto della divisione di  $a$  per  $b$ , scriveremo  $r = \text{rest}(a, b)$ .

Il resto ha le seguenti proprietà:

- $\forall m \in \mathbb{Z} \setminus \{0\}, \forall a \in \mathbb{Z}, \text{rest}(a, m) = \text{rest}(a, -m)$   
 $a = qm + r \ (0 \leq r < |m|) \quad a = (-q)(-m) + r \ (0 \leq r < |m| = |-m|)$
- I resti della divisione per  $m$  con  $m > 0$  sono i numeri  $0 \leq r < m$ , ovvero,  $r \in \{0, 1, \dots, m - 1\}$  quindi i resti possibili della divisione per  $m$  sono  $m$ .
- Se  $r \in \{0, 1, \dots, m - 1\}$  è un resto possibile nella divisione per  $m$ , allora  $r = 0m + r$  (il resto coincide con il suo resto per la divisione per  $m$ )  
 $0, 1, 2, 3$  sono i resti nella divisione per 4, se divido ulteriormente avrò  $0 = 0 \cdot 4 + 0; 1 = 0 \cdot 4 + 1; \dots$

Sia  $m > 0$ . Considero l'applicazione  $f_m: x \in \mathbb{Z} \rightarrow \text{rest}(x, m) \in \mathbb{N}$ , essa avrà tante immagini quanti sono i resti di  $m$ , ad esempio per  $m = 5$ ,  $f_5(5) = 0$ ,  $f_5(11) = 1$ ,  $f_5(27) = 2$ , ...

Sia  $\rho$  il nucleo di equivalenza di  $f_m: \forall x, y \in \mathbb{Z} (x \rho y \Leftrightarrow f_m(x) = f_m(y) \Leftrightarrow \text{rest}(x, m) = \text{rest}(y, m))$ , quindi questa relazione di equivalenza ci dice che due elementi sono in relazione quando danno lo stesso resto nella divisione per  $m$ . Classe costituita da tutti gli elementi che danno resto zero, tra questi c'è 0:  $[0]$ ; classe costituita da tutti gli elementi che danno resto uno, tra questi c'è 1:  $[1]$ ; ...  $[m - 1]$ . Posso a questo punto scrivere che  $\mathbb{Z}/\rho = \{[0], [1], \dots, [m - 1]\}$ .

**Congruenza modulo  $m$ :** Sia  $m \in \mathbb{Z}$ .  $\forall a, b \in \mathbb{Z}$ , definiamo la seguente relazione binaria  $a(m\mathbb{Z})b \Leftrightarrow m|a - b \Leftrightarrow \exists h \in \mathbb{Z} \mid a - b = mh$ . **Se  $m \neq 0$  si ha che  $m|a \Leftrightarrow \text{rest}(a, m) = 0$**

Dim  $\Rightarrow$ : se  $m|a \exists h \in \mathbb{Z}: a = mh = mh + 0$  dove  $h$  è il quoziente e 0 il resto.

Dim  $\Leftarrow$ : se il resto è  $r = \text{rest}(a, m) = 0$  allora  $a = mq + r = mq \Rightarrow m|a$

La congruenza in modulo  $m$  si indica con il simbolo  $\equiv_m: a \equiv_m b \Leftrightarrow m|a - b$  oppure con  $a \equiv b(\text{mod } m)$  e si legge "a congruo b modulo m" e significa che  $m$  divide  $a - b$ . Ad esempio  $7 \equiv 1(\text{mod } 6)$  è vera.

**Proposizione 1:** Sia  $m \in \mathbb{N}^*$ . Allora  $\forall a, b \in \mathbb{Z}, a \equiv b(\text{mod } m) \Leftrightarrow \text{rest}(a, m) = \text{rest}(b, m)$

Dimostrazione:  $a \equiv b(\text{mod } m) \Rightarrow \text{rest}(a, m) = \text{rest}(b, m)$ : essendo  $a \equiv b(\text{mod } m) \Rightarrow \exists h \in \mathbb{Z} \mid a - b = hm$  ragion per cui  $a = b + hm$ . Applico la proprietà della divisione a  $b$  ed  $m$ :  $\exists! (q, r) \in \mathbb{Z} \times \mathbb{N} \mid b = mq + r \wedge 0 \leq r < |m| = m$  quindi abbiamo che  $a = b + hm = mq + r + hm = m(q + h) + r \wedge 0 \leq r < m$  di conseguenza  $q + h$  ed  $r$  sono quoziente e resto della divisione di  $a$  per  $m$ ; si noti che  $r = \text{rest}(a, m)$  ma esso è anche resto della divisione di  $b$  per  $m$ :  $r = \text{rest}(b, m)$ . Dimostriamo ora che  $\text{rest}(a, m) = \text{rest}(b, m) \Rightarrow a \equiv b(\text{mod } m)$ : supponiamo  $r$  sia il resto della divisione di  $a$  per  $m$  che di  $b$  per  $m$  quindi possiamo scrivere  $a = mq_1 + r$  e  $b = mq_2 + r$ , facciamo la differenza  $a - b = (mq_1 + r) - (mq_2 + r) = mq_1 - mq_2$  e  $r = mq_1 - mq_2 + r - r = m(q_1 - q_2) \Rightarrow m|a - b$  che per definizione è  $a \equiv b(\text{mod } m)$ . C.V.D.

**Corollario 2:**  $\forall m \in \mathbb{Z}$  la congruenza modulo  $m$  è una relazione di equivalenza in  $\mathbb{Z}$

Esercizio: Dimostrare che la congruenza modulo  $m$  è una relazione di equivalenza studiandone le proprietà, e quindi che sia riflessiva, simmetrica e transitiva.

**Teorema 3:** Sia  $m \in \mathbb{N}^*$ . Allora  $\mathbb{Z}/\equiv_m = \{[0], [1], \dots, [m - 1]\}$  ed ha ordine  $m$  (già dimostrato in precedenza)

Nei casi in cui c'è confusione di notazione si può scrivere  $[a]_m = \{x \in \mathbb{Z} \mid x \equiv_m a\}$  invece di  $[a]$ , ma un modo più rapido per indicare la classe di equivalenza è il simbolo  $\bar{a}$ . Con questa notazione l'insieme quoziente del teorema precedente sarà scritto come segue:  $\mathbb{Z}/\equiv_m = \{\bar{0}, \bar{1}, \dots, \overline{m - 1}\}$

**Proposizione 4:** Siano  $m \in \mathbb{N}^*, a \in \mathbb{Z}$ . Allora  $[a]_m = \{a + mk \mid k \in \mathbb{Z}\} (a + m\mathbb{Z})$ . Inoltre, se  $r = \text{rest}(a, m)$ ,  $[a]_m = [r]_m$  (questo ci dice che il rappresentante della classe può essere scelto come resto della divisione)

Dimostrazione:  $x \in [a]_m \Leftrightarrow x \equiv_m a \Leftrightarrow m|x - a \Leftrightarrow \exists h \in \mathbb{Z} \mid x - a = mh \Leftrightarrow \exists h \in \mathbb{Z} \mid x = a + mh$  quindi  $[a]_m = \{x \in \mathbb{Z} \mid x \equiv_m a\} = \{a + mh \mid h \in \mathbb{Z}\}$  e abbiamo dimostrato la prima parte, dimostriamo ora la seconda: due classi sono uguali se i rappresentanti sono in relazione quindi iniziamo con il dividere  $a$  per  $m$ :  $\exists! (q, r) \in \mathbb{Z} \times \mathbb{N}$  tale che  $a = mq + r \wedge (0 \leq r < m)$ , considero  $a - r = mq \Rightarrow m|a - r$  ma se  $m$  divide  $a - r$  avrò che per definizione  $a \equiv r(\text{mod } m)$  e quindi  $[a]_m = [r]_m$ .

Ad esempio:  $[21]_3 = \{21 + k5 \mid k \in \mathbb{Z}\}$ , quindi saranno  $21 + 5, 26 + 5, \dots$  ed anche  $21 - 5, 16 - 5, \dots$

Esercizio: Determinare quali sono gli elementi di  $[7]_3$  compresi tra 18 e 30. Ricordando poi che  $[a] = [b] \Leftrightarrow a \rho b$  vedere per quali  $m > 0$  risulta: **1)**  $[5] = [22]$ ; **2)**  $[5] = [13]$ ; **3)**  $[5] = [-5]$  si noti:  $\forall m > 0, [0]_m = m\mathbb{Z}$

Si osservi che  $a \equiv b(\text{mod } m) \Leftrightarrow \text{rest}(a, m) = \text{rest}(b, m)$  e quindi essendo la congruenza una relazione di equivalenza lo sono entrambe, inoltre la precedente proposizione ci dice che ogni classe può essere



rappresentata dal resto del rappresentante. Ad esempio in  $\mathbb{Z}/\equiv_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$  posso rappresentare la classe di 6 con la classe di uno essendo  $6 = 5 \cdot 1 + 1$  e quindi  $\overline{6} = \overline{1}$ .

Per velocizzare la notazione si indica l'insieme quoziente  $\mathbb{Z}/\equiv_m$  semplicemente con  $\mathbb{Z}_m$  e questo è detto l'insieme degli interi modulo  $m$  oppure delle classi resto modulo  $m$ .

Se conosciamo la decomposizione in numeri primi di un elemento allora i divisori positivi di questo numero li possiamo scrivere direttamente tutti. Facciamo un esempio: sia  $n = 2^3 \cdot 5^2 \cdot 11$ , quindi se prendo un divisore di  $n$ :  $m|n \Rightarrow n = m \cdot h$  questo  $m$  dovrà essere diviso per forza da 2 da 5 o da 11 altrimenti avremo una decomposizione di  $n$  dove compare un altro numero primo (cosa assurda per il teorema fondamentale dell'aritmetica) quindi  $m = 2^\alpha \cdot 5^\beta \cdot 11^\gamma$ , più precisamente gli esponenti devono essere minori o uguali a quelli di  $n$ , quindi:  $0 \leq \alpha \leq 3, 0 \leq \beta \leq 2, 0 \leq \gamma \leq 1$ ; ed ad ogni scelta di questi  $\alpha, \beta, \gamma$  corrisponde uno ed un solo divisore. Da questo si può dedurre il numero di divisori, infatti essendo  $\alpha \in \{0, 1, 2, 3\}, \beta \in \{0, 1, 2\}$  e  $\gamma \in \{0, 1\}$  la terna  $(\alpha, \beta, \gamma)$  appartiene al prodotto cartesiano di tre insiemi finiti; infatti,  $(\alpha, \beta, \gamma) \in \{0, 1, 2, 3\} \times \{0, 1, 2\} \times \{0, 1\}$  ed ha ordine  $4 \cdot 3 \cdot 2$  di conseguenza il numero di divisori è 24.

#### 4.4 Massimo comun divisore e minimo comune multiplo per una coppia di interi

Sia  $(a, b) \in \mathbb{Z} \times \mathbb{Z}$  un elemento  $d \in \mathbb{Z}$  si dice un **massimo comun divisore** (M.C.D.) per la coppia  $(a, b)$  se e solo se  $d$  verifica due proprietà:

1.  $d|a \wedge d|b$  ( $d$  è divisore comune di  $a$  e  $b$ )
2.  $\forall t \in \mathbb{Z} (t|a \wedge t|b \Rightarrow t|d)$  ( $d$  è diviso da tutti i divisori comuni di  $a$  e  $b$ )

Esempio:  $D(4) \cap D(6) = \{\pm 1, \pm 2\}$  quindi  $+2$  e  $-2$  sono MCD di  $(4, 6)$

Sia  $(a, b) \in \mathbb{Z} \times \mathbb{Z}$  un elemento  $m \in \mathbb{Z}$  si dice un **minimo comune multiplo** (m.c.m.) per la coppia  $(a, b)$  se e solo se  $m$  verifica due proprietà:

1.  $a|m \wedge b|m$  ( $m$  è multiplo comune di  $a$  e  $b$ )
2.  $\forall t \in \mathbb{Z} (a|t \wedge b|t \Rightarrow m|t)$  ( $m$  divide tutti i multipli comuni di  $a$  e  $b$ )

Anche per il mcm se un certo  $a > 0$  verifica le proprietà precedenti allora anche  $-a$  le verifica ed è mcm

$d$  è un MCD di  $(a, b) \Leftrightarrow d$  è un MCD di  $(\pm a, \pm b)$ , di conseguenza possiamo sempre supporre  $a, b \geq 0$ :

- Se  $a = b = 0$  il massimo comune divisore è solo 0, allo stesso modo mcm  $(0, 0) = 0$
- Se  $a \neq 0 \wedge b = 0$  un MCD  $(a, 0)$  sarà  $\pm a$  mentre mcm  $(a, 0) = 0$
- Se  $d$  è un MCD  $(a, b)$ , si ha che  $l$  è un MCD  $(a, b) \Leftrightarrow l = d \vee l = -d$   
Se  $d$  è un mcm  $(a, b)$ , si ha che  $l$  è un mcm  $(a, b) \Leftrightarrow l = d \vee l = -d$

Dim. per MCD (analogo per il mcm):  $d$  è un MCD  $\Rightarrow -d$  è un MCD poiché la divisibilità vale a meno del segno. Supponiamo adesso che  $l$  è un MCD  $(a, b)$ ; sia  $l$  che  $d$ , quindi, sono divisori comuni di  $a$  e  $b$  ed in quanto tali ognuno dei due è divisibile da tutti i divisori comuni, ma ciò significa che  $l$  è diviso da  $d$  e analogamente anche  $d$  è diviso da  $l$ , ma allora per una delle proprietà di divisibilità in  $\mathbb{Z}$  si ha che  $l = \pm d$ .

Per convenzione, se scriviamo  $d = \text{MCD}(a, b)$  senza la parola "un" ci riferiamo al MCD non negativo. Analogamente con  $d = \text{mcm}(a, b)$  intendiamo che  $d$  è il mcm  $(a, b) \geq 0$ .

#### 4.5 Determinazione di MCD e mcm attraverso la decomposizione in numeri primi

Nel caso in cui uno dei due sia 1 si ha che  $\text{MCD}(a, 1) = 1$  mentre  $\text{mcm}(a, 1) = a$ . Siano, quindi,  $a, b > 1$  scriviamo  $a$  e  $b$  come prodotto di primi:  $a = p_1^{\alpha_1} \cdot \dots \cdot p_t^{\alpha_t}$  e  $b = q_1^{\beta_1} \cdot \dots \cdot q_s^{\beta_s}$  ( $\alpha_i, \beta_i > 0$  e  $p_i \neq p_j, q_i \neq q_j$  per  $i \neq j$ ). Per costruire il MCD si prende il prodotto dei divisori primi **comuni** presi con il **minimo** tra i due esponenti (se non ci sono divisori primi comuni allora il MCD è 1). Mentre risulta  $\text{mcm}(a, b)$  il prodotto di **tutti** i primi presenti nelle decomposizioni elevati al **massimo** tra i due esponenti.

Esempio: siano  $a = 2^2 \cdot 3 \cdot 5^3$  e  $b = 2 \cdot 5^2 \cdot 7$  si ha che  $\text{MCD}(a, b) = 2 \cdot 5^2$  e  $\text{mcm}(a, b) = 2^2 \cdot 3 \cdot 5^3 \cdot 7$

Proprietà:  $\forall (a, b) \in \mathbb{Z} \times \mathbb{Z}$ , esistono un  $\text{MCD}(a, b)$  ed un  $\text{mcm}(a, b)$

#### 4.6 Teorema di Euclide delle divisioni successive

Siano  $a, b \in \mathbb{Z}$  e sia  $b > 0$ . Poniamo  $r_{-1} = a$  e  $r_0 = b$  e consideriamo la sequenza (finita) di divisioni:  $r_{-1} = r_0 \cdot q_1 + r_1$ , per la proprietà della divisione si ha che  $0 \leq r_1 < r_0 < b$  se  $r_1 \neq 0$  divido  $r_0$  per  $r_1$  quindi avrò  $r_0 = r_1 \cdot q_2 + r_2$  con  $0 \leq r_2 < r_1 < b$ , se  $r_2 \neq 0$  allora  $r_1 = r_2 q_3 + r_3$  e così via... Poiché questa sequenza di resti decresce strettamente dopo  $n$  passi si avrà l'ultimo resto non nullo:  $r_{n-2} = r_{n-1} q_n + r_n$  e, quindi,  $r_{n-1} = r_n q_{n+1} + 0$ . **L'ultimo resto non nullo,  $r_n$  è MCD tra  $a$  e  $b$ .**

Praticamente si divide  $a$  per  $b$  e si esegue una sequenza di divisioni fino a trovare un resto pari a zero, dopodiché l'ultimo resto non nullo è il massimo comune divisore. Diamo alcuni esempi:  $\text{MCD}(10, 7)$  si ha che  $10 = 7 \cdot 1 + 3$ ;  $7 = 3 \cdot 2 + 1$ ;  $3 = 1 \cdot 3 + 0$ , quindi, l'ultimo resto non nullo è 1 e quindi  $\text{MCD}(10, 7) = 1$ .

Esercizio: Determinare con l'algoritmo delle divisioni successive il MCD delle seguenti coppie: (25, 7), (24, 15)

#### 4.7 Teorema di Bezout e interi coprimi

Se  $d$  è un  $\text{MCD}(a, b)$  allora esistono  $\alpha, \beta \in \mathbb{Z}$  tali che  $d = \alpha a + \beta b$  (si può scrivere come combinazione lineare di  $a, b$  con coefficienti in  $\mathbb{Z}$ ). Questa condizione è necessaria ma non sufficiente, infatti,  $d$  è un MCD  $\Rightarrow d = \alpha a + \beta b$  ma il viceversa (l'altra implicazione) non sussiste.

Se  $\text{MCD}(a, b) = 1$ , gli interi  $a$  e  $b$  si dicono **interi coprimi** (o primi tra loro), ciò non significa che  $a, b$  siano numeri primi, infatti  $\text{MCD}(6, 25) = 1$  (e quindi sono coprimi), ma due numeri primi  $p, q$  con  $p \neq q$  sono sempre coprimi, quindi  $\text{MCD}(p, q) = 1$ .

Teorema di Bezout: Siano  $a, b \in \mathbb{Z}$ . Se  $d$  è un  $\text{MCD}(a, b)$ , allora esistono  $x, y \in \mathbb{Z}$  tali che  $d = xa + yb$ .

Quindi essendo condizione necessaria ma non sufficiente, trovare un numero che può essere scritto nella forma  $d = xa + yb$  non significa che  $d$  sia un MCD, in realtà esiste un caso in cui un numero  $d = xa + yb$  sia effettivamente un MCD, ovvero quando la combinazione è 1 o  $-1$ .

Proposizione 1: Siano  $a, b \in \mathbb{Z}$ . Allora sono equivalenti le seguenti proprietà:

- I.  $a$  e  $b$  sono coprimi
- II.  $\exists x, y \in \mathbb{Z} \mid 1 = xa + yb$

Dimostrazione:  $I \Rightarrow II$  è vera per il teorema di Bezout. Per dimostrare che  $II \Rightarrow I$  bisogna verificare che se 1 si può scrivere in quella forma allora 1 verifica le due proprietà che definiscono un massimo comune divisore.  $1$  è  $\text{MCD}(a, b) \Leftrightarrow 1|a \wedge 1|b$  che è vero per la natura di 1 (esso divide tutti i numeri); la seconda proprietà da verificare è  $\forall t \in \mathbb{Z} (t|a \wedge t|b \Rightarrow t|1)$ . Dire  $t|a \Rightarrow \exists h \in \mathbb{Z} | a = th$ , mentre  $t|b \Rightarrow \exists k \in \mathbb{Z} | b = tk$  che sono entrambe vere poiché ho come ipotesi che  $t|a \wedge t|b$ , ora essendo  $1 = xa + yb$ , sempre per ipotesi, posso scrivere  $1 = xth + ytk = t(xh + yk) \Rightarrow t|1$  come volevasi dimostrare.

Proposizione 2: Siano  $a, b, c \in \mathbb{Z}$ , e siano  $a$  e  $b$  primi tra loro (coprimi). Se  $a|bc$  allora  $a|c$  (se un elemento divide un prodotto ed è primo con uno dei due fattori allora divide l'altro fattore).

Esempio: Se  $6|ab$  e  $\text{MCD}(a, 6) = 1$  allora  $6|b$

Data una coppia di interi andiamo a cercare il MCD utilizzando l'algoritmo delle divisioni successive e vediamo come a partire da quelle divisioni possiamo scrivere il MCD come combinazione di  $a$  e  $b$  con certi  $x, y \in \mathbb{Z}$ . Prendiamo a tal scopo il  $\text{MCD}(30, 18)$ : Si ha  $30 = 18 \cdot 1 + 12$ ,  $18 = 12 \cdot 1 + 6$  ed infine  $12 = 6 \cdot 2 + 0$ ; ora si ha che  $6 = \text{MCD}(30, 18)$  e quindi si può scrivere come  $6 = \alpha 18 + \beta 30$ , a tal scopo prendiamo i resti delle divisioni successive come differenza, quindi,  $6 = 18 - 12 \cdot 1$  e  $12 = 30 - 18 \cdot 1$  di conseguenza possiamo scrivere  $6 = 18 - (30 - 18 \cdot 1) \cdot 1 = 18 - 30 + 18 \cdot 1 = 18(1 + 1) + 30(-1) = (2)18 + (-1)30$ .

Esercizio: trovare una combinazione come l'esempio tra  $\text{MCD}(32, 18)$  e  $\text{MCD}(15, 11)$

#### 4.8 L'anello degli interi modulo $m$ (anello delle classi resto)

Sia  $(A, *)$  una struttura algebrica,  $\mathcal{R}$  una relazione di equivalenza in  $A$ . Considero  $A/\mathcal{R} = \{[a]_{\mathcal{R}} | a \in A\}$  (l'insieme di tutte le classi, vedi [capitolo 4.3](#)) dove l'operazione  $*$ :  $(a, b) \in A \times A \rightarrow a * b \in A$ . Verifichiamo che questa applicazione sia ben posta, consideriamo  $\otimes : ([a]_{\mathcal{R}}, [b]_{\mathcal{R}}) \in A/\mathcal{R} \times A/\mathcal{R} \rightarrow [a * b]_{\mathcal{R}} \in A/\mathcal{R}$  e poiché le classi di equivalenza si possono scrivere in più modi affinché l'applicazione sia tale ogni oggetto ne associa uno ed uno solo dobbiamo verificare che anche se cambio il modo di vedere l'oggetto quello che associo è sempre lo stesso. Nel nostro caso gli oggetti che possono variare sono i rappresentanti di  $[a]_{\mathcal{R}}$  e  $[b]_{\mathcal{R}}$ , l'esistenza della classe  $[a * b]_{\mathcal{R}}$  è ovvia, quindi, bisogna verificare solo la sua unicità. Deve valere, dunque, questa implicazione:  $([a]_{\mathcal{R}}, [b]_{\mathcal{R}}) = ([a_1]_{\mathcal{R}}, [b_1]_{\mathcal{R}}) \Rightarrow [a * b]_{\mathcal{R}} = [a_1 * b_1]_{\mathcal{R}}, \forall a, b, a_1, b_1 \in A$ , questa implicazione è equivalente alla seguente proprietà:  $a\mathcal{R}a_1 \wedge b\mathcal{R}b_1 \Rightarrow (a * b)\mathcal{R}(a_1 * b_1)$ . Se questa proprietà vale, allora  $\mathcal{R}$  si dice **compatibile** rispetto a  $*$  (oppure  $\mathcal{R}$  si dice una congruenza rispetto ad  $*$ ).

Se  $\mathcal{R}$  è compatibile rispetto ad  $*$ , si può definire in  $A/\mathcal{R}$  l'operazione, chiamata **operazione quoziente**,  $\otimes : ([a]_{\mathcal{R}}, [b]_{\mathcal{R}}) \in A/\mathcal{R} \times A/\mathcal{R} \rightarrow [a * b]_{\mathcal{R}} \in A/\mathcal{R}$ . Per l'operazione quoziente c'è la convenzione di usare lo stesso simbolo dell'operazione di partenza:  $[a]_{\mathcal{R}} * [b]_{\mathcal{R}} = [a * b]_{\mathcal{R}}$ .

**Teorema:** Sia  $m \in \mathbb{N}^*$ , e siano  $a, a_1, b, b_1 \in \mathbb{Z}$ . Allora:

1. Se  $a \equiv a_1 \pmod{m}$  e  $b \equiv b_1 \pmod{m}$  allora  $a + b \equiv a_1 + b_1 \pmod{m}$   
(la congruenza modulo  $m$  è compatibile con la somma di  $\mathbb{Z}$ )
2. Se  $a \equiv a_1 \pmod{m}$  e  $b \equiv b_1 \pmod{m}$  allora  $a \cdot b \equiv a_1 b_1 \pmod{m}$   
(la congruenza modulo  $m$  è compatibile rispetto al prodotto di  $\mathbb{Z}$ )

Come conseguenza di questo teorema, in  $\mathbb{Z}_m$  possono definirsi le due operazioni quoziente:

1.  $+: (\overline{a}, \overline{b}) \in \mathbb{Z}_m \times \mathbb{Z}_m \rightarrow \overline{a + b} \in \mathbb{Z}_m$
2.  $\cdot: (\overline{a}, \overline{b}) \in \mathbb{Z}_m \times \mathbb{Z}_m \rightarrow \overline{ab} \in \mathbb{Z}_m$

Questo significa che  $\mathbb{Z}_m$ , così come  $\mathbb{Z}$ , deve essere dotato di due operazioni:  $(\mathbb{Z}_m, +, \cdot)$ . Diamo un esempio con la struttura  $(\mathbb{Z}_m, +, \cdot)$  così ottenuta. Prendiamo  $m = 9$ , abbiamo che  $\overline{2} + \overline{5} = \overline{7}$ , ora anche se vario i rappresentanti avrò sempre la classe di 7; scriviamo infatti  $\overline{2} = \overline{11}$  e  $\overline{5} = \overline{-3}$ , e quindi  $\overline{11} + \overline{-3} = \overline{-2}$  che è uguale alla classe di 7.

$(\mathbb{Z}_m, +, \cdot)$  è un **anello commutativo unitario** (Anello degli interi mod.  $m$  oppure l'anello delle classi resto). Verifichiamo che questa struttura sia effettivamente un anello commutativo unitario:

- $(\mathbb{Z}_m, +)$  è un gruppo abeliano
  - È associativa:  $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$ , infatti  $(\overline{a} + \overline{b}) + \overline{c} = \overline{a + b} + \overline{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \overline{a} + \overline{b + c} = \overline{a} + (\overline{b} + \overline{c})$   
Siamo in  $\mathbb{Z}$
  - Ha elemento neutro:  $\overline{0}$ , infatti  $\overline{a} + \overline{0} = \overline{a + 0} = \overline{a}$
  - Opposto:  $\overline{-a} = -(\overline{a})$
- $(\mathbb{Z}_m, \cdot)$  è un semigrupp
  - È associativo poiché in  $\mathbb{Z}$  il prodotto è associativo (verificare come esercizio)
  - È distributivo in  $\mathbb{Z}_m$  rispetto a  $+$ :  $\overline{a}(\overline{b} + \overline{c}) = \overline{a \cdot b} + \overline{a \cdot c}$ , infatti  $\overline{a}(\overline{b} + \overline{c}) = \overline{a \cdot (b + c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{a \cdot b} + \overline{a \cdot c}$
- È unitario con unità  $\overline{1}$
- È commutativo:  $\overline{a} \cdot \overline{b} = \overline{b \cdot a}$  poiché in  $\mathbb{Z}$  il prodotto è commutativo (verificare come esercizio)

Queste proprietà valgono sia in  $\mathbb{Z}$  che in  $\mathbb{Z}_m$ , ma sappiamo che  $\mathbb{Z}$  è integro poiché non ha divisori dello zero, diversamente da  $\mathbb{Z}_m$  che può avere divisori dello zero, consideriamo, ad esempio, l'insieme  $\mathbb{Z}_6 = \{\overline{0}, \dots, \overline{5}\}$ , queste classi sono a due a due distinte, quindi, cerchiamo due classi non nulle il cui prodotto dia la classe di

zero:  $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$ , di conseguenza  $\overline{3}, \overline{2}$  sono divisori dello zero e quindi posso dire che  $\mathbb{Z}_6$  non è un dominio di integrità. In effetti, questi quozienti si comportano diversamente a seconda della natura di  $m$ .

$\mathbb{Z}$  non è un campo, infatti gli unici elementi invertibili in  $(\mathbb{Z}, \cdot)$  sono  $\pm 1$ ; prendiamo adesso  $m = 5$  e prendiamo  $\mathbb{Z}_5 = \{\overline{0}, \dots, \overline{4}\}$ , dimostriamo che  $\mathbb{Z}_5$  sia effettivamente un campo, e quindi che verifichi la seguente proprietà:  $\forall \overline{a} \in \mathbb{Z}_5 \setminus \{\overline{0}\}$ ,  $\overline{a}$  è dotato di inverso. La classe di uno è ovviamente invertibile, ma anche tutte le classi ad esso equivalenti sono invertibili, quindi  $\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$ , ciò significa che anche  $\overline{2}$  e  $\overline{3}$  sono invertibili; allo stesso modo  $\overline{4}$  è invertibile poiché  $\overline{4} \cdot \overline{4} = \overline{16} = \overline{1}$  e di conseguenza  $(\mathbb{Z}_5, \cdot)$  è un campo. Ovviamente non tutti i  $\mathbb{Z}_m$  sono campi, anche se ci sono casi in cui la maggior parte degli elementi sono invertibili.

#### 4.9 Altre proposizioni sulle congruenze

**Proposizione 1:** Sia  $m > 1$  (per  $m = 1$  lo studio dell'anello è banale), e sia  $\overline{a} \in \mathbb{Z}_m \setminus \{\overline{0}\}$ . Allora  $\overline{a}$  è invertibile se e solo se  $\text{MCD}(a, m) = 1$  (quindi solo se  $a$  ed  $m$  sono coprimi).

**Dimostrazione:** Implicazione  $\Rightarrow$ : Sia  $\overline{a}$  invertibile, allora  $\exists \overline{b} \in \mathbb{Z}_m | \overline{a} \cdot \overline{b} = \overline{1}$ , questo significa dire che  $\overline{ab} = \overline{1}$  ma ciò significa che  $ab \equiv 1 \pmod{m} \Rightarrow m | ab - 1 \Rightarrow \exists h \in \mathbb{Z} | ab - 1 = mh$ , isolando uno si ha  $1 = ab - mh = ab + (-h)m$  e quindi abbiamo scritto uno nella forma  $1 = \alpha a + \beta m$  e possiamo dire che  $\text{MCD}(a, m) = 1$  (abbiamo praticamente usato l'inverso del teorema di Bezout). Implicazione  $\Leftarrow$ : Sia  $\text{MCD}(a, m) = 1$ , per il teorema di Bezout,  $\exists \alpha, \beta \in \mathbb{Z} | 1 = \alpha a + \beta m$  e da questa uguaglianza risulta  $\overline{1} = \overline{\alpha a + \beta m} = \overline{\alpha} \cdot \overline{a} + \overline{\beta} \cdot \overline{m}$ , ma essendo  $\overline{m} = \overline{0}$ , ne segue  $\overline{1} = \overline{\alpha} \cdot \overline{a}$ , ovvero  $\overline{a}$  è invertibile ed ha come inverso  $\overline{\alpha}$ .

La proposizione precedente è condizione necessaria e sufficiente per dire se una classe è invertibile senza trovare il suo inverso. Vediamo ora cosa succede se gli elementi non sono coprimi.

**Proposizione 2:** Sia  $m > 1$ , e sia  $\overline{a} \in \mathbb{Z}_m \setminus \{\overline{0}\}$ . Allora  $\overline{a}$  è divisore dello zero se e solo se  $d = \text{MCD}(a, m) > 1$

**Dimostrazione:** Implicazione  $\Rightarrow$ : Se  $\overline{a}$  è divisore dello zero ovviamente non è cancellabile, di conseguenza  $\overline{a}$  non è invertibile (essendo gli elementi invertibili sempre cancellabili), quindi  $\text{MCD}(a, m) > 1$  per la proposizione precedente (scegliamo il MCD positivo). Implicazione  $\Leftarrow$ : Sia  $d > 1$ , essendo MCD tra  $a$  ed  $m$ , si ha  $d | a \Rightarrow \exists a_1 | a = d \cdot a_1$  e anche  $d | m \Rightarrow \exists m_1 | m = d \cdot m_1$ ; moltiplichiamo la classe di  $a$  per la classe di  $m_1$  (il nostro scopo è trovare due classi non nulle tali che il loro prodotto sia la classe di zero), risulta  $\overline{a} \cdot \overline{m_1} = \overline{da_1} \cdot \overline{m_1} = \overline{a_1} \cdot \overline{dm} = \overline{a_1} \cdot \overline{m} = \overline{0}$ , ora  $\overline{a}$  è non nulla per ipotesi, inoltre, essendo  $m_1$  un divisore di  $m$  è ovviamente non nullo essendo  $0 < m_1 \leq m$ , inoltre  $m$ , se fosse uguale ad  $m_1$ , risulterebbe  $d = 1$  ma per ipotesi  $d > 1$ , di conseguenza  $0 < m_1 \leq m - 1$  e quindi  $m_1$  diventa un resto per la divisione di  $m$  che non è zero, ne segue  $\overline{m_1} \neq \overline{0}$  e quindi  $\overline{a}$  è divisore dello zero.

Quindi un elemento di  $\mathbb{Z}_m$  o è invertibile oppure è divisore dello zero, ovvero, non può essere cancellabile senza essere invertibile, cosa che invece può succedere in  $\mathbb{Z}$ .

Esempio con  $m = 10$ :  $\mathbb{Z}_{10} = \{\overline{0}, \dots, \overline{9}\}$ , gli elementi invertibili  $\mathcal{U}(\mathbb{Z}_{10}) = \{\overline{a} \in \mathbb{Z}_{10} \setminus \{\overline{0}\} | \text{MCD}(a, 10) = 1\}$  quindi  $\mathcal{U}(\mathbb{Z}_{10}) = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$ , ed automaticamente i divisori dello zero sono  $\{\overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}\}$ . Troviamo adesso una classe che moltiplicata per sei dia lo zero di questo anello (sappiamo già che è divisore dello zero poiché  $\text{MCD}(6, 10) = 2 > 1$ : scriviamo 6 e 10 come prodotto di 2 per un altro intero:  $6 = 2 \cdot 3$  e  $10 = 2 \cdot 5$ , ora moltiplichiamo  $\overline{6}$  per  $\overline{5}$ :  $\overline{6} \cdot \overline{5} = \overline{2 \cdot 3} \cdot \overline{5} = \overline{3} \cdot \overline{10} = \overline{0}$ . Facciamo la stessa cosa con 8:  $\text{MCD}(8, 10) = 2$  quindi  $8 = 2 \cdot 4$  e  $10 = 2 \cdot 5$  ne segue  $\overline{8} \cdot \overline{5} = \overline{40} = \overline{0}$ .

**Corollario 3:** Sia  $m > 1$  e sia  $\overline{a} \in \mathbb{Z}_m \setminus \{\overline{0}\}$ . Allora  $\overline{a}$  non è invertibile se e solo se  $\overline{a}$  è un divisore dello zero.

**Teorema 4:** Sia  $m > 1$ . Allora sono equivalenti queste condizioni:

1.  $m$  è numero primo;
2.  $\mathbb{Z}_m$  è un campo;
3.  $\mathbb{Z}_m$  è un dominio di integrità

**Dimostrazione:**  $1 \Rightarrow 2$ :  $\mathbb{Z}_m = \{\overline{0}, \dots, \overline{m-1}\}$ ,  $\forall \overline{a} \in \mathbb{Z}_m \setminus \{\overline{0}\}$ , posso pensare  $a \in \{1, \dots, m-1\}$  (scegliendo il rappresentante canonico), essendo  $m$  primo, per ipotesi, si ha che  $\text{MCD}(a, m) = 1$  poiché, può essere solo 1 od  $m$ , ma quest'ultimo è escluso avendo scelto  $a$  tra i rappresentanti canonici.  $2 \Rightarrow 3$  è banale poiché sappiamo che tutti i campi sono sempre domini di integrità (in un campo ogni elemento diverso da zero è invertibile ed elemento invertibile significa elemento cancellabile, quindi non è divisore dello zero).  $3 \Rightarrow 1$ : supponiamo  $\mathbb{Z}_m$  integro e per assurdo che  $m > 1$  non sia primo; quindi ammette un divisore non banale  $c$ , che come tale  $1 < c < m$ . Segue che  $\text{MCD}(c, m) = c$ , poiché  $c|m$ , risulta dunque che  $\overline{c}$  è divisore dello zero che è assurdo poiché  $\mathbb{Z}_m$  è un dominio di integrità.

**Esercizio:** Trovare gli elementi invertibili ed i divisori dello zero in  $\mathbb{Z}_{12}$  e determinare (senza andare a tentativi) l'inverso di  $\overline{5}$ . Soluzioni:  $\mathcal{U}(\mathbb{Z}_{12}) = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$  i div. dello zero sono le classi restanti, l'inverso di  $\overline{5}$  è  $\overline{5}_{12}$

#### 4.10 Equazioni congruenziali

Sia  $\overline{a} \in \mathbb{Z}_m \setminus \{\overline{0}\}$ ,  $\overline{a}$  è invertibile, per definizione, se e solo se  $\exists \overline{b} \in \mathbb{Z}_m | \overline{a} \cdot \overline{b} = \overline{1} (= \overline{b} \cdot \overline{a})$ . Più in generale, se considero  $\overline{a}, \overline{c} \in \mathbb{Z}_m$  mi posso chiedere se esiste un  $\overline{b}$  tale che  $\overline{a} \cdot \overline{b} = \overline{c}$ , osserviamo che questa uguaglianza tra classi è equivalente ad una congruenza, ovvero  $\overline{a} \cdot \overline{b} = \overline{c} \Leftrightarrow \overline{ab} = \overline{c} \Leftrightarrow ab \equiv c \pmod{m}$ . Quindi il nostro problema, che in seguito studieremo formalmente, è il seguente:  $\exists \overline{b}: \overline{a} \cdot \overline{b} = \overline{c} \Leftrightarrow \exists b \in \mathbb{Z} | ab \equiv c \pmod{m}$ .

Si dice che un elemento  $b \in \mathbb{Z}$  è soluzione dell'**equazione congruenziale**  $ax \equiv c \pmod{m}$  (con  $a, c \in \mathbb{Z}$ ) se e solo se risulta  $ab \equiv c \pmod{m}$ . Studieremo il caso generale.

$\overline{a} \in \mathbb{Z}_m \setminus \{\overline{0}\}$  è invertibile  $\Leftrightarrow \exists \overline{b} \in \mathbb{Z}_m: \overline{a} \cdot \overline{b} = \overline{1} \Leftrightarrow \exists \overline{b} \in \mathbb{Z}_m: \overline{ab} = \overline{1} \Leftrightarrow \exists b \in \mathbb{Z}: ab \equiv 1 \pmod{m} \Leftrightarrow$  l'equazione congruenziale  $ax \equiv 1 \pmod{m}$  ha soluzione.

**Teorema 1** (condizione necessaria e sufficiente affinché un'equazione congruenziale sia risolubile): Siano  $a, b \in \mathbb{Z}, n \in \mathbb{N}^*, d = \text{MCD}(a, n)$ . Allora l'equazione congruenziale  $ax \equiv b \pmod{n}$  ha soluzione se e solo se  $d|b$ .

**Dimostrazione:**  $\Rightarrow$ : Supponiamo che  $ax \equiv b \pmod{n}$  abbia soluzione, allora  $\exists c \in \mathbb{Z} | ac \equiv b \pmod{n}$ , allora  $n|ac - b$  e  $\exists k \in \mathbb{Z} | ac - b = kn$ , ne consegue che  $b = ac - kn$ , inoltre, essendo  $d = \text{MCD}(a, n) \Rightarrow d|a \wedge d|n$ , sia  $a$  che  $n$  sono prodotti di  $d$  per un certo intero, quindi  $\exists r, s \in \mathbb{Z} | a = dr \wedge n = ds$ . Risulta dunque  $b = ac - kn = drc - kds = d(rc - ks)$  e quindi ho che  $b$  si può scrivere come  $d$  per un certo intero, ovvero, come volevasi dimostrare, che  $d|b$ . Implicazione  $\Leftarrow$ : l'ipotesi è che  $d = \text{MCD}(a, n) | b$  e devo trovare una soluzione per  $ax \equiv b \pmod{n}$  in  $\mathbb{Z}$ ; per il teorema di Bezout,  $\exists r, s \in \mathbb{Z} | d = ra + sn$ , per ipotesi ho che  $d|b \Rightarrow b = dh$  con  $h \in \mathbb{Z}$ , ne segue  $b = dh = (ra + sn)h = rha + snh$ , se considero  $rha - b = -snh = n(-sh)$  ed ho dunque che  $n|rha - b$  che per definizione significa  $(rh)a \equiv b \pmod{n}$  e quindi  $rh$  è una soluzione dell'equazione  $ax \equiv b \pmod{n}$ . Come volevasi dimostrare.

**Corollario 2:** Sia  $\overline{a} \in \mathbb{Z}_m \setminus \{\overline{0}\}$ . Allora  $\overline{a}$  è invertibile se e solo se  $\text{MCD}(a, m) = 1$ .

Questo corollario è una conseguenza del teorema 1, infatti  $\overline{a}$  è invertibile  $\Leftrightarrow ax \equiv 1 \pmod{m}$  ha soluzione  $\Leftrightarrow \text{MCD}(a, m) = 1 \Leftrightarrow \text{MCD}(a, n) = 1$

**Esempio** in  $\mathbb{Z}_{10}$ : Vediamo se esiste una classe  $\overline{a} \in \mathbb{Z}_{10} | \overline{4} \cdot \overline{a} = \overline{3}$ , questo problema di uguaglianza tra classi si trasforma in un problema di congruenza dei rappresentanti; quindi  $4a \equiv 3 \pmod{10} \Leftrightarrow a$  è soluzione di  $4x \equiv 3 \pmod{10}$ , questa soluzione, per il teorema 1, non esiste poiché il  $\text{MCD}(4, 10) = 2$  non divide 3.

Due equazioni congruenziali si dicono **equivalenti** se ammettono le stesse soluzioni intere. Di conseguenza, per risolvere le nostre equazioni congruenziali ci ridurremo a risolvere una equazione congruenziale equivalente in cui il  $\text{MCD}(a, n) = 1$ .

**Proposizione 3:** Si consideri l'equazione congruenziale  $ax \equiv b \pmod{n}$ , e sia  $1 = \text{MCD}(a, n)$ . Allora, se  $c$  è una soluzione di  $ax \equiv b \pmod{n}$ , l'insieme  $X$  delle soluzioni di  $ax \equiv b \pmod{n}$  è  $X = [c]_n = \{c + kn | k \in \mathbb{Z}\}$

Questo significa che trovata una soluzione, le abbiamo trovate tutte. Prendiamo ad esempio  $3x \equiv 2 \pmod{5}$ , che sappiamo avere soluzione poiché  $1 = \text{MCD}(3, 5)$  divide 2, una soluzione è 4, infatti  $\overline{3} \cdot \overline{4} = \overline{12} = \overline{2}$ , ne consegue che il nostro insieme delle soluzioni  $X = [4]_5 = \{4 + k5 | k \in \mathbb{Z}\}$ .

**Algoritmo per risolvere l'equazione congruenziale  $ax \equiv 1 \pmod{n}$  con  $\text{MCD}(a, n) = 1$ :**

- 1) Poiché  $1 = \text{MCD}(a, n) \Rightarrow \exists h, k \in \mathbb{Z} | 1 = ah + nk$  (teorema di Bezout)
- 2) Determiniamo una coppia  $(h, k)$  con l'algoritmo delle divisioni successive
- 3) Di conseguenza, ragionando in modulo  $n$ ,  $\overline{1} = \overline{ah + nk} = \overline{ah} + \overline{nk} = \overline{a} \cdot \overline{h} \Rightarrow ha \equiv 1 \pmod{n} \Rightarrow h$  è una soluzione
- 4) L'insieme  $X$  di tutte le soluzioni è  $[h]_n = \{h + kn | k \in \mathbb{Z}\}$

Esempio,  $10x \equiv 1 \pmod{17}$ :

- 1)  $\text{MCD}(17, 10) = 1 \Rightarrow \exists h, k \in \mathbb{Z} | 1 = 10h + 17k$
- 2)  $(h, k) = (-5, 3)$ 
  - a.  $17 = 10 \cdot 1 + 7 \rightarrow 7 = 17 - 10$
  - b.  $10 = 7 \cdot 1 + 3 \rightarrow 3 = 10 - 7$
  - c.  $7 = 3 \cdot 2 + 1 \rightarrow 1 = 7 - 3 \cdot 2$
  - d.  $1 = 7 - (10 - 7) \cdot 2 = 7 \cdot 3 - 10 \cdot 2 = (17 - 10) \cdot 3 - 10 \cdot 2 = 10(-5) + 17(3)$
- 3) Una soluzione è quindi  $-5$
- 4)  $[-5]_{17} = \{-5 + k17 | k \in \mathbb{Z}\}$  è l'insieme di tutte le soluzioni

**Proposizione 4:** Siano  $a, b \in \mathbb{Z}, n \in \mathbb{N}^*$ . Se  $t$  è un divisore comune di  $a, b$  e  $n$ , allora l'equazione congruenziale  $ax \equiv b \pmod{n}$  ammette tutte e sole le soluzioni di (si noti che le successive frazioni sono numeri interi, poiché  $t$  divide sia  $a$ , che  $b$  che  $n$ ):  $\frac{a}{t}x \equiv \frac{b}{t} \pmod{\frac{n}{t}}$

**Proposizione 5:** Siano  $a, b \in \mathbb{Z}, n \in \mathbb{N}^*$ . Se  $c$  è una soluzione di  $ax \equiv 1 \pmod{n}$  ( $\text{MCD}(a, n) = 1$ ), allora  $cb$  è soluzione di  $ax \equiv b \pmod{n}$ .

Questi due tipi di riduzioni fa in modo che si possa ritornare all'equazione di tipo particolare  $ax \equiv 1 \pmod{n}$ .

**Risoluzione di un'equazione risolubile di tipo generale:  $ax \equiv b \pmod{n}$**

- 1)  $d = \text{MCD}(a, n)$  deve dividere  $b$  (condizione necessaria e sufficiente per la risolubilità) a questo punto abbiamo  $d|a \wedge d|n \wedge d|b$
- 2) Posto  $\frac{a}{d} = a', \frac{b}{d} = b', \frac{n}{d} = n'$ , l'equazione  $a'x \equiv b' \pmod{n'}$  ammette tutte e sole le soluzioni intere di  $ax \equiv b \pmod{n}$   
**Osservazione:** se divido  $a$  e  $n$  per  $d = \text{MCD}(a, n)$  i numeri che rimangono fuori sono coprimi quindi risulterà  $\text{MCD}(a', n') = 1$
- 3) Risolvo l'equazione  $a'x \equiv 1 \pmod{n'}$  con l'algoritmo precedente
- 4) Se  $c$  è una soluzione di  $a'x \equiv 1 \pmod{n'}$ ,  $c' = cb'$  è soluzione di  $a'x \equiv b' \pmod{n'}$ , e poiché  $\text{MCD}(a', n') = 1$ , l'insieme di tutte le soluzioni è  $[c']_{n'} = \{c' + kn' | k \in \mathbb{Z}\}$

Esempio,  $30x \equiv 6 \pmod{51}$ :

- 1)  $\text{MCD}(30, 51) = 3$  e poiché  $3|6$  questa equazione è risolubile e posso procedere
- 2) L'equazione è equivalente a  $\frac{30}{3}x \equiv \frac{6}{3} \pmod{\frac{51}{3}}$ , ovvero  $10x \equiv 2 \pmod{17}$

- 3) Risolvo l'equazione  $10x \equiv 1 \pmod{17}$  che ha come soluzione  $-5$  (esercizio precedente)
- 4) Moltiplico  $-5 \cdot 2 = -10$  e quindi, essendo  $\text{MCD}(10,17) = 1$ , l'insieme delle soluzioni sarà  $[-10]_{17} = \{-10 + k17 | k \in \mathbb{Z}\}$

**Esercizi:** Determinare in  $\mathbb{Z}_{44}$  una classe  $\bar{a}$  (se esiste) tale che  $\overline{26} \cdot \bar{a} = \bar{6}$  (Aiuto: questa forma può essere scritta come  $26a \equiv 6 \pmod{44} \Rightarrow a$ , se esiste, è soluzione di  $26x \equiv 6 \pmod{44}$ ) Soluzione:  $\bar{a} \in [-15]_{22}$   
 Risolvere le seguenti equazioni congruenziali:  $45x \equiv 12 \pmod{102}$ ;  $25x \equiv 2 \pmod{48}$ ;  $22x \equiv 6 \pmod{50}$

Ricordando che  $ax \equiv b \pmod{m}$  equivale a  $\bar{a} \cdot \bar{x} = \bar{b}$  in  $\mathbb{Z}_m$ :

- Se in  $ax \equiv b \pmod{m}$   $a$  o  $b$  sono maggiori di  $m$  si possono scegliere in  $a$  e in  $b$  i **rappresentanti canonici**.  
 Ad esempio,  $17x \equiv 11 \pmod{6}$  è equivalente a  $5x \equiv 5 \pmod{6}$  (così da semplificare i calcoli)
- Se  $c$  è soluzione di  $ax \equiv b \pmod{m}$ , tutti gli elementi di  $[c]_m$  sono ancora soluzioni.  
 Sia  $c$  una soluzione di  $ax \equiv b \pmod{m}$  allora  $\bar{a} \cdot \bar{c} = \bar{b}$  in  $\mathbb{Z}_m$ . Se  $d \in \bar{c}$  posso, essendo  $\bar{c} = \bar{d}$ , scrivere  $\bar{a} \cdot \bar{d} = \bar{b}$  e quindi che  $ad \equiv b \pmod{m}$
- Sia  $ax \equiv b \pmod{m}$  un'equazione congruenziale,  $d = \text{MCD}(a, m)$ ,  $d|b$  (quindi ha soluzione), le soluzioni intere costituiscono  $d$  classi (modulo  $m$ )  
 $6x \equiv 10 \pmod{20}$ ,  $d = \text{MCD}(20,6) = 2$ ,  $2|10$  e quindi le soluzioni costituiranno due classi (modulo 20)



## 5. Polinomi

### 5.1 L'anello dei polinomi

Sia  $A$  un anello commutativo unitario non nullo. Allora è possibile costruire un anello, che si denota con  $A[x]$ , che sia commutativo unitario, che contenga  $A$  come sottoanello e un elemento  $x \notin A$ , e tale che ogni elemento di  $A[x]$  si possa scrivere sotto la forma (**forma canonica**):  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  con  $a_i \in A$ .

Posto,  $\forall j > n, a_j = 0$ , gli elementi  $a_0, a_1, \dots, a_n, a_{n+1}, \dots$  si dicono i **coefficienti** dell'elemento  $a_0 + a_1x + \dots + a_nx^n$ . Un oggetto dell'anello si dirà **polinomio** e  $A[x]$  si dice anello dei polinomi a coefficienti in  $A$  nell'indeterminata  $x$ .

Due polinomi  $f = a_0 + a_1x + \dots + a_nx^n$  e  $g = b_0 + b_1x + \dots + b_mx^m$  sono **uguali** se hanno tutti i coefficienti ordinatamente uguali ( $\forall i \in \mathbb{N}, a_i = b_i$ ).

Prendiamo  $f = 3 + 2x + 5x^2$  e  $g = 3 + 2x + 12x^2$  con coefficienti in  $\mathbb{Z}$ , ed è ovvio che i due polinomi non sono uguali, ma se invece prendiamo i coefficienti in  $\mathbb{Z}_7$  avremo  $f = \overline{3} + \overline{2}x + \overline{5}x^2$  e  $g = \overline{3} + \overline{2}x + \overline{12}x^2$  e quindi, essendo in  $\mathbb{Z}_7$  (e solo in  $\mathbb{Z}_7$ )  $\overline{5} = \overline{12}$ , i due polinomi sono uguali. **Esercizio:** Dire se esistono degli  $m$  per cui i polinomi  $f = \overline{2} + \overline{10}x + \overline{25}x^3$  e  $g = \overline{2} - \overline{10}x + \overline{30}x^3$  presi in  $\mathbb{Z}_m$  sono uguali.

$(A[x], +, \cdot)$  è un anello commutativo unitario, sia  $n \leq m$ , così da poter porre  $a_{n+1} = \dots = a_m = 0$  e siano  $f = a_0 + a_1x + \dots + a_nx^n$  e  $g = b_0 + b_1x + \dots + b_mx^m$  due polinomi. Allora:

- $f + g = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_m + b_m)x^m$
- $f \cdot g = c_0 + c_1x + \dots + c_{n+m}x^{n+m}$  dove un generico coefficiente è  $c_k = \sum_{i+j=k} a_i b_j$ 
  - $c_0 = a_0 b_0$
  - $c_1 = a_0 b_1 + a_1 b_0$
  - $c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$
  - $c_{n+m} = a_n b_m$
- L'elemento neutro della somma sarà  $f = 0$  mentre il neutro del prodotto sarà  $f = 1$

Un polinomio  $f$  si dice **costante** se ogni suo coefficiente  $a_i$  (con  $i \geq 1$ ) è nullo e quindi  $f = a_0$ . I polinomi costanti sono gli elementi di  $A$ . Quindi 0 e 1 sono due polinomi costanti.

**Esercizio:** Dire se due polinomi di  $\mathbb{Z}_5[x]$ ,  $f = \overline{1} + \overline{3}x + \overline{24}x^2 + \overline{2}x$  e  $g = -x^2 - \overline{9}$  sono uguali. Si consiglia di portarli sotto la forma canonica. (soluzione: i polinomi sono uguali).

### 5.2 Grado di un polinomio

Sia  $f \in A[x] \setminus \{0\}$ ,  $f = a_0 + a_1x + \dots + a_nx^n$  ( $f$  ha qualche coefficiente non nullo) prendiamoci gli indici dei coefficienti non nulli  $T = \{k \in \mathbb{N} | a_k \neq 0\}$  che è un insieme finito e non vuoto. Sia  $m$  il massimo di  $T$  ( $m = \max T \Leftrightarrow m \in T \wedge \forall t \in T (t \leq m)$ ),  $m$  è detto **grado di  $f$**  e si scrive  $m = \delta(f)$  (o anche  $\text{gr}(f)$ ). Se  $m = \text{gr}(f)$  posso scrivere  $f = a_0 + a_1x + \dots + a_mx^m$  con  $a_m \neq 0$  (praticamente mi fermo all'ultimo coefficiente non nullo e scrivo il polinomio senza coefficienti nulli).

$a_m$  è detto **parametro direttore** di  $f$ . Se  $a_m = 1$  il polinomio  $f$  si dice **monico**. Se  $\delta(f) = 0$  allora  $f = a_0$  e quindi il polinomio è una costante non nulla, cioè  $f \in A \setminus \{0\}$ . Se  $f = 0$  si pone  $\delta(f) = -\infty$  (convenzione usata per racchiudere sotto un'unica forma le proposizioni sui gradi dei polinomi).

Sia, ad esempio,  $f = \overline{1} + \overline{4}x + \overline{6}x^2$ , questo polinomio è monico di grado 2 per  $f \in \mathbb{Z}_5[x]$ , mentre è monico di grado 0 per  $f \in \mathbb{Z}_2[x]$ , mentre non è monico per  $f \in \mathbb{Z}_6[x]$

**Proposizione 1:** Siano  $f, g \in A[x]$ . Allora:

1.  $\delta(f + g) \leq \max\{\delta(f), \delta(g)\}$
2.  $\delta(f \cdot g) \leq \delta(f) + \delta(g)$



Osservazioni: Se  $\delta(f) = \delta(g) = m$  e  $a_m = -b_m$ ,  $\delta(f + g) < m$  (ne segue che sarà  $-\infty$  se  $f + g = 0$ ).  
Se  $a_n b_m = 0$  (quindi sono divisori dello zero),  $\delta(f \cdot g) < n + m$ .

### 5.3 Proposizioni sull'anello dei polinomi

**Proposizione 1:** Se  $A$  è un dominio d'integrità, in  $A$  vale la **regola di addizione dei gradi**:  $\forall f, g \in A[x]$   
 $\delta(fg) = \delta(f) + \delta(g)$  (molto importante quando si lavora con i campi, che non hanno divisori dello zero)

**Proposizione 2:** Sia  $A$  un anello commutativo unitario.  $A$  è un dominio d'integrità se e solo se  $A[x]$  è un dominio di integrità.

**Dimostrazione:**  $\Leftarrow$ :  $A[x]$  dominio d'integrità, quindi non ha divisori dello zero, di conseguenza anche  $A(\subseteq A[x])$  è integro.  $\Rightarrow$ : dimostriamo che  $\forall f, g \in A[x] (f \neq 0 \wedge g \neq 0) \Rightarrow fg \neq 0$ ; essendo  $f$  e  $g$  non nulli si ha che  $\delta(f) = n (\geq 0)$  e  $\delta(g) = m (\geq 0)$ . Poiché  $A$  è dominio d'integrità, vale la regola di addizione dei gradi e dunque  $\delta(fg) = \delta(f) + \delta(g) = n + m (\geq 0)$  e dunque  $fg \neq 0$  (altrimenti avremo grado  $-\infty$ )

**Osservazione:** Se  $A[x]$  è dominio di integrità. Il parametro direttore  $fg$  è il prodotto dei parametri direttori di  $f$  e di  $g$  (ad esempio, un prodotto di polinomi monici, il prodotto sarà ancora monico)

**Teorema 3:** Sia  $A$  un dominio d'integrità. Allora i **polinomi invertibili** in  $A[x]$  sono **tutti e soli** gli elementi di  $A$  invertibili in  $A$  (un polinomio  $f \in A[x]$  è invertibile  $\Leftrightarrow \exists g \in A[x] \mid fg = gf = 1$ ).

**Dimostrazione:**  $1_A = 1_{A[x]}$ ; banalmente se  $a \in A$  è invertibile in  $A \Rightarrow \exists b \in A \mid ab = ba = 1_A$  quindi, poiché gli stessi  $a, b \in A[x]$  (polinomi costanti) e  $1_A = 1_{A[x]}$ , si ha che  $a$  è invertibile in  $A[x]$  ed ha come inverso  $a$ . Prendiamo ora un polinomio  $f$  invertibile in  $A[x]$ , quindi, per definizione,  $f \in A[x]$  è invertibile  $\Leftrightarrow \exists g \in A[x] \mid fg = gf = 1_{A[x]}$ . In  $A[x]$  (integro) vale la regola di addizione dei gradi, di conseguenza  $\delta(fg) = \delta(1) = 0 = \delta(f) + \delta(g)$ , i gradi per definizione sono numeri maggiori od uguale a zero, ciò implica che entrambi i gradi debbano essere pari a zero, dunque,  $\delta(f) = \delta(g) = 0$  e quindi sono polinomi costanti, ovvero  $f = a \in A \wedge g = b \in A$  e  $fg = ab = 1 \Rightarrow f = a \in A$  ed è invertibile.

**Corollario 4:** Sia  $A$  un campo, allora i polinomi invertibili in  $A[x]$  sono tutti e soli gli elementi di  $A \setminus \{0\}$  (ovvero le costanti non nulle, ovvero i polinomi di grado zero).

**Esempio:** elementi invertibili in  $Q[x]$  sono  $Q \setminus \{0\}$ . Gli elementi invertibili in  $\mathbb{Z}_7[x]$  sono  $\mathbb{Z}_7 \setminus \{0\}$  (sono 6).

### 5.4 L'anello dei polinomi a coefficienti in un campo

Ricordiamo la seguente proprietà:  $\forall (a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ ,  $\exists! (q, r) \in \mathbb{Z} \times \mathbb{N} \mid a = bq + r \wedge 0 \leq r < |b|$ , dove resto e quoziente sono unici, una proprietà simile vale anche per l'anello dei polinomi a coefficienti in un campo:

**Teorema** (Proprietà della divisione in  $A[x]$  con  $A$  campo): Sia  $A$  un campo. Allora  $\forall (f, g) \in A[x] \times A[x] \setminus \{0\}$   
 $\exists! (q, r) \in A[x] \times A[x] \mid f = gq + r \wedge \delta(r) < \delta(g)$  (tra polinomi non c'è relazione d'ordine quindi non ha senso dire che un polinomi è minore o uguale ad un altro, ma possiamo mettere in relazione i loro gradi).

**Esempio in  $\mathbb{R}[x]$ :** Sia  $f = x^3 + x + 1$  e  $g = 2x + 1$ ; scriviamo  $x^3 + x + 1 \div 2x + 1$  e confrontiamo i primi termini dei due polinomi, moltiplichiamo il coefficiente di  $x^3$  per l'inverso del coefficiente di  $2x$ , quindi avremo  $1(2^{-1})x^{3-1}$  (eleviamo la differenza tra le potenze dei due elementi confrontati). Moltiplichiamo il risultato per  $g$  e sottraiamolo ad  $f$ , quindi avremo  $x^3 + x + 1 - x^3 - \frac{1}{2}x^2 = -\frac{1}{2}x^2 + x + 1$ , questo algoritmo si ripete finché il grado del resto non sarà minore del grado del secondo polinomio (come da teorema). Risulterà  $r = \frac{3}{8}$  e  $q = \frac{1}{2}x^2 - \frac{1}{4}x + \frac{5}{8}$ , quindi  $f = g \left( \frac{1}{2}x^2 - \frac{1}{4}x + \frac{5}{8} \right) + \frac{3}{8}$ .

Per maggiore chiarezza si riporta successivamente l'esercizio completo in una forma più leggibile:

$$\begin{array}{r}
 x^3 + 0x^2 + x + 1 : 2x + 1 \\
 \underline{-x^3 - \frac{1}{2}x^2} \\
 // -\frac{1}{2}x^2 + x + 1 \\
 \underline{+\frac{1}{2}x^2 + \frac{1}{4}x} \\
 // \frac{5}{4}x + 1 \\
 \underline{-\frac{5}{4}x - \frac{5}{8}} \\
 // \frac{3}{8}
 \end{array}
 \quad
 \begin{array}{l}
 \frac{1}{2}x^2 - \frac{1}{4}x + \frac{5}{8} \\
 r = \frac{3}{8} \quad \delta(r) = 0 < 1 = \delta(q) \\
 q = \frac{1}{2}x^2 - \frac{1}{4}x + \frac{5}{8} \\
 f = \delta \left( \frac{1}{2}x^2 - \frac{1}{4}x + \frac{5}{8} \right) + \frac{3}{8}
 \end{array}$$

Esercizi: Dividere  $f = 2x^3 - x + 2$  per  $g = 3x^2 - 1$  in  $\mathbb{R}[x]$ . In  $\mathbb{Z}_5[x]$   $f = x^3 + x + \bar{1}$  per  $g = \bar{2}x + \bar{1}$ , si faccia attenzione all'inverso di  $\bar{2}$  che è  $\bar{3}$ . Dividere  $f = x^4 - \bar{2}$  per  $g = \bar{2}x - 1$  in  $\mathbb{Z}_7[x]$  e poi in  $\mathbb{Z}_{11}[x]$ .

## 5.5 Funzione polinomiale

Si tenga presente che la funzione polinomiale è una funzione che si associa al polinomio, ma il polinomio non è una funzione, bensì un oggetto di un insieme.

Sia  $A$  un campo, e sia  $f = b_0 + b_1x + \dots + b_nx^n \in A[x]$  si dice **applicazione polinomiale** determinata da  $f$ , l'applicazione  $\bar{f}: c \in A \rightarrow b_0 + b_1c + \dots + b_nc^n \in A$ .

Valgono inoltre le seguenti proprietà,  $\forall f, g \in A[x]$ :

- $\overline{f+g}(c) = \bar{f}(c) + \bar{g}(c)$
- $\overline{fg}(c) = \bar{f}(c) \cdot \bar{g}(c)$

Per semplicità scriveremo  $\bar{f}(c)$  come  $f(c)$  (si riconosce dal polinomio poiché quest'ultimo non si calcola).

$c \in A$  è **radice** di  $f \Leftrightarrow f(c) = 0$ .

Proposizione 1: Sia  $A$  un campo, sia  $f \in A[x]$  di grado 1. Allora  $f$  ha una radice in  $A$

Dimostrazione:  $f = ax + b$  con  $a \neq 0$  poiché  $\delta(f) = 1$ , se prendiamo un elemento  $c = -a^{-1}b \in A$  si ha che  $f(c) = a(-a^{-1}b) + b = -b + b = 0$ .

Proposizione 2: Siano  $A$  un campo,  $c \in A$  e  $f, g, h \in A[x]$ . Se  $f = gh$ ,  $f(c) = 0 \Leftrightarrow g(c) = 0 \vee h(c) = 0$

Dimostrazione:  $f = gh$ ,  $f(c) = gh(c) = g(c)h(c)$  e quindi la tesi, poiché siamo in un dominio di integrità.

Osservazione: Questa proposizione ci permette di scomporre un polinomio per trovarne le radici, ad esempio, in  $\mathbb{R}[x]$ :  $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$  e quindi le radici saranno le radici dei primi due fattori, ovvero  $c = \pm 1$ , poiché  $x^2 + 1 \in \mathbb{R}[x]$  non ha radici in  $\mathbb{R}$ .

Corollario 3: Se  $f \in A[x]$ , con  $A$  campo, e  $f$  ha un fattore di grado 1,  $f$  ha una radice.

Dimostrazione:  $f = gh$ , sia  $\delta(g) = 1 \Rightarrow g$  ha una radice  $c$ , che è anche radice di  $f$  e quindi  $f(c) = 0$ .

## 5.6 Teorema di Ruffini e sue conseguenze

**Teorema di Ruffini:** Siano  $A$  un campo,  $f \in A[x]$ ,  $c \in A$ . Allora  $c$  è radice di  $f \Leftrightarrow x - c | f$  (questa uguaglianza significa che  $f(c) = 0 \Leftrightarrow \exists g \in A[x] | f = g(x - c)$ )

**Dimostrazione:** Implicazione banale,  $\Leftarrow$ : Sia  $x - c | f$ , quindi  $\exists g \in A[x] | f = (x - c)g$ , e quindi sarà semplicemente  $f(c) = (c - c)g(c) = 0$ . Implicazione  $\Rightarrow$ : Sia  $f(c) = 0$ , applichiamo la proprietà della divisione di  $A[x]$  alla coppia  $(f, x - c)$ .  $\exists! (q, r) \in A[x] \times A[x]$  tale che  $f = (x - c)q + r \wedge \delta(r) < \delta(x - c)$  e in questo caso sappiamo quindi che  $\delta(r) < 1$  e questo significa che  $\delta(r)$  può essere o pari a zero o a  $-\infty$ . Per dimostrare che  $x - c | f$  dobbiamo dimostrare che  $\delta(r) = -\infty$  (ovvero il grado di zero), in ogni caso  $\delta(r) = 0 \Rightarrow r \in A \setminus \{0\}$ , mentre,  $\delta(r) = -\infty \Rightarrow r = 0$ , quindi  $r \in A$  è un polinomio costante (l'applicazione polinomiale determinata da un polinomio costante  $r$  agisce così:  $\bar{r}: a \in A \rightarrow r = r_0$ , e quindi  $r(a) = r_0$ , cioè determina l'applicazione costante  $r$ ).  $f = (x - c)q + r$  e per ipotesi  $0 = f(c) = (c - c)q(c) + r(c) = 0 + r(c) = r$  (come osservato tra parentesi poco fa), di conseguenza  $r = 0$  e quindi posso scrivere  $f = (x - c)q$ .

**Corollario 1:** Sia  $A$  un campo e sia  $f \in A[x]$ . Allora  $f$  ammette una radice in  $A$  se e solo se ammette un fattore di grado 1.

**Dimostrazione:** Implicazione  $\Rightarrow$ :  $f$  ammette  $c$  come radice  $\Rightarrow x - c | f \Rightarrow f$  ha un fattore di grado 1. Per l'implicazione  $\Leftarrow$  si veda il corollario 3 del capitolo precedente.

**Teorema generalizzato di Ruffini:** Siano  $A$  un campo,  $f \in A[x]$  e  $c_1, c_2, \dots, c_n$   $n$  elementi distinti di  $A$ . Allora  $c_1, c_2, \dots, c_n$  sono radici distinte di  $f \Leftrightarrow (x - c_1)(x - c_2) \dots (x - c_n) | f$  (anche il loro prodotto divide  $f$ )

Esempi di applicazione del teorema di Ruffini: Sia  $f \in \mathbb{Z}_5[x]$ ,  $f: x^2 + \bar{a}x + \bar{1}$ . Determinare  $\bar{a} \in \mathbb{Z}_5$  tale che  $x - \bar{2} | f$ . Ruffini ci dice che  $x - \bar{2} | f \Leftrightarrow f(\bar{2}) = \bar{0}$ , quindi  $f(\bar{2}) = \bar{4} + \bar{2}\bar{a} + \bar{1} = \bar{0} \Rightarrow \bar{2}\bar{a} = \bar{-5} = \bar{0} \Rightarrow \bar{a} = \bar{0}$ . Scrivere tutti i polinomi in  $\mathbb{Z}_5[x]$  che ammettono  $\bar{2}$  come radice e hanno grado 5:  $f = (x - \bar{2})g \Rightarrow \delta(g) = 4$  essendo  $\delta(f) = 5$  e  $\delta(x - \bar{2}) = 1$ . Segue che  $g = a_0 + a_1x^2 + a_3x^3 + a_4x^4$  con  $a_i \in \mathbb{Z}_5$  e  $a_4 \neq \bar{0}$ . Bisogna dunque vedere come varia la quintupla  $(a_0, a_1, a_2, a_3, a_4) \in \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \setminus \{\bar{0}\}$ ; e quindi la quintupla varia in  $5 \cdot 5 \cdot 5 \cdot 5 \cdot 4$  modi, ovvero i polinomi che ammettono  $\bar{2}$  sono  $5^4 \cdot 2^2$ .

**Esercizi:** In  $\mathbb{Z}_5[x]$ , scrivere i polinomi di grado 3 che ammettono  $\bar{0}$  e  $\bar{1}$  come radici. Suggerimento: usare il teorema generalizzato di Ruffini:  $f = (x - \bar{0})(x - \bar{1})h = x(x - \bar{1})h$

Dire per quali  $p$  il polinomio  $x^2 + x - \bar{4}$  ammette  $\bar{3}$  come radice in  $\mathbb{Z}_p[x]$ .

## 5.7 Polinomi irriducibili

Sia  $A$  un campo, definiamo i divisori in  $A[x]$ : Siano  $f, g \in A[x]$ ,  $f$  è un **divisore** di  $g$  (o  $f$  divide  $g$ , oppure  $g$  è multiplo di  $f$ ), quindi  $f | g \Leftrightarrow \exists h \in A[x] : g = fh$ . A questo punto i **divisori banali** di  $g \in A[x] \setminus \{0\}$  sono i **polinomi invertibili**:  $u$  è invertibile  $\Rightarrow g = u(u^{-1}g) \Rightarrow u | g$ ; ed i **polinomi associati** a  $g$ , ovvero l'insieme  $\{ug | u \in A[x] \text{ è invertibile}\}$ . Se  $ug$  è associato a  $g \Rightarrow g = u^{-1}(ug) \Rightarrow ug | g$ .

Sia  $A$  un campo e sia  $f \in A[x] \setminus \{0\}$  un polinomio non nullo.  $f$  si dice **irriducibile** se, e solo se:

- 1)  $f$  non è invertibile
- 2) I divisori di  $f$  sono solo quelli banali (gli invertibili e gli associati di  $f$ )  
(si noti che è praticamente la definizione che abbiamo dato in  $\mathbb{Z}$  per i numeri primi nel [capitolo 4.1](#))

**Definizione equivalente di polinomio irriducibile:**  $f \in A[x] \setminus \{0\}$  ( $A$  campo) è irriducibile se, e solo se:

- 1)  $\delta(f) > 0$  ( $f$  non è invertibile)
- 2)  $\forall h, k \in A[x] (f = hk \Rightarrow \delta(h) = 0 \vee \delta(k) = 0)$  (questa proprietà ci dice che un fattore è invertibile e, di conseguenza, l'altro automaticamente associato, ovvero che i divisori di  $f$  sono quelli banali)

Diamo a questo punto delle proposizioni sui polinomi irriducibili che hanno validità in un qualunque campo: Sia  $A$  un campo.

- 1) Se  $f \in A[x]$  e  $\delta(f) = 1$ ,  $f$  è irriducibile (i polinomi di grado 1 sono sempre irriducibili)  
Dim.:  $\delta(f) = 1 > 0$  (prima proprietà verificata), essendo, inoltre,  $\delta(f) = 1$  se  $f = hk$ , per la regola di addizione dei gradi  $\delta(f) = 1 = \delta(h) + \delta(k)$  ed essendo per definizione i gradi  $\geq 0$  abbiamo concluso.
- 2) Se  $f \in A[x]$ ,  $\delta(f) > 1$  e  $f$  è irriducibile,  $f$  non ha radici in  $A$ .  
Dim.: i divisori di  $f$  hanno grado 0 (gli invertibili) oppure  $n = \delta(f)$ . Se per assurdo  $f$  ha radice in  $A$  esso avrebbe grado 1 per il teorema di Ruffini e si arriverebbe ad una contraddizione.  
 Il viceversa non sussiste, infatti, esistono polinomi di grado  $> 1$  senza radici che non sono irriducibili  
 Esempio:  $f \in \mathbb{R}[x]$  dove  $f = (x^2 + 1)(x^2 + 1)$ , quindi abbiamo scritto un polinomio di grado 4 come due polinomi di grado 2 e ciò significa che  $f$  non è irriducibile.
- 3) Sia  $f \in A[x]$  e sia  $\delta(f) = 2$  oppure  $\delta(f) = 3$ . Allora  $f$  è irriducibile, se e solo se,  $f$  non ha radici in  $A$  (in questo caso, quindi, vale anche il viceversa; a differenza della proposizione 2)  
Dim.:  $\Rightarrow$ :  $f$  è irriducibile e  $\delta(f) > 1 \Rightarrow f$  non ha radici per la proposizione 2.  $\Leftarrow$ : Supponiamo  $f = hk$  e  $\delta(f) = 3$  (dobbiamo mostrare che uno dei due gradi è pari a zero), essendo  $\delta(f) = \delta(h) + \delta(k)$  questa equazione si può ottenere solo con le seguenti combinazioni:  $3 + 0, 2 + 1, 1 + 2, 0 + 3$ ; ma per ipotesi  $f$  non ha radici (che sono di grado 1) e quindi le uniche opzioni sono  $\delta(h) = 0 \wedge \delta(k) = 0$ .

## 5.8 Teorema di fattorizzazione nell'anello dei polinomi a coefficienti in un campo

Teorema (solo enunciato): Siano  $A$  un campo ed  $f \in A[x]$  con  $\delta(f) > 0$  (escludiamo quindi che  $f$  sia nullo o che sia invertibile). Allora  $f$  è irriducibile o è prodotto di polinomi irriducibili. Inoltre, tale fattorizzazione è essenzialmente unica: se  $f = p_1 \cdot \dots \cdot p_k = q_1 \cdot \dots \cdot q_h$  ( $p_i$  e  $q_j$  irriducibili), allora  $h = k$  ed è possibile riordinare i fattori in modo che  $\forall i \in \{1, \dots, h\} p_i$  è associato a  $q_i$

Questo teorema (che è praticamente l'analogo del [teorema fondamentale dell'aritmetica](#)) ci dice che ogni polinomio si può scrivere come prodotto di polinomi irriducibili.

Esercizi: sia  $x^3 + x + \bar{1} \in \mathbb{Z}_3[x]$ , vedere se il polinomio è irriducibile e nel caso scriverlo come prodotto di polinomi irriducibili. Fare la stessa cosa anche per il polinomi  $x^3 + x + \bar{3} \in \mathbb{Z}_5[x]$ . Suggerimento: per un polinomio di grado 3 si possono avere solo due casi:  $\delta(f) = 3 \Rightarrow f$  ha radice  $c \Rightarrow f = (x - c)g$  e  $\delta(g) = 2$   
 $f$  non ha radici  $\Rightarrow f$  è irriducibile

## 5.9 Criteri di irriducibilità in $\mathbb{R}[x]$ , $\mathbb{Q}[x]$

Sia  $f \in \mathbb{R}[x]$  e  $\delta(f) = 2$ . Allora  $f = a + bx + cx^2$  dove  $c \neq 0$  ed il discriminante di  $f$   $\Delta(f) = b^2 - 4ac$ .

Per  $f \in \mathbb{R}[x]$  si ha che  $f$  è irriducibile  $\Leftrightarrow \delta(f) = 1$  oppure  $(\delta(f) = 2 \wedge \Delta(f) < 0)$  (quindi se un polinomio è irriducibile è per forza uno di questi due tipi).

Quando  $\Delta(f) > 0$ , invece, è possibile trovare due radici (eventualmente coincidenti); se  $\alpha_1, \alpha_2$  sono le due radici (eventualmente uguali, se  $\Delta = 0$ )  $f = c(x - \alpha_1)(x - \alpha_2)$  dove  $c$  è detto **parametro direttore**.

Non c'è una caratterizzazione di questo tipo, purtroppo, per i polinomi definiti in  $\mathbb{Q}[x]$ , infatti per quest'ultimi esiste una condizione sufficiente, la quale ci dice quando un polinomio in  $\mathbb{Q}[x]$  è irriducibile. Questa condizione è nota come il **criterio di Eisenstein**:

Criterio di Eisenstein: Sia  $f = a_0 + a_1x + \dots + a_nx^n$  (con  $a_n \neq 0$ ) un polinomio in  $\mathbb{Q}[x]$  con coefficienti interi. Se esiste un primo  $p \in \mathbb{Z}$  tale che  $p$  verifichi le seguenti condizioni:

- 1)  $p \nmid a_n$  ( $p$  non divide il parametro direttore)
- 2)  $p \mid a_0, \dots, a_{n-1}$  ( $p$  divide tutti gli altri coefficienti)
- 3)  $p^2 \nmid a_0$

Allora il polinomio  $f$  è irriducibile in  $\mathbb{Q}[x]$

Proprietà (segue dai criteri di irriducibilità in  $\mathbb{R}[x]$  e dal [teorema di fattorizzazione](#)):

Se  $f \in \mathbb{R}[x]$  ed il grado di  $f$  è dispari allora  $f$  ammette sicuramente una radice in  $\mathbb{R}$

Dimostrazione:  $\exists p_1, \dots, p_k$  irriducibili in  $\mathbb{R}[x]$  tali che  $f = p_1 \cdot \dots \cdot p_k$  in  $\mathbb{R}[x]$  tali che  $f = p_1 \dots p_k$ ; di questi  $p_i$  almeno uno deve avere radice pari ad 1 perché, se per assurdo avessero grado 2 allora il grado di  $f$  sarebbe pari, più precisamente  $\delta(f) = 2k$  (poiché  $p_i$  sono irriducibili hanno o grado 1 oppure 2), C.V.D.

Se  $g$  è un fattore irriducibile di  $f$ , esiste sempre una decomposizione di  $f$  in fattori irriducibili in cui compare  $g$ , infatti se  $g|f$  possiamo scrivere  $f = g \cdot h$  e possiamo a questo punto decomporre  $h$ . Questo vale solo se  $\delta(h) = 0$ , poiché significa che  $f$  e  $g$  sono associati e quindi hanno stessi insiemi di divisori e stessi insiemi di multipli:  $D(f) = D(g)$  e  $M(f) = M(g)$ . Dunque, si può osservare che se  $f \sim g$  e  $f$  è irriducibile, anche  $g$  è irriducibile; infatti,  $\delta(f) > 0 \Rightarrow \delta(g) = \delta(f) > 0$  e  $g$  ammette solo divisori banali:  $D(g) = D(f) = \mathcal{U}(A[x]) \cup \{af | a \in A \setminus \{0\}\} = \mathcal{U}(A[x]) \cup \{ag | a \in A \setminus \{0\}\} \Rightarrow$  divisori banali di  $g$ , C.V.D.

Esempio: Quanti sono i polinomi irriducibili di grado due a coefficienti in  $\mathbb{Z}_2[x]$ ?  $\delta(f) = 2$  con  $f \in \mathbb{Z}_2[x]$ ; si ha quindi  $f = a_0 + a_1x + a_2x^2$  con  $a_2 \neq 0$ , ma essendo  $f \in \mathbb{Z}_2[x]$  allora  $a_2 = 1$  quindi  $f = a_0 + a_1x + x^2$ ; dunque la variazione di  $f$  la fanno  $a_0$  e  $a_1$  che variano in  $\mathbb{Z}_2$  e quindi i possibili  $f$  sono banalmente 4 (nota che è il prodotto  $2 \times 2$  e non la somma). Questi polinomi sono irriducibili se e solo se non hanno radici; dunque, degli  $f$  possibili si ha che  $x^2 = x \cdot x$  (quindi è riducibile),  $\bar{1} + x + x^2$  (irriducibile),  $x + x^2 = x(\bar{1} + x)$  (riducibile), e  $x^2 + \bar{1} = x^2 - \bar{1} = (x - \bar{1})(x + \bar{1})$  (riducibile). In definitiva esiste un unico polinomio irriducibile di grado due a coefficienti in  $\mathbb{Z}_2$ .

Scriviamo, adesso, i polinomi di grado 4 non irriducibili e privi di radici in  $\mathbb{Z}_2[x]$ . Soluzione:  $f$  è per forza prodotto di due fattori irriducibili di grado 2 (che abbiamo visto essere unico:  $\bar{1} + x + x^2$ ) quindi l'unico polinomio non irriducibile e privo di radici di grado 4 dovrà essere  $f = (x^2 + x + \bar{1})(x^2 + x + \bar{1})$ .

## 6. Teoria dei reticoli

### 6.1 Reticoli

Un insieme ordinato  $(S, \leq)$  si dice un **reticolo** se, e solo se,  $\forall x, y \in S, \exists \inf\{x, y\} \wedge \exists \sup\{x, y\}$

N.B.: l'estremo inferiore e superiore di questa proprietà non fa riferimento a tutti gli elementi dell'insieme  $S$  ma solo ai sottoinsiemi composti da due elementi (proprietà puntuale: vale solo per piccoli sottoinsiemi). Informalmente, comunque presi due elementi di un insieme, essi hanno estremo inferiore e superiore, e se questo è valido per tutti gli elementi dell'insieme esso è detto reticolo.

Ne consegue che  $S$  non è un reticolo  $\Leftrightarrow \exists x, y \in S (\nexists \inf\{x, y\} \vee \nexists \sup\{x, y\})$

Poiché qui trattiamo insiemi di due elementi, possiamo semplificare le [definizioni di estremo inferiore e superiore](#) nel seguente modo: Sia  $x, y \in S$

$$z = \inf\{x, y\} \Leftrightarrow \begin{array}{l} 1) z \leq x \wedge z \leq y \\ 2) \forall t \in S (t \leq x \wedge t \leq y \Rightarrow t \leq z) \end{array} \quad a = \sup\{x, y\} \Leftrightarrow \begin{array}{l} 1) x \leq a \wedge y \leq a \\ 2) \forall t \in S (x \leq t \wedge y \leq t \Rightarrow a \leq t) \end{array}$$

Si intuisce che tutti gli insiemi ordinati studiati finora siano reticoli, ma vediamo alcuni:

- $(\mathcal{P}(S), \subseteq)$  è un reticolo: dobbiamo dunque dimostrare che  $\forall X, Y \in \mathcal{P}(S), \exists \inf\{X, Y\} \wedge \exists \sup\{X, Y\}$  rispetto l'inclusione. Quindi, ridefinendo:  $A = \sup\{X, Y\} \Leftrightarrow \begin{array}{l} 1) X \subseteq A \wedge Y \subseteq A \\ 2) \forall T \in \mathcal{P}(S) (X \subseteq T \wedge Y \subseteq T \Rightarrow A \subseteq T) \end{array}$  (l'estremo inferiore sarà analogo). Ovvero, cerchiamo il più piccolo sottoinsieme che contiene sia  $X$  che  $Y$ , quindi l'estremo superiore è  $X \cup Y$ . Analogamente si ragiona per l'estremo inferiore, e quindi, si avrà  $\inf\{X, Y\} = X \cap Y$ , essendo  $B = \inf\{X, Y\} \Leftrightarrow \begin{array}{l} 1) B \subseteq X \wedge B \subseteq Y \\ 2) \forall T \in \mathcal{P}(S) (T \subseteq X \wedge T \subseteq Y \Rightarrow T \subseteq B) \end{array}$
- $(\mathbb{N}, |)$  è un reticolo:  $z = \inf\{x, y\} \Leftrightarrow \begin{array}{l} 1) z | x \wedge z | y \\ 2) \forall t \in \mathbb{N} (t | x \wedge t | y \Rightarrow t | z) \end{array}$ ; ma quindi  $z = \text{MCD}(x, y)$ ; in modo analogo si ha che  $m = \sup\{x, y\} \Leftrightarrow \begin{array}{l} 1) x | m \wedge y | m \\ 2) \forall t \in \mathbb{N} (x | t \wedge y | t \Rightarrow m | t) \end{array}$ , ovvero  $m = \text{mcm}(x, y)$

Esercizio: provare che un insieme totalmente ordinato  $(\mathbb{Z}, \leq)$  è sempre un reticolo

Consiglio (utile anche per il compito): quando si studia un insieme ordinato e si vuole vedere se è un reticolo basta limitarsi a vedere cosa succede quando i due elementi non sono confrontabili.

Sia  $S$  un insieme ordinato **finito**, se  $S$  è un reticolo allora esistono minimo e massimo di  $S$ . Ma (nota bene) se  $\exists \max S$  e  $\exists \min S \nRightarrow S$  reticolo (quindi avere massimo e minimo è condizione necessaria ma **non** sufficiente per essere un reticolo; dunque, si può solo dire che se non ha minimo e massimo allora non è un reticolo).

Esempio: sia  $\mathcal{P}(\{1, 2, 3\})$  dove  $\forall X, Y \in \mathcal{P}(\{1, 2, 3\})$  si ha  $X \sigma Y \Leftrightarrow X = Y \vee |X| < |Y|$ , abbiamo che questo insieme ha minimo, costituito dall'insieme vuoto, ed ha massimo, l'insieme  $\{1, 2, 3\}$ ; ma se prendiamo come elementi  $X = \{1, 2\}$  e  $Y = \{1, 3\}$ , abbiamo che i minoranti di  $\{X, Y\}$  (rispetto la relazione d'ordine) sono  $\emptyset, \{1\}, \{2\}, \{3\}$ , ma non esiste nessun massimo di questo insieme poiché ci sono 3 elementi massimali (i diagrammi di Hasse possono essere utili per una migliore comprensione) e dunque  $\mathcal{P}(\{1, 2, 3\})$  non è reticolo.

### 6.2 Reticoli come strutture algebriche a due operazioni

Definiamo due operazioni sui reticoli:

- $\wedge: (x, y) \in S \times S \rightarrow \inf\{x, y\} \in S$  (ad ogni coppia associa l'estremo inferiore dell'insieme  $\{x, y\}$ ),  $\wedge$  è un'applicazione (esiste ed è unica) in  $S$  detta **intersezione reticolare**, in simboli  $\inf\{x, y\} = x \wedge y$
- $\vee: (x, y) \in S \times S \rightarrow \sup\{x, y\} \in S$ ,  $\vee$  è un'applicazione in  $S$  detta **unione reticolare**: scriviamo  $x \vee y$

Esempio: in  $(\mathcal{P}(S), \subseteq)$  l'intersezione reticolare coincide con l'intersezione insiemistica. Infatti,  $\inf\{X, Y\} = X \cap Y = X \wedge Y$ , allo stesso modo l'unione:  $\sup\{X, Y\} = X \cup Y = X \vee Y$ . Mentre, per  $(\mathbb{Z}, \leq)$  si ha che  $\inf\{x, y\} = \min\{x, y\} = x \wedge y$  e  $\sup\{x, y\} = \max\{x, y\} = x \vee y$  (questo in tutti gli insiemi totalmente ordinati). Infine, in  $(\mathbb{N}, |)$  abbiamo  $x \wedge y = \text{MCD}(x, y)$  e  $x \vee y = \text{mcm}(x, y)$ .

Avendo definito, dato un reticolo, due operazioni, possiamo associare ad ogni reticolo  $(S, \leq)$  una struttura algebrica  $(S, \wedge, \vee)$ . Definiamo ora le proprietà di quest'ultima (valide per un reticolo qualunque).

Proprietà della struttura algebrica  $(S, \wedge, \vee)$

- 1)  $\wedge$  e  $\vee$  sono commutative:  $\forall a, b \in S$   
 $a \vee b = b \vee a$   
 $a \wedge b = b \wedge a$
- 2)  $\wedge$  e  $\vee$  sono associative:  $\forall a, b, c \in S$   
 $a \vee (b \vee c) = (a \vee b) \vee c$   
 $a \wedge (b \wedge c) = (a \wedge b) \wedge c$
- 3)  $\forall a, b \in S$  ( $a = a \wedge (a \vee b) = a \vee (a \wedge b)$ ) (**proprietà di assorbimento**)  
 Basti pensare che  $a = a \wedge (a \vee b) = \inf\{a, a \vee b\}$  e  $a = a \vee (a \wedge b) = \sup\{a, a \wedge b\}$

È possibile dimostrare il seguente teorema (ma noi non lo faremo :D)

**Teorema:** Sia  $(S, \tilde{\wedge}, \tilde{\vee})$  una struttura algebrica a due operazioni che verificano le proprietà di commutatività, associatività e assorbimento (le 3 precedenti). Allora è possibile definire in  $S$  una relazione d'ordine  $\rho$  tale che  $(S, \rho)$  sia un reticolo e le sue operazioni reticolari coincidono con  $\tilde{\wedge}, \tilde{\vee}$  e  $\rho$  è così definita:

- $\forall x, y \in S$   $x \rho y \Leftrightarrow x = x \tilde{\wedge} y$ 
  - 1)  $\rho$  è di ordine
  - 2)  $\forall x, y \in S$ ,  $\inf_{\rho}\{x, y\} = x \tilde{\wedge} y$  e  $\sup_{\rho}\{x, y\} = x \tilde{\vee} y$

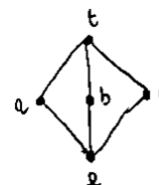
**Esempio:** Prendiamo la struttura algebrica  $(\mathcal{P}(S), \cap, \cup)$ , questa struttura algebrica rispetta le tre proprietà viste precedentemente (commutativa e associativa sono ovvie, per la tre:  $A \cap (A \cup B) = A = A \cup (A \cap B)$ ), mentre  $\forall X, Y \in \mathcal{P}(S)$  si ha  $X \rho Y \Leftrightarrow X = X \cap Y \Leftrightarrow X \subseteq Y$  (questo significa che se conosco il reticolo conosco la struttura algebrica e se conosco la struttura algebrica conosco il reticolo).

Sia  $\mathcal{S}$  i reticoli con sostegno  $S$  e sia  $\mathcal{R}$  una struttura algebrica a due operazioni su  $S$  che verificano quelle tre proprietà. Allora  $f: (S, \leq) \in \mathcal{S} \rightarrow (S, \wedge, \vee) \in \mathcal{R}$  (posso associare a qualunque reticolo una struttura algebrica). Mentre si evince dal teorema che  $g: (S, \tilde{\wedge}, \tilde{\vee}) \in \mathcal{R} \rightarrow (S, \rho) \in \mathcal{S}$  (passo da struttura a reticolo e viceversa).

### 6.3 Reticoli distributivi

In generale,  $\wedge$  e  $\vee$  non sono distributive una rispetto all'altra. Sia ad esempio il seguente reticolo disegnato con il diagramma di Hasse (ogni reticolo di questa forma prende il nome di trirettangolo):

Si ha  $a \vee (b \wedge c) = a \vee e = a$ , mentre  $(a \vee b) \wedge (a \vee c) = t \wedge t = t$  (se ci fosse stata la distributività avremmo dovuto avere nuovamente  $a$ ).



Un reticolo  $(S, \leq)$  si dice distributivo se, e solo se,  $\vee$  è distributiva rispetto a  $\wedge$  e,  $\wedge$  è distributiva rispetto a  $\vee$ . (quindi deve valere la doppia distributività). I reticoli trirettangoli e pentagonali ( $\Diamond$ ) non sono distributivi (se, facendo il diagramma di Hasse, si trova almeno una delle due forme allora il reticolo non è distributivo).

In un reticolo  $(S, \leq)$  vale la seguente proprietà:  $\vee$  è distributiva rispetto a  $\wedge$  se, e solo se,  $\wedge$  è distributiva rispetto a  $\vee$  (quindi o sono tutte e due distributive o non lo è nessuna delle due, di conseguenza per dimostrare che un reticolo sia distributivo basta verificare la proprietà solo per un'operazione rispetto l'altra).

**Esercizio:** dimostrare che  $(\mathcal{P}(S), \subseteq)$  è un reticolo distributivo.

### 6.4 Sottoreticoli e Teorema di Birkoff

Sia  $(S, \leq)$  un reticolo. Allora una parte  $H \neq \emptyset$  di  $S$  si dice un **sottoreticolo** di  $S$  se, e solo se,  $\forall x, y \in H$  ( $x \vee y \in H$  e  $x \wedge y \in H$ ) (chiediamo praticamente che  $H$  sia una parte chiusa rispetto le due operazioni).

**Teorema** (Birkoff): Un reticolo  $(S, \leq)$  è distributivo se, e solo se,  $S$  non ha sottoreticoli trirettangoli o pentagonali (utile poiché dimostrare la distributività non è sempre facile, quindi, se è possibile disegnare il diagramma di Hasse, allora sarà facile dire se quel reticolo è distributivo o meno).



Ogni insieme totalmente ordinato è un reticolo distributivo (non esistono elementi non confrontabili quindi è ovvio che non si avrà mai la forma trirettangolare o pentagonale).

Esempio:  $(\mathbb{Z}, \leq)$  è distributivo, così come  $(\mathbb{N}, |)$ , anche se la sua dimostrazione (non sarà svolta) è meno ovvia

## 6.5 Reticoli limitati

Un reticolo  $(S, \leq)$  si dice **limitato** se dotato di minimo e di massimo, ovvero se esistono il  $\min S$  e il  $\max S$ , i quali, per velocità di notazione, si denotano  $0_S$  e  $1_S$  rispettivamente.

Se  $0_S = \min S$  e  $1_S = \max S$  si ha che  $0_S$  in  $(S, \wedge, \vee)$  è l'elemento neutro rispetto a  $\wedge$  e  $1_S$  è l'elemento neutro rispetto a  $\vee$  (quindi dire che esiste elemento neutro rispetto le due operazioni equivale a dire che nella struttura algebrica ci siano minimo e massimo). Infatti,  $\forall x \in S, 0_S \leq x$  e quindi  $0_S \vee x = x = x \vee 0_S$ , analogamente  $1_S \wedge x = x = x \wedge 1_S$ . Viceversa, se in  $(S, \wedge, \vee)$  c'è un elemento neutro  $\varepsilon$  per  $\vee$  allora  $\forall x \in S, \varepsilon \vee x = x \Rightarrow \varepsilon \leq \varepsilon \vee x = x \Rightarrow \varepsilon = \min S$  e, in modo analogo,  $m \wedge x = x \Rightarrow x = m \wedge x \leq m \Rightarrow m = \max S$ .

Esempio:  $(\mathcal{P}(S), \subseteq)$  è limitato; infatti,  $\min \mathcal{P}(S) = \emptyset (= 0_{\mathcal{P}(S)})$  e  $\max \mathcal{P}(S) = S (= 1_{\mathcal{P}(S)})$ , mentre l'insieme  $(\mathbb{Z}, \leq)$  è non limitato, non avendo n'è minimo e n'è massimo. Per  $(\mathbb{N}, |)$  sappiamo che  $\min \mathbb{N} = 1 = 0_S$  e  $\max \mathbb{N} = 0 = 1_S$  e quindi  $(\mathbb{N}, |)$  è un reticolo limitato.

Un reticolo **finito** è sempre limitato (quindi ha sempre massimo e minimo). Infatti, sia  $(S, \leq)$  un reticolo con  $|S| = n$ , essendo  $S = \{x_1, x_2, \dots, x_n\}$  composto da un numero finito di elementi, la proprietà associativa mi consente di scrivere un certo elemento  $a = x_1 \wedge x_2 \wedge \dots \wedge x_n = \inf\{x_1, x_2 \wedge \dots \wedge x_n\} \Rightarrow a \leq x_i$  e quindi, per definizione,  $a = \min S$ . Analogamente  $b = x_1 \vee \dots \vee x_n = \max S$ . Ne consegue che se  $(S, \leq)$  è **finito** e non ha o massimo o minimo, sicuramente  $S$  non è un reticolo (N.B.: che se siamo in presenza di un insieme finito con sia massimo che minimo allora questo **potrebbe** essere un reticolo, ma non è detto che lo sia).

## 6.6 Reticoli complementati

Sia  $(S, \leq)$  un reticolo **limitato** e sia  $a \in S$ . Un elemento  $b \in S$  si dice un **complemento** di  $a$  se, e solo se, gode contemporaneamente delle seguenti proprietà:  $\begin{cases} a \vee b = 1_S \\ a \wedge b = 0_S \end{cases}$ . Il complemento può non essere **unico**.

Esempio: Sia il reticolo in figura. In questo caso ogni elemento di questa riga ha come complementi gli altri due, ad esempio  $a$  ha come complementi sia  $b$  che  $c$ .



Un reticolo limitato si dice **complementato** se ogni suo elemento ha almeno un complemento.

Si noti come il reticolo dell'esempio precedente sia complementato, infatti gli elementi non specificati prima, ovvero il minimo ed il massimo sono uno il complemento dell'altro. In generale,  $0_S$  e  $1_S$  sono sempre uno il complemento dell'altro:  $\begin{matrix} 0 \vee 1 = 1 \\ 1 \wedge 0 = 0 \end{matrix}$ . In particolare, il reticolo trirettangolo è sempre complementato.

Se  $x \in S \setminus \{0, 1\}$ , un complemento  $y$  di  $x$  è necessariamente non confrontabile con  $x$  (quindi se si deve cercare il complemento di un elemento lo si deve cercare tra quelli non confrontabili).

Infatti, sia per assurdo  $x$  e  $y$  confrontabili allora o  $x \leq y$  oppure  $y \leq x$ . Sia  $x \leq y$  allora  $\inf\{x, y\} = \min\{x, y\} = x$  e quindi risulta  $x \wedge y \neq 0$ , il caso  $y \leq x$  è analogo (si lascia come esercizio).

Ne segue che se in  $S \setminus \{0, 1\}$  c'è un elemento confrontabile con tutti gli altri allora  $S$  non è complementato.

Formalmente:  $(S, \leq)$  è **complementato**  $\Leftrightarrow \forall x \in S, \exists \bar{x} \in S (x \vee \bar{x} = 1_S \text{ e } x \wedge \bar{x} = 0_S)$ .

Come conseguenza di ciò che abbiamo visto; se  $(S, \leq)$  è un insieme totalmente ordinato e limitato con almeno tre elementi,  $S$  non è complementato (poiché tutti gli elementi diversi da minimo e massimo sono confrontabili con tutti e quindi non hanno complemento).

Se  $(S, \leq)$  è un reticolo distributivo, ogni elemento di  $S$  ha al più un complemento (se esiste, è unico).

$(\mathcal{P}(S), \subseteq)$  è un reticolo distributivo: abbiamo già visto come  $1_S = S$  e  $0_S = \emptyset$ , mentre  $\vee = \cup$  e  $\wedge = \cap$ . Si ha che  $X \in \mathcal{P}(S)$  è un complemento di  $X \Leftrightarrow X \cup Y = S$  e  $X \cap Y = \emptyset$  (quindi quando cerco un complemento di  $X$  devo trovare un  $Y$  con queste proprietà, ovvero il complemento è un insieme disgiunto che unito all'elemento dà tutto  $S$ ). Banalmente  $Y = S \setminus X$  (complemento reticolare coincide con il complemento insiemistico). Ed essendo  $\mathcal{P}(S)$  anche un reticolo distributivo, siamo sicuri che sia l'unico complemento. Di conseguenza  $(\mathcal{P}(S), \subseteq)$  è un reticolo distributivo e complementato.

## 6.7 Reticolari Booleani e Teorema di Stone

Un reticolo  $(S, \leq)$  si dice **booleano** se  $S$  è un reticolo distributivo e complementato.

Esempio:  $(\mathcal{P}(S), \subseteq)$  è un reticolo booleano (abbiamo già dimostrato che sia distributivo e complementato).

**Teorema di Stone:** Sia  $(S, \leq)$  un reticolo booleano. Allora:

- Se  $S$  è finito, esiste un insieme  $X$  (finito) tale che  $(S, \leq)$  è isomorfo (applicazione biettiva che conserva l'ordine) a  $(\mathcal{P}(X), \subseteq)$ .
- Se  $S$  è infinito, esiste un insieme  $X$  (infinito) tale che  $(S, \leq)$  è isomorfo ad un sottoreticolo di  $(\mathcal{P}(X), \subseteq)$ .

**Osservazioni:** ci dà informazioni sull'ordine di  $S$  quando  $S$  è un reticolo booleano finito, dicendo, in particolare, che  $S$  ha lo stesso ordine di  $\mathcal{P}(S)$  (essendo isomorfo). Quindi se  $|X| = n$  si ha  $S = 2^n$ .

**Corollario:** se  $S$  è un reticolo booleano finito, l'ordine di  $|S| = 2^n$  con  $n \in \mathbb{N}$ .

N.B.: Questa condizione è necessaria ma non sufficiente affinché il reticolo sia booleano.

**Esempio:** Sia  $(S, \leq)$  un insieme ordinato con  $|S| = 7$ , se si dimostra essere un reticolo, essendo  $7 \neq 2^n$  con  $n \in \mathbb{N}$  possiamo sicuramente dire che non è booleano. Quindi supponendo di aver dimostrato che  $S$  sia un reticolo complementato possiamo già dire che  $S$  non è anche distributivo (senza necessità di dimostrarlo). Se invece  $|S| = 8$  **potrebbe** essere booleano, ma non è detto che lo sia.

## 6.8 Algebra di Boole e anelli booleani

Supponiamo che  $(S, \leq)$  è un reticolo booleano; quindi, essendo distributivo sappiamo che  $\forall a \in S$  esiste un unico complemento  $a'$ ; dunque, ha senso considerare la seguente applicazione:  $' : a \in S \rightarrow a' \in S$  che è vista come operazione unaria, cioè applicazione di  $S$  in  $S$ . Ne consegue che su un reticolo booleano, oltre le solite due operazioni posso aggiungere questa operazione unaria arricchendo la struttura ( $'$  si legge primo).

Se  $(S, \leq)$  è booleano posso associare ad  $S$  la struttura algebrica  $(S, \vee, \wedge, ')$  dove  $\vee$  e  $\wedge$  sono operazioni binarie e  $'$  è un'operazione unaria, che unifica le seguenti proprietà:

- 1)  $\vee$  e  $\wedge$  sono associative
- 2)  $\vee$  e  $\wedge$  sono commutative
- 3) Vale la legge di assorbimento
- 4)  $\vee$  e  $\wedge$  sono distributiva rispetto all'altra
- 5) Esiste elemento neutro  $1_S$  e  $0_S$  per  $\vee$  e  $\wedge$ , rispettivamente
- 6)  $\forall a \in S, a \vee a' = 1_S$  e  $a \wedge a' = 0_S$

Più in generale, una struttura algebrica  $(S, \vee, \wedge, ')$  che verifichi le proprietà da 1 a 6 si dice **algebra di Boole**.

**Esempio**  $(\mathcal{P}(S), \subseteq)$ :  $\wedge = \cap$ ,  $\vee = \cup$ ,  $' = S \setminus : X \rightarrow S \setminus X$ , la struttura  $(\mathcal{P}(S), \cup, \cap, S \setminus)$  è algebra di Boole.

Sia  $A$  un anello,  $A$  si dice **anello booleano**, se  $A$  è un anello unitario tale che  $\forall a \in A, a^2 = a$  (quando  $a^2 = a$  si dice che  $a$  è idempotente:  $\forall n \geq 2, a^n = a$ ).

**Esempio:**  $(\mathcal{P}(S), \Delta, \cap)$  è booleano se  $S \neq \emptyset$  e unitario (l'unità è  $S$ ) e  $\forall X \in \mathcal{P}(S) X^2 = X \cap X = X$

**Osservazione:** Se  $A$  è un anello booleano, il suo prodotto è commutativo e,  $\forall a \in A, a + a = 2a = 0$  (si dice anche che  $A$  ha caratteristica 2).

**Esempio:**  $X \in \mathcal{P}(S), X + X = X \Delta X = \emptyset$

**Teorema 1:** Sia  $(S, \leq)$  un reticolo booleano con almeno due elementi. Allora definite in  $S$  le seguenti operazioni:  $+: (a, b) \in S^2 \rightarrow (a \wedge b') \vee (a' \wedge b) \in S$  e  $\cdot: (a, b) \in S^2 \rightarrow a \wedge b \in S$ . La struttura  $(S, +, \cdot)$  è un anello booleano.

**Esempio:** Per  $(\mathcal{P}(S), \subseteq): X + Y = (X \cap (S \setminus Y)) \cup ((S \setminus X) \cap Y) = (X \setminus Y) \cup (Y \setminus X) = X \Delta Y$ , mentre  $\forall X, Y \in \mathcal{P}(S), X \cdot Y = X \cap Y$ . In definitiva l'anello così costruito è proprio  $(\mathcal{P}(S), \Delta, \cap)$ .

**Teorema 2:** Sia  $(S, +, \cdot)$  un anello booleano. Allora la relazione così definita in  $S: \forall a, b \in S \quad a \rho b \Leftrightarrow a = a \cdot b$  è di ordine e  $(S, \rho)$  è un reticolo booleano (con almeno due elementi).

**Esempio:** Sia l'anello booleano di partenza  $(\mathcal{P}(S), \Delta, \cap)$ , la relazione sarà  $X \rho Y \Leftrightarrow X = X \cap Y \Leftrightarrow X \subseteq Y$ .

L'analogo del [teorema di Stone](#) vale anche per l'algebra di Boole e per gli anelli booleani.

## 6.9 Esercizi sui reticoli: Cheat

Se un insieme ordinato ha più di un elemento minimale (analogamente massimale) non è un reticolo.

Siano  $x$  e  $y$  minimali (con  $x \neq y$ ) allora l'insieme dei minoranti di  $\{x, y\}$  è ovviamente vuoto (per definizione di minimale) e quindi  $\nexists \inf\{x, y\}$ . Analogamente si descrive il caso per due massimali distinti.

Per definizione  $(S, \leq)$  è un reticolo  $\Leftrightarrow \forall x, y \in S (\exists \inf\{x, y\} \wedge \exists \sup\{x, y\})$  e quindi non è un reticolo se, e solo se,  $\exists \bar{x}, \bar{y} \in S (\nexists \inf\{x, y\} \vee \nexists \sup\{x, y\})$ .

Se si trovano due elementi che non hanno estremo inferiore e/o superiore allora si può dire che quell'insieme ordinato non è un reticolo.

Preso un insieme, per dimostrare che sia un reticolo a volte basta generalizzare lo stesso ragionamento usato per trovare l'estremo inferiore e superiore di una sola coppia.

Consideriamo in  $\mathbb{N} \times \mathbb{N}$  la relazione  $\sigma: \forall (a, b), (c, d) \Leftrightarrow (a \leq c) \wedge (b \leq d)$ . Sia  $X = \{(1, 3), (2, 2)\}$ ,  $(a, b)$  è un minorante di  $X \Leftrightarrow (a, b)\sigma(1, 3) \wedge (a, b)\sigma(2, 2) \Rightarrow a \leq 1 \wedge b \leq 3 \wedge a \leq 2 \wedge b \leq 2 \Leftrightarrow a \leq 1 \wedge b \leq 2$ ; ed il massimo dei minoranti è dunque  $(1, 2) = \inf X = (\min\{1, 2\}, \min\{3, 2\})$ . Allo stesso modo i maggioranti di  $X$  sono le coppie  $(a, b) : (1, 3)\sigma(a, b) \wedge (2, 2)\sigma(a, b) \Leftrightarrow a \geq 2 \wedge b \geq 3$  ed il minimo dei maggioranti sarà  $(2, 3) = \sup X$ . In entrambi i casi non abbiamo fatto altro che confrontare le coordinate e prendere in un caso il minimo e nell'altro il massimo, ed è evidente che questo vada bene qualunque sia la coppia  $(a, b)$ . In generale per  $X = \{(a, b), (c, d)\}$  si ha  $\inf X = (\min\{a, c\}, \min\{b, d\})$  e  $\sup X = (\max\{a, c\}, \max\{b, d\})$  e quindi questo è un reticolo.

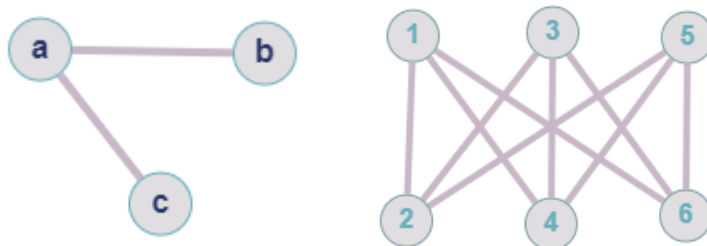
## 7. Elementi di teoria dei grafi

### 7.1 Grafi (semplici non orientati)

Sia  $V$  un insieme non vuoto e  $\rho$  una relazione binaria in  $V$ . La coppia  $(V, \rho)$  si dice un **grafo** se, e solo se:

1.  $\rho$  è simmetrica:  $\forall x, y \in V (x\rho y \Leftrightarrow y\rho x)$
2.  $\rho$  è antiriflessiva:  $\forall x \in V, x \not\rho x$

Esempi:  $V = \{a, b, c\}$  e  $\rho = \{(a, b), (b, a), (a, c), (c, a)\}$ ;  $V_1 = \{1, 2, 3, 4, 5, 6\}$  e  $\rho_1 : \forall x, y \in V, x\rho_1 y \Leftrightarrow 2 \nmid x + y$  (non divide; quindi la somma non deve essere pari). Che vengono rappresentati graficamente come:



Se  $(V, \rho)$  è un grafo, gli elementi di  $V$  si dicono **vertici** del grafo, mentre un sottoinsieme  $\{v, w\} \in \mathcal{P}(V)$  è detto **lato** di  $V$  se, e solo se,  $v\rho w$  (essendo simmetrica e antiriflessiva  $|\{v, w\}| = 2$ ).

Un grafo è **determinato** se conosco l'insieme dei suoi vertici e l'insieme dei suoi lati. Se indichiamo con  $V$  l'insieme dei vertici di  $(V, \rho)$  e con  $L$  l'insieme dei lati,  $(V, \rho)$  si può anche denotare con  $(V, L)$ . Viceversa, sia  $V$  un insieme non vuoto, e  $L \subseteq \mathcal{P}(V)$  tale che  $\forall X \in L, |X| = 2$ , la relazione  $\rho$  così definita in  $V$ :  $\forall x, y \in V, x\rho y \Leftrightarrow \{x, y\} \in L$  è un grafo e  $L$  è l'insieme dei lati del grafo.

Sia  $G = (V, L)$  grafo. Due vertici  $v, w$  di  $V$  si dicono **adiacenti** se  $\{v, w\} \in L$  (se sono vertici di uno stesso lato).

Due lati distinti si dicono **incidenti** se hanno un (unico) vertice in comune (se entrambi i vertici sono in comune è banalmente lo stesso lato).

### 7.2 Isomorfismi tra grafi e sottografi

Siano  $G = (V, L)$  e  $G' = (V', L')$  grafi.  $G$  e  $G'$  si dicono **isomorfi** se, e solo se, esiste un'applicazione tra vertici  $f: V \rightarrow V'$  biettiva tale che  $\forall v, w \in V ((v, w) \in L \Leftrightarrow (f(v), f(w)) \in L')$  (i lati se ne vanno nei lati).

Siano  $G = (V, L)$  e  $G' = (V', L')$  grafi.  $G'$  si dice **sottografo** di  $G$  se, e solo se,  $V' \subseteq V \wedge L' \subseteq L$ .

Sia  $G = (V, L)$  un grafo, e sia  $V' (\neq \emptyset)$  una parte di  $V$ . Si dice **sottografo** di  $G$  **generato** da  $V'$  il grafo  $\overline{G} = (V', \mathcal{P}(V') \cap L)$  (praticamente il sottografo generato è il più grande sottografo formato dai vertici in  $V'$ ).

### 7.3 Grado di un vertice e numero dei lati in un grafo finito

Sia  $G$  un grafo finito (ovvero, sia  $V$  finito) e sia  $v \in V$ . Si dice **grado di  $v$**  il numero dei lati di  $G$  in cui  $v$  è vertice. Il grado di  $v$  sarà indicato con il simbolo  $d(v)$ . Il vertice  $v$  si dice **isolato** se  $d(v) = 0$ , mentre  $v$  si dice **pari**, se e solo se,  $d(v)$  è pari (i vertici isolati sono pari), invece,  $v$  si dirà **dispari** se, e solo se,  $d(v)$  è dispari.

Proposizione 1: Sia  $G = (V, L)$  un grafo finito. Allora  $|L| = \frac{1}{2} \sum_{v \in V} d(v)$  (il numero dei lati sarà dunque la sommatoria dei gradi dei vertici diviso due).

Dimostrazione: Contiamo quanti sono gli estremi di tutti i lati (che sono  $|L|$ ), quindi  $2|L| = \sum_{v \in V} d(v)$ .

Corollario 2:  $\sum_{v \in V} d(v)$  è un numero pari. Ciò che è lo stesso, deve esserci in  $G$  un numero pari di vertici dispari (altrimenti significherebbe che un lato ha un estremo non collegato a nessun vertice).

Un grafo finito  $G$  si dice **regolare** (di grado  $n$ ) se, e solo se,  $\forall v \in G, d(v) = n$ .

## 7.4 Cammini e grafi connessi

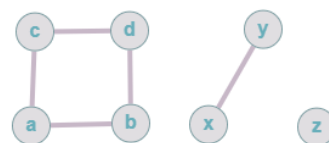
Sia  $G = (V, L)$  un grafo, e siano  $v, w \in V$ . Si dice un **cammino da  $v$  a  $w$**  una sequenza finita  $(l_1, l_2, \dots, l_n)$  di lati di  $G$  con  $l_1 = (z_1, z_2), l_2 = (z_2, z_3), \dots, l_n = (z_n, z_{n+1})$  e  $(z_1 = v \wedge z_{n+1} = w)$ ; mentre  $n$  si dice **lunghezza** del cammino. Per convenzione  $\forall v \in V$  esiste un cammino di lunghezza 0 da  $v$  a  $v$ .

Il grafo  $G$  si dice **connesso** se, e solo se,  $\forall v, w \in V$  esiste un cammino da  $v$  a  $w$  (ogni vertice può essere raggiunto partendo da qualsiasi altro vertice). Sia  $G = (V, L)$  un grafo. Definiamo in  $V$  la seguente relazione  $\sim$ :  $\forall v, w \in V, v \sim w \Leftrightarrow$  esiste un cammino da  $v$  a  $w$ . Inoltre,  $\sim$  è di equivalenza in  $V$ :

- 1)  $\sim$  è riflessiva (c'è infatti il cammino di lunghezza 0)
- 2)  $\sim$  è simmetrica:  $v \sim w \Rightarrow w \sim v$  (è banalmente lo stesso lato con i vertici in ordine inverso)
- 3)  $\sim$  è transitiva:  $\forall v, w, u$  se  $v \sim w \wedge w \sim u \Rightarrow v \sim u$  (è evidente se si disegna un grafo)

Essendo una relazione di equivalenza, la classe  $[v]_{\sim} = \{w \in V \mid \text{esiste un cammino da } v \text{ a } w\}$ . Ne consegue che  $G$  è connesso  $\Leftrightarrow \sim$  ha un'unica classe di equivalenza. Le classi di equivalenza rispetto a  $\sim$  prendono il nome di **componenti connesse di  $G$** .

Esempio:  $[a]_{\sim} = \{a, c, b, d\}$ ,  $[x]_{\sim} = \{x, y\}$ ,  $[z]_{\sim} = \{z\}$ . Di conseguenza il sottografo generato da  $[a]_{\sim} \subseteq V$  è  $V' = \{a, b, c, d\}$  che è un anch'esso un grafo connesso.



Le componenti connesse generano sempre dei sottografi connessi.

Un grafo  $G = (V, L)$  si dice **completo** se  $\forall v, w \in V$  con  $v \neq w$ ,  $v$  e  $w$  sono adiacenti (praticamente connesso tutti i vertici con tutti gli altri vertici).  $\forall v, w \in V$  ( $v \neq w \Rightarrow \{v, w\} \in L$ ). Se  $|V| = n$  finito. Allora  $G$  si dice completo di grado  $n - 1$  e si indica con  $K_n$  (è evidente che a patto di isomorfismi, questo  $K_n$  è unico). Inoltre,  $K_n$  è regolare di grado  $n - 1$  ed ha  $\frac{1}{2} \sum_{v \in V} d(v) = \frac{1}{2} n(n - 1)$  lati.

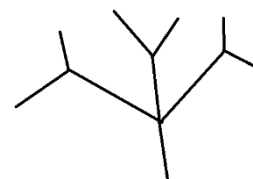
## 7.5 Foreste e Alberi

Sia  $G$  un grafo, e sia  $v$  un elemento di  $V$ . Si dice **circuito** un cammino di lunghezza  $\neq 0$  da  $v$  a  $v$  (parto da  $v$ , mi allontano da  $v$  e ritorno a  $v$ , praticamente ci deve essere un loop nel grafo); la lunghezza sarà  $n \geq 3$  (ovviamente per chiudere un circuito servono almeno tre lati) e due elementi in un circuito sono legati da almeno due cammini (un percorso in senso orario e l'altro in senso antiorario).

Si dice **foresta** un grafo privo di circuiti.

Si dice **albero** un grafo connesso privo di circuiti.

Le componenti connesse di una foresta "sono" alberi (generano sempre sottografi che sono alberi). Nota: se togliamo un lato da un albero questo si sconnette.



## 7.6 Teoremi di caratterizzazione degli alberi (solo enunciati)

**Teorema 1:** Sia  $G = (V, L)$  un grafo. Allora sono equivalenti le seguenti proprietà:

- 1)  $G$  è un albero;
- 2)  $\forall v, w \in V$  se  $v \neq w$ , esiste un solo cammino da  $v$  a  $w$ ;
- 3)  $G$  è connesso e,  $\forall l \in L$ , il sottografo di  $G$ :  $G' = (V, L \setminus \{l\})$  è sconnesso;
- 4)  $G$  è privo di circuiti e, se  $v, w \in V$  sono vertici non adiacenti, il grafo  $G = (V, L \cup \{v, w\})$  ha uno e un solo circuito

**Teorema 2:** Sia  $G = (V, L)$  un grafo finito con  $|V| = n$ . Allora sono equivalenti le seguenti proprietà:

- 1)  $G$  è un albero;
- 2)  $G$  è connesso e ha  $n - 1$  lati;
- 3)  $G$  è privo di circuiti e  $n - 1$  lati.