Cap. 1 - Introduzione: l'Algebra e la sua didattica

Che cos'è l'algebra?

Mi pare indubbio che gli scopi dell'Algebra siano *generalizzare* ed *unificare*, ossia fornire algoritmi, formule di calcolo e concetti di carattere generale, applicabili in svariate circostanze, riconoscendo quello che c'è di simile in situazioni diverse.

Essa si presenta inizialmente come un superamento del calcolo aritmetico elementare, nel quale si eseguono operazioni solo su numeri particolari; al contrario, attraverso il *calcolo letterale*, essa insegna a manipolare dei simboli, le lettere, che potranno assumere poi valori numerici o anche di altro tipo, mantenendo pressoché intatta la validità delle identità ricavate in astratto.

Essa ci aiuta poi a formulare le *equazioni* ed a risolverle in molti casi usando i metodi del calcolo letterale e fornendo così uno strumento potente per costruire modelli matematici di fenomeni reali.

Infine, a seguito proprio dello studio della risolubilità delle equazioni, si passa in epoca contemporanea all'introduzione delle *strutture algebriche*, costituite da un insieme e da una o più operazioni, che portano all'unificazione in schemi astratti di una lista di casi particolari, di cui sono messi in luce i tratti essenziali rispetto a quelli accessori. Si viene allora a precisare l'ambito di validità delle identità del calcolo letterale, ossia dell'algebra classica, e si introducono nuove situazioni in cui alcune di queste identità perdono di significato, mentre ne nascono altre (algebre non commutative, di Boole, di Lie, ...).

Qual è il ruolo delle lettere? Variabili o indeterminate?

Le lettere nella matematica scolastica entrano di norma come abbreviazioni, come iniziali di parole note, talora con significato univoco (75 centimetri diventa 75 cm), talora con significato locale ("Area = base per altezza" diventa A = b×h), talora con distinzioni tra maiuscole e minuscole. Esse hanno però sempre un significato "concreto", anche se nel secondo esempio si è già passati ad una identità valida per tutti i rettangoli e non solo per il rettangolo di base 7 metri ed altezza 5 metri.

Si comincia ad intravedere la differenza tra lettere, o gruppi di lettere, con significato fisso in un determinato contesto, ossia le *costanti*, e quelle che non ce l'hanno, le *variabili*.

Esempi del primo tipo sono, in Fisica, la *h* di Plank, la *c* della velocità della luce o, in Geometria, il numero π di Archimede o il numero *e* di Nepero.

Tuttavia, cambiando contesto anche di poco, una costante può tornare ad essere variabile: per esempio, in Geometria dello spazio π denota spesso un piano generico; in Algebra talora *e* denota l'elemento neutro di un gruppo astratto; in Fisica *m* può denotare la massa di un corpo.

Nel calcolo letterale, una volta introdotto, le lettere possono assumere come minimo due significati diversi: *variabili* o *indeterminate*.

Le **variabili** sono elementi non specificati di un determinato insieme, quasi sempre numerico, per esempio l'insieme dei numeri reali, e sono sottoposte a tutte le leggi valide per le operazioni in questo insieme. Avremo così che "espressioni" del tipo a^2, $5a-2b+1$, $\frac{b-1}{a\cdot b}$ hanno un significato univoco: dati i numeri a, b, si eseguono le operazioni indicate, ossia la potenza, i prodotti, le somme e differenze, il quoziente. Naturalmente, quest'ultimo sarà eseguibile solo se il divisore, ossia il denominatore, è diverso da zero, ossia $a\cdot b\neq 0$; la proprietà della moltiplicazione nei numeri reali detta "legge d'annullamento del prodotto" dice che ciò accade se e solo se $\begin{cases} a\neq 0 \\ b\neq 0 \end{cases}$.

Inoltre, le identità $a+b=b+a$, $a^2-b^2=(a+b)\cdot(a-b)$ ecc. sono *teoremi*, conseguenza delle proprietà delle operazioni sui numeri reali. Osserviamo infine che dietro questa impostazione si nasconde il concetto di *funzione* di una o più variabili reali, con il suo apparato di difficoltà e con il suo grafico: le espressioni sono cioè delle funzioni, che ad ogni valore attribuito alle lettere, preso da un opportuno dominio, restituiscono uno ed un solo numero reale. Nascono allora anche problemi di unicità della rappresentazione algebrica, per esempio di una funzione polinomiale, ossia occorre un teorema di identità dei polinomi.

Le **indeterminate** invece sono puri simboli, estranei all'ambiente dei numeri, e per poterle manipolare occorre adottare regole di formazione, postulare alcune identità e ricavarne altre come conseguenza.

Per esempio, vogliamo estendere l'insieme dei numeri reali aggiungendovi l'oggetto *a*. Notiamo che al suo posto potremmo usare una tacca o uno stuzzicadenti o

un bottone: sarebbe allora più evidente che tutto quel che possiamo fare è riprodurlo e formare delle file: a aa aaa … aa⋯a, di lunghezza grande a piacere.

Per farci altre cose dobbiamo introdurre delle convenzioni, per esempio porre $a^4 = aaaa$; dire che espressioni del tipo $3a^2$ oppure $7 + \frac{3}{4}a - a^3 + 2a^7$ (i *polinomi*) sono lecite; postulare o no che si abbia $3a = a3$, che si possano eseguire operazioni di addizione, sottrazione e moltiplicazione e che queste abbiano proprietà come le omonime operazioni sui numeri reali.

A questo punto, la scelta delle regole di formazione e degli assiomi da imporre diviene largamente arbitraria. Per esempio, se imponessimo l'assioma $a^2 = -1$, che cosa otterremmo? Otterremmo che le espressioni lecite si riducono alla forma $x + a \cdot y$, dove qui *x* ed *y* sono variabili ed *a* è l'indeterminata, sottoposta a quello strano assioma (se al posto di *a* mettiamo *i*, il tutto ha un aspetto assai più familiare, no?).

Ma supponiamo pure di non imporre all'indeterminata proprietà diverse da quelle naturali. Per dare significato ad una scrittura del tipo $7 + \frac{3}{4}a - a^3 + 2a^7 \left(= 7 + \frac{3}{4}a - aaa + 2aaaaaaa \right)$, ossia ad un *polinomio*, dovremmo immaginare che essa sia una parola scritta in un alfabeto comprendente: i numeri reali rappresentati in qualche modo, per esempio mediante variabili; i segni + e -; la lettera a. L'insieme di queste parole va poi strutturato definendovi convenzioni, operazioni e postulandone le proprietà (guidati nella scelta di queste ultime dal modello funzionale, che però per tradizione vorremmo evitare).

Si ha allora che i segni + e – assumono ciascuno vari significati: sono elementi dell'alfabeto e simboli non solo di operazioni tra i numeri reali, ma anche delle nuove operazioni nell'insieme di queste parole che abbiamo chiamato polinomi.

Per il segno -, inoltre, c'è almeno anche il significato di *operatore unario* che fa passare da un elemento all'opposto. Occorrerà giustificare l'uso dello stesso simbolo per indicare cose in partenza abbastanza diverse.

Credo che quanto precede illustri abbastanza bene la complessità e le complicazioni intrinseche del calcolo letterale, ossia metta in evidenza le difficoltà e le misconcezioni che spesso troviamo negli allievi dei primi anni. Certo, nessun insegnante si sognerebbe di imporre esplicitamente agli allievi questi ragionamenti, perché nessuno forse capirebbe. Allora, la scelta è quasi sempre di non parlarne

affatto, mischiare ben bene i vari approcci, sperare che gli allievi imparino per imitazione a fare i calcoli, e dare del somaro ad un allievo in difficoltà. È giusto?

Qual è il ruolo delle lettere nelle equazioni: incognite o parametri?

L'idea di equazione si può presentare in vari modi, e per questo basta scorrere i libri di testo. Una possibile presentazione è la seguente, che la trasforma in un problema: date due funzioni f, g con lo stesso dominio A e lo stesso codominio B, trovare per quali $x \in A$ si ha $f(x) = g(x)$.

In questo caso, la variabile x prende il nome di *incognita*, ossia di lettera della quale si vorrebbe determinare il o i "valori" possibili, secondo la richiesta del problema stesso.

Seguono poi metodi risolutivi, di tipo esatto o approssimato a seconda dell'uso e del contesto, sovente ricondotti a formule da imparare a memoria. Fin qui tutto bene. Il guaio è che, nelle applicazioni:

a) si ha a che fare in genere con funzioni di più variabili;
b) le variabili sono denotate da lettere talora diverse dalla canonica x derivante dalla tradizione scolastica;
c) non è chiaro quindi che cosa sia "la soluzione" di un'equazione di questo tipo;
d) in definitiva, non è sempre immediatamente riconoscibile l'incognita e, talora, neppure l'equazione è riconoscibile come tale.

Esempio. Supponiamo di osservare due veicoli che viaggiano da Rimini a Bologna in autostrada: il primo proviene da Rimini sud e viaggia a una velocità costante di 120 Km/h; il secondo parte dal casello di Rimini nord nel momento in cui transita il primo veicolo, poi accelera costantemente fino a raggiungere l'altro veicolo in 15 minuti. Che accelerazione ha avuto il secondo veicolo?

Le lettere che compaiono nelle formule di meccanica sono: *v* per la velocità, *t* per il tempo, *s* per lo spazio percorso, *a* per l'accelerazione. I Fisici suggeriscono di operare quanto possibile con le lettere, rinviando alla fine la sostituzione dei loro valori numerici. Seguiamo il loro consiglio e ragioniamo. La prima auto viaggia in moto rettilineo (a grandi linee…) e uniforme, secondo la legge $s = v \cdot t$; la seconda, con moto uniformemente accelerato e partenza da fermo, viaggia secondo la legge $s = \frac{1}{2} a \cdot t^2$. Lo spazio percorso è lo stesso, dal casello al punto del ricongiungimento, ed ovviamente il tempo trascorso è lo stesso. Si ha così, per confronto tra le due espressioni di *s*,

l'equazione $\frac{1}{2}a \cdot t^2 = v \cdot t$. Ma è una equazione? Di che grado? Chi è l'incognita? Che ci fanno le altre lettere? E' facile che un allievo a questo punto non sappia che cosa fare. Se ci fosse scritto: $\frac{1}{2}x \cdot b^2 = a \cdot b$ saprebbe subito ricavare $x = \frac{2a}{b}$ (e se b = 0?). Nell'uguaglianza $\frac{1}{2}a \cdot t^2 = v \cdot t$ però la x non c'è, il succedaneo d'incognita più probabile è certamente la *t* e quindi al massimo qualche allievo ricava $t = \frac{2v}{a}$. Ma dovevamo trovare l'accelerazione …

La lettera scelta per essere ricavata risolvendo l'equazione si continua a chiamarla *incognita*, ed allora alle altre si dà talora il nome di *parametri*. Questi ultimi di norma non sono costanti, e quindi è necessario accertarsi che possano assumere valori tali da rendere risolubile l'equazione rispetto all'incognita da noi prescelta. Nel nostro esempio, se l'incognita è *a*, come dovrebbe, si deve porre $t \neq 0$ per l'univocità della soluzione. Più ci si riflette, più complicazioni si ritrovano …

Come evitare l'accusa di far parte di un *Ufficio Complicazione Cose Semplici*?

Un insegnamento che si chiama "Elementi di Algebra da un punto di vista superiore" sembra proprio uscire da tale ufficio!

Eppure, talora siamo noi insegnanti a ritenere semplici dei concetti che non lo sono affatto, o a far diventare complicati altri che in realtà non lo sarebbero.

Del primo tipo sono le nozioni di angolo, poligono, polinomio, frazione algebrica, equazione, il segno -, il segno =. Del secondo tipo è, forse, il concetto di integrale.

Credo si possa riuscire ad evitare che l'algebra sia vista o come un insieme arido di formule e calcoli inutili ed incomprensibili, o come un terreno minato, in cui ogni concetto oscilla pericolosamente tra significati talora opposti. Vediamo:

- L'algebra sembra talora astrusa perché non diamo le informazioni giuste agli allievi.
- Dare risposte a domande non poste è spesso didatticamente infruttuoso. La matematica nel suo complesso può correre questo rischio, e l'algebra in particolare.
- La complicazione è quasi sempre indispensabile, ma penso vada preparata e inserita quando serve, per dare le risposte giuste quando altri approcci sono inutili.

Esempio. Nulla vieta di rappresentare i numeri naturali come file di tacche: le operazioni sono abbastanza semplici, le proprietà abbastanza evidenti, l'ordinamento è intuitivo. Tuttavia, per scrivere un numero grande, per esempio quello degli iscritti all'Università di Bologna, occorre tracciare decine di migliaia di tacche. Dove? Su che supporto? Come controllare? Ecco che un modo più efficiente di rappresentare i numeri diventa necessario. Dopo molti tentativi, il sistema posizionale in base 10 che usiamo diventa una liberazione: numeri grandi scritti in poco spazio, calcoli non difficili, ordinamento comprensibile. Ma con i numeri naturali nasce l'idea di successione e di serie. Come calcolare $\sum_{k=0}^{n} k^2$ al variare di n? C'è una formula in funzione di n che eviti tutte quelle addizioni? Come essere certi che sia vera per ogni n? Ecco allora la necessità di una descrizione globale dei numeri naturali attraverso un *sistema di assiomi*, tra cui il principio d'induzione, e di regole di formazione, dai quali dedurre ciò che sappiamo già, ma anche scoprire e dimostrare altre proprietà, come per esempio l'identità $\sum_{k=0}^{n} k^2 = \frac{n \cdot (n+1) \cdot (2n+1)}{6}$ o l'infinità dei numeri primi.

Un'ultima considerazione sul titolo del corso. Non sarebbe meglio il contrario: "Algebra superiore da un punto di vista elementare"?

Sembra più attraente cercare di spiegare come la Scienza incida nella nostra vita quotidiana e sia perciò importante conoscerla. Poi, molti potrebbero essere attratti dalla sensazione di entrare a sbirciare nelle stanze segrete frequentate solo dagli "iniziati", di essere ammessi a far parte di una elite di "*egregi*", di essere a loro volta "*illuminati*".

Credo siano necessari entrambi i punti di vista: vedere dal basso le cime delle montagne, per sapere quel che ci circonda, ma anche contemplare dall'alto il panorama, meglio se con un ottimo binocolo, per sapere dove portano quelle strade che possiamo imboccare o, se serve e si può, costruirne altre, per arrivare anche da altre parti.

§ 2 – FUNZIONI, OPERAZIONI E STRUTTURE ALGEBRICHE

Contenuti: Funzioni tra insiemi; rappresentazioni tabulari, grafiche e matriciali delle funzioni; *grafi e digrafi*. Operazioni in un insieme, rappresentazione, proprietà; tipi elementari di strutture algebriche: monoidi e gruppi, anelli e campi; esempi e proprietà di base.

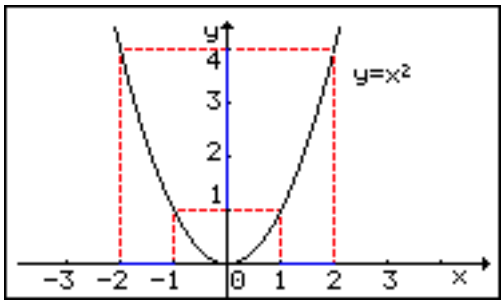
FUNZIONI. Dati due insiemi A e B si chiama *funzione* da A a B, e si denota con $f:A\to B$, una relazione $f\subseteq A\times B$ tale che per ogni $x\in A$ esiste uno ed un solo $y\in B$ tale che $(a,b)\in f$. Si scrive di solito $f:a\to b$ oppure $b = f(a)$ anziché $(a,b)\in f$.

Per indicare le funzioni, si usano lettere minuscole o talora maiuscole, latine o greche (f, g, F, Φ, σ, ...). Se $f:A\to B$, l'insieme A si dice *dominio* e l'insieme B si dice *codominio* di f. L'insieme $\{b\in B \mid \exists a\in A, f(a) = b\}$ si chiama *immagine di f*, e si denota con Im f o con f(A).

Sia $f:A\to B$ una funzione e siano $C\subseteq A$, $D\subseteq B$. Indichiamo con f(C) l'insieme $\{b\in B \mid \exists a\in C,\ f(c) = b\}$, che si può descrivere anche come $\{f(c) \mid c\in C\}$, e che si chiama *immagine di C in B tramite f*. In particolare, come già detto, $f(A)$ è l'immagine di f.

L'insieme $\{a\in A \mid f(a)\in D\}$ è un sottoinsieme di A detto *controimmagine di D in A tramite f*, e si denota spesso con $f^{-1}(D)$, anche se talora questo simbolo può assumere significati diversi.

Nell'esempio qui a lato c'è la funzione $f:\mathbf{R}\to\mathbf{R}$, $f(x) = x^2$. L'immagine dell'intervallo $[1,2]$ è l'intervallo $[1,4]$, mentre la controimmagine dell'intervallo $[1,4]$ è $[-2,-1]\cup[1,2]$. Si ha poi $\mathrm{Im}\, f = [0,+\infty[$.



Date due funzioni $f:A\to B$ e $g:A\to B$, con lo stesso dominio A e lo stesso codominio B, si ha $f = g$ quando (come insiemi di coppie ordinate) esse posseggono gli stessi elementi. Si ricava allora che $f = g \Leftrightarrow \forall x\in A,\ f(x) = g(x)$.

Siano ora A e B due insiemi. Dal punto di vista "insiemistico" le classi di funzioni più notevoli sono le seguenti:

funzioni iniettive. Una funzione f:A→B si dice iniettiva, e si scrive $f : A \xrightarrow{1\text{–}1} B$, se per ogni y∈B esiste al massimo un x∈A tale che y = f(x);

funzioni suriettive. Una funzione f:A→B si dice suriettiva, e si scrive $f : A \xrightarrow{su} B$, se per ogni y∈B esiste almeno un x∈A tale che y = f(x);

funzioni biiettive (o biiezioni). Una funzione f:A→B si dice biiiettiva, e si scrive $f : A \xrightarrow[su]{1\text{–}1} B$, se per ogni y∈B esiste uno ed un solo x∈A tale che y = f(x).

Una funzione biiettiva è pertanto iniettiva e suriettiva.

Una definizione equivalente di funzione iniettiva è la seguente: f:A→B è iniettiva se e solo se per ogni x_1 ed x_2∈A, se $f(x_1) = f(x_2)$ allora $x_1 = x_2$. Per dimostrare che una data funzione è iniettiva si fa generalmente uso di quest'ultima definizione.

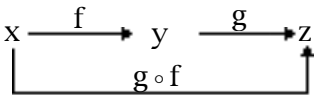
Per quanto riguarda le funzioni suriettive, si può dire che una funzione f:A→B è suriettiva se e solo se la sua immagine f(A) coincide col codominio B.

Data una relazione $\Re$ tra due insiemi A e B, si può definire una nuova relazione tra B ed A, detta *trasposta* di $\Re$ ed indicata con $\Re^t$, nel modo seguente:

$$\Re^t = \{(b,a) \mid (a,b) \in \Re\}.$$

Se in particolare consideriamo una funzione f:A→B, la relazione trasposta in generale non è una funzione. Se però f è una biiezione allora la trasposta non solo è una funzione, ma è addirittura una biiezione. Essa si denota con f^{-1} e viene chiamata *funzione inversa* di f. Un nome tradizionale per le biiezioni è *corrispondenza biunivoca*, termine che sottintende proprio questa possibilità di definire l'inversa di f. Se invece f non è una biiezione allora la sua trasposta non è mai una funzione.

Siano A, B, C tre insiemi e siano f:A→B e g:B→C due funzioni. Definiamo una funzione, che denoteremo con g∘f, tra A e C nel modo seguente: per ogni x∈A sia y = f(x) e sia z = g(y); poniamo g∘f(x) = z, ovvero g∘f(x) = g(f(x)).



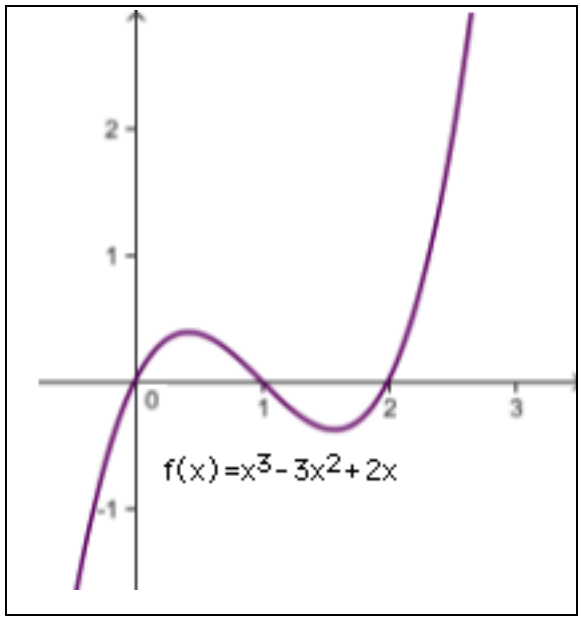
Come ben noto, valgono le seguenti proprietà:

Siano A, B, C, D quattro insiemi e siano f:A→B, g:B→C, h:C→D. Siano id_A e id_B le funzioni identità su A e B rispettivamente.

- Si ha $(f \circ g) \circ h = f \circ (g \circ h)$ (associatività)
- Se $f : A \xrightarrow[su]{1\text{–}1} B$ allora $f^{-1} \circ f = id_A$; $f \circ f^{-1} = id_B$
- Se $f : A \xrightarrow[su]{1\text{–}1} B$ e $g : B \xrightarrow[su]{1\text{–}1} C$ allora $g \circ f : A \xrightarrow[su]{1\text{–}1} C$.
- $id_B \circ f = f = f \circ id_A$.

RAPPRESENTAZIONE DI FUNZIONI.

Nel caso reale, ossia per una funzione f da un sottoinsieme E del campo reale **R** in **R**, è possibile usare un grafico cartesiano, in cui ogni coppia $(x, f(x))$ è rappresentata dal punto P che ha quelle coordinate. Il grafico di f è quindi in generale una curva del piano. L'Analisi Matematica interviene in questo caso. Qui accanto vediamo una cubica con tre zeri, un punto di massimo ed uno di minimo relativi ed un punto di flesso. Per trovarli servono limiti e derivate.



Nel caso finito, è possibile servirsi di rappresentazioni *tabulari, matriciali o mediante digrafi*. Per esempio, consideriamo un insieme X con $m \geq 1$ elementi. Possiamo ordinarlo totalmente in uno degli m! modi possibili e quindi per $1 \leq i \leq m$ denotare con x_i il suo elemento che occupa il posto i. Meglio ancora, in qualche caso potremmo denotare tale elemento direttamente con i, quindi assimilare X ad $\mathbf{N}_m = \{i \in \mathbf{N} \mid 1 \leq i \leq m\}$

Una funzione tra un insieme X con m elementi ed uno, Y, con n elementi diventa una tabella $\begin{array}{c|cccc} x & x_1 & x_2 & \dots & x_m \\ \hline f(x) & f(x_1) & f(x_2) & \dots & f(x_m) \end{array}$, che può trasformarsi anche nella *matrice a due*

righe $\begin{pmatrix} x_1 & x_2 & \dots & x_m \\ f(x_1) & f(x_2) & \dots & f(x_m) \end{pmatrix}$, più usata per le *permutazioni*, ossia le funzioni biiettive da un insieme in sé, o anche direttamente nella seconda riga della matrice, ossia nella *stringa* $\begin{pmatrix} f(x_1) & f(x_2) & \dots & f(x_m) \end{pmatrix}$. Ogni casella può essere un qualunque elemento di Y, quindi ha n possibilità. Ne viene che, per il *principio di moltiplicazione*, ci sono n^m funzioni $f : X \to Y$.

Un'altra possibile rappresentazione è mediante le *matrici booleane d'incidenza*. Codifichiamo X ed Y mediante i tratti iniziali $\mathbf{N}_m$ ed $\mathbf{N}_n$ di **N**. Definiamo la seguente matrice $M = M_f$, di tipo m×n, ponendo $m_{ij} = \begin{cases} 1 & \text{se } f(i) = j \\ 0 & \text{se } f(i) \neq j \end{cases}$. In questa matrice, in ogni riga c'è uno ed un solo 1; se f è iniettiva, anche in ogni colonna c'è un solo 1 ed $m \leq n$; se è suriettiva, in ogni colonna c'è almeno un 1 e $m \geq n$; infine, se f è biiettiva, M è necessariamente quadrata ed è detta *matrice di permutazione*, perché in ogni riga e colonna c'è uno ed un solo 1.

Nel caso Y = X, con n elementi, allora M è sempre quadrata. La sua *traccia* indica quanti sono gli elementi *uniti*, ossia portati da f in se stessi; il *determinante* è 0 se f non è biiettiva, altrimenti è ±1. La matrice *trasposta* di M è la matrice della relazione trasposta. Se f è biiettiva, M è *ortogonale* e l'inversa coincide con la trasposta: $M_{f^{-1}} = (M_f)^{-1} = (M_f)^t$.

Oltre alla rappresentazione cartesiana, che qui è assai più convenzionale rispetto alle funzioni dell'analisi, si può usare un'altra rappresentazione geometrica, mediante *un grafo orientato* o digrafo, di tipo opportuno.

GRAFI E DIGRAFI. Chiameremo *grafo (non orientato)* Γ = (V, B) una coppia formata da un insieme non vuoto V, i cui elementi sono detti *vertici* ed un insieme B di coppie non ordinate di elementi di V, dette *spigoli*.

Se V è finito, $V = \{v_1, \dots, v_n\}$, il grafo Γ si rappresenta nel piano nel modo seguente: ogni vertice si rappresenta con un punto, contrassegnato con il suo stesso nome, e ogni spigolo $\{v_i, v_j\}$ si rappresenta mediante un arco di curva continua e semplice di estremi v_i, v_j e che non passi per alcun altro vertice.

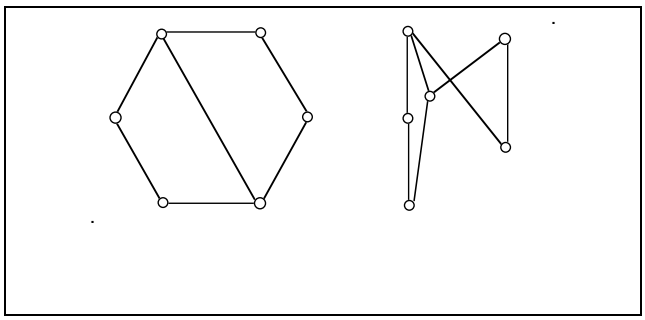
Il grafo si dice *planare* se si può rappresentare sul piano in modo che gli spigoli non abbiano altri punti in comune al di fuori dei vertici

Si chiama *laccio* uno spigolo con gli estremi nello stesso vertice. In tal caso il vertice in questione si può rappresentare con un cerchietto vuoto.

Una *catena di lunghezza r* che congiunge i vertici v_i e v_j è una sequenza di spigoli consecutivi distinti del tipo $\{v_{i_0} = v_1, v_{i_1}\}, \{v_{i_1}, v_{i_2}\}, ..., \{v_{i_{r-1}}, v_{i_r} = v_j\}$. Dati due vertici v_i e v_j, poniamo $v_i \sim v_j$ se esiste una catena che li congiunge. Si ha così una relazione d'equivalenza in V, le cui classi si dicono *componenti connesse*. Un grafo si dice *connesso* se ha una sola componente connessa.Un grafo sconnesso è planare se e solo se lo sono le sue componenti.

Un grafo si dice *completo* se per ogni i, j = 1,..., n si ha $\{v_i, v_j\} \in B$. Un tal grafo è connesso e tutti i suoi vertici sono rappresentati da cerchietti. E' planare solo per n = 1, 2, 3.

Due grafi $\Gamma_1 = (V_1, B_1)$ e $\Gamma_2 = (V_2, B_2)$ si dicono *isomorfi* se esiste una biiezione $f:V_1 \to V_2$ tale che per ogni v, v'∈V, $\{v, v'\} \in B_1 \Leftrightarrow (f(v), f(v')\} \in B_2$. I grafi della figura seguente sono isomorfi, pur avendo un aspetto differente, e sono planari.



Un *grafo orientato* o *digrafo* (V, B) si può riguardare come una struttura relazionale costituita da un insieme V e da una relazione $B \subseteq V \times V$. Ogni elemento $(x, y) \in B$ si chiama *arco* e si rappresenta con un arco orientato (o *freccia*) dal punto che rappresenta x a quello che rappresenta y. Le catene di archi equiorientati si dicono *cammini*, e i lacci orientati si dicono *cappi*. Con ovvie modifiche per rispettare gli orientamenti, l'isomorfismo si può definire anche tra due digrafi.

Tra i digrafi, molto importanti sono gli **alberi**: sono connessi, privi di circuiti e di cammini distinti con lo stesso punto iniziale e finale, e con un solo vertice iniziale, detto *radice*, e uno o più vertici finali, detti *foglie*. Se si rovescia l'orientamento degli archi, dalle foglie verso la radice, si ottiene un *albero duale* o *coalbero*.

Esiste una rappresentazione geometrica di una funzione $f:X \to X$ mediante un digrafo $\Gamma = \Gamma(X, f)$ di tipo particolare: i suoi vertici sono gli elementi di X e $x \to y \Leftrightarrow y = f(x)$. Poiché f è una funzione, allora da ogni vertice esce una ed una sola freccia. In particolare, partendo da un elemento $x_0 \in X$ ed applicando ripetutamente f, si ottiene una successione finita

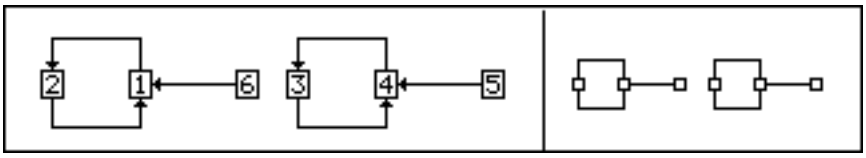
$$x_0 \to x_1 = f(x_0) \to \ldots \to x_{i+1} = f(x_i)$$

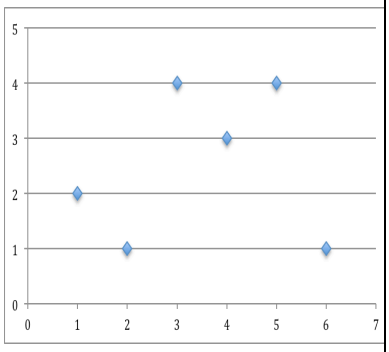
dove l'ultimo termine uguaglia uno dei termini x_j già incontrati. Si genera così un *circuito* comprendente $x_j, x_{j+1}, \ldots, x_i$, a cui è "attaccato" il *coalbero* $x_0, x_1, \ldots, x_{j-1}$. Ogni circuito può avere più "accessi", ma non ha "uscite". Più precisamente, ad ogni nodo di un circuito possono essere attaccati dei coalberi attraverso il loro nodo terminale.

ESEMPIO 2.1 Sia data la funzione seguente funzione dall'insieme $\{1,2,3,4,5,6\}$ a se stesso. Essa si può rappresentare nei modi seguenti: tabulare, matriciale, cartesiano. Sono poi mostrate due versioni del digrafo, una dettagliata ed una più astratta astratta.

x	f(x)
1	2
2	1
3	4
4	3
5	4
6	1

$$\Rightarrow f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 4 & 1 \end{pmatrix} \Rightarrow M_f = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$





OPERAZIONI. Una *operazione binaria (interna)* in un insieme non vuoto X è una applicazione (o funzione) da X×X ad X. Per indicare una operazione si usano i simboli +, × , ·, *, ° ecc. Di solito nelle considerazioni "astratte" si adopera il simbolo · ; in tal caso il risultato dell'operazione sulla coppia (x,y) è detto *prodotto* ed è indicato con x · y o più brevemente con xy.

Se X è un insieme finito con n elementi, per definire un'operazione si può costruire una tabella, simile alla tavola pitagorica, che contiene i risultati.

ESEMPIO 2.2. Sia $X = \{1,2,3\}$. La tabella seguente definisce una operazione in X. In essa per esempio: $2*3 = 1$, $2*1 = 1$, ecc. Ognuna delle 9 caselle interne della tavola contiene uno ed uno solo dei 3 elementi di X.

*	1	2	3
1	1	3	2
2	1	3	1
3	2	3	2

Ne segue che sull'insieme X si possono definire ben $3^9 = 19.683$ operazioni diverse!

Naturalmente non tutte le operazioni definibili in un insieme saranno in qualche modo interessanti. Ciò che le rende tali è la presenza di particolari proprietà. Vediamo un elenco delle proprietà più comuni.

1. *Proprietà associativa*: per ogni a, b, c∈X si ha a·(b·c) = (a·b)·c.
2. *Proprietà commutativa*: per ogni a,b∈X si ha a·b = b·a.
3. *Elemento neutro*: esiste un elemento e∈X tale che:

per ogni a∈X, a · e = e · a = a .

4. *Elementi simmetrici* (se c'è un elemento neutro e):

   per ogni $a \in X$ esiste $a' \in X$ tale che $a \cdot a' = a' \cdot a = e$.

5. *Leggi di cancellazione*:

   destra: da $a \cdot b = c \cdot b$ segue $a = c$;

   sinistra: da $a \cdot b = a \cdot c$ segue $b = c$.

6. *Proprietà di idempotenza*: per ogni $a \in X$ si ha $a \cdot a = a$.

7. *Elemento assorbente*: esiste $u \in X$ tale che, per ogni $a \in X$, $a \cdot u = u \cdot a = u$.

La lista si potrebbe allungare. Le proprietà elencate si trovano negli esempi più importanti, ma non contemporaneamente. Il primo passo è scoprire quali di queste proprietà possano coesistere, quali si escludano a vicenda, quali siano conseguenza di altre.

Alcune relazioni tra queste proprietà si scoprono facilmente perché sono conseguenza immediata delle definizioni. Per esempio in una struttura $(X, \cdot)$ c'è al massimo un elemento neutro: difatti dati due elementi neutri e_1 ed e_2, si ha $e_1 \cdot e_2 = e_2$, poiché e_1 è elemento neutro, ma anche $e_1 \cdot e_2 = e_1$ poiché anche e_2 è elemento neutro, dunque per l'unicità del prodotto si ha $e_1 = e_2$. Per questo è possibile usare l'articolo determinativo "lo". L'elemento neutro di solito è indicato con 1_X. Allo stesso modo si prova che c'è al più un elemento assorbente.

La parte dell'algebra che studia le proprietà generali delle strutture algebriche si chiama "Algebra universale". Essa prende in considerazione anche operazioni con un numero di fattori diverso da due; per esempio le operazioni *ternarie* operano su tre fattori, e così via. Si definisce poi *operazione unaria* su X ogni funzione da X ad X ed operazione *zeroaria* ogni elemento di X. Chiameremo sinteticamente *operazione finitaria* su X una operazione *n-aria*, con n intero ≥ 0. Una struttura algebrica è una sequenza formata da un insieme e da una o più operazioni finitarie: $\left(X, f_1, f_2, \ldots, f_r\right)$.

In questo paragrafo ripassiamo alcuni tipi di strutture algebriche con operazioni *interne*, ossia nelle quali i termini ed il risultato appartengono ad uno stesso insieme X. Per ciascuna di esse vedremo alcuni esempi ed alcune nozioni. Non saranno trattate tutte le strutture interessanti, ma solo alcune di esse, funzionali agli scopi ed al contenuto di questo corso.

Osserviamo che, quando non vi sia pericolo di ambiguità, una struttura algebrica $\left(X, f_1, f_2, \ldots, f_r\right)$ sarà denotata anche solo con X.

2.A. Sistemi di Peano $(N,\sigma,0)$: qui $0\in N$, $\sigma : N \xrightarrow{1\text{–}1} N$, $Im(\sigma) = N\setminus\{0\}$ e $\forall M \subseteq N$, se $0\in N$ e per ogni $x\in M$ anche $\sigma(x) \in M$ allora $M = N$ (*principio d'induzione*). Si tratta dei numeri naturali definiti dagli assiomi di Peano.

2.B. Semigruppo $(S,\cdot)$: l'operazione binaria $\cdot$ è associativa. Questo tipo di struttura ha grande importanza soprattutto nell'Analisi Matematica. Nel caso algebrico è più comune considerare il caso in cui l'operazione possiede l'elemento neutro.

2.C. Monoide $(M,\cdot,1_M)$: l'operazione binaria $\cdot$ è associativa ed 1_M ne è l'elemento neutro.

Un monoide $(M,\cdot,1_M)$ si dice *commutativo* se $\forall x,y \in M,\ x\cdot y = y\cdot x$.

Un monoide $(M,\cdot,1_M)$ si dice *idempotente* se $\forall x \in M,\ x\cdot x = x$.

Un elemento $x \in M$ si dice:

- *cancellabile a sinistra* se $\forall y,z \in M,\ x\cdot y = x\cdot z \Rightarrow y = z$
- *cancellabile a destra* se $\forall y,z \in M,\ y\cdot x = z\cdot x \Rightarrow y = z$

Un monoide commutativo $(M,\cdot,1_M)$ si dice *regolare* se ogni $x \in M$ è cancellabile a destra ed a sinistra.

Un elemento $x \in M$ si dice *invertibile* se esiste $x' \in M$ tale che $x\cdot x' = x'\cdot x = 1_M$; in tal caso, x' è il *simmetrico* (o l'*inverso*) di x, ed è unico, infatti, se x ha due simmetrici x' ed x'' si ha:

$$x' = x'\cdot 1_M = x'\cdot(x\cdot x'') = (x'\cdot x)\cdot x'' = 1_M\cdot x'' = x''.$$

L'insieme degli elementi invertibili di M si denota spesso con M^*: non è vuoto perché contiene 1_M. Inoltre, $\forall x,y \in M^*$ anche $x\cdot y \in M^*$ dato che ha per simmetrico $y'\cdot x'$. Infine, $(x')' = x$.

Esempi 2.3. a) *I monoidi di funzioni*: sia X un insieme non vuoto e sia X^X l'insieme delle funzioni da X in sé; definiamo in X^X l'operazione $\circ$ di composizione: è noto che è associativa e che ha per elemento neutro la *funzione identità* id_X che ad ogni $x \in X$ associa se stesso. Il monoide $(X^X,\circ,id_X)$ è detto il *monoide delle funzioni di X*. Se X ha n elementi, dal calcolo combinatorio sappiamo che esso possiede n^n elementi. Se X ha almeno due elementi, il monoide non ha la legge di cancellazione, a

causa per esempio delle funzioni costanti, non ha elemento assorbente e non è commutativo né idempotente. Gli elementi dotati di inverso sono le funzioni biiettive, dette *permutazioni* di X; se X ha n elementi, ce ne sono n!.

b) Sia X un insieme e sia $\wp(X)$ l'insieme dei suoi sottoinsiemi. Allora $(\wp(X), \cup, \varnothing)$ è un monoide commutativo idempotente. Ha l'elemento assorbente, X, dato che per ogni $A \subseteq X$, $A \cup X = X$. Non ha la legge di cancellazione, e ø è il solo elemento dotato di inverso.

c) *I monoidi di parole*: sia A un insieme finito di oggetti che chiameremo *lettere*; con esse formiamo delle sequenze finite, le *parole* nell'*alfabeto* A. Consideriamo anche la *parola vuota*, indicata per esempio con ø. Sia $\mathcal{F}_A$ l'insieme delle parole nell'alfabeto A, compresa la parola vuota, e definiamo in esso la seguente operazione: date due parole w_1 e w_2, attacchiamo la seconda dietro alla prima ottenendo una nuova parola formata dalla sequenza delle lettere della prima e della seconda. Per esempio, se w_1="abra" e w_2="cadabra", la parola ottenuta è w="abracadabra". Indichiamo con & questa operazione, detta *concatenazione di parole*: essa possiede la proprietà associativa e la parola vuota è il suo elemento neutro. Pertanto ($\mathcal{F}_A$, &, ø) è un monoide, detto *monoide delle parole nell'alfabeto* A. Tale monoide ha in ogni caso infiniti elementi, vale la legge di cancellazione, non ha elemento assorbente, non è idempotente, ed è commutativo solo se c'è una lettera sola. La parola vuota è il solo elemento invertibile. Si osservi che ogni parola w ha una *lunghezza* $\ell(w)$ data dal numero delle sue lettere. In particolare, $\ell(\varnothing) = 0$, e inoltre $\ell(w_1 * w_2) = \ell(w_1) + \ell(w_2)$.

d) In un sistema di Peano $(N, \sigma, 0)$ definiamo induttivamente l'operazione + ponendo: $\forall m, n \in N$,

$\begin{cases} m + 0 = m \\ m + \sigma(n) = \sigma(m + n) \end{cases}$. Quest'operazione si chiama *addizione*, ha 0 come elemento neutro, è associativa, commutativa, ha la legge di cancellazione e quindi non ha elemento assorbente e non è idempotente. Allora $(N, +, 0)$ è un monoide commutativo regolare.

Una nozione che si può introdurre in un monoide è quella di *potenza*. Sia $(M, \cdot, 1_M)$ un monoide e sia $x \in M$. Poniamo $\forall n \in \mathbf{N}$, $\begin{cases} x^0 = 1_M \\ x^{n+1} = x^n \cdot x \end{cases}$.

Valgono per le potenze le due proprietà seguenti:

$$\forall x \in M,\ \forall m, n \in \mathbf{N},\ \begin{cases} x^n \cdot x^m = x^{n+m} \\ \left(x^n\right)^m = x^{nm} \end{cases}.$$

Si noti che $\forall x, y \in M,\ (x \cdot y)^n = x^n \cdot y^n\ \forall n \in \mathbf{N} \Leftrightarrow x \cdot y = y \cdot x$.

Di un elemento invertibile x si possono definire inoltre anche le *potenze con esponente intero negativo*: se x' è il suo simmetrico, per ogni $n \in \mathbf{N}$, $n > 0$, poniamo $x^{-n} = (x')^n$. In tal modo $x^{-1} = x'$ e per questo il simmetrico di x è usualmente denotato con x^{-1}. Inoltre valgono anche in questo nuovo caso le proprietà già viste per le potenze ad esponente positivo.

Un monoide M tale che $M = M^*$, ossia nel quale ogni elemento sia invertibile è detto *gruppo*. In tal caso, associando ad ogni $x \in M$ il suo simmetrico x^{-1} otteniamo una funzione biiettiva $s : M \to M$.

2.D. Gruppo $(G, \cdot, 1_G, s)$: l'operazione binaria $\cdot$ è associativa, 1_G ne è l'elemento neutro e ogni elemento x ha il simmetrico $x^{-1} = s(x)$, dove con il simbolo s indichiamo la funzione, cioè l'operazione unaria, che ad ogni x associa il suo simmetrico x^{-1}. Tale funzione σ è biiettiva e coincide con la sua inversa.
Se l'operazione $\cdot$ possiede anche la proprietà commutativa il gruppo si dice *abeliano*.
Di solito nei testi di algebra un gruppo è indicato soltanto con $(G, \cdot)$. Vediamo qualche esempio.

Esempi 2.4.a. *Il gruppo delle unità di un monoide*. Gli elementi di un monoide M che hanno l'inverso rispetto alla moltiplicazione $\cdot$ si dicono *elementi unitari* e costituiscono il gruppo M^*, detto *gruppo delle unità* del monoide.
Nel caso del monoide X^X delle funzioni da X ad X il gruppo delle unità è precisamente il *gruppo simmetrico* S_X, i cui elementi sono le biiezioni da X in sé e che si chiamano *permutazioni di X*. Se $X = \{1, 2, \dots, n\}$, il suo gruppo simmetrico si denota con S_n. Dal calcolo combinatorio sappiamo che S_n possiede n! elementi.

b) *Gruppi di isometrie*. In un insieme non vuoto X sia data una funzione $d : X \times X \to \mathbf{R}$; la chiameremo *distanza* se soddisfa le seguenti condizioni: $\forall x, y, z \in X$,

a) $d(x, y) = d(y, x)$
b) $d(x, y) \geq 0$
c) $d(x, y) = 0 \Leftrightarrow x = y$
d) $d(x, y) + d(y, z) \geq d(x, z)$

In tal caso, la coppia (X,d) è detta *spazio metrico*. Un'*isometria* di (X,d) è una biiezione $f : X \to X$ tale che $\forall x, y \in X,\ d(f(x),f(y)) = d(x,y)$. Si può dimostrare facilmente che, rispetto all'usuale operazione di composizione, l'insieme Iso(X,d) delle isometrie di (X,d) è un gruppo. Nel caso particolare del piano euclideo, in cui, fissata un'unità di misura, la distanza di due punti è la lunghezza del segmento che li congiunge, il gruppo delle isometrie coincide con quello visto nel modulo di Elementi di Geometria, ed è costituito da rotazioni, traslazioni, simmetrie assiali e antitraslazioni.

c) *I gruppi diedrali*. Dato un poligono regolare con n lati (n ≥ 3), vi sono 2n *isometrie* del piano che lo trasformano in sé e precisamente le n rotazioni di ampiezza $\frac{2k\pi}{n}, k = 0,1,\dots,n-1$, intorno al centro O del poligono e le n simmetrie assiali rispetto agli n assi di simmetria del poligono (tutti passanti per O). L'insieme di tali isometrie si indica con D_n, (D_{2n} su qualche testo) e si può dimostrare che la composizione di due elementi di D_n è ancora un elemento di D_n. L'elemento neutro è la funzione identità del piano, identificabile come la rotazione di ampiezza nulla intorno ad O. Se r è una rotazione di ampiezza $\frac{2k\pi}{n}$, la sua inversa è la rotazione di ampiezza $\frac{2(n-k)\pi}{n}$; invece, ogni simmetria assiale ha per inversa se stessa. Il gruppo D_n ha 2n elementi e si vede facilmente che non è abeliano: detta s una qualunque simmetria assiale ed r una rotazione, si ha $s \circ r = r^{-1} \circ s$. Quindi, purché r non sia la simmetria centrale, ossia la rotazione di ampiezza π, si ha $r^{-1} \neq r$ e quindi $s \circ r = r^{-1} \circ s \neq r \circ s$.

Poiché ogni elemento è invertibile, un gruppo $(G,\cdot)$ possiede la legge di cancellazione. Si noti poi che se l'operazione non è commutativa non è detto che le due "equazioni" $a \cdot x = b$ e $y \cdot a = b$ abbiano la stessa soluzione: si ha infatti $x = a^{-1} \cdot b$, mentre $y = b \cdot a^{-1}$ e può accadere che $a^{-1} \cdot b$ sia diverso da $b \cdot a^{-1}$.

L'insieme delle potenze ad esponente intero relativo di un elemento x si denota con $\langle x \rangle$. Il numero di elementi di questo insieme si chiama *periodo* o anche *ordine* di x e si denota con |x|.

TEOREMA 2.5. Sia G un gruppo e sia $x \in G$.

a) Il periodo di x è infinito se e solo se $\forall h,k \in \mathbf{Z},\ x^h = x^k \Rightarrow h = k$.

b) Se $|x| = n$, si ha $x^n = 1_G$. In tal caso si ha:

$$\langle x \rangle = \left\{ 1_G = x^0, x^1, \ldots, x^{n-1} \right\}$$

c) Se |x| = n, si ha $x^k = 1_G \Leftrightarrow$ n divide k.

Per esempio, nel gruppo D_n ogni simmetria ha periodo 2, la rotazione di ampiezza $\frac{2\pi}{n}$ ha periodo n e le altre rotazioni sono le sue potenze. Nel gruppo $(\mathbf{Z}, +)$ ogni elemento diverso da 0 ha periodo infinito; si ha inoltre $\langle 1 \rangle = \mathbf{Z}$ (ricordiamo che se l'operazione è indicata con + si parla di multipli anziché di potenze).

Quando in un gruppo $(G, \cdot)$ c'è un elemento x tale che $\langle x \rangle = G$ allora il gruppo si dice *ciclico* ed x si chiama *generatore* di G. Con questa terminologia, $(\mathbf{Z}, +)$ è ciclico, generato da 1. Un gruppo ciclico è sempre abeliano.

2.E. Anello (associativo con unità) $(A, +, \cdot, 1_A) = (A, +, 0_A, \sigma, \cdot, 1_A)$, dove $(A, +) = (A, +, 0_A, \sigma)$ è un gruppo abeliano; $(A, \cdot, 1_A)$ è un monoide e valgono le due *proprietà distributive* (destra e sinistra) di · rispetto a +, ossia:

$$\forall a, b, c \in A, \begin{cases} a \cdot (b + c) = a \cdot b + a \cdot c \\ (a + b) \cdot c = a \cdot c + b \cdot c \end{cases}.$$

Si ha: $\forall x \in A,\ x \cdot 0_A = x \cdot (0_A + 0_A) = x \cdot 0_A + x \cdot 0_A \Rightarrow x \cdot 0_A = 0_A$. Si osservi poi che i due elementi neutri possono coincidere, ma in tal caso l'anello stesso si riduce ad un solo elemento, ossia è *banale.* Infatti, se $0_A = 1_A$, allora $\forall x \in A,\ x = x \cdot 1_A = x \cdot 0_A = 0_A$.
Se l'operazione · è commutativa l'anello si dice *commutativo*. $(\mathbf{Z}, +, \cdot, 1)$ è un anello commutativo. Vediamo altri esempi.

Esempi 2.6. a). *Anelli di funzioni*. Siano X un insieme ed $(A, +, \cdot, 1_A)$ un anello. Nell'insieme A^X costituito dalle funzioni da X ad A definiamo le seguenti operazioni, dette operazioni *punto per punto*:

$$\forall f, g \in A^X,\ \forall x \in X,\ \begin{cases} (f + g)(x) = f(x) + g(x) \\ (f \cdot g)(x) = f(x) \cdot g(x) \\ (-f)(x) = -f(x) \end{cases}.$$

Consideriamo inoltre le due funzioni costanti **0** ed **1** tali che $\forall x \in X$, $\mathbf{0} : x \mapsto 0_A$ ed $\mathbf{1} : x \mapsto 1_A$. Si prova facilmente che con queste operazioni A^X è un anello in cui **0** è l'elemento neutro di + ed **1** quello di $\cdot$. Se l'anello A è commutativo lo è anche l'anello delle funzioni.

Esempio 2.6.b). *Anelli di successioni*. Sia A un anello commutativo e consideriamo l'insieme $A^{\mathbf{N}}$ delle *successioni*, cioè delle funzioni da **N** ad A. Definiamo in esso la seguente moltiplicazione (detta *convoluzione*):

$$f * g : n \mapsto \sum_{j=0}^{n} f(j)g(n-j).$$

Questa operazione è associativa ed ha per elemento neutro la funzione 1 tale che

$$1 : n \mapsto \begin{cases} 1_A & \text{se } n = 0 \\ 0_A & \text{se } n > 0 \end{cases}.$$

Indichiamo poi con + l'addizione punto per punto: $\left(A^{\mathbf{N}}, +, *, 1\right)$ è un anello commutativo.

Esempio 2.6.c). *Anelli di polinomi*. Più in particolare, consideriamo l'insieme A[x] delle successioni $f : \mathbf{N} \to A$ "definitivamente nulle", ossia tali che $\exists n \in \mathbf{N}$ tale che $\forall k > n$, $f(k) = 0$. Queste successioni si identificano spesso con i *polinomi in una indeterminata* a coefficienti in A. Si vede facilmente che somma ed il prodotto (convoluzione) di polinomi è un polinomio e che $\left(A[x], +, \cdot, 1\right)$ è un anello commutativo.

Sia $x : n \mapsto \begin{cases} 1_A & \text{se } n = 1 \\ 0_A & \text{se } n \neq 1 \end{cases}$ e, per ogni $\forall a \in A$ sia $\bar{a} : n \mapsto \begin{cases} a & \text{se } n = 0 \\ 0_A & \text{se } n \neq 0 \end{cases}$.

Per ogni f∈A[x], $f : k \to \begin{cases} a_k, & 0 \le k \le n \\ 0_A, & k > n \end{cases}$, allora $f = \sum_{k=0}^{n} \bar{a}_k \cdot x^k$. Se $a_n \neq 0_A$ allora n si dice *grado del polinomio*.

Esempio 2.6.d). *Gli anelli Z_m*. Sia $m \in \mathbf{N}$, $m > 0$ e sia $\mathbf{Z}_m = \{0, 1, ..., m-1\}$. In questo insieme definiamo le seguenti operazioni:

$$\begin{cases} x +_m y = & \text{resto della divisione di } x + y \text{ per } m \\ x \times_m y = & \text{resto della divisione di } xy \text{ per } m \end{cases}.$$

L'elemento neutro di $+_m$ è 0, quello di $\times_m$ è 1; l'opposto di x è m-x. Si può dimostrare che $\left(\mathbf{Z}_m, +_m, \times_m, 1\right)$ è un anello commutativo. Nel seguito, per comodità, le operazioni in quest'anello saranno denotate con i simboli usuali + e $\cdot$ come in **Z**.

Come già osservato, in un anello $(A, +, \cdot, 1_A)$ si ha sempre $x \cdot 0_A = 0_A \cdot x = 0_A$. Un anello si dice *integro* se vale la *legge di annullamento del prodotto*:

$$x \cdot y = 0_A \Rightarrow x = 0_A \text{ oppure } y = 0_A.$$

Per esempio, $(\mathbf{Z}, +, \cdot, 1)$ è integro, mentre $(\mathbf{Z}_6, +, \cdot, 1)$ non lo è, in quanto $3 \cdot 2 = 0$. Si noti che in quest'ultimo anello l'equazione $3x^2 = 3x$ ha 6 soluzioni!
Un *dominio d'integrità* è un anello commutativo integro. In tal caso, il monoide $(A \setminus \{0_A\}, \cdot, 1_A)$ è regolare.

Gli elementi di un anello $(A, +, \cdot, 1_A)$ che hanno l'inverso rispetto alla moltiplicazione $\cdot$ si dicono *elementi unitari* e costituiscono il gruppo A^* delle unità del monoide moltiplicativo dell'anello. Tale gruppo è detto *gruppo delle unità* dell'anello. Nel caso di $\mathbf{Z}$ gli elementi unitari sono 1 e -1. Nel caso di $\mathbf{Z}_m$, gli elementi unitari sono quelli *primi con m*, per cui $\mathbf{Z}_m^*$ ha $\varphi(m)$ elementi, dove φ è la ben nota *funzione di Eulero*. Se m è primo si ha $\mathbf{Z}_m^* = \mathbf{Z}_m^* \setminus \{0\}$.

In un anello $(A, +, \cdot, 1_A)$ il periodo di 1_A nel gruppo additivo (A, +) si chiama *caratteristica* di A. Per esempio $\mathbf{Z}$ ha caratteristica infinita (e si usa dire però che ha *caratteristica zero*), mentre $\mathbf{Z}_m$ e l'anello $\mathbf{Z}_m^X$ delle funzioni da un insieme qualunque $X \neq \emptyset$ a $\mathbf{Z}_m$ hanno caratteristica m. Il seguente risultato è ben noto dai corsi di Algebra del triennio.

TEOREMA 2.7. Se l'anello A è un dominio d'integrità allora la caratteristica o è zero oppure è un numero primo p. In quest'ultimo caso ogni elemento diverso da 0_A nel gruppo additivo ha periodo p.

Un *campo* (F, +, $\cdot$): è un anello commutativo in cui tutti gli elementi diversi da 0_F sono invertibili. Posto $F^* = F \setminus \{0_F\}$, si ha che $(F^*, \cdot)$ è un gruppo abeliano, coincidente con il gruppo degli elementi invertibili. Un campo è un anello integro, quindi ha caratteristica 0 oppure un numero primo p.
Esempi di campi sono $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ e $\mathbf{Z}_p$, con p primo.

Un campo finito con q elementi si denota con GF(q). La sua caratteristica è necessariamente un numero primo p e si può dimostrare che si ha sempre $q = p^n$ per un opportuno $n > 0$. Si può anche dimostrare che per ogni primo p e per ogni $n \geq 1$ esiste uno e "sostanzialmente" un solo campo di ordine p^n.

2.F. Reticolo $(R, \vee, \wedge)$, dove $\vee$ e $\wedge$ sono operazioni binarie associative, commutative e tali che per ogni $a, b \in R$ si ha:

$a \vee a = a = a \wedge a$ (*idempotenza* delle due operazioni)

$a \vee (a \wedge b) = a = a \wedge (a \vee b)$ (*legge di assorbimento*).

Esempio 2.8. Due esempi di reticoli costruiti sull'insieme dei numeri naturali sono:
- (N, MCD, mcm), in cui le due operazioni hanno anche elementi neutri (0 e 1 rispettivamente) e le due operazioni sono anche *distributive* l'una rispetto all'altra;
- (N, max, min), dove max{a, b} e min{a, b} indicano rispettivamente il più grande ed il più piccolo fra a e b. In quest'ultimo, solo max ha elemento neutro, lo zero.

Gli (eventuali) elementi neutri di $\vee$ ed $\wedge$ si indicano con 0_R ed 1_R rispettivamente. Un reticolo si dice *complementato* se ha gli elementi neutri e per ogni elemento x esiste un elemento x' tale che $x \vee x' = 1_R$, $x \wedge x' = 0_R$.

Un reticolo si dice *distributivo* se le due operazioni sono distributive l'una rispetto all'altra. Se è anche complementato, ogni suo elemento ha un solo complemento.

Un reticolo si dice infine *algebra di Boole* se è distributivo e complementato, e si indica in tal caso con $(A, \vee, \wedge, 0_A, 1_A, ')$.

Esempio 2.9. a) Se X è un insieme e $\wp(X)$ è l'insieme dei suoi sottoinsiemi, $\left(\wp(X), \cup, \cap, \varnothing, X, '\right)$ è un'algebra di Boole, indicando con Y' il complementare di un sottoinsieme Y di X.

b). Un altro esempio è fornito dall'insieme D = {1, 2, 3, 5, 6, 10, 15, 30} dei divisori di 30: indicando con x' il quoziente 30/x, si ha che (D, MCD, mcm, 30, 1, ') è un'algebra di Boole. Si può dimostrare che un'algebra di Boole finita ha 2^n elementi, per un $n \in \mathbf{N}$ opportuno.

In un'algebra di Boole $(A, \vee, \wedge, 0_A, 1_A, ')$ definiamo la seguente operazione, detta *differenza simmetrica*: $x+y = (x \wedge y') \vee (x' \wedge y)$. Si può dimostrare che $(A, +)$ è un gruppo abeliano e che $(A, +, \wedge, 1_A)$ è un anello, detto *anello di Boole*. In esso ogni

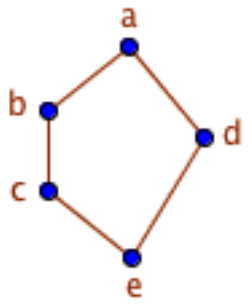
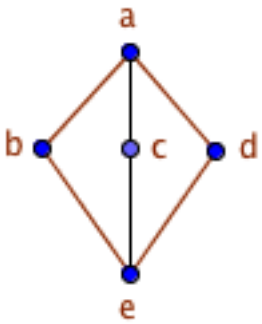
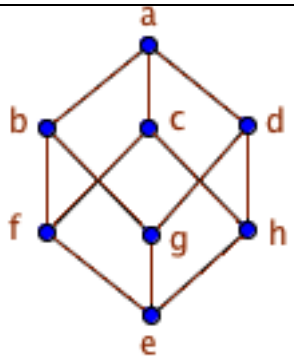
elemento è opposto di se stesso (cioè A ha caratteristica 2) ed è il quadrato di se stesso, ossia A è idempotente. Inversamente, da ogni anello di Boole si può costruire un'algebra di Boole ponendo $x \wedge y = x \cdot y,\ x \vee y = x + y + x \cdot y,\ x' = 1_A + x$.

In un reticolo $(R, \vee, \wedge)$ poniamo: $x \leq y$ se $x \wedge y = x$. Si può dimostrare che la relazione $\leq$ è un ordine in R, tale che per ogni $a,b \in R$ si ha

$$\begin{cases} \sup(a,b) = a \vee b \\ \inf(a,b) = a \wedge b \end{cases}.$$

Per esempio, in (**N**, mcm, MCD) la relazione d'ordine associata è "a è divisore di b"; in $\left(\wp(X), \cup, \cap\right)$ la relazione è "A è sottoinsieme di B". Inversamente, ogni insieme ordinato $(R, \leq)$ nel quale per ogni coppia {x, y} di elementi esistano l'estremo superiore ed inferiore, è un reticolo in cui $x \vee y = \sup\{x, y\}$ ed $x \wedge y = \inf\{x, y\}$. In particolare, ogni insieme totalmente ordinato è un reticolo ed è distributivo.

Esempio 2.10. Ogni reticolo finito è rappresentabile mediante *diagrammi di Hasse*. Qui sotto vediamo tre esempi che hanno ciascuno qualcosa di interessante.

		
Reticolo N_5	Reticolo M_5	Algebra di Boole

Il secondo non è distributivo, il terzo è un'algebra di Boole, ma in entrambi tutti i percorsi da *a* ad *e* hanno la stessa lunghezza, e si può parlare di elementi allo stesso livello rispetto al minimo *e* ed al massimo *a*. Il primo non è *modulare*: i due percorsi da *a* ad e hanno lunghezze differenti e non si può parlare di livelli.

Descriviamo ora alcune nozioni ed alcune procedure che si ritrovano in ogni tipo di struttura algebrica con operazioni interne. Con un piccolo abuso di linguaggio e com'è consuetudine quando non vi siano ambiguità, le strutture algebriche saranno

identificate mediante i loro sostegni; per esempio, un gruppo $(G,\cdot,1_G,\sigma)$ sarà sovente denotato solo con G, e così via.

2.G. Sottostruttura. Sia (X, ·) una struttura algebrica. Un sottoinsieme Y di X si dice *chiuso* rispetto all'operazione se, ogni volta che si esegue l'operazione su elementi appartenenti ad Y, anche il risultato appartiene ad Y. In tal caso possiamo considerare l'operazione · ristretta ad Y ed ottenere la nuova struttura algebrica (Y, ·). Se l'operazione è *zeroaria*, cioè è un fissato elemento u∈X, affermare che Y è chiuso rispetto a tale operazione significa affermare che u∈Y.

Più in generale, data una struttura algebrica $(X,f_1,f_2,\ldots,f_r)$, una sua *sottostruttura* è costituita da un sottoinsieme Y di X, chiuso rispetto a tutte le operazioni di X, e dalle restrizioni ad Y delle operazioni di X. In tal caso, $(Y,f_1,f_2,\ldots,f_r)$ risulta una struttura dello stesso tipo di $(X,f_1,f_2,\ldots,f_r)$.

Si osservi che se non ci sono operazioni zeroarie, anche l'insieme vuoto è una sottostruttura.

Esempio 2.11. *Sottogruppo*. Se (G, ·) = $(G,\cdot,1_G,\sigma)$ è un gruppo, un sottogruppo è una struttura $(H,\cdot,1_G,\sigma)$, dove H è chiuso rispetto alle tre operazioni finitarie di G; in particolare H contiene 1_G e contiene il simmetrico di ogni suo elemento. Si ha così che $(H,\cdot,1_G,\sigma)$ è un gruppo e $1_H = 1_G$.

Per esempio, l'insieme degli interi pari 2**Z** dà luogo ad un sottogruppo di (**Z**, +). Più in generale, dato un gruppo (G, ·) ed un elemento a∈G, l'insieme $\langle a\rangle$ delle potenze di a costituisce un sottogruppo, detto *sottogruppo ciclico* generato da a.

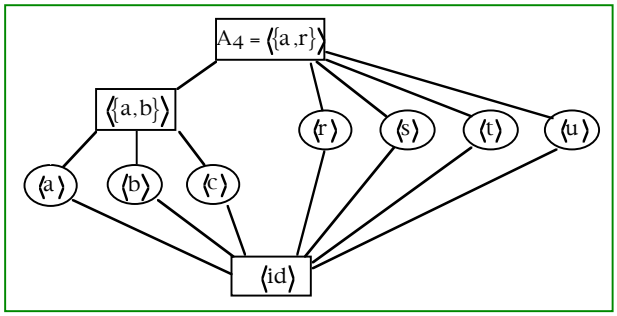
Ogni sottogruppo H di un gruppo G dà luogo a due partizioni di G, costituite rispettivamente dai sottoinsiemi Hg, g∈G, detti *laterali destri* di H, e gH, g∈G, detti *laterali sinistri* di H. Ciascuno di questi sottoinsiemi è equipotente ad H e quindi, denotato con [G:H] il numero dei laterali destri, si ha il seguente risultato, ben noto dai corsi di Algebra del triennio.

TEOREMA 2.12. (Lagrange). Per ogni sottogruppo H del gruppo G si ha |G| = |H|·[G:H]. Se poi G è un gruppo finito, |H| e [G:H] dividono |G|.

Come conseguenza immediata si ha che il periodo di ogni elemento di un gruppo finito G divide l'ordine di G. Inoltre, se G ha ordine primo, è necessariamente ciclico.

NOTA. Se G è un gruppo finito d'ordine n e k è un divisore di n, non è detto che ci sia un sottogruppo d'ordine k. Il più piccolo controesempio è il gruppo alterno A_4: ha ordine 12, ma non ha sottogruppi di ordine 6.

Un gruppo finito d'ordine n nel quale per ogni divisore k di n esiste un sottogruppo d'ordine k è detto *lagrangiano*. I gruppi abeliani ed il gruppo simmetrico S_4 lo sono.



Esempio 2.13. *Sottoanello*. Dato un anello $(A,+,\cdot,1_A)$= $(A,+,0_A,\sigma,\cdot,1_A)$, un sottoanello è costituito da un sottoinsieme B chiuso rispetto alle cinque operazioni finitarie di A, ed è a sua volta un anello. In particolare, usando la notazione abbreviata per i gruppi, (B, +) è un sottogruppo di (A, +) e $(B,\cdot,1_A)$ è un *sottomonoide* di $(A,\cdot,1_A)$. Ne segue che anche per i sottoanelli vale il teorema di Lagrange.

Esempio 2.14. Similmente, un *sottoreticolo* di un reticolo (R, $\vee$, $\wedge$) è costituito da un sottoinsieme chiuso rispetto alle due operazioni $\vee$, $\wedge$. Per esempio, l'insieme dei divisori di n è un sottoreticolo del reticolo $(\mathbf{N},\mathrm{mcm},\mathrm{MCD})$.

Per indicare che Y è una sottostruttura di X si scrive usualmente $Y \le X$. Si osservi che se H e K sono sottostrutture di X, con $H \subseteq K$, si ha anche $H \le K$; inversamente, se $K \le X$ e $H \le K$, si ha $H \subseteq K$ e $H \le X$.

LEMMA 2.15. Sia $(X,f_1,f_2,\ldots,f_r)$ una struttura algebrica e sia Ω un insieme di sottostrutture. Allora $Y = \bigcap_{H\in\Omega} H$ è una sottostruttura.

Dimostrazione. Per ogni $i\in\{1, 2, ..., r\}$ sia f_i operazione k -aria. Se k > 0, siano $x_1, ..., x_k\in Y$ e proviamo che $f(x_1, ..., x_k)\in Y$. Poiché $x_1, ..., x_k\in Y$, allora essi appartengono ad ogni $H \in \Omega$ e quindi, essendo H una sottostruttura di X, si ha $f(x_1, ..., x_k)\in H$. Ma allora $f(x_1, ..., x_k)\in \bigcap_{H\in\Omega} H$. Se k = 0, f_i è un elemento u di X: poiché ogni H è una sottostruttura, si ha $u\in H$, quindi $u\in Y$.

Pertanto, Y è chiuso rispetto a tutte le operazioni $f_1, \ldots, f_r$ ed è una sottostruttura.

Dal lemma precedente segue che l'insieme $\mathcal{L}(X)$ delle sottostrutture di una struttura X è chiuso rispetto alla intersezione.
Non è vero in generale per l'unione: nel monoide $(\mathbf{N}, +, 0)$ consideriamo i due sottomonoidi $2\mathbf{N}$ e $3\mathbf{N}$ costituiti dai pari e dai multipli di 3: l'intersezione è l'insieme $6\mathbf{N}$ dei multipli di 6 ed è un sottomonoide, mentre l'unione è {0, 2, 3, 4, 6, 8, 9, ...} che non è chiuso rispetto all'addizione.

Dato un sottoinsieme Y della struttura X, consideriamo l'intersezione $\langle Y \rangle$ di tutte le sottostrutture di X che contengono Y, e la chiamiamo *sottostruttura generata* da Y. Date ora due sottostrutture H e K di X, definiamo *sottostruttura somma* di H e K la sottostruttura $\langle H \cup K \rangle$ generata dall'unione insiemistica di H e K. Ne segue che $\mathcal{L}(X)$ è un reticolo, ed è *completo*, nel senso che ogni sottoinsieme non vuoto possiede estremi superiore ed inferiore. In particolare, questo reticolo ha per massimo X e per minimo l'intersezione di tutte le sottostrutture, che è il vuoto se non ci sono operazioni zeroarie. A partire quindi da ogni struttura algebrica è possibile costruire un reticolo, *il reticolo delle sottostrutture*. Esso non è in generale un sottoreticolo di $(\wp(x), \cup, \cap)$, poiché, come già detto, se H e $K \in \mathcal{L}(X)$ di solito si ha $H \cup K \neq \langle H \cup K \rangle$.

2.H. Congruenze e strutture quoziente. Data una struttura con una operazione binaria $(X, \cdot)$, una relazione d'equivalenza $\sim$ in X si dice *congruenza* rispetto a $\cdot$ se dati a, b, a', b' $\in$ X, dall'essere $a \sim a'$, $b \sim b'$ segue $a \cdot b \sim a' \cdot b'$. Indichiamo con [x] la classe di equivalenza di x, ossia $[x] = \{y \in X \mid y \sim x\}$ e consideriamo l'insieme quoziente $X/\sim$ costituito dalle classi di equivalenza. Definiamo tra le classi l'operazione seguente: per ogni a,b $\in$ X

$$[a] \cdot [b] = [a \cdot b] .$$

Otteniamo così una nuova struttura $(X/\sim, \cdot)$, detta *struttura quoziente* di X rispetto alla congruenza $\sim$. Si noti che vi è un epimorfismo tra $(X, \cdot)$ e $(X/\sim, \cdot)$: è la *proiezione canonica* $\pi : X \to X/\sim$ tale che $\pi(x) = [x]$ per ogni $x \in X$.

Se l'operazione in X possiede elemento neutro 1_X anche l'operazione quoziente lo possiede, ed è $[1_X]$. Inoltre, se x ha un simmetrico x', allora la classe [x] ha per simmetrica la classe [x'].

Tutto ciò si può ripetere in una struttura qualunque: una congruenza della struttura è una relazione d'equivalenza che è congruenza rispetto a tutte le operazioni della struttura. Si può allora costruire la struttura quoziente. Vediamo alcuni esempi.

Esempio 2.16. Data una congruenza ~ in un gruppo G, la classe K contenente l'elemento neutro 1_G è un sottogruppo di G ed è *normale* in G, ossia tale che $\forall x \in G$, posto $xK = \{xk \mid k \in K\}$ e $Kx = \{kx \mid k \in K\}$, si ha xK = Kx. Non solo, ma la classe di equivalenza [x] di x coincide con Kx e la congruenza data coincide con la relazione $x \Re y \Leftrightarrow x \cdot y^{-1} \in K$. Per indicare che K è un sottogruppo normale in G si scrive $K \lhd G$.

Inversamente, per ogni sottogruppo $K \lhd G$ la relazione $x \Re y \Leftrightarrow x \cdot y^{-1} \in K$ è una congruenza, di cui K è la classe contenente l'elemento neutro e per ogni x si ha [x] = Kx. Pertanto, **le congruenze nei gruppi sono completamente descritte dai sottogruppi normali**. Il gruppo quoziente di G rispetto alla congruenza associata al sottogruppo normale K si denota con G/K. Nel caso abeliano, tutti i sottogruppi sono normali, per cui si può determinare il gruppo quoziente rispetto ad ogni sottogruppo.

Esempio 2.17. Nel gruppo (**Z**, +) si considerino il numero m ≥ 1 ed il sottogruppo ciclico $\langle m \rangle$ generato da m ed indicato di solito con m**Z**. La relazione d'equivalenza associata è la *congruenza modulo m*: si ha $x \equiv y$ (mod m) se e solo se x-y∈m**Z**, ovvero se e solo se x-y è multiplo di m. Le classi d'equivalenza sono le *classi di resti modulo m*. L'insieme quoziente **Z**/m**Z** ha come elementi le classi [0], [1],..., [m-1]. Si può verificare inoltre che la congruenza modulo m in **Z** è una congruenza anche rispetto alla moltiplicazione; essa dunque consente di ottenere l'anello quoziente **Z**/m**Z**, che risulta isomorfo all'anello $\mathbf{Z}_m$.

Esempio 2.18. Nel gruppo (**R**,+) si consideri il sottogruppo ciclico $\langle 2\pi \rangle \leq (\mathbf{R}, +)$, generato da 2π = 6,28.... Gli elementi del gruppo quoziente sono le classi $\alpha + \langle 2\pi \rangle$, $\alpha \in [0, 2\pi[$; in particolare, [0] = [2π] = [4π] = ... In qualche testo è usato questo procedimento per definire gli angoli o le rotazioni, poiché l'operazione quoziente corrisponde alla somma di angoli o alla composizione di rotazioni con lo stesso centro.

Esempio 2.19. In un anello $(A, +, \cdot, 1_A)$ un sottoinsieme I si dice *ideale* se è un sottogruppo di (A,+) e se per ogni i∈I e per ogni x∈A si ha x·i∈I e i·x∈I.

La relazione x ~$_I$ y ⇔ x-y∈I è una congruenza nell'anello, nella quale la classe di 0_A è I e la classe di un elemento a è a+I = {a+i | i∈I}. Inversamente, data una congruenza ~ in A, posto I = $[0_A]_{\sim}$, I è un

ideale e si ha $\sim = \sim_I$. Pertanto, **le congruenze negli anelli sono completamente descritte dagli ideali**. L'anello quoziente di A rispetto alla congruenza associata all'ideale I si denota con A/I .

NOTE. a) Se un anello è integro, non è detto che un suo anello quoziente lo sia. Per esempio, l'anello **Z** è integro ma, se m non è primo, $\mathbf{Z}_m$ non lo è. Per altro, se m è primo, è ben noto che $\mathbf{Z}_m$ è addirittura un campo.

b) Un ideale I dell'anello $\left(A, +, \cdot, 1_A\right)$ di solito non è un sottoanello, perché non contiene l'unità 1_A. Se infatti $1_A \in I$, allora $\forall x \in A,\ x = x \cdot 1_A \in I \Rightarrow A \subseteq I$ e quindi I = A.

2.I. Omomorfismi e isomorfismi. Date due strutture (X, *) e (Y, ·), si chiama *omomorfismo* una funzione $\varphi : X \to Y$ tale che per ogni coppia a, b di elementi di X sia $\varphi\left(a * b\right) = \varphi\left(a\right) \cdot \varphi\left(b\right)$. Un omomorfismo biiettivo si chiama *isomorfismo*. In tal caso, anche l'inversa φ^{-1} di φ è un isomorfismo e le due strutture differiscono solo per il nome degli oggetti ed i simboli usati per descriverli, ma sono essenzialmente coincidenti.

Nozioni analoghe si danno per operazioni finitarie qualsiasi; in particolare, un omomorfismo rispetto ad operazioni zeroarie u∈X e v∈Y deve portare u in v; rispetto ad operazioni unarie f in X e h in Y, si deve avere $\Phi\left(f(x)\right) = h\left(\Phi(x)\right)$ per ogni x∈X. Definiamo *omomorfismo* tra due strutture algebriche $\left(X, f_1, f_2, \ldots, f_r\right)$ e $\left(Y, g_1, g_2, \ldots, g_r\right)$ dello stesso tipo, una funzione $\varphi : X \to Y$ tale che sia omomorfismo tra (X, f_i) e (Y, g_i) per ogni i = 1, 2,.., r.

Un omomorfismo suriettivo si chiama *epimorfismo* e in tal caso si dice che Y è *immagine omomorfa* di X. Un omomorfismo iniettivo si chiama *monomorfismo* o immersione di X in Y, e Y si chiama *estensione* di X. Un omomorfismo biiettivo si chiama *isomorfismo*. Vale allora il seguente teorema:

TEOREMA 2.20 (teorema fondamentale di omomorfismo). Date due strutture algebriche dello stesso tipo X ed Y ed un omomorfismo $\varphi : X \to Y$, si ha:

a) L'immagine $\Phi(X)$ è una sottostruttura di Y.

b) Posto in X, $x_1 \sim x_2 \Leftrightarrow \varphi(x_1) = \varphi(x_2)$, allora $\sim$ è una congruenza in X e quindi X/$\sim$ è una struttura dello stesso tipo di X.

c) La proiezione canonica $\pi : X \to X/\sim$, definita da $\pi(x) = [x]_\sim$, è un epimorfismo.

d) La funzione $\Phi : X/\sim \to Y$, $\Phi : [x]_\sim \mapsto \varphi(x)$, è ben definita, è un monomorfismo ed è l'unica tale che $\varphi = \Phi \circ \pi$.

Dal teorema precedente segue che Φ è un isomorfismo tra X/$\sim$ e φ(X). Se quindi φ è un epimorfismo, allora che Φ è un isomorfismo tra X/$\sim$ ed Y.

Si noti che una funzione che sia omomorfismo rispetto ad una operazione può non esserlo rispetto ad altre. Ciò accade per esempio nel caso dei monoidi: un omomorfismo rispetto all'operazione binaria non porta necessariamente l'elemento neutro del dominio nell'elemento neutro del codominio. Pertanto, un omomorfismo tra due monoidi $(M, \cdot, 1_M)$ ed $(H, *, 1_H)$ è una funzione $f : M \to H$ tale che

$$\begin{cases} \forall x, y \in M, f(x \cdot y) = f(x) * f(y) \\ f(1_M) = 1_H \end{cases}$$

Invece, nel caso dei gruppi, una funzione che sia omomorfismo rispetto all'operazione binaria lo è automaticamente rispetto all'operazione zeroaria e a quella unaria. Questo giustifica l'uso della notazione abbreviata $(G, \cdot)$ per indicare un gruppo.

Di conseguenza, nel caso degli anelli con unità è sufficiente che la funzione sia omomorfismo rispetto all'addizione, alla moltiplicazione ed all'elemento neutro moltiplicativo. Quest'ultima condizione non è necessaria nel caso di anelli più generali o in quello dei campi. Per questo un campo si denota solo con $(F, +, \cdot)$.

Esempio 2.21. Un esempio di omomorfismo tra anelli: la funzione $r_m : \mathbf{Z} \to \mathbf{Z}_m$ definita da: $r_m(x)$ = resto della divisione di x per m, è un epimorfismo.

Esempio 2.22. La funzione esponenziale $f(x) = e^x$ è un isomorfismo tra il gruppo $(\mathbf{R}, +)$ ed il gruppo moltiplicativo ($\mathbf{R}^+$, $\cdot$) dei numeri reali strettamente positivi. Infatti la funzione f è una biiezione e per ogni $x,y \in R$ si ha: $f(x+y) = e^{x+y} = e^x e^y = f(x)f(y)$.
I gruppi ($\mathbf{R}$, +) ed ($\mathbf{R}^+$, $\cdot$) sono dunque isomorfi.

Esempio 2.23. Sia $(M, *, 1_M)$ un monoide e sia $(M^M, \circ, id_M)$ il monoide delle funzioni su M. Associamo ad ogni elemento $a \in M$ la funzione $\tau_a : M \to M$, $\tau_a : x \mapsto a * x$. La funzione $\rho : M \to M^M$, $\rho : a \mapsto \tau_a$, è un monomorfismo di monoidi. Ogni monoide, pertanto, è isomorfo ad un monoide di funzioni.

Esempio 2.24. Sia G un gruppo e sia S_G il gruppo simmetrico sull'insieme sostegno di G. Associamo ad ogni elemento $a \in G$ la funzione $\tau_a : G \to G$, $\tau_a : x \mapsto a \cdot x$. Si prova subito che $\tau_a \in S_G$. La funzione $\rho : G \to S_G$, $\rho : a \mapsto \tau_a$, è un monomorfismo di gruppi. Infatti, per ogni a, b∈G ed x∈G si ha:

$$\rho(ab)(x) = \tau_{ab}(x) = (ab)x = a(bx) = \tau_a(\tau_b(x)) = (\tau_a \circ \tau_b)(x) = (\rho(a) \circ \rho(b))(x)$$

da cui segue $\rho(ab) = \rho(a) \circ \rho(b)$. Inoltre, per ogni a, b, x∈G, se $\rho(a) = \rho(b)$ si ha:

$$\rho(a) = \rho(b) \Rightarrow \rho(a)(1_G) = \rho(b)(1_G) \Rightarrow a \cdot 1_G = b \cdot 1_G \Rightarrow a = b,$$

quindi ρ è iniettiva.

Abbiamo così dimostrato il **Teorema di Cayley**: ogni gruppo è isomorfo ad un gruppo di permutazioni sul suo insieme sostegno.

Esempio 2.25. Un'applicazione f tra due insiemi ordinati (X, ≤) ed (Y, ≤) è detta *(monotona) crescente* se $\forall x, x' \in R,\ x \le x' \Rightarrow f(x) \le f(x')$. In particolare, siano $(R, \vee, \wedge)$ ed $(S, \vee, \wedge)$ due reticoli. Allora

a) Ogni omomorfismo di reticoli $f : R \to S$ è crescente

b) Un'applicazione biiettiva $f : R \to S$ è un isomorfismo di reticoli se e solo se f ed f^{-1} sono entrambe crescenti, ossia $\forall x, x' \in R,\ x \le x' \Leftrightarrow f(x) \le f(x')$

Esempio 2.26. Ogni reticolo $(R, \vee, \wedge)$ ha il *duale* $(R, \wedge, \vee)$ ottenuto scambiando le due operazioni. Un isomorfismo tra un reticolo $(R, \vee, \wedge)$ ed il duale di un altro reticolo $(S, \vee, \wedge)$ è detto *isomorfismo inverso* tra R ed S: esso è caratterizzato dall'essere una funzione *decrescente* insieme con la sua inversa.

Può accadere che un reticolo sia isomorfo al proprio duale, ed in tal caso è detto *autoduale.* Un esempio è costituito dalle algebre di Boole: l'isomorfismo è dato dall'applicazione che ad ogni elemento associa il complementare.

Per provare che due strutture dello stesso tipo sono isomorfe occorre trovare una biiezione che sia un isomorfismo tra di esse. Per provare che non lo sono occorre invece dimostrare che un tale isomorfismo non può esistere. La via seguita normalmente è esibire una proprietà posseduta da una di esse e non dall'altra.

Esempio 2.27. ($\mathbf{Q}$, +) e ($\mathbf{Q}^+$, ·) non sono gruppi isomorfi: infatti nel primo gruppo, dati $x \in \mathbf{Q}$, $x \neq 0$, ed $n \in \mathbf{N}$, $n > 0$, esiste sempre y tale che $ny = x$. Invece ($\mathbf{Q}^+$, ·) non possiede questa proprietà, che tradotta in notazione moltiplicativa diviene: "dati $x \in \mathbf{Q}^+$, $x \neq 1$, ed $n \in \mathbf{N}$, $n > 0$, esiste $y \in \mathbf{Q}^+$, tale che $y^n = x$". Pertanto questi due gruppi, a differenza di ($\mathbf{R}$, +) ed ($\mathbf{R}^+$, ·), non sono isomorfi.

Nel caso particolare di un omomorfismo $f : G \to H$ fra i due gruppi G ed H, la congruenza $\sim_f$ dà luogo in G ad un sottogruppo normale $K = \operatorname{Ker} f$, detto *nucleo* di f, che costituisce la classe dell'elemento neutro. Più esplicitamente, si ha $\operatorname{Ker} f = \left\{ x \in G \,\middle|\, f(x) = 1_H \right\}$. Le altre classi sono i suoi laterali, così che il teorema 2.20 si riformula in modo riassuntivo come segue, con una piccola aggiunta:

TEOREMA 2.28. Dati due gruppi G ed H ed un omomorfismo $f : G \to H$ tra di essi:

a) l'immagine Im f è un sottogruppo di H;

b) il *nucleo* $\operatorname{Ker} f$ è un sottogruppo normale in G;

c) $G/\operatorname{Ker} f$ è isomorfo ad Im f. (L'isomorfismo è definito da: $F : x\operatorname{Ker} f \mapsto f(x)$;

d) f è un monomorfismo se e solo se $\operatorname{Ker} f = \{1_G\}$.

Esempio 2.29. Sia K un campo e sia $SL_n(K)$ l'insieme delle matrici quadrate di ordine n con determinante 1. Per il teorema di Binét, il determinante è un omomorfismo dal gruppo $GL_n(K)$ al gruppo moltiplicativo K^* del campo K. Il suo nucleo è ovviamente $SL_n(K)$, che risulta così un sottogruppo normale. L'immagine è, come si vede facilmente, tutto K^*, per cui $GL_n(K)/SL_n(K) = K^*$.

Nel caso degli anelli, la formulazione del teorema fondamentale di omomorfismo è sostanzialmente simile a quella dei gruppi, solo che Ker f è ora un ideale. Si ha così:

TEOREMA 2.30. Dati due anelli A e B ed un omomorfismo $f : A \to B$:

a) l'immagine Im f è un sottoanello di B;

b) il *nucleo* $\operatorname{Ker} f = \left\{ x \in A \,\middle|\, f(x) = 0_H \right\}$ è un ideale di A;

c) $A/\operatorname{Ker} f$ è isomorfo ad Im f. (L'isomorfismo è definito da: $F : x\operatorname{Ker} f \mapsto f(x)$;

d) f è un monomorfismo se e solo se $\operatorname{Ker} f = \{0_G\}$.

2.L. Il monoide degli endomorfismi ed il gruppo degli automorfismi. Gli omomorfismi tra una struttura algebrica $(X, f_1, f_2, \ldots, f_r)$ e se stessa si chiamano *endomorfismi,* e formano il sottomonoide End(X) del monoide $(X^X, \circ, id_X)$ delle funzioni da X ad X. Gli isomorfismi tra la struttura X e se stessa si chiamano *automorfismi,* e formano il gruppo delle unità di End(X). Tale gruppo si denota di solito con Aut(X), è un sottogruppo del gruppo simmetrico S_X e viene detto *automorfo* di X. Dunque, a partire da ogni struttura algebrica è possibile costruire un gruppo, il gruppo degli automorfismi della struttura. Vediamo alcuni esempi.

Esempio 2.31. Aut(**Z**, +) possiede due soli elementi: l'identità e la funzione σ che ad ogni x associa l'opposto -x. Invece, Aut(**Z**, +, ·, 1) è costituito solo dall'identità.

Esempio 2.32. Il campo reale ha solo l'automorfismo banale. Infatti, per cominciare, se f è un automorfismo del campo **R**, allora f(1) = 1, quindi per ogni $m \in \mathbf{N}$ si ha $f(m) = f\left(\sum_{i=1}^{m} 1\right) = \sum_{i=1}^{m} f(1) = m \cdot 1 = m$. Ma allora si ha anche f(-m) = -m e, in definitiva, per ogni numero razionale $\frac{m}{n}$ si ha $f\left(\frac{m}{n}\right) = \frac{f(m)}{f(n)} = \frac{m}{n}$ e quindi f induce l'identità sui razionali. Inoltre, $\forall x > 0 \Rightarrow \exists y \in \mathbf{R}$ tale che $x = y^2$, quindi $f(x) = f\left(y^2\right) = \left(f(y)\right)^2 \Rightarrow f(x) > 0$. Pertanto, f conserva la positività e quindi l'ordinamento di **R**. Ne viene che, essendo **Q** denso in **R**, allora f è l'identità anche su **R**.

2.M. Prodotto diretto. Siano date due strutture algebriche che denoteremo con (G, *) ed (H, •). Sul loro prodotto cartesiano $G \times H$ definiamo la seguente operazione: per ogni $g_1, g_2 \in G$, $h_1, h_2 \in H$,

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \bullet h_2).$$

La struttura $(G \times H, \cdot)$ è detta *prodotto diretto* delle due strutture date. Se si usa la notazione additiva, si parla di *somma diretta*.

La stessa nozione si può dare per due strutture qualunque, purché dello stesso tipo, e si può estendere ad un numero $n \geq 2$ di strutture dello stesso tipo.

Si verifica facilmente che se le due operazioni $*$ e $\bullet$ possiedono una stessa proprietà (associativa, commutativa, idempotenza, assorbimento, legge di cancellazione, elemento neutro), anche l'operazione $\cdot$ la possiede, e lo stesso vale per le proprietà distributive. In particolare, se G ed H sono strutture algebriche dello stesso tipo (semigruppi, monoidi, gruppi, anelli, reticoli) anche il prodotto diretto lo è. Altre proprietà invece non si conservano: l'essere ciclico (per un gruppo), la legge d'annullamento del prodotto o l'essere campo (per gli anelli).

OPERAZIONI ESTERNE O AZIONI. Oltre alle operazioni binarie "interne" $* : X \times X \to X$, ossia nelle quali i termini ed il risultato appartengono allo stesso insieme X, è possibile considerare anche operazioni "esterne" *sinistra* $\mu : \Omega \times X \to X$ o *destra* $\mu : X \times \Omega \to X$, nelle quali un termine appartiene ad un insieme Ω eventualmente diverso da quello, X, al quale appartengono l'altro termine ed il risultato. Sovente una operazione esterna di questo tipo è anche detta *azione sinistra* o rispettivamente *destra* di Ω su X.

Fissato $\omega \in \Omega$, posto $\omega x = \mu(x,\omega)$, si ottiene la funzione $\tau_\omega : X \to X, \tau_\omega : x \mapsto \omega x$. Allora nasce una funzione $\rho_\mu : \Omega \to X^X$, $\rho_\mu : \omega \to \tau_\omega$, che viene spesso chiamata *rappresentazione* di Ω.

Inversamente, ad ogni applicazione $\rho : \Omega \to X^X$ si può associare un'azione destra μ_ρ di Ω su X ponendo $\mu_\rho(x,\omega) = \rho(\omega)(x)$.

Dall'insieme X l'azione di Ω passa all'insieme $\wp(X)$ ponendo per ogni $Y \subseteq X$, per ogni $\omega \in \Omega$, $\mu(\omega,Y) = \{\mu(\omega,y) \mid y \in Y\}$.

NOTA. Se su Ω o su X c'è un qualche tipo di struttura algebrica, si richiede di norma che l'azione sia *compatibile* con la struttura. In tal caso, anche la rappresentazione associata dovrà essere un omomorfismo oppure avere immagine costituita da endomorfismi.

Esempio 2.33. Spazi vettoriali: abbiamo un campo K nel ruolo di Ω ed un gruppo abeliano (in notazione additiva) V in quello di X. In tal caso, l'azione di K su V, indifferentemente destra o sinistra, viene denotata come un prodotto kv, che deve avere le ben note proprietà di compatibilità con le operazioni di V e di K:

(i) $\forall h,k \in K, \forall v \in V, \begin{cases} (h+k)v = hv + kv \\ h(kv) = (hk)v \end{cases}$

(ii) $\forall k \in K, \forall v,w \in V, k(v+w) = kv + kw$

(iii) $\forall v \in V,\ 1_K v = v$

Lo spazio vettoriale ottenuto si denota spesso con V(K).

In uno spazio vettoriale vale la *legge d'annullamento del prodotto*:

$$kv = 0_V \Leftrightarrow k = 0_K \text{ oppure } v = 0_V$$

Inoltre, l'opposto -v di v è dato dal prodotto $(-1_K)v$.

Una nozione fondamentale per uno spazio vettoriale V(K) è quella ben nota di *dimensione*, definita come il numero di elementi di una sua qualunque *base*. E' inoltre ben noto che se $\{e_1, e_2 \ldots, e_n\}$ è una base, ogni elemento $v \in V$ si esprime in uno ed un solo modo nella forma $\sum_{i=1}^{n} \xi_i e_i$, con $\xi_i \in K$ per ogni $i = 1, \ldots, n$.

Oltre agli spazi vettoriali reali o complessi, vediamo altri esempi. Sia p un numero primo. Un gruppo abeliano (V,+) si dice *p-gruppo abeliano elementare* se ogni elemento diverso da 0_V ha periodo p.

Si può definire su V una struttura di spazio vettoriale sul campo K = $\mathbf{Z}_p$ ponendo: per ogni k∈$\mathbf{Z}_p$ e per ogni v∈V, $kv = \underbrace{v + v + \ldots + v}_{k}$.

Si osservi che se k' è un intero tale che k' = k+pq per un opportuno q∈**Z**, allora, per le proprietà delle potenze in notazione additiva (= multipli interi) si ha:

$$k'v = (k+pq)v = kv + q(pv) = kv + 0_V = kv$$

Pertanto, dette $+_p$ e $\times_p$ le operazioni in $\mathbf{Z}_p$, si ha:

$$\forall h,k \in \mathbf{Z}_p,\ \forall v \in V,\ \begin{cases} (h +_p k)v = (h+k)v \\ (h \times_p k)v = (h \cdot k)v \end{cases}$$

Allora, la verifica delle proprietà richieste nella definizione di spazio vettoriale è immediata, per le proprietà dei multipli interi. Ne segue che se V ha dimensione n su $\mathbf{Z}_p$ e se $\{e_1, e_2 \ldots, e_n\}$ è una base, allora ogni elemento $v \in V$ si esprime in uno ed un solo modo nella forma $\sum_{i=1}^{n} \xi_i e_i$, con $\xi_i \in \mathbf{Z}_p$ per ogni $i = 1, \ldots, n$. Dunque, la corrispondenza $v \mapsto (\xi_1, \ldots, \xi_n)$ definisce una biiezione tra V e $(\mathbf{Z}_p)^n$ e quindi V ha p^n elementi.

Esempio 2.34. Si è provato già che se A è un dominio d'integrità la sua caratteristica è 0 oppure un primo p. In quest'ultimo caso ogni elemento non nullo ha periodo p. Pertanto, il gruppo additivo (A,+) è

un p-gruppo abeliano elementare e diviene uno spazio vettoriale sul campo $\mathbf{Z}_p$. Se poi A è finito, allora per quanto precede, esiste un numero intero n ≥ 1 tale che A ha p^n elementi. In questo caso, però, A è un campo. Infatti, sia a un elemento non nullo; la funzione $x \mapsto a \cdot x$ è iniettiva, perché a è cancellabile, quindi, essendo A finito, è anche suriettiva. Ma allora 1_A appartiene alla sua immagine, ossia esiste $x_0 \in A$ tale che $a \cdot x_0 = 1_A$ e quindi a ha l'inverso.

Esempio 2.35. - Siano K ed F due campi, con F *sottocampo* di K. Allora è definita in modo naturale la moltiplicazione di F per K, che trasforma K in un F-spazio vettoriale. Se la dimensione di K come F−spazio vettoriale è n e se $\{e_1, e_2 \ldots, e_n\}$ è una base, allora ogni elemento $v \in K$ si esprime in uno ed un solo modo nella forma $\sum_{i=1}^{n} \xi_i e_i$, con $\xi_i \in F$ per ogni $i = 1, \ldots, n$. Dunque, la corrispondenza $v \mapsto (\xi_1, \ldots, \xi_n)$ definisce una biiezione tra K e F^n. Ciò vale in particolare se K = F. In tal caso la dimensione è 1 ed una base è $\{1_F\}$. Ovviamente i due campi K ed F hanno la stessa caratteristica. Se sono finiti e la caratteristica è p, posto $|F| = p^h$, $|K| = p^k$, allora $p^k = (p^h)^n = p^{hn}$. In particolare, h divide k.

Esempio 2.36 A-moduli su un anello: si ha un anello commutativo A nel ruolo di Ω ed un gruppo abeliano (in notazione additiva) V in quello di X, con le stesse proprietà (i), (ii), (iii), ma con risultato finale, detto A-modulo, un poco diverso dal caso degli spazi vettoriali; inoltre, se A non è commutativo, la destra e la sinistra non sono indifferenti, per cui avremo A-moduli destri ed A-moduli sinistri.
Come esempi abbiamo gli **Z**-*moduli*: ogni gruppo abeliano (moltiplicativo) G diventa uno **Z**−modulo se poniamo $\mu(g, n) = g^n$ (oppure, in notazione additiva, $\mu(g, n) = ng$). Non è detto che valga la legge d'annullamento del prodotto: $ng = 0_G$ implica n = 0 solo se g ha periodo infinito.
Inoltre, ogni anello A è interpretabile come A-modulo. Consideriamo il gruppo additivo (A,+) dell'anello. La moltiplicazione "esterna" di A per A è rispettivamente:

$\forall a \in A, \forall x \in A, \mu(a, x) = a \cdot x$ (A-modulo sinistro)

$\forall a \in A, \forall x \in A, \nu(x, a) = x \cdot a$ (A-modulo destro)

e soddisfa ovviamente le proprietà richieste. Dunque, l'anello A è un A-modulo destro o sinistro su se stesso.

Esempio 2.37. Algebre associative. Possiamo considerare il caso di un campo K come Ω ed un anello (anche non associativo) A come X. In tal caso, oltre alle richieste (i), (ii), (iii), che fanno sì che (A,+) divenga uno spazio vettoriale, avremo anche la proprietà seguente:

(iv) $\forall k \in K, \forall v, w \in A, k(v \cdot w) = (kv) \cdot w = v \cdot (kw)$

La struttura ottenuta è detta *algebra* KA. Se l'anello A è associativo, l'algebra è detta *associativa.* Esempi sono l'algebra delle funzioni da E⊆R ad R con le operazioni punto per punto, l'algebra delle matrici quadrate d'ordine n ad elementi reali ecc.

Esempio 2.38. Azione di un gruppo su un insieme. Ne abbiamo già parlato nel modulo di Elementi di Geometria. Siano G un gruppo ed X un insieme. Chiamiamo *azione di G su X* ogni applicazione $\mu: X \times G \to X$ tale che:

a) per ogni $x \in X$, $\mu(x, 1_G) = x$.

b) per ogni $x \in X$ e $g_1, g_2 \in G$, $\mu(x, g_1 g_2) = \mu(\mu(x, g_1), g_2)$.

Scriveremo x^g anziché $\mu(x,g)$. Con questa notazione, le due proprietà a) e b) diventano rispettivamente:

a) $x^{1_G} = x$,

b) $x^{g_1 g_2} = \left(x^{g_1}\right)^{g_2}$.

Una *rappresentazione di G come gruppo di permutazioni su X* è un omomorfismo $\rho: G \to S_X$. Una rappresentazione si dice *fedele* se è iniettiva. Come nel caso generale, ad ogni azione $\mu: X \times G \to X$ si può associare una rappresentazione ρ_μ e ad ogni rappresentazione $\rho: G \to S_X$ si può associare un'azione μ_ρ. Pertanto, si può parlare indifferentemente in termini di azione o di rappresentazione.

Un caso particolare è ***l'azione per moltiplicazione a destra***. Sia G un gruppo e sia X = G. Per ogni $x, g \in G$ poniamo $\mu(x, g) = xg$. Si ha un'azione fedele di G su se stesso e G è isomorfo alla sua immagine in S_G. Questo è quanto affermato dal *teorema di Cayley*.

Un altro esempio è ***l'azione per coniugio*** di un gruppo G su se stesso. L'operazione esterna è: $\mu(x, g) = g^{-1}xg$. Allora, la funzione $f_g : G \to G, f_g(x) = \mu(x, g) = g^{-1}xg$ è un automorfismo di G, detto *automorfismo interno* di G. Possiamo supporre quindi $\rho_\mu : G \to \mathrm{Aut}(G)$. Di più, si può dimostrare facilmente che ρ_μ è un omomorfismo di gruppi, il cui nucleo è $Z(G) = \left\{ g \in G \mid \forall x \in G,\ g^{-1}xg = x \right\}$, che è detto *centro* di G ed è un sottogruppo normale in G. L'immagine si denota con Inn(G) ed è un sottogruppo di Aut(G), detto *gruppo degli automorfismi interni.* Pertanto, $\mathrm{Inn}(G) \cong G / Z(G)$.

Anche alle strutture algebriche con operazioni esterne si possono applicare le nozioni generali già viste in precedenza.

2.G'. Sottostruttura: è un sottoinsieme chiuso rispetto a tutte le operazioni coinvolte, comprese le esterne. Naturalmente, l'insieme sostegno della struttura costituisce sempre una sottostruttura. Vediamo alcuni esempi:

Esempio 2.39. Un *sottospazio vettoriale* W di uno spazio vettoriale V su un campo K è un sottogruppo del gruppo (V, +), chiuso rispetto alla moltiplicazione esterna per K. In realtà, quest'ultima condizione implica che W sia chiuso rispetto allo zero ed agli opposti, dato che $0_K v = 0$ e -v = (-1_K)v, perciò è sufficiente per W l'essere non vuoto e chiuso rispetto all'addizione ed alla moltiplicazione esterna. Fra i sottospazi notiamo l'insieme dei *multipli secondo K* di un qualsiasi vettore v:

$$\mathrm{Span}(v) = \left\{ kv \;\middle|\; k \in K \right\}.$$

Esempio 2.40. Nel caso dell'azione per coniugio, un G-sottogruppo è chiuso rispetto all'azione per automorfismi interni, ossia è un sottogruppo K di G tale che $\forall x \in K, \forall g \in G,\ g^{-1}xg \in K$. Il seguente risultato è ben noto dai corsi di Algebra del triennio: un sottogruppo K di un gruppo G è un G-sottogruppo se e solo se $K \lhd G$.

Esempio 2.41. - Consideriamo il gruppo additivo (A,+) di un anello come A–modulo (destro o sinistro) rispetto all'anello stesso. La moltiplicazione esterna di A per A è, ricordiamolo, rispettivamente:

$\forall a \in A,\ \forall x \in A,\ \mu(a,x) = a \cdot x$ (A-modulo sinistro)

$\forall a \in A,\ \forall x \in A,\ \nu(x,a) = x \cdot a$ (A-modulo destro)

Gli A-sottomoduli sinistri sono sottogruppi I di (A,+) tali che $\forall a \in A, \forall i \in I,\ a \cdot i \in I$, e sono detti *ideali sinistri di A*.

Analogamente, gli A-sottomoduli destri sono sottogruppi I di (A,+) tali che $\forall a \in A, \forall i \in I,\ i \cdot a \in I$, e sono detti *ideali destri di A*.

Un *ideale* (bilatero) di A è contemporaneamente ideale destro e sinistro. Fra gli ideali (bilateri) si annoverano sempre A e $\{0_A\}$.

Anche nel caso di una struttura algebrica X con operazioni esterne si può dimostrare che l'intersezione di sottostrutture è una sottostruttura. Ne segue che per ogni sottoinsieme S di X è definita la *sottostruttura generata* come l'intersezione delle sottostrutture che lo contengono. In particolare, date due sottostrutture Y_1 ed Y_2, è definita la *sottostruttura congiungente* $\langle Y_1 \cup Y_2 \rangle$ come l'intersezione di tutte le sottostrutture che contengono $Y_1 \cup Y_2$. Si ha quindi il *reticolo delle sottostrutture*, che è completo anche in questo caso.

Esempio 2.42. I sottospazi di uno spazio vettoriale V su un campo K formano un reticolo. Se la dimensione è n, esso prende il nome di *spazio proiettivo n-1-dimensionale* su K. E' ben noto che se U e W sono sottospazi, denotato con Span(U ∪W) il sottospazio unione, si ha:

$$\text{Span}(U \cup W) = U+V = \left\{ u + v \;\middle|\; u \in U, w \in W \right\},$$

coincidente con la somma dei due gruppi additivi dei sottospazi. Si ha poi *l'identità di Grassman*:

$$\dim(U)+\dim(W) = \dim(U+V)+\dim(U \cap W)$$

2.H'. Congruenze e strutture quoziente. Dato un insieme X con operazione esterna per l'insieme Ω, una Ω-*congruenza* è una relazione d'equivalenza in X tale che, per ogni a, a'∈X, ω∈Ω, dall'essere $a \sim a'$ segue $a^\omega \sim a'^\omega$. Indichiamo come di consueto con [x] la classe di equivalenza di x. Possiamo porre $[x]^\omega = [x^\omega]$, e la definizione è corretta.

2.I'. Omomorfismi e isomorfismi. Dati due insiemi X ed Y con operazioni esterne sullo stesso insieme Ω, un Ω-omomorfismo tra di essi è una funzione $f : X \to Y$ tale che $\forall \omega \in \Omega,\ \forall x \in X,\ f(x^\omega) = f(x)^\omega$.

Naturalmente, se accanto all'operazione esterna ce ne sono delle interne, un Ω–omomorfismo deve essere omomorfismo anche rispetto ad esse. In particolare, ciò deve accadere per gli Ω-gruppi, gli spazi vettoriali, le algebre ecc.

Un Ω-isomorfismo è un Ω-omomorfismo biiettivo. L'insieme degli Ω-omomorfismi tra X ed Y si denota con $\text{Hom}_\Omega(X, Y)$.

Esempio 2.43. Nel caso di due spazi vettoriali V e W su un campo K, i K–omomorfismi sono le *applicazioni lineari*. Nel caso di due algebre A e B sullo stesso campo K i K-omomorfismi sono le applicazioni lineari che sono anche omomorfismi di anelli.

LEMMA 2.44. Siano X, Y, Z tre insiemi con operazioni esterne sullo stesso insieme Ω e siano $f : X \to Y$ e $g : Y \to Z$ due Ω-omomorfismi, allora anche $g \circ f : X \to Z$ è un Ω-omomorfismo.

Dimostrazione: $\forall \omega \in \Omega, \forall f, g \in \text{Hom}_\Omega(X, Y)$,

$$(g \circ f)(x^\omega) = g(f(x^\omega)) = g((f(x))^\omega) = (g(f(x)))^\omega = ((g \circ f)(x))^\omega$$

Come per le strutture con operazioni solo interne, vale il seguente teorema:

TEOREMA 2.45. (*Teorema fondamentale di omomorfismo*). Siano X ed Y due strutture dello stesso tipo, con operazioni esterne sullo stesso insieme Ω, ed f un Ω–omomorfismo tra di esse.

a) L'immagine Im f è una Ω-sottostruttura di Y.

b) La relazione $\sim_f$ in X così definita, per ogni a, b∈X:

$$a \sim_f b \text{ se } f(a) = f(b)$$

è una Ω-congruenza in X.

c) Detta [x] la classe d'equivalenza di x, la funzione $\pi : X \to X/\sim_f$ tale che $\pi(x) = [x]$, è un Ω-epimorfismo.

d) Ponendo F([x]) = f(x), è ben definita la funzione F da $X/\sim_f$ ad Y, la cui immagine coincide con quella di f e che risulta un Ω-monomorfismo.

e) Risulta: $f = F \circ \pi$, ed F è la sola funzione da $X/\sim_f$ ad Y che ha questa proprietà.

2.L'. Il monoide degli endomorfismi ed il gruppo degli automorfismi. Gli endomorfismi e gli automorfismi della struttura formano rispettivamente un monoide ed un gruppo rispetto alla composizione.

Esempio 2.46. *I gruppi generali lineari*. Sia K un campo e sia V un K-spazio vettoriale di dimensione finita n. Gli endomorfismi di V sono le applicazioni lineari dello spazio V in sé, che, come si sa dall'Algebra Lineare, fissata una base sono identificabili con le matrici d'ordine n sul campo K. L'automorfo dello spazio vettoriale V è pertanto isomorfo al gruppo $GL_n(K)$ delle matrici invertibili d'ordine n sul campo K. Tale gruppo viene detto *gruppo generale lineare*. Se $A \in GL_n(K)$, le sue righe formano una base (ordinata) dello spazio vettoriale K^n; viceversa, incolonnando i vettori di una base ordinata di K^n si ha una matrice invertibile. Pertanto, c'è una biiezione fra $GL_n(K)$ e l'insieme delle basi ordinate di K^n.

2.M'. Prodotti diretti. Anche nel caso delle algebre con operazioni esterne è definito il prodotto diretto.

In particolare, nel caso di spazi vettoriali, la dimensione del prodotto diretto (ossia somma diretta) è la somma delle dimensioni dei fattori.

Questi sono gli strumenti con cui affronteremo il resto del corso.