NOZIONI DI BASE DI ALGEBRA

Si presentano qui alcune nozioni di base di Algebra sugli insiemi e sulle strutture algebriche, a scopo di ripasso e di ripensamento in chiave generale.

Contenuto:

Introduzione: l'Algebra e la sua didattica (domande e risposte)

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*. Un esempio del primo tipo è, 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 *cm* può denotare la quantità di moto di un corpo di massa *m* alla velocità della luce *c*, data l'abitudine di omettere il segno di prodotto nei monomi.

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 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: sarebbe allora più evidente che tutto

quel che possiamo fare è riprodurlo e formare delle file: $a \quad aa \quad aaa \quad \ldots \quad aa\cdots a$, 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.

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 che cosa sia "la soluzione" di un'equazione di questo tipo;
d) in definitiva, non è 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, al momento in cui transita da quelle parti il primo veicolo, parte dal casello di Rimini nord, 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 avere $t \neq 0$ per l'univocità della soluzione. Più ci si riflette, più complicazioni si ritrovano …

Come evitare l'accusa di far parte di un U.C.C.S.?

Si tratta naturalmente dell'*Ufficio Complicazione Cose Semplici*. Un insegnamento che si chiama "Algebra elementare dal 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 che 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 tre considerazioni.

- 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 $\sum_{k=0}^{n} k^2 = \frac{n \cdot (n+1) \cdot (2n+1)}{6}$.

§ 1 – INSIEMI, RELAZIONI E FUNZIONI

Si può introdurre "ingenuamente" l'insiemistica dicendo che il termine *insieme* è sinonimo di collezione, raccolta, ecc. Ci si accorge ben presto di cadere però in alcune contraddizioni, come fu scoperto da subito, alla fine del 1800. Di qui la necessità di trattare la teoria degli insiemi secondo lo stesso schema seguito per esempio dalla geometria razionale e che comprende alcuni passi che riassumiamo per semplicità nell'elenco seguente.

- **Termini primitivi:** *insieme, elemento, appartenenza*. Tali termini vengono rappresentati con i seguenti simboli: gli insiemi con lettere maiuscole, tipo A, B, X,...; gli elementi con lettere minuscole: a, b, x, y,...; l'appartenenza dell'elemento x all'insieme X, con la scrittura $x \in X$; la non appartenenza, con $x \notin X$.

- **Assiomi o postulati:** si tratta di affermazioni (proposizioni) concernenti i termini primitivi (o altri termini da essi derivati), poste all'inizio della teoria, la cui funzione è tra l'altro quella di definire implicitamente i termini primitivi stessi. Per esempio, il *postulato di estensione* recita:

"*due insiemi cui appartengano gli stessi elementi sono lo stesso insieme*".

- **Definizione di nuovi termini:** ogni termine nuovo che viene introdotto deve essere specificato solo mediante termini già noti. Per esempio: dati due insiemi A e B, si dice che B è sottoinsieme di A, e si scrive $B \subseteq A$, se ogni elemento x appartenente a B appartiene anche ad A.

- **Dimostrazione di teoremi:** una proposizione (= affermazione) è "vera" (cioè fa parte della teoria) se è dedotta, mediante le regole della logica, dai postulati e dai teoremi precedentemente dimostrati. Non si tratta quindi di sperimentare (come in Fisica), di votare (come per le Leggi) o esibire documenti (come in Storia). Per esempio, l'affermazione:

"*Se A e B sono due insiemi e si ha* $A \subseteq B$ *e* $B \subseteq A$, *allora* $A = B$"

si può dimostrare mediante l'assioma di estensione nel modo seguente: da $A \subseteq B$, per definizione di sottoinsieme, segue che ogni elemento x appartenente ad A appartiene anche a B; da $B \subseteq A$ segue analogamente che ogni elemento di B appartiene anche ad A;

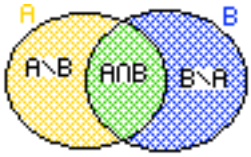
pertanto per ogni elemento x si ha $x \in A$ se e solo se $x \in B$; dal postulato di estensione segue allora $A = B$.

Il postulato di estensione ci consente di descrivere un insieme mediante l'elenco dei suoi elementi (se possibile), raccolti entro due parentesi graffe; per esempio $A = \{\text{Carlo, Anna, Luca}\}$. In generale però un tale elenco non è possibile, ed allora si ricorre ad una proprietà posseduta da tutti e soli gli elementi dell'insieme; per esempio,

$$A = \{x \mid x \text{ è un cittadino italiano}\}.$$

Quest'ultima procedura non sempre è atta a definire un insieme, ma la proprietà scelta deve essere compatibile con gli assiomi. Non ci sono invece problemi se gli oggetti x fra i quali scegliere quelli che soddisfano una data proprietà fanno già parte di un insieme. Più chiaramente, se P(x) è una certa proprietà ed X è un insieme, la scrittura $\{x \in X \mid P(x) \text{ è vera}\}$ definisce sempre un insieme, un sottoinsieme di X.

Una rappresentazione grafica degli insiemi è costituita dai ben noti "diagrammi di Venn". Essi possono costituire un valido strumento didattico per comunicare ed illustrare le varie nozioni, non per dimostrare teoremi.



Ora vediamo un elenco di procedure che definiscono nuovi insiemi a partire da insiemi dati. Si tenga presente che in alcuni casi è un postulato che il risultato sia un insieme.

- *Unione*. Siano A e B due insiemi. Poniamo $A \cup B = \{x \mid x \in A \text{ oppure } x \in B\}$.
- *Intersezione*. Siano A e B due insiemi. Poniamo $A \cap B = \{x \mid x \in A \text{ e } x \in B\}$.
- *Differenza*. Siano A e B due insiemi. Poniamo $A \setminus B = \{x \mid x \in A \text{ e } x \notin B\}$.
- *Differenza simmetrica*. Siano A e B due insiemi. Poniamo $A \Delta B = (A \setminus B) \cup (B \setminus A)$.
- *Insieme delle parti*. Sia X un insieme. Poniamo $\wp(X) = \{A \mid A \subseteq X\}$.
- *Complementare*. Dati un insieme X ed un suo sottoinsieme A, chiamiamo complementare di A in X l'insieme $A' = X \setminus A$.

Indichiamo infine con *ø l'insieme vuoto*, cioè privo di elementi. L'articolo "lo" è giustificato dal postulato di estensione: c'è un solo insieme vuoto.

Un procedimento per definire insiemi e per dimostrare l'eguaglianza di insiemi è costituito dalle tavole di verità. Esse sono relative al calcolo proposizionale e servono per calcolare il valore di verità di una proposizione ottenuta da proposizioni date mediante i connettivi logici "oppure", "e", "implica" ecc. Relativamente agli insiemi, le tavole di verità servono a verificare la proposizione "x∈X" per un dato elemento x ed un dato insieme X. Indichiamo con V la verità di tale proposizione e con F la sua falsità. La tavola seguente dimostra il seguente teorema:

"Per ogni coppia di insiemi A e B si ha AΔB = A∪B\A∩B",

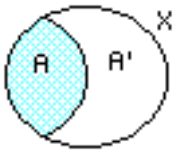
mostrando che per ogni x si ha x∈AΔB se e solo se x∈ A∪B\A∩B. Si noti che si dovrebbe scrivere (A∪B)\(A∩B), ma si può convenire che ∪ ed ∩ abbiano la precedenza su \.

x∈A	x∈B	x∈A∪B	x∈A∩B	x∈A\B	x∈B\A	x∈AΔB	x∈A∪B\A∩B
V	V	V	V	F	F	**F**	**F**
V	F	V	F	V	F	**V**	**V**
F	V	V	F	F	V	**V**	**V**
F	F	F	F	F	F	**F**	**F**

In modo analogo (ma con 8 righe) si possono dimostrare le seguenti proprietà:
Siano A, B, C tre insiemi. Allora A∪(B∪C)=(A∪B)∪C, A∪(B∩C)=(A∪B)∩(A∪C), A∩(BΔC)=(A∩B)Δ(A∩C), ecc.

Un altro esempio: sia X un insieme, siano A ⊆ X ed A' il complementare di A in X. Questa volta supponiamo in partenza x∈X, per cui avremo:

$x \in A$	$x \in A'$	$x \in A \cup A'$	$x \in A \cap A'$
V	F	**V**	**F**
F	V	**V**	**F**

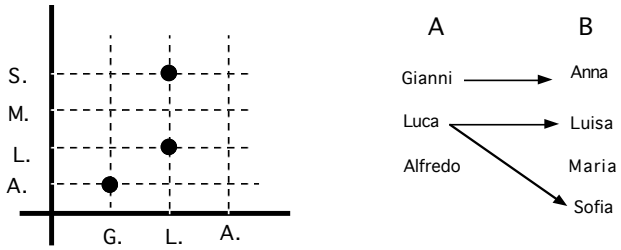


Si ha quindi A∩A' = Ø e A∪A' = X. Due insiemi si dicono *disgiunti* se hanno intersezione vuota. Un sottoinsieme ed il suo complementare sono sempre disgiunti.

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 $A\times B = \{(a,b) \mid a\in A, b\in B\}$ si chiama *prodotto cartesiano* di A e B. Chiamiamo *relazione* tra A e B ogni terna $(A, B, \Re)$ dove $\Re$ è un sottoinsieme del prodotto cartesiano $A\times B$. Per semplicità di linguaggio, se non ci sono ambiguità, spesso viene chiamata relazione l'insieme $\Re$.

Rappresentazioni grafiche delle relazioni sono i grafici cartesiani e i diagrammi a frecce. Per esempio, dati gli insiemi A = {Gianni, Luca, Alfredo} e B = {Luisa, Anna, Maria, Sofia}, la relazione $\Re$ = {(Gianni, Anna), (Luca, Luisa), (Luca, Sofia)} si può rappresentare come nella figura seguente.



Il rappresentare le coppie ordinate (a,b) mediante frecce a→b è usato soprattutto in un particolare tipo di relazioni: le funzioni (o applicazioni) tra insiemi.

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).

ESEMPIO 2.1 Indichiamo con **Z** l'insieme dei numeri interi relativi e con **Q** l'insieme dei numeri razionali relativi. Siano ora date le seguenti relazioni:

$F_1=\{(x,y) \mid x,y\in\mathbf{Z}, x = |y|\}$ (dove |y| indica il valore assoluto di y).

$F_2 = \{(x,y) \mid x,y\in\mathbf{Z}, y = |x|\}$.

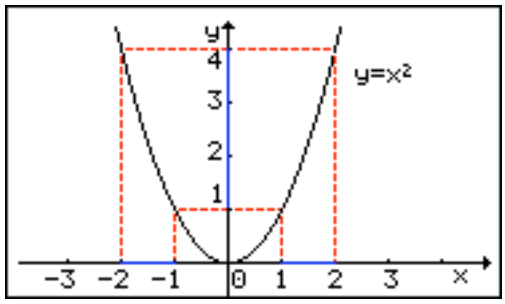
$F_3 = \{(x,y) \mid x\in\mathbf{Q}, y\in\mathbf{Z}, \exists q\in\mathbf{Z}, q\neq 0, x = y/q\}$.

Di queste tre relazioni, F_2 è una funzione, mentre F_1 non lo è perché esistono degli $x\in\mathbf{Z}$ che non hanno un corrispondente y: per esempio x = -1 non è il valore assoluto di alcun $y\in\mathbf{Z}$. Neppure F_3 è una funzione, poiché ogni numero razionale si può rappresentare con infinite frazioni diverse, quindi ad ogni

$x \in \mathbf{Q}$ corrispondono mediante F_3 infiniti numeri interi e non uno solo. Per esempio, ad $x = \frac{1}{2}$ corrisponde non solo 1, ma anche 2, perché per q = 4 si ha $\frac{2}{4} = \frac{1}{2} = x$, ecc.

Sia f:A→B una funzione e siano C⊆A, D⊆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, $f(A)$ si chiama immagine di f, e si denota spesso con Im 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 $\operatorname{Im} f = [0,+\infty[$.



Date due funzioni f:A→B e g:A→B, aventi quindi 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 se e solo se per ogni x∈A si ha 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 $x_2 \in A$, 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.

ESEMPI 1.2.A. - Sia f:**Z**→**Z** così definita: per ogni x∈**Z** sia f(x) = 2x. Allora f è una funzione iniettiva. Infatti se $f(x_1) = f(x_2)$ allora $2x_1 = 2x_2$, quindi $2x_1-2x_2 = 0$, da cui $2(x_1-x_2) = 0$ e, per la legge di annullamento del prodotto, essendo $2 \neq 0$ deve essere $x_1-x_2 = 0$, ossia $x_1 = x_2$. Questa funzione non è suriettiva. Infatti la sua immagine f(**Z**) contiene solo i numeri pari.

1.2.B. - Sia g:**Q**→**Z** così definita: per ogni x∈**Q** sia g(x) il massimo intero minore o uguale ad x. Per esempio g(-5/4) = -2. Questa funzione è suriettiva, poiché per ogni y∈**Z** esiste certamente almeno un x∈**Q** tale che y = g(x): per esempio il numero razionale rappresentato dalla frazione apparente y/1: g(y/1) = y. La funzione g non è iniettiva: per esempio, g(5/4) = 1 = g(6/5), ma 6/5 e 5/4 non sono lo stesso numero razionale.

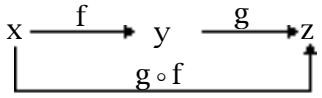
1.2.C. - Sia X un insieme qualsiasi e sia id_X:X→X così definita: per ogni x∈X sia $id_X(x) = x$. Questa funzione si chiama *identità su X* ed è una biiezione.

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)).



ESEMPIO 1.3. Siano **N** = {0, 1, 2, ...} l'insieme dei numeri naturali, f:**N**→**N** e g:**N**→**N** così definite: $f(x) = x^2+1$, $g(x) = 2x+3$. Allora:

$$g\circ f(x) = g(f(x)) = 2f(x)+3 = 2(x^2+1)+3 = 2x^2+5.$$

In questo particolare caso, i tre insiemi A, B, C della definizione coincidono con **N**, quindi si può calcolare anche f°g. Si ha: $f\circ g(x) = (2x+3)^2+1 = 4x^2+12x+10$. Si noti che $f\circ g \neq g\circ f$.

PROPOSIZIONE 1.4. Siano A, B, C, D quattro insiemi e siano f:A→B, g:B→C, h:C→D. Si ha $(h\circ g)\circ f = h\circ(g\circ f)$.

Dimostrazione. Per ogni x∈A siano y = f(x), z = g(y), t = h(z). Allora:

$((h\circ g)\circ f)(x) = (h\circ g)(f(x)) = (h\circ g)(y) = h(g(y)) = h(z) = t.$

Analogamente:

$(h\circ(g\circ f))(x) = h((g\circ f)(x)) = h(z) = t.$

Perciò per ogni x∈A si ha $((h\circ g)\circ f)(x) = ((h\circ(g\circ f))(x)$, dunque $(h\circ g)\circ f = h\circ(g\circ f)$.

PROPOSIZIONE 1.5. Siano A, B, C tre insiemi.

a) Se $f : A \xrightarrow[su]{1\text{–}1} B$ allora $f^{-1}\circ f = id_A$, $f\circ f^{-1} = id_B$.

b) Se $f : A \xrightarrow[su]{1\text{–}1} B$ e $g : B \xrightarrow[su]{1\text{–}1} C$ allora $g\circ f : A \xrightarrow[su]{1\text{–}1} C$.

c) Se f:A→B allora $id_B\circ f = f$ e $f\circ id_A = f$.

Dimostrazione a) per ogni a∈A, posto b = f(a) si ha $f^{-1}(b) = a$, dunque,

$$f^{-1}\circ f(a) = f^{-1}(f(a)) = f^{-1}(b) = a = id_A(a) \Rightarrow f^{-1}\circ f = id_A$$

Allo stesso modo si dimostra che $f\circ f^{-1} = id_B$.

b) Essendo g suriettiva, per ogni c∈C esiste b∈B tale che g(b) = c. Poiché anche f è suriettiva, esiste a∈A tale che f(a) = b. Allora $g\circ f(a) = c$ e quindi $g\circ f$ è suriettiva. Se si ha anche $g\circ f(a') = c$, allora

$$g(f(a')) = c = g(b) \Rightarrow f(a') = b = f(a) \Rightarrow a' = a.$$

Perciò $g\circ f$ è anche iniettiva.

c) Per ogni a∈A, posto b = f(a) si ha

$$id_B\circ f(a) = id_B(f(a)) = id_B(b) = b = f(a) \Rightarrow id_B\circ f = f$$

Analogamente si dimostra che $f\circ id_A = f$.

Definiamo ora due tipi importanti di relazioni tra un insieme e se stesso, le relazioni d'equivalenza e le relazioni d'ordine.

Relazioni d'equivalenza. Sia A un insieme. Sia $\mathfrak{R}$ una relazione su A, ossia un sottoinsieme di A×A. Scriviamo $x\mathfrak{R}y$ anziché $(x,y)\in\mathfrak{R}$. Ciò posto, $\mathfrak{R}$ si dirà *relazione d'equivalenza* se possiede le seguenti tre proprietà:

a) *Riflessiva*: per ogni x∈A si ha $x\mathfrak{R}x$.

b) *Simmetrica*: per ogni x,y∈A, se $x\mathfrak{R}y$ allora anche $y\mathfrak{R}x$.

c) *Transitiva*: per ogni x, y, z∈A, se $x\mathfrak{R}y$ ed $y\mathfrak{R}z$ allora anche $x\mathfrak{R}z$.

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

L'insieme quoziente A/~ 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∈A appartiene ad uno (ed uno solo) di essi.

ESEMPI 17.

1.7.A. - 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).

1.7.B. - 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, che considera accanto ai punti e alle rette del piano anche i punti e la retta impropri: in essa due rette hanno sempre uno ed un solo punto in comune, proprio o improprio. 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.

1.7.C. - In ogni insieme A sono relazioni d'equivalenza sia il prodotto cartesiano A×A, sia l'identità id_A. Per la proprietà riflessiva, ogni altra relazione d'equivalenza contiene id_A come sottoinsieme.

1.7.D. - Nell'insieme **Z** dei numeri interi relativi fissiamo un numero m e definiamo la seguente relazione: per ogni x,y∈**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∈**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∈**Z** si ha x-x = 0 = m·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 $[x]_m$ la classe d'equivalenza di x 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·q, ossia se e solo se x = y. Dunque la congruenza modulo 0 è l'identità. La congruenza modulo 1 è il prodotto cartesiano **Z**×**Z**. Negli altri casi vediamo quante sono le classi. Innanzitutto osserviamo che 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. Sappiamo che per ogni x∈**Z** esistono q, r∈**Z** tali che x = mq+r, con $0 \le r \le m$. Allora si ha x-r = mq, quindi $x \equiv r \pmod m$ e allora $[x]_m = [r]_m$.

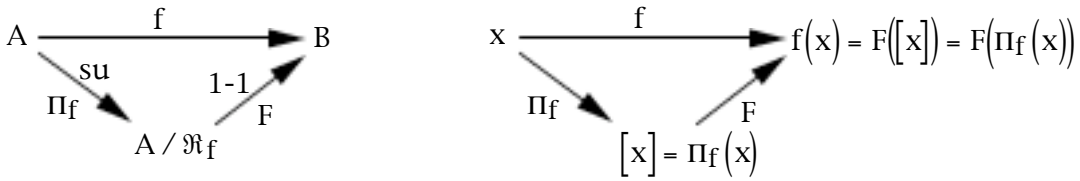
Allora si ha $\mathbf{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$. Le classi indicate entro le graffe sono tutte distinte; se infatti si ha $0 \le r \le s \le m$ non può accadere che sia s-r = mq, poiché $0 \le s-r \le s < m$. Allora $\mathbf{Z}_m$ ha esattamente

m elementi. In particolare, $\mathbf{Z}_2$ ha due soli elementi: $[0]_2$, costituita dai numeri pari e $[1]_2$, costituita dai numeri dispari.

1.7.E. Dati due insiemi A e B ed f:A→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 $\Pi_f : A \to A/\Re_f$, $\Pi_f(x) = [x]_{\Re_f}$, è suriettiva. La funzione $F: A/\Re_f \to B$, definita da $F([x]_{\Re_f}) = f(x)$, 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 $F : A/\Re_f \xrightarrow[su]{1-1} \operatorname{Im} f$, e $f = F \circ \pi$.



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

Relazioni d'ordine. Sia A un insieme. Una relazione $\Re \subseteq A \times A$ si dice *relazione d'ordine* su A se possiede le seguenti proprietà:

a) *Riflessiva*: per ogni x∈A si ha x$\Re$x.

b) *Antisimmetrica*: per ogni x,y∈A, se x$\Re$y e y$\Re$x allora x = y.

c) *Transitiva*: per ogni x, y, z∈A, se x$\Re$y ed y$\Re$z allora anche x$\Re$z.

Una relazione d'ordine si dice *totale* se possiede inoltre la seguente proprietà:

d) *Dicotomia*: per ogni x, y∈A si ha x$\Re$y oppure y$\Re$x.

Se $\Re$ non possiede questa proprietà, viene detta *ordine parziale*. I simboli usati per le relazioni d'ordine sono di solito: ≤, ⊆, |, ⇒, ecc.

Se A è un insieme e ≤ è una relazione d'ordine su A allora la coppia (A, ≤) si chiama *insieme ordinato* o anche *poset* (partially ordered set).

Sia (A, ≤) un insieme ordinato e sia B⊆A. Si chiama *maggiorante di B* ogni elemento y∈A tale che per ogni x∈B sia x ≤ y. Si chiama *estremo superiore* di B un maggiorante x_0 di B tale che per ogni altro maggiorante y di B sia $x_0 \le y$. Si vede subito che se l'estremo superiore esiste allora è unico e si denota con *sup B*. Analogamente

sono definiti i minoranti di B e l'*estremo inferiore inf B*. Se sup B esiste ed appartiene a B allora esso si chiama *massimo* di B e si denota con *max B*. Analogamente, se inf B∈B esso si chiama *minimo* di B e si denota con *min B*.

ESEMPI 1.8.

1.8.A. - Indichiamo con ≤ l'usuale ordinamento di **N**, definito nel modo seguente: se x,y∈**N** poniamo x ≤ y se esiste d∈**N** tale che y = x+d. Allora (**N**, ≤) è un insieme totalmente ordinato. Ogni sottoinsieme non vuoto di **N** ha minimo. Il minimo di **N** è lo zero; invece, **N** non ha estremo superiore.

1.8.B. - In **N** poniamo x|y (e diciamo che x divide y) se esiste q∈**N** tale che y = xq. Allora (**N**, |) è un insieme parzialmente ordinato. **N** ha massimo 0 e minimo 1 e per ogni coppia di elementi x, y∈**N** si ha;

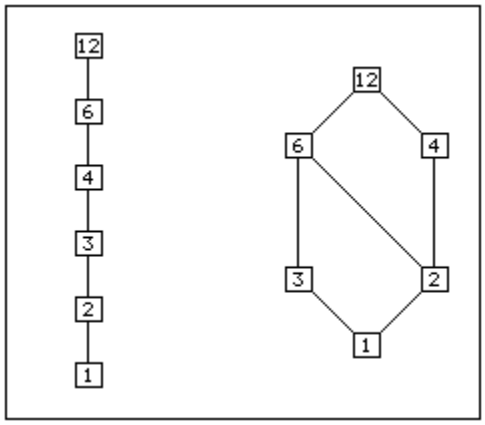
$$\sup\{x,y\} = \text{mcm}(x,y), \quad \inf\{x,y\} = \text{MCD}(x,y).$$

1.8.C. - Sia X un insieme. Allora ($\wp(X)$, ⊆) è un insieme parzialmente ordinato. Il massimo di $\wp(X)$ è X ed il minimo è l'insieme vuoto. Per ogni coppia di elementi A, B∈$\wp(X)$ si ha sup{A,B} = A∪B e inf{A,B} = A∩B.

1.8.D. - Nell'insieme **Z** dei numeri interi relativi chiamiamo *positivi* lo zero ed i numeri preceduti dal segno +. Definiamo poi la relazione ≤ ponendo, per ogni x,y∈**Z**, x ≤ y se y-x è positivo. Allora (**Z**, ≤) è un insieme totalmente ordinato e ≤ è il consueto ordinamento di **Z**.

Nel caso finito è possibile rappresentare un poset $(X, \leq)$ mediante un *diagramma di Hasse*. Esso è basato sulla relazione seguente, detta di *copertura*: $\forall x, y \in X,\ x \prec y$ se $x < y$ e non esiste $z \in X$, $x < z < y$.

Nel diagramma gli elementi di X sono rappresentati mediante punti, con le condizioni seguenti: se $x < y$ allora x è più in basso di y e una linea collega x ed y se $x \prec y$. In figura i diagrammi di Hasse dell'insieme dei divisori di 12 ordinato sia mediante l'ordine naturale di **N** sia mediante la relazione "è divisore di".



§ 2 – OPERAZIONI E STRUTTURE ALGEBRICHE

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 $x \cdot y$ o più brevemente con xy.

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

ESEMPIO 2.1. 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, $a \cdot e = e \cdot a = a$.
4. *Elementi simmetrici* (se c'è un elemento neutro e):

   per ogni a∈X esiste a'∈X tale che $a \cdot a' = a' \cdot a = e$.
5. *Leggi di cancellazione*:

   destra: da a·b = c·b segue a = c;

   sinistra: da a·b = a·c segue b = c.
6. *Proprietà di idempotenza*: per ogni a∈X si ha $a \cdot a = a$.
7. *Elemento assorbente*: esiste u∈X tale che, per ogni a∈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 viene 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 che 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. Semigruppo $\left(S, \cdot\right)$: 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.B. Monoide $(M,\cdot,1_M)$: l'operazione binaria $\cdot$ è associativa ed 1_M ne è l'elemento neutro. Vediamo un esempio importante:

Esempio 2.2. *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 il *monoide delle funzioni di X*. Se X ha n elementi, dal calcolo combinatorio sappiamo che esso possiede n^n elementi.

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

Un monoide $(M,\cdot,1_M)$ si dice *commutativo* se $\forall x,y \in M,\ x\cdot y = y\cdot x$. Un esempio è $(\mathbf{N},+,0)$.

Un monoide $(M,\cdot,1_M)$ si dice *idempotente* se $\forall x \in M,\ x\cdot x = x$. Un esempio è $(\wp(X),\cup,\varnothing)$, dove X è un insieme non vuoto.

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 esempio è $(\mathbf{N},+,0)$.

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:

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

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, $(x')' = x$.

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 $\sigma : M \to M$.

2.C. Gruppo $(G, \cdot, 1_G, \sigma)$: l'operazione binaria $\cdot$ è associativa, 1_G ne è l'elemento neutro e ogni elemento x ha il simmetrico $x^{-1} = \sigma(x)$, dove con il simbolo σ 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.

Esempio 2.3.I. *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 $X = \{1, 2, \ldots, n\}$, il suo gruppo simmetrico si denota con S_n. Dal calcolo combinatorio sappiamo che S_n possiede n! elementi.

Esempio 2.3.II *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 una unità di misura, la distanza di due punti è la lunghezza del segmento che li congiunge, il gruppo delle isometrie è ben noto, ed è costituito da rotazioni, traslazioni, simmetrie assiali e antitraslazioni.

Esempio 2.3.III. *I gruppi diedrali*. Dato un poligono regolare con n lati (n ≥ 3), vi sono 2n *isometrie* del piano che lo trasformano in sé, come sappiamo dalla geometria, e precisamente le n rotazioni di ampiezza $\frac{2k\pi}{n}, k = 0,1,\ldots,n-1$, 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 2.4. 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.D. 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 $\cdot$ 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 $\cdot$ è commutativa l'anello si dice *commutativo*. $(\mathbf{Z},+,\cdot,1)$ è un anello commutativo. Vediamo altri esempi.

ESEMPI 2.5. I. *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 + e 1 quello di $\cdot$. Se l'anello A è commutativo lo è anche l'anello delle funzioni.

Esempio 2.5.II. *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 2.5.III. *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 chiamano *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 2.5.IV. *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 questo 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 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 2.6. 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.E. 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.I. 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.

Esempio 2.9.II. 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

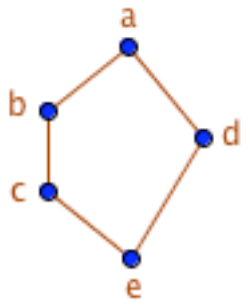
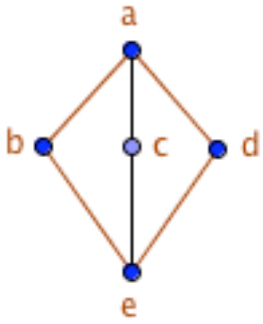
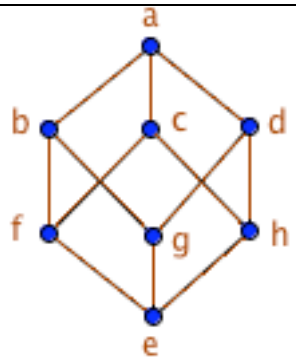
elemento è opposto di se stesso (cioè A ha caratteristica 2) ed è il quadrato di se stesso, ossia A è idempotente. Inversamente, da ogni anello di Boole si può costruire un'algebra di Boole ponendo $x \wedge y = x \cdot y$, $x \vee y = x + y + x \cdot y$, $x' = 1_A + x$.

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.

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.

§3 Nozioni generali sulle strutture algebriche

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 come 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.

3.A. 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 3.1. *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,

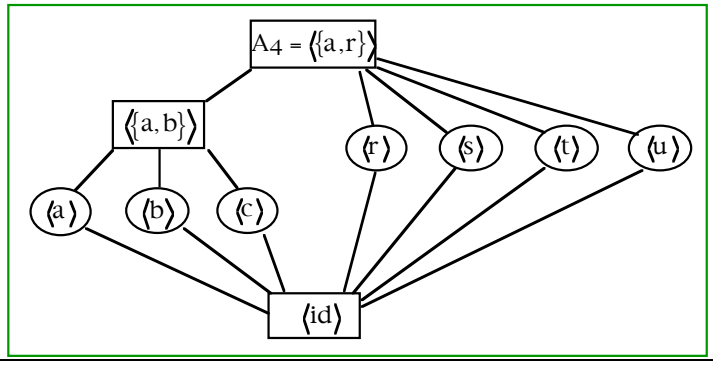
denotato con [G:H] il numero dei laterali destri, si ha il seguente risultato, ben noto dai corsi di Algebra del triennio.

TEOREMA 3.2. (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 3.3.I. *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 3.3.II. Similmente, un *sottoreticolo* di un reticolo (R, ∨, ∧) è costituito da un sottoinsieme chiuso rispetto alle due operazioni ∨, ∧. Per esempio, l'insieme dei divisori di n è un sottoreticolo del reticolo $(\mathbf{N}, mcm, MCD)$.

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

LEMMA 3.4. 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 $i \in \{1, 2, \ldots, r\}$ sia f_i operazione k -aria. Se $k > 0$, siano $x_1, \ldots, x_k \in Y$ e proviamo che $f(x_1, \ldots, x_k) \in Y$. Poiché $x_1, \ldots, x_k \in Y$, allora essi appartengono ad ogni $H \in \Omega$ e quindi, essendo H una sottostruttura di X, si ha $f(x_1, \ldots, x_k) \in H$. Ma allora $f(x_1, \ldots, x_k) \in \bigcap_{H \in \Omega} H$. 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 $\{0, 2, 3, 4, 6, 8, 9, \ldots\}$ 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 $H \cup K \neq \langle H \cup K \rangle$.

3.C. Omomorfismi e isomorfismi. Date due strutture (X, *) e (Y, ·), si chiama *omomorfismo* una funzione $\Phi : X \to Y$ tale che per ogni coppia a, b di elementi di X sia $\Phi(a * b) = \Phi(a) \cdot \Phi(b)$. 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 $u \in X$ e $v \in Y$ deve portare u in v; rispetto ad operazioni unarie f in X e h in Y, si deve avere $\Phi(f(x)) = h(\Phi(x))$ per ogni $x \in X$. Definiamo *omomorfismo* tra due strutture algebriche $(X, f_1, f_2, \ldots, f_r)$ e $(Y, g_1, g_2, \ldots, g_r)$ dello stesso tipo, una funzione $\Phi : X \to Y$ tale che sia omomorfismo tra (X, f_i) e (Y, g_i) per ogni i = 1, 2,.., r. In ogni caso, l'immagine $\Phi(X)$ è una sottostruttura di Y.

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.

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 3.5.I. 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 3.5.II. 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 3.5.III. Sia (M, *, 1_M) un monoide e sia (M^M, ∘, id_M) il monoide delle funzioni su M. Associamo ad ogni elemento a∈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 3.5.IV. Sia G un gruppo e sia S_G il gruppo simmetrico sull'insieme sostegno di G. Associamo ad ogni elemento a∈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 3.5.V. 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 3.5.VI. 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 3.6. (**Q**, +) e ($\mathbf{Q}^+$, ·) non sono gruppi isomorfi: infatti nel primo gruppo, dati $x \in \mathbf{Q}$, $x \neq 0$, ed $n \in N$, $n > 0$, 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 $n \in N$, $n > 0$, esiste $y \in \mathbf{Q}^+$, tale che $y^n = x$". Pertanto questi due gruppi, a differenza di (**R**, +) ed ($\mathbf{R}^+$, ·), non sono isomorfi.

3.D. 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 3.7.I. 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 3.7.II. 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**.

3.E. Congruenze e strutture quoziente. Data una struttura con una operazione binaria (X, ·), una relazione d'equivalenza ~ in X si dice *congruenza* rispetto a · se dati a, b, a', b'∈X, dall'essere a ~ a', b ~ b' segue a·b ~ a'·b'. Indichiamo con [x] la classe di equivalenza di x, ossia [x] = {y∈X | y ~ x} e consideriamo l'insieme quoziente X/~ costituito dalle classi di equivalenza. Definiamo tra le classi l'operazione seguente: per ogni a,b∈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 3.8.I. 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 3.8.II. Nel gruppo (**Z**, +) si considerino il numero $m \geq 1$ 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 $x \equiv y \pmod m$ se e solo se $x-y \in m\mathbf{Z}$, 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 3.8.III. 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,

$[0] = [2\pi] = [4\pi] = \ldots$. 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 3.8.IV. In un anello $\left(A,+,\cdot,1_A\right)$ un sottoinsieme I si dice *ideale* se è un sottogruppo di (A,+) e se per ogni $i\in I$ e per ogni $x\in A$ si ha $x\cdot i\in I$ e $i\cdot x\in I$.
La relazione $x \sim_I y \Leftrightarrow x-y\in I$ è una congruenza nell'anello, nella quale la classe di 0_A è I e la classe di un elemento a è $a+I = \{a+i \mid i\in I\}$. 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 $\mathbf{Z}$ 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.

C'è una connessione tra omomorfismi e congruenze, come prova il seguente ben noto teorema, detto *teorema fondamentale d'omomorfismo.*

TEOREMA 3.9. Siano X ed Y due strutture dello stesso tipo ed f un omomorfismo tra di esse.
a) L'immagine Im f è una sottostruttura di Y
b) La relazione $\sim_f$ in X così definita, per ogni $a, b\in X$:

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

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

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 = Ker f, detto *nucleo* di f, che costituisce la classe dell'elemento neutro. Più esplicitamente, si ha $\mathrm{Ker}\, f = \{x \in G \mid f(x) = 1_H\}$. Le altre classi sono i suoi laterali, così che il teorema 2.1.4 si riformula in modo riassuntivo come segue, con una piccola aggiunta:

TEOREMA 3.10. 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* Ker f è un sottogruppo normale in G;

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

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

Dati un gruppo G e $K \leq G$, il *normalizzante* $N_G(K)$ di K in G è l'insieme degli elementi $g \in G$ tali che $g^{-1}Kg = K$. Si verifica facilmente che $N_G(K)$ è un sottogruppo di G contenente K ed è il più grande nel quale K sia normale. Inoltre, $K \lhd G \Leftrightarrow N_G(K) = G$. Per ogni H, $K \leq G$, poniamo $HK = \{x \in G \mid x = hk,\ h \in H,\ k \in K\}$. Ciò posto, si ha:

COROLLARIO 3.11. *I teoremi d'isomorfismo*.

a) (Primo teorema d'isomorfismo). Siano G ed H due gruppi e sia $f: G \to H$ un epimorfismo. Allora G/Ker F = H.

b) (Secondo teorema d'isomorfismo). Siano G un gruppo, H, K sottogruppi di G, con $H \leq N_G(K)$. Allora $HK \leq G$, $H \cap K \lhd H$ e si ha $HK/K \cong H/H \cap K$.

c) (Terzo teorema d'isomorfismo). Siano G un gruppo, H, K sottogruppi normali, con $H \leq K$. Allora, $\frac{G}{K} \cong \frac{G/H}{K/H}$.

Dimostrazione. a) Segue immediatamente dal teorema fondamentale di omomorfismo.

b) Si consideri l'applicazione $\varphi : H \to N_G(K)/K$ definita da: $\varphi(h) = hK$. E' immediato provare che è un epimorfismo, che ha HK per immagine e che il suo nucleo è proprio $H \cap K$. La conclusione segue da a).

c) Si consideri la relazione $\{(gH, gK) \mid g \in G\} \subseteq G/H \times G/K$. Poiché $H \leq K$, si ha $gH = g'H \Rightarrow gK = g'K$, per cui tale relazione è un'applicazione tra G/H e G/K. Si prova ora immediatamente che è un epimorfismo e che il suo nucleo è K/H, per cui la conclusione segue da a)

Esempio 3.12. 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 3.13. 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* $\operatorname{Ker} f = \{x \in A \mid f(x) = 0_H\}$ è un ideale di A;

c) A/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 Ker f = $\{0_G\}$.

3.G. 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 • possiedono una stessa proprietà (associativa, commutativa, idempotenza, assorbimento, legge di cancellazione, elemento neutro), anche l'operazione · 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).

§ 4. Operazioni esterne ed 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" (destre) $\mu : X \times \Omega \to X$, 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 destra* di Ω su X. Si può considerare ovviamente anche il caso di un'azione *sinistra* $\mu : \Omega \times X \to X$.

Fissato $\omega \in \Omega$, posto $x^\omega = \mu(x, \omega)$, si ottiene la funzione $\tau_\omega : X \to X, \tau_\omega : x \mapsto x^\omega$. 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 $\mu_\rho(x, \omega) = \rho(\omega)(x)$.

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.

4.A. 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

$$\sum_{i=1}^{n} \xi_i e_i, \text{con } \xi_i \in K \text{per ogni } i = 1, \ldots, n.$$

Oltre agli spazi vettoriali reali o complessi, vediamo altri esempi.

Esempio 4.A.I. 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 $k \in \mathbf{Z}_p$ e per ogni $v \in V$, $kv = \underbrace{v + v + \ldots + v}_{k}$.

Si osservi che se k' è un intero tale che k' = k+pq per un opportuno $q \in \mathbf{Z}$, 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 4.A.II. Sia Δ la differenza simmetrica d'insiemi, definita da

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

Sia X un insieme. La struttura $(\wp(X), \Delta)$ è un gruppo abeliano nel quale l'elemento neutro è l'insieme vuoto ø e in cui $\forall A \subseteq X, A \Delta A = \varnothing$. Dunque, si tratta di un 2-gruppo abeliano elementare, quindi di

uno spazio vettoriale sul campo $\mathbf{Z}_2$. Si prova facilmente che se X ha n elementi, allora $\left\{\{x\} \mid x \in X\right\}$ è una base di questo spazio vettoriale e pertanto $\wp(X)$ ha 2^n elementi.

Esempio 4.A.III. 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 $n \geq 1$ tale che A ha p^n elementi.

Esempio 4.A.IV. - 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 $p^k = \left(p^h\right)^n = p^{hn}$. In particolare, h divide k.

4.B. 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. Vediamo alcuni esempi:

Esempio 4.B.I. 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.

Esempio 4.B.II. Gli anelli come *moduli su se stessi*. 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 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.

4.C. 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) $\forall k \in K,\ \forall v, w \in V,\ k(v \cdot w) = (kv) \cdot w = v \cdot (kw)$

La struttura ottenuta è detta *algebra* KA. Se l'anello A è associativo, l'algebra è detta *associativa.* Vediamo alcuni esempi di algebre associative:

Esempio 4.C.I. Sia $E \subseteq \mathbf{R}$. L'insieme $\mathbf{R}^E = \{f \mid f : E \to \mathbf{R}\}$ è un'algebra sul campo reale, rispetto alle usuali operazioni "punto per punto". La moltiplicazione di una funzione $f : E \to R$ per un numero reale k è definita punto per punto identificando k con la funzione costante k ristretta ad E: (kf)(x) = k·f(x).
Allo stesso modo, i polinomi in una o più indeterminate a coefficienti in un campo K sono un'algebra sul campo K.

Esempio 4.C.II. L'insieme End(V) degli endomorfismi di uno spazio vettoriale su un campo K è un'algebra sul campo K rispetto all'addizione punto per punto, la composizione e la moltiplicazione esterna per K, definita da (kf)(v) = k(f(v)).
Similmente, l'insieme delle matrici quadrate d'ordine n ad elementi in un campo K costituisce l'algebra $M_n(K)$ sul campo K.

5.D. Azione di un insieme su un gruppo. Sia G un gruppo nel ruolo di X ed Ω un insieme. Sia poi data $\mu : G \times \Omega \to G$ tale che:

$$\forall x, y \in G, \forall \omega \in \Omega,\ \mu(x \cdot y, \omega) = \mu(x, \omega) \cdot \mu(y, \omega)$$

Allora, posto $f_\omega : G \to G,\ f_\omega(x) = \mu(x, \omega)$, si ha $f_\omega \in \mathrm{End}(G)$. Pertanto, possiamo supporre $\rho_\mu : \Omega \to \mathrm{End}(G)$. La struttura ottenuta si chiama Ω-gruppo.

Questo esempio generalizza tutti i casi precedenti, nei quali è sempre coinvolto un gruppo abeliano come insieme X. In tal caso, può essere utile scrivere il gruppo in notazione additiva e quindi esprimere la proprietà precedente nella forma:

$$\forall x, y \in G, \forall \omega \in \Omega,\ (x + y)\omega = x\omega + y\omega$$

che si può assimilare ad una proprietà distributiva a destra dell'operazione esterna rispetto all'interna.

Esempio 4.D.I. Azione per coniugio. Un caso particolare si ha considerando l'insieme sostegno di G come Ω e definendo l'operazione esterna nel modo seguente: $\mu(x, g) = g^{-1}xg$. 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, $\mathrm{Inn}(G) \cong G / Z(G)$.
In modo analogo si può procedere prendendo come Ω l'insieme degli automorfismi oppure quello degli endomorfismi e definendo l'operazione esterna nel modo seguente: $\mu(x, f) = f(x)$.

Anche alle strutture algebriche con operazioni esterne si possono applicare le nozioni generali già viste nel § 3. Esaminiamo brevemente alcuni esempi.

4.E. 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 4.E.I. 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:

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

Esempio 4.E.II. Una sottostruttura di un Ω-gruppo G è un sottogruppo H tale che $\forall \omega \in \Omega, \forall h \in H,\ \mu(h, \omega) \in H$. Ciò equivale a dire che per ogni endomorfismo f appartenente all'immagine di ρ_μ si deve avere $f(H) \subseteq H$. Fra gli Ω-sottogruppi, oltre a G stesso, c'è sempre $\{1_G\}$. L'esempio degli spazi vettoriali ne è un sottocaso.

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:

PROPOSIZIONE 4.1. Un sottogruppo K di un gruppo G è un G-sottogruppo se e solo se $K \lhd G$.

Nel caso in cui $\Omega = \mathrm{Aut}(G)$, le sottostrutture sono sottogruppi trasformati in sé da ogni automorfismo di G e sono dette *sottogruppi caratteristici.* Un esempio è il centro Z(G) di G.

Infine, nel caso in cui $\Omega = \mathrm{End}(G)$, le sottostrutture sono sottogruppi trasformati in sé da ogni endomorfismo di G e sono dette *sottogruppi pienamente invarianti.* Un esempio è il *derivato* G' di G, definito come il sottogruppo generato dall'insieme dei *commutatori* $[a,b] = a^{-1}b^{-1}ab,\ a,b \in G$, e che è il più piccolo sottogruppo normale K di G tale che G/K sia abeliano.

Esempio 4.E.III. - 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. Vediamo esempi:

LEMMA 4.2. Se H e K sono due sottogruppi di un gruppo G e $K \lhd G$ allora $\langle H \cup K \rangle = HK = \{hk \mid h \in H, k \in K\}$. Inoltre, $H, K \lhd G \Rightarrow HK \lhd G$.

Dimostrazione. Naturalmente $\langle H \cup K \rangle$ contiene H e K e quindi ogni elemento di HK. Perciò $HK \subseteq \langle H \cup K \rangle$. Se dimostriamo che HK è un sottogruppo contenente sia H sia K, allora HK è uno dei sottogruppi che contengono $H \cup K$ e quindi contiene il minimo di essi, ossia $\langle H \cup K \rangle$.

Per cominciare, 1_G appartiene sia ad H sia a K, quindi $1_G = 1_G \cdot 1_G \in HK$.

Poi, siano $h, h' \in H$, $k, k' \in K$. Allora $(hk)(h'k') = (hh')((h'^{-1}kh')k') \in HK$. Inoltre, $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}(hk^{-1}h^{-1}) \in HK$, essendo $H \leq N_G(K)$. Infine, $h = h \cdot 1_G \in HK$ e quindi $H \subseteq HK$; analogamente, $K \subseteq HK$. Pertanto, HK è un sottogruppo contenente $H \cup K$ e dunque $\langle H \cup K \rangle \leq HK$. Ma allora $\langle H \cup K \rangle = HK$.

Siano infine $H \lhd G$, $K \lhd G$, $hk \in HK$, $g \in G$. Allora $g^{-1}(hk)g = (g^{-1}hg)(g^{-1}kg) \in HK$ perché entrambi i fattori sono normali in G, quindi $HK \lhd G$.

NOTA. Il sottogruppo HK si dice *prodotto* dei due sottogruppi H e K. In notazione additiva ovviamente si denota con H+K e si chiama *somma* di H e K.
Se H e K sono normali e $H \cap K = \{1_G\}$ il prodotto HK si dice *prodotto diretto interno* di H e K, ed è isomorfo al prodotto diretto $H \times K$.

Esempio 4.F. 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:

$$\text{Span}(U \cup W) = U+V = \{u + v \mid u \in U, w \in W\},$$

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

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

4.G. 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 di 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 $\mathrm{Hom}_{\Omega}(X,Y)$.

Esempio 4.G.I. 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 4.3. 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: $\forall \omega \in \Omega, \forall f, g \in \mathrm{Hom}_{\Omega}(X,Y)$,

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

4.H. 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 4.H.I. *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. Se K = GF(q) è un campo finito d'ordine q, allora V ha q^n elementi e non è difficile contare le sue basi. Se infatti vogliamo costruire una base $\{v_1, ..., v_n\}$ possiamo scegliere v_1 in $V\backslash\{0\}$, cioè in q^n-1 modi. Scelto v_1, si deve scegliere v_2 indipendente da v_1, ossia $v_2 \in V\backslash \mathrm{span}(v_1)$, per cui vi sono per v_2 solo q^n-q scelte. Analogamente, dovrà essere $v_3 \in V\backslash \mathrm{span}(v_1, v_2)$, quindi per lui solo q^n-q^2 scelte, e così via. Pertanto, in V ci sono $(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$ basi ordinate, quindi il

gruppo $GL_n(K)$, che si denota in questo caso con $GL_n(q)$, ha in definitiva $\prod_{i=0}^{n-1}\left(q^n - q^i\right) = q^{\binom{n}{2}}\prod_{i=1}^{n}\left(q^i - 1\right)$ elementi.

4.I. 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 ~ 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. Vale allora il seguente risultato, la cui dimostrazione è lasciata per esercizio.

TEOREMA 4.4. (*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.

Nel caso in cui X sia un Ω-gruppo, allora vale per le congruenze una caratterizzazione analoga a quella vista per i gruppi e gli anelli, ossia valgono i seguenti risultati, applicabili poi anche agli spazi vettoriali ed agli A-moduli:

TEOREMA 4.5. Sia $\mathfrak{R}$ una congruenza per l'Ω-gruppo (X,+). Allora la classe [0] è un sottogruppo normale ed una Ω-sottostruttura e le altre classi sono i suoi laterali destri. Inversamente, data una Ω-sottostruttura I di X che sia un sottogruppo normale, la relazione $x\mathfrak{R}y \Leftrightarrow y\text{-}x\in I$ è una congruenza.

Dimostrazione. Sia I la classe dell'elemento neutro 0 del gruppo (X, +). Poiché in particolare $\Re$ è una congruenza del gruppo additivo, allora I è un sottogruppo normale. Siano ora $x \in I$ e $\omega \in \Omega$. Poiché $0^\omega = 0$, dato che ω agisce come un endomorfismo del gruppo additivo, allora $x \in I \Rightarrow x \Re 0 \Rightarrow x^\omega \Re 0^\omega = 0 \Rightarrow x^\omega \in I$, quindi I è una sottostruttura. Se poi x ed y sono due elementi di X in relazione $\Re$ tra loro, per le proprietà delle congruenze nei gruppi essi devono appartenere allo stesso laterale di I.

Inversamente, se I è un sottogruppo normale ed una Ω-sottostruttura, e $x, y \in X$ sono appartenenti ad uno stesso laterale di I, per cui $y = x+i$, con $i \in I$, allora, posto $x \Re y \Leftrightarrow y - x \in I$,

$$y - x = i \in I \Rightarrow \forall \omega \in \Omega, \left(y - x\right)^\omega = i^\omega \in I \Rightarrow y^\omega - x^\omega \in I \Rightarrow y^\omega \Re x^\omega$$

e quindi $\Re$ è una congruenza.

TEOREMA 4.6. (Primo teorema di **Ω**-isomorfismo). Siano G ed H due **Ω**–gruppi ed $f : G \xrightarrow{\text{su}} H$ un **Ω**-omomorfismo, allora $G / \mathrm{Ker}(f) \cong_\Omega H$.

4.L. 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 è la somma delle dimensioni dei fattori.

§ 5. Azione di un gruppo su un insieme

Concludiamo questa sezione con un caso particolare di operazione esterna, che svilupperemo un poco di più: l'azione di un gruppo G su un insieme X. In questo caso, la compatibilità con la struttura di G fa sì che G agisca come gruppo di permutazioni su X, ossia che la rappresentazione associata sia un omomorfismo tra G ed il gruppo simmetrico su X.

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 $g_1, g_2\in G$, $\mu(x, g_1g_2) = \mu(\mu(x, g_1), g_2)$.

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

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

b) $x^{g_1g_2} = \left(x^{g_1}\right)^{g_2}$.

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, si ha:

TEOREMA 5.1. a) Ad ogni azione $\mu: X\times G\to X$ si può associare una rappresentazione ρ_μ.

b) Ad ogni rappresentazione $\rho: G\to S_X$ si può associare un'azione μ_ρ.

Dimostrazione. a) Per ogni $g\in G$, la funzione $\rho(g): x \to x^g$ è una permutazione di X, infatti ha come inversa $\rho(g^{-1})$. La funzione $\rho_\mu: G \to S_X$, $\rho_\mu: g\to \rho(g)$, è, come si prova facilmente, un omomorfismo.

b) La funzione $\mu_\rho: X\times G \to X$ tale che per ogni $x\in X$ e $g\in G$, $\mu_\rho(x, g) = x\rho(g)$, è un'azione, come si prova facilmente.

Osservazione. Risulta: $\mu_{\rho_\mu} = \mu$ e $\rho_{\mu_\rho} = \rho$.

Il teorema precedente consente di parlare indifferentemente in termini di azione o di rappresentazione.

Esempio 5.A.I. - *Azione per coniugio*. Abbiamo già visto nella sezione precedente, dato un gruppo G, l'azione per coniugio dell'insieme sostegno di G sul gruppo G stesso, ma naturalmente si può rivedere il coniugio anche come azione del gruppo sul suo insieme sostegno.

Esempio 5.A.II. - *Azione per moltiplicazione a destra*. Sia G un gruppo e sia X = G. Per ogni x, g∈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*.

Esempio 5.A.III. - Ogni azione μ del gruppo G sull'insieme X induce un'azione sull'insieme $\wp(X)$ dei sottoinsiemi di X, ponendo, per ogni Y⊆X, per ogni g∈G,

$$\mu^*(Y, g) = Y^g = \{y^g \mid y \in Y\}$$

Di conseguenza, l'azione per moltiplicazione a destra di G su di sé induce un'analoga azione per moltiplicazione di G sui suoi sottoinsiemi; lo stesso fa l'azione per coniugio.

Sia data un'azione di G sull'insieme X e sia x∈X. Si chiama *stabilizzatore* $St_G(x)$ in G l'insieme $\{g \in G \mid x^g = x\}$. Come si prova facilmente, esso risulta essere un sottogruppo di G. Il nucleo della rappresentazione associata ρ è $\{ g \in G \mid \forall x \in X, x^g = x\}$. Pertanto, $\operatorname{Ker}\rho = \bigcap_{x \in X} St_G(x)$.

Un'azione si dice *semiregolare* se per ogni x∈X si ha $St_G(x) = 1$. Ne segue che ogni azione semiregolare è fedele.

Siano ora x, y∈X: poniamo $x \sim y$ se esiste g∈G tale che $y = x^g$. Questa è, come si prova facilmente, una relazione d'equivalenza in X, le cui classi si chiamano *G-orbite* e sono denotate con $[x]_G$. Il numero cardinale di $[x]_G$ si dice *lunghezza* della G-orbita.

L'azione si dice *transitiva* se $X/\sim = \{X\}$. Ciò significa che per ogni coppia di oggetti x, y∈X, esiste g∈G tale che $y = x^g$.

L'azione si dice *regolare* se è transitiva e semiregolare.

NOTE. a) Sia data un'azione m di un gruppo G su un insieme X, sia x∈X e sia $[x]_G$ la sua G-orbita. Allora è indotta da m su $[x]_G$ un'azione, e tale azione è transitiva.

b) Si dimostra facilmente che per ogni x∈X e g∈G si ha $St_G(x^g) = g^{-1}St_G(x)g$. Ne segue che due elementi x ed y di X sono nella stessa G-orbita se e solo se gli stabilizzatori $St_G(x)$ e $St_G(y)$ sono coniugati.

TEOREMA 5.2. Sia data un'azione del gruppo G sull'insieme X e sia $x \in X$. Allora:

a) L'insieme D dei laterali destri di $St_G(x)$ è equipotente a $[x]_G$.

b) Se G è finito si ha $|G| = |St_G(x)| \cdot |[x]_G|$. In particolare, se l'azione è transitiva e G è finito si ha $|G| = |St_G(x)| \cdot |X|$.

c) Se l'azione è regolare allora $|X| = |G|$.

Dimostrazione. a) La relazione tra $D = \{St_G(x)g \mid g \in G\}$ e $[x]_G$ definita da: $St_G(x)g \to x^g$, è una funzione ed è biiettiva: infatti, per ogni $g, h \in G$ si ha:

$$x^g = x^h \Leftrightarrow x^{gh^{-1}} = x \Leftrightarrow gh^{-1} \in St_G(x) \Leftrightarrow g \in St_G(x)h \Leftrightarrow St_G(x)g = St_G(x)h.$$

La suriettività è poi ovvia.

b) Segue da a) e dal teorema di Lagrange.

c) Segue da b) e dal fatto che, qualunque sia $x \in X$, si ha $St_G(x) = 1$.

Esempio 5.B.I. L'azione per moltiplicazione a destra di un gruppo G su se stesso è regolare.

Esempio 5.B.II. Se G non è il gruppo banale, l'azione per coniugio non è semiregolare e neppure transitiva. Il sottogruppo $St_G(x) = \{g \in G \mid g^{-1}xg = x\}$ è detto *centralizzante* di x in G e viene denotato con $C_G(x)$. La G-orbita [x] di x è la sua *classe di coniugio* e si ha: $|[x]| = [G:C_G(x)]$. L'intersezione dei centralizzanti è il nucleo della rappresentazione, ovvero è il centro Z(G). Si osservi che per ogni $x \in G$ si ha $\langle x \rangle Z(G) \leq C_G(x)$.

Esempio 5.B.III. Il gruppo G delle isometrie piane agisce naturalmente sul piano euclideo, e quindi induce un'azione sulle figure piane.

Determiniamo l'orbita e lo stabilizzatore di un quadrato e di una retta del piano euclideo nell'azione indotta dal gruppo G delle isometrie. Lo stabilizzatore di un quadrato è costituito dalle isometrie che lo trasformano in se stesso: in particolare si tratta delle 4 rotazioni intorno al suo centro ed ampiezze 0, $\pi/2$, π, $3\pi/2$, e delle quattro simmetrie assiali rispetto agli assi dei lati ed alle diagonali. Si ottiene un gruppo isomorfo a D_4. L'orbita di quel quadrato è costituita dai quadrati ad esso congruenti.

L'azione di G sulle rette è transitiva. Lo stabilizzatore di una retta comprende tutte e sole: le traslazioni di direzione parallela alla retta; le rotazioni di ampiezza π e centro sulla retta; le simmetrie rispetto alla retta data ed alle sue perpendicolari; le antitraslazioni di asse coincidente con la retta data.

L'azione per moltiplicazione a destra si trasferisce all'insieme $\wp(G)$ delle parti di G. Poiché i sottoinsiemi S ed Sg sono equipotenti, si hanno azioni sulle famiglie di sottoinsiemi con la stessa cardinalità.

In particolare, sia $H \leq G$ e sia $D = \{Hx \mid x \in G\}$ l'insieme dei suoi laterali destri. Allora per ogni $g \in G$ si ha $(Hx)g = H(xg) \in D$ e si ha un'azione transitiva di G su D. Per ogni $x \in G$ si ha: $St_G(Hx) = x^{-1}Hx$, coniugato di H e sottogruppo di G. Il nucleo della rappresentazione è $Cor_G(H) = \bigcap_{x \in G} x^{-1}Hx$: questo sottogruppo è detto *nocciolo* di H ed è il più grande sottogruppo normale di G contenuto in H. Il quoziente $G/Cor_G(H)$ è isomorfo ad un sottogruppo del gruppo simmetrico S_D. Ciò posto:

TEOREMA 5.3. (Poincaré). Sia G un gruppo e sia H un sottogruppo d'indice finito n. Allora esiste $K \lhd G$, $K \leq H$, tale che [G:K] divide n!

Dimostrazione. $K = Cor_G(H)$ è il nucleo della rappresentazione ρ di G come gruppo di permutazioni sull'insieme D degli n laterali destri di H. Allora $K \leq H$ e $G/K \cong Im(\rho) \leq S_D \cong S_n$. Di conseguenza, [G:K] divide n!

COROLLARIO 5.4. Sia G un gruppo finito e sia p il più piccolo primo che divida |G|. Sia poi $H \leq G$, tale che $[G:H] = p$: allora $H \lhd G$.

Dimostrazione. Per il teorema di Poincaré esiste $K \lhd G$, $K \leq H$, tale che [G:K] divide p!. Si ha anche [G:K] divisore di |G|, dunque [G:K] divide (|G|, p!) = p. Ma allora [G:K] = p, quindi $H = K \lhd G$.

NORMALIZZANTI E CENTRALIZZANTI DEI SOTTOGRUPPI. L'azione per coniugio si trasferisce all'insieme $\wp(G)$ dei sottogruppi. Si hanno così le G-orbite di sottogruppi [H] e l'azione, se G non è banale, non è né semiregolare né transitiva. Lo stabilizzatore di un sottogruppo H è detto *normalizzante* $N_G(H)$ di H in G, ed è il più grande sottogruppo di G in cui H sia normale. Il normalizzante $N_G(H)$ agisce su H per coniugio: per ogni $h \in H$, $n \in N_G(H)$ si ha infatti $n^{-1}hn \in H$. L'immagine della rappresentazione è un sottogruppo di Aut(H) (contenente Inn(H)). Il suo nucleo è detto *centralizzante di H in G*, viene denotato con $C_G(H)$, è normale in $N_G(H)$ ed è costituito dagli elementi di G che commutano con ogni elemento di H. Applicando il primo teorema di isomorfismo si ottiene il seguente:

TEOREMA 5.5. (*Teorema N/C di Burnside*). Siano G un gruppo, H un sottogruppo. Allora $N_G(H)/C_G(H)$ è isomorfo ad un sottogruppo di Aut(H).

NOTA. Sia $K \leq N_G(H)$. Allora essendo $H \lhd N_G(H)$ si ha che HK è un sottogruppo.

Il teorema di Lagrange afferma che se G è un gruppo finito ed H un suo sottogruppo, |H| è un divisore di |G|. Si pone allora il problema inverso: è vero che, dato un divisore h di |G|, esiste un sottogruppo d'ordine h? Per qualche classe di gruppi finiti è vero per ogni h: per esempio per i gruppi ciclici o, più in generale, per i gruppi abeliani. Per un gruppo finito G qualsiasi, è vero per particolari divisori dell'ordine del gruppo, come sarà mostrato ora.

PROPOSIZIONE 5.6. Sia G un gruppo tale che $|G| = p^n$, p primo, $n \in \mathbf{N}$.

i) La lunghezza di ogni classe di coniugio di elementi di G è una potenza di p.

ii) $Z(G) \neq 1$. In particolare, G non è semplice.

iii) Per ogni $0 \leq k \leq n$ esiste un sottogruppo K d'ordine p^k.

iv) Sia $k < n$. Ogni sottogruppo d'ordine p^k è incluso in uno d'ordine p^{k+1}.

Dimostrazione. i) Sia $x \in G$. La classe di coniugio [x] di x è l'orbita di x nell'azione di G per coniugio. Per il teorema 2.4.2, $|[x]|$ è un divisore di |G|, dunque è una potenza di p.

ii) Siano $[1_G]$, $[x_2]$, ..., $[x_r]$ le classi di coniugio distinte, di cui G è unione disgiunta. Sia poi $\left|\left[x_i\right]\right| = p^{k_i}$, con $k_i \geq 0$. Ovviamente, $|[1_G]| = 1 = p^0$. Si ha:

$$p^n = |G| = \sum_{i=1}^{r} p^{k_i} = 1 + \sum_{i=2}^{r} p^{k_i},$$

quindi almeno un altro k_i deve essere nullo, altrimenti p dividerebbe 1. Pertanto almeno un altro elemento deve stare nel centro di G, ossia $Z(G) \neq 1$.

iii) Procediamo per induzione rispetto a n. Se n = 0 l'affermazione è ovviamente vera. Sia vera per n e proviamola per n+1. Se k = 0, si ha $K = \{1_G\}$. Sia ora k > 0. Poiché $Z(G) \neq 1$ ed è abeliano, esiste $x \in Z(G)$, di periodo p. Essendo $P = \langle x \rangle \lhd G$, consideriamo G/P, che ha ordine p^n. Per ipotesi induttiva esiste in G/P un sottogruppo K/P d'ordine p^{k-1}: la sua controimmagine K in G ha ordine p^k.

iv) Procediamo di nuovo per induzione rispetto ad n. Sia P d'ordine p incluso in Z(G) e sia $K \leq G$, $|K| = p^k$. Se K non contiene P, allora PK è un sottogruppo d'ordine p^{k+1} contenente K. Se invece $P \leq K$ consideriamo G/P: per ipotesi induttiva, K/P è incluso in un sottogruppo H/P tale che [H/P:K/P] = p: allora $K \leq H$, [H:K] = p e $|H| = p^{k+1}$.

NOTA. Il punto iii) prova che in un gruppo d'ordine p^n, con p primo, il teorema di Lagrange è invertibile.

PROPOSIZIONE 5.7. Sia G un gruppo.

i) Se G/Z(G) è ciclico allora Z(G) = G.

ii) Se $|G| = p^2$, con p primo, allora G è abeliano.

Dimostrazione. i) Sia $G/Z(G) = \langle aZ(G)\rangle$: allora $G = \langle\{a\}\cup Z(G)\rangle$ è necessariamente abeliano, poiché i suoi generatori commutano fra loro. Perciò Z(G) = G.

ii) Abbiamo provato nella proposizione 5.6 che $Z(G) \neq 1$. Se fosse $|Z(G)| = p$, allora G/Z(G) avrebbe ordine p, dunque sarebbe ciclico, assurdo. Pertanto, Z(G) = G e G è abeliano.

Sia G un gruppo finito d'ordine $p^a m$, p primo, $(p, m) = 1$, $a \geq 1$. Ogni sottogruppo d'ordine p^k è detto *p-sottogruppo*. Per il teorema di Lagrange deve essere $k \leq a$. Ogni sottogruppo d'ordine p^a è detto *p-sottogruppo di Sylow* di G. Un tal sottogruppo non può essere incluso propriamente in altri p-sottogruppi.

TEOREMA 5.8 (*Teorema di Sylow*). Sia G un gruppo finito d'ordine $p^a m$, p primo, $(p, m) = 1$, $a \geq 1$. Allora:

a) G possiede p-sottogruppi di Sylow.

b) Ogni p-sottogruppo è incluso in un p-sottogruppo di Sylow.

c) Tutti i p-sottogruppi di Sylow sono coniugati.

d) Detto n_p il loro numero, si ha $n_p \equiv 1 \pmod p$ ed n_p divisore di m.

Dimostrazione. (a) Sia **X** l'insieme dei sottoinsiemi X di G con p^a elementi. Si ha, dal calcolo combinatorio:

$$|\mathbf{X}| = \binom{p^a m}{p^a} = \frac{p^a m\left(p^a m - 1\right)\cdots\left(p^a m - p^a + 1\right)}{1\cdot 2\cdots\left(p^a - 1\right)p^a} = m\cdot\prod_{i=1}^{p^a-1}\frac{p^a m - i}{i}$$

Per ogni $h \geq 0$, p^h divide $p^a m - i \Leftrightarrow p^h$ divide i, ed in tal caso nella frazione $\frac{p^a m - i}{i}$ il fattore p^h si può elidere. Ne segue che p non divide $|\mathbf{X}|$.

Siano ora $X\in\mathbf{X}$ e $g\in G$: l'insieme $Xg = \{xg \mid x\in X\}$ ha anch'esso p^a elementi ed appartiene ad **X**. Possiamo perciò definire l'azione di G su **X** per moltiplicazione a destra.

Se tutte le G-orbite avessero lunghezza multipla di p anche $|\mathbf{X}|$ sarebbe multiplo di p, dunque deve esistere almeno una G-orbita $[X]_G$ di lunghezza non multipla di p. Sia P il suo stabilizzatore in G: essendo $|G| = |[X]_G| \cdot |P|$ ne segue che p^a deve dividere |P|. In particolare, $p^a \leq |P|$. Ma per ogni $g \in P$ si ha $Xg = X$, perché P è lo stabilizzatore di X, dunque, preso $x_0 \in X$, per ogni $g \in P$ si ha $x_0 g \in X$, ossia $x_0 P$ è un sottoinsieme di X.

Ma allora $|P| = |x_0 P| \leq |X| = p^a$. Dunque $|P| = p^a$ e P è un p-sottogruppo di Sylow di G. Ciò prova (a).

Per provare gli altri asserti del teorema, occorrono alcune considerazioni preliminari.

Sia P un p-sottogruppo di Sylow. Denotiamo con $[P]_G$ la classe di coniugio di P in G, cioè poniamo $[P]_G = \{x^{-1}Px \mid x \in G\}$. Sia T un p-sottogruppo di G. Consideriamo l'azione di T su $[P]_G$ mediante coniugio: sappiamo che ogni T-orbita ha lunghezza che divide |T|, cioè è una potenza di p. Supponiamo ora che un'orbita abbia lunghezza $p^0 = 1$, cioè che esista $P_1 \in [P]_G$ tale che $\forall g \in T$ sia $g^{-1}P_1 g = P_1$. Allora $T \leq N_G(P_1)$. Ne segue che P_1T è un sottogruppo di G, incluso in $N_G(P_1)$ e contenente P_1 e T. Dunque, per il II teorema di isomorfismo, $P_1 \cap T \lhd T$ e $\frac{P_1 T}{P_1} \cong \frac{T}{P_1 \cap T}$.

Quest'ultimo è un quoziente di T, quindi il suo ordine è una potenza di p.

Poiché $|P_1| = p^a$, ne segue che anche $|P_1T| = |P_1| \cdot \left|\frac{T}{P_1 \cap T}\right|$ è una potenza di p.

Di conseguenza, P_1T è un p-sottogruppo di G contenente P_1, ed allora, essendo P_1 un p-sottogruppo di Sylow, deve essere $P_1T = P_1$. Ma allora si ha $T \leq P_1$.

Tutto ciò vale in particolare se scegliamo T = P: innanzitutto {P} è effettivamente un'orbita di lunghezza 1 per l'azione di P su $[P]_G$. Di più, per ogni P-orbita $\{P_1\}$ di lunghezza 1, deve essere $P \leq P_1$ e dunque $P_1 = P$ perché sono insiemi con la stessa cardinalità. Allora {P} è l'unica P-orbita di lunghezza 1 e tutte le altre hanno lunghezze multiple di p: ne segue $|[P]_G| \equiv 1 \pmod p$.

Possiamo ora provare la parte restante del teorema.

(b) Sia T un qualunque p-sottogruppo di G: le T-orbite in $[P]_G$ non possono avere tutte lunghezza multipla di p, altrimenti $|[P]_G| \equiv 0 \pmod p$. Pertanto almeno un'orbita ha lunghezza 1, dunque esiste $P_1 \in [P]_G$ (cioè un coniugato di P) tale che $T \leq P_1$.

(c) Se come T in particolare scegliamo un altro p-sottogruppo di Sylow di G, per (b) esiste un coniugato P_1 di P tale che $T \leq P_1$, ma avendo lo stesso ordine, T e P_1 devono essere uguali. Perciò ogni p-sottogruppo di Sylow è un coniugato di P.

(d) Per (c) si ha $n_p = |[P]_G|$, dunque $n_p \equiv 1 \pmod p$. Inoltre, $n_p = [G:N_G(P)]$, ed essendo $P \leq N_G(P)$ si ha che $[G:N_G(P)]$ divide $[G:P] = m$.

COROLLARIO 5.9. (*Inverso parziale del teorema di Lagrange*). Siano G un gruppo finito e p un primo. Se p^h divide |G| esiste $H \leq G$ tale che $|H| = p^h$.

Dimostrazione. Sia P un p-sottogruppo di Sylow di G; poiché p^h divide |P| allora, per 5.6.iii, in P esiste un tal sottogruppo H.

COROLLARIO 5.10. (*Teorema di Cauchy*) Sia G un gruppo finito e sia p un numero primo divisore di |G|. Allora esiste $x \in G$ di periodo p.

Dimostrazione. Si applichi il risultato precedente al caso di h = 1: allora H è ciclico ed un suo generatore x soddisfa l'asserto.

COROLLARIO 5.11. Sia p un numero primo. Per un gruppo finito G sono equivalenti:

a) $|G| = p^n$

b) Ogni $x \in G$ ha periodo potenza di p.

Esempio 5.12. Verifichiamo che se |G| = 15 allora $G \cong \mathbf{Z}_{15}$. Siano P un 3-sottogruppo di Sylow e Q un 5-sottogruppo di Sylow di G. Da $n_3 \equiv 1 \pmod 3$ e n_3 divisore di 15/3 = 5 segue $n_3 = 1$ e $P \lhd G$. Analogamente, $Q \lhd G$. Allora da $P \cap Q = \{1_G\}$ e G = PQ segue $G \cong P \times Q$.
Inoltre, $|P| = 3 \Rightarrow P \cong \mathbf{Z}_3$; $|Q| = 5 \Rightarrow Q \cong \mathbf{Z}_5$, dunque $G \cong \mathbf{Z}_3 \times \mathbf{Z}_5 \cong \mathbf{Z}_{15}$, essendo MCD(3, 5) = 1.

COROLLARIO 5.12. Sia G un gruppo abeliano d'ordine $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_r^{\alpha_r}$, $p_1 < p_2 < \ldots < p_r$, primi. Allora per ogni i, $1 \leq i \leq r$, G ha uno ed un solo sottogruppo P_i d'ordine $p_i^{\alpha_i}$, necessariamente normale in G, e G è isomorfo al prodotto diretto $P_1 \times P_2 \times \ldots \times P_r$.

§ 6. Gruppi risolubili

SERIE SUBNORMALI. Sia G un gruppo. Una sequenza finita di sottogruppi come la seguente:

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_n = G$$

è detta *serie subnormale*. I sottogruppi G_0, ..., G_n sono detti *termini*; ciascuno di essi è normale nel successivo (ma non necessariamente in G). I quozienti G_{i+1}/G_i sono detti *fattori* della serie. Il numero n si dice *lunghezza* della serie. Se i termini sono tutti distinti, la serie si dice *ridotta.* Chiaramente, ogni serie si può ridurre eliminando un termine se è uguale a quello che lo precede. Un sottogruppo si dice *subnormale* in G se appartiene come termine ad una serie subnormale. Ovviamente, ogni gruppo contiene la serie subnormale: $1 = G_0 \lhd G_1 = G$.

Sia G un gruppo. Una serie subnormale

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_n = G$$

è detta *serie abeliana* se i fattori G_{i+1}/G_i sono tutti abeliani. Un gruppo G si dice *risolubile* se possiede una serie abeliana. La minima lunghezza delle sue serie abeliane è detta *lunghezza di risolubilità* o lunghezza derivata di G ed è denotata con dl(G).

Un gruppo G è abeliano (non banale) se e solo se G è risolubile e dl(G) = 1. Se dl(G) = 2, G è detto *metabeliano*.

Esempio 6.1. Il gruppo S_3 è metabeliano, perché contiene la serie abeliana 1, A_3, S_3.
Anche il gruppo S_4 è risolubile: ha infatti la serie principale 1, K, A_4, S_4, a fattori abeliani (dove K è il gruppo di Klein {id, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)}). Questa è anche la sua serie abeliana più breve, dunque $dl(S_4) = 3$. Invece, per $n > 4$, S_n non è risolubile. Infatti per $n \geq 5$, le sole serie subnormali di S_n sono quella banale e 1, A_n, S_n, entrambe non abeliane.

Sia G un gruppo. Per ogni $a, b \in G$, sia $[a, b] = a^{-1}b^{-1}ab$ il loro *commutatore*. Il *derivato* G' di G è il sottogruppo generato dai commutatori. Esso ha la seguente importante proprietà:

PROPOSIZIONE 6.2. Il derivato G' di un gruppo G è invariante per endomorfismi ed è il minimo dei sottogruppi normali K di G tali che G/K sia abeliano.

Dimostrazione. Sia f un endomorfismo di G, allora $\left[a,b\right]^f = \left[a^f, b^f\right]$, quindi $\left(G'\right)^f \subseteq G'$. In particolare, G' è normale in G. Allora $\forall a,b \in G$,

$$\left(aG'\right)\left(bG'\right) = \left(ab\right)G' = \left(ba\left[a,b\right]\right)G' = (ba)G' = \left(bG'\right)\left(aG'\right)$$

Quindi G/G' è abeliano. D'altra parte, se $K \lhd G$ e G/K è abeliano, allora $\forall a,b \in G$,

$$\left[a,b\right]K = \left(a^{-1}b^{-1}ab\right)K = \left(a^{-1}K\right)\left(b^{-1}K\right)\left(aK\right)\left(bK\right) = K \Rightarrow \left[a,b\right] \in K$$

quindi $G' \leq K$. Di qui segue l'asserto.

Esempio 6.3. Per ogni $n > 1$ si ha $(S_n)' = A_n$. Infatti, per $n = 2$ è ovvio. Per $n > 2$, $\left|S_n / A_n\right| = 2 \Rightarrow 1 \neq \left(S_n\right)' \leq A_n$, ma A_n è semplice per $n \neq 4$ e quindi $(S_n)' = A_n$. Per $n = 4$ c'è un sottogruppo Q d'ordine 4 normale in S_4, ma S_4/Q non è abeliano. Perciò $(S_4)' = A_4$.

Sia G un gruppo. Poniamo $G^{(1)} = G'$, $G^{(n+1)} = (G^{(n)})'$. Per la proposizione 6.2, $G^{(n)}/G^{(n+1)}$ è abeliano per ogni n. Si ha:

TEOREMA 6.4. Sia G un gruppo. Allora:

a) G è risolubile se e solo se esiste $n \in N$ tale che $G^{(n)} = 1$.

b) Se G è risolubile, la *serie derivata* $G = G^{(0)} > G^{(1)} > \ldots > G^{(d)} = 1$ ha lunghezza $d = dl(G)$.

Dimostrazione. a) Se esiste n tale che $G^{(n)} = 1$ allora G ha la serie abeliana: $1 = G^{(n)} \lhd G^{(n-1)} \lhd \ldots \lhd G^{(0)} = G$, e dunque è risolubile.

Viceversa, G abbia la serie abeliana $1 = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_n = G$. Poiché $G_{n-1} \lhd G$ e G/G_{n-1} è abeliano, ne segue $G^{(1)} = G' \leq G_{n-1}$. Per induzione su i si prova che $G^{(i)} \leq G_{n-i}$. Perciò $G^{(n)} \leq G_0 = 1$.

b) Per quanto precede, se una serie abeliana ha lunghezza n, allora $G^{(n)} = 1$, dunque certamente $d \leq n$. Di qui segue la minimalità della serie derivata.

PROPOSIZIONE 6.5. La classe dei gruppi risolubili è chiusa per sottogruppi, quozienti ed estensioni.

Dimostrazione. Sia G un gruppo risolubile e sia $G = G^{(0)} > G^{(1)} > \ldots > G^{(d)} = 1$ la sua serie derivata.

Sia H ≤ G e proviamo che anche H è risolubile. Poiché per ogni i ≥ 0 si ha $H^{(i)} \leq G^{(i)}$, allora $H^{(d)} \leq G^{(d)} = 1$; in particolare dl(H) ≤ d = dl(G).

Sia ora K ◁ G e proviamo che anche G/K è risolubile.

Poiché $\forall aK, bK \in G/K$ si ha [aK, bK] = [a, b]K, allora (G/K)' = G'K/K e, per induzione, $\left(G/K\right)^{(i)} = G^{(i)}K/K$ per ogni i ≥ 0. Allora $\left(G/K\right)^{(d)} = G^{(d)}K/K = K/K = 1$, per cui G/K è risolubile e dl(G/K) ≤ d = dl(G).

Sia infine G un gruppo contenente un sottogruppo normale K tale che K ed U = G/K siano risolubili e proviamo che G è risolubile. Per quanto precede, si ha $G^{(i)}K/K = \left(G/K\right)^{(i)} = U^{(i)}$ per ogni i, quindi se m = dl(U) allora

$$G^{(m)}K/K = \left(G/K\right)^{(m)} \cong U^{(m)} = 1 \Rightarrow G^{(m)} \leq K$$

Ma se n = dl(K) si ha ora $G^{(m+n)} = \left(G^{(m)}\right)^{(n)} \leq K^{(n)} = 1$, quindi G è risolubile e dl(G) ≤ m+n.

Osservazioni. **1)**. Da 6.5 segue che il prodotto diretto di due gruppi risolubili è risolubile.
2). La classe dei gruppi abeliani, chiusa per sottogruppi, quozienti e prodotti diretti, non è chiusa per estensioni: infatti S_3 non è abeliano pur essendo A_3 ed S_3/A_3 abeliani.

Date due serie subnormali Σ e T, si dice che T è *più fine* (o *raffinamento*) di Σ se ogni termine di Σ è anche termine di T. Questa è una relazione d'ordine tra le serie subnormali di G. Il raffinamento si dice *proprio* se esiste quanche sottogruppo di G che sia termine di T ma non termine di Σ.

Diremo che due serie subnormali Σ e T sono *isomorfe* se esiste una biiezione dall'insieme dei fattori di Σ a quello dei fattori di T tale che fattori corrispondenti siano isomorfi. Questa è una relazione d'equivalenza tra le serie subnormali di G. Si osservi che due serie subnormali isomorfe restano tali anche eliminando i termini ripetuti, e quindi i fattori banali, poiché tali fattori devono corrispondersi nell'isomorfismo. Citiamo ora senza dimostrazione due importanti teoremi sulle serie subnormali.

TEOREMA 6.6. (Schreier). Due serie subnormali di G possiedono sempre raffinamenti isomorfi.

Una serie subnormale si dice *serie di composizione* se i suoi termini sono tutti distinti e non ha raffinamenti propri.

Può accadere che una serie subnormale abbia tutti i termini normali in G; in tal caso è detta *serie normale*. Una serie normale in cui non si possano inserire altri termini normali in G è detta *serie principale*.

Un gruppo G non banale si dice *semplice* se i soli suoi sottogruppi normali sono 1 e G. Per esempio, se |G| è primo, per il teorema di Lagrange G non ha altri sottogruppi che se stesso ed 1, quindi è certamente semplice. I gruppi semplici non abeliani non sono ovviamente risolubili: l'unica serie subnormale che possiedono è $1 = G_0 \lhd G_1 = G$, che non è abeliana.

TEOREMA 6.7. a) Una serie subnormale è una serie di composizione se e solo se i suoi fattori sono tutti semplici.
b) Una serie normale è principale se in ciascun fattore non ci sono sottogruppi, propri e non banali, invarianti per automorfismi.

TEOREMA 6.8. (Jordan, Hölder, Dedekind). Sia G un gruppo con una serie di composizione Σ. Allora:
a) Ogni serie subnormale [normale] T si può raffinare fino ad ottenere una serie di composizione [principale].
b) Tutte le serie di composizione [principali] sono isomorfe tra loro.

Dimostrazione. Per il teorema di Schreier, le serie Σ e T hanno raffinamenti isomorfi, ma il raffinamento di Σ, eliminati i termini ripetuti, coincide con Σ, dunque anche il raffinamento T' di T, eliminati i termini ripetuti, è una serie di composizione [principale]. Se poi T è a sua volta una serie di composizione [principale], coincide con T', dunque è isomorfa a Σ.

TEOREMA 6.9. Sono equivalenti per un gruppo finito G:
a) G è risolubile.
b) G ha una serie di composizione a fattori ciclici d'ordine primo.
c) G ha una serie principale a fattori abeliani elementari.

Dimostrazione. Se G è finito e risolubile, raffinando una serie abeliana si ottiene una serie di composizione a fattori contemporaneamente abeliani e semplici, dunque ciclici d'ordine primo. Raffinando invece la serie derivata, che è normale, si

ottiene una serie principale con i fattori abeliani e privi di sottogruppi caratteristici, quindi abeliani elementari. Inversamente, sia le serie di composizione a fattori ciclici d'ordine primo, sia le serie principali a fattori abeliani elementari sono serie abeliane.

Dato un gruppo G, un sottogruppo P si dice *normale minimo* se è normale non banale e da $1 \leq K \leq P$, $K \lhd G$, segue $K = 1$ oppure $K = P$.

Un sottogruppo M si dice *massimale* in G se da $M \leq S \leq G$ segue $S = M$ oppure $S = G$. Si ha:

PROPOSIZIONE 6.10. Sia G un gruppo finito risolubile.

a) Sia P un sottogruppo normale minimo. Allora P è un p-gruppo abeliano elementare.

b) Sia M un sottogruppo massimale. Allora [G:M] è la potenza di un primo.

Dimostrazione. a) La serie normale 1, P, G si raffina ad una serie principale, di cui tutti i fattori, compreso $P \cong P/1$, sono p-gruppi abeliani elementari.

b) Procediamo per induzione rispetto a |G|, essendo vero il risultato se $|G| = 1$. Sia P un sottogruppo normale minimo P di G. Per a), P è abeliano elementare d'ordine p^k per un certo primo p ed un certo k. Se $P \leq M$ allora [G:M] = [G/P:M/P] è potenza di un primo per ipotesi induttiva. Se P non è incluso in M, allora $M < PM$, quindi $PM = G$. Sia $L = P \cap M$: si ha $L \lhd P$, perché P è abeliano, e $L \lhd M$, perché $P \lhd G$. Ne segue $G = PM \leq N_G(L)$, cioè $L \lhd G$. Per la minimalità di P, deve essere di conseguenza $L = 1$. Ma allora $|G| = |P| \cdot |M|$, cioè $[G:M] = |G|/|M| = |P| = p^k$.

Osservazione. Il risultato precedente è falso per i gruppi non risolubili: per esempio, A_5 è normale minimo in S_5, ma non è un p-gruppo abeliano elementare. Inoltre, in A_5 si ha $n_5 = 6$, dunque A_5 ha un sottogruppo M d'indice 6, necessariamente massimale per il teorema di Poincaré, ma 6 non è la potenza di un primo.

OSSERVAZIONE. Mediante la *teoria dei caratteri*, W. Burnside (inizio 900) provò che se p, q sono primi e $|G| = p^a q^b$, G è risolubile. M la teoria dei *caratteri modulari*, Feit e Thompson nel 1963 provarono che se |G| è dispari allora G è risolubile.

Siano $|G| = \prod_{i=1}^{n} p_i^{\alpha_i}$, p_i primo, $\pi(G) = \{p_1, \ldots, p_n\}$, $\pi = \{p_{i_1}, \ldots, p_{i_r}\} \subseteq \pi(G)$. Un sottogruppo H il cui ordine sia multiplo solo dei primi $p_{i_j} \in \pi$ è detto *π-sottogruppo* di G e, se ha ordine $|H| = \prod_{j=1}^{r} p_{i_j}^{\alpha_{i_j}}$, è detto *π-sottogruppo di Hall* di G.

Per un π-sottogruppo di Hall H di G si ha (|H|, [G:H]) = 1. Viceversa, se (|H|, [G:H]) = 1, posto π = π(H), H è un π-sottogruppo di Hall di G.

Per |π| = 1 si ritrovano le nozioni di p-sottogruppo e di p-sottogruppo di Sylow. Se |π| > 1, non è però detto esista un π-sottogruppo di Hall. Per esempio, A_5 non ha sottogruppi d'ordine 15. Inoltre, a differenza di quanto accade per i p-sottogruppi di Sylow, se esistono π-sottogruppi di Hall di G, non è detto che siano coniugati, o che ogni π-sottogruppo sia incluso in un π-sottogruppo di Hall. Tuttavia si hanno i seguenti importanti risultati, dei quali non si riporta la dimostrazione, e che coinvolgono la risolubilità:

TEOREMA 6.11. (Schur - Zassenhaus). Se un gruppo finito G ha un sottogruppo di Hall K normale in G ed inoltre almeno uno tra K e G/K è risolubile, allora K ha un complemento in G, due qualunque complementi di K sono coniugati in G ed inoltre ogni sottogruppo d'ordine primo con |K| è incluso in uno di tali complementi.

Osservazione. Poiché (|K|, [G:K]) = 1, almeno uno dei due fra |K| e |G/K| è dispari. Per il teorema di Feit-Thompson, l'ipotesi di risolubilità di K o di G/K è quindi automaticamente verificata.

TEOREMA 6.12. (P. Hall). Se G è un gruppo finito e risolubile, per ogni $\pi \subseteq \pi(G)$ esiste un π-sottogruppo di Hall, ogni altro π-sottogruppo è incluso in uno di essi e due π-sottogruppi di Hall sono coniugati.

§ 7. Polinomi e frazioni algebriche

In alcuni testi universitari (p. es. G. Scorza Dragoni) si vede talora la nozione di polinomio $p(x) = \sum_{k=0}^{n} a_k \cdot x^k$ come *funzione polinomiale* $p : K \to K$, dove K è il campo reale o complesso, tale che $p(x) = \sum_{k=0}^{n} a_k \cdot x^k$. In questo caso, x è la *variabile* reale o complessa. I polinomi costituiscono il sottoanello K[x] dell'anello delle funzioni da K in sé, con le operazioni punto per punto, ma serve un teorema di unicità che affermi l'unicità dei coefficienti di p(x) (teorema d'identità dei polinomi), per potere tra l'altro parlare di grado di un polinomio. Il polinomio nullo è la costante nulla e non ha grado. Per gli altri polinomi, almeno un coefficiente è non nullo ed il grado è il massimo dei k tali che $a_k \neq 0$. Un lato negativo di questa definizione è che non si può generalizzare ad un anello commutativo A qualsiasi, e neppure ad un campo qualsiasi, perché non è detto valga il teorema d'identità: la funzione polinomiale nulla potrebbe scriversi infatti in forme diverse, anche con coefficienti non nulli. Funziona se A è un dominio d'integrità almeno numerabile.

Un modo alternativo (p. es. G. Corsi Tani) presenta un polinomio come successione $p : \mathbf{N} \to A$ in un anello commutativo A, nulla da un certo $n \geq 0$ in poi. Qui la x è un polinomio particolare, $x(n) = \begin{cases} 1_A & \text{se } n = 1 \\ 0_A & \text{se } n \neq 1 \end{cases}$. L'anello dei polinomi A[x] è un sottoanello dell'anello delle successioni $A^{\mathbf{N}}$, con le sue operazioni di addizione e convoluzione. Non serve in questo caso un teorema d'identitità, perché ogni successione è una funzione ed i coefficienti sono i suoi valori. Il grado è il massimo $n \in \mathbf{N}$ per il quale $p(n) \neq 0_A$. Il polinomio nullo è la successione nulla e non ha grado. Il polinomio x ha grado 1.

Un approccio più astratto e generale (p. es. Courant & Robbins, Israel) costruisce l'anello dei polinomi a coefficienti in un anello commutativo A come sottoanello generato dall'insieme $A \cup \{x\}$ in un qualsiasi anello commutativo B che contenga, oltre ad A, un elemento "trascendente" x rispetto ad A: i suoi elementi sono

del tipo $p = \sum_{k=0}^{n} a_k \cdot x^k$ e qui serve postulare il *principio d'identità dei polinomi*, espresso appunto dalla trascendenza di x rispetto ad A, in modo che i coefficienti siano univocamente determinati e poter parlare di grado. In questo caso, abbiamo una classe di "anelli di polinomi in una indeterminata" a coefficienti in A, isomorfi tra loro. Uno qualunque di essi può essere riguardato come A[x]. Possono rientrare in questo approccio i due precedenti, nel momento in cui si consideri come B rispettivamente l'anello A^A delle funzioni da A (dominio d'integrità infinito) in sé, con le operazioni punto per punto, in cui A è identificato con l'insieme delle funzioni costanti ed x è la funzione identità, oppure, rispettivamente, come B l'anello $A^{\mathbf{N}}$ delle successioni in A, in cui A è identificato con l'insieme delle successioni del tipo $(a, 0, 0, \ldots, 0, \ldots)$ ed x la successione più sopra definita $(0, 1, 0, \ldots, 0, \ldots)$.

Un approccio ancora diverso, presente in alcuni testi scolastici ed universitari, (p. es. Zappa, Vistoli) considera un polinomio come *parola* (non vuota) in un alfabeto comprendente: gli elementi dell'anello A, un oggetto x non appartenente ad A (detto "indeterminata"), i simboli + e -; sono date opportune regole di formazione, che evitino di avere in una parola due elementi di A consecutivi, o due "segni" +, - consecutivi, e di usare la notazione x^n in luogo di n lettere x consecutive. Occorre poi una relazione d'equivalenza tra le parole, che consenta riordini e semplificazioni, in modo che in ogni classe d'equivalenza, con l'eccezione della classe della parola 0_A, si abbia una ed una sola parola nella forma $a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n$, con $a_n \neq 0$; in tal caso, n si dice grado del polinomio. Si definiscono poi esplicitamente le operazioni, e dalle regole di formazione e dall'equivalenza si ricavano le proprietà. Il principio d'identità è conseguenza dell'unicità della scelta del rappresentante della classe in quella forma.

Si osservi infine che in alcuni testi, per esigenze didattiche non sempre condivise, talora si preferisce distinguere dapprima il caso dei monomi, della forma $a \cdot x^n$, $n \geq 0$, definire il grado di un monomio, la riduzione (somma) di monomi *simili*, il prodotto di monomi e, infine, i polinomi come *somma* (concreta o formale) di monomi. Il grado del polinomio, se non nullo, è allora il massimo dei gradi dei monomi. Ciò è possibile con l'approccio funzionale, in cui la somma è quella punto per punto, oppure in quello delle parole, in cui i monomi ed il segno + diventano il

nuovo alfabeto ed i polinomi le nuove parole. Non ha senso invece nel caso delle successioni ed in quello delle estensioni.

Comunque si faccia a definire l'anello dei polinomi A[x] a coefficienti nell'anello commutativo A, se A è un dominio d'integrità lo è anche A[x] e, se A è un campo, A[x] è un dominio euclideo. Il grado del prodotto di polinomi non nulli è la somma dei gradi dei fattori.

La nozione di *radice di un polinomio* p(x) a coefficienti in A è naturale nell'approccio funzionale: è un elemento c∈A tale che $p(c) = 0_A$. Negli altri approcci, per ogni c∈A occorre definire un operatore *sostituzione* $\mu_C : A[x] \to A$ che sia un omomorfismo di anelli e che consenta di trasformare ogni polinomio p in un elemento $p(c) = \mu_C(p)$ di A. Allora, c è radice del polinomio p se p appartiene al *nucleo* $\mathrm{Ker}(\mu_C)$ di μ_C, ossia se $p(c) = \mu_C(p) = 0_A$. Ci sono ovviamente dei vantaggi, soprattutto nel caso di un campo K, per il quale K[x] è euclideo e quindi ad ideali principali: all'elemento c∈A è associato l'ideale $\mathrm{Ker}(\mu_C)$ dei polinomi di cui c è radice, e questo ideale è generato da un suo polinomio di grado minimo, detto *polinomio minimo* di c. Lo svantaggio è però evidente: si usano concetti troppo complicati. Si ovvia a questa difficoltà dicendo che c è radice di $p = \sum_{k=0}^{n} a_k \cdot x^k$ se $\sum_{k=0}^{n} a_k \cdot c^k = 0_A$, dove qui i coefficienti a_k sono ripensati come elementi di A e non come polinomi costanti.

In tutti i casi, se A è un dominio d'integrità, se p(x) ha grado $n \geq 1$ e c è una sua radice, allora $p(x) = (x - c) \cdot q(x)$, dove q(x) ha grado n-1, e si trova con l'algoritmo di Ruffini-Horner. Ne segue che il numero delle radici di un polinomio non nullo non supera il grado. Inoltre, nasce il concetto di molteplicità di una radice.

Nelle applicazioni e nell'insegnamento si considerano in generale i polinomi con più di una lettera. L'approccio è naturalmente diverso nelle varie impostazioni.

Il più semplice concettualmente è, paradossalmente, quello dei polinomi come parole: nell'alfabeto, oltre agli elementi dell'anello A ed ai segni + e -, si considerano tutte le lettere che si vogliono: x, y, z, t, a , b, ... Si scrivono quindi le parole in questo alfabeto, con le stesse regole di formazione e con l'aggiunta dell'assioma di commutatività delle lettere. È utile distinguere dapprima il caso dei monomi, parlare

di grado di un monomio come numero delle lettere che lo compongono, poi procedere come per una sola indeterminata.

L'approccio funzionale è più difficile, per il fatto che è complicato scrivere esplicitamente l'espressione generale di un polinomio in più variabili; inoltre, il principio d'identità è meno immediato da dimostrare. Anche qui è utile parlare prima di monomi, di grado di un monomio e poi definire il grado di un polinomio non nullo come il massimo dei gradi dei suoi monomi.

L'approccio per successioni di coefficienti è impraticabile direttamente, dato che non è chiaro come ordinare i monomi in più indeterminate. Si procede allora ricorsivamente, definendo $A\left[x_1,\ldots,x_{n+1}\right]=\left(A\left[x_1,\ldots,x_n\right]\right)\left[x_{n+1}\right]$, ossia come l'anello dei polinomi nell'indeterminata x_{n+1}, a coefficienti nell'anello $A\left[x_1,\ldots,x_n\right]$. In questo caso, occorre dimostrare che ogni permutazione α delle lettere produce un isomorfismo degli anelli finali: $A\left[x_{\alpha(1)},\ldots,x_{\alpha(n)}\right]\cong A\left[x_1,\ldots,x_n\right]$. Anche qui è utile definire prima il grado di un monomio e poi definire il grado di un polinomio non nullo come il massimo dei gradi dei suoi monomi.

Lo stesso approccio induttivo si può usare nel caso astratto, considerando via via un sovra-anello B_{k+1} con un elemento trascendente x_{k+1} rispetto ad $A\left[x_1,\ldots,x_k\right]$. Però, l'astrazione dell'approccio funzionale si può fare direttamente, considerando l'estensione del campo (reale o complesso) K nell'anello delle funzioni da K^n a K mediante, per $1\le k\le n$, la proiezione x_k che associa ad ogni $\left(\xi_1,\ldots,\xi_n\right)\in K^n$ la k–esima coordinata ξ_k. Si pone cioè $K\left[x_1,\ldots,x_n\right]=\left\langle K\cup\left\{x_1,\ldots,x_n\right\}\right\rangle\le K^{\left(K^n\right)}$. Occorre ovviamente dimostrare un teorema di identità e definire il grado di un polinomio.

Comunque si faccia, anche se l'anello A dei coefficienti è un campo, quando le indeterminate sono due o più, non è possibile eseguire la divisione euclidea se non in casi particolari; perciò non si ottiene un dominio euclideo, e neppure ad ideali principali. Ci si deve accontentare di meno: se A è un dominio d'integrità *gaussiano* o *fattoriale*, ossia nel quale esiste ed è unica (sostanzialmente) la scomposizione in fattori primi, anche A[x] lo è, quindi, per induzione, lo è anche $A\left[x_1,\ldots,x_n\right]$. In particolare, se K è un campo, K[x] è un dominio euclideo, quindi fattoriale, ed allora

anche $K[x_1,\ldots,x_n]$ è fattoriale. Ossia, ogni polinomio di grado ≥ 1 o è primo (ossia *irriducibile* o *indecomponibile*) oppure è scomponibile in uno ed un solo modo in fattori primi, a meno dell'ordine dei fattori e della presenza di fattori costanti.

La classificazione dei polinomi irriducibili è fuori discussione, e così pure lo studio delle radici, che riguarda quella parte della matematica detta "Geometria Algebrica". Una certa importanza nelle applicazioni ha la ricerca dei generatori di un ideale, mediante le *basi di Groebner*.

Il passaggio successivo è dai polinomi alle frazioni algebriche. Poiché si parte classicamente da un dominio d'integrità A, anche $A[x_1,\ldots,x_n]$ lo è, comunque sia stato definito. Allora è possibile costruire il *suo campo dei quozienti*, che risulta essere costituito dalle classi di equivalenza delle frazioni $\frac{p(x_1,\ldots,x_n)}{q(x_1,\ldots,x_n)}$, ossia delle coppie ordinate di polinomi, nelle quali il secondo, il denominatore, è diverso dal polinomio nullo. Poiché $A[x_1,\ldots,x_n]$ è un dominio fattoriale, allora ogni frazione è equivalente ad un'altra ridotta ai minimi termini, ottenuta dividendo numeratore e denominatore per il (un) loro MCD. Nel caso astratto è più o meno tutto: si può semplificare una frazione, eseguire operazioni, trasformare espressioni con frazioni algebriche.

Nel caso funzionale, per A = **R** o A = **C,** la situazione è assai differente. Infatti, ogni funzione razionale fratta $\frac{p(x_1,\ldots,x_n)}{q(x_1,\ldots,x_n)}$ ha il campo di esistenza costituito dalle n-uple $(x_1,\ldots,x_n)$ che non annullano il denominatore. Ne segue che le due funzioni fratte $\frac{p(x_1,\ldots,x_n)}{q(x_1,\ldots,x_n)}$ e $\frac{p(x_1,\ldots,x_n)\cdot h(x_1,\ldots,x_n)}{q(x_1,\ldots,x_n)\cdot h(x_1,\ldots,x_n)}$ in generale non sono la stessa funzione. Pertanto, o si rinuncia a parlare di campo e si procede con i teoremi di Analisi Matematica (nel caso di A = **R** o A = **C**) oppure si cambia l'equivalenza.

In particolare, secondo un altro approccio, due funzioni razionali fratte si dicono equivalenti se si ottengono l'una dall'altra mediante un numero finito di passaggi del tipo: moltiplicare o semplificare numeratore e denominatore per un polinomio non nullo. Allora si ottiene una relazione d'equivalenza, compatibile con le operazioni punto per punto, nella quale frazioni equivalenti non hanno però lo stesso

dominio. Si ottiene allora che, data una frazione $\frac{p(x_1,\ldots,x_n)}{q(x_1,\ldots,x_n)}$ col numeratore che non sia il polinomio nullo, il prodotto per la sua reciproca $\frac{q(x_1,\ldots,x_n)}{p(x_1,\ldots,x_n)}$ dà una frazione equivalente alla frazione $\frac{1}{1}$, cioè all'elemento neutro. Si ottiene così che le classi di frazioni equivalenti formano un campo, isomorfo al campo dei quozienti dell'anello $A[x_1,\ldots,x_n]$.