SCHEDA G1. – Le relazioni d'equivalenza

Siano A e B due insiemi e siano a∈A e b∈B. Chiamiamo *coppia ordinata* (a,b) l'insieme {{a},{a,b}}.

Con questa definizione si ha $(a,b)=(c,d) \Leftrightarrow \begin{cases} a=c \\ b=d \end{cases}$.

In particolare $(a,b)=(b,a) \Leftrightarrow a=b$.

In modo analogo si definiscono le terne ordinate: siano A, B, C tre insiemi e siano a∈A, b∈B, c∈C; si pone $(a,b,c)=((a,b),c)$.

L'insieme A×B = {(a,b) | a∈A, b∈B} si chiama *prodotto cartesiano* di A e B.

Chiamiamo *relazione* tra A e B ogni terna (A, B, ℜ) dove ℜ è un sottoinsieme del prodotto cartesiano A×B. Per semplicità di linguaggio, se non ci sono ambiguità, spesso viene chiamata relazione l'insieme ℜ.

Si usa scrivere spesso aℜb anziché (a, b)∈ℜ.

Relazioni d'equivalenza. Sia A un insieme. Sia ℜ una relazione su A, ossia un sottoinsieme di A×A. ℜ si dirà *relazione d'equivalenza* se possiede le seguenti tre proprietà:

a) *Riflessiva*: per ogni x∈A si ha xℜx.

b) *Simmetrica*: per ogni x,y∈A, se xℜy allora anche yℜx.

c) *Transitiva*: per ogni x, y, z∈A, se xℜy ed yℜz allora anche xℜz.

Per le relazioni d'equivalenza si usano spesso notazioni particolari: ≅, ~, ≡, = . Data nell'insieme A una relazione d'equivalenza ~, si chiama *classe d'equivalenza* dell'elemento x∈A l'insieme $[x]_{\sim} = \{y \in A \mid x \sim y\}$. Questo insieme $[x]_{\sim}$ non è vuoto perché, per la proprietà riflessiva, esso contiene per lo meno x stesso.

L'insieme delle classi d'equivalenza si chiama *insieme quoziente* di A rispetto a ~ e si denota con A/~. Una proprietà notevole delle classi d'equivalenza è la seguente:

PROPOSIZIONE 1.1. Siano dati un insieme A ed una relazione d'equivalenza ~ su A,

a) Per ogni x, y∈A si ha $[x]_{\sim} = [y]_{\sim}$ se e solo se x ~ y.

b) Per ogni x, y∈A, se $[x]_{\sim} \neq [y]_{\sim}$ allora $[x]_{\sim} \cap [y]_{\sim} = \emptyset$.

Dimostrazione. a) Se $[x]_\sim = [y]_\sim$ allora certamente $y \in [x]_\sim$, quindi $x \sim y$. Viceversa, supponiamo che sia $x \sim y$ e dimostriamo che $[x]_\sim = [y]_\sim$. Per questo proviamo dapprima che $[x]_\sim \subseteq [y]_\sim$. Sia $z \in [x]_\sim$: allora $x \sim z$. Essendo poi per ipotesi $x \sim y$, per la proprietà simmetrica si ha anche $y \sim x$. Per la proprietà transitiva, da $y \sim x$ e $x \sim z$ segue $y \sim z$. Pertanto $z \in [y]_\sim$. Abbiamo quindi provato che ogni elemento $z \in [x]_\sim$ appartiene anche a $[y]_\sim$, dunque $[x]_\sim \subseteq [y]_\sim$. Viceversa, sia $z \in [y]_\sim$: allora $y \sim z$ ed essendo per ipotesi $x \sim y$, per la proprietà transitiva si ha $x \sim z$, quindi $z \in [x]_\sim$. Dunque $[y]_\sim \subseteq [x]_\sim$. Avendo già provato che $[x] \subseteq [y]_\sim$, si ha quindi $[x]_\sim = [y]_\sim$.
b) Siano $x, y \in A$ tali che $[x]_\sim \neq [y]_\sim$. Se per assurdo vi fosse un elemento $z \in [x]_\sim \cap [y]_\sim$ allora $x \sim z$ e $y \sim z$, dunque $x \sim y$ e allora $[x]_\sim = [y]_\sim$.

L'insieme quoziente $A/\sim$ è quindi una *partizione* dell'insieme A, ossia un insieme di sottoinsiemi non vuoti di A tali che a due a due hanno intersezione vuota e ogni $x \in A$ appartiene ad uno (ed uno solo) di essi.

ESEMPI 1.2.

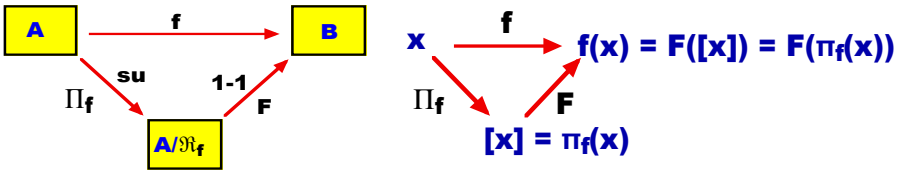
1.2.A. - In ogni insieme A sono relazioni d'equivalenza sia il prodotto cartesiano $A \times A$, in cui ogni elementoè in relazione con tutti gli altri, sia l'identità id_A, costituita dalle coppie (x, x), in cui ogni elemento è in relazione solo con se stesso. Per la proprietà riflessiva, ogni altra relazione d'equivalenza contiene id_A come sottoinsieme.

1.2.B. Data una partizione $\wp$ in un insieme A, diciamo equivalenti due elementi x, y se appartengono allo stesso blocco della partizione. Banalmente si ottiene una relazione d'equivalenza, le cui classi sono i blocchi della partizione.

1.2.C. Dati due insiemi A e B ed $f:A \to B$, in A è definita la relazione $\Re_f$ seguente: per ogni $x_1, x_2 \in A$ poniamo $x_1 \Re_f x_2$ se $f(x_1) = f(x_2)$. E' immediato provare che $\Re_f$ è una relazione d'equivalenza. la funzione $\pi:A \to A/\Re_f$, $\pi(x) = [x]_{\Re_f}$, è suriettiva. La funzione $F:A/\Re_f \to B$, definita da $F\left([x]_{\Re_f}\right) = f(x)$, è ben definita, ed è iniettiva:

$$F([x]_{\Re_f}) = F([x']_{\Re_f}) \Leftrightarrow f(x) = f(x') \Leftrightarrow x \Re_f x' \Leftrightarrow [x]_{\Re_f} = [x']_{\Re_f};$$

ha poi per immagine Im(f), quindi $F : A/\Re_f \xrightarrow[\text{su}]{1\text{–}1} \mathrm{Im}(f)$, e $f = F \circ \pi$.



Viceversa, data in un insieme A una relazione d'equivalenza ~, si definisca la funzione $\pi:A\to A/\sim$ nel modo seguente: per ogni $x\in A$ sia $\pi(x) = [x]_\sim$. Allora $\Re_\pi = \sim$.

Quest'ultimo modo, ossia partire da una funzione, è forse didatticamente il più naturale per definire una relazione d'equivalenza, o equivalentemente, per costruire una partizione.

1.2.D. - Nell'insieme **Z** dei numeri interi relativi fissiamo un numero m e definiamo la seguente relazione: per ogni $x,y\in\mathbf{Z}$, diciamo che x è congruo ad y modulo m, e scriviamo $x \equiv y \pmod m$, se x-y è multiplo di m, ossia esiste $q\in\mathbf{Z}$ tale che $x-y = mq$. Non è difficile provare che la congruenza modulo m è una relazione d'equivalenza:

- *Proprietà riflessiva*: per ogni $x\in Z$ si ha $x-x = 0 = m\cdot 0$, dunque $x \equiv x \pmod m$.
- *Proprietà simmetrica*: se $x \equiv y \pmod m$ allora $x-y = mq$, ma allora $y-x = m(-q)$, quindi anche $y \equiv x \pmod m$.
- *Proprietà transitiva*: se $x \equiv y \pmod m$ ed $y \equiv z \pmod m$ allora $x-y = mq$ e $y-z = mq'$, quindi $y = z+mq'$ e, sostituendo, si ricava $x-(z+mq') = mq$, da cui $x-z = m(q+q')$, ossia $x \equiv z \pmod m$.

Denotiamo con $[x]_m$ le classi d'equivalenza e con $\mathbf{Z}_m$ l'insieme quoziente.

Se $m = 0$ allora si ha: $x \equiv y \pmod 0$ se e solo se $x-y = 0\cdot q$, ossia se e solo se $x = y$. Dunque la congruenza modulo 0 è l'identità su **Z**.

La congruenza modulo 1 è il prodotto cartesiano $\mathbf{Z}\times\mathbf{Z}$.

Se a ed m sono numeri interi e a è multiplo di m allora a è multiplo anche di -m. Pertanto la congruenza modulo m e la congruenza modulo -m coincidono. Supponiamo quindi $m > 0$. Vediamo quante sono le classi. Sappiamo che per ogni $x\in\mathbf{Z}$ esistono $q, r\in\mathbf{Z}$ tali che $x = mq+r$, con $0 \le r < m$. Allora si ha $x-r = mq$, quindi $x \equiv r \pmod m$ e allora $[x]_m = [r]_m$. Allora si ha $\mathbf{Z}_m = \{[0]_m, [1]_m,\ldots, [m-1]_m\}$. Le classi indicate entro le graffe sono tutte distinte; se infatti si ha $0 \le r < s < m$ non può accadere che sia $s-r = mq$, poiché $0 < s-r < s < m$. Allora $\mathbf{Z}_m$ ha esattamente m elementi. In particolare, $\mathbf{Z}_2$ ha due soli elementi: $[0]_2$, costituita dai numeri pari e $[1]_2$, costituita dai numeri dispari.

1.2.E. - Nell'insieme delle rette del piano la relazione di *parallelismo in senso debole*, secondo la quale due rette sono parallele se coincidono oppure se non hanno punti comuni,

è una relazione d'equivalenza. Le classi d'equivalenza si chiamano *fasci di rette parallele* o anche *punti impropri* del piano e l'insieme quoziente si chiama *retta impropria*. Nasce di qui la geometria proiettiva, cui si accenna nel corso. Si può osservare che la proprietà transitiva della relazione di parallelismo è equivalente al postulato euclideo delle parallele, nel senso che, se assunta come postulato, da essa discende che per ogni punto del piano passa una ed una sola parallela ad una retta data.

1.2.F. - Nell'insieme dei poligoni del piano sono note varie relazioni d'equivalenza: la congruenza, la similitudine, l'equiscomponibilità, l'equivalenza (nel senso dell'avere la stessa area). Le rivedremo nel corso.

Spesso le *classificazioni* sono basate su partizioni, quindi su relazioni d'equivalenza.
Per esempio, la suddivisione degli animali in specie, la suddivisione degli iscritti all'Università in corsi di studio, la suddivisione dei cittadini a seconda del comune di residenza, sono esempi di partizioni.
Tuttavia, non tutte le classificazioni sono basate su partizioni, ma talvolta su specializzazioni successive all'interno di una stessa classe, e questo è un rischio di confusione per gli allievi, che da un anno all'altro, da un insegnante all'altro si trovano definizioni diverse.
Per esempio, è indubbio che il numero dei lati ripartisca i *poligoni convessi* in blocchi, quindi è una classificazione per partizione associata ad una funzione: ad ogni poligono convesso si associa il numero dei suoi lati.
Ma nella classe dei quadrilateri, sono messi in evidenza i *trapezi*, con (almeno?) *due* lati opposti paralleli, detti usualmente *basi*. Fra questi ci sono i *parallelogrammi*, in cui anche gli altri due lati sono paralleli, ed i *trapezi isosceli*, in cui i lati che non sono scelti come basi sono congruenti.
I parallelogrammi hanno questa proprietà, quindi sarebbero a loro volta trapezi isosceli.
Se però si definiscono isosceli quei trapezi i cui angoli che hanno per lato una stessa base sono congruenti, ecco che i due lati che non sono basi sono congruenti come prima, ma i parallelogrammi non hanno questa proprietà e quindi non sono più necessariamente trapezi isosceli.
Personalmente, preferisco quest'ultima situazione, perché i trapezi isosceli hanno le diagonali congruenti, mentre i parallelogrammi hanno le diagonali con lo stesso punto medio, e le due proprietà di solito non coesistono.

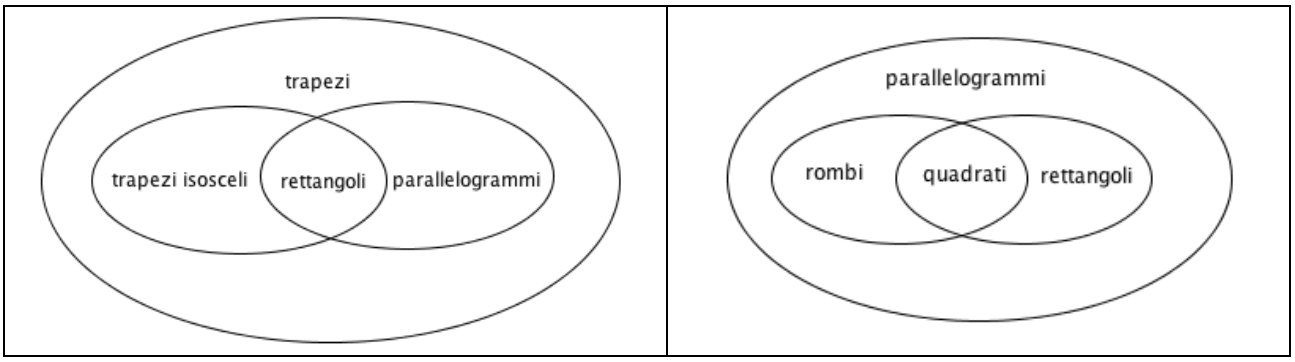
Però, i *rettangoli* sono quadrilateri con i quattro angoli congruenti, e si dimostra che sono parallelogrammi, ma soddisfano comunque la definizione di trapezio isoscele, quindi lo sono. Difatti, le loro diagonali sono congruenti e si bisecano.

I *rombi* sono quadrilateri coi quattro lati congruenti. Si dimostra che i lati opposti sono paralleli, quindi sono parallelogrammi, e le loro diagonali si bisecano, ma sono anche perpendicolari fra loro e sono bisettrici degli angoli da cui escono.

Gli *aquiloni*, o *deltoidi*, sono quadrilateri che hanno le diagonali perpendicolari, ed una di queste è anche bisettrice degli angoli da cui esce.

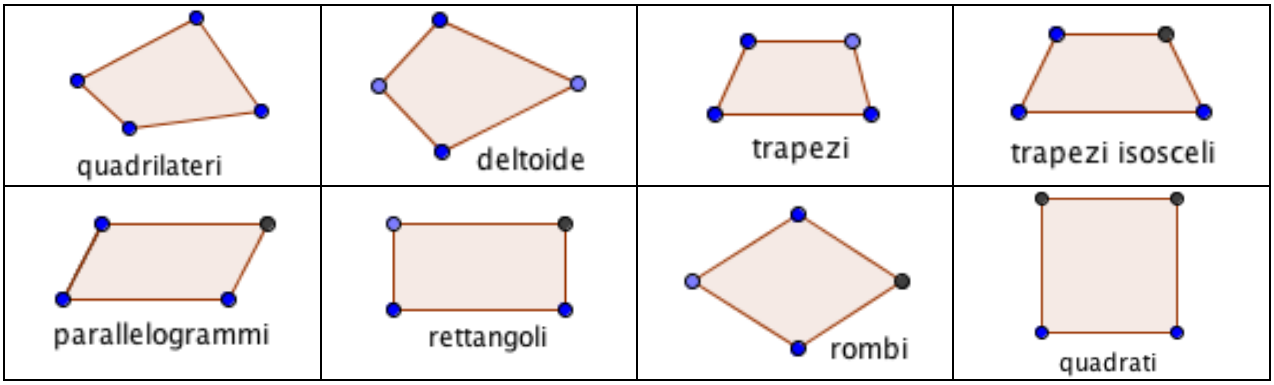
Quindi i rombi sono particolari deltoidi.

Un quadrilatero che abbia sia i lati sia gli angoli congruenti è detto *quadrato*. Esso è quindi un rombo ed anche un rettangolo; ha le diagonali congruenti, che si bisecano e sono perpendicolari e bisettrici degli angoli da cui escono.



In generale, gli allievi (e la cultura comune) comprendono meglio le classificazioni per partizione, per cui i rettangoli non si pensano con i lati congruenti ed i rombi non hanno gli angoli congruenti, se no sarebbero quadrati; i trapezi hanno solo una coppia di lati opposti paralleli e non entrambe, quindi i rettangoli non sono pensati come trapezi particolari, ecc.

Come sono intese queste figure lo vediamo nella figura sottostante:



Un altro modo di costruire una partizione in un insieme è basato sul concetto di *azione di un gruppo su un insieme*, sul quale torneremo nel modulo di Algebra.

Sappiamo che, dato un insieme non vuoto X e due *funzioni biiettive* f, g da X a se stesso, la loro composta $g \circ f : X \to X$ è ancora biiettiva; inoltre, l'identità, che abbiamo visto come relazione d'equivalenza, è anche una funzione biieettiva. Infine, la relazione trasposta di una funzione biiettiva f è a sua volta una funzione biiettiva, detta *inversa* di f e denotata con f^{-1}. L'inversa dell'inversa di f è proprio f. La composta di ogni funzione biiettiva con la sua inversa è l'identità. Sappiamo poi che la composizione di funzionimè associativa.

Tutte queste proprietà si riassumono dicendo che l'insieme delle funzioni biiettive da X a se stesso è un *gruppo* rispetto alla composizione.

Tale gruppo è detto *gruppo simmetrico* S_X sull'insieme X.

I suoi elementi sono anche chiamati *permutazioni* di X. I suoi *sottogruppi* sono anche detti *gruppi di permutazioni* su X.

G-Orbite. Sia G un gruppo di permutazioni su X. Per ogni $x, y \in X$ poniamo $x \sim_G y$ se esiste una permutazione $\alpha \in G$ tale che $y = \alpha(x)$.

Si dimostra facilmente che questa è una relazione d'equivalenza in X.

Le classi d'equivalenza sono dette G-orbite.

La relazione è detta *transitiva* se c'è una sola G-orbita comprendente tutto X. In questo caso, per ogni x, y si ha sempre $x \sim_G y$.

Dato un elemento x∈X, lo *stabilizzatore* di x in G è $G_X = \{\alpha \in G \mid \alpha(x) = x\}$ ed è un sottogruppo di G.

Un teorema che vedremo nella sezione di Algebra afferma che se x ed y sono nella stessa G-orbita, ossia se esiste α∈G tale che $y = \alpha(x)$, allora $G_y = \alpha \circ G_X \circ \alpha^{-1}$. In particolare, i due sottogruppi G_X e G_y sono *isomorfi*.

Osserviamo infine che possiamo *prolungare* l'azione di G dagli elementi ai sottoinsiemi di X: se Y è un sottoinsieme di X, ed α∈G, poniamo $Y' = \alpha(Y) = \{\alpha(y) \mid y \in Y\}$.

In questo modo, anche l'insieme dei sottoinsiemi $\wp(X)$ è ripartito in G-orbite.

Poiché gli elementi di G sono funzioni biiettive, sottoinsiemi nella stessa G-orbita devono essere *equipotenti*, cioè avere lo stesso numero (cardinale) di elementi.

Questi concetti sono entrati nella Geometria per opera di *Felix Klein*, un matematico di Erlangen, nella seconda metà dell'ottocento.

A differenza dell'impostazione euclidea, gli autori moderni definiscono infatti la congruenza di figure piane attraverso l'azione di un opportuno gruppo di permutazioni dell'insieme dei punti, detto *gruppo delle isometrie*, individuato mediante opportuni postulati, tra i quali:

- l'orbita di un punto contiene tutti e soli i punti (azione transitiva sui punti)
- l'orbita di una retta contiene tutte e sole le rette
- l'orbita di una semiretta contiene tutte e sole le semirette
- l'orbita di un semipiano contiene tutti e soli i semipiani, ecc

Così, figure nella stessa orbita sono dette anche *isometriche* anziché congruenti.

Realmente, la faccenda è più complicata di come sembra, perché ci sono tanti gruppi di permutazioni dei punti con queste proprietà, quindi a seconda del gruppo prescelto si ha una geometria oppure un'altra.

Per esempio, tutti questi sottogruppi trasformano rette parallele in rette parallele, perché, essendo costituiti da biiezioni, la cardinalità dell'intersezione di sottoinsiemi è conservata. Si conserva anche il numero dei vertici di un poligono.

Pertanto, hanno senso le nozioni di trapezio e di parallelogramma, ma forse non quella di angolo retto e di circonferenza come li intendiamo noi.

Di conseguenza, tutti i triangoli potrebbero appartenere ad un'unica orbita, e così pure tutti i parallelogrammi.

Pertanto, occorrono altri postulati per restringere le possibili scelte.

Se viceversa si segue l'impostazione euclidea della congruenza, con tutti i postulati necessari, si può definire *isometria* una permutazione del piano che trasforma un segmento AB in un segmento A'B' congruente ad AB. Le isometrie così definite, tra le quali c'è ovviamente l'identità, costituiscono un gruppo, la cui struttura sarà esaminata in un capitolo apposito.

Congruenze (algebriche). In un insieme X spesso facciamo coabitare una operazione binaria, ossia una funzione $* : X \times X \to X$, ed una relazione d'equivalenza $\sim$. Si dicono *compatibili* se per ogni x, x', y, y'$\in$X, se x$\sim$x', y$\sim$y' allora anche i risultati x$*$y e x'$*$y' sono equivalenti, ossia x$*$y $\sim$ x'$*$y'.

In tal caso è possibile trasferire l'operazione all'insieme quoziente X/$\sim$, ossia fra le classi d'equivalenza, ponendo: $\left[x\right]_{\sim} * \left[y\right]_{\sim} = \left[x * y\right]_{\sim}$.

Se manca la compatibilità, cambiando i *rappresentanti* delle classi la classe risultato potrebbe cambiare, quindi non si avrebbe più una operazione in X/~.

ESEMPI 1.3.

a) La *congruenza mod m* in $\mathbf{Z}$ è compatibile sia con l'addizione sia con la moltiplicazione, ossia per ogni x, y, x', y' si ha: $\begin{cases} x \equiv x' \pmod m \\ y \equiv y' \pmod m \end{cases} \Rightarrow \begin{cases} x+y \equiv x'+y' \pmod m \\ x \cdot y \equiv x' \cdot y' \pmod m \end{cases}$. Pertanto, si possono trasferire queste operazioni nel quoziente $\mathbf{Z}_m$.

Una applicazione scolastica di questa proprietà, per altro non esplicitata, è costituita dai *criteri di divisibilità* e dalla *prova del 9*. In particolare, poiché 10 ≡ 1 (mod 9), allora anche le sue potenze sono congrue ad 1 mod 9. Ne segue che, per esempio,

$$7548 = 7 \cdot 10^3 + 5 \cdot 10^2 + 4 \cdot 10 + 8 \equiv 7 + 5 + 4 + 8 = 24 = 2 \cdot 10 + 4 \equiv 2 + 4 = 6 \pmod 9$$

Poiché invece 10 ≡ -1 (mod 11), allora

$$7548 = 7 \cdot 10^3 + 5 \cdot 10^2 + 4 \cdot 10 + 8 \equiv -7 + 5 - 4 + 8 = (8+5) - (7+4) = 2 \pmod{11}$$

Ne seguono le note regole: un numero diviso per 9 dà resto uguale al resto della somma delle cifre divisa per 9 e, iterando, all'ultima somma di cifre.

Invece, un numero è divisibile per 11 se e solo se la differenza fra la somma delle cifre di posto pari e quella delle cifre di posto dispari è divisibile per 11.

In modo analogo si ottengono i criteri di divisibilità per 2, 3, 4, 5, 10, 25, che si insegnano nella scuola media.

La prova del 9 si esegue per controllare se il risultato di una operazione è sbagliato: si calcolano i resti dei termini dell'operazione e su di essi si esegue la stessa operazione. Il resto della divisione per 9 del risultato originale e di quest'ultimo devono coincidere, se no c'è un errore o nell'operazione originale, o nella riduzione mod 9 oppure nell'operazione fra i resti. Ovviamente, l'uguaglianza non garantisce la correttezza, perché basta una inversione di cifre e tutto è vanificato: $13+8=21$ oppure $13+8=12$ sarebbero entrambe "approvate" dalla prova del 9.

b) La congruenza di figure piane, limitatamente alle classi dei segmenti, è postulata compatibile con la somma. Lo stesso discorso per la somma degli angoli.

La congruenza di figure piane è *compatibile* anche con le disuguaglianze di segmenti: se AB ≤ CD e se A'B' = AB, C'D'=CD, allora A'B'≤C'D'. Lo stesso discorso per le disuguaglianze di angoli.

Chiusura transitiva di una relazione. Data la relazione $\Re$ fra A e B, possiamo definire una relazione $\Re^T$ fra B ed A, che chiameremo *trasposta* di $\Re$, definita come l'insieme delle coppie (b, a) tali che $(a, b)\in\Re$.

Date le relazioni $(A, B, \Re)$ e $(B, C, \mathcal{S})$, si può definire la *relazione composta* $(A, C, \mathcal{T})$, dove $\mathcal{T} = \Re \circ \mathcal{S}$ è definita da: per ogni $a\in A$, $c\in C$,

$$a \mathcal{T} c \Leftrightarrow \exists\ b\in B \text{ tale che } a\Re b \text{ e } b \mathcal{S} c.$$

Questa "operazione" tra relazioni, non sempre possibile, possiede una proprietà simile alla proprietà *associativa* delle usuali operazioni.

Osserviamo che l'insieme delle relazioni in un insieme X, con la composizione e l'identità costituisce un *monoide*.

Qualora una relazione $\Re$ sia in un insieme X, possiamo comporla con se stessa e costruirne ricorsivamente le *potenze*: $\begin{cases}\Re^1 = \Re \\ \Re^{n+1} = \Re^n \circ \Re\end{cases}$. Forzando un po' le cose, se la relazione non è vuota potremmo anche porre $\Re^0 = id_X$.

Le potenze possiedono le consuete proprietà: per ogni $\Re \in \mathscr{P}(X)$, $m, n\in\mathbf{N}$ si ha:

$$\Re^m \circ \Re^n = \Re^{m+n},\ \left(\Re^m\right)^n = \Re^{mn}$$

Esercizio 1.4. Sia $\Re$ una relazione nell'insieme X e sia $n\in\mathbf{N}$, $n > 1$. Si provi che:

a) Per ogni $x, y\in X$ si ha: $x\Re^n y \Leftrightarrow \exists x_i \in X,\ 1 \le i \le n-1$, tali che, posto $x_0 = x,\ x_n = y$, si ha $\forall i,\ 0 \le i < n,\ x_i \Re x_{i+1}$.

b) Sia $\mathcal{S}$ un'altra relazione in X, tale che $\Re \subseteq \mathcal{S}$, allora per ogni $n\in\mathbf{N}$ si ha $\Re^n \subseteq \mathcal{S}^n$.

Traduciamo ora alcune proprietà delle relazioni in un insieme X in termini di operazioni e di inclusione fra le relazioni stesse. Sappiamo che cosa significa per una relazione essere, *riflessiva, simmetrica, antisimmetrica o transitiva*. Si ha:

PROPOSIZIONE 1.5. Sia data una relazione $\Re$ in un insieme X:

a) $\Re$ è *riflessiva* $\Leftrightarrow\ id_X \subseteq \Re$; è *antiriflessiva* $\Leftrightarrow \Re \cap id_X = \varnothing$

b) $\Re$ è *simmetrica* $\Leftrightarrow \Re = \Re^t$.

c) $\Re$ è *antisimmetrica* $\Leftrightarrow \Re \cap \Re^t \subseteq id_X$; è *emisimmetrica* $\Leftrightarrow \Re \cap \Re^t = \varnothing$

d) $\Re$ è *transitiva* $\Leftrightarrow \Re^2 \subseteq \Re$.

e) $\Re$ è *totale* $\Leftrightarrow \Re \cup \Re^t = X \times X$. Altrimenti, è parziale.

Una *relazione d'equivalenza* $\Re$ in X, che è una relazione riflessiva, simmetrica e transitiva, è allora tale che $id_X \subseteq \Re$, $\Re = \Re^t$, $\Re^2 \subseteq \Re$.

Sia data una relazione $\Re$ in un insieme X. La relazione $\overline{\Re} = \bigcup_{n=1}^{\infty} \Re^n$ si chiama *chiusura transitiva* della relazione $\Re$. Si ha infatti:

PROPOSIZIONE 1.6. Sia data una relazione $\Re$ in un insieme X e sia $\overline{\Re}$ la chiusura transitiva di $\Re$.

a) $\overline{\Re}$ è transitiva.

b) $\overline{\Re}$ è inclusa in ogni relazione transitiva contenente $\Re$.

c) Se $\Re$ è simmetrica, la relazione $\sim_{\Re} = id_X \cup \overline{\Re} = \bigcup_{n=0}^{\infty} \Re^n$ è una relazione d'equivalenza.

Dimostrazione. a) Siano a, b, c∈X, tali che $a \overline{\Re} b$ e $b \overline{\Re} c$. Esistono m, n tali che $a \Re^m b$ e $b \Re^n c$, quindi $a \Re^{m+n} c$. Ne segue $a \overline{\Re} c$, cioè $\overline{\Re}$ è transitiva.

b) Sia $\Im$ una relazione transitiva tale che $\Re \subseteq \Im$. Allora $\Re^2 \subseteq \Im^2 \subseteq \Im$ e, per induzione su n, per ogni $n \geq 1$ si ha $\Re^n \subseteq \Im^n \subseteq \Im$. Pertanto, $\overline{\Re} \subseteq \Im$.

c) Se $\Re$ è simmetrica, anche ogni sua potenza lo è ed anche $\overline{\Re}$ di conseguenza lo è. Dato che anche l'identità è simmetrica, ne segue che $\sim_{\Re}$ è simmetrica, oltre che contenere l'identità ed essere transitiva.

Molte relazioni d'equivalenza sono in effetti costruite come chiusura transitiva di una relazione simmetrica in unione con l'identità.

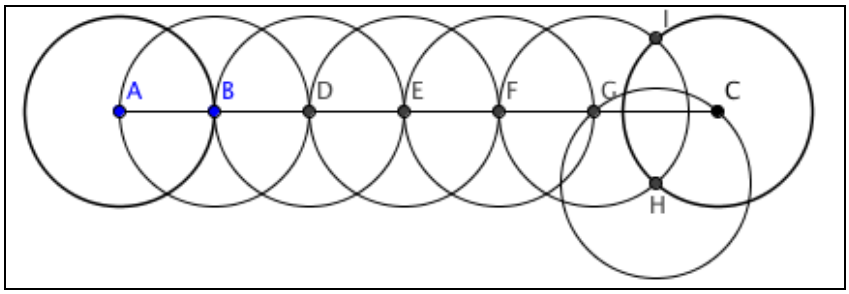
ESEMPI 1.7. 1) Un esempio curioso, anche se un po' nebuloso nella formulazione: diciamo *conoscenti* due esseri umani se hanno avuto almeno una occasione di incontrarsi, parlarsi stringersi la mano, presentarsi. Questa relazione $\Re$ è simmetrica. La sua chiusura transitiva suddivide la popolazione umana in classi d'equivalenza tali che, date due persone della stessa

classe, esiste una catena finita di conoscenze che li collega. Il problema è: quante sono le classi? La risposta è sorprendente: sembra proprio che sia una sola!

2) La relazione di perpendicolarità $\perp$ nell'insieme delle rette del piano è simmetrica. La sua chiusura transitiva, unita all'identità, è una relazione d'equivalenza. Che cosa c'è nella classe di una retta r? Innanzi tutto ci sono tutte le rette perpendicolari ad r. Poi, le rette perpendicolari alle perpendicolari ad r. Ma queste ultime sono parallele ad r, quindi $\perp \circ \perp = \parallel$, ossia il parallelismo è il quadrato della perpendicolarità. Però, una retta perpendicolare ad una parallela ad r è a sua volta perpendicolare ad r, quindi $\perp \circ \perp \circ \perp = \perp$. Pertanto, la relazione d'equivalenza generata dalla perpendicolarità è unione del parallelismo e della perpendicolarità, e nella classe di r ci sono il fascio di parallele ad r e il fascio di perpendicolari ad r.

3) Nell'insieme delle circonferenze del piano diciamo che due circonferenze sono in relazione se ciascuna contiene il centro dell'altra. In tal caso, hanno raggi congruenti. La relazione è simmetrica, quindi la sua chiusura transitiva unita all'identità è una relazione d'equivalenza. Nella classe d'equivalenza di una data circonferenza ci sono solo circonferenze con lo stesso raggio. Ma ci sono tutte?

Sia A il centro della circonferenza γ e sia C il centro di una circonferenza δ con lo stesso raggio. Consideriamo la semiretta AC, di origine A e sia B il punto in cui essa interseca γ, per cui il raggio è AB. Allora per la proprietà di Archimede dell'ordinamento dei segmenti, esiste un multiplo nAB ≥ AC. Se nAB = AC allora, posto C_k il punto della semiretta tale che $kAB = AC_k$, con $0 \le k \le n$, le circonferenze di centri nei punti C_k e raggio AB sono tali che ciascuna contiene il centro della precedente e della successiva, quindi quella di raggio $G = C_{n-1}$ passa per C e appartiene a δ.



Se invece (n-1)AB < AC < nAB, allora la circonferenza di centro $G = C_{n-1}$ interseca δ in due punti H ed I. La circonferenza di centro H e raggio AB passa per G, ma anche per C. In ogni caso, quindi δ appartiene alla classe di γ.

SCHEDA G2. Insiemi ordinati.

Siano X un insieme (non vuoto) ed $\Re$ una relazione in X. Diremo che $\Re$ è una relazione d'ordine se è *riflessiva, antisimmetrica e transitiva*, ossia, usando le nozioni introdotte nella scheda precedente, se

I. Per ogni $id_X \subseteq \Re$

II. $\Re \cap \Re^t \subseteq id_X$

III. $\Re^2 \subseteq \Re$.

La coppia (X, $\Re$) si dice *insieme ordinato* o *poset*. Due elementi di X si dicono *confrontabili* se si ha $x\Re y$ oppure $y\Re x$. Li diremo *inconfrontabili* in caso contrario.
In una relazione d'ordine la proprietà antisimmetrica assicura che se due elementi distinti sono confrontabili, lo sono in un unico modo.

Diremo che $\Re$ è un ordine *totale* se $\Re \cup \Re^t = X \times X$, ossia se tutti gli elementi sono a due a due confrontabili. Altrimenti, è un ordine *parziale*.
Come noto, gli ordinamenti naturali di **N, Z , Q , R** sono totali, e così pure è totale l'ordine alfabetico (o *lessicografico*) fra le parole della lingua italiana.
Esempi di ordini non totali, in cui esistono coppie di elementi inconfrontabili, sono l'*inclusione* nell'insieme delle parti di un insieme con almeno due elementi, o la relazione | ("è divisore di") in **N**.

Usualmente, per le relazioni d'ordine si usa il simbolo $\leq$. La relazione $<$, detta *ordine stretto*, si definisce ponendo:

$$x < y \text{ se } x \leq y \text{ e } x \neq y.$$

La relazione trasposta di $\leq$ è a sua volta una relazione d'ordine, viene denotata con $\geq$ e viene detta *ordine duale.*

Sia (X, $\leq$) un poset e sia $<$ l'ordine stretto associato. La relazione $<$ è transitiva e disgiunta dall'identità e dalla sua trasposta.
Inversamente, data una *struttura relazionale* (X, $\Re$) con $\Re$ transitiva, disgiunta dall'identità e dalla sua trasposta $\Re^t$, posto

$$x \leq y \text{ se } x = y \text{ oppure } x \Re y$$

allora $\leq$ è un ordine in X, di cui $\Re$ è l'ordine stretto associato.

Sia $(X, \leq)$ un poset e siano $x, y \in X$, $x < y$. Una *catena* è un sottoinsieme di X totalmente ordinato. Una catena finita necessariamente ha due *estremi* x ed y:

$$x = x_0 < x_1 < \ldots < x_r = y$$

Il numero r si chiama *lunghezza* della catena. Se le catene di X sono tutte finite e di lunghezza non superiore ad un dato numero $m \in \mathbf{N}$, la massima lunghezza delle catene di X è detta *lunghezza* di $(X, \leq)$. Se un tal numero m non esiste, si dice che $(X, \leq)$ ha lunghezza infinita.

Al contrario, una *anticatena* è un sottoinsieme di elementi a due a due inconfrontabili. Se esiste $n \in \mathbf{N}$ tale che ogni anticatena abbia al più n elementi, il numero massimo di elementi delle anticatene è detto *numero di Dilworth* del poset.
Chiaramente, un ordine è totale se e solo se tutte le anticatene hanno un solo elemento ciascuna, cioè se il numero di Dilworth del poset è 1.

Gli ordinamenti naturali degli insiemi numerici **Z, Q, R** sono ordini totali, ma presentano comunque delle differenze importanti. A titolo di ripasso, ricordiamo alcune di queste. Sia $(X, \leq)$ un insieme ordinato. L'ordine si dice *denso* se per ogni $x, y \in X$, con $x < y$, esiste $z \in X$ tale che $x < z < y$. Come noto dai corsi di Algebra e di Analisi Matematica, gli ordinamenti di **Q** e di **R** hanno questa proprietà, mentre quello di **Z** non ce l'ha. In ogni caso, è immediato verificare che se l'ordine è denso, allora X è infinito.

Sia $(X, \leq)$ un insieme ordinato. Siano poi $x, y \in X$ con $x < y$. L'insieme:

$$[x, y] = \{z \in X \mid x \leq z \leq y\}$$

è detto *intervallo chiuso di estremi x ed y*. L'ordine si dice *localmente finito* se per ogni $x, y \in X$ con $x < y$, l'intervallo $[x, y]$ è finito. Si dice *discreto* se per ogni $x, y \in X$ con $x < y$, l'intervallo $[x, y]$ ha lunghezza finita. Un ordine localmente finito è discreto, ma non viceversa(1). I poset finiti hanno queste proprietà, ma anche $(\mathbf{Z}, \leq)$ ce le ha, pur essendo infinito, mentre un ordine denso non è localmente finito né discreto.

Sia $(X, \leq)$ un insieme ordinato e siano $x, y \in X$, $x < y$. Si dice che x *è coperto da* y (e si scrive $x \prec y$) se l'intervallo $[x, y]$ contiene solo x ed y, quindi se non esiste alcun altro

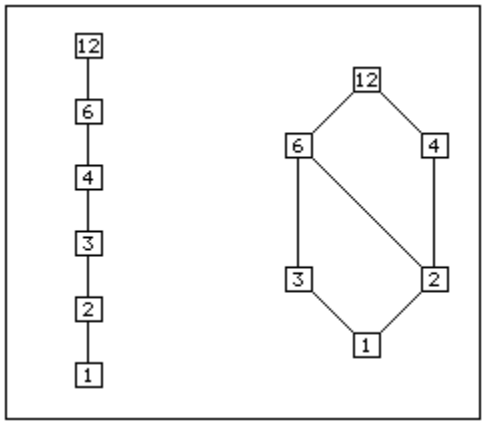
(1) Un esempio è l'insieme dei sottospazi vettoriali di R^n, $n \geq 2$, ordinato mediante l'inclusione. L'ordine è discreto, perché la lunghezza massima delle catene è n, ma non localmente finito, perché per esempio tra $\{0\}$ e un sottospazio di dimensione 2 ci sono infiniti sottospazi di dimensione 1.

$z \in X$ tale che $x < z < y$. La relazione $\prec$ così definita viene detta *relazione di copertura* associata all'ordine dato. Chiaramente, se l'ordine è denso, tale relazione è vuota. Si ha:

PROPOSIZIONE 2.1. Sia $(X, \leq)$ un insieme ordinato discreto. Allora la relazione di ordine stretto associata $<$ è la chiusura transitiva $\overline{\prec}$ della relazione di copertura $\prec$.

Dimostrazione. Siano $x, y \in X$ tali che $x < y$. Poiché l'ordine è discreto, le catene che li congiungono hanno lunghezza finita non superiore ad un certo k. Esiste pertanto una catena $x_0 = x < x_1 < \ldots < x_m = y$ di lunghezza massima $m \leq k$. Chiaramente, per ogni $i = 0, 1, \ldots, m-1$, fra x_i ed x_{i+1} non si possono inserire altri elementi di X, perché la catena si allungherebbe. Ne segue che ogni x_i è coperto da x_{i+1} e dunque per ogni i si ha $x \prec^i x_i$. Ma allora si ha $x \prec^m y$, e ciò prova che se $x < y$ allora $x \overline{\prec} y$. Essendo però $<$ transitiva, vale anche l'implicazione inversa e quindi l'uguaglianza di $<$ e $\overline{\prec}$.

Sia $(X, \leq)$ un insieme ordinato finito. L'ordine si rappresenta graficamente mediante il *diagramma di Hasse*, nel quale ogni elemento è rappresentato da un punto contrassegnato col nome dell'elemento; se $a < b$ allora a è più in basso di b e se $a \prec b$ un segmento li congiunge.



Nella figura qui accanto sono mostrati i diagrammi di Hasse dell'insieme dei divisori di 12 ordinato rispettivamente con l'ordine naturale di **N** e con l'ordine parziale $m|n \Leftrightarrow \exists q \in \mathbf{N},\ n = mq$. Si evidenziano così le varie proprietà dei due insiemi ordinati.

Dato un poset $(X, \leq)$ ed un suo sottoinsieme non vuoto A, si chiama *minimo* di A un elemento $a_0 \in A$ tale che per ogni $a \in A$ si abbia $a_0 \leq a$. Chiaramente, se esiste è unico, per la proprietà di antisimmetria della relazione d'ordine, e viene denotato con *min(A)*. Analogamente, si chiama *massimo* di A un elemento $a_1 \in A$ tale che per ogni $a \in A$ si abbia $a \leq a_1$. Anche il massimo, se esiste, è unico e viene denotato con *max(A)*.

Se il poset $(X, \leq)$ possiede il minimo, questo viene denotato con 0_X (o con 0, se non ci sono ambiguità). L'eventuale massimo viene denotato con 1_X (o con 1).

Completezza. Un elemento $b \in X$ si dice *maggiorante* (o *confine superiore*) di A se per ogni $a \in A$ si ha $a \leq b$. Se l'insieme dei maggioranti di A è vuoto, A si dice *superiormente illimitato*; se non è vuoto, A si dice *superiormente limitato;* se non è vuoto ed ha minimo, questo si chiama *estremo superiore* (o *supremo*) di A e viene denotato con *sup(A)*.

Analogamente, un elemento $c \in X$ si dice *minorante* (o *confine inferiore*) di A se per ogni $a \in A$ si ha $c \leq a$. Se l'insieme dei minoranti non è vuoto ed ha massimo, questo si chiama *estremo inferiore* (o *infimo*) di A e viene denotato con *inf(A)*.

Se $\inf(A) \in A$ oppure se esiste $\min(A)$ allora si ha $\inf(A) = \min(A)$. Analoga situazione si ha per $\sup(A)$ e $\max(A)$.

L'insieme ordinato $(X, \leq)$ si dice *completo* se ogni sottoinsieme non vuoto che possieda maggioranti ha anche l'estremo superiore.

Esercizio 2.2. Sia $(X, \leq)$ un insieme ordinato. Si provi che è completo se e solo se ogni sottoinsieme non vuoto che possieda minoranti ha anche l'estremo inferiore.

Esercizio 2.3. Sia dato un poset $(X, \leq)$ con il minimo 0_X ed il massimo 1_X.
a) Si provi che è localmente finito se e solo se è finito.
b) Si provi che è completo se e solo se ogni sottoinsieme non vuoto ha l'estremo superiore.

Dai corsi di Algebra e di Analisi è noto che $(\mathbf{R}, \leq)$ e $(\mathbf{Z}, \leq)$ sono completi, mentre $(\mathbf{Q}, \leq)$ non lo è, perché il sottoinsieme $A = \{x \in \mathbf{Q} \mid x \geq 1, x^2 \leq 2\}$ non possiede l'estremo superiore in $(\mathbf{Q}, \leq)$. E' poi facile provare che per ogni insieme X, $(\wp(X), \subseteq)$ è completo, perché l'estremo superiore di ogni famiglia di sottoinsiemi di X è la sua unione.

Un poset $(X, \leq)$ si chiama *reticolo* se per ogni coppia $\{x, y\}$ di suoi elementi esistono $\sup\{x, y\}$ ed $\inf\{x, y\}$. Ne segue che ogni sottoinsieme finito ha sup ed inf.
Per esempio, $\left(\wp(X), \subseteq\right)$ è un reticolo, ma anche ogni insieme totalmente ordinato ed ogni insieme ordinato completo dotato di massimo e minimo sono reticoli.

Sia $(X, \leq)$ un insieme ordinato. Un elemento $m \in X$ si dice *massimale* se per ogni $x \in X$, se $m \leq x$ allora $x = m$. Chiaramente, se X ha massimo allora questo è l'unico elemento massimale, ma in generale gli elementi massimali non è detto che esistano né

che ce ne sia uno solo. Se un insieme ordinato è finito, ovviamente ha elementi massimali, ma per esempio, (**Z**, ≤) non ne ha. L'insieme degli interi compresi fra 1 e 10, ordinato mediante la divisibilità, ha come elementi massimali 6, 7, 8, 9, 10. La seguente proposizione stabilisce una ben nota condizione sufficiente per l'esistenza di elementi massimali:

PROPOSIZIONE 2.4. ("Assioma" o Lemma di Kuratowski-Zorn). Sia (X, ≤) un insieme ordinato. Se ogni catena non vuota di X è limitata superiormente, allora in X esistono elementi massimali.

E' noto il problema relativo al Lemma di Zorn: è indipendente dagli assiomi base della Teoria degli Insiemi, ma è equivalente ad altre proposizioni quali l'*assioma di Zermelo* (o *assioma di scelta*), il quale asserisce la possibilità, data una comunque grande famiglia di insiemi non vuoti $\Im$, di definire una *funzione* $f : \Im \to \bigcup_{A\in\Im} A$ tale che per ogni $A \in \Im$ si abbia f(A)∈A. In particolare, esso dà la possibilità di scegliere un rappresentante da ogni classe di equivalenza ~ in un insieme X.

Una ulteriore proposizione equivalente al Lemma di Zorn ed all'assioma di scelta è *l'assioma del buon ordinamento*. Un insieme ordinato (X, ≤) si dice *bene ordinato* se ogni suo sottoinsieme non vuoto possiede il minimo. E' ben noto che (**N**, ≤) ha questa proprietà (*principio del minimo*). Si ha la ben poco intuitiva proprietà:

PROPOSIZIONE 2.5. ("Assioma" del buon ordinamento). In ogni insieme non vuoto X è possibile definire una relazione d'ordine ≤ in modo che (X, ≤) sia bene ordinato.

NOTA. Dall'assioma del buon ordinamento si ricava facilmente l'assioma di scelta: data la famiglia di insiemi non vuoti $\Im$, definiamo in $X = \bigcup_{A\in\Im} A$ un buon ordine. Allora anche ogni sottoinsieme A ha il minimo. Allora definiamo la funzione $f : \Im \to \bigcup_{A\in\Im} A$ tale che $A \mapsto \min(A)$ e questa è una ben definita funzione di scelta. Il viceversa non è così banale.

Le catene in (X, ≤) si possono ordinare nel modo seguente: date due catene Σ e Σ', diremo che Σ' è *più fine* di Σ se ogni termine di Σ lo è anche di Σ'. Sostanzialmente,

questo ordinamento coincide con l'inclusione in $\wp(\wp(X))$. Ha senso quindi parlare di catene massimali, cioè che non possono essere *raffinate*. Anche la seguente proposizione è equivalente all'assioma di scelta:

PROPOSIZIONE 2.6. ("Assioma" delle catene o di Hausdorff-Birchkoff) Ogni catena di un poset $(X, \leq)$ è inclusa in almeno una catena massimale.

Sia $(X, \leq)$ un poset. Una *catena ascendente* di origine $x_0 \in X$ è una successione:

$$x_0 \leq x_1 \leq x_2 \leq \ldots \leq x_n \leq \ldots$$

di elementi di X. Diremo che è *finita* se esiste $n \in \mathbf{N}$ tale che per ogni $k > n$ si ha $x_k = x_n$. Diremo che $(X, \leq)$ soddisfa la *condizione sulle catene ascendenti (a.c.c.)* se ogni catena ascendente è finita. Analogamente si definiscono le catene discendenti e la condizione sulle catene discendenti (d.c.c).

Queste condizioni sono importanti in vari settori dell'Algebra. Per esempio, consideriamo un dominio d'integrità A ed ordiniamo i suoi ideali bilateri mediante l'inclusione. Otteniamo un poset $(\mathscr{I}(A), \subseteq)$ con minimo $\{0_A\}$ e massimo A. L'anello A si dice *nœtheriano* se il poset $(\mathscr{I}(A), \subseteq)$ soddisfa (a.c.c), *artiniano* se soddisfa (d.c.c). La prima situazione è equivalente al fatto che ogni ideale abbia un numero finito di generatori, e si verifica per esempio se A ha gli ideali principali. Un celebre teorema di Hilbert afferma che se A è nœtheriano anche l'anello dei polinomi A[x] lo è. Queste nozioni sono alla base della Geometria Algebrica.

Esercizio 2.6. Si provi che se un poset $(X, \leq)$ soddisfa la condizione sulle catene ascendenti (a.c.c), ogni $x \in X$ è contenuto in un elemento massimale.

Esercizio 2.7. Si provi che il poset $(\mathbf{N}, |)$ soddisfa la (d.c.c) ma non la (a.c.c).

Dati due insiemi ordinati $(X, \leq)$ ed $(Y, \subseteq)$, un *omomorfismo d'ordine* (o funzione monotona non decrescente) è un'applicazione $f:X \to Y$ tale che:

$$x \leq x' \Rightarrow f(x) \subseteq f(x')$$

Un *antiomomorfismo d'ordine* (o funzione monotona non crescente) è invece tale che $x \leq x' \Leftrightarrow f(x) \geq f(x')$. Si possono anche definire le funzioni strettamente monotone (crescenti o decrescenti), che conservano (o rispettivamente invertono) l'ordine stretto nei due poset. L'interesse per queste funzioni si ha principalmente nell'Analisi Matematica reale, dove le funzioni monotone $f:A(\subseteq \mathbf{R}) \to \mathbf{R}$ sono oggetto di studio per le loro proprietà quali l'integrabilità sugli intervalli chiusi e limitati. Inoltre, la

monotonicità è legata al segno della derivata prima. In campo algebrico sono naturalmente più interessanti gli *isomorfismi*.

Un *isomorfismo d'ordine* tra due insiemi ordinati $(X, \leq)$ ed $(Y, \subseteq)$ è una biiezione $f:X \to Y$, tale che per ogni $x, x' \in X$ si ha:

$$x \leq x' \Leftrightarrow f(x) \subseteq f(x')$$

Si possono definire anche gli *antiisomorfismi d'ordine*, come gli isomorfismi d'ordine tra $(X, \leq)$ ed $(Y, \subseteq)$. Per esempio, considerando i due insiemi ordinati $(\mathbf{R}, \leq)$ e $(\mathbf{R}^+, \leq)$, per ogni $a \in R$, $a > 1$ funzione $x \to a^x$ è un isomorfismo d'ordine, mentre se $0 < a < 1$ la funzione $x \to a^x$ è un antiisomorfismo d'ordine.

Due insiemi ordinati isomorfi hanno ovviamente le stesse proprietà: se uno è denso, localmente finito, completo, reticolo, ecc. lo è anche l'altro e viceversa. Inoltre, nel caso finito, i due ordini si possono rappresentare con la stessa matrice d'incidenza e con lo stesso diagramma di Hasse, e viceversa.

Per esempio, due insiemi totalmente ordinati finiti con lo stesso numero di elementi sono isomorfi (ed anche antiisomorfi). Non è vero per gli insiemi infiniti: $(\mathbf{Z}, \leq)$ e $(\mathbf{Q}, \leq)$ sono entrambi totalmente ordinati e numerabili, ma il primo è localmente finito ed il secondo è denso.

Un poset $(X, \leq)$ che sia isomorfo al suo duale $(X, \geq)$ è detto *autoduale.* Per esempio, per ogni insieme X, $(\wp(X), \subseteq)$ è autoduale: basta far corrispondere ad ogni $A \in \wp(X)$ il suo complementare $A' = X \setminus A$. Anche ogni insieme totalmente ordinato finito è autoduale. Non è vero nel caso infinito: $(\mathbf{N}, \leq)$ ha minimo, 0, mentre $(\mathbf{N}, \geq)$ non ce l'ha (ossia, non esiste un elemento $u \in \mathbf{N}$ tale che $u \geq n$ per ogni $n \in \mathbf{N}$.)

Poiché la trasposta $\geq$ di una relazione d'ordine $\leq$ è ancora una relazione d'ordine, è possibile formulare il cosiddetto *principio di dualità dei poset*. Sia dato un enunciato P sui poset: il suo *duale* P^t è ottenuto scambiando dappertutto il simbolo $\leq$ col simbolo trasposto $\geq$. In tal modo, per esempio, si scambiano fra loro le nozioni di maggiorante e minorante, massimo e minimo, sup ed inf, catena ascendente e catena discendente. Tale procedimento è detto *dualizzazione* dell'enunciato P.
Si osservi che la nozione duale di intervallo $[x, y]$ non cambia l'insieme:

$$[x, y] = \{z \in X \mid x \leq z \leq y\} = \{z \in X \mid y \geq z \geq x\} = [y, x]^t.$$

PROPOSIZIONE 2.8 (Principio di dualità per i poset). Se un enunciato P della teoria dei poset è vero, allora è vero anche il suo duale P^t, e la dimostrazione di P^t si ottiene da quella di P per dualizzazione.

Per finire osserviamo che dati due poset, esistono vari modi per fabbricarne altri. Per esempio, si ha:

Esercizio 2.9. Dati due insiemi ordinati $(X, \preceq)$ ed $(Y, \subseteq)$, nell'insieme $X \times Y$ si ponga:

$$(x, y)\ \Re\ (x', y') \text{ se } x \preceq x' \text{ e } y \subseteq y'.$$

Si provi che $(X \times Y, \Re)$ è un insieme ordinato (*prodotto diretto* dei due poset dati), ma non totalmente.

Esercizio 2.10. Dati due insiemi ordinati $(X, \preceq)$ ed $(Y, \subseteq)$, nell'insieme $X \times Y$ si ponga:

$$(x, y)\ \Re\ (x', y') \text{ se } x \preceq x' \text{ oppure se } x = y \text{ e } y \subseteq y'.$$

Si provi che $(X \times Y, \Re)$ è un insieme totalmente ordinato (ordine *lessicografico*).

Completezza e continuità. Abbiamo visto la nozione di ordine completo: ogni sottoinsieme non vuoto, che possieda dei maggioranti, ha l'estremo superiore.
Se l'ordine è totale, una nozione equivalente è la seguente, detta *continuità secondo Dedekind*. Sia $(X, \leq)$ un insieme totalmente ordinato e siano A e B due sottoinsiemi non vuoti. Si dicono *separati* se per ogni $a \in A$, $b \in B$ si ha $a \leq b$.
L'ordine si dice *continuo* se per ogni coppia di sottoinsiemi separati esiste almeno un elemento separatore x, tale che per ogni $a \in A$, $b \in B$, si ha $a \leq x \leq b$.

Completezza e continuità per gli ordini totali sono la stessa proprietà. Infatti, se l'ordine è completo, ed A e B sono separati, B è un insieme di maggioranti per A, quindi esiste sup(A) ed è un elemento separatore tra A e B.
Viceversa, se l'ordine è continuo, preso un sottoinsieme non vuoto A che abbia maggioranti, detto B l'insieme dei maggioranti, A e B sono separati, ovviamente, e quindi fra di essi esiste un elemento separatore x; quest'ultimo è un maggiorante di A, quindi appartiene a B, ma è il minimo di B, perché se ci fosse un altro elemento di B minore di x, x non sarebbe elemento separatore di A e B. Dunque, $x = \sup(A)$.

In un ordine completo (= continuo) due sottoinsiemi separati A e B si dicono *contigui* se sup(A) = inf (B). In tal caso, c'è un solo elemento separatore, appunto sup(A).

Ordine e operazioni. Talora in un insieme X facciamo convivere una operazione binaria associativa + ed una relazione d'ordine totale ≤.
Sono *compatibili* se per ogni a, b, c si ha $a \le b \Rightarrow a+c \le b+c$.
Ne segue che per ogni a, a', b, b', $\begin{cases} a \le a' \\ b \le b' \end{cases} \Rightarrow a+b \le a'+b'$.
Se c'è anche l'elemento neutro 0_X (e quindi siamo in un monoide), chiamiamo *positivi* gli elementi maggiori di 0_X, *negativi* gli altri.
Se a è positivo ed ha l'opposto –a, allora

$$0_X < a \Rightarrow -a = -a + 0_X < -a + a = 0_X \Rightarrow \text{-a negativo}$$

e viceversa. Ossia, tra a e –a uno ed uno solo è positivo.
Inoltre, la somma di positivi è positiva.

Chiamiamo *monoide ordinato* un monoide M (in notazione additiva) con una relazione d'ordine compatibile con l'addizione.

L'addizione associativa consente di definire i multipli interi $na = \underbrace{a + a + \ldots + a}_{n}$ di un elemento a.

Se a è positivo, i suoi multipli sono tutti positivi e, al crescere del numero n, anche na cresce: $0 < a < 2a < 3a < \ldots < na < (n+1)a < \ldots$ Pertanto, un monoide ordinato è infinito.

Se a è negativo la successione dei multipli è decrescente: $a > 2a > 3a > \ldots$
I multipli di 0_X sono tutti nulli.

L'ordinamento nel monoide si dice *archimedeo* se per ogni coppia di elementi positivi a e b esiste un multiplo di a maggiore di b.

Gli ordini negli insiemi numerici e nei segmenti sono tutti archimedei. La proprietà che segue e la relativa dimostrazione riproducono quella vista nel corso per i segmenti.

Proposizione 2.9. Sia dato un monoide totalmente ordinato completo M.

a) M è archimedeo
b) Se M è anche denso, due insiemi separati A e B tali che, per ogni $\varepsilon \in M$ positivo, esistono $a \in A$, $b \in B$ tali che $b - a < \varepsilon$, sono contigui.
c) Se M è anche denso, per ogni $a \in M$ positivo e per ogni numero intero positivo n esiste $b \in M$, positivo, tale che $nb = a$.

Dimostrazione. a) Siano a e b elementi positivi di M. Sia $a < b$. L'insieme dei multipli di a non è vuoto, perché contiene a. Se per assurdo nessun multiplo na è maggiore di b, allora b è un maggiorante dell'insieme dei multipli di a, quindi quest'ultimo ha l'estremo superiore, sia s. Certamente, $s > a$, perché $0_M < a \Rightarrow a = 0_M + a < a + a = 2a$. Allora, $s > s - a > 0_M$, quindi esiste un multiplo na di a, maggiore di s-a. Ne segue $(n+1)a = na + a > (s - a) + a = s$, quindi s non è l'estremo superiore dei multipli di a, assurdo. Dunque, b non è maggiore di tutti i multipli di a e M è archimedeo.

b) La completezza assicura l'esistenza di sup(A) e inf(B). Se $\inf(B) - \sup(A) > 0_M$ la densità assicura la possibilità di trovare un elemento $\varepsilon \in M$ tale che $0_M < \varepsilon < \inf(B) - \sup(A)$. Presi allora due elementi $a \in A$, $b \in B$ tali che $b - a < \varepsilon$, si ha:

$$\varepsilon < \inf(B) - \sup(A) \leq b - a < \varepsilon,$$

e questo è assurdo. Allora, $\inf(B) = \sup(A)$ e i due insiemi sono contigui.

c) Si dimostra come per i segmenti. Si invitano gli allievi a tradurre quella dimostrazione in termini astratti.

NOTA. Di campi ordinati si parlerà nel modulo di Elementi di Algebra.