1

Capitolo B41
semigruppi, gruppi, anelli, campi

Contenuti delle sezioni

a. semigruppi p. 3
b. gruppi [1] p. 7
c. anelli p. 21
d. campi p. 25
e. polinomi p. 27

30 pagine

B41 0.01 Come si è già osservato, nella matematica svolgono un ruolo essenziale le **strutture algebriche**, sia per l'organizzazione formale del complesso delle sue conoscenze, sia per la precia definizione della portata di vari algoritmi e di metodi di calcolo che fanno riferimento a caratterizzazioni 'a algebriche.

Le strutture algebriche più semplici e fondamentali sono costituite da un insieme, il cosiddetto **terreno della struttura**, da alcune costruzioni che da una o due elementi del terreno ricavano un altro suo elemento, costruzioni che sono dette **leggi di composizione della struttura**.

Queste composizioni si possono considerare generalizzazioni delle usuali operazioni numeriche.

In molte strutture si assegnano ruoli particolari a singoli elementi del terreno.

Il terreno di una struttura può essere finito, numerabile, continuo e può essere introdotto costruttivamente o essere definito formalmente precisando solo le sue caratteristiche mediante assiomi.

Le strutture ora abbozzate sono chiamate **strutture algebriche monoterreno**; altre strutture più articolate presentano due o più insiemi che fanno da terreni, leggi di composizione che riguardano uno, due o, raramente, più terreni e anche elementi dei terreni con ruoli specifici.

Le singole operazioni e spesso coppie di operazioni sono caratterizzate da proprietà formali che sono presentate soprattutto come uguaglianze di espressioni nelle quali intervengono elementi generici o specifici dei terreni con i ruoli di operandi e di operazioni binarie e unarie.

Lo studio delle strutture algebriche si concentra sulle proprietà formali delle composizioni e si propone di dimostrare proprietà valide per ampie gamme di situazioni; questo in effetti permette di realizzare elevate economie di pensiero e trattazioni di risultati di interesse generale notevolmente compatte.

B41 0.02 In questo capitolo prenderemo in considerazione solo strutture algebriche monoterreno per le quali, semplificando, useremo il solo termine "strutture".

Consideriamo due strutture i cui terreni potrebbero essere diversamente individuati e potrebbero avere diversi cardinali, ma che presentano due sistemi di operazioni che si trovano in una corrispondenza biunivoca che rispetta i generi e le proprietà delle operazioni. Queste strutture si dicono strutture appartenentire alla stessa **specie di strutture**.

Assegnamo alla stessa specie anche due strutture con lo stesso terren e con due sistemi di operazioni diversi i quali si trovano in una corrispondenza biunivoca che rispetta i loro generi e le loro proprietà.

Una specie di strutture monoterreno è quindi caratterizzata dalle sue leggi di composizione, ossia dalle sue operazioni, da suoi elementi specifici e dalle proprietà formali che coinvolgono tutti i loro componenti.

Gli studi dell'algebra si sviluppano a diversi livelli di generalità e di astrattezza. Al livello delle specie di strutture si studiano le proprietà che dipendono solo dalle proprietà formali delle leggi di composizione, mentre le indagini sulle strutture apecifiche in generale si devono occupare anche delle caratteristiche dei rispettivi terreni.

Altri studi perseguono due scopi: quello di individuare delle sottospecie, cioè sottoinsiemi delle specie che differiscono per proprietà diverse da quelle che qualificano le specie e lo scopo di precisare le relazioni che collegano le sottospecie e di collocare le strutture specifiche nelle varie sottospecie.

In questo capitolo si perseguono due obiettivi: introdurre tipi di entità (corredati da loro termini e da loro notazioni) che conviene avere presenti quando si affrontano nuovi temi; introdurre alcuni modi di procedere di elevata generalità tipici dell'algebra.

Il raggiungimento di questi obiettivi spesso consente di realizzare elevate economie di pensiero e vantaggi nella organizzazione delle conoscenze grazie alla individuazione di proprietà che valgono per intere specie di strutture o per loro ampie sottospecie e grazie al riconoscimento che strutture definite con costruzioni specifiche e in relazione a soluzioni di problemi possono assegnarsi alle suaccennate sottospecie.

B41 0.03 Il capitolo tratta le specie di strutture algebriche monoterreno più note e utilizzate.

Le prime due, i semigruppi e i gruppi, presentano una sola operazione binaria. Ai semigruppi si chiede solo che l'operazione di cui sono muniti sia associativa e questo consente di individuare facilmente semigruppi il cui terreno è costituito da enti matematici molto semplici e fondamentali come stringhe e numeri interi ed enti di largo uso come relazioni e funzioni.

I gruppi si possono considerare semigruppi la cui operazione binaria sia dotata di inversa, proprietà che rende i gruppi in grado di affrontare e chiarire un gran numero di problemi: si noti in particolare che le endofunzioni di un qualsiasi insieme costituiscono un semigruppo, mentre le privilegiate endofunzioni invertibili costituiscono un gruppo.

Vengono poi introdotti gli anelli, strutture più ricche delle precedenti in quanto munite di due operazioni binarie di cui solo una dotata di inversa; in particolare è un anello l'insieme dei numeri interi munito delle ben note operazioni di somma (la cui operazione inversa è la differenza) e di prodotto.
La disponibilità di queste due operazioni rende gli anelli, rispetto ai gruppi, degli strumenti collocabili in posizioni più avanzate sul fronte della risoluzione dei problemi.

Successivamente si introducono i campi, strutture che si possono vedere come anelli particolarmente efficaci, grazie alla possibilità per risolvere problemi che si presentano molto spesso.

B41 a. semigruppi

B41 a.01 Diciamo **semigruppo** una `struttura algebrica (wi)` costituita da un insieme nonvuoto, detto terreno del semigruppo, e da un'operazione binaria associativa definita su tale insieme.

Più formalmente un semigruppo è una coppia $\langle A, * \rangle$ con A insieme nonvuoto ed $*$ operazione binaria associativa su A, cioè funzione del genere $* \in \lceil A \times A \longmapsto A \rceil$ tale che

$$\forall a, b, c \in A \ : \ a * (b * c) \ = \ (a * b) * c \ .$$

Riprendendo nozioni definite in precedenza si riconoscono facilmente molti semigruppi.

[1] L'insieme $\{1, 2, 3, 4\}$ munito della operazione "scelta del massimo tra due numeri" che possiamo scrivere $\max(m, n)$: per l'associatività basta osservare che, evidentemente, sia $\max(\max(m, n), p)$ che $\max(m, \max(n, p))$ individuano il maggiore dei tre numeri m, n e p; questo rende lecito denotare tale numero con $\max(m, n, p)$.

[2] L'insieme dei numeri interi positivi munito dell'addizione, operazione notoriamente associativa); la struttura $\langle \mathbb{P} \ , \ + \rangle$ viene detta **semigruppo additivo degli interi positivi**.

[3] L'insieme dei numeri interi naturali munito della moltiplicazione (anche questa operazione è notoriamente associativa); tale struttura, cioè $\langle \mathbb{P} \ , \ \cdot \rangle$, viene detta **semigruppo moltiplicativo degli interi naturali**.

[4] L'insieme, numerabile, di tutte le stringhe di lunghezza positiva sopra un dato alfabeto A formato da 2 o più caratteri dotato della giustapposizione tra stringhe; questa struttura si chiama **semigruppo libero** su A e si può denotare con $\langle \mathsf{A}^+ \ , \ _{\shortmid} \rangle$.

[5] La collezione dei sottoinsiemi di un qualsiasi insieme U munita dell'operazione di unione, operazione evidentemente associativa.

[6] La collezione dei sottoinsiemi di un qualsiasi insieme U munita dell'intersezione, operazione notoriamente associativa.

[7] Per un qualsiasi insieme U costituisce semigruppo l'insieme $\mathbf{Endo}(U)$ di tutte le endofunzioni definite sopra U munito del prodotto di composizione tra funzioni, in quanto anche questa operazione è associativa.
Infatti se consideriamo $f, g, h \in \mathbf{Endo}(U)$ e $x \in U$ e usiamo per le applicazioni la composizione destra-sinistra, cioè se definiamo $(f \circ_{rl} g)(x) := f(g(x))$, sia l'endofunzione $(f \circ_{lr} g) \circ_{lr} h$ che la $f \circ_{lr} (g \circ_{lr} h)$ applicate al generico $x \in U$ forniscono $f(g(h(x)))$.

[8] L'insieme dei numeri naturali pari munito della somma che possiamo scrivere $\langle 2 \cdot \mathbb{N} \ , \ + \rangle$.

[9] L'insieme dei numeri naturali pari munito del prodotto $\langle 2 \cdot \mathbb{N} \ , \ \cdot \rangle$.

B41 a.02 Una distinzione immediatamente comprensibile vede da una parte i semigruppi finiti, aventi come terreno un insieme finito, e dall'altra i semigruppi infiniti.

Tra gli esempi precedenti [1] è semigruppo finito, mentre i terreni dei semigruppi [2], [3], [4], [8] e [9] sono insiemi numerabili.

Gli esempi [5], [6] e [7] prescindono completamente dalla natura dell'insieme nel quale sono ambientati e permettono di considerare collezioni di semigruppi che si incontrano di frequente.
Essi si basano su tipiche argomentazioni che si avvalgono della generalità e della astrazione della nozione di insieme che viene consentita dall'approccio assiomatico [B66b].

Dato che $\mathfrak{P}(U)$ ed **Endo**(U) sono insiemi finiti sse U è un insieme finito, possiamo affermare che i semigruppi [5], [6] e [7] sono finiti se i corrispondenti ambienti U sono finiti.

Si dice **cardinale di un semigruppo** il cardinale del suo insieme terreno. Occorre segnalare che spesso tale entità viene chiamata "ordine" del semigruppo.
Il semigruppo [1] ha ordine 4 e la sua operazione di binaria viene presentata dalla tavola di composizione costituita dalla seguente matrice di profilo 4×4

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 2 & 3 & 4 \\ 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 \end{bmatrix} .$$

La simmetria della matrice rende evidente che l'operazione binaria di quasto semigruppo è commutativa.

B41 a.03 In generale un semigruppo con l'operazione commutativa si dice **semigruppo commutativo** o **semigruppo abeliano**. Anche i semigruppi [2], [3], [5], [6], [8] e [9] sono commutativi.

Non è invece commutativo il semigruppo libero [4], in quanto la giustapposizione di stringhe su due o più caratteri non è commutativa.

Non è commutativo neppure il semigruppo [7] di tutte le endofunzioni di un qualsiasi insieme ambiente U formato da 2 o più elementi.
Per questo basta considerare il controesempio di due endofunzioni che non commutano. Consideriamo due elementi diversi di $U \overset{\searrow}{} \; x$ e y e le corrispondenti funzioni a valore costante x^{cstnt} e y^{cstnt} che conviene denotare come trasformazioni postfisse, da scrivere a destra dell'argomento, e quindi definire mediante la $\forall z = 1, 2, 3, 4 : z\, x^{cstnt} := x$ (equivalente alla $x^{cstnt}(z) := x$) .
Con tale notazione risulta ovvio che per le due composizioni delle due endofunzioni si ha

$$x^{cstnt} \circ_{lr} y^{cstnt} \;=\; y^{cstnt} \;\neq\; y^{cstnt} \circ x^{cstnt} \;=\; x^{cstnt} .$$

B41 a.04 In molti dei semigruppi esaminati in precedenza si individua un elemento neutro (bilatero) per l'operazione binaria.

Osserviamo preliminarmente che un tale elemento di semigruppo deve essere unico: infatti supposta la presenza di due elementi neutri e ed e' sarebbe $e = e * e' = e'$.

Osserviamo alcuni esempi precedenti.

Per il semigruppo [1] è elemento neutro il numero minimo dell'insieme terreno;
del semigruppo [3] il numero 1 è l'elemento neutro;
per il semigruppo [5] elemento neutro è l'insieme vuoto;
per il semigruppo [6] elemento neutro è l'insieme ambiente U;
per il semigruppo [7] elemento neutro è la endofunzione identità di U.

Si constata invece che non si può avere un elemento neutro in alcuno dei semigruppi [2], [4], [8] e [9].

I semigruppi contenenti un elemento neutro li chiamiamo **semigruppi uniferi**.

B41 a.05 Chiamiamo **monoide** una struttura costituita da una terna $\langle A, *, e \rangle$ dove $\langle A, * \rangle$ è un semigruppo ed $e \in A$ è l'elemento neutro per $*$.
Quando l'operazione binaria è commutativa si parla di **monoide abeliano**.

Oltre ai monoidi ottenibili dall'iniziale elenco di semigruppi uniferi conviene considerarne alcuni altri.

Viene detto **monoide singoletto**, una struttura il cui terreno è costituito da un solo elemento che composto con se stesso si riproduce. Può essere individuata dalla scrittura $\langle\{1\},\cdot,1\rangle$.

Ogni semigruppo $\langle A,*\rangle$ può venire trasformato in un monoide semplicemente aggiungendogli un elemento e scelto fuori da A (possiamo chiamarlo "nuovo elemento") e definendo $e{*}e := e$, $e{*}a := a =: a{*}e$ per ogni $a \in A$.
Per esempio il precedente semigruppo [2] viene ampliato in un monoide aggiungendogli l'intero 0 e il semigruppo libero [4] con l'aggiunta della stringa muta diventa il monoide $\langle \mathsf{A}^*, \text{ }, \sqcup \rangle$ chiamato **monoide libero su un alfabeto** A.

B41 a.06 Si può considerare inversa della precedente la manovra che, dato un monoide $\boldsymbol{S} = \langle S,*,e\rangle$, elimina il suo elemento neutro e, nonché la riga e la colonna che lo rappresentano nella tavola di composizione; essa evidentemente porta a un semigruppo, in quanto la suddetta riduzione mantiene la sua associatività.

Il semigruppo così ottenuto potrebbe o meno contenere un elemento neutro per $S \setminus \{e\}$; nel caso di presenza di un nuovo elemento neutro si potrebbe procedere a una ulteriore riduzione.

Può essere utile presentare un elenco di coppie costituite da un semigruppo unifero e dal monoide associato. In particolare si hanno:

Semigruppo additivo degli interi positivi – monoide additivo degli interi naturali .

Semigruppo libero delle stringhe su A, senza $\sqcup$ – monoide libero delle stringhe su A, $\sqcup$ inclusa .

In seguito alle precedenti considerazioni si può dire che lo studio dei semigruppi e lo studio dei monoidi sono strettamente collegati.

B41 a.07 Il collegamento tra semigruppi uniferi e monoidi si esprime formalmente servendosi di un cosiddetto **operatore dimenticanza**.

Per ogni sequenza a di h componenti e per ogni $I \subset \{1,2,...,h\}$ si definisce come operatore dimenticanza relativo ad I e si denota con $\boldsymbol{Frgt}_I$ la trasformazione che alla a fa corrispondere la sequenza ottenuta eliminando tutte le componenti delle posizioni i appartenenti a I.
In particolare interessano le dimenticanze di singole componenti i che denotiamo con $\boldsymbol{Frgt}_i$, ossia con la semplificazione-se della $\boldsymbol{Frgt}_{\{i\}}$.

L'operatore dimenticanza, una sorta di proiettore applicabile alle sequenze, risulta utile per segnalare collegamenti tra strutture esprimibili come sequenze e anche tra intere specie di tali strutture.

In particolare possiamo affermare che per un qualsiasi monoide $\boldsymbol{M} = \langle M{*},e\rangle$ $\boldsymbol{Frgt}_3(\boldsymbol{M}) = \langle M,*\rangle$ è un semigruppo e più comprensivamente, che $\boldsymbol{Frgt}_3(\mathsf{Mnd}) = \mathsf{Sgrp}$.

Conveniamo allora di dichiarare che ogni monoide è una **struttura più attrezzata** o una **struttura più ricca** del corrispondente semigruppo. Al livello più comprensivo delle specie di strutture si può dichiarare che la specie dei monoidi è una **specie di strutture più ricca** della specie dei semigruppi.

Equivalentemente si dice che i semigruppi costituiscono una **specie di strutture più povera** della specie dei monoidi.

Evidentemente le relazioni "essere struttura più ricca" e "essere struttura più povera" sono relazioni di ordine stretto, l'una la trasposta dell'altra.

B41 a.08 Nella trattazione di molti sviluppi della matematica, come vedremo, si incontrano enunciati che possono essere semplificate al fine di evitare giri di frase eccessivamente verbosi.

Per le strutture algebriche momoterreno come semigruppi e monoidi si possono segnalare tre tipi di semplificazioni.

Il primo consiste nella sostituzione di una struttura come un semigruppo o un monoide (o un gruppo, ...) con il suo terreno; questo non risulta ambiguo quando l'operazione binaria si può sottintendere (per la tradizione del tema trattato, per le consuetudini dell'auditorio al quale ci si rivolge o per la influenza del contesto).

Un esempio di semplificazione di questo tipo si riscontra quando il semigruppo delle endofunzioni dell'insieme U viene individuato come se fosse il semplice insieme $\mathbf{Endo}(U)$.

Il secondo tipo di semplificazione riguarda la semplificazione di un termine come "elemento del terreno di un semigruppo" (o di un monoide, o di un gruppo, ...) con "elemento di un semigruppo" (o di un monoide, o di un gruppo, ...).

Accade per esempio di dire che il passaggio di un intero nel suo opposto è un elemento del monoide delle endofunzioni di $\mathbb{Z}$.

Il terzo tipo di semplificazione si riscontra quando due strutture una più ricca dell'altra vengono discusse come se avessero lo stesso livello di ricchezza.

Un esempio consiste nel dichiarare che il semigruppo moltiplicativo degli interi pari è contenuto nel monoide moltiplicativo degli interi $\mathbb{Z}$.

Eserc. 1 Individuare le semplificazioni dei tipi sopra segnalati che si incontrano nel successivo b01.

B41 b. gruppi [1]

B41 b.01 I gruppi sono strutture algebriche di grande importanza e la teoria dei gruppi [`teoria dei gruppi (wi)`] è una parte della matematica particolarmente ricca di risultati che si è dimostrata in grado di fornire efficaci strumenti a molti altri settori della matematica (geometria, combinatoria, ...) e a molte sue applicazioni.
In particolare ha un ruolo importante nella `meccanica classica (wi)`, nella `meccanica quantistica (wi)`, nella `strutturistica chimica (wi)` e nella `cristallografia (wi)`.
Inoltre è notevole la sua influenza sugli algoritmi e sull'architettura.

Come si è visto in B20f, i gruppi si possono introdurre mediante due approcci complementari. Si possono introdurre i cosiddetti **gruppi astratti** come insiemi muniti di operazioni che soddisfano determinati assiomi

In alternativa si introduce in modo più costruttivo un gruppo come sottoinsieme "privilegiato" dell'insieme di tutte le endofunzioni di un insieme che può essere scelto senza alcuna restrizione; per un tale insieme strutturato si usa il termine **gruppo di trasformazioni**.

Il "pregio" che si richiede per primo alle trasformazioni che costituiscono un gruppo consiste nel fatto che ciascuna di esse possieda l'inversa, ossia che si tratta di endofunzioni biiettive, cioè di permutazioni. Evidentemente il pregio dell'invertibilità si mantiene con la composizione delle endofunzioni e con la stessa loro inversione; di conseguenza le permutazioni sopra un qualsiasi insieme si possono comporre e invertire senza restrizioni.

Tra le permutazioni di un qualsiasi insieme ambiente U va inclusa anche la trasformazione identità Id_U; in effetti la sua presenza viene presupposta anche quando si richiede la presenza di una trasformazione inversa per ogni permutazione.

Ci proponiamo quindi di esaminare le strutture costituite da endofunzioni invertibili aventi la forma $\langle G, \circ_{lr}, {}^{-\mathbf{1}}, \mathsf{Id}_U \rangle$, con $G \subseteq \lceil U \lhd\!\!\longrightarrow\!\!\rhd U \rceil$, dove U può denotare qualsiasi insieme.
Conveniamo che l'insieme U sia chiamato "campo d'azione del gruppo", mentre l'insieme G delle permutazioni viene detto "il terreno" della struttura gruppo, come accade per tutte le altre strutture qualificate, per questo, come "monoterreno".

Qui e nel seguito con il segno da usare come operatore unario postfisso "$-\mathbf{1}$" denotiamo la funzione che a ogni biiezione, non solo a ogni permutazione costituente un gruppo, fa corrispondere la biiezione inversa.

Va osservato che per due biiezioni qualsiasi f e g si ha

$$(f \circ_{lr} g)^{-\mathbf{1}} \;=\; g^{-\mathbf{1}} \circ f^{-\mathbf{1}} \;.$$

La struttura più comprensiva tra i gruppi che hanno U come campo d'azione, ossia $\langle \lceil U \lhd\!\!\longrightarrow\!\!\rhd U \rceil, \circ_{lr}, {}^{-\mathbf{1}}, \mathsf{Id}_U \rangle$, viene detta gruppo totale delle permutazioni di U o **gruppo simmetrico** di U e viene denotato con Sym_U.

B41 b.02 Dei gruppi astratti si possono dare varie definizioni formali; qui ne diamo una che presenta alcune ridondanze, ma che consente di ottenere le proprietà basilari dei gruppi più direttamente di altre definizioni più concise, prive di ridondanze.

Diciamo **gruppo** una struttura algebrica della forma $\boldsymbol{G} = \langle G, \odot, {}^{-1}, e \rangle$ dove
(1) G è un insieme che costituisce il terreno del gruppo;

(2) $\odot$ è un'operazione binaria su G che gode della proprietà associativa: $\forall a, b, c \in R \ : \ a \odot (b \odot c) = (a \odot b) \odot c$;
(3) e è elemento neutro bilatero per l'operazione di prodotto, cioè $\forall a \in G : \ a \odot e = e \odot a = a$;
(4) $^{-1}$ è l'operazione unaria che a ogni $a \in G$ associa l'elemento che denotiamo con a^{-1} e per il quale $a \odot a^{-1} = a^{-1} \odot a = e$.

Quando si considera un gruppo generico l'operazione binaria di solito viene chiamata prodotto e spesso invece di $a \odot b$ si scrive $a \cdot b$ o anche semplicemente $a\,b$; inoltre l'elemento neutro di solito viene chiamato **unità**.

Un gruppo $\boldsymbol{G}$ il cui prodotto è commutativo, cioè tale che $\forall a, b \in G \ : \ a \odot b = b \odot a$, si dice **gruppo commutativo** o **gruppo abeliano**.

B41 b.03 Vediamo alcuni gruppi finiti, cioè gruppi il cui terreno è un insieme finito, cominciando con alcuni di essi costituiti da pochi elementi.

Molti dei gruppi con terreno ridotto si individuano efficacemente dando esplicitamente le loro tavole di composizione, cioè la rappresentazioni sotto forma di matrice dell'azione dell'operazione prodotto; questa matrice nel caso dei gruppi viene spesso chiamata spesso **tavola di moltiplicazione** o **tavole di Cayley**, in onore di Arthur Cayley.

I gruppi di due e tre elementi sostanzialmente si riducono ai due caratterizzati dalle seguenti tavole di Cayley

	1	-1
1	1	-1
-1	-1	1

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

.

Il primo si può considerare isomorfo a Sym_2 [b24]; il secondo è un gruppo ciclico di tre elementi [b16].

È sensibilmente più elaborato e interessante il gruppo Sym_3 che consideriamo come gruppo delle permutazioni dell'insieme $\{1, 2, 3\}$.

	e	(12)	(13)	(23)	(123)	(132)
e	e	(12)	(13)	(23)	(123)	(132)
(12)	(12)	e	(123)	(132)	(13)	(23)
(13)	(13)	(132)	e	(123)	(23)	(12)
(23)	(23)	(123)	(132)	e	(12)	(13)
(123)	(123)	(23)	(12)	(13)	(132)	e
(132)	(132)	(13)	(23)	(12)	e	(123)

.

Questo gruppo si può anche considerare il gruppo delle simmetrie di un triangolo regolare nel piano. Per questo conviene contrassegnare i vertici del triangolo con 1, 2 e 3 e visualizzare la permutazione ciclica $\langle_{cy} 1, 2, 3\rangle$ che denotiamo anche con (123), come il movimento rigido del triangolo che manda il vertice 1 nel vertice 2, il vertice 2 in 3 e 3 in 1. In tal modo gli scambi (12), (23) e (13) esprimono riflessioni del piano rispetto agli assi del triangolo, mentre la permutazione ciclica (132) è l'inversa della (123); queste due si visualizzano come le rotazioni rispetto al centro del triangolo di 120° nei versi, risp., orario e antiorario.

B41 b.04 Si denota con V_K e si dice **Viergruppe** o gruppo di Klein (in onore di Felix Klein), il gruppo di 4 elementi caratterizzato dalla seguente tavola di Cayley:

	e	h	v	c
e	e	h	v	c
h	h	e	c	v
v	v	c	e	h
c	c	v	h	e

Questa tavola, osservando la sua simmetrica rispetto alla diagonale principale e il fatto che tutte le caselle della diagonale stessa contengono l'unità, dice che si tratta di un gruppo abeliano il quale, oltre all'elemento unità, presenta tre involuzioni.

Esso si può interpretare come gruppo delle simmetrie di un rettangolo nonquadrato che conviene pensare con i lati maggiori disposti orizzontalmente; con tale raffigurazione la involuzione h riguarda la riflessione ripetto alla sua linea mediana orizzontal, la v corrisponde alla riflessione riapetto alla linea mediana verticale e la c alla rotazione di 180° intorno al suo centro.

Questo gruppo si può anche interpretare come il gruppo costituito delle seguenti 4 trasformazioni del piano combinatorio $\mathbb{Z} \times \mathbb{Z}$ (ma anche dei piani $\mathbb{Q} \times \mathbb{Q}$ e $\mathbb{R} \times \mathbb{R}$): e, identità del piano, h, riflessione rispetto all'asse orizzontale, v riflessione rispetto all'asse verticale e c riflessione rispetto all'origine o simmetria centrale.

Segnaliamo anche che molti altri gruppi finiti con pochi elementi sono presentati in `Small groups (we)`.

B41 b.05 Introduciamo una successione di gruppi finiti elementari.

Consideriamo l'intero positivo $m = 2, 3, 4, ...$ e ricordiamo le seguenti nozioni introdotte in B25b06:

congruenza modulo m $=_m$;
le m classi di questa relazione $[0]_m$, $[1]_m$, $[2]_m$, ..., $[m-1]_m$;
l'insieme di queste classi $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$;
l'operazione di somma modulo m $+_m$.

Definiamo come **gruppo ciclico degli interi modulo** m :

$$\mathbb{Z}_{mGrp} := \left\langle \mathbb{Z}_m, +_m, \left\lceil\, [h]_m \in \mathbb{Z}_m \mapsto [m-h]_m \,\right\rceil, [0]_m \right\rangle$$

Negli sviluppi argomentati nelle quali risulta evidente che si esaminano le suddette nozioni si possono adottare le semplificazioni che emergono dalla seguente riscrittura (non molto razionale) della definizione precedente:

$$\mathbb{Z}_m := \langle \mathbb{Z}_m, +, -, 0 \rangle \ .$$

Le tavole di Cayley di questi gruppi si ottengono facilmente. Per esempio per $m = 5$:

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

.

B41 b.06 Tra le permutazioni di un insieme U si possono evidenziare quelle che non modificano una determinata entità $\boldsymbol{I}$ associata a U; questa $\boldsymbol{I}$ può essere un sottoinsieme di U, una costruzione che si serve di elementi di U o una relazione che coinvolge elementi di U.

Evidentemente una tale $\boldsymbol{I}$ viene conservata dalla azione successiva di due permutazioni che la conservano, dalla permutazione inversa di ogni permutazione che la conserva e dalla identità Id_U.

Questa situazione si esprime dicendo che l'insieme delle permutazioni di U che rispettano la $\boldsymbol{I}$ è un insieme chiuso per la composizione, e che, munito della composizione costituisce un gruppo.

Siamo quindi indotti a prendere in considerazione anche la struttura ottenuta dalla Sym_U riducendo il terreno all'insieme delle permutazioni che lasciano invariata la $\boldsymbol{I}$ e riducendo di conseguenza prodotto, passaggio all'inverso e e identità.

Evidentemente ciascuna di queste strutture costituisce un gruppo di permutazioni di U e viene chiamata **sottogruppo di permutazioni** del gruppo Sym_U. L'entità $\boldsymbol{I}$ viene detta **invariante** che caratterizza il sottogruppo.

B41 b.07 Vediamo alcuni esempi di richieste di conservazione che portano a sottogruppi.

(1) non modificare, ovvero mantenere fissi, uno o più elementi di U;
(2) rispettare un sottoinsieme V di U, cioè trasformare ogni elemento di V in un elemento di V; rispettare più sottoinsiemi di U;
(3) rispettare una data partizione di U, cioè trasformare gli elementi di ciascun blocco della partizione in altri elementi dello stesso blocco (questo tipo di richiesta costituisce un rafforzamento della richiesta di (2));
(4) mantenere determinate relazioni tra gli elementi di U: un caso evidente riguarda le permutazioni dei nodi di un grafo che mantengono l'adiacenza [D35];
(5) conservare i valori di determinate funzioni definite sugli elementi di U; questa richiesta nel caso di funzioni con un insieme finito di valori si può presentare intuitivamente come mantenimento di colori assegnati agli elementi di U.

Vediamo anche gli invarianti che caratterizzano le precedenti richieste.

Le proprietà di conservazione nelle richieste (1) riguardano l'invarianza di elementi dell'ambiente.

Per le richieste (2) gli invarianti sono le relazioni di appartenenza a specificati sottoinsiemi.

Più in particolare le richieste (3) riguardano il mantenimento dell'appartenenza a ciascun blocco della partizione.

Nel caso (4) si mantiene l'appartenenza o meno delle coppie di elementi dell'ambiente U a una relazione del genere $R \subset U \times U$.

Le richieste (5) riguardano una o più funzioni che si vogliono invarianti.

B41 b.08 In generale diciamo **gruppo di permutazioni** ogni struttura della forma $\langle G, \circ, {}^{-\mathbf{1}}, \mathsf{Id}_U \rangle$ con G sottoinsieme della totalità delle permutazioni di un dato campo d'azione U che sia chiuso rispetto alla composizione di tali permutazioni e rispetto al passaggio alla permutazione inversa.

Va segnalato che mediante richieste di conservazione come le precedenti si ottengono gruppi di permutazioni di grande interesse.

Questo risulta particolarmente notevole quando gli insiemi ambiente U presentano caratteristiche geometriche o sono dei sistemi fisici, ad esempio sistemi atomici o cristalli.

Per esempio tra le permutazioni di un piano come $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q} \times \mathbb{Q}$ o $\mathbb{R} \times \mathbb{R}$ si distinguono quelle che mantengono le quadranze (e le distanze) tra i punti, le trasformazioni chiamate isometrie [B46].

Tra le isometrie di $\mathbb{R} \times \mathbb{R}$ per molti problemi conviene privilegiare quelle che mantengono fisso un punto C; queste sottopongono tutti i rimanenti punti a rotazioni intorno a C dello stesso angolo e sono chiamate **rotazioni** di centro C.

Tra queste si possono ulteriormente scegliere quelle che trasformano in se un poligono regolare con centro in C, per esempio un esagono regolare con il centro nell'origine.
Per questa figura si hanno sei rotazioni che costituiscono un gruppo di sei elementi. Tra queste si possono selezionare le rotazioni che trasformano in se uno dei due triangoli regolari individuati da una terna di vertici che a coppie non sono estremi di un lato dell'esagono (in effetti queste rotazioni conservano entrambi i triangoli ottenibili in questo modo); con questa restrizione si individua un gruppo costituito solo da tre delle precedenti rotazioni.

Abbiamo quindi individuato una sequenza di richieste di invarianza via via più stringenti a ciascuna delle quali corrisponde un sottogruppo di $\mathsf{Sym}(\mathbb{R} \times \mathbb{R})$; chiaramente al crescere delle richieste di invarianza corrisponde il ridursi del terreno del sottogruppo.

Considerazioni come le precedenti si possono sviluppare per ogni genere di ambiente U e questo induce, genericamente, a prestare particolare attenzione alle relazioni tra i gruppi di permutazioni dei vari U che interessano i problemi di maggiore interesse. (in particolare alle relazioni "essere sottogruppo di") in collegamento con le relazioni tra gli insiemi di invarianti richiesti.

Segnaliamo anche che si studiano diversi tipi di geometrie (euclidea, iperbolica, parabolica, ...) caratterizzando ciascuna di esse con determianti sistemi di invarianti dei rispettivi gruppi di simmetria.

B41 b.09 I gruppi di permutazioni rivestono grandissima importanza in quanto sopra di essi si basa lo studio delle simmetrie di numerose entità (figure, strutture, relazioni, equazioni, costruzioni, sistemi fisici, ...) presi in considerazione dalla matematica, da molti capitoli della fisica e dalle varie altre discipline [v.o. e `Symmetry (we)`].

Per molte persone le simmetrie rivestono grande interesse grazie alle loro valenze estetico. Qui invece non ci azzardiamo ad affrontare questioni che conducono a fenomeni complessi riguardanti la psiche umana e ci limitiamo agli aspetti delle simmetrie che riguardano la loro utilità nello sviluppo e nella organizzazione delle conoscenze che possono influire su procedimenti risolutivi che presentano in misura affidabile caratteristiche quali riproducibilità, adattabilità, efficacia e precisione.

Consideriamo il caso delle permutazioni che lasciano invariato l'esagono regolare, permutazioni che costituiscono la struttura algebrica chiamata **gruppo dell'esagono**.

Oltre alle sei rotazioni viste in b07, sono da considerare anche le riflessioni rispetto alle 3 rette definite dalle tre coppie di vertici opposti e le riflessioni rispetto alle 3 rette che sono assi di simmetria per riflessione per ciascuna delle tre coppie di lati opposti.

Supponiamo di dover studiare una costruzione che inizia con un vertice o con un lato dell'esagono e prosegue con altri elementi (vertici, lati, angoli, bisettrici, corde, ...) da prendere in esame successivamente, fino ad ottenere un oggetto geometrico (punto, segmento, distanza, configurazione, ...) che goda di determinati requisiti.

La conoscenza del gruppo delle simmetrie dell'esagono, cioè delle simmetrie della configurazione alla quale si rivolge la costruzione, dice quali altre costruzioni portano a risultati con gli stessi requisiti ottenibili applicando una qualsiasi delle permutazioni del gruppo a tutti i passi della costruzione stessa.

In tal modo la conoscenza del gruppo di simmetria consente di controllare intere collezioni di costruzioni, e dunque apre la strada a economie di pensiero e a risparmi in elaborazioni di rilevanza applicativa.

Queste economie possono risultare molto vantaggiose, sia per attività specifiche, sia in interi settori lavorativi, sia per la organizzazione complessiva di interi settori di conoscenze.

Stante questa prospettiva risulta evidente la convenienza di studiare con sistematicità gruppi di permutazioni di vari generi di campi d'azione e in particolare di permutazioni di configurazioni discrete e di procedure.

Dal punto di vista dell'assetto teorico, lo studio delle simmetrie risulta determinante in molte analisi che hanno l'obiettivo di classificare tutte le strutture che soddisfano determinate proprietà.

Per esempio esse sono cruciali per la determinazione delle collezioni di tutti i poliedri caratterizzati da proprietà delle facce, degli spigoli e dei vertici [D33].

B41 b.10 Procediamo ora a presentare le più evidenti proprietà generali dei gruppi.

Facciamo riferimento a un gruppo $\boldsymbol{G} = \langle G, \cdot, ^{-1}, e\rangle$ e per essere più concisi adottiamo semplificazioni espositive ampiamente diffuse che non dovrebbero portare effettive ambiguità.

Una prima semplificazione consiste nel trascurare le occorrenze dell'operazione $\cdot$ tra due operandi.
Spesso poi con il solo terreno si richiama l'intera struttura; questo modo di esprimersi si può applicare a ogni struttura monoterreno o con un insieme che si impone come tale; lo chiamiamo **identificazione struttura-terreno**.

Inoltre, se H e K sono sottoinsiemi di G, scriviamo $H \cdot K := \{h \in H, k \in K :| \ h \cdot k\}$ e $H^{-1} := \{h \in H :| \ h^{-1}\}$, cioè non distinguiamo le operazioni "$\cdot$" e "$^{-1}$" dalle rispettive estensioni booleane.

Dati due gruppi $\boldsymbol{G} = \langle G, \cdot, ^{-1}, e\rangle$ e $\boldsymbol{H} = \langle H, \odot, j, u\rangle$, si dice che $\boldsymbol{H}$ è **sottogruppo** di $\boldsymbol{G}$ e si scrive $\boldsymbol{H} \leq_{Grp} \boldsymbol{G}$ sse $H \subset G$, $u = e$ e le operazioni $\odot$ e j si ottengono come riduzioni, risp., di $\cdot$ e j indotte dalla riduzione di G ad H.
Se $\boldsymbol{H} \leq_{Grp} \boldsymbol{G}$ si dice anche che $\boldsymbol{G}$ è sovragruppo di $\boldsymbol{H}$ e si scrive $\boldsymbol{G} \geq_{Grp} \boldsymbol{H}$.
Se in particolare H è sottoinsieme proprio di G si dice che $\boldsymbol{H}$ è **sottogruppo proprio** di $\boldsymbol{G}$ e si scrive $\boldsymbol{H} <_{Grp} \boldsymbol{G}$.

Spesso le scritture $\boldsymbol{H} \leq_{Grp} \boldsymbol{G}$ e $\boldsymbol{H} <_{Grp} \boldsymbol{G}$ si abbreviano, risp., con le scritture $H \leq G$ e $H < G$.
Queste abbreviazioni, come altre analoghe, sono accettabili senza timori nei contesti che non coinvolgono strutture diverse dai gruppi.

B41 b.11 Ogni gruppo $\boldsymbol{G}$ possiede il sottogruppo banale costituito solo dalla sua unità e il sottogruppo improprio $\boldsymbol{G}$.

(1) Prop.: Sia $H \subset G$. $H <_{Grp} G \iff H \cdot H^{-1} \subseteq H$.

Dim.: "$\Longrightarrow$" $H < G$ equivale alle tre relazioni $e \in H$, $H^{-1} \subseteq H$ e $H \cdot H \subseteq H$. Di conseguenza $H \cdot H^{-1} \subseteq H \cdot H \subseteq H$.
"$\Longleftarrow$" Per ogni $a \in H$, $a \cdot a^{-1} \in H$, ovvero $e \in H$. $H^{-1} = e \cdot H^{-1} \subseteq H \cdot H^{-1} \subseteq H$. Per la terza relazione e per l'ipotesi $H \cdot H \subseteq H \cdot H^{-1} \subseteq H$ ∎

B41 b.12 Introduciamo il **gruppo additivo degli interi** $\mathbb{Z}_{ag} := \langle \mathbb{Z}, +, -, 0\rangle$, ove $-$ denota il meno unario) e per ogni $z \in \mathbb{Z}$ consideriamo gli insiemi $z \cdot \mathbb{Z} := \{k \in \mathbb{Z} :| \ k \cdot z\}$.

Si osserva che $0 \cdot \mathbb{Z} = \{0\}$, cioè $\{0\}$ costituisce il sottogruppo banale di $\mathbb{Z}_{ag}$, che $-z \cdot \mathbb{Z} = z \cdot \mathbb{Z}$ e che $1 \cdot \mathbb{Z} = \mathbb{Z}$ costituisce il cosiddetto sottogruppo improprio di $\mathbb{Z}_{ag}$.

Prop. I sottogruppi di $\mathbb{Z}_{ag}$ costituiscono la famiglia $\lceil m \in \mathbb{N} \nrightarrow m \cdot \mathbb{Z} \rceil$.

Dim.: Ciascuno degli insiemi $m \cdot \mathbb{Z}$ è terreno di un sottogruppo di $\mathbb{Z}_{ag}$: infatti contiene 0, la sua unità, coincide con l'insieme dei suoi inversi (i numeri opposti) e per ogni $n_1, n_2 \in \mathbb{Z}$ si ha $m\,n_1 + m\,n_2 = m(n_1 + n_2)$, ovvero $\forall m \in \mathbb{Z} \ : \ m \cdot \mathbb{Z} + m \cdot \mathbb{Z} = m \cdot \mathbb{Z}$.

Viceversa troviamo che ogni H terreno di un sottogruppo di $\mathbb{Z}_{ag}$ deve avere la forma $z \cdot \mathbb{Z}$. Infatti, se H non è il sottogruppo banale, deve contenere un intero nonnullo e il suo inverso, cioè deve contenere almeno un intero positivo; denotato con m il minimo di tali possibili interi positivi, per ogni altro $n \in H$ si può scrivere $n = q\,m + r$ con $r \in \mathbf{[}m\mathbf{)}$; ma $r = n - q\,m$ deve appartenere ad H e per la minimalità di m deve essere $r = 0$ e quindi ogni elemento di H è un multiplo di m ∎

B41 b.13 Come vedremo in seguito, oltre a $\mathbb{Z}_{ag}$ presentano interesse vari altri gruppi numerici.

$\mathbb{Q}_{ag} := \langle \mathbb{Q}, +, -, 0 \rangle$, gruppo additivo dei razionali.
$\mathbb{R}_{ag} := \langle \mathbb{R}, +, -, 0 \rangle$, gruppo additivo dei reali [B42].
$\mathbb{C}_{ag} := \langle \mathbb{C}, +, -, 0 \rangle$, gruppo additivo dei complessi [B50].
$\mathbb{Q}_{+:mg} := \langle \mathbb{Q}_+, \cdot, ^{-1}, 1 \rangle$, gruppo moltiplicativo dei razionali positivi.
$\mathbb{Q}_{nz:mg} := \langle \mathbb{Q}_{nz}, \cdot, ^{-1}, 1 \rangle$, gruppo moltiplicativo dei razionali.
$\mathbb{R}_{+:mg} := \langle \mathbb{R}_+, \cdot, ^{-1}, 1 \rangle$, gruppo moltiplicativo dei reali positivi [B42].
$\mathbb{R}_{mg} := \langle \mathbb{R}_{nz}, \cdot, ^{-1}, 1 \rangle$, gruppo moltiplicativo dei reali [B42].
$\mathbb{C}_{nz:mg} := \langle \mathbb{C}_{nz}, \cdot, ^{-1}, 1 \rangle$, gruppo moltiplicativo dei complessi [B50].

Conviene segnalare che sono terreni di gruppi additivi e moltiplicativi anche l'insieme dei numeri algebrici e l'insieme dei reali costruibili [B38].

Ricordando l'importante distinzione tra i gruppi abeliani dotati di operazione binaria commutativa e i gruppi nonabeliani, osserviamo che tutti i precedenti gruppi numerici sono abeliani.

B41 b.14 L'insieme delle potenze positive e negative di un elemento a di un gruppo G, $P := \{z \in \mathbb{Z} :| \ a^z\}$, costituisce un sottogruppo di G: infatti da due elementi generici di questo sottoinsieme P che scriviamo $g := a^q$ ed $h := a^r$ si ottiene $g \cdot h^{-1} = a^{q-r}$, cioè un altro elemento di P e questo consente di applicare b11(1).

Questo sottogruppo viene detto **sottogruppo ciclico generato da** a o sottogruppo delle potenze di a e qui lo individuiamo con la notazione $\langle a \rangle_{\mathsf{G}}$.

Evidentemente ogni guppo ciclico è un gruppo abeliano.

Ogni elemento di un qualsiasi gruppo, dunque, genera un sottogruppo ciclico.

Per alcuni gruppi e alcuni loro elementi il corrispondente sottogruppo ciclico è un gruppo finito, mentre in altri casi è infinito numerabile.

Quindi a livello astratto si distinguono i gruppi ciclici finiti della forma $\{a, a^2, a^3, ..., a^m = e\}$ e i gruppi ciclici infiniti come $\mathbb{Z}_{ag}$.

B41 b.15 Consideriamo due gruppi $\boldsymbol{G}_i = \langle G_i, \bullet_i, j_i, e_i \rangle$ per $i = 1, 2$. Si dice **prodotto diretto dei due gruppi** il gruppo che ha come terreno il prodotto cartesiano dei terreni $G := G_1 \times G_2$, come unità la coppia delle due unità $\langle e_1, e_2 \rangle$, come prodotto la funzione che a partire da due coppie di G $\langle g_1, g_2 \rangle$ e $\langle h_1, h_2 \rangle$ fornisce la coppia ottenuta con i prodotti delle componenti dei due gruppi $\langle g_1 \bullet_1 h_1, g_2 \bullet_2 h_2 \rangle$ (prodotto componente per componente) e come risultato del passaggio all'inverso la coppia dei rispettivi inversi. (operazione unaria componente per componente).

Questo gruppo lo denotiamo con

$$\boldsymbol{G}_1 \times \boldsymbol{G}_2 := \left\langle G_1 \times G_2, \bullet_1 \times \bullet_2, j_1 \times j_2, \langle e_1, e_2 \rangle \right\rangle ,$$

dove per le due operazioni introdotte intendiamo:

$\langle g_1, g_2\rangle(\bullet_1 \times \bullet_2)\langle h_1, h_2\rangle = \langle g_1 \bullet_1 h_1, g_2 \bullet_2 h_2\rangle$,

$\langle g_1, g_2\rangle(j_1 \times j_2) = \langle g_1 j_1, g_2 j_2\rangle$

e l'uguaglianza dell'unità

$\langle g_1, g_2\rangle(\bullet_1 \times \bullet_2)\langle g_1 j_1, g_2 j_2\rangle = \langle e_1, e_2\rangle$.

B41 b.16 La costruzione prodotto diretto di gruppi consente di definire a partire da gruppi noti nuovi gruppi più articolati che possono costituire efficaci strumenti di indagine.

L'esempio più semplice è il prodotto diretto del gruppo moltiplicativo su $\{1, -1\}$ con se stesso: il suo terreno è

$\{\langle 1, 1\rangle, \langle 1, -1\rangle, \langle -1, 1\rangle, \langle -1, -1\rangle\}$, la sua unità $\langle 1, 1\rangle$ e le due operazioni il prodotto componente per componente e la trasformazione da $\langle \pm 1, \pm 1\rangle$ a $\langle \mp 1, \mp 1\rangle$.

Altri esempi poco impegnativi sono costituiti dagli insiemi delle coppie dei numeri interi, oppure razionali, oppure reali muniti della somma termine a termine.
Questi gruppi possiamo denotarli, risp., con $(\mathbb{Z} \times \mathbb{Z})_{ag}$, $(\mathbb{Q} \times \mathbb{Q})_{ag}$ e $(\mathbb{R} \times \mathbb{R})_{ag}$. Evidentemente si tratta di gruppi abeliani; più in generale è evidente che i prodotti diretti di gruppi abeliani sono gruppi abeliani.

Per ogni $d = 2, 3, 4, ...$ si possono considerare gli insiemi delle d-uple (terne, quaterne,...) di elementi di un gruppo $\boldsymbol{G} = \langle G, \odot, j, e\rangle$ e munirli della estensione cartesiana della operazione $\odot$, cioè della applicazione componente per componente della operazione $\odot$. Un tale gruppo lo chiamiamo potenza diretta d-esima del gruppo $\boldsymbol{G}$.

In accordo con queste locuzioni i precedenti tre gruppi additivi di coppie di numeri sono anche chiamati quadrati diretti, risp., di $\mathbb{Z}_{ag}$, di $\mathbb{Q}_{ag}$ e di $\mathbb{R}_{ag}$.

Particolarmente importanti per la geometria e quindi per la fisica e per tutte le loro applicazioni sono $(\mathbb{R} \times \mathbb{R})_{ag}$ e $(\mathbb{R}^{\times 3})_{ag}$, gli ambienti nei quali si collocano la geometria del piano e la geometria dello spazio tridimensionale [B43, B45].

B41 b.17 Consideriamo un gruppo $\boldsymbol{G} = \langle G, \cdot, ^{-1}, e\rangle$, un suo elemento a e un suo sottogruppo H.

Si dice **laterale destro** o **coset destro** di H in G rappresentato da a l'insieme $H \cdot a := \{h \in H :|\ h\, a\}$.

Si definisce invece **laterale sinistro** o **coset sinistro** di H in G rappresentato da a l'insieme $a \cdot H := \{h \in H :|\ h\}$.

Le due nozioni precedenti si possono definire mutuamente duali-LR in quanto le due definizioni si possono ottenere l'una dall'altra mediante la riflessione delle espressioni sulle quali si basano.

Definiamo la relazione entro G $^{\searrow}\sim_{*H}$ ponendo:

$$\forall a, b \in G \ : \ a \sim_{*H} b \iff b \in a \cdot H \iff a^{-1}b \in H \iff (a^{-1}b)^{-1} = b^{-1}a \in H \iff a \in b \cdot H \ .$$

Evidentemente $\sim_{*H}$ è una relazione di equivalenza e la sua classe contenente l'elemento g è proprio $g \cdot H$: infatti $g = g\, e$ e, dato che e appartiene al sottogruppo H, $g \in g \cdot H$.

Similmente ogni laterale destro può essere definito come classe d'equivalenza per una relazione di equivalenza $\sim_{H*}$ duale-LR della precedente:

$$\forall a, b \in G \ : \ a \sim_{H*} b \iff b \in H \cdot a \iff b\, a^{-1} \in H \iff (b\, a^r ecE)^{-1} = a\, b^{-1} \in H \iff a \in H \cdot b \ .$$

Ovviamente per un gruppo abeliano i laterali sinistri di un suo qualsiasi sottogruppo coincidono con i suoi laterali destri; nel caso di un gruppo nonabeliano questo avviene solo per particolari sottogruppi.

Consideriamo un intero $m = 2, 3, ...$, il gruppo additivo degli interi $\mathbb{Z}_{ag}$ e il suo sottogruppo $m \cdot \mathbb{Z}$.
I laterali (sinistri e destri) di tale sottogruppo sono gli m insiemi numerabil

$$m \cdot \mathbb{Z},\ m \cdot \mathbb{Z} + 1,\ m \cdot \mathbb{Z} + 2,\ ...,\ m \cdot \mathbb{Z} + m - 1\ .$$

B41 b.18 Osserviamo che, a causa delle due equivalenze $\sim_{H*}$ e $\sim_{*H}$, sia i laterali sinistri che i destri del gruppo G sono sottoinsiemi mutuamente disgiunti del terreno del gruppo.

Per ogni gruppo G, ogni $H \leq_{Grp} G$ e ogni $g \in G$ la funzione $\lceil\, h \in H \mapsto g\,h \,\rceil$ è una biiezione tra H e il laterale sinistro $g \cdot H$ e dualmente-LR la $\lceil\, h \in H \mapsto h\,g \,\rceil \in \lceil\, H \lhd\!\!\rightarrow\!\!\rhd H \cdot g \,\rceil$ è una biiezione tra H e il laterale destro $H \cdot g$.

Questo implica che tutti i laterali sinistri e destri di H in G hanno lo stesso cardinale di H.

Tale cardinale è detto **indice del sottogruppo** H nel gruppo G e in genere si denota con $(G : H)$; tale notazione esprime un numero che può essere sia finito che transfinito [B19f03].

Si osserva anche che la permutazione di un gruppo G che a ogni suo elemento fa corrispondere l'inverso stabilisce una biiezione tra i laterali destri e i laterali sinistri di un suo sottogruppo H.

B41 b.19 Se in particolare G è finito e denotiamo con n il suo cardinale e con k quella di H, si ha $n = k \cdot (G : H)$: si può quindi enunciare un classico risultato.

(1) Teorema (**teorema di Lagrange**) Il cardinale di ogni sottogruppo H di un gruppo finito G e il suo indice $(G : H)$ sono divisori del cardinale di G.

Da questo teorema si ricavano agevolmente varie proprietà dei gruppi finiti.
Preliminarmente segnaliamo che un gruppo privo di sottogruppi diversi dal sottogruppo banale e da se stesso si dice **gruppo semplice**.

Dal teorema di Lagrange segue subito che i sottogruppi di ogni gruppo finito G vanno ricercati tra i suoi sottoinsiemi il cui cardinale è un divisore di $|G|$.

Si può anche affermare che ogni gruppo finito il cui ordine è un numero primo è un gruppo semplice.
Inoltre ogni gruppo di ordine primo è un gruppo ciclico: infatti se g è un suo qualsiasi elemento diverso dalla sua unità, il sottogruppo delle potenze di g deve avere $|G|$ elementi e quindi deve coincidere con l'intero G.

B41 b.20 Si osserva che per ogni gruppo abeliano ciascuno dei suoi sottogruppi presenta la partizione nei laterali sinistri coincidente con quella dei laterali destri.

Esempi piuttosto evidenti di questi gruppi sono forniti dai gruppi che sono potenze dirette dei gruppi numerici additivi.

Consideriamo in particolare $(\mathbb{R} \times \mathbb{R})_{ag}$. Evidentemente tra i suoi sottogruppi vi sono quelli aventi come terreno $\{x \in \mathbb{R} :|\ \langle x, 0\rangle\}$ e $\{y \in \mathbb{R} :|\ \langle 0, y\rangle\}$, ossia quelli che in termini geometrici sono, risp., l'asse Ox e l'asse Oy.

I laterali di Ox sono gli insiemi

$$\{x \in \mathbb{R} :|\ \langle x, 0\rangle + \langle \overline{x}, \overline{y}\rangle\}\ =\ \{x \in \mathbb{R} :|\ \langle x, \overline{y}\rangle\}\ ,$$

per i vari $\overline{y} \in \mathbb{R}$ corrispondenti alle rette orizzontali, parallele all'asse Ox.

Dualmente-LR i laterali di Oy sono gli insiemi

$$\{y \in \mathbb{R} :|\ \langle 0, y\rangle + \langle \overline{x}, \overline{y}\rangle\}\ =\ \{y \in \mathbb{R} :|\ \langle \overline{x}, y\rangle\}\ ,$$

per i vari $\overline{x} \in \mathbb{R}$ corrispondenti alle rette verticali, parallele all'asse Oy.

Eserc. 1 Dimostrare che tutti i sottogruppi propri di $(\mathbb{Z} \times \mathbb{Z})_{ag}$ non ridotti all'elemento neutro $\langle 0, 0 \rangle$ corrispondono alle diverse rette-Z del piano passanti per l'origine.

Eserc. 2 Descrivere i sottogruppi e i sistemi di laterali del gruppo dell'esagono e del gruppo ciclico di cardinale 8.

B41 b.21 Un gruppo nonabeliano può avere sottogruppi con le due partizioni di laterali coincidenti e sottogruppi con le due partizioni diverse.

Un sottogruppo N di un gruppo G per il quale le due partizioni di G in laterali sinistri e in laterali destri coincidono, cioè tale che $\forall g \in G : g\,N = N\,g$, si dice **sottogruppo normale di un gruppo** G.
In particolare tutti i sottogruppi dei gruppi abeliani sono sottogruppi normali.

Si osserva che il prodotto di due laterali (bilateri) di un sottogruppo normale N è anch'esso un laterale di N: infatti se $g, h \in G$ si ha $(g\,N)(h\,N) = g\,h\,N\,N = (g\,h)\,N$.

Questo permette di definire come **gruppo quoziente** di un gruppo G e di un suo sottogruppo normale N il gruppo avente come terreno l'insieme dei laterali di N e avente come prodotto l'estensione booleana del prodotto di G.
Questo gruppo quoziente si denota con G/N.

Sym_3 non è un gruppo semplice, mentre lo è ogni gruppo di 5 elementi, ad esempio quello avente come tavola di composizione

	e	1	2	3	4
e	e	1	2	3	4
1	1	2	3	4	e
2	2	3	4	e	1
3	3	4	e	1	2
4	4	e	1	2	3

.

Più in generale si è trovato che i gruppi ciclici il cui cardinale è un numero primo sono gruppi semplici, mentre non lo sono i gruppi ciclici di cardinale fattorizzabile.

Possiamo affermare che i gruppi semplici sono i più essenziali, in quanto si trova che i gruppi non semplici si possono esprimere come opportune composizioni di gruppi semplici.
Lo studio dei gruppi semplici finiti riveste quindi grande importanza e va segnalato che la classificazione di tutti i gruppi semplici ha costituito uno dei maggiori successi della matematica della seconda metà del XX secolo [`Classification of finite simple groups (we)`, `gruppi finiti semplici (wi)`] .

Il comportamento di un gruppo G dotato di un sottogruppo normale N si può in buona parte spiegare riconducendosi al comportamento di N e di G/N.
In effetti molti comportamenti dei gruppi si possono ricondurre a comportamenti dei gruppi semplici. Questi quindi si possono considerare come i gruppi più essenziali, ovvero le strutture che individuano le simmetrie fondamentali che si possono ricercare in tutte le configurazioni discrete che possono essere utili a indagini di interesse applicativo.

B41 b.22 Riprendiamo a considerare un elemento a di un gruppo $\boldsymbol{G}$ e le sue successive potenze a, a^2, a^3, ...

Se $\boldsymbol{G}$ è finito queste potenze non possono essere tutte diverse e scorrendole si trova un intero naturale p, il più piccolo tale che sia $a^p = e$; da questa segue che $a^{-1} o a^{p-1}$; inoltre per ogni numero intero

positivo m si può scrivere $m = q\,p + r$ con $r \in [p)$ e $q \in \mathbb{Z}$; di conseguenza $a^m = a^r$ e le potenze di a costituiscono un gruppo ciclico finito.

Se invece $\boldsymbol{G}$ è infinito si possono avere elementi con un numero finito di potenze diverse ed elementi b con infinite potenze diverse, tutte riconducibili alla forma b^z con $z \in \mathbb{Z}$.

Si dice periodo dell'elemento a del gruppo G, e si denota con $\mathrm{prd}(a)$, il minimo intero positivo p per il quale $a^p = e$ se questo esiste, mentre per un elemento a per il quale questo elemento non si trova si pone $\mathrm{prd}(a) := +\infty$.

Ovviamente in un gruppo finito tutti gli elementi hanno periodo finito e in ogni gruppo l'unità è l'unico elemento di periodo 1.

Gli elementi di periodo 2, cioè gli elementi a caratterizzati dall'equazione $a^2 = e$, sono tutti e soli gli elementi che coincidono con il proprio inverso: infatti $a^2 = e$ sse $a = a^{-1}$. Essi sono quindi chiamati **involuzioni**.

La scelta del termine involuzione, nel caso di un gruppo di permutazioni è coerente con il termine usato per le particolari permutazioni di un generico campo d'azione che applicate due volte danno l'identità, o, equivalentemente, con le permutazioni coincidenti con la propria inversa.

Per chiarire questo punto a ciascuno degli elementi h di un qualsiasi gruppo G associamo la traslazione a sinistra e la traslazione a destra ponendo

$$h^{\mathsf{trslL}} := \lceil g \in G \mapsto h\,g \rceil \qquad \text{e} \qquad h^{\mathsf{trslR}} := \lceil g \in G \mapsto g\,h \rceil \ .$$

Per ogni gruppo queste endofunzioni sono più precisamente due permutazioni del suo terreno.

Nei gruppi additivi $\mathbb{Z}_{ag}$, $\mathbb{Q}_{ag}$, $\mathbb{R}_{ag}$ e $\mathbb{C}_{ag}$ tutti gli elementi diversi dall'elemento neutro, cioè da 0, hanno periodo infinito.
Nel gruppo moltiplicativo dei reali $\mathbb{R}_{mg} := \langle \mathbb{R}_{nz}, \cdot, {}^{-1}, 1\rangle$ e nei suoi sottogruppi $\mathbb{Q}_{mg}$ e $\mathbb{Z}_{mg}$ l'elemento -1 ha periodo 2, mentre tutti gli elementi diversi da 1 e -1 hanno periodo infinito.

B41 b.23 Consideriamo il gruppo i cui elementi sono le successioni infinite le cui componenti sono 1 o -1 e la cui operazione binaria è la moltiplicazione componente a componente; l'unità di questo gruppo è la successione avente tutte le componenti uguali ad 1 $1^{\mathbb{Z}} = \lceil z \in \mathbb{Z} \mapsto 1 \rceil$.
Tutti gli elementi di questo gruppo diversi dall'unità hanno periodo 2.

Un gruppo si dice **gruppo di torsione** sse tutti i suoi elementi hanno periodo finito; ovviamente tutti i gruppi finiti sono gruppi di torsione; il gruppo precedente è un gruppo di torsione infinito.

All'opposto un gruppo si dice **gruppo privo di torsione** sse tutti i suoi elementi diversi dall'unità hanno periodo infinito;

Sono gruppi privi di torsione $\mathbb{Z}_{ag}$, $\mathbb{Q}_{ag}$, $\mathbb{R}_{ag}$, $\mathbb{Q}_{mg}$, $\mathbb{Q}_{+\,mg}$, $\mathbb{R}_{mg}$ ed $\mathbb{R}_{+\,mg}$.

Un gruppo (infinito) si dice **gruppo misto** sse possiede sia elementi diversi dall'unità di periodo finito, che elementi di periodo infinito.
I gruppi moltiplicativi $\mathbb{Q}_{mg}$ e $\mathbb{R}_{mg}$ sono gruppi misti, in quanto il loro elemento -1 ha periodo 2 mentre tutti gli elementi diversi da 1 e -1 hanno periodo infinito.

In B50b risulta chiaro che un gruppo misto con infiniti elementi di periodo finito e infiniti elementi di periodo infinito è il gruppo moltiplicativo dei numeri complessi $\mathbb{C}_{mg}$: infatti per ogni $n = 3, 4, ...$ si trovano $n-1$ radici n-esime dell'unità che hanno periodo n [B50c03].

B41 b.24 Eserc. 1 Consideriamo il gruppo G, un suo elemento diverso dall'unità a e un intero positivo k. Dimostrare che:

(a) $a^k = e \implies \lceil\!\lceil\, k \in \mathrm{prd}(a) \cdot \mathbb{P} \ \wedge\ a^{-1} = a^{k-1} \,\rceil\!\rceil$.
(b) $\mathrm{prd}(a) = \mathrm{prd}(a^{-1})$.

Eserc. 2 Consideriamo il gruppo G e due suoi elementi diversi dall'unità a e b. Dimostrare che:
$\mathrm{prd}(a), \mathrm{prd}(b) \in \mathbb{P} \ \wedge\ a\,b = b\,a \implies \mathrm{prd}(a\,b) = \mathrm{prd}(b\,a) \nmid \mathrm{mcm}(\mathrm{prd}(a), \mathrm{prd}(b))$.

B41 b.25 In b05 abbiamo osservato che per ogni $m = 2, 3, 4, ...$ il gruppo ciclico $\mathbb{Z}_{mGrp}$ si comporta sostanzialmente come il gruppo delle rotazioni di un poligono regolare di m lati intorno al suo centro. Vogliamo ora generalizzare e chiarire formalmente questo tipo di relazione tra gruppi.

Consideriamo due gruppi $\boldsymbol{G} = \langle G, \odot, {}^{-1}, e\rangle$ e $\boldsymbol{H} = \langle H, *, j, u\rangle$
Si dice **isomorfismo** di $\boldsymbol{G}$ su $\boldsymbol{H}$ (o tra $\boldsymbol{G}$ e $\boldsymbol{H}$) una biiezione $\beta \in \lceil\!\lceil\, G \lhd\!\longrightarrow\!\rhd H \,\rceil\!\rceil$ che rispetta le operazioni delle due strutture, ossia tale che

$$\forall a, b \in G \ :\ \beta(a \odot b) = \beta(a) * \beta(b)\ ,\ \beta(a^{-1}) = (\beta(a))j\ ,\ \beta(e) = u\ .$$

Per affermare che $\boldsymbol{G}$ e $\boldsymbol{H}$ sono isomorfi si scrive $\boldsymbol{G} \lhd\!\longrightarrow\!\rhd_{Grp} \boldsymbol{H}$, mentre l'insieme degli isomorfismi tra $\boldsymbol{G}$ e $\boldsymbol{H}$ si denota con $\lceil\!\lceil\, \boldsymbol{G} \lhd\!\longrightarrow\!\rhd_{Grp} \boldsymbol{H} \,\rceil\!\rceil$.

Evidentemente la biiezione inversa dell'isomorfismo β è un isomorfismo di $\boldsymbol{H}$ su $\boldsymbol{G}$; è anche evidente che tutte le costruzioni, le dimostrazioni e le proprietà del gruppo $\boldsymbol{H}$ sono ottenuti applicando β alle corrispondenti coastruzioni, dimostrazioni e risultati di $\boldsymbol{G}$.

In particolare ogni gruppo isomorfo di un gruppo abeliano è un gruppo abeliano, a ogni sottogruppo di $\boldsymbol{G}$ corrisponde un sottogruppo di $\boldsymbol{H}$ che risulta isomorfo al gruppo precedente, a ogni famiglia di laterali (destri o sinistri) di $\boldsymbol{G}$ corrisponde una famiglia di laterali(destri o sinistri) di $\boldsymbol{H}$, il periodo di un $h := \beta(g) \in H$ coincide con il periodo di g.

Questa situazione spesso viene espressa colloquialmente con una frase del tipo "due gruppi isomorfi sono sostanzialmente uguali".

Presentiamo alcuni esempi di isomorfismi.

Il gruppo di Klein è isomorfo al quadrato diretto $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Ogni gruppo ciclico infinito è isomorfo al gruppo additivo dei naturali $\mathbb{Z}_{ag} = \langle \mathbb{Z}, +, -, 0\rangle$.

La funzione $\beta(x) = \mathsf{e}^x$ è un isomorfismo del gruppo additivo dei reali $\mathbb{R}_{ag}$ sul gruppo moltiplicativo dei reali positivi $\mathbb{R}_{+mg}$ e il suo isomorfismo inverso è fornito dalla funzione logaritmo naturale.

Altri isomorfismi tra questi due gruppi sono costituiti da funzioni esponenziali B^x e da $\log_B(y)$ per ogni reale $B \neq 1$.

B41 b.26 Se $\boldsymbol{H} = \boldsymbol{G}$ la biiezione β è una permutazione di G e viene detta **automorfismo**. L'insieme degli automorfismi di un gruppo $\boldsymbol{G}$ si denota con $\mathrm{Aut}(\boldsymbol{G})$

Ogni automorfismo di un gruppo è una permutazione del suo terreno, ossia per ogni gruppo $\boldsymbol{G}$ si ha $\mathrm{Aut}(\boldsymbol{G}) \subseteq \mathsf{Perm}(G)$.

Quindi l'insieme degli automorfismi di un gruppo munito della composizione costituisce esso stesso un gruppo di permutazioni.

Va segnalato che le caratteristiche del gruppo degli automorfismi di un gruppo $\boldsymbol{G}$ costituisce quasi sempre una caratterizzazione molto significativa dello stesso $\boldsymbol{G}$.

La relazione di isomorfismo tra gruppi è una relazione transitiva: infatti se G, H e K denotano tre gruppi e $\beta \in \lceil\!\lceil\, G \lhd\!\longrightarrow\!\rhd_{Grp} H \,\rceil\!\rceil$ e $\gamma \in \lceil\!\lceil\, H \lhd\!\longrightarrow\!\rhd_{Grp} K \,\rceil\!\rceil$ accade che

$$\forall a, b \in G \ :\ (\gamma \circ_{rl} \beta)_{\shortmid}(a\,b) = \gamma(\beta(a\,b)) = \gamma(\beta(a)\,\beta(b)) = \gamma(\beta(a)\,\gamma(\beta(b)) = ((\gamma \circ_{rl} \beta)_{\shortmid} a)\,(\gamma \circ_{rl} \beta)_{\shortmid} b) \ .$$

Quindi la relazione di isomorfismo tra gruppi, evidentemente riflesiva e simmetrica, è una relazione di equivalenza tra gruppi.

Il termine **gruppi astratti** viene spesso utilizzato per le denotare le classi della equivalenza $\lhd\!\!\longrightarrow\!\!\rhd_{Grp}$.

B41 b.27 Varie altre relazioni tra gruppi si possono assimilare all'isomorfismo tra gruppi.

Si dice **isomorfismo** di $\boldsymbol{G} = \langle G, \odot, {}^{-1}, e\rangle$ in $\boldsymbol{H}$ una funzione $\beta \in \lceil\, G \lhd\!\!\longrightarrow H \,\rceil$ che rispetta le operazioni delle due strutture.

L'immagine di un tale isomorfismo $\beta(\boldsymbol{G})$ è un gruppo in quanto il suo terreno $\beta(G)$ è chiuso per l'operazione $\beta^{-\mathbf{1}}$ e quindi per la $\beta({}^{-1})$ e contiene $\beta(e)$.
Quindi $\beta(\boldsymbol{G}) \subseteq_{Grp} \boldsymbol{H}$. È evidente anche che ogni isomorfismo "di su" è un particolare isomorfismo "di in".

Si dice **omomorfismo** di $\boldsymbol{G}$ in $\boldsymbol{H}$ una funzione $\omega \in \lceil\, G \longmapsto H \,\rceil$ che rispetta le operazioni delle due strutture, ossia tale che

$$\forall a, b \in G \;:\; \beta(a \odot b) = \beta(a) * \beta(b)\ ,\ \beta(a^{-1}) = (\beta(a))j\ ,\ \beta(e) = u\ .$$

In generale un omomorfismo non è una funzione invertibile; se in particolare lo fosse sarebbe un isomorfismo.

Come per gli isomorfismi si dimostra che il trasformato $\omega(\boldsymbol{G})$ è sottogruppo di $\boldsymbol{H}$.

Casi particolari degli omomorfismi di un gruppo in un altro sono gli omomorfismi di un gruppo su un altro. Un tale omomorfismo viene detto anche **epimorfismo**.

L'insieme degli omomorfismi di $\boldsymbol{G}$ in $\boldsymbol{H}$ si denota con $\lceil\, \boldsymbol{G} \longmapsto_{Grp} \boldsymbol{H} \,\rceil$, mentre l'insieme degli omomorfismi di $\boldsymbol{G}$ su $\boldsymbol{H}$ si denota con $\lceil\, \boldsymbol{G} \longmapsto\!\!\rhd_{Grp} \boldsymbol{H} \,\rceil$.

Per affermare che si trova un omomorfismo di $\boldsymbol{G}$ su $\boldsymbol{H}$ si scrive $\boldsymbol{G} \supseteq_{Grp} \boldsymbol{H}$. in questa espressione compare $\supseteq_{Grp}$ che è una relazione tra gruppi.

Si dimostra senza difficoltà che questa è una relazione d'ordine parziale tra classi di isomorfismo tra gruppi.

Va segnalato che lo studio di questa relazione fornisce molti chiarimenti sul complesso dei gruppi.

B41 b.28 Consideriamo due elementi g ed h di un gruppo G; essi si dicono **elementi coniugati del gruppo** sse esiste un altro elemento x del gruppo tale che $x\,g\,x^{-1} = h$.

Questa relazione per i gruppi abeliani è priva di interesse, in quanto ogni elemento x di un tale gruppo A è coniugato solo di se stesso, in forza della $\forall x, g \in A \;:\; x\,g\,x^{-1} = x\,x^{-1}\,g = g$.

(1) Prop.: La relazione di coniugio tra gli elementi di un gruppo è una equivalenza entro il terreno del gruppo.

Dim.: Infatti $e\,g\,e^{-1} = g$, quindi la relazione di coniugio è riflessiva;
da $x\,g\,x^{-1} = h$ segue $x^{-1}\,h\,x = g$, cioè il coniugio è una relazione simmetrica;
da $x\,g\,x^{-1} = h$ e $y\,h\,y^{-1} = k$ segue $y\,x\,g\,x^{-1}\,y^{-1} = (y\,x)g(y\,x)^{-1} = yhy^{-1} = k$, cioè che il coniugio è una relazione transitiva ∎

La partizione del terreno di un gruppo (nonabeliano) in classi di coniugio in genere presenta aspetti interessanti.
In particolare per ogni gruppo finito di permutazioni gli elementi di una classe di coniugio sono caratterizzati da un unico tipo di fattorizzazione in cicli.

B41 b.29 Riprendiamo più formalmente la nozione di automorfismo di un gruppo.

Una permutazione del terreno G di un gruppo $\boldsymbol{G}$ $\alpha \in \mathbf{Perm}(G)$ è un automorfismo di $\boldsymbol{G}$ sse sse $\forall a, b \in G \ : \ \alpha(a) \cdot \alpha(b) \ = \ \alpha(a \cdot b)$.

Denotiamo con $\mathrm{Aut}(\boldsymbol{G})$ l'insieme degli automorfismi del gruppo $\boldsymbol{G}$. Se $\alpha, \beta \in \mathrm{Aut}(\boldsymbol{G})$ anche la composizione $\alpha \circ \beta$ è automorfismo di $\boldsymbol{G}$. L'insieme degli automorfismi di un gruppo $\boldsymbol{G}$ munito del prodotto di composizione costituisce quindi un gruppo associato a $\boldsymbol{G}$ chiamato **gruppo degli automorfismi del gruppo $\boldsymbol{G}$**.

(1) Eserc. Dimostrare che, per ogni elemento x di un gruppo G l'applicazione $\alpha_x \ := \ \llbracket g \in G \mapsto x\, g\, x^{-1} \rrbracket$ è un automorfismo di G.

(2) Eserc. Dimostrare che tutti gli elementi di una classe di coniugio di un gruppo hanno lo stesso periodo. Più in generale mostrare che due elementi di un gruppo collegati da un automorfismo hanno lo stesso periodo.

B41 c. anelli

B41 c.01 Nella massima parte delle attività matematiche ed elaborative, a partire da quelle elementari riguardanti stringhe, numeri naturali e insiemi si possono definire procedimenti incisivi solo se si hanno a disposizione almeno due operazioni binarie ben distinte e se queste sono ben coordinate.

Per servirsi dei numeri interi risulta assai conveniente definire l'operazione di prodotto a partire dall'operazione somma.
Per operare efficacemente sugli insiemi si devono utilizzare sia l'unione e che l'intersezione.

In questa sezione esaminiamo le più essenziali tra le specie di strutture algebriche monoterreno munite di due operazioni.

B41 c.02 Si dice **semianello** una struttura algebrica della forma $\boldsymbol{R} = \langle R, \oplus, \mathbf{0}, \otimes \rangle$, dove

R è un insieme detto terreno del semianello,

$\oplus$ e $\otimes$ sono operazioni binarie,

$\mathbf{0}$ è una operazione nullaria, ossia un elemento di R

e dove valgono le seguenti proprietà:

(a) $\langle R, \oplus, \mathbf{0} \rangle$ è un monoide abeliano;

(b) $\langle R, \otimes \rangle$ costituisce un semigruppo;

(c) $\forall a, b, c \in R \ : \ (a \oplus b) \otimes c \ = \ (a \otimes c) \oplus (b \otimes c) \quad \text{e} \quad a \otimes (b \oplus c) \ = \ (a \otimes b) \oplus (a \otimes c)$.

Per ogni insieme U la struttura $\langle \mathfrak{P}(U), \cup, \emptyset, \cap \rangle$ è un semianello chiamato **semianello dei sottoinsiemi** dell'ambiente U.

Per ogni alfabeto A la struttura $\langle \mathfrak{P}(\mathsf{A}^*), \cup, \emptyset, \, , \rangle$ è un semianello chiamato **semianello dei linguaggi** sull'alfabeto A.

Un semianello si dice **semianello abeliano**, o **semianello commutativo**, sse è commutativa anche la seconda delle sue operazioni binarie.

Denotiamo, risp., con **Srng**, **SrngAb** e **SrngNab** le classi dei semianelli, dei semianelli abeliani e dei semianelli nonabeliani.

Il semianello dei linguaggi sopra un alfabeto A è nonabeliano sse l'alfabeto A contiene più di un carattere.
Nel caso sia $|\mathsf{A}| = 1$ si ha un semianello abeliano che è sostanzialmente equivalente (isomorfo) con il seguente semianello dei sottoinsiemi dell'insieme dei numeri naturali $\langle \mathfrak{P}(\mathbb{N}), \cup, \emptyset, + \rangle$.

I semianelli dei sottoinsiemi sono evidentemente abeliani.

Vedremo [B50b] che anche l'insieme delle coppie di interi munito del prodotto complesso, che denoteremo con $(\mathbb{Z} \times \mathbb{Z})_{cmpx}$, è un semianello abeliano.

B41 c.03 Vi sono semianelli nei quali si individua un elemento che costituisce l'elemento neutro bilatero (necessariamente unico) per la seconda operazione, elemento che non si trova in altri semianelli.

Questa distinzione induce a introdurre, similmente a quanto accade tra semigruppi e monoidi [a04], una specie di struttura strettamente collegata a quella dei semianelli.

Si dice **semianello unifero** una struttura algebrica (monoterreno) $\boldsymbol{R} = \langle R, \oplus, \mathbf{0}, \otimes, \mathbf{1} \rangle$ per la quale

(a) $\langle R, \oplus, \mathbf{0}, \otimes \rangle$ è un semianello;

(b) $\langle R, \otimes, \mathbf{1}\rangle$ costituisce un monoide.

Denotiamo con **Srngu** la classe dei semianelli uniferi. Servendoci dell'operatore di dimenticanza [a06] si ha che per ogni semianello unifero $\boldsymbol{S}$ la struttura $\boldsymbol{Frgt}_6(\boldsymbol{S})$ è un semianello.

Ogni semianello ottenuto da un semianello unifero va considerato un **impoverimento** di quest'ultimo; viceversa un semianello unifero va considerato un **arricchimento** del semianello che si ottiene applicandogli $\boldsymbol{Frgt}_6$.

Chiaramente si possono distinguere i semianelli uniferi abeliani dai nonabeliani secondo che i corrispondenti semianelli ottenuti per impoverimento sono abeliani dai nonabeliani.

Molti dei semianelli visti in precedenza si possono arricchire con evidenti elementi neutri.
Si individuano quindi:

il semianello unifero dei sottoinsiemi di un qualsiasi insieme U $\quad \langle \mathfrak{P}(U), \cup, \emptyset, \cap, U\rangle$, abeliano;

il semianello unifero dei linguaggi su un alfabeto A $\quad \langle \mathfrak{P}(\mathsf{A}^*), \cup, \emptyset, \cdot, \{\sqcup\}\rangle$, nonabelian sse $|\mathsf{A} > 1$;

il semianello unifero degli insiemi di interi $\quad \langle \mathfrak{P}(\mathbb{N}), \cup, \emptyset, +, \{0\}\rangle$.

Un semianello con un prodotto privo di elemento neutro è fornito dall'insieme $2 \cdot \mathbb{Z}$ dei numeri interi pari munito della somma e del prodotto usuali. Stessa considerazione vale per ogni semianello il cui terreno ha la forma $m \cdot \mathbb{Z}$ con $m = 3, 4, 5, \ \ldots$.

B41 c.04 Un importante arricchimento (e sostanzialmente una particolarizzazione) dei semianelli uniferi si ottiene chiedendo che il monoide sottostante sia abeliano.

Si dice quindi **anello unifero** una struttura $\langle R, \oplus, \ominus, \mathbf{0}, \otimes, \mathbf{1}\rangle$ per la quale valgano le seguenti proprietà:

(a) $\langle R, \oplus, \ominus, \mathbf{0}\rangle$ è un gruppo abeliano;

(b) $\langle R \setminus \{\mathbf{0}\}, \otimes, \mathbf{1}\rangle$ costituisce un monoide abeliano;

(c) $\langle R, \oplus, \mathbf{0}, \otimes, \mathbf{1}\rangle$ è un semianello unifero.

Un anello unifero si dice **anello unifero abeliano**, o anche anello unifero commutativo, sse è commutativa la seconda delle sue operazioni binarie.

Denotiamo, risp., con **RngU**, **RngUAb** e **RngUNab** le classi degli anelli uniferi, quella degli anelli uniferi abeliani e quella degli anelli uniferi nonabeliani.

Come per monoidi e semianelli uniferi si può considerare l'impoverimento degli anelli uniferi (con la individuazione di una specie di strutture più frequente) facendo cadere la richiesta di un elemento neutro per la seconda operazione e quindi senza operazione di inversione.

Diciamo quindi **anello** una struttura algebrica della forma $\langle R, \oplus, \ominus, \mathbf{0}, \otimes, \mathbf{1}\rangle$ per la quale $\langle R, \oplus, \ominus, \mathbf{0}, \otimes\rangle$ è un semianello e $\langle R, \otimes, \mathbf{1}\rangle$ è un monoide abeliano.

B41 c.05 Un esempio fondamentale di anello unifero abeliano è dato dall'insieme degli interi munito delle usuali operazioni di somma, differenza e prodotto, $\mathbb{Z}_{Rngu} := \langle \mathbb{Z}, +, -, 0, \cdot, 1\rangle$.

Altri anelli uniferi abeliani con terreni numerici sono costituiti similmente dai numeri razionali, dai numeri algebrici [B38a], dai numeri reali costruibili [B38b], dai numeri reali [B42] e dai numeri complessi [B50]:

$$\mathbb{Q}_{Rngu} := \langle \mathbb{Q}, +, -, 0, \cdot, 1\rangle \quad , \quad \mathbb{R}_{\mathsf{a}\ Rngu} := \langle \mathbb{R}_{\mathsf{A}}, +, -, 0, \cdot, 1\rangle \quad , \quad \mathbb{R}_{\mathsf{c}\ Rngu} := \langle \mathbb{R}_{\mathsf{c}}, +, -, 0, \cdot, 1\rangle \quad ,$$
$$\mathbb{R}_{Rngu} := \langle \mathbb{R}, +, -, 0, \cdot, 1\rangle \quad , \quad \mathbb{C}_{Rngu} := \langle \mathbb{C}, +, -, 0, \cdot, 1\rangle \ .$$

Altri importanti anelli abeliani sono costituiti per un qualsiasi intero $m \geq 2$ dalle classi di resti $\mathbb{Z}_m$ modulo [B26].

Osserviamo che non è stata avanzata alcuna richiesta sull'esistenza di elementi inversi per il prodotto. Per un imprecisato anello unifero si può garantire l'inverso solo per il suo elemento unità.
Nel caso di $\mathbb{Z}_{Rngu}$, tra gli elementi diversi da 1, solo -1 possiede elemento inverso.
Per tutti gli altri anelli numerici sopra citati tutti gli elementi a esclusione dello 0 posseggono inverso.

B41 c.06 Un sottoinsieme S del terreno R di un anello unifero $\boldsymbol{R} = \langle R, \oplus, \ominus, \mathbf{0}, \otimes, \mathbf{1} \rangle$ si dice terreno di sottoanello unifero di $\boldsymbol{R}$ sse è chiuso rispetto alle operazioni di somma, differenza e prodotto e contiene $\mathbf{1}$, cioè sse

$$\forall a, b \in S \quad : \quad a \oplus b \ , \ a \ominus b \ , \ a \otimes b \in S \ \text{ e } \ 1 \in S \ .$$

In questo caso si dice che $\langle S, \oplus, \ominus, \mathbf{0}, \otimes, \mathbf{1} \rangle$ è sottoanello unifero di $\boldsymbol{R}$ e si scrive

$$\langle S, +, -, 0, 1 \rangle \ \leq_{Rngu} \ \langle R, +, -, 0, 1 \rangle \ .$$

La relazione $\leq_{Rngu}$ si legge "essere sottoanello unifero". Similmente si definiscono le relazioni
essere sottoanello, denotata con $\leq_{Rng}$;
essere sottosemianello, denotata con $\leq_{Srng}$;
essere sottosemianello unifero, denotata con $\leq_{Srngu}$.

Occorre tuttavia osservare che in molti passi espositivi sopra strutture algebriche come anelli, anelli uniferi, semianelli e semianelli uniferi, in pratica, si adotta la identificazione struttura-terreno e il contesto consente di evitare ambiguità; in particolare sono considerate sufficienti scritture come $S \leq_{Rng} R$. o $\overline{S} \leq_{Rngu} \overline{R}$.

Come per le altre specie di strutture nelle situazioni nelle quali il sottoinsieme che fa da terreno a una sottostruttura è sottoinsieme proprio della struttura che viene ridotta si usano le notazioni nell quali il segno "$\leq$" viene sostituito dal segno "$<$".
Quindi si incontrano affermazioni formalizzate della forma $S <_{Rng} R$ e della forma $\overline{S} <_{Rngu} \overline{R}$.

B41 c.07 Si constata facilmente che valgono le seguenti relazioni tra strutture di largo uso:

$$\mathbb{Z}_{Rng} \ <_{Rng} \ \mathbb{Q}_{Rng} \quad \text{e} \quad \mathbb{Q}_{Rngu} \ <_{Rngu} \ \mathbb{R}_{\mathsf{A}\ Rngu} \ <_{Rngu} \ \mathbb{R}_{\mathsf{C}\ Rngu} \ <_{Rngu} \ <_{Rngu} \ \mathbb{C}_{Rngu} \ .$$

Eserc. Dimostrare che per $m, k = 2, 3, ...$ si ha $(m\,k)\,\mathbb{Z} <_{Rngu} m\mathbb{Z}$.

B41 c.08 Consideriamo un anello unifero $\boldsymbol{R} = \langle R, \oplus, \ominus, \mathbf{0}, \otimes, \mathbf{1} \rangle$ e un intero positivo d; si dice **anello delle matrici quadrate** di profilo $d \times d$ su $\boldsymbol{R}$ [G40] la struttura

$$\left\langle \mathsf{Mat}_{d;\boldsymbol{R}}, \oplus_{mat}, \ominus_{mat}, \mathsf{matZr}_{d;\boldsymbol{R}}, \otimes_{mat}, \mathsf{matId}_{d;\boldsymbol{R}} \right\rangle \ ,$$

dove con $\oplus_{mat}$ e $\ominus_{mat}$ denotiamo, risp., le estensioni alle matrici quadrate, ossia delle matrici con un profilo $d \times d$, delle operazioni $\oplus$ e $\ominus$, mentre con $\otimes_{dxd}$ denotiamo il prodotto righe per colonne tra matrici quadrate (indicazione più specifica della $\dashv$), con $\mathsf{matZr}_{d;\boldsymbol{R}}$ la matrice di profilo $d \times d$ avente tutte le componenti uguali all'elemento neutro $\mathbf{0}$ e con $\mathsf{matId}_{d;\boldsymbol{R}}$ denotiamo la matrice quadrata di profilo $d \times d$ avente le entrate sulla diagonale uguali a $\mathbf{1}$ e le altre entrate uguali a $\mathbf{0}$.

In effetti la matrice opposta di una data A, cioè la sua inversa rispetto alla somma $\oplus_{mat}$, si ottiene modificando tutte le componenti $a_{i,j}$ della A nelle opposte $\ominus a_{i,j}$, mentre l'elemento neutro rispetto alla somma è la matrice $\mathsf{matZr}_{d;\boldsymbol{R}}$ avente tutte le componenti uguali all'elemento neutro $\mathbf{0}$ di $\boldsymbol{R}$.

Le matrici quadrate sugli anelli uniferi degli interi, dei razionali, dei reali e dei complessi costituiscono strumenti computazionali ricchi di applicazioni.

B41 c.09 Gli anelli uniferi di matrici di ordine maggiore di 1 sono nonabeliani, anche se costruiti a partire da un anello abeliano. Per esempio non commutano le matrici con entrteintere:

$$\begin{bmatrix}0 & 1\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix} = \begin{bmatrix}0 & 1\\ 1 & 2\end{bmatrix} \neq \begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 1\end{bmatrix} = \begin{bmatrix}1 & 2\\ 1 & 1\end{bmatrix}$$

$$\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}\begin{bmatrix}5 & 6\\ 7 & 8\end{bmatrix} = \begin{bmatrix}19 & 43\\ 22 & 50\end{bmatrix} \neq \begin{bmatrix}5 & 6\\ 7 & 8\end{bmatrix}\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix} = \begin{bmatrix}23 & 31\\ 34 & 46\end{bmatrix}$$

B41 c.10 In un anello unifero $\boldsymbol{R} = \langle R, +, -, 0, \cdot, 1\rangle$ può accadere che presi due elementi $r, s \in R$ diversi dallo zero e dall'unità , abbiano il prodotto $r\,s$ sia uguale allo stesso elemento zero.
Questi elementi r ed s si dicono **divisori dello zero** per $\boldsymbol{R}$.

Consideriamo l'anello unifero $\langle \mathbb{Z}_6, +_6, -_6, 0, \cdot_6, 1\rangle$ [B26]; in esso $2 \cdot_6 3 = 0_6$, e quindi 2_6 e 3_6 sono divisori dello zero.

Più in generale In ogni anello unifero $\mathbb{Z}_m$ con m numero nonprimo si trovano divisori dello zero, in quanto si trovano una o più fattorizzazioni $m = r\,s$ con $r, s \neq 0, 1$ ed evidentemente $r \cdot_m s = 0_m$.

B41 c.11 Si dice **dominio di integrità** ogni anello abeliano privo di divisori dello zero.

(1) Eserc. Dimostrare che nell'anello $\mathbb{Z}_m$ l'insieme dei divisori dello zero coincide con gli interi in $\{2, ..., m-1\}$ nonprimi con m.
Concludere che ogni anello $\mathbb{Z}_p$ con p numero primo è privo di divisori dello zero.

B41 c.12 Si trovano molte coppie di matrici 2×2 sui reali che forniscono divisori dello zero per l'anello delle matrici di ordine 2; per esempio:

$$\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix} \quad \text{e} \quad \begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix} \quad ; \quad \begin{bmatrix}a & -a\\ b & -b\end{bmatrix} \quad \text{e} \quad \begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}$$

B41 d. campi

B41 d.01 Si dice **corpo** un anello unifero $\boldsymbol{R}$, in cui gli elementi diversi dallo zero formano gruppo rispetto all'operazione prodotto.
Perché questa definizione abbia senso è necessario che $\boldsymbol{R}$ possegga almeno due elementi.
Il corpo meno esteso ha come terreno $\mathbb{B} = \{0, 1\}$, come operazione di somma la somma modulo 2 che denotiamo con "$+_2$" [B26], e come prodotto il prodotto ordinario.

L'insieme degli elementi del corpo $\boldsymbol{R}$ diversi dallo zero, prende il nome di **gruppo moltiplicativo** di $\boldsymbol{R}$ e in genere si denota con $\boldsymbol{R}^\times$.
Il gruppo moltiplicativo del corpo a due elementi è il gruppo costituito dal solo elemento unità.

Un corpo in cui il prodotto è commutativo viene detto **corpo commutativo** o **campo**.
Un corpo noncommutativo viene anche chiamato **corpo sghembo** o corpo obliquo (*skewfield*).

Denotiamo con **Krp** la classe dei corpi, con **Fld** la classe dei campi e con **KrpNab** la classe dei corpi sghembi.

B41 d.02 Dunque per campo in algebra si intende una struttura della forma $\boldsymbol{F} = \langle F, +, -, 0, \cdot, ^{-1}, 1\rangle$ tale che $\langle F, +, -, 0\rangle$ e $\langle F \setminus 0, \cdot, ^{-1}, 1\rangle$ sono gruppi commutativi e l'operazione binaria "$\cdot$", chiamata prodotto, è distributiva rispetto all'operazione binaria $+$, chiamata somma.
I due gruppi citati sono detti, risp., **gruppo additivo** e **gruppo moltiplicativo** del campo $\boldsymbol{F}$.

In modo sbrigativo si dice che un campo è un anello nel quale tutti gli elementi diversi dall'elemento neutro per la somma, lo 0, possiedono un inverso moltiplicativo.

Sono noti e ampiamente utilizzati importanti campi finiti e importanti campi infiniti.

B41 d.03 Campi infiniti si ottengono munendo con le usuali operazioni di somma e prodotto l'insieme $\mathbb{Q}$ dei numeri razionali relativi, l'insieme $\mathbb{R}_\mathsf{a}$ dei numeri algebrici, l'insieme $\mathbb{R}_\mathsf{c}$ dei numeri reali costruibili, l'insieme $\mathbb{R}$ dei numeri reali [B42], l'insieme $\mathbb{C}_\mathsf{A}$ dei numeri complessi algebrici, l'insieme $\mathbb{C}_\mathsf{c}$ dei numeri complessi costruibili, l'insieme $\mathbb{C}$ dei numeri complessi [B50]. Un altro interessante campo infinito è costituito dalle funzioni razionali, cioè dalle funzioni esprimibili come quoziente di due polinomi [B33w].

B41 d.04 Rivestono grande importanza anche i **campi finiti** che, come vedremo, si possono classificare completamente con relativa facilità. Denotiamo quindi con **FldF** la loro classe.

I campi finiti che si possono individuare più semplicemente sono gli anelli della forma $\mathbb{Z}_p$ con p numero primo.

(1) Prop.: Tra gli anelli $\mathbb{Z}_m$ con $m = 2, 3, 4, ...$ quelli che costituiscono dei campi sono precisamente gli $\mathbb{Z}_p$ con p primo.

Dim.: Procediamo semplificando le notazioni per gli elementi di $\mathbb{Z}_m$ $[x]_m$ sostituendole con le corrispondenti x.
Consideriamo l'anello $\mathbb{Z}_m$ con m intero non primo, assumendo che possa fattorizzarsi come $m = h\,k$ con $h, k = 2, 3, 4, ...$ (in genere in più modi) e dimostriamo che l'elemento h non possiede inverso procedendo per assurdo.

Se h fosse invertibile ci sarebbe un $x \in \mathbb{Z}_m$ tale che $h\,x =_m 1$ e quindi tale che $h\,x - 1 = q\,m$ con $q \in \mathbb{Z}$, ovvero $h\,x - q\,m = 1$. Di conseguenza il massimo comun divisore di h e m, cioè h dovrebbe dividere 1, cioè dovrebbe essere $h = 1$, contro l'ipotesi.

Viceversa consideriamo un $h \in \mathbb{Z}_m$ coprimo con m, cioè tale che $\text{MCD}(h, m) = 1$; in tal caso esistono due interi x e y tali che $h\,x + m\,y = 1$. Questo equivale ad affermare che $h\,x =_m 1$; quindi ogni coprimo con m è invertibile ∎

B41 d.05 Una importante proprietà dei campi riguarda la nonesistenza di divisori dello 0 diversi da tale elemento.

(1) Prop.: Se a e b sono due elementi di un campo tale che $a \cdot b = 0$, allora si ha $a = 0$, oppure $b = 0$.

Dim.: Se fosse $a \neq 0$ esisterebbe a^{-1}; quindi sarebbe $a^{-1} \cdot (a \cdot b) = 0$, cioè $b = 0$. Simmetricamente si trova che se fosse $b \neq 0$ dovrebbe essere $a = 0$ ∎

I campi sono quindi particolari domini di integrità [c11].
La precedente proprietà e l'invertibilità di quasi tutti gli elementi fanno dei campi delle piattaforme computazionali di elevata efficacia.

B41 d.06 Concludiamo segnalando alcune proprietà dei corpi.

(1) Teorema Ogni corpo è privo di divisori dello zero.

(2) Teorema Ogni anello finito $\boldsymbol{R}$ privo di divisori dello zero, cioè ogni dominio di integrità finito, è un corpo.

(3) Teorema Ogni corpo finito è un campo.

B41 e. polinomi

B41 e.01 Riprendiamo da un punto di vista algebrico servendoci di varie nozioni introdotte nelle sezioni precedenti le considerazioni sui polinomi introdotti in B33 come funzioni numeriche.

In matematica si trattano molti generi di polinomi in relazione alle loro molteplici applicazioni.
I diversi generi di polinomi si possono distinguere sulla base di diversi generi di espressioni che consentono di individuarli, espressioni che corrispondono a diverse modalità utilizzate per costruirli e per effettuare loro composizioni e manipolazioni.
Si distinguono quindi diversi generi di espressioni formali, che chiameremo, prevedibilmente, **espressioni polinomiali**.

Questi generi di espressioni costituiscono linguaggi le cui stringhe sono costruite servendosi di varibili formali e di elementi di strutture algebriche che devono essere dotate di due operazioni binarie e che in generale costituiscono semianelli [c02] che chiamiamo **semianelli dei coefficienti dei polinomi**.
I vari generi di polinomi si distinguono quindi per gli insiemi delle loro variabili formali e per i semianelli dei loro coefficienti.
Tra questi semianelli si distinguono nettamente i semianelli abeliani dai semianelli noncommutativi.

B41 e.02 I vari linguaggi delle espressioni polinomiali sono definiti progressivamente con procedimenti simili cominciando dalle componenti elementari, cioè dalle variabili formali e dagli elementi del semianello dei coefficienti, proseguendo con costrutti intermedi, i monomi formali, e procedendo con manovre che forniscono espressioni sempre più articolate.

Le variabili formali sono entità elementari trattabili come i caratteri di un alfabeto e quindi adatte a fare da componenti elementari delle stringhe qualificabili come espressioni monomiali e polinomiali.

Consideriamo un intero positivo m e un insieme di m caratteri $\mathbf{X}$ che chiamiamo insieme delle variabili formali.
Se $m = 1$ scriviamo $\mathbf{X} = \{X\}$, se $m > 1$ per gli elementi di $\mathbf{X}$ ci riserviamo di servirci sia delle lettere X, Y, Z, ... che delle scritture X_1, X_2,...,X_m.
Per talune considerazioni è necessario attribuire alle m varabili un ordinamento che viene individuato organizzando una lista degli elementi di $\mathbf{X}$.

Consideriamo poi come semianello dei coefficienti $\boldsymbol{R} = \langle R, +, \mathbf{0}, \cdot \rangle$ per i cui elementi ci serviamo delle lettere a, b, c, ..., oppure delle scritture a_1, a_2, a_3, ...

B41 e.03 Diciamo **monomio formale** su $\mathbf{X}$ e $\boldsymbol{R}$ ogni stringa di coefficienti e di variabili formali; in particolare vi sono i monomi aventi la forma $a\, X_{j_1}\, X_{j_2} ... X_{j_n}$ con $a \in R$ e per ogni $i = 1, 2, ..., n$ $j_i \in \{1, 2, ..., m\}$.

Diciamo **grado di un monomio $\boldsymbol{m}$** e denotiamo con $deg(\boldsymbol{m})$ il numero delle occorrenze delle sue variabili; al precedente monomio attribuiamo quindi il grado n; ammettiamo anche i monomi di grado 0 costituiti da stringhe di soli coefficienti.

Introduciamo una prima equivalenza $\sim_{Mnm}$ tra le espressioni polinomiali considerando equivalenti due espressioni monomiali trasformabili l'una nell'altra attraverso le manovre che seguono. La prima manovra è lo scambio tra coefficienti e variabili e quindi:

$$aXYbYZXXaX \sim_{Mnm} XabYYaZXXX \sim_{Mnm} abaXYYZXXX \sim_{Mnm} XYYZXXXbaa\ .$$

Una seconda richiesta consiste nel considerare equivalenti le giustapposizioni dei coefficienti con i loro prodotti nell'ambito del semianello $\boldsymbol{R}$.
Consideriamo inoltre equivalenti secondo $\sim_{Mnm}$ due epressioni nelle quali il prodotto di più coefficienti sia sostituito dalla corispondente potenza e la giustapposizione di più repliche di una variabile sia sostituita dalla corispondente potenza.

Ammettiamo anche monomi costituiti solo da coefficienti, senza variabili ed anche il monomio ridotto solo allo zero di $\boldsymbol{R}$.
Nel caso in cui $\boldsymbol{R}$ possiede unità ammettiamo monomi privi di coefficienti e li consideriamo equivalenti-$\sim_{Mnm}$ i monomi aventi come coefficiente la detta unità.

Attribuiamo la forma canonica ai monomi con un solo coefficiente nella prima posizione e con le variabili che rispettano un ordinamento prefissato degli elementi di X, ai monomi ridotti a un elemento di $\boldsymbol{R}$ e ai monomi privi di coefficienti espliciti (nel caso di $\boldsymbol{R}$ unifero).

Le classi della equivalenza $\sim_{Mnm}$ le chiamiamo **monomi formali** e in genere adottiamo la semplificazione consistente nell'identificare un monomio formale con una sua espressione preferibilmente comoda per le esigenze espositive attuali, spesso con una sua espressione canonica.

B41 e.04 Definiamo l'operazione di prodotto tra due monomi formali scrivendo

$$a\,X_{j_1}\,X_{j_2}...X_{j_n}\ \odot b\,X_{j_{n+1}}\,X_{j_{n+2}}...X_{j_{n+q}}\ :=\ a\cdot b\,X_{j_1}\,X_{j_2}...X_{j_n}X_{j_{n+1}}\,X_{j_{n+2}}...X_{j_{n+q}}$$

Chiediamo inoltre che questa operazione binaria sia associativa; questo consente di ridurre un prodotto di più monomi ad un solo monomio.

Introduciamo insieme l'operazione binaria somma tra monomi che denotiamo con il segno $\oplus$ e le espressioni polinomiali come espressioni ottenibili a partire da monomi applicando ai monomi e alle sottoespressioni polinomiali eventualmente delimitate dalle parentesi coniugate "(" e ")" le operazioni $\oplus$ e $\odot$.

Definiamo ora la equivalenza tra polinomi $\sim_{Poln}$ come ampliamento dell'equivalenza $\sim_{Mnm}$ ottenibile dalle richieste di associatività della somma (oltre che del prodotto), di commutatività della somma, della neutralità per la somma dello zero di $\boldsymbol{R}$, della neutralità per il prodotto dell'eventuale unità di $\boldsymbol{R}$ e dalla distributività del prodotto ripetto alla somma.

Chiamiamo **polinomio formale** su A e $\boldsymbol{R}$ ogni classe di espressioni polinomiali per l'equivalenza $\sim_{Pln}$.
Ci proponiamo inoltre di adottare spesso la semplificazione consistente nell'identificare un polinomio formale con una sua espressione che tendenzialmente risultrà comoda per le esigenze espositive del momento.
Risulta in genere vantaggiosa quella che possiamo assumere come espressione canonica dei polinomi consistente nella somma di monomi in forma canonica in ordine di grado decresente e a parità di grado in ordine dei gradi decrescenti delle diverse variabili da considerare a loro volta ordinate nell'ambito di A.

B41 e.05 A questo punto i devono distinguere i polinomi di variabili commutative dai polinomi di variabili noncommutative.
Nel primo caso l'equivalenza $\sim_{Pln}$ va ampliata per tener conto della commutatività tra le variabili

Si osserva che in questo case ricadono i polinomi come funzioni di variabili appartenenti a semianelli numerici e in particolare ad anelli e a campi numerici introdotti in B33.
In questi casi sono utili le considerazioni del paragrafo che segue.

B41 e.06 Sia A un alfabeto qualsiasi e consideriamo la relazione $\sim_{Ab}$ costituita dalla coppie di stringhe ottenibili l'una dall'altra con una permutazione dei suoi componenti.

Diciamo **stringa abeliana** su A ogni classe dell'equivalenza $\sim_{Ab}$. Evidentemente la giustapposizione applicata alle stringhe abeliane è una operazione binaria commutativa.

In particolare possono interessare le stringhe abeliane dell'alfabeto **X** delle variabili formali e i cosiddetti **monomi formali abeliani**, ottenuti dai monomi formali sostituendo la stringa di variabili formali con la corrispondente stringa abeliana.
In altre parole possiamo chiamare monomio formale abeliano una classe dell'equivalenza tra monomi formali derivante dalla possibilità di commutatare due sue variabili formali.

L'insieme dei monomi formali su A e $\boldsymbol{R}$ munito della giustapposizione semplificabile applicando la commutabilità tra elementi di $\boldsymbol{R}$ e stringhe su **X** si dimostra senza difficoltà costituire un monoide.

A sua volta l'insieme dei monomi formali abeliani su A e $\boldsymbol{R}$ munito della giustapposizione semplificabile come sopra costituisce un monoide abeliano.

B41 e.07 Arricchiamo i precedenti monoidi con una operazione binaria commutativa e associativa $\oplus$ che chiamiamo somma formale, in modo di avere la possibilità di trattare espressioni come le seguenti

$$a\,X\,Y^2\,X\,Z + b\,c\,Z^3\,X\,Y^2 \qquad \text{e} \qquad (c^2 - b^2)\,X_1\,X_3\,{x_2}^2 - X_2^3\ .$$

Ampliamo ulteriormente l'insieme di queste somme consentendo di effettuare quante volte si vogliono la delimitazione tra parentesi, la somma formale e il prodotto formale, intendendo con questo termine una estensione del prodotto nei monoidi.

L'insieme delle espressioni così ottenute si dice insieme delle **espressioni polinomiali nonabeliane** su ASs e $\boldsymbol{R}$.
Sostituendo le variabili formali di A con le variabili abeliane si ottiene l'insieme delle **espressioni polinomiali** su A e $\boldsymbol{R}$.

Su questo insieme definiamo la relazione **equivalenza polinomiale** $\sim_{Pln}$ come la relazione che collega due espressioni che si possono trasformare l'una nell'altra applicando le equivalenze elementari consistenti nella eliminazione o aggiunta di coppie di parentesi coniugare e nella applicazione della proprietà associativa di addizione e prodotto, della proprietà commutativa dell'addizione, della proprietà commutativa del prodotto limitatamente al caso delle variabil formali abeliane e della proprietà distributiva di somma e prodotto.

Le attività di trasformazione delle espressioni polinomiali in altre loro collegate attraverso l'equivalenza $\sim_{Pln}$ viene spesso chiamata **calcolo letterale applicato ai polinomi**. Esempi di questa attività si incontrano nella matematica delle scuole secondarie.

Definiamo come insieme dei **polinomi nonabeliani** sull'alfabeto A e sul semianello $\boldsymbol{R}$ l'insieme delle classi dell'equivalenza $\sim_{Pln}$.

Definiamo come insieme dei **polinomi** (abeliani) sull'alfabeto A e sul semianello $\boldsymbol{R}$ l'insieme delle classi dell'equivalenza $\sim_{Pln}$. delle espressioni polinomiali su ASs e $\boldsymbol{R}$.

Si osserva che i polinomi nonabeliani in una sola variabile non hanno senso. II polinomi in una sola variabile non possono che essere abeliani; si tratta dei più semplici e fondamentali.

L'insieme dei polinomi nella variabile X sul semianello $\boldsymbol{R}$ si denota con $\boldsymbol{R}[x]$.

B41 e.08 i polinomi in una variabile formale su un semianello si possono arricchire senza difficoltà ed essere associati a un semianello abeliano unifero, a un anello abeliano, a un anello abeliano unifero o a un campo.

D'altra parte la variabile formale può essere pensata come variabile su un semianello abeliano, su un anello abeliano o su un campo.

In effetti i polinomi di utilizzo più comune sono i polinomi sui campi finiti, sui reali e sui complessi riguardanti variabili nelle stesse strutture.

Polinomi che si incontrano più raramente sono, per esempio, i polinomi sull'anello dei sottoinsiemi con $\oplus = \cup$ e $\otimes = \cap$, i polinomi di matrici quadrate di un dato profilo e i polinomi sull'anello di due elementi $\{0, 1\}$.
Tra i polinomi noncommutativi accenniamo solo a quelli le cui variabili sono i caratteri di un alfabeto.

B41 e.09 Ogni espressione polinomiale in una sola variabile X sul semianello $\boldsymbol{R}$ può essere messa nella cosiddetta forma canonica

$$a_0 + a_1\,X + a_2\,X^2 + \cdots + c_m\,X^m \;=\; \sum_{i=1}^{m} a_i\,X^i \quad \text{con} \quad a_1, a_1, a_2, ..., a_m \in R\ .$$

Infatti da ogni espressione polinomiale possono essere eliminate le parentesi coniugate in forza della distributività del prodotto rispetto alla somma e la espressione così ottenuta può avere gli addendi ordinati per potenze della X crescenti grazie alla commutatività della somma dei monomi.
Tra gli addendi $a_i\,X^i$ della forma canonica il coefficiente a_0 viene detto addendo costante, $a_1\,X$ addendo lineare, $a_2\,X^2$ addendo quadratico, $a_3\,X^3$ addendo cubico, $a_4\,X^4$ addendo quartico e così via.

In genere in questa scrittura gli addendi con il relativo coefficiente nullo vengono tralasciati.

Testo fruibile in https://www.mi.imati.cnr.it/alberto/ e https://arm.mi.imati.cnr.it/Matexp/matexp_main.php