1

Capitolo T15
strutture algebriche sopra un terreno

Contenuti delle sezioni

a. magmi e loro elementi caratteristici p. 3
b. semigruppi e monoidi p. 10
c. quasigruppi e loops p. 13
d. gruppi p. 16
e. specie di strutture algebriche p. 18
f. prodotti di strutture p. 21
g. morfismi di strutture p. 24
h. semianelli e matrici p. 25
i. anelli e strutture collegate p. 29
j. ideali p. 33
k. campi p. 36
l. campi finiti p. 37
m. semireticoli e reticoli p. 41

47 pagine

T15 0.01 Questo è il primo di due capitoli dedicati a una rassegna che vuole essere autonoma, sistematica e ampia delle specie di strutture algebriche di maggiore importanza e che più sono richiamate dalle varie parti di questa *esposizione*.

In questi capitoli viene presentata una rilevante varietà di entità matematiche per le quali è cruciale porre in evidenza le caratteristiche comuni e le nozioni unificanti.

Nelle prossime pagine sono trattate le strutture algebriche monoterreno e tutte sono definite presentando un insieme, una sequenza di operazioni (tra le quali si distinguono le binarie, le unarie e le nullarie) e un sistema di assiomi prevalentemente espressi mediante equazioni.

Questo genere di formalizzazione, in certi punti troppo schematico, in genere favorisce la definitezza e facilita la distinzione tra le molte strutture specifiche e i molteplici raggruppamenti di strutture determinati da requisiti formali comuni che consentono di individuare proprietà condivise da strutture costruite su terreni anche notevolmente diversi.

Per ciascuna delle specie di strutture sono definiti identificatori che consentono, tra l'altro, di caratterizzare i morfismi tra strutture specifiche (cioè le trasformazioni tra strutture della stessa specie che rispettano le loro operazioni), le relazioni tra strutture e sottostrutture e varie loro composizioni, in particolare i prodotti diretti.

T15 0.02 Cercando di procedere sistematicamente nel modo accennato si ottengono vari vantaggi.

Sono facilitate le presentazioni dei collegamenti tra raggruppamenti di strutture con assiomi più o meno stringenti e tra specie di strutture più o meno ricche di operazioni.
Accade anche che la nitidezza di questi collegamenti facilita il riutilizzo di costruzioni e di proprietà quando ci si muove tra strutture con più caratteristiche in comune.
Nell'ambito delle considerazioni sopra una specie viene facilitata la individuazione delle caratteristiche delle componenti della specie stessa.
Nell'ambito della classificazione delle strutture di una data specie agevola la individuazione di collezioni più o meno estese e dei relativi esempi e controesempi.

Per perseguire la sistematicità si devono introdurre un numero rilevante di termini, di sigle e di simboli che possono rendere faticosa la comprensione; questo problema può essere affrontato solo con la disponibilità degli indici dei simboli e dei termini, elenchi che richiedono di essere mantenuti completi e di essere aggiornati dopo ogni modifica dei contenuti.

L'elevato numero delle notazioni specifiche porta anche l'esigenza di introdurre notazioni e dizioni semplificate in grado di alleggerire i discorsi circoscritti. Queste notazioni e dizioni devono essere riconducibili alle più complete in seguito a dichiarazioni esplicite e devono essere collocate in contesti ben delimitati che consentono di evitare le ambiguità.

T15 a. magmi e loro elementi caratteristici

T15 a.01 Consideriamo un insieme M nonvuoto; si dice **legge di composizione [interna]** su M ogni funzione del genere $\lceil M \times M \longmapsto M \rceil$.

Si dice **magma** ogni coppia $\boldsymbol{M} = \langle M, C \rangle$ con C legge di composizione interna su M; di tale magma M si chiama il **terreno del magma**; si dice anche che il magma $\boldsymbol{M}$ si ottiene munendo l'insieme M di una sua legge di composizione C.

Il termine magma è stato introdotto nel trattato *Éléments de Mathématiques* del matematico policefalo Nicolas Bourbaki.
Taluni come sinonimo di magma usano anche il termine *gruppoide*; sembra però opportuno riservare questo termine a strutture algebriche come il `gruppoide di Brandt (wi)` introdotta da Heinrich Brandt.

Un magma $\boldsymbol{M}$ si dice, risp., finito, infinito, numerabile, contabile, più che numerabile, continuo, ... sse il suo terreno è, risp., un insieme finito, infinito, numerabile, contabile, più che numerabile, continuo ... .

Si dice **ordine di un magma** o **cardinale di un magma** $\boldsymbol{M} = \langle M, \cdot \rangle$ il cardinale del suo terreno $|M|$.

T15 a.02 Un esempio di magma di ordine 4 è $\big\langle \{1,2,3,4\}, \min \big\rangle$, dove con min denotiamo la funzione che a due interi compresi tra 1 e 4 fa corrispondere il minore dei due.
Due esempi di magmi infiniti numerabili sono $\langle \mathbb{N}, g \rangle$, dove g denota la funzione che a due interi naturali i e j associa $i + 2\,j$ e $\langle \mathbb{Z}, - \rangle$, dove "$-$" denota la differenza di interi.

Magmi infiniti più che numerabile sono dati dall'insieme dei numeri reali e da funzioni che ad ogni coppia di reali associano un reale (somma, differenza, prodotto, espressione polinomiale in due variabili, ...). La divisione tra reali non fornisce un magma ma, come ogni funzione definita su un sottoinsieme proprio del quadrato cartesiano del terreno definisce un cosiddetto **magma parziale**.

T15 a.03 Ora prestiamo particolare attenzione ai **magmi discreti**, magmi con un terreno (finito o) costruibile e con una cosiddetta **legge di composizione interna calcolabile** che denotiamo con C, ossia una legge di composizioe per la quale si conosce qualche algoritmo che, a partire da due elementi qualsiasi a e b di M, consenta di individuare effettivamente $C(a,b)$, cioè attraverso un procedimento che per ogni coppia di reali $\langle a, b \rangle$ fornisce un valore in un numero finito di passi.

Spesso per tali magmi la legge di composizione si individua con una matrice (finita) o con una matrice.ZZ nelle quali ogni riga e ogni colonna è caratterizzata da un elemento di M; questi a loro volta si possono sequenzializzare, ossia porre in corrispondenza con gli interi costituenti un intervallo o un insieme come $\mathbb{N} \times \mathbb{N}$ o $\mathbb{Z} \times \mathbb{Z}$.

Per i magmi finiti in genere si utilizza un intervallo della forma **[**n **)** o della forma **(**n **]** per n intero positivo.
Se r e c rappresentano due elementi di un tale intervallo la componente della matrice relativa alla riga r e alla colonna c fornisce $C(r,c)$.

Le matrici dei primi due magmi in a02 sono

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

	0	1	2	3	...
0	0	2	4	6	...
1	1	3	5	7	...
2	2	4	6	8	...
3	3	5	7	9	...
⋮	⋮	⋮	⋮	⋮	⋱

Queste matrici sono dette **tavole di Cayley** dei rispettivi magmi.

T15 a.04 Spesso per le espressioni riguardanti la legge di composizione si usa la notazione infissa, secondo la quale in luogo di $C(a,b)$ o dell'equivalente $\langle a,b\rangle$‚C si scrive a‚C‚b o ancor più semplicemente $a\,C\,b$.
La legge di composizione C di un magma viene chiamata **operazione binaria** del magma; in una scrittura come $a\,C\,b$ si dice che a e b costituiscono, risp., il **primo operando** e il **secondo operando** dell'operazione C, oppure l'operando sinistro e l'operando destro di C.
Quando si utilizzano notazioni infisse per gli operatori in genere si preferiscono simboli nonletterali come "$+$" , "$\cdot$", "$\perp$", "$\oplus$" o "$\odot$". Un tipico esempio di magma più che numerabile è $\langle\mathbb{R},\cdot\rangle$.

In molti discorsi sufficientemente circoscritti risulta piuttosto pedante denotare un magma $\boldsymbol{M}$ con una scrittura come $\langle M,\odot\rangle$; spesso risulta pesante anche la stessa distinzione tra $\boldsymbol{M}$ ed M. Quindi frequentemente si riesce a rendere l'esposizion più scorrevole adottando la semplificazione che identifica il magma con il suo terreno. Questa semplificazione è lecita quando ci si trova in un contesto che rende possibile stabilire se, per esempio, un simbolo M identifica un terreno o un più articolato magma.

Questa semplificazione si adotta convenientemente per molte strutture monoterreno che vedremo qui di seguito come monoidi, gruppi, anelli e reticoli. Essa in effetti si usa anche per strutture algebriche multiterreno come spazi vettoriali e algebre su campo [T16] e anche per strutture nonalgebriche come spazi metrici [B46] e spazi topologici [T30]. Essa può chiamarsi **semplificazione strGrnd**.
In particolare l'ordine di un magma $\boldsymbol{M}=\langle M,\odot\rangle$ si può anche denotare con $|\boldsymbol{M}|$ o con $|M|$.

T15 a.05 La classe dei magmi si denota con **Mgm**; più specificamente denotiamo con $\mathbf{Mgm}_M$ l'insieme dei magmi che hanno l'insieme M come terreno, con **MgmF** l'insieme dei magmi sopra un terreno finito, con **MgmI** l'insieme dei magmi sopra un terreno infinito, con $\mathbf{Mgm}_n$ con n intero positivo l'insieme dei magmi su un terreno di n elementi, con $\mathbf{Mgm}_{\aleph_k}$ l'insieme dei magmi su un terreno di cardinale $\aleph_k$.

La classe dei magmi costituisce un primo esempio di **specie di struttura algebrica**. Questo termine sarà ampiamente chiarito ed esemplificato in :e.

Per le varie altre specie di strutture algebriche e di strutture di natura diversa useremo notazioni simili alle precedenti. Per una specie di strutture con un solo terreno per le quali adottiamo una notazione della forma **Xyz**, scriveremo:
Xyz_S per l'insieme delle strutture aventi come terreno l'insieme S, **XyzF** per l'insieme delle strutture finite, mentre per ogni $n\in\mathbb{P}$ scriveremo $\mathbf{Xyz}_n$ per l'insieme delle strutture di ordine n, cioè aventi un terreno di cardinale n.

Talvolta risultano più opportune scritture della forma $\mathbf{Xyz}[S]$ o $\mathbf{Xyz}[n]$, specialmente quando i segni S e n riguardano espressioni elaborate.
Si presenterà anche l'opportunità di individuare insiemi di strutture caratterizzati da più di una specificazione: in questi casi dovranno essere specificate notazioni delle forme $\mathbf{XyzF}\mathsf{AbC}_(S)$, $\mathbf{Xyz}_{\alpha,n}[\mathcal{K}]$ e $\mathbf{Xyz}_{\alpha;\beta}[\mathcal{G},m]$.

T15 a.06 La specie dei magmi è una collezione di strutture piuttosto vaga, in quanto all'operazione binaria si chiede solo di essere definita per ogni coppia di elementi: quindi si possono individuare numerosi magmi, ma per gran parte di essi non si trovano utili applicazioni, in quanto si possono controllare solo con meccanismi ad hoc e non mediante procedimenti efficienti e di portata sufficientemente ampia, come accade per tipi di strutture introdotte a partire da loro riconosciute applicazioni come per le strutture basate su classici insiemi numerici o su insiemi di trasformazioni di spazi che mantengono rigide ddotate di opportune proprietà.

I magmi finiti aventi come terreno un $A_n = \{a_1, ..., a_n\}$ sono equivalenti alle matrici $n \times n$ ottenibili collocando ad arbitrio in ciascuna delle loro n^2 caselle un elemento di A_n: vi sono quindi n^{n^2} magmi su A_n: per $n = 10$ si hanno ben 10^{100} magmi, un `Googol (wi)` di magmi.
Non è difficile precisare un meccanismo che in linea di principio consenta di generarli tutti: l'elenco così ottenuto, però, risulterebbe lunghissimo e ben poco significativo. Secondo certi modelli cosmologici il numero delle molecole dell'intero universo si aggira intorno a 10^{83}.
È comprensibile che quelli che vedono la matematica come la disciplina che fornisce regole e procedure per calcoli effettivi siano indotti a giudicare un perdigiorno chi si soffermasse più di tanto su un elenco come il precedente che dovrebbe contenere più matrici di quante sono le molecole dell'universo.

T15 a.07 Mettiamoci nella prospettiva opposta: per $n = 2$ si hanno 16 magmi che possono essere facilmente individuati, assumendo per esempio $M = \mathbb{B} = \{0, 1\}$.

$$\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} \qquad \begin{matrix} 0 & 0 \\ 0 & 1 \end{matrix} \qquad \begin{matrix} 0 & 0 \\ 1 & 0 \end{matrix} \qquad \begin{matrix} 0 & 0 \\ 1 & 1 \end{matrix}$$

$$\begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix} \qquad \begin{matrix} 0 & 1 \\ 0 & 1 \end{matrix} \qquad \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \qquad \begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix}$$

$$\begin{matrix} 1 & 0 \\ 0 & 0 \end{matrix} \qquad \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} \qquad \begin{matrix} 1 & 0 \\ 1 & 0 \end{matrix} \qquad \begin{matrix} 1 & 0 \\ 1 & 1 \end{matrix}$$

$$\begin{matrix} 1 & 1 \\ 0 & 0 \end{matrix} \qquad \begin{matrix} 1 & 1 \\ 0 & 1 \end{matrix} \qquad \begin{matrix} 1 & 1 \\ 1 & 0 \end{matrix} \qquad \begin{matrix} 1 & 1 \\ 1 & 1 \end{matrix}$$

Interpretando 0 ed 1 come valori di verità si ottengono interpretazioni abbastanza significative per tutti i magmi su $\mathbb{B}$. In particolare

$$\cdot_2 = \wedge = \begin{matrix} 0 & 0 \\ 0 & 1 \end{matrix} \qquad \vee = \begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix} \qquad +_2 = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \qquad \Longrightarrow = \begin{matrix} 1 & 1 \\ 0 & 1 \end{matrix} \qquad \Longleftrightarrow = \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} .$$

(1) Eserc. Cercare interpretazioni nel calcolo proposizionale, nella teoria degli insiemi e nella teoria dei circuiti digitali per tutte le precedenti matrici di Cayley, prima di consultare B60.

T15 a.08 Nello studio di un magma $\boldsymbol{M} = \langle M, \odot \rangle$ in genere risulta molto utile individuare elementi del terreno con proprietà algebriche particolari.

Si dice **elemento neutro a sinistra**, o anche **unità a sinistra**, ogni $u_l \in M$ tale che $\forall a \in M : u_l \odot a = a$.

Si dice **elemento neutro a destra**, o anche **unità a destra**, ogni $u_r \in M$ tale che $\forall a \in M : a \odot u_r = a$.

Si dice **elemento neutro bilatero**, o più in breve **elemento neutro**, o anche unità bilatera o più in breve **unità**, ogni $u \in M$ tale che $\forall a \in M : u \odot a = a \odot u = a$. Molto spesso l'unità bilatera è denotata dal segno "1".

Si dice **elemento assorbente a sinistra**, o anche **zero a sinistra**, ogni $z_l \in M$ tale che $\forall a \in M : z_l \odot a = z_l$.

Si dice **elemento assorbente a destra**, o anche **zero a destra**, ogni $z_r \in M$ tale che $\forall a \in M : a \odot z_r = z_r$.

Si dice **elemento assorbente bilatero**, o semplicemente **elemento assorbente**, o zero bilatero, o concisamente **zero**, ogni $z \in M$ tale che $\forall a \in M : z \odot a = a \odot z = z$. Il segno più usato per l'elemento assorbente bilatero è tuttavia "0".

Si dice **elemento idempotente** ogni $j \in M$ tale che $j \odot j = j$.

In un magma dotato di un elemento zero bilatero 0 si dice **elemento nilpotente** ogni $\nu \in M \setminus \{0\}$ tale che per un opportuno $k \in \mathbb{P}$ risulta $\nu^k = 0$.

T15 a.09 Le matrici di Cayley dei precedenti elementi hanno caratterizzazioni piuttosto evidenti. Vediamo il caso dei magmi finiti aventi come terreno un insieme dato dalla sequenza della forma $\langle x, a, b, c, d\rangle$. Assumendo per x, risp., i precedenti elementi u_l, u_r, u, z_l, z_r, z, j abbiamo i seguenti schemi di matrice di Cayley nei quali x occupa la casella $\langle 1, 1\rangle$:

$$\begin{array}{ccccc} u_l & a & b & c & d \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \end{array} \qquad \begin{array}{ccccc} u_r & . & . & . & . \\ a & . & . & . & . \\ b & . & . & . & . \\ c & . & . & . & . \\ d & . & . & . & . \end{array} \qquad \begin{array}{ccccc} u & a & b & c & d \\ a & . & . & . & . \\ b & . & . & . & . \\ c & . & . & . & . \\ d & . & . & . & . \end{array}$$

$$\begin{array}{ccccc} z_l & z_l & z_l & z_l & z_l \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \end{array} \qquad \begin{array}{ccccc} z_r & . & . & . & . \\ z_r & . & . & . & . \\ z_r & . & . & . & . \\ z_r & . & . & . & . \\ z_r & . & . & . & . \end{array} \qquad \begin{array}{ccccc} z & z & z & z & z \\ z & . & . & . & . \\ z & . & . & . & . \\ z & . & . & . & . \\ z & . & . & . & . \end{array} \qquad \begin{array}{ccccc} j & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \end{array}$$

Dalla semplice osservazione dei precedenti schemi di matrici di Cayley risulta evidente che i vari tipi di elementi neutri e di elementi assorbenti sono casi particolari di elementi idempotenti.

T15 a.10 Prop. Esistono magmi con più elementi neutri a sinistra, magmi con più elementi neutri a destra, magmi con più elementi assorbenti a sinistra, e magmi con più elementi assorbenti a destra. Lo mostrano, risp., le matrici di Cayley con forme come le seguenti:

$$\begin{array}{ccccc} u_l & u'_l & u''_l & c & d \\ u_l & u'_l & u''_l & c & d \\ u_l & u'_l & u''_l & c & d \\ . & . & . & . & . \\ . & . & . & . & . \end{array} \qquad \begin{array}{ccccc} u_r & . & u_r & . & . \\ a & . & a & . & . \\ u'_r & . & u'_r & . & . \\ c & . & c & . & . \\ d & . & d & . & . \end{array} \qquad \begin{array}{ccccc} z_l & z_l & z_l & z_l & z_l \\ . & . & . & . & . \\ . & . & . & . & . \\ z'_l & z'_l & z'_l & z'_l & z'_l \\ . & . & . & . & . \end{array} \qquad \begin{array}{ccccc} z_r & z'_r & . & z''_r & . \\ z_r & z'_r & . & z''_r & . \\ z_r & z'_r & . & z''_r & . \\ z_r & z'_r & . & z''_r & . \\ z_r & z'_r & . & z''_r & . \end{array}$$

Inoltre esistono magmi con elementi neutri a sinistra ed elementi assorbenti a sinistra, esistono magmi con elementi neutri a destra ed elementi assorbenti a destra ed esistono magmi con un elemento assorbente bilatero e magmi con un elemento neutro bilatero: essi sono magmi caratterizzati da matrici di Cayley, risp., delle forme seguenti:

$$\begin{array}{ccccc} z_l & z_l & z_l & z_l & z_l \\ z'_l & z'_l & z'_l & z'_l & z'_l \\ z_l & z'_l & u_l & u'_l & d \\ z_l & z'_l & u_l & u'_l & d \\ . & . & . & . & . \end{array} \qquad \begin{array}{ccccc} z_r & z'_r & z_r & z_r & . \\ z_r & z'_r & z'_r & z'_r & . \\ z_r & z'_r & u_r & u_r & . \\ z_r & z'_r & u'_r & u'_r & . \\ z_r & z'_r & d & d & . \end{array} \qquad \begin{array}{ccccc} z & z & z & z & z \\ z & u & b & c & d \\ z & b & . & . & . \\ z & c & . & . & . \\ z & d & . & . & . \end{array}$$

In un magma possono coesistere anche elementi neutri a sinistra con elementi assorbenti a destra e elementi neutri a destra con elementi assorbenti a sinistra, come mostrano, risp., le matrici di Cayley con forme come le seguenti:

$$\begin{array}{ccccc} z_r & {z'}_r & . & . & . \\ z_r & {z'}_r & . & . & . \\ z_r & {z'}_r & u_l & {u'}_l & d \\ z_r & {z'}_r & u_l & {u'}_l & d \\ z_r & {z'}_r & . & . & . \end{array} \qquad \begin{array}{ccccc} z_l & z_l & z_l & z_l & z_l \\ {z'}_l & {z'}_l & {z'}_l & {z'}_l & {z'}_l \\ . & . & u_r & u_r & . \\ . & . & {u'}_r & {u'}_r & . \\ . & . & d & d & . \end{array}$$

T15 a.11 **(1) Prop.**: In un magma non possono coesistere un elemento neutro a sinistra e un elemento neutro a destra diversi tra di loro; di conseguenza non possono coesistere due diversi elementi neutri bilateri: in altre parole, se è presente un elemento neutro (a sinistra, a destra o bilatero) esso è unico, non ve ne sono altri.

Dim.: Se M contenesse un u_l e un u_r tale che $\forall a \in M \ : \ u_l \odot a = a \odot u_r = a$, l'elemento $u_l \odot u_r$ dovrebbe coincidere sia con u_l che con u_r ∎

(2) Prop.: In un magma non possono coesistere, diversi, un elemento assorbente a sinistra e un elemento assorbente a destra; di conseguenza non possono coesistere due elementi assorbenti bilateri: in altre parole, può essere presente un solo elemento assorbente.

Dim.: Se M contenesse un z_l e un z_r tale che $\forall a \in M \ : \ z_l \odot a = z_l$ e $a \odot z_r \odot z_r$, l'elemento $z_l \odot z_r$ dovrebbe coincidere sia con z_l che con z_r ∎

T15 a.12 Un magma dotato di unità lo chiamiamo **magma unifero**. Talora si usano invece come termini equivalenti "magma unitale" e "magma unitario", termini che qui sconsigliamo in quanto gli aggettivi unitale e unitario vengono usati per altre qualificazioni ben diverse: si parla di razionali unitali in B30 e di operatori unitari in T34.

Vediamo alcuni esempi di magmi uniferi.

0 è elemento neutro di $\langle \mathbb{B}, +_2 \rangle$ ed 1 è elemento neutro di $\langle \mathbb{B}, \cdot \rangle$.

0 è elemento neutro di $\langle \mathbb{N}, + \rangle$, $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}_\mathsf{a}, + \rangle$, $\langle \mathbb{R}_\mathsf{c}, + \rangle$, $\langle \mathbb{R}, + \rangle$ e $\langle \mathbb{C}, + \rangle$.

1 è elemento neutro di $\langle \mathbb{P}, \cdot \rangle$, $\langle \mathbb{N}, \cdot \rangle$, $\langle \mathbb{Z}, \cdot \rangle$, $\langle \mathbb{Q}, \cdot \rangle$, $\langle \mathbb{R}_\mathsf{a}, \cdot \rangle$, $\langle \mathbb{R}_\mathsf{c}, \cdot \rangle$, $\langle \mathbb{R}, \cdot \rangle$, $\langle \mathbb{Q}_+, \cdot \rangle$, $\langle \mathbb{R}_+, \cdot \rangle$ e $\langle \mathbb{C}, \cdot \rangle$.

Non posseggono invece elemento neutro i magmi (semigruppi) $\langle \mathbb{P}, + \rangle$ e $\langle k\mathbb{Z}, \cdot \rangle$ per $k = 2, 3, 4, \ldots$.

T15 a.13 In generale si può ampliare un qualsiasi magma $\langle M, \odot \rangle$ con un oggetto non appartenente ad M in modo da farlo diventare magma unifero. Questo oggetto potrebbe anche essere solo una **entità formale introdotta ad hoc**, ossia una entità caratterizzata solo dal segno che la identifica e dalle proprietà postulate all'atto della sua definizione.

Se si denota con ν l'entità da aggiungere ad M per ottenere un magma unifero, basta estendere $\odot$ ponendo

$$\nu \odot \nu := \nu \quad \text{e} \quad \forall a \in M \ : \ \nu \odot a := a \odot \nu := a \ .$$

In termini di tavola di Cayley si tratta semplicemente di aggiungerle una nuova riga e una nuova colonna associate a ν e di porre a nelle posizioni $\langle \nu, a \rangle$ ed $\langle a, \nu \rangle$ e ν nella posizione $\langle \nu, \nu \rangle$.

L'ampliamento di un magma con un nuovo elemento neutro si può ripetere quante volte si vuole. Per esempio il magma di cui si è presentata la prima delle tavole di Cayley in a03 si può pensare ottenuto dal monoide costituito dal solo elemento 4 mediante le successive aggiunte degli elementi 3, 2 ed 1 ai quali di volta in volta viene assegnato il ruolo di elemento neutro.

Procedendo nella direzione opposta, da un qualsiasi magma unifero, attraverso l'eliminazione del suo elemento neutro si ricava un altro magma; inoltre per taluni magmi questa eliminazione può essere reiterata.

Si verifica facilmente che queste estensioni e riduzioni mantengono caratteristiche dell'operazione $\odot$ di essere commutative [a16] o associative b01], caratteristiche espresse dalle cosiddette **identità di algebra universale**, identità nelle quali compaiono solo variabili che possono variare nell'intero terreno e che quindi mantengono la loro validità con le riduzioni del terreno.

T15 a.14 Si dice **magma trasposto** o magma duale del magma $\boldsymbol{M} = \langle M, \odot \rangle$ il magma $\boldsymbol{M}^{\mathsf{T}} := \langle M, \odot^{\mathsf{T}} \rangle$, dove $\odot^{\mathsf{T}} := \left\lceil\!\left\lceil \langle a, b \rangle \mapsto b \odot a \right\rceil\!\right\rceil$, cioè il magma con l'operazione binaria trasposta di quella del magma di partenza.

In altre parole il magma trasposto di un dato magma è il magma avente come tavola di Cayley la matrice trasposta di quella del magma di partenza.

Evidentemente la trasposizione tra magmi è una involuzione entro la classe dei magmi; di questa endofunzione entro **Mgm** sono punti fissi i magmi abeliani.

La trasposizione scambia il ruolo di elemento neutro a sinistra con quello di elemento neutro a destra, il ruolo di elemento assorbente a sinistra con quello di elemento assorbente a destra, la funzione traslazione a sinistra con la funzione traslazione a destra. Lascia invece invariati i ruoli di elemento neutro bilatero e di elemento assorbente bilatero.

T15 a.15 Si ottengono collezioni di magmi maneggevoli e utili che la loro operazione binaria goda di proprietà specifiche.
Dunque presentiamo alcune delle proprietà che si possono proficuamente richiedere a un'operazione binaria $\odot \in \left\lceil\!\left\lceil M \times M \longmapsto M \right\rceil\!\right\rceil$.

L'operazione $\odot$ si dice **operazione commutativa**, o, equivalentemente, **operazione abeliana** , sse $\forall a, b \in M \;:\; a \odot b = b \odot a$; in questo caso $\langle M, \odot \rangle$ viene detto **magma commutativo** o, equivalentemente, **magma abeliano**.
Sono abeliani il primo magma presentato in a02, $\langle \mathbb{R}, \cdot \rangle$ e $\langle \mathbb{R}, + \rangle$; non è invece abeliano $\langle \mathbb{N}, g \rangle$ con $g := \left\lceil\!\left\lceil \langle i, j \rangle \in \mathbb{N} \times \mathbb{N} \mapsto i + 2\,j \right\rceil\!\right\rceil$, dato che $i \neq j \Longrightarrow g(i,j) = i + 2\,j \neq g(j,i) = 2\,i + j$.

Chiaramente un magma è abeliano sse la sua tavola di Cayley è una matrice simmetrica. Di conseguenza i magmi abeliani aventi un terreno di n elementi $\{a_1, ..., a_n\}$, a meno di isomorfismi, sono $n^{n(n+1)/2}$.
Denotiamo con **MgmAb** la classe dei magmi abeliani.

Non sono abeliani magmi numerici come $\langle \mathbb{Z}, - \rangle$, $\langle \mathbb{Q}, - \rangle$, $\langle \mathbb{R}, - \rangle$ e $\langle \mathbb{C}, - \rangle$; non sono abeliani neppure $\langle \mathbb{Q}_+, / \rangle$, $\langle \mathbb{R}_+, / \rangle$ e $\langle \mathbb{C}_{nz}, / \rangle$.

T15 a.16 Un'operazione binaria $\odot$ su M si dice **operazione associativa** sse $\forall a, b, c \in M \;:\; a \odot (b \odot c) = (a \odot b) \odot c$. Come vedremo in b01, in questo caso $\langle M, \odot \rangle$ si dice semigruppo. Quando è manifesto che un'operazione binaria $\odot$ è associativa, nelle espressioni come le due precedenti che individuano in due modi un elemento di M mediante ripetute applicazioni dell'operazione le parentesi non sono indispensabili: possiamo quindi scrivere

$$a \odot b \odot c \;:=\; a \odot (b \odot c) = (a \odot b) \odot c \;.$$

T15 a.17 L'endofunzione cha a ogni elemento x di un magma $\langle M, \odot \rangle$ associa $a \odot x$ si dice **traslazione a sinistra** di a e si denota con a^{trslLt}. L'endofunzione cha a ogni x di tale magma associa $x \odot a$ si dice

traslazione a destra di a e si denota con a^{trslRt}. Quindi

$$a^{trslLt} := \ulcorner\, x \in M \mapsto a \odot x \,\urcorner \qquad\qquad a^{trslRt} := \ulcorner\, x \in M \mapsto x \odot a \,\urcorner \ .$$

La prima endofunzione equivale alla riga della tavola di Cayley associata all'elemento a; la seconda alla colonna della tavola di Cayley associata ad a.

T15 a.18 ( ) Eserc. Spiegare le seguenti affermazioni concernenti un magma $\langle M, \odot \rangle$
(i) La traslazione a sinistra associata a un elemento neutro a sinistra è Id_M.
(ii) La traslazione a destra associata a un elemento neutro a destra è Id_M.
(iii) La traslazione a sinistra associata a un elemento assorbente a sinistra z_l è $\ulcorner\, a \in M \mapsto z_l \,\urcorner = {z_l}^{cnst}$.
(iv) La traslazione a destra associata a un elemento assorbente a destra z_r è $\ulcorner\, a \in M \mapsto z_r \,\urcorner = {z_r}^{cnst}$.
(v) Ogni traslazione associata a elementi idempotenti possiede almeno un punto fisso.

T15 a.19 Consideriamo un magma $\boldsymbol{M} = \langle M, * \rangle$. Esso si dice **magma alternativo a sinistra** sse

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

Dualmente-LR si dice **magma alternativo a destra** sse

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

Si dice invece **magma alternativo [bilatero]** sse è alternativo a sinistra e a destra.
Chiaramente la classe dei magmi alternativi è un'estensione dei magmi associativi (cioè dei semigruppi).
La proprietà di un magma di essere alternativo si dice alternatività.

Un magma $\boldsymbol{M}$ si dice **magma associativo sulle potenze** sse ciascuno dei suoi elementi genera un sotto-magma associativo. In altre parole ciascuno degli $a \in M$ quando viene moltiplicato per se stesso un dato numero k di volte fornisce lo stesso elemento, indipendentemente dai modi di organizzare le composizioni, ossia indipendentemente dai modi di disporre le coppie di parentesi coniugate nelle corrispondenti espressioni. Per esempio, per $k = 3$, se scriviamo il prodotto mediante la semplice giustapposizione, deve essere

$$a(a(aa)) = a((aa)a) = (aa)(aa) = (a(aa))a = ((aa)a)a \ .$$

Evidentemente la richiesta di associatività sulle potenze è molto meno forte della associatività che chiede $\forall a, b, c \in M : \ (ab)c = a(bc)$, e molto meno forte della idempotenza che esige $\forall a \in m : \ xx = x$.

T15 b. semigruppi e monoidi

T15 b.01 Si dice **semigruppo** un magma $\langle M, \cdot \rangle$ munito di una operazione binaria associativa, cioè tale che

$$\forall a, b, c \in M \ : \ a \odot (b \odot c) = (a \odot b) \odot c \ .$$

Denotiamo con **Sgrp** la classe dei semigruppi e, in coerenza con a05, con $\mathbf{Sgrp}_M$ l'insieme dei semigruppi aventi come terreno M, con **SgrpF** l'insieme dei semigruppi finiti, con $\mathbf{Sgrp}_n$ l'insieme dei semigruppi di ordine n e con $\mathbf{Sgrp}_{\aleph_k}$ l'insieme dei semigruppi con terreno di cardinale $\aleph_k$ per ogni $k \in \mathbb{N}$.

Dalla tavola di Cayley di un magma in genere non è agevole riconoscere il carattere associativo della operazione binaria, cioè stabilire se si tratta di un semigruppo.

Si individuano però facilmente molti importanti esempi di semigruppi. Sono associative la giustapposizione di stringhe, il prodotto di numeri interi, razionali, algebrici, costruibili, reali e complessi, il prodotto delle classi di resti, le composizioni di relazioni (e di funzioni) e il prodotto di quaternioni [G54]. Questa varietà di esempi induce a pensare che l'associatività sia una proprietà importante e che convenga esaminarla con cura.

T15 b.02 Un semigruppo si dice **semigruppo abeliano** sse è abeliano come magma, cioè sse la sua operazione binaria è commutativa. Denotiamo con **SgrpAb** la classe dei semigruppi abeliani.
In particolare sono semigruppi abeliani $\langle \mathbb{P}, + \rangle$ e $\langle \mathbb{P}, \cdot \rangle$. Altri semigruppi abeliani si ottengono munendo insiemi numerici come $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}_{\mathsf{a}}$, $\mathbb{R}_{\mathsf{c}}$, $\mathbb{R}$, $\mathbb{C}$ di operazioni come la usuale somma e l'usuale prodotto, oppure munendo $\mathbb{P}$ delle operazioni di MCD e mcm, e munendo un qualsiasi insieme di numeri reali delle operazioni di scelta dell'estremo inferiore, dell'estremo superiore o anche del minimo e del massimo.

Al contrario gli insiemi numerici muniti dell'operazione differenza, come $\langle \mathbb{Z}, - \rangle$, non sono semigruppi, in quanto la differenza non è associativa: $c \neq 0 \iff a - (b - c) \neq (a - b) - c$. Similmente un magma come $\langle \mathbb{Q}_+, / \rangle$ non è semigruppo, dato che $b, c \neq 0$ implica $c \neq 1 \iff a/(b/c) \neq (a/b)/c$.

T15 b.03 Un semigruppo dotato di elemento neutro si dice **monoide**.
Denotiamo con **Mnd** la loro classe, con **MndAb** la classe dei monoidi abeliani, cioè dei monoidi commutativi, con **MndF** l'insieme dei monoidi finiti e con **MndFAb** l'insieme dei monoidi abeliani finiti.

In particolare con l'estensione (eventualmente ad hoc) di un elemento neutro, da un qualsiasi semigruppo si ricava un monoide.
Per esempio il monoide abeliano $\langle \mathbb{N}, +, 0 \rangle$ si può pensare ottenuto dal semigruppo $\langle \mathbb{P}, + \rangle$ per aggiunta di un elemento neutro formale denotato con 0. Similmente dal semigruppo libero delle stringhe su un alfabeto A munite di giustapposizione $\langle \mathsf{A}^*, \shortmid \rangle \in \mathbf{Sgrp}$ si ottiene il monoide libero $\langle A^*, \shortmid, \sqcup \rangle \in \mathbf{Mnd}$.
Le due specie di strutture sono quindi assai vicine: studio dei semigruppi e studio dei monoidi sono quasi completamente sovrapponibili.

T15 b.04 Sul piano formale è chiarificante e conveniente individuare un monoide come terna $\langle M, \odot, u \rangle$ con M insieme terreno, $\odot$ operazione binaria su M associativa e $u \in M \ \S \ \forall a \in M \ : \ u \odot a = a \odot u = a$.
In tal modo sono esplicitati tutti gli oggetti che caratterizzano un monoide e tutti gli assiomi che essi soddisfano.

Come vedremo questo genere di formalizzazione può essere adottata per tutte le specie di strutture algebriche.
Essa tuttavia in molti brani espositivi risulta decisamente pesante.

Come già evidenziato, si possono avere discorsi pesanti anche se si vuole mantenere costantemente la distinzione tra una struttura come un monoide e l'insieme che è il suo terreno.
In molti brani, soprattutto in molti sviluppi di valenza applicativa, non è necessario e opportuno insistere su queste distinzioni, in quanto il contesto permette a ogni lettore attento di evitare ambiguità. Nel seguito quindi spesso adotteremo degli "abusi di linguaggio", ossia la semplificazione consistente nel parlare di elementi di una struttura invece che di elementi del terreno di tale struttura.

T15 b.05 È opportuno segnalare altri tipi di monoidi attraverso caratterizzazioni generali.

Per ogni insieme S costituisce monoide la totalità delle relazioni binarie entro S munita dell'operazione di prodotto di composizione delle relazioni e dalla relazione identica su S: $\langle \mathfrak{P}(S \times S), \circ, \mathsf{Id}_S \rangle$.

Accanto a un tale monoide si può considerare quello costituito dalle matrici binarie quadrate di profilo $S \times S$, dal loro prodotto $*$ basato sulle due operazioni $\cdot$ e $+_2$ e dalla matrice unità di profilo $S \times S$ $\searrow$ $\boldsymbol{Idmat}_S$: questo monoide $\langle \mathsf{Mat}_{S;\mathbb{B}}, *, \boldsymbol{Idmat}_S \rangle$ è isomorfo al precedente e costituisce una sua rappresentazione matriciale.

Per ogni intero $m \geq 2$ sono monoidi $\langle \mathbb{Z}_m, +_m, 0 \rangle$ e $\langle \mathbb{Z}_m, \cdot_m, 1 \rangle$ [B25].

T15 b.06 Consideriamo un monoide $\boldsymbol{M} = \langle M, \odot, \mathbf{1} \rangle$ e un suo elemento $a \in M$.
Si dice **inverso a sinistra** di a un elemento $a' \in M$ tale che $a' \odot a = \mathbf{1}$.
Si dice **inverso a destra** di a un elemento $a'' \in M$ tale che $a \odot a'' = \mathbf{1}$.
Si dice inverso bilatero o semplicemente **elemento inverso** di a un elemento $a' \in M$ tale che $a \odot a' = a' \odot a = \mathbf{1}$, cioè un elemento del magma che è sia inverso a sinistra, che inverso a destra di a.

(1) Prop.: Un elemento inverso bilatero di un elemento a del monoide, se esiste, è unico.

Dim.: Se un elemento a di un magma avesse due elementi inversi a' e a'', cioè se fosse

$$a \odot a' = a' \odot a = \mathbf{1} = a \odot a'' = a'' \odot a = \mathbf{1} \ ,$$

si avrebbe $a' \odot a \odot a'' = a' \odot (a \odot a'') = a' \odot \mathbf{1} = a' = (a' \odot a) \odot a'' = \mathbf{1} \odot a'' = a''$, cioè $a' = a''$ ∎

T15 b.07 Un elemento a di un monoide si dice **elemento invertibile** sse possiede l'inverso.

Denotiamo l'insieme degli elementi invertibili del monoide $\boldsymbol{M}$ con $\mathbf{Invelm}[\boldsymbol{M}]$ o con $\mathbf{Invelm}_{\boldsymbol{M}}$.

Spesso per l'inverso di un elemento $a \in \mathbf{Invelm}[MBi]$ si usa la **notazione suffissa a esponente** a^{-1}.

Conviene segnalare che queste notazioni sono adottate per operazioni omologhe di molte altre specie di strutture algebriche.
Qui di seguito per fare riferimento a monoidi generici useremo preferibilmente la notazione funzionale $\mathcal{I}(a)$. In particolare osserviamo che per l'elemento neutro di un monoide $\boldsymbol{M}$ $\mathcal{I}(\mathbf{1}) = \mathbf{1}$ e che evidentemente $\mathbf{1} \in \mathbf{Invelm}[\boldsymbol{M}]$.

Il passaggio all'inverso è una funzione che possiamo sicuramente assegnare al genere $\lceil\!\lceil \mathbf{Invelm}(\boldsymbol{M}) \longmapsto M \rceil\!\rceil$.

Le due uguaglianze che caratterizzano il passaggio all'elemento inverso conviene riscriverle

$$a \odot \mathcal{I}(a) = \mathcal{I}(a) \odot a = \mathbf{1} \ .$$

Esse dicono che anche $\mathcal{I}(a)$ è elemento invertibile e che il suo inverso è a; quindi abbiamo

$$\forall a \in \mathbf{Invelm}[\boldsymbol{M}] \ : \ \mathcal{I}(\mathcal{I}(a)) = a \ .$$

Dobbiamo anche precisare il genere al quale appartiene il passaggio all'inverso,

$$\mathcal{I} \in \lceil\!\lceil \mathbf{Invelm}(\boldsymbol{M}) \lhd\!\!\longrightarrow\!\!\rhd \mathbf{Invelm}(\boldsymbol{M}) \rceil\!\rceil \ .$$

Tra gli elementi invertibili può essere utile distinguere quelli che coincidono con il proprio inverso, come l'unità, da quelli distinti dal proprio inverso. I primi sono chiamati elementi involutori o **involuzioni**.

T15 b.08 Prop. Il prodotto di due elementi invertibili di un monoide a e b è anch'esso invertibile e si ha $\mathcal{I}(a \odot b) = \mathcal{I}(b) \odot \mathcal{I}(a)$.

Dim.: Siano a e b due elementi invertibili;

$$(a \odot b) \odot (\mathcal{I}(b) \odot \mathcal{I}(a)) = a \odot \mathbf{1} \odot \mathcal{I}(a) = \mathbf{1}, \text{ e } (\mathcal{I}(b) \odot \mathcal{I}(a)) \odot (a \odot b) = \mathcal{I}(b) \odot \mathbf{1} \odot b = \mathbf{1}$$ ∎

Spesso per denotare l'operazione binaria di un semigruppo, anche generico, si usa il simbolo "$\cdot$" e la si chiama prodotto; inoltre nelle espressioni spesso si adotta l'abbreviazione consistente nel trascurare lo stesso segno "$\cdot$" scrivendo $a\,b$ invece di $a \cdot b$; in questi casi di solito l'inverso di a si denota con a^{-1}.

Quando si trattano due o più operazioni binarie $\odot$, $\otimes$, ... entro un unico insieme M, cioè quando si trattano i magmi $\langle M, \odot\rangle$, $\langle M, \otimes\rangle$, ..., e inoltre si devono distinguere le operazioni di passaggio all'inverso, può essere opportuno esprimere queste con notazioni come $inv(\odot)$, $inv(\otimes)$ ... ,

T15 b.09 Vi sono monoidi come $\langle \mathbb{N}, +, 0\rangle$ nei quali solo l'elemento neutro è invertibile; viceversa tutti gli elementi dei monoidi $\langle \mathbb{Z}, +, 0\rangle$, $\langle \mathbb{Q}_+, \cdot, 1\rangle$, $\langle \mathbb{Q}_{nz}, \cdot, 1\rangle$, $\langle \mathbb{R}_+, \cdot, 1\rangle$, $\langle \mathbb{R}_{nz}, \cdot, 1\rangle$, $\langle \mathbb{C}_{nz}, \cdot, 1\rangle$, posseggono inverso. Chiaramente l'inverso di $n \in \mathbb{Z}$ è $-n$, mentre l'inverso di $r \in \mathbb{C}_{nz}$ è $1/r$; in $\mathbb{R}_+$ e in $\mathbb{Q}_+$ solo l'unità coincide con il proprio inverso; in $\mathbb{C}_{nz}$, $\mathbb{R}_{nz}$ e $\mathbb{Q}_{nz}$ coincide con il proprio inverso anche l'elemento -1.

Dall'aritmetica modulare [B26] si ricava che per ogni $m \in \mathbf{[}2 : +\infty\mathbf{)}$ la struttura $\langle \mathbb{Z}_m, \cdot_m, 1\rangle$ costituisce un monoide chiamato **monoide moltiplicativo delle classi di resti** modulo m.

Gli elementi invertibili di tale monoide sono gli interi r primi con m, cioè tali che $r \perp m$.

Per esempio $\mathbf{Invelm}(\mathbb{Z}_7) = \{1, 2, 3, 4, 5, 6\}$, $\mathbf{Invelm}(\mathbb{Z}_8) = \{1, 3, 5, 7\}$ e $\mathbf{Invelm}(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$. In generale il cardinale di $\mathbf{Invelm}(\mathbb{Z}_m)$ è dato dal valore $\Phi_{eu}(m)$ della funzione totient di Eulero [B26e04].

T15 c. quasigruppi e loops

T15 c.01 Definiamo **quasigruppo** un coppia $\langle Q, * \rangle$ dove Q è un insieme e $* \in \lceil\!\lceil\, Q \times Q \longmapsto Q \,\rceil\!\rceil$ ai quali si chiede:

(1) $\forall a, b \in Q \;:\;$ esiste unico $x \in Q$ tale che $a * x = b$;

(2) $\forall a, b \in Q \;:\;$ esiste unico $y \in Q$ tale che $y * a = b$.

Per questi due elementi in genere si scrive, risp., $x = a \backslash b$ e $y = b / a$.

Le operazioni binarie così introdotte sono chiamate, risp., **divisione a sinistra** e **divisione a destra**.

Denotiamo con Qgrp_Q l'insieme dei quasigruppi aventi l'insieme Q come terreno e denotiamo con Qgrp la classe dei quasigruppi.

T15 c.02 Si osserverà che la specie dei quasigruppi estende quella dei gruppi, in quanto per la loro operazione binaria non si chiede la proprietà associativa.

Un quasigruppo è dunque un magma la cui operazione binaria (prodotto) è tale da consentire di individuare due operazioni che la invertono.
Si osserva che quando vale la proprietà associativa divisione a sinistra e divisione a destra devono coincidere.

Per un quasigruppo valgono le **proprietà di cancellazione**:

(1) $$\forall a, b, c \in Q \quad : \quad a * b = a * c \implies b = c \,,$$

(2) $$\forall a, b, d \in Q \quad : \quad a * b = d * b \implies a = d \,.$$

Si constata che la (1) equivale alla $\mathsf{c01}(1)$ e che la (2) equivale alla $\mathsf{c01}(2)$. Quindi si possono definire i quasigruppi postulando (1) e (2) invece di $\mathsf{c02}(1)$ e $\mathsf{c02}(2)$.

T15 c.03 Vediamo alcuni esempi di quasigruppi che non siano gruppi.

È un quasigruppo la coppia $\langle S, *_\mu \rangle$, dove S è il terreno di uno spazio vettoriale $\boldsymbol{S}$ sopra un campo di caratteristica diversa da 2 e contenente i numeri razionali e con $*_\mu$ si denota l'operazione di passaggio al punto medio:

$$*_\mu \;:=\; \lceil\!\lceil\, \langle \mathsf{v}, \mathsf{w} \rangle \in S \times S \;\mapsto\; \frac{1}{2}\,(\mathsf{v} + \mathsf{w}) \,\rceil\!\rceil \;.$$

Infatti $*_\mu$ è evidentemente un'operazione idempotente; chiaro anche che si tratta di un quasigruppo abeliano. Si osserva che per $\mathsf{v}, \mathsf{u} \in S$ si ha $\mathsf{v} / \mathsf{u} = \mathsf{v} + 2(\mathsf{u} - \mathsf{v})$.

T15 c.04 Eserc. Verificare che sono quasigruppi:

(a) $\langle \mathbb{Z}, - \rangle$;

(b) $\langle \mathbb{Q}_{nz}, / \rangle$, $\langle \mathbb{R}_{nz}, / \rangle$ e $\langle \mathbb{C}_{nz}, / \rangle$.

T15 c.05 Rivediamo le proprietà $\mathsf{c01}(1)$ e $\mathsf{c01}(2)$ della definizione della specie dei quasigruppi per le loro conseguenze sopra un quasigruppo finito $\boldsymbol{Q} = \langle Q, * \rangle$ e sulla sua tavola di Cayley T.

La prima equivale ad affermare che per ogni $\langle a, b \rangle \in Q \times Q$ nella riga a della tavola T l'elemento b si trova una e una sola volta.
La seconda equivale a dire che per ogni $\langle a, b \rangle \in Q \times Q$ nella colonna a della T l'elemento b si trova una e una sola volta.

Di conseguenza la tavola di moltiplicazione per un quasigruppo finito è un quadrato latino con le entrate in Q. Viceversa si constata che ogni quadrato latino L di ordine n con entrate costituenti un insieme E di n elementi, cioè ogni matrice $n \times n$ che in ciascuna delle sue righe e colonne presenta una permutazione di E individua il quasigruppo su E avente come tavola di moltiplicazione la matrice L.

Dunque quasigruppi finiti e quadrati latini costituiscono due specie di strutture criptomorfe.

I quadrati latini sono presentati con una certa ampiezza in D63.

T15 c.06 Vi sono quasigruppi dotati di unità e quasigruppi privi di tale elemento.
Un quasigruppo dotato di unità, ossia un quasigruppo unifero, viene detto loop.

Più formalmente diciamo **loop** una struttura algebrica avente una costituzione della forma $\langle Q, *, e\rangle$ dove $\langle Q, *\rangle$ è un quasigruppo ed e è un elemento di Q tale che

$$\forall a \in Q \ : \ a * e = e * a = a \ .$$

Dunque e è elemento neutro bilatero per l'operazione $*$, tale elemento è unico e ogni elemento $a \in Q$ è dotato di inverso a sinistra e di inverso a destra.

Denotiamo con Loop_Q l'insieme dei loops aventi come terreno un insieme S e con Loop la classe dei loops.

Evidentemente Loop estende la classe dei gruppi; più precisamente la classe dei gruppi coincide con la classe dei loops associativi.

T15 c.07 Consideriamo un generico loop $\langle Q, *, e\rangle$.
Ogni elemento $a \in Q$ possiede un unico inverso a sinistra che possiamo scrivere $invLt(a) := e/a$; per esso $invLt(a) * a = e$.
Ogni a possiede anche un unico inverso a destra per il quale adottiamo la notazione $invRt(a) := e/a$; per esso si ha $a * invRt(a) = e$.

Un elemento a di un loop di dice **possedere inverso bilatero** sse $invLt(a) = invRt(a)$.
Un loop $\langle Q, *, e\rangle$ si dice possedere inversione bilatera sse ciascuno dei suoi elementi possiede inverso bilatero, ossia sse $\forall a \in Q \ : \ invLt(a) = invRt(a)$.
Per un tale loop di solito l'inverso di un elemento a si scrive a^{-1}.

T15 c.08 Introduciamo ora una interessante specie di strutture più ampia della specie dei loops.

Si dice **loop a sinistra** una struttura avente una costituzione della forma $\langle Q, *, e_{Lt}\rangle$, dove Q è un insieme nonvuoto, $*$ un'operazione binaria tale che (1) $\forall a, b \in Q \ : \ $ esiste unico $x \in Q$ tale che $a * x = b$ ed e_{Lt} è elemento neutro per $*$, ossia un elemento tale che $\forall a \in Q \ : \ e_{Lt} * a = a * e_{Lt}$.

Dualmente-LR si definisce la specie di struttura **loop a destra.**

T15 c.09 Un tipo notevole di loops a sinistra è costituito dalle sezioni relative a una coppia $\langle G, H\rangle$ con $G \in$ **Grp** e $H \leq_{Grp} G$.

T15 c.10 Si dice **loop di Moufang** un loop $\langle Q, *, e\rangle$ che soddisfa le seguenti uguaglianze equivalenti

$$\forall a, b, c \in Q \ : \ \begin{array}{c} c(a(cb)) \ = \ ((ca)c)b \quad , \quad ((ac)b)c \ = \ a(c(bc)) \quad , \\ (ca)(bc) = (c(ab))c \quad , \quad (ca)(bc) = c((ab)c) \end{array} \ .$$

Esse sono dette **identità di Moufang**, in onore di Ruth Moufang .

T15 c.11 Evidentemente le identità di Moufang sono proprietà meno forti della associatività, espressa dall'uguaglianza $\forall a, b, c \in Q \ : \ a(bc) = (ab)c$.

In effetti la classe dei gruppi coincide con la classe dei loops di Moufang associativi ed è contenuta propriamente nella classe dei loops di Moufang.
Vengono studiati vari loops di Moufang non associativi di rilevante interesse.

Le identità di Moufang implicano rilevanti identità che esplicitano proprietà di queste strutture:

$\forall a, b, c \in Q \ :$

$a(ab) = a(ab)$, **identità alternativa a sinistra**;

$(ab)b = a(bb)$, **identità alternativa a destra**;

$a(ba) = (ab)a$, chiamata **identità flessibile**.

Esse si ottengono dalle identità in c10 facendo coincidere uno degli elementi in gioco con l'elemento neutro e.

T15 c.12 Vari loops di Moufang si ottengono da elementi particolari dell'algebra degli octonioni [G55a].

Un'ampia collezione di loops di Moufang si ottengono da un generico gruppo $\boldsymbol{G} = \langle G, \cdot, e \rangle$ con la seguente costruzione.

Si introduce un oggetto formale u estraneo a G e si assume come terreno $M(G, 2) := G \dot\cup \{g \in G :| \langle g, u \rangle\}$.
Si assume come operazione binaria di $M(G, 2)$ l'estensione del prodotto in G derivata dalle seguenti definizioni

$$\forall g, h \in G \ : \ (gu)h := (gh^{-1})u \quad , \quad g(hu := (hg)u \quad , \quad (gu)(hu) := h^{-1}\, g \ .$$

Queste implicano $u^2 = e$ e $ug = g^{-1}\, u$ e successivamente che $M(\boldsymbol{G}, 2)$ è un loop di Moufang.
Si trova poi che questo loop è associativo, ossia che è un gruppo, sse $\boldsymbol{G}$ è un gruppo abeliano.

T15 c.13 Un loop $\langle Q, *, e \rangle$ si dice **loop di Bol sinistro** sse accade che

$$\forall a, b, c \in Q \ : \ a(b(ac)) = (a(ba))c \ .$$

Si dice invece **loop di Bol destro** sse

$$\forall a, b, c \in Q \ : \ ((ca)b)a = (c(ab))a \ .$$

Il loro nome ricorda il matematico olandese Gerrit Bol.

Si segnala che le precedenti identità esprimono richieste meno forti della associatività.

Si dimostra che un loop che risulta essere sia loop di Bol a sinistra che loop di Bol a destra è un loop di Moufang.

T15 d. gruppi

T15 d.01 In ogni monoide $\boldsymbol{M}$, grazie alla invertibilità della composizione di due elementi invertibili si ha che **Invelm**($\boldsymbol{M}$) costituisce un sottomonoide [e05].
Per tale sottomonoide il passaggio all'inverso è una funzione definita su tutto l'insieme terreno e più precisamente è una permutazione che coincide con la propria inversa, cioè è una involuzione.

Per qualsiasi insieme S una funzione del genere $\lceil\, S \longmapsto S \,\rceil$, come l'inversione in un insieme esprimibile come **Invelm**($\boldsymbol{M}$), può essere chiamata **operazione unaria** o anche **operatore unario**. Questo operatore nelle espressioni degli elementi della struttura può essere denotato:

- con una **notazione funzionale usuale**, per esempio con $\mathcal{I}(a)$;
- con un segno che precede il relativo operando, cioè con una cosiddetta **notazione prefissa** (questo accade con $-n$ per ogni n numero intero,reale e complesso);
- con un segno che lo segue, cioè con una **notazione suffissa a esponente** (come accade con $f^{-\mathbf{1}}$ o a^{-1}).

T15 d.02 Un monoide $\boldsymbol{M}$ nel quale ogni elemento è invertibile, cioè tale che $M =$ **Invelm**($\boldsymbol{M}$), si dice costituire una struttura che chiameremo gruppo.
Definiamo ora la specie delle strutture di gruppo basandola esplicitamente sopra una operazione binaria, una unaria e una nullaria.

Diciamo **gruppo** una quaterna $\boldsymbol{G} = \langle G, \cdot, {}^{-1}, e\rangle$ nella quale:
G è un insieme (il terreno del gruppo),
$\cdot$ è una operazione binaria su G,
e è un elemento rilevante della struttura G, cioè una operazione nullaria,
$^{-1}$ è una operazione unaria su G e inoltre valgono le seguenti uguaglianze

$$\forall a, b, c \in G \;:\; a \cdot b \in G \;,\quad a \cdot e = e \cdot a = a \;,\quad a \cdot (b \cdot c) = (a \cdot b) \cdot c \;,$$
$$a \cdot (a^{-1}) = (a^{-1}) \cdot a = e \;.$$

Un gruppo si dice **gruppo abeliano** o **gruppo commutativo** sse la sua operazione binaria è commutativa, cioè sse il corrispondente monoide è abeliano.
Denoteremo con **Grp** la classe dei gruppi, con **GrpAb** quella dei gruppi abeliani, con **GrpF** l'insieme dei gruppi finiti e con **GrpAbF** l'insieme dei gruppi finiti abeliani.

T15 d.03 Molti esempi di gruppi si ricavano direttamente dagli esempi di monoidi visti in precedenza. I monoidi con tutti gli insiemi invertibili si possono considerare automaticamente dei gruppi. Dai monoidi numerici abeliani visti in precedenza si ricavano svariati gruppi abeliani
$\langle \mathbb{Z}, +, -, 0\rangle$, $\langle \mathbb{Q}, +, -, 0\rangle$, $\langle \mathbb{R}_{\mathsf{a}}, +, -, 0\rangle$, $\langle \mathbb{R}_{\mathsf{c}}, +, -, 0\rangle$, $\langle \mathbb{R}, +, -, 0\rangle$, $\langle \mathbb{C}, +, -, 0\rangle$,
$\langle \mathbb{Q}_{+}, \cdot, {}^{-1}, 1\rangle$, $\langle \mathbb{R}_{\mathsf{A},+}, \cdot, {}^{-1}, 1\rangle$, $\langle \mathbb{R}_{\mathsf{C},+}, \cdot, {}^{-1}, 1\rangle$, $\langle \mathbb{R}_{+}, \cdot, {}^{-1}, 1\rangle$, $\langle \mathbb{C}_{+}, \cdot, {}^{-1}, 1\rangle$,
$\langle \mathbb{Q}_{nz}, \cdot, {}^{-1}, 1\rangle$, $\langle \mathbb{R}_{\mathsf{A},nz}, \cdot, {}^{-1}, 1\rangle$, $\langle \mathbb{R}_{\mathsf{C},nz}, \cdot, {}^{-1}, 1\rangle$, $\langle \mathbb{R}_{nz}, \cdot, {}^{-1}, 1\rangle$, $\langle \mathbb{C}_{nz}, \cdot, {}^{-1}, 1\rangle$.

T15 d.04 Per ogni intero p primo dal monoide moltiplicativo delle classi di resti modulo p si ricava un gruppo di ordine $p-1$ trascurando la sola classe $[0]_p$.
Per ogni m fattorizzabile dal monoide moltiplicativo delle classi di resti modulo m si ricava un gruppo di ordine $\Phi_{eu}(m)$ [B26e04] trascurando $[0]_m$ e tutte le classi $[k]_m$ per k divisore di m.

Le tavole di Cayley dei gruppi **Invelm**($\mathbb{Z}_5$), **Invelm**($\mathbb{Z}_6$) e **Invelm**($\mathbb{Z}_8$) sono:

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

,

	1	5
1	1	5
5	5	1

e

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

T15 d.05 **Eserc.** Precisare le tavole di moltiplicazione di **InvElm**$(\mathbb{Z}_7)$ e **InvElm**$(\mathbb{Z}_9)$.

T15 d.06 Per un generico insieme S, dal monoide delle endofunzioni, riducendo il terreno $\lceil S \longmapsto S \rceil$ all'insieme delle funzioni invertibili si ricava il gruppo delle biiezioni di S $\lceil S \longmapsto\!\!\triangleright S \rceil$.
Questa struttura è chiamata **gruppo delle permutazioni** dell'insieme S o **gruppo simmetrico** dell'insieme S e viene denotato con Sym_S .

A partire dai gruppi di permutazioni, come vedremo, si individuano vari altri gruppi di grande interesse attraverso limitazioni alle permutazioni consistenti nel richiedere che conservino determinate configurazioni di elementi di S o determinate funzioni aventi come dominio S, $S \times S$ o altre costruzioni su S.
Infatti se due permutazioni π e ρ soddisfano una di queste richieste, la soddisfano anche le loro inverse $\pi^{-\mathbf{1}}$ e $\rho^{-\mathbf{1}}$ e le loro composizioni come $\pi \circ \rho$.
Dai monoidi liberi non si possono ricavare gruppi interessanti, in quanto essi presentano come unico elemento invertibile la stringa muta.

T15 d.07 Della struttura di gruppo si possono dare varie altre definizioni equivalenti.
Una definizione chiaramente equivalente alla precedente è la seguente.
Si definisce **gruppo** una quaterna $\boldsymbol{G} = \langle G, \cdot, {}^{-1}, e \rangle$ tale che $\langle G, \cdot, e \rangle \in$ **Mnd** e "$^{-1}$" è una operazione unaria su G tale che

$$\forall a \in G \ : \ a \cdot (a^{-1}) = (a^{-1}) \cdot a = e \ .$$

T15 e. specie di strutture algebriche

T15 e.01 Magmi, semigruppi, monoidi e gruppi sono esempi di **strutture algebriche monoterreno**. In generale con questo termine si intendono sistemi della forma

$$\boldsymbol{S} = \langle S, \beta_1, ..., \beta_b, y_1, .., y_u, \nu_1, ..., \nu_n \rangle$$

dove S è un insieme detto **terreno** di $\boldsymbol{S}$, i β_i denotano operazioni binarie su S, gli y_i individuano operatori unari di S e i ν_i sono elementi particolari di S.
In questa definizione si può far entrare una vastissima varietà di oggetti matematici, ma gran parte di questi riveste interesse scarso o nullo; si ottengono strutture interessanti e utili imponendo agli operatori sistemi di assiomi opportuni.

Un elemento particolare di una struttura algebrica, come l'unità per un monoide, viene chiamato anche **operazione nullaria** della struttura. Questa dizione corrisponde a dare a questi elementi particolari il nome di operazioni con 0 operandi, in modo da assimilarli alle operazioni unarie (con un operando) e alle binarie (con due operandi) con qualche vantaggio espositivo.

T15 e.02 Può essere utile anche studiare strutture algebriche munite di operazioni che richiedono 3, 4, ... operandi, cioè, se con S denotiamo il terreno, muniti di funzioni dei generi $\lceil S^3 \longmapsto S \rceil$, $\lceil S^4 \longmapsto S \rceil$, ...; in questi casi, non molto studiati, si parla di **operazioni ternarie**, di **operazioni quaternarie** e così via.

Il numero degli operandi richiesti da una operazione viene chiamata **arietà della operazione**.

Conviene segnalare che si incontrano importanti strutture algebriche basate su due o più insiemi le quali vengono chiamate **strutture algebriche multiterreno**.

Una struttura algebrica è quindi un sistema formale individuato da uno o più insiemi terreno, da leggi di composizione che riguardano tali insiemi e da proprietà che devono essere soddisfatte dai precedenti oggetti. Queste proprietà sono espresse prevalentemente da equazioni nelle quali entrano generici elementi degli insiemi terreno o di loro determinati sottoinsiemi.

Diciamo **costituzione di una struttura algebrica** la famiglia dei generi funzionali che caratterizzano le sue operazioni.

Segnaliamo anche che svolgono ruoli importanti nella matematica strutture formali che si servono di costruzioni che non si riducono a operazioni con una determinata arietà; un esempio è dato dalle strutture topologiche. Talune di queste strutture non richiedono operazioni con determinata arietà, altre invece richiedono operazioni algebriche e in genere possono essere considerate arricchimenti di strutture ampiamente studiate con metodi algebrici.

T15 e.03 Vengono studiate proficuamente anche strutture di genere algebrico munite di operazioni definite in sottoinsiemi dei propri terreni o dei prodotti cartesiani dei detti terreni.
Per esempio una struttura dotata di un solo terreno S si può dotare di operatori unari definiti su un sottoinsieme proprio di S e/o di operazioni binarie definite su un sottoinsieme proprio di $S \times S$.
In uno di questi casi si parla di **struttura munita di operazioni parziali**. [e.g. D26d03].

Si considerano anche strutture dotate di operazioni che forniscono non singoli elementi ma insiemi di elementi degli insiemi terreno. In uno di questi casi si parla di **struttura munita di operazioni larghe**.

Alcune delle strutture formali studiate sono munite di relazioni.

Per trattare molti problemi combinatorici, computazionali e di elaborazione delle informazioni, e quindi per affrontare fattivamente molte applicazioni, risultano utili strutture nelle quali compaiono relazioni, eventualmente accanto a operazioni, alle quali si impongono opportuni assiomi espressi non solo da equazioni, ma anche da relazioni.
In questi casi si parla anche di **strutture relazionali** o di **strutture algebrico-relazionali**.
Queste spesso conviene vederle come arricchimenti delle più semplici strutture relazionali, cioè dei digrafi [D27].

T15 e.04 Una distinzione importante tra le specie di strutture riguarda le cosiddette **strutture equazionali**, strutture i cui assiomi possono essere espressi esclusivamente da equazioni.
Alcune di queste strutture sono caratterizzate da sottoinsiemi degli insiemi terreno e da proprietà espresse da relazioni e in genere per esse le equazioni non svolgono ruoli di primo piano. Talora però tra queste strutture e strutture algebriche più classiche ed "equazionali" si trovano collegamenti non evidenti, ma utili per chiarire situazioni sostanziali (come per la teoria algebrica degli automi). Tra le strutture di questo tipo si possono ricordare i riconoscitori di Rabin-Scott, le grammatiche e in genere le macchine formali.

T15 e.05 Diciamo **schema costitutivo** o, più specificamente, **echelon** di una struttura algebrica e/o relazionale il complesso delle operazioni munite delle caratterizzazioni dei rispettivi domini e codomini.
Si dice **specie di strutture algebriche** ogni collezione di strutture algebriche che seguono uno stesso schema costitutivo, cioè che dispongono dello stesso numero di insiemi terreno, sono munite di operazioni delle stesse arietà e soddisfano richieste formalmente uguali, fornite da equazioni o da enunciati equivalenti.
Le collezioni dei magmi, dei semigruppi, dei monoidi, dei semireticoli, dei quasigruppi, dei loops, dei gruppi, dei magmi abeliani, ... dei gruppi abeliani costituiscono esempi di specie di strutture algebriche monoterreno.

Più in generale vengono trattate le **specie di strutture matematiche**, collezioni di strutture che seguono uno stesso schema costitutivo e soddisfano agli stessi assiomi.
In particolare vengono prese in considerazione la specie delle relazioni binarie, le più particolari specie delle relazioni simmetriche e le specie delle relazioni simmetriche su insiemi di n elementi.
Si possono considerare anche le specie delle funzioni e le più particolari specie delle permutazioni, le specie delle involuzioni, le specie delle involuzioni su insiemi di un particolare numero n edi elementi.
Le specie su insiemi con cardinale finito sono gli oggetti centrali per le indagini combinatoriche.

T15 e.06 Una specie di strutture $\mathcal{S}_1$ si dice **specie di strutture più ricca** di una seconda specie $\mathcal{S}_2$ sse lo schema costitutivo della prima specie è un ampliamento dello schema della seconda.
Equivalentemente si dice che $\mathcal{S}_2$ è una **specie di strutture più povera** della $\mathcal{S}_1$.
Nello schema costitutivo della specie $\mathcal{S}_1$ potrebbero intervenire più insiemi terreno e/o più operazioni su tali insiemi che nello schema costruttivo della specie $\mathcal{S}_2$.
Ad esempio la specie dei gruppi è più ricca della specie dei monoidi e questa è più ricca di quella dei semigruppi.

Si dice invece che si ha una **specie di strutture più stringente** di una seconda sse la prima deve ubbidire a un insieme di assiomi più forte, ovvero a un sistema di assiomi equivalente a uno più restrittivo (in genere consistente in requisiti più cogenti).

Per esempio la specie dei gruppi abeliani è più stringente (ma non più ricca) della specie dei gruppi.
La specie dei semigruppi è più stringente (ma non più ricca) della specie dei magmi.
I gruppi costituiscono una specie di struttura più ricca e più stringente della specie dei monoidi.

T15 e.07 Naturalmente tra le strutture di ogni specie è importante distinguere tra **strutture finite**, aventi insiemi terreno finiti e quindi operazioni finite, e le **strutture infinite**; tra queste si distinguono le **strutture numerabili** aventi terreni e operazioni numerabili, e le **strutture più che numerabili**.

Collettivamente strutture finite e numerabili si dicono **strutture contabili**; si parla inoltre di **strutture esplicite** nel caso di strutture aventi insiemi di terreno e operazioni forniti da elenchi espliciti e di **strutture costruibili** nel caso di strutture per le quali sono date procedure per la costruzione effettiva degli insiemi di terreno e delle leggi di composizione, ovvero delle tavole di Cayley.

T15 f. prodotti di strutture

T15 f.01 Introduciamo ora la costruzione più ampiamente utilizzata per ricavare nuove strutture da strutture note procedento su specie di strutture via via più ricche.

Consideriamo due magmi $\boldsymbol{M}_1 = \langle M_1, \odot_1 \rangle$ e $\boldsymbol{M}_2 = \langle M_2, \odot_2 \rangle$; si dice **prodotto diretto di magmi** di tali magmi la struttura

$$\boldsymbol{M}_1 \times \boldsymbol{M}_2 \ := \big\langle M_1 \times M_2, \odot_1 \times \odot_2 \big\rangle \ ,$$

Il secondo componente di questo prodotto diretto è l'operazione binaria $\odot_1 \times \odot_2$ definita chiedendo

$$\forall a_1, b_1 \in S_1 \ , \ a_2, b_2 \in S_2 \ : \ \big\langle a_1, a_2 \big\rangle (\odot_1 \times \odot_2) \big\langle b_1, b_2 \big\rangle := \big\langle a_1 \odot_1 b_1, a_2 \odot_2 b_2 \big\rangle \ .$$

L'operatore $\odot_1 \times \odot_2$ può chiamarsi **prodotto cartesiano delle operazioni** $\odot_1$ e $\odot_2$.
Dato che $\odot_1 \times \odot_2$ è definita su tutto $S_1 \times S_2$, anche la nuova struttura è un magma.

Inoltre il prodotto diretto di due semigruppi è un semigruppo, in quanto la associatività delle operazioni $\odot_1$ e $\odot_2$ si mantiene quando si compongono le coppie di elementi di semigruppi.

La costruzione prodotto diretto si può replicare e si dimostra facilmente che è associativa.
Si può quindi considerare la potenza diretta d-esima di un magma per ogni d intero positivo, insieme delle sequenze di lunghezza d di elementi del magma munito della composizione componente per componente.

Più in generale si può considerare il magma delle funzioni da un insieme qualsiasi S su un magma $\langle M, \odot \rangle$ avente come composizione

$$\Big\lceil \ \langle f, g \rangle \in \big\lceil \, S \longmapsto M \, \big\rceil^{\times 2} \Big\rceil \ \mapsto \ \big\lceil \, x \in S \mapsto f(x) \odot g(x) \, \big\rceil \ \Big\rceil \ .$$

Si ha in particolare il magma dato dall'insieme delle successioni di numeri razionali $\big\lceil \, \mathbb{N} \longmapsto \mathbb{Q} \, \big\rceil$ e dalla somma termine a termine delle successioni.

T15 f.02 Si dice **prodotto diretto di due monoidi** $\boldsymbol{M}_1 = \langle M_1, \odot_1, \mathbf{1}_1 \rangle$ e $\boldsymbol{M}_2 = \langle M_2, \odot_2, \mathbf{1}_2 \rangle$ la struttura

$$\boldsymbol{M}_1 \times \boldsymbol{M}_2 \ := \big\langle M_1 \times M_2, \odot_1 \times \odot_2, \langle \mathbf{1}_1, \mathbf{1}_2 \rangle \big\rangle \ .$$

È facile convincersi che $\big\langle \mathbf{1}_1, \mathbf{1}_2 \big\rangle$ è l'unità per $\odot_1 \times \odot_2$ e quindi che con $\boldsymbol{M}_1 \times \boldsymbol{M}_2$ si è costruito un nuovo monoide.

In particolare si ha un monoide come $\langle \mathbb{N}^2, \mathbf{+}, \langle 0, 0 \rangle \rangle$, dove $\mathbf{+}$ denota la somma termine a termine delle coppie di numeri o in generale la somma componente per componente delle sequenze numeriche della stessa lunghezza.

T15 f.03 Si dice **prodotto diretto di due gruppi** $\boldsymbol{G}_1 = \big\langle G_1, \odot_1, \mathcal{I}_1, e_1 \big\rangle$ e $\boldsymbol{G}_2 = \big\langle G_2, \odot_2, \mathcal{I}_2, e_2 \big\rangle$ la struttura

$$\boldsymbol{G}_1 \times \boldsymbol{G}_2 \ := \ \Big\langle G_1 \times G_2, \odot_1 \times \odot_2, \mathcal{I}_1 \times \mathcal{I}_2, \big\langle e_1, e_2 \big\rangle \Big\rangle \ ,$$

il terzo membro della quale essendo l'operazione unaria definita da

$$\mathcal{I}_1 \times \mathcal{I}_2 \ := \ \Big\lceil \, \big\langle a_1, a_2 \big\rangle \in G_1 \times G_2 \mapsto \big\langle \mathcal{I}_1(a_1), \mathcal{I}_2(a_2) \big\rangle \, \Big\rceil \ .$$

Si verifica senza difficoltà che questa costruzione produce un nuovo gruppo.

In particolare si hanno i gruppi $\big\langle \mathbb{Z}^{\times 2}, \mathbf{+}, \mathbf{-}, \langle 0, 0 \rangle \big\rangle$, $\big\langle \mathbb{R}^{\times 2}, \mathbf{+}, \mathbf{-}, \langle 0, 0 \rangle \big\rangle$ e $\big\langle \mathbb{C}^{\times 2}, \mathbf{+}, \mathbf{-}, \langle 0, 0 \rangle \big\rangle$, dove $\mathbf{-}$ è l'operatore unario per coppie, per terne e per altre sequenze di numeri definito da $\mathbf{-}\big\langle z_1, z_2 \big\rangle \ := \big\langle -z_1, -z_2 \big\rangle$.

Questi gruppi si possono chiamare, risp., **gruppo additivo dei vettori piani a coordinate intere**, **gruppo additivo dei vettori piani a coordinate reali**, **gruppo additivo dei vettori bidimensionali a coordinate complesse**.

T15 f.04 Le diverse generalizzazioni di prodotto diretto si possono applicare anche a monoidi e gruppi. Si hanno per esempio, per d intero positivo, monoidi come $\langle \mathbb{N}^{\times d}, \mathbf{+}, \langle 0, ..., 0\rangle\rangle$ e gruppi come il **gruppo additivo dei vettori d-dimensionali reali** $\langle \mathbb{R}^{\times d}, \mathbf{+}, \mathbf{-}, \langle 0, ..., 0\rangle\rangle$.

Visto come si possono "comporre cartesianamente" le operazioni delle diverse arietà, si può intuire come si possano introdurre i prodotti diretti e le potenze dirette per strutture di molte altre specie.

Si osserva che i prodotti diretti e le potenze dirette di strutture costruibili hanno come terreno un insieme costruibile e sono dotati di operazioni costruibili, e di conseguenza costituiscono anch'essi strutture algebriche della stessa specie costruibili.

T15 f.05 Introduciamo altre nozioni di portata generale, ma facendo riferimento alle strutture monoterreno considerate in precedenza.

Relativamente a un magma $\boldsymbol{M} = \langle M, \odot\rangle$, un sottoinsieme $N \subseteq M$ si dice **insieme chiuso** rispetto all'operazione $\odot$ sse $\forall a, b \in N \ : \ a \odot b \in N$.

Si dice **sottomagma** di un magma $\langle M, \odot\rangle$ un sistema $\langle N, \odot|_N\rangle$, con N sottoinsieme di M chiuso rispetto alla operazione $\odot|_N$, restrizione all'insieme N dell'operazione $\odot$.

La richiesta di chiusura di N si può anche esprimere scrivendo $N \odot^{be} N \subseteq N$; qui con $\odot^{be}$ si è denotata l'**estensione booleana dell'operazione** $\odot$, ossia l'operazione definita per due sottoinsiemi N e P di M ponendo

$$N \odot^{be} P \ := \ \{a \in N, b \in P :| \ a \odot b\} \ .$$

La notazione $\odot^{be}$ in genere si può semplificare nella semplice $\odot$ portando solo ad ambiguità risolvibili esaminando il contesto.

Ogni sottomagma di un magma è esso stesso un magma.
Per enunciare che N è sottomagma di M, ovvero che è terreno di un sottomagma del magma avente M come terreno, si scrive $N \leq_{Mgm} M$.
Per enunciare che N è sottomagma proprio di M, cioè che $N \leq_{Mgm} M$ e che $N \subset M$, si scrive $N <_{Mgm} M$.

T15 f.06 Un sottomagma di un semigruppo costituisce un semigruppo, in quanto l'operazione binaria ristretta ad un tale sottoinsieme mantiene la proprietà di associatività; tale sottomagma si dice **sottosemigruppo**.
Per enunciare che N è sottosemigruppo di M, ovvero che è terreno di un sottosemigruppo del semigruppo avente M come terreno, si scrive $N \leq_{Sgrp} M$.
Per enunciare che N è sottosemigruppo proprio di M, cioè che $N \leq_{Sgrp} M$ e che $N \subset M$, si scrive $N <_{Sgrp} M$.

Si dice **sottomonoide** di un monoide $\langle M, \cdot, \mathbf{1}\rangle$ ogni suo sottosemigruppo N, ovvero ogni suo sottomagma, contenente l'unità. N viene quindi caratterizzato dalle relazioni $N \odot N \subseteq N$ e $\mathbf{1} \in N$. Si verifica facilmente che le due uguaglianze precedenti equivalgono alla $N \odot N = N$.

Per segnalare che che N è sottomonoide di M scriviamo $N \leq_{Mnd} M$, mentre per segnalare che che N è sottomonoide proprio di M scriviamo $N <_{Mnd} M$.

T15 f.07 (1) Eserc. Provare che $\langle \mathbb{Z}, +, 0\rangle <_{Mnd} \langle \mathbb{Q}, +, 0\rangle$ e che $\langle \mathbb{Q}, +, 0\rangle <_{Mnd} \langle \mathbb{R}, +, 0\rangle$; verificare che $\langle \mathbb{Q}_+, \cdot, 1\rangle <_{Mnd} \langle \mathbb{R}_+, \cdot, 1\rangle$.

Dal fatto che la composizione di due endofunzioni è ancora una endofunzione, si ha anche che il monoide delle endofunzioni relative a un certo insieme S, $\left\langle \lceil S \longmapsto S \rceil, \circ, \mathsf{Id}_S \right\rangle$ è sottomonoide del monoide delle relazioni su S, $\langle \mathfrak{P}(S \times S), \circ, \mathsf{Id}_S \rangle$.

Dal fatto che l'insieme delle biiezioni di un certo insieme S è chiuso rispetto alla composizione si deduce che $\left\langle \lceil S \lhd\!\!\longrightarrow\!\!\rhd S \rceil, \circ, \mathsf{Id}_S \right\rangle$ è sottomonoide del monoide delle endofunzioni di S.

Se k è un intero maggiore di 1, per il monoide delle parole aventi lunghezza multiplo di k si ricava che $\langle (A^k)^*, \cdot, \sqcup \rangle <_{Mnd} \langle A^*, \cdot, \sqcup \rangle$.

T15 f.08 Si dice **sottogruppo** di un gruppo $\langle G, \odot, ^{-1}, e \rangle$ ogni suo sottomonoide che contiene l'inverso di ogni suo elemento. In altri termini un sottogruppo H del gruppo $\langle G, \odot, ^{-1}, e \rangle$ è un sottoinsieme di G chiuso rispetto alle operazioni $\odot$ e $^{-1}$ ed e.
Essere chiuso rispetto a un'operazione unaria come $^{-1}$ corrisponde all'essere invariante rispetto al passaggio all'inverso; questo fatto, servendosi della estensione booleana della funzione $^{-1}$, ai sottoinsiemi di G, estensione che denotiamo con lo stesso $^{-1}$, si esprime efficacemente scrivendo $H^{-1} \subseteq H$.
Essere chiuso rispetto a una operazione nullaria come e significa contenere tale elemento, $e \in G$.
Da $H \odot H^{-1} = H$ discendono $e \in H{-}1$ e quindi $e \in H$ e $H^{-1} \supseteq H$; ma, essendo $|H| = |H^{-1}|$, deve essere $H^{-1} = H$.

T15 f.09 In generale per ogni struttura algebrica monoterreno si dice **sottostruttura** di una struttura S di qualche genere che abbia come terreno un sottoinsieme del terreno di S e questo sia chiuso rispetto a tutte le operazioni che caratterizzano la S.

Un modo di procedere per individuare sottostrutture di una struttura monoterreno $\boldsymbol{M} = \langle M, ... \rangle$ consiste nel considerare un sottoinsieme $H \subset M$ e nel procedere ad ampliarlo aggiungendogli le operazioni nullarie eventualmente non appartenenti ad H e i risultati delle operazioni unarie e binarie su operandi facenti parte di H e dei suoi successivi ampliamenti. Se si riesce a individuare l'ampliamento di H per il quale non sono possibili ulteriori ampliamenti, si ottiene un sottoinsieme di M che evidentemente è chiuso rispetto alle operazioni della specie di struttura e quindi è una sottostruttura di $\boldsymbol{M}$.

Bisogna osservare che queste considerazioni conducono a un procedimento costruttivo solo quando le manovre individuate si sanno effettuare concretamente e questo dipende dalle caratteristiche costruttive della struttura $\boldsymbol{M}$ e del sottoinsieme H.

T15 f.10 La precedente costruzione di ampliamento di un generico sottoinsieme K dell'insieme G terreno di una struttura algebrica che fornisce una sottostruttura che denotiamo con $\overline{K}$, viene detta **chiusura algebrica** di K in G.
Si tratta di una costruzione molto generale a causa dell'arbitrarietà della specie di struttura, della struttura G e del sottoinsieme K.

Qui abbiamo definita la chiusura algebrica solo per le strutture monoterreno, ma questa nozione si può introdurre proficuamente anche per altre strutture algebriche.
Inoltre essa costituisce un caso particolare della nozione generale di funzione di chiusura, funzione di insieme che risulta ampliante, isotona e idempotente come vedremo più compiutamente in B54d .

Dalle considerazioni generali sulle funzioni di chiusura, segue che la trasformazione da K a $\overline{K}$ porta anche alla intersezione di tutte le sottostrutture contenenti K, ovvero alla più ristretta, in senso insiemistico, delle sottostrutture contenenti K.
Vedremo anche che essa ha come terreno il minimo nel reticolo dei sottoinsiemi di G dei sovrainsiemi di K.

T15 g. morfismi di strutture

T15 g.01 Nel seguito chiameremo **strutture omogenee** due o più strutture della stessa specie.

Introduciamo ora delle classi di funzioni tra due strutture omogenee monoterreno che denotiamo con $\boldsymbol{S}_j = \langle S_j, \odot_{j,1}, ..., \mathcal{I}_{j,1}, ..., \nu_{j,1}, ... \rangle$ per $j = 1, 2$, dove ogni $\odot_{j,h}$ individua un'operazione binaria, ogni $\mathcal{I}_{j,h}$ un'operazione unaria e ogni $\nu_{j,h}$ un'operazione nullaria.
Lasciamo aperta la possibilità che S_2 sia un sottoinsieme di S_1 e anche che coincida con esso.
Consideriamo anche una funzione $\varphi \in \lceil S_1 \longmapsto S_2 \rceil$;

Si dice che φ sia una **funzione che rispetta una operazione binaria** $\odot_{1,h}$ sse $\forall a, b \in S_1 \ : \ \varphi(a \odot_{1,h} b) = \varphi(a) \odot_{2,h} \varphi(b)$.

Si dice che φ sia una **funzione che rispetta una operazione unaria** $\mathcal{I}_{1,h}$ sse
$\forall a \in S_1 \ : \ \varphi\left(\mathcal{I}_{1,h}(a)\right) \ = \ \mathcal{I}_{2,h}\big(\varphi(a)\big)$;
si dice che φ sia una **funzione che rispetta una operazione nullaria** $\nu_{1,h}$ sse $\varphi(\nu_{1,h}) = \nu_{2,h}$.

Una funzione come la precedente φ si dice **morfismo di $\boldsymbol{S}_1$ in $\boldsymbol{S}_2$** sse rispetta tutte le operazioni di $\boldsymbol{S}_1$ trasformandole nelle omologhe della $\boldsymbol{S}_2$.

In particolare si dice **epimorfismo di $\boldsymbol{S}_1$ su $\boldsymbol{S}_2$** un morfismo che sia una applicazione suriettiva di S_1 su S_2.
Si dice **endomorfismo** un morfismo di una struttura sopra un suo sottoinsieme, proprio o meno.
Si dice **isomorfismo di $\boldsymbol{S}_1$ ed $\boldsymbol{S}_2$** un morfismo tra S_1 ed S_2 che sia una applicazione biiettiva .
Si dice **automorfismo** di $\boldsymbol{S}_1$ un isomorfismo che costituisce una permutazione di S_1, cioè un morfismo entro S_1 che che sia endomorfismo ed automorfismo.

Talora invece che di rispetto delle operazioni da parte di un morfismo tra $\boldsymbol{S}_1$ e $\boldsymbol{S}_2$ si dice che tale trasformazione effettua un *trasporto* delle operazioni di una struttura ad un'altra.

T15 g.02 È semplice vedere che il codominio $\varphi(S_1)$ di un morfismo φ di $\boldsymbol{S}_1$ in $\boldsymbol{S}_2$ conduce a una sottostruttura di $\boldsymbol{S}_2$. Infatti tale insieme munito delle riduzioni delle operazioni che caratterizzano S_2 costituisce una struttura omogenea a $\boldsymbol{S}_1$ chiusa rispetto a tali operazioni e tutte le uguaglianze che esprimono le proprietà della specie alla quale $\boldsymbol{S}_1$ ed $\boldsymbol{S}_2$ appartengono sono trasportate da $\boldsymbol{S}_1$ in $\boldsymbol{S}_2$.

T15 g.03 L'insieme degli isomorfismi tra due strutture $\boldsymbol{S}_1$ e $\boldsymbol{S}_2$ facenti parte della specie **Xyz** viene individuato dalla scrittura $\lceil \boldsymbol{S}_1 \lhd\!\!\longmapsto\!\!\rhd_{\mathbf{Xyz}} \boldsymbol{S}_2 \rceil$

T15 h. semianelli e matrici

T15 h.01 Nelle maggior parte delle attività matematiche ed elaborative, a partire dalle più elementari riguardanti insiemi espliciti e numeri naturali, si rivela necessario disporre di almeno due operazioni binarie ben distinte.
Questo è evidente, ad esempio, per le attività computazionali riguardanti numeri interi (o numeri razionali o reali costruibili) per le quali servono la somma e il prodotto e per le operazioni su insiemi le quali si servono di unione e intersezione.

In questo paragrafo introdurremo le più generali coppie di operazioni che caratterizzano varie specie di strutture algebriche monoterreno.

T15 h.02 Si dice **semianello** una struttura della forma $\boldsymbol{R} = \langle R, \oplus, \odot \rangle$, dove:
– $\langle R, \oplus, \mathbf{0} \rangle$ è un semigruppo commutativo,
– $\langle R, \odot \rangle$ è un semigruppo.
– l'operazione $\odot$ è distributiva rispetto alla $\oplus$, cioè:

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

Qui come al solito R si dice terreno della struttura e spesso l'operazione $\oplus$ è detta somma e la $\odot$ è chiamata prodotto.

Diciamo invece **semianello unifero** una struttura della forma $\left\langle R, \oplus, \mathbf{0}, \odot \right\rangle$, dove:
$\langle R, \oplus, \mathbf{0} \rangle$ è un monoide commutativo,
$\langle R, \odot \rangle$ è un semigruppo.
Spesso $\mathbf{0}$, elemento assorbente della operazione $\oplus$, viene chiamato zero della struttura $\boldsymbol{R}$.
Segnalamo anche che spesso, invece di semianello unifero si usa il termine "semianello unitale".

Denotiamo con **Srng** la classe dei semianelli e con **Srngu** la classe dei semianelli uniferi.

Evidentemente si tratta di due specie di strutture strettamente collegate e servendosi dell'operatore dimenticanza [B41a05 B41c03] possiamo affermare $\left|\!\left|\!\left| \boldsymbol{Frgt}_3(\mathsf{Srngu}) = \mathsf{Srng} \right|\!\right|\!\right|$.
È anche evidente che tra i semianelli si distinguono quelli che possono essere dotati di uno zero, che deve essere unico, e possono condurre ad un anello unifero, dai rimamenti.

T15 h.03 Una distinzione rilevante tra i semianelli e i semianelli uniferi riguarda la commmutatività dell'opperazione prodotto. Se vale questa proprietà si parla di semianelli [uniferi] abeliani , se no di semianelli [uniferi] nonabeliani.
Conseguentemente si distinguono le classi delle strutture abeliane **SrngAb** e **SrnguAb**, dalla classi delle strutture nonabeliane **SrngNab** e **SrnguNab**.

Dopo il caso del **semianello banale** formato da un solo elemento, il più ridotto semianello è il cosiddetto **semianello binario** o **semianello dei bits**, $\left\langle \mathbb{B}, +_2, \cdot \right\rangle$, dove $\mathbb{B}$ è l'insieme dei numeri binari o bits $\{0, 1\}$ e $+_2$ è la somma booleana.

Si individuano vari semianelli numerici munendo delle ordinarie operazioni di somma e prodotto insiemi come $\mathbb{P}$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}_{\mathsf{a}}$, $\mathbb{R}_{\mathsf{c}}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}_+$, $\mathbb{Q}_{0+}$, $\mathbb{R}_+$, $\mathbb{R}_{0+}$, ...

Altri importanti semianelli commutativi sono costituiti, per qualsiasi m intero maggiore o uguale a 2, dalla classe di resti modulo m $\mathbb{Z}_m$ munita delle operazioni somma modulo m $+_m$, prodotto modulo m $\cdot_m$ e dello zero $[0]_m = m\mathbb{Z}$ [B25].

Ad ogni insieme S si associa il **semianello booleano** $\langle \mathfrak{P}(S), \cup, \emptyset, \cap \rangle$.

È utile osservare che questo semianello si può vedere come prodotto diretto della famiglia dei semianelli binari indicizzata dagli elementi di S.

Altri semianelli con interessanti applicazioni sono i semianelli dei linguaggi formali su dati alfabeti finiti A; il terreno di un tale semianello è l'insieme $\mathfrak{P}(\mathsf{A}^*)$, la somma è l'unione dei linguaggi e il prodotto la loro giustapposizione [C10].

Vanno segnalati anche i semianelli delle relazioni entro un dato insieme E; il terreno di una tale semianello è l'insieme $\mathfrak{P}(E \times E)) = \mathbf{Rel}_E$ [B08b08], la somma è l'unione delle relazioni e il prodotto la loro composizione, cioè il prodotto di Peirce tra relazioni.

In questa ampia collezione si collocano anche i semianelli delle relazioni tra linguaggi: il ruolo di zero di questi semianelli è svolto dalla coppia di linguaggi vuoti e il prodotto dalla giustapposizione componente per componente tra le coppie di linguaggi.

Tra i semianelli precedenti sono noncommutativi solo i semianelli delle relazioni su un insieme e in particolare delle relazioni tra linguaggi formali su un alfabeto di almeno due lettere.

T15 h.04 Si dice **semianello unifero** una struttura della forma $\langle R, \oplus, \mathbf{0}, \odot, \mathbf{1} \rangle$ che costituisce un arricchimento di un semianello $\langle R, \oplus, \mathbf{0}, \odot \rangle$ con il terreno R contenente almeno due elementi, $\mathbf{0}$ elemento neutro per $\oplus$ e $\mathbf{1}$ elemento neutro bilatero per l'operazione $\odot$, cioè tali che

$$\forall a \in R \ : \ a \odot \mathbf{0} = \mathbf{0} \odot a = \mathbf{0}$$

e $\mathbf{1}$ elemento neutro per $\odot$.
L'elemento $\mathbf{0}$ viene detto **zero** e l'elemento $\mathbf{1}$ viene chiamato **unità** del semianello unifero.

Per ogni insieme S contenente almeno due elementi dal semianello booleano $\langle \mathfrak{P}(S), \cup, \emptyset, \cap \rangle$ si può ricavare il più ricco semianello unifero $\langle \mathfrak{P}(S), \cup, \emptyset, \cap, S \rangle$.

I precedenti semianelli numerici per i quali il terreno contiene l'elemento 0 si possono arricchire aggiungendo tale oggetto alle loro componenti e diventare semianelli uniferi.

I semianelli dei linguaggi, quelli delle relazioni ed i semianelli delle relazioni tra linguaggi diventano uniferi quando si arricchiscono, risp., con l'elemento neutro $\{ \sqcup \}$, con la relazione identità Id_E e con la coppia di linguaggi $\langle \{ \sqcup \}, \{ \sqcup \} \rangle$.

Conviene segnalare che i semianelli dei linguaggi e i semianelli delle relazioni sono studiati nell'ambito delle algebre di Kleene [C32].

T15 h.05 Denotiamo con **Srng** la classe dei semianelli, con **Srngu** quella dei semianelli uniferi, con **SrngAb** la classe dei semianelli commutativi e con **SrnguAb** la classe dei semianelli uniferi abeliani.

Un sottoinsieme S del terreno di un semianello si dice **terreno di sottosemianello**, o sbrigativamente **sottosemianello**, sse è chiuso rispetto alle operazioni di somma e prodotto e contiene l'elemento $\mathbf{0}$.

Un sottoinsieme S del terreno di un semianello unifero si dice **terreno di sottosemianello unifero** sse è chiuso rispetto alle operazioni di somma e prodotto e contiene zero e unità.
In molti contesti si può semplificare il suddetto termine in "sottosemianello unifero" senza rischi di ambiguità.

T15 h.06 Le matrici le cui entrate sono elementi di un semianello presentano un interesse algebrico e computazionale che è opportuno evidenziare.

Consideriamo gli interi positivi d, e, f e g, un semianello $\boldsymbol{R} = \langle R, \oplus, 0, \odot \rangle$ e le matrici (di estensioni finite) le cui linee per semplicità etichettiamo con intervalli di interi come **(**d **]** $= \{1, ..., d\}$, **(**e **]**, **(**f **]** o **(**g**]**.

Denotiamo con $\mathbf{Mat}_{d,e}(\boldsymbol{R})$ l'insieme delle matrici di profilo $d \times e$ sul semianello $\boldsymbol{R}$.

Focalizziamo l'attenzione su due matrici dello stesso profilo:

$$A = [i \in (\mathrm{d}\,], j \in (\mathrm{e}\,] :| \; a_{i,j}] \quad \text{e} \quad B = [i \in (\mathrm{d}\,], j \in (\mathrm{e}\,] :| \; b_{i,j}] \in \mathbf{Mat}_{d,e}(\boldsymbol{R}) \ .$$

Si definisce **somma di matrici**

$$A \oplus^{me} B \ := \ \big[i \in (\mathrm{d}\,], j \in (\mathrm{e}\,] :| \; a_{i,j} \oplus b_{i,j}\big] \ .$$

L'operazione matriciale $\oplus^{me}$ si può chiamare **estensione matriciale dell'operazione somma** $\oplus$; la trasformazione di $\oplus$ nella $\oplus^{me}$ si può vedere come caso particolare di estensione funzionale o di estensione cartesiana. Essa può descriversi come una somma componente per componente sulla potenza cartesiana $d \cdot e$-esima del monoide abeliano $\langle R, \oplus, 0\rangle$.

In genere la notazione $\oplus^{me}$ si semplifica nella $\oplus$, confidando che il significato di questa scrittura possa essere imposto dal contesto in modo che la semplificazione non porti ad ambiguità.

Osserviamo anche che $\big\langle \mathbf{Mat}_{d,e}(\boldsymbol{R}), \oplus^{me}, \mathbf{0}_{d,e}\big\rangle$ è un monoide abeliano.

T15 h.07 Si dice **coppia di matrici conformabili** o anche coppia di matrici moltiplicabili sul semianello $\boldsymbol{R}$ una coppia di matrici tale che le colonne della prima e le righe della seconda sono indicizzate dallo stesso insieme di indici, in particolare dallo stesso intervallo di numeri interi.

Consideriamo una tale coppia

$$\langle A, B\rangle \ \in \ \mathbf{Mat}_{d,e}(\boldsymbol{R}) \times \mathbf{Mat}_{e,f}(\boldsymbol{R}) \ .$$

Si definisce come **prodotto [righe per colonne]** delle due matrici A per B

$$A \odot_{\oplus} B \ := \ [i \in (\mathrm{d}\,], k \in (\mathrm{f}\,] :| \; a_{i,1} \odot b_{1,k} \oplus \ldots \oplus a_{i,d} \odot b_{d,k}] \ .$$

Si dimostra facilmente che questo prodotto di matrici è associativo e che si ha la distributività a sinistra e a destra di questo prodotto rispetto alla somma:

$$\forall A \in \mathbf{Mat}_{d,e}, B \in \mathbf{Mat}_{e,f}, C \in \mathbf{Mat}_{f,g} \ : \ A \odot_{\oplus} (B \odot_{\oplus} C) = (A \odot_{\oplus} B) \odot_{\oplus} C \ ,$$

$$\forall A, B \in \mathbf{Mat}_{d,e}, \ C \in \mathbf{Mat}_{e,f} \ : \ (A \oplus^{me} B) \odot_{\oplus} C \ = \ (A \odot_{\oplus} C) \oplus^{me} (B \odot_{\oplus} C) \ ,$$

$$\forall A \in \mathbf{Mat}_{d,e}, \ B, C \in \mathbf{Mat}_{e,f} \ : \ A \odot_{\oplus} (B \oplus^{me} C) \ = \ (A \odot_{\oplus} B) \oplus^{me} (A \odot_{\oplus} C) \ .$$

La nozione di matrice su semianelli generalizza la nozione classica di matrice a componenti numeriche e, come vedremo, rende canonico e in pratica più agevole organizzare calcoli su matrici costituite da elementi non del tutto tradizionali come bits, insiemi, linguaggi formali, elementi di algebre di Kleene, funzioni, matrici e altri candidati ad essere elementi di semianelli.

Può essere utile ricordare il significato e l'utilità del prodotto di matrici sul fondamentale semianello binario [B16c].

T15 h.08 Consideriamo la collezione delle matrici sul semianello $\boldsymbol{R}$ quadrate e più precisamente di profilo $d \times d$ che denotiamo, oltre che con $\mathbf{Mat}_{d,d}(\boldsymbol{R})$, con la più semplice scrittura $\mathbf{Mat}_{d}(\boldsymbol{R})$.

Munendo questo insieme della somma e del prodotto tra matrici sopra definiti si ottiene un semianello. Questo è detto **semianello delle matrici quadrate** $d \times d$ sul semianello $\boldsymbol{R}$.

Conviene osservare che il prodotto di matrici $d \times d$ con $d > 1$, anche se definite su un semianello commutativo, non è commutativo. Per esempio si hanno le seguenti differenze per matrici booleane 2×2:

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

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

T15 h.09 Consideriamo un semianello unifero $\boldsymbol{R} = \langle R, \oplus, \mathbf{0}, \odot, \mathbf{1} \rangle$ la collezione delle matrici $\mathsf{Mat}_d(R)$ e tra queste la **matrice zero** $\mathsf{matZr}(d; \boldsymbol{R}) := [i, j \in (\mathrm{d}\ ] :| \mathbf{0}]$ e la **matrice unità** $\mathsf{matId}(d; \boldsymbol{R}) := \big[i, j \in (\mathrm{d}\ ] :| \delta_{\boldsymbol{R}}(i, j)\big]$; qui si è utilizzata la funzione **delta di Kronecker sul semianello unifero** $\boldsymbol{R}$ definita da

$$\delta_{\boldsymbol{R}}(i, j) := \begin{cases} \mathbf{0} & \text{sse } i \neq j, \\ \mathbf{1} & \text{sse } i = j\ . \end{cases}$$

Si dice **semianello unifero delle matrici quadrate** su $\boldsymbol{R}$

$$\mathsf{Mat}(d; \boldsymbol{R})_{Sringu} := \big\langle \mathsf{Mat}_d(R), \oplus^{me}, \mathsf{matZr}_d(\boldsymbol{R}), \odot^{me}, \mathsf{matId}(d; \boldsymbol{R}) \big\rangle\ .$$

Si dimostra senza difficoltà che questa struttura costituisce effettivamente un semianello unifero.

T15 h.10 Sulle matrici dei vari generi è definita un'importante involuzione, la trasposizione:

$$\lceil M \in \mathsf{Mat}_d \mapsto M^{\mathsf{T}} \rceil\ .$$

È utile considerare i rapporti tra la trasposizione e le operazioni di somma e prodotto tra matrici su semianelli.

(1) Eserc. Dimostrare che la trasposta di una somma di matrici è la somma delle trasposte:

$$(A \oplus^{me} B)^{\mathsf{T}} = A^{\mathsf{T}} \oplus^{me} B^{\mathsf{T}}\ .$$

(2) Eserc. Dimostrare che se due matrici A e B sono conformabili lo è anche la matrice $B^{\mathsf{T}} \odot A^{\mathsf{T}}$.

(3) Eserc. Dimostrare che la trasposta di un prodotto di due matrici conformabili A e B è il prodotto dei fattori trasposti considerati nell'ordine opposto: $(A\ odotB)^{\mathsf{T}} = B^{\mathsf{T}} \odot A^{\mathsf{T}}$.

Per il semianello delle matrici quadrate questa proprietà si presenta anche dicendo che la trasposizione costituisce un **antimorfismo del semianello** suddetto.

T15 h.11 Qui può essere utile segnalare che si possono introdurre utili matrici anche servendosi di una struttura più debole del semianello che chiamiamo **quasisemigruppo**, struttura avente la forma $\langle R, \oplus, \mathbf{0}, \odot \rangle$, dove $\langle R, \oplus, \mathbf{0} \rangle$ è un monoide e $\langle R, \odot \rangle$ è un semigruppo;

Eserc. Verificare che, se S è un qualsiasi insieme, le matrici

$$\begin{bmatrix} \emptyset & \emptyset \\ \emptyset & \emptyset \end{bmatrix} \qquad \text{e} \qquad \begin{bmatrix} S & \emptyset \\ \emptyset & S \end{bmatrix}$$

sono le matrici zero e unità del semianello unifero delle matrici 2×2 sul semianello unifero booleano $\langle \mathfrak{P}(S), \cup, \emptyset, \cap, S \rangle$.

T15 i. anelli e strutture collegate

T15 i.01 I semianelli e i semianelli uniferi si possono arricchire richiedendo che contengano elementi con proprietà ben determinate in modo da costituire strutture più stringenti spesso definite in seguito a esigenze espresse da applicazioni.

Quando si chiede la presenza di un elemento zero che, oltre ad essere elemento neutro per l'operazione commutativa somma, sia assorbente per l'operazione prodotto si ottiene una struttura che chiamiamo pseudoanello.
Chiedendo anche la presenza di un elemento diverso dal precedente neutro per il prodotto abbiamo una struttura che chiamiamo anello.
Per questa scelta di termini seguiamo la terminologia del trattato di Bourbaki ; altri autori preferiscono usare il termine anello invece di pseudoanello e il termine di anello unifero invece di anello.

Diciamo dunque **pseudoanello** una struttura $\boldsymbol{P} = \langle R, \oplus, \ominus, \mathbf{0}, \odot \rangle$ nella quale $\boldsymbol{P}_{mg} := \langle R, \oplus, \ominus, \mathbf{0} \rangle$ è un gruppo abeliano chiamato **gruppo moltiplicativo del pseudoanello** e $\langle R, \oplus, \odot \rangle$ è un semianello.
Prevedibilmente uno pseudoanello si dice **pseudoanello abeliano** o anche **pseudoanello commutativo**, sse è commutativo il suo prodotto.

Quando il prodotto di uno pseudoanello possiede unità $\mathbf{1}$, cioè quando la terna $\langle \boldsymbol{R}, \odot, \mathbf{1} \rangle$ costituisce un monoide, risulta utile considerare il corrispondente arricchimento della struttura precedente chiamato **anello**, struttura della forma $\langle R, \oplus, \ominus, \mathbf{0}, \odot, \mathbf{1} \rangle$.

Un anello si dice **anello abeliano** o anche anello commutativo, sse è abeliano il suo pseudoanello sottostante.

Denotiamo la classe degli pseudoanelli con **Psrng**, la classe degli pseudoanelli abeliani con **PsrngAb**, la classe degli anelli con **Rng** e la classe degli anelli abeliani con **RngAb**.

Osserviamo che ogni anello è costituito da almeno due elementi.

T15 i.02 Gran parte dei semianelli visti in precedenza si possono promuovere a pseudoanelli e gran parte dei semianelli uniferi visti in precedenza si possono arricchire per diventare anelli. Gli pseudoanelli privi di unità si rivelano meno importanti degli anelli.

Un esempio fondamentale di anello commutativo è dato dall'insieme degli interi munito delle usuali operazioni di somma, differenza e prodotto, $\langle \mathbb{Z}, +, -, 0, \cdot, 1 \rangle$.
Altri anelli commutativi sono ricavati similmente da $\mathbb{Q}$, $\mathbb{R}_{\mathsf{a}}$, $\mathbb{R}_{\mathsf{c}}$, $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{Z} \times \mathbb{Z}$ munito del prodotto complesso.

Ulteriori importanti anelli commutativi sono costituiti, per un qualsiasi intero $m \geq 2$, dalle classi di resti modulo m $\mathbb{Z}_m$.

Per ogni intero $m = 2, 3, \ldots$ $\langle m\,\mathbb{Z}, +, -, 0, \cdot \rangle$ è uno pseudoanello abeliano che non può essere dotato di una unità.

T15 i.03 Un sottoinsieme S del terreno R di uno pseudoanello $\boldsymbol{R}$ si dice **terreno di un sottopseudoanello** di $\boldsymbol{R}$ sse è chiuso rispetto alle operazioni di somma e prodotto, cioè sse $\forall a, b \in S \;:\; a+b \in S, a \cdot b \in S$.
In questo caso scriviamo $S \leq_{Psrng} R$.

Si parla più precisamente di **sottoanello** nel caso di sottoinsieme del terreno di un anello che, oltre a essere chiuso rispetto a somma e prodotto, contenga l'elemento unità.

In questo caso scriviamo $S \leq_{Rng} R$.

T15 i.04 **(1) Eserc.** Dimostrare che per $m, k = 2, 3, ...$ si ha $m \cdot k \cdot \mathbb{Z} <_{Psrng} m \cdot \mathbb{Z} <_{Rng} \mathbb{Z}$.
(2) Eserc. Dimostrare che $\mathbb{Z} <_{Rng} \mathbb{Q} <_{Rng} \mathbb{R}_{\mathsf{a}} <_{Rng} \mathbb{R}_{\mathsf{c}} <_{Rng} \mathbb{R} <_{Rng} \mathbb{C}$.

T15 i.05 Le matrici quadrate di ordine finito le cui componenti sono elementi di un anello costituiscono anelli di rilevante importanza.

A partire da un anello $\boldsymbol{R} = \langle R, \oplus, \ominus, \mathbf{0}, \odot, \mathbf{1} \rangle$ per ogni intero positivo d si può prendere in considerazione l'insieme di matrici

$$\mathsf{Mat}(d; \boldsymbol{R}) \ := \langle \mathsf{Mat}_d(R), \oplus, \ominus, \mathsf{matZr}_d(\boldsymbol{R}), \odot_{\mathsf{M}}, \mathsf{matId}(d; \boldsymbol{R}) \rangle$$

e constatare che si tratta di un anello.
Infatti $\mathsf{Mat}_d(\boldsymbol{R})$ è l'arricchimento di un semianello di matrici, la **matrice opposta** di una data A, cioè la sua inversa rispetto alla somma $\oplus$, 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 quadrata di ordine d $MatCnst_d(\mathbf{0})$ avente tutte le componenti uguali all'elemento neutro $\mathbf{0}$ di $\boldsymbol{R}$.

T15 i.06 Come si è osservato per i semianelli, gli anelli di matrici di ordine maggiore di 1 sono noncommutativi anche se costruiti a partire da un anello commutativo; per i controesempi alla commutatività di $\mathsf{Mat}_d(\boldsymbol{R})$ basta trovarne tra le matrici di ordine 2 con componenti intere. Per esempio

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

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

T15 i.07 Come per ogni monoide, anche per ogni anello, che denotiamo con $\boldsymbol{R} = \langle R, \oplus, \ominus, \mathbf{0}, \odot, \mathbf{1} \rangle$, rivestono grande importanza gli **elementi invertibili**, cioè gli elementi invertibili per il sottostante monoide $\langle R, \odot, \mathbf{1} \rangle$ che sappiamo formare un gruppo che si chiama **gruppo moltiplicativo** dell'anello $\boldsymbol{R}$ e per il quale scriviamo

$$\boldsymbol{R}_{mg} \ := \ \mathsf{Invelm}(\boldsymbol{R}) \ := \langle R, \odot, inv(\odot), \mathbf{1} \rangle \ .$$

Ad ogni anello $\boldsymbol{R}$, come ad ogni pseudoanello, si associa un altro gruppo, il **gruppo additivo** $\boldsymbol{R}_{ag} \ := \langle R, \oplus, \ominus, \mathbf{0} \rangle$.

T15 i.08 Per uno pseudoanello $\langle R, +, -, 0, \cdot \rangle$ può accadere che presi due elementi $r, s \in R$, diversi dallo zero, il loro prodotto $r \cdot s$ sia uguale allo stesso elemento zero.
Tali elementi si dicono **divisori dello zero**; più precisamente se lo pseudoanello non è abeliano r si dice divisore a sinistra dello 0 ed s divisore a destra.

Consideriamo ad esempio lo pseudoanello $\langle \mathbb{Z}_6, +_6, -_6, 0, \cdot_6, 1 \rangle$; in esso $2 \cdot_6 3 = 0$, cioè 2 e 3 sono divisori dello zero.
Più in generale in ogni pseudoanello $\mathbb{Z}_m$ con m intero naturale maggiore di 1 e non primo, ossia fattorizzabile, si trovano divisori dello zero; infatti se si può scrivere $m = r \cdot s$ con $r, s \neq 0, 1$, si ha $[r]_m \cdot_m [s]_m = [0]_m = [m]_m$.

T15 i.09 **Eserc.** Dimostrare che nell'anello $\mathbb{Z}_m$ l'insieme dei divisori dello zero coincide con l'insieme degli interi in $\{2, ..., m-1\}$ non primi con m, cioè dotati di un divisore comune con m.

Concludere che per ogni numero primo p l'anello $\mathbb{Z}_{p\,Rng}$ è privo di divisori dello zero.

T15 i.10 Si trovano molte coppie di matrici 2×2 sui reali che costituiscono divisori dello zero $\mathbf{0}_{2,2}$: in particolare:

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

Si dice **dominio di integrità** ogni anello commutativo privo di divisori dello zero.

T15 i.11 Come per un magma abeliano $\langle R, \cdot \rangle$, per uno pseudoanello abeliano $\langle R, +, -, 0, \cdot \rangle$ si dice che vale la **legge di cancellazione** sse

$$\forall x, y \in R \ , \ r \in R \setminus \{0\} \ : \ r \cdot x = r \cdot y \Longrightarrow x = y \ .$$

Vi sono pseudoanelli abeliani nei quali la legge di cancellazione non vale.
Per esempio in $\mathbb{Z}_4$ abbiamo

$$2 \cdot_4 3 = 2 \cdot_4 1 = 2 \implies 3 = 1 \ .$$

(1) Prop.: Sia $\boldsymbol{R}$ un anello abeliano.

$$\boldsymbol{R} \text{ è un dominio di integrità} \iff \text{per } \boldsymbol{R} \text{ vale la legge di cancellazione} \ .$$

Dim.: "$\Longrightarrow$": se $\boldsymbol{R}$ è un dominio di integrità si ha:

$$r \neq 0 \wedge r \cdot x = r \cdot y \implies r \cdot (x - y) = 0 \implies x - y = 0 \implies x = y \ .$$

"$\Longleftarrow$": se in $\boldsymbol{R}$ vale la legge di cancellazione ed $r \cdot s = 0$, se $r \neq 0$, $r \cdot 0 = 0 = r \cdot s$ e quindi $s = 0$, mentre se $s \neq 0$, $0 \cdot s = 0 = r \cdot s$ e quindi $r = 0$ ∎

La legge di cancellazione apre la possibilità di numerose utili elaborazioni; i domini di integrità sono quindi da considerare come anelli che costituiscono ambienti elaborativi particolarmente efficaci.

T15 i.12 Come per un magma dotato di un elemento assorbente o zero 0, un elemento q diverso dallo zero di uno pseudoanello $\boldsymbol{R}$ viene chiamato **elemento nilpotente** sse si trova un intero positivo h tale che la sua potenza q^h è uguale allo zero della struttura. Il più piccolo di tali h viene detto **grado di nilpotenza** dell'elemento q.

Come per un magma unifero o per un monoide, un elemento q diverso dall'unità di un anello $\boldsymbol{R}$ per il quale esiste un intero positivo h tale che $q^h = \mathbf{1}$ si dice **elemento periodico**; se h è il più piccolo intero positivo per cui questo si verifica, si dice che q ha **periodo di elemento** h (talora si dice invece che q ha ordine h).

L'unità ha sempre periodo 1, lo zero non è mai periodico.
In $\mathbb{Z}_5$ 2 e 3 hanno periodo 4, 4 ha periodo 2.
In $\mathbb{Z}_6$ 5 ha periodo 2, mentre 2, 3 e 4 non sono periodici.
In $\mathbb{Z}_7$ 2 ha periodo 3, 3 ha periodo 5, 4 ha periodo 3, 5 ha periodo 6, 6 ha periodo 2.

T15 i.13 Si dice **corpo** un anello $\boldsymbol{R}$ in cui gli elementi diversi dallo zero formano gruppo rispetto all'operazione prodotto.
Denotiamo con **Krp** la classe dei corpi. Formalmente:

$$\mathbf{Krp} \ := \ \left\{ \langle R, \oplus, \ominus, \mathbf{0}, \odot, \mathbf{1} \rangle \in \mathbf{Rng} \quad \text{tale che} \quad \langle R \setminus 0, \odot, inv(\odot), \mathbf{1} \rangle \in \mathbf{Grp} \right\}$$

$$\boldsymbol{R} = \langle R, \oplus, \ominus, \mathbf{0}, \odot, \mathbf{1} \rangle \in \mathbf{Rng} \wedge \langle R \setminus 0, \odot, inv(\odot), \mathbf{1} \rangle \in \mathbf{Grp} \text{ '} \implies \quad \boldsymbol{R} \in \mathbf{Krp} \ .$$

Perché la definizione abbia senso un corpo deve presentare almeno due elementi distinti, lo zero e l'unità.

L'anello binario $\langle \mathbb{B}, +_2, 0, \cdot, 1 \rangle$, oltre a essere l'anello nonnullo meno esteso, è il corpo meno esteso.

L'insieme degli elementi del corpo $\boldsymbol{R}$ diversi dallo zero, prende il nome di **gruppo moltiplicativo del corpo** $\boldsymbol{R}$; in genere si denota localmente con $\boldsymbol{R}^{\times}$.

Un corpo in cui il prodotto sia commutativo viene detto **campo** o corpo commutativo.

Un corpo noncommutativo viene anche chiamato **corpo sghembo** (*skewfield*).

Denotiamo con **KrpNab** la classe dei corpi sghembi.

T15 i.14 Segnaliamo queste altre 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.

T15 j. ideali

T15 j.01 Per gli pseudoanelli e gli anelli, oltre ai sottopseudoanelli e e ai sottoanelli, si può definire un'altro importante genere di sottostrutture: gli ideali.

Si dice **ideale [bilatero] di un anello** $\boldsymbol{R} = \langle R, \oplus, \ominus, \mathbf{0}, \odot, \mathbf{1} \rangle$ un sottoinsieme $I \subseteq R$ che soddisfa queste condizioni:

[Idl 1] I è sottogruppo del gruppo additivo $\boldsymbol{R}_{ag}$, ossia $I + I \subseteq I$;

[Idl 2] $\forall a \in I\ ,\ \forall r \in R\ :\ a \cdot r \in I\ ,\ r \cdot a \in I$.

La stessa definizione si può applicare agli pseudoanelli.

La richiesta [Idl1] si può sostituire con la equivalente
[Idl 1'] I è chiuso rispetto alla sottrazione, cioè $\forall a, b \in I\ :\ a - b \in I$, ossia $I - I \subseteq I$.

L'ultima richiesta è più stringente della chiusura di un sottoinsieme rispetto al prodotto: quindi un qualunque ideale di un anello è un suo particolare sottoanello e un qualunque ideale di uno pseudoanello è un suo particolare sottoanello.

Sono ideali di uno pseudoanello $\boldsymbol{R} = \langle R, +, -, \mathbf{0}, \cdot \rangle$ i due sottoinsiemi di R l'uno costituito dal solo zero di R e l'altro coincidente con l'intero terreno; essi sono detti, risp., **ideale zero** e **ideale improprio** di $\boldsymbol{R}$. Ogni altro ideale, ammesso che esista, viene chiamato **ideale nonnullo proprio** di $\boldsymbol{R}$.

Denotiamo con $Idl(\boldsymbol{R})$ la collezione degli ideali dell'anello $\boldsymbol{R}$.

T15 j.02 Diamo qualche esempio di ideali.

Per l'anello degli interi naturali $\mathbb{N}$ sono ideali propri gli insiemi dei multipli $m \cdot \mathbb{N}$ per ogni intero $m = 2, 3, 4, ...$

Sia $p(x)$ un polinomio in $\boldsymbol{F}[x]$; L'insieme di tutti i multipli di $p(x)$, per il quale usiamo la notazione $\langle p(x) \rangle\ :=\ \{q(x)\, p(x)\ \ |:\ q(x) \in \boldsymbol{F}[x]\}$, è un ideale in $\boldsymbol{F}[x]$.

Per ogni pseudoanello o anello $\boldsymbol{R}$ e per ogni suo elemento a il sottoinsieme RaR è ideale (proprio o improprio).

T15 j.03 (1) Prop.: Ogni ideale I di uno pseudoanello o di un anello $\boldsymbol{R}$ contiene lo zero di questa struttura.

Dim.: Discende subito da [Idl 2] ∎

(2) Prop.: Per ogni anello dotato di ideali propri l'unità non appartiene ad alcuno di questi sottoinsiemi.

dim
Preso un qualsiasi ideale proprio I dell'anello $\boldsymbol{R}$ e un qualsiasi elemento $r \in R$ non contenuto in I, se $\mathbf{1}$ denota l'unità di $\boldsymbol{R}$, risulta $\mathbf{1} \cdot r = r \cdot \mathbf{1} = r$. Se $\mathbf{1}$ fosse un elemento di I si dedurrebbe, dalla definizione di ideale, che anche r apparterrebbe ad I, contro l'ipotesi ∎

(3) Prop.: Un corpo $\boldsymbol{K}$ non possiede alcun ideale proprio.

Dim.: Supponiamo per assurdo che $\boldsymbol{K}$ possegga un ideale proprio I e consideriamo un elemento $i \in I$ diverso dallo zero. Poiché $\boldsymbol{K}$ è un corpo, in $\boldsymbol{K}$ si trova il reciproco di i, i^{-1} e quindi anche $i^{-1} \cdot i = i \cdot i^{-1} = \mathbf{1}$, fatto in contrasto con la precedente proposizione ∎

T15 j.04 (1) Prop.: Consideriamo un anello $\boldsymbol{R}$, un suo sottoinsieme $S = \{s_1, ..., s_n\}$ e il sottoinsieme

$$\langle S \rangle \ := \bigcup_{\{s_1,...,s_n\} \subseteq S} \{r_1, ..., r_n \in R :|\ r_1 s_1 + \cdots + r_n s_n\}\ .$$

Questo costituisce un ideale in $\boldsymbol{R}$ ed è il più piccolo ideale di $\boldsymbol{R}$ che contiene S.

Dim.: Dato che l'anello contiene zero e unità, deve essere $\langle S \rangle \supseteq S$; inoltre dalla sua espressione si ricava facilmente che soddisfa le richieste [Idl 1] e [Idl 2]. ∎

L'ideale $\langle S \rangle$ è chiamato **ideale generato** da S

Sono particolarmente interessanti gli ideali generati da un singoletto, cioè da un solo elemento dell'anello diverso dallo zero e dall'unità; gli ideali dell'anello $\boldsymbol{R}$ hanno la forma $\langle s \rangle_R = \{r \in R :|\ r \cdot s\}$ per qualche elemento $s \in R \setminus \{\mathbf{0}, \mathbf{1}\}$; un tale ideale è chiamato **ideale principale dell'anello $\boldsymbol{R}$**.

T15 j.05 (1) Prop.: L'intersezione di due ideali I_1 e I_2 di un $\boldsymbol{R}$ pseudoanello o anello è anch'essa un ideale di tale struttura.

Dim.: La richiesta [Idl1] è soddisfatta in quanto anche l'intersezione di due sottogruppi è sottogruppo. Equivalentemente per la richiesta [Idl1'] basta osservare che $a, b \in I_1 \cap I_2 \implies a - b \in I_1\ ,\ a - b \in I_2$. Considerazione analoga per la [Idl2] ∎

La precedente dimostrazione si generalizza senza difficoltà alle intersezioni di famiglie di ideali.

(2) Prop.: Consideriamo una famiglia di ideali del pseudoanello $\boldsymbol{R}$ relativa all'insieme di indici $J \searrow \{I_j\ |:\ j \in J\}$; anche l'intersezione di tale famiglia di ideali $\bigcap\{j \in J\ :|\ I_j\}$ è un ideale di $\boldsymbol{R}$ ∎

(3) Prop.: Sia $I_1 \subset I_2 \subset ...$ è una successione ascendente di ideali di un pseudoanello $\boldsymbol{R}$. Anche la loro unione $\bigcup\{j \in J\ :|\ I_j\}$ è un ideale di $\boldsymbol{R}$.

Dim.: Viene esposta in T23 ∎

T15 j.06 Un dominio di integrità $\boldsymbol{R}$ in cui ogni ideale è principale è detto **dominio a ideali principali**. Questo termine l'abbrevieremo con **PID**, acronimo di *principal ideal domain*.

(1) Prop.: Ogni campo $\boldsymbol{F}$ è un anello a ideali principali.

Dim.: $\boldsymbol{F}$ è un anello commutativo che possiede soltanto i due ideali che si possono esprimere come $< 0 >$ ed $< e >= F$, e quindi che sono ideali principali ∎

Il dominio di integrità degli interi naturali $\mathbb{N}$ è un dominio a ideali principali. Infatti, ogni ideale I ha la forma $m \cdot \mathbb{N}$ per qualche $m = 2, 3, 4, ...$ e risulta generato dal più piccolo intero maggiore di 1 che è contenuto in I, cioè ha la forma $< m >$.
Anche l'anello $\boldsymbol{F}[x]$ è un dominio a ideali principali. Infatti ogni ideale I è generato dall'unico polinomio monico contenuto in I e avente grado minimo.

T15 j.07 Si dice **ideale massimale di un anello $\boldsymbol{R}$** un suo ideale I che soddisfa le due seguenti condizioni:

[IdlM 1] I è incluso propriamente in R;

[IdlM 2] I non è incluso propriamente in alcun ideale proprio di $\boldsymbol{R}$ diverso da I; in altri termini $I \subset R\ \wedge\ I \subseteq J \subset R \implies I = J$.

(1) Prop.: Sia $\boldsymbol{K}$ un corpo; l'ideale $< 0 >$ costituito dal solo zero di K è massimale, perché un corpo non possiede ideali propri.

T15 j.08 Un ideale I di un anello commutativo $\boldsymbol{R}$ si dice **ideale primo** sse, per ogni coppia di elementi $a, b \in R$ con $a \cdot b \in I$, accade che almeno uno dei due fattori a o b appartiene ad I.

(1) Prop.: Sia I un ideale di un anello commutativo $\boldsymbol{R}$. Se I è ideale massimale, esso è anche un ideale primo.

T15 j.09 Si chiama **radicale di un ideale** I di un anello $\boldsymbol{R}$, e lo si denota con $\mathsf{Rdcl}(I)$, il sottoinsieme di $\boldsymbol{R}$ costituito dagli elementi r di R, tali che $r^h \in I$ per qualche esponente intero positivo h.
Il radicale di I contiene I, in quanto per ogni $b \in I$, risulta $b^1 \in I$.

(1) Prop.: Il radicale di un ideale I di un anello commutativo $\boldsymbol{R}$ è anch'esso un'ideale di $\boldsymbol{R}$.

Dim.: Sia $r \in \mathsf{Rdcl}(I)$ ed $h \in \mathbb{P}$ sia il minimo esponente tale che $r^h \in I$.
Per ogni $a \in R$ si ha $(a\,r)^h = a^h\,r^h \in a^h\,I = I$ ∎

T15 j.10 Un ideale I di un anello commutativo $\boldsymbol{R}$ si dice **ideale primario** sse, ogniqualvolta il prodotto $a \cdot b$ di due elementi a, b di R appartiene ad I, ed a non sta in I, allora una opportuna potenza b^h di b sta in I, ovvero b appartiene al radicale di I.

(1) Prop.: Ogni ideale primo è anche ideale primario.

T15 k. campi

T15 k.01 Un campo è una struttura presentabile con una espressione della forma $\boldsymbol{F} = \langle F, +, -, 0, \cdot, ^{-1}, 1\rangle$, dove $\langle F, +, -, 0\rangle$ e $\langle F \setminus 0, \cdot, ^{-1}, 1\rangle$ sono gruppi commutativi e il prodotto $\cdot$ è distributivo rispetto alla somma $+$. I due gruppi citati sono detti **gruppo additivo del campo** e **gruppo moltiplicativo del campo** $\boldsymbol{F}$ e, per uniformità, sono denotati, risp., con $\boldsymbol{F}_{ag}$ e con $\boldsymbol{F}_{mg}$.
Denotiamo con **Fld** la classe dei campi e con **FldF** la classe dei campi finiti.

T15 k.02 Campi numerabili sono forniti dall'insieme dei numeri razionali relativi $\mathbb{Q}$, dall'insieme dei numeri algebrici $\mathbb{R}_{\mathsf{a}}$ e dall'insieme dei numeri reali costruibili $\mathbb{R}_{\mathsf{c}}$. Campi più che numerabili sono forniti dagli insiemi $\mathbb{R}$ dei numeri reali e $\mathbb{C}$ dei numeri complessi, muniti delle usuali operazioni di somma, prodotto, cambiamento di segno, zero e unità. Per questi campi usiamo notazioni come:

$$\mathbb{Q}_{Fld} := \langle \mathbb{Q}, +, -, 0, \cdot, 1\rangle \qquad \mathbb{R}_{Fld} := \langle \mathbb{R}, +, -, 0, \cdot, 1\rangle \qquad \mathbb{C}_{Fld} := \langle \mathbb{Q}, +, -, 0, \cdot, 1\rangle \ .$$

T15 k.03 Sono molto importanti anche i campi finiti che, come vedremo, si possono classificare esaurientemente con relativa facilità.

In particolare sono campi finiti gli anelli della forma $\mathbb{Z}_p$ con p numero primo (a rigore dopo essere stati arricchiti dell'operazione unaria di passaggio all'inverso.
Tra gli anelli $\mathbb{Z}_m$ con $m = 2, 3, 4, ...$ essi sono i soli che possono essere arricchiti per costituire un campo.

T15 k.04 Una importante proprietà dei campi riguarda la non esistenza di divisori dello 0 diversi da tale elemento.

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

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

I campi sono quindi particolari domini di integrità.

La precedente proprietà e l'invertibilità di quasi tutti i loro elementi fanno dei campi delle piattaforme computazionali molto efficaci.

T15 k.05 Ricordiamo anche la già citata proprietà:

Teorema Ogni corpo finito è un campo.

T15 I. campi finiti

T15 I.01 Vediamo ora come conviene procedere per trovare una fattorizzazione irriducibile per polinomi su $\mathbb{Z}_p$ con p primo. Chiaramente è lecito limitarsi alla ricerca di fattori irriducibili monici di un polinomio monico.

I primi fattori irriducibili da provare sono i p polinomi lineari aventi la forma $x-k$ per $k = 0, 1, ..., p-1$.

Successivamente conviene considerare i polinomi quadratici x^2+bx+c. Questi sono p^2; di essi $p(p-1)/2$ hanno la forma $(x-k)(x-h)$ con $k \neq h$ e p la forma $(x-k)^2$; i rimanenti $p(p-1)/2$ sono i polinomi monici quadratici irriducibili. In particolare in $\mathbb{Z}_2[x]$ si ha come unico polinomio quadratico monico irriducibile $x^2 + x + 1$.

Ogni polinomio cubico riducibile deve possedere un fattore lineare; quindi si può decidere la riducibilità di un polinomio cubico stabilendo se esso si annulla per uno dei valori $x = 0, ..., p-1$.

La irriducibilità di polinomi di gradi superiori al terzo costituisce un problema abbastanza impegnativo per il quale sono stati trovati algoritmi piuttosto complessi.

T15 I.02 Vediamo ora quali possono essere i cardinali dei campi finiti.

Osserviamo innanzi tutto che ogni campo contiene gli elementi 1, 1+1=2, 1+1+1=3, ... questi elementi costituiscono un sottogruppo ciclico del gruppo additivo del campo che denotiamo con $\langle 1 \rangle_+$.
Nel caso di un campo finito $\boldsymbol{F}$, per il teorema di Lagrange l'ordine di $\langle 1 \rangle_+$ divide $|F|$; questo intero positivo viene detto **caratteristica del campo $\boldsymbol{F}$**.
Per esempio per $\mathbb{Z}_p$ $\langle 1 \rangle_+$ coincide con l'intero campo: quindi la caratteristica di $\mathbb{Z}_p$ è p. In generale la caratteristica di un campo F è il minimo intero k per il quale $k \cdot 1 = 0$.

T15 I.03 Sia $\boldsymbol{R}$ un anello e r un suo elemento. Se n è un intero positivo, con l'espressione $n \cdot r$, si sottointende: $n \cdot r = \underbrace{r + \cdots + r}_{n-volte}$. Può succedere che esista un intero positivo c per il quale sia $c \cdot 1 = \underbrace{1 + \cdots + 1}_{c-volte} = 0$. Per esempio in $\mathbb{Z}_n$ si verifica che $n \cdot 1 = n = 0$. Invece, in $\mathbb{Z}$, $c \cdot 1 = 0$ implica che $c = 0$, e quindi che non esiste questo intero positivo che annulla il prodotto.

Si dice **caratteristica di un anello $\boldsymbol{R}$** il più piccolo intero positivo c per il quale si verifica $c \cdot 1 = 0$. Se un tale numero c non esiste, si dice che $\boldsymbol{R}$ è un **anello di caratteristica zero**.

Per denotare la caratteristica di $\boldsymbol{R}$ si usa la notazione $chrt(\boldsymbol{R})$.
Se $chrt(\boldsymbol{R}) = c$, allora per ogni $r \in R$ si ha che:

$$c \cdot r = \underbrace{r + \cdots + r}_{c-volte} = \underbrace{(1 + \cdots + 1)}_{c-volte} \cdot r = 0 \cdot r = 0 \ .$$

T15 I.04 Sia $\boldsymbol{F}$ un campo dotato di almeno due elementi. Se gli elementi di $\boldsymbol{F}$ hanno tutti caratteristica maggiore o uguale a 2, e se l'insieme di dette caratteristiche ammette un massimo finito k, si dice che $\boldsymbol{F}$ è un **campo di caratteristica** k; in caso contrario si dice che $\boldsymbol{F}$ è un **campo di caratteristica zero**. Prescindendo dall'intero particolare n si parla di **campo di caratteristica positiva**.

Si noti che in ogni campo $\boldsymbol{F}$ di caratteristica 2, si ha $\forall a \in F : 2\,a = 0$; quindi in tale $\boldsymbol{F}$, $2 = 0$ e $\forall a \in F : a = -a$.

T15 I.05 Prop. Un campo F di caratteristica zero è infinito.

Dim.: ∎

T15 I.06 Prop. Ogni anello finito ha caratteristica diversa da zero.

Dim.: ∎

T15 I.07 Prop. La caratteristica di un campo finito deve essere un numero primo.

Dim.: Se la caratteristica fosse esprimibile come $m_1 \cdot m_2$ sarebbe $m_1 \cdot m_2 = 0$ e quindi $m_1 = 0$ aut $m_2 = 0$, contro la minimalità richiesta per la caratteristica ∎

T15 I.08 Prop. Il gruppo additivo di un campo finito di caratteristica p è isomorfo a una certa potenza diretta del gruppo ciclico di ordine p, $(\boldsymbol{Cycl}_p)^r$.

Dim.: Per ogni $a \in F$ si individua un sottogruppo del gruppo additivo di $\boldsymbol{F}$, $\langle a \rangle_+ := \{a, 2a, 3a, ...\}$; dato che $p = 0$ in $\boldsymbol{F}$, questo sottogruppo è ciclico e isomorfo a $\boldsymbol{Cycl}_p$.
Un sottoinsieme di F $\{f_1, f_2, ..., f_s\}$ si dice **generatore del campo $\boldsymbol{F}$** sse ogni elemento di F si può esprimere nella forma $h_1\, f_1 + h_2\, f_2 + ... + h_s\, f_s$ per qualche intero positivo S e per qualche $\langle h_1, h_2, ..., h_s \rangle \in F^s$.
Un generatore individuabile banalmente è F stesso; naturalmente tra i generatori sono più pregevoli i minimali rispetto all'inclusione; sia dunque $\{f_1, ..., f_r\}$ uno di questi.
Ogni $a \in F$ si può esprimere come $a = a_1\, f_1 + a_2\, f_2 + ... + a_r\, f_r$ con $a_1, ..., a_r \in \mathbb{Z}_p$; se fosse possibile esprimere a con una diversa combinazione lineare $a = b_1\, f_1 + b_2\, f_2 + ... + b_r\, f_r$, detto i il primo indice per il quale fosse $a_i \neq b_i$, si avrebbe $(a_i - b_i) f_i = (b_{i+1} - a_{i+1}) f_{i+1} + ... + (b_n - a_n) f_n$, ovvero $f_i = (a_i - b_i)^{-1} \Big((b_{i+1} - a_{i+1}) f_{i+1} + ... + (b_n - a_n) f_n \Big)$, contro l'ipotesi di minimalità di $\{f_1, ..., f_r\}$.
Quindi vi è una biiezione tra F e l'insieme delle r-uple $\langle a_1, ..., a_r \rangle$ di coefficienti in $\mathbb{Z}_p$.
Dato che l'addizione in F corrisponde all'addizione modulo p nell'insieme delle r-uple di ${\mathbb{Z}_p}^r$, si ha un isomorfismo tra il gruppo additivo di F e ${\boldsymbol{Cycl}_p}^r$ ∎

(1) Coroll.: Ogni campo finito ha come cardinale una potenza di un numero primo ∎

T15 I.09 Sia p un primo qualsiasi e $k(x)$ un polinomio di $\mathbb{Z}_p$ irriducibile il cui grado scriviamo r.
Definiamo in $\mathbb{Z}_p[x]$ la relazione $\sim_k (x)$ con la seguente richiesta

$$f(x) \sim_k (x) g(x) \iff f(x) - g(x) \text{ è multiplo di } k(x) .$$

Si vede facilmente che si tratta di una relazione di equivalenza. Essa inoltre rispetta le operazioni di somma e prodotto del campo:

$$\forall f_1(x), f_2(x), g_1(x), g_2(x) \in \boldsymbol{F}[x] \;:\; f_1(x) \sim_k g_1(x),\; f_2(x) \sim_k g_2(x) \implies$$
$$f_1(x) + f_2(x) \sim_k g_1(x) + g_2(x),\; f_1(x) \cdot f_2(x) \sim_k g_1(x) \cdot g_2(x)$$

Questa equivalenza quindi viene detta **congruenza sul campo** $\mathbb{Z}_p$.
Si può quindi considerare l'insieme quoziente $\mathbb{Z}_p/\!\sim_k$; ogni suo elemento, cioè ogni classe della congruenza $\sim_k$, si può denotare con $\big[\!\big[f(x) \big]\!\big]_k$ intendendo che $f(x)$ rappresenti il generico polinomio $f(x) \in \mathbb{Z}_p[x]$.

Su $\mathbb{Z}_p/\!\sim_k$ si definiscono le operazioni di somma $+_k$ e prodotto $\cdot_k$ ponendo

$$\big[\!\big[f(x) \big]\!\big]_k +_k \big[\!\big[g(x) \big]\!\big]_k := \big[\!\big[f(x) + g(x) \big]\!\big]_k \qquad \big[\!\big[f(x) \big]\!\big]_k \cdot_k \big[\!\big[g(x) \big]\!\big]_k := \big[\!\big[f(x) \cdot g(x) \big]\!\big]_k .$$

T15 I.10 Prop. La struttura $\langle \mathbb{Z}_p/\!\sim_k, +_k, -_k, [0], \cdot_k, [1] \rangle$ è un campo di ordine p^r.

Dim.: Chiaramente ogni classe di $\sim_k$ è rappresentata da qualche polinomio di grado minore o uguale ad $r - 1$; l'insieme di questi polinomi è in corrispondenza biunivoca con ${\mathbb{Z}_p}^r$ e quindi le classi sono p^r.

Risulta routinario dimostrare che $\mathbb{Z}_p[x]/\sim_k$ munito di somma e prodotto costituisce un anello unifero commutativo.
Questi risultati non dipendono dalla irriducibilità di $k(x)$.
Resta quindi da dimostrare che la irriducibilità di $k(x)$ comporta che ogni $[f(x)]_k$ diverso da $[0]_k$ è dotato di inverso rispetto a $-_k$.
Per ogni $f(x) \in \mathbb{Z}_p[x]$ l'irriducibilità di $k(x)$ implica $\text{MCD}(f(x), k(x)) = 1$; quindi, per B41, si trovano $a(x), b(x) \in \mathbb{Z}_p[x]$ tali che $f(x)a(x) + k(x)b(x) = 1$.
Ppassando alle classi dell'equivalenza $\sim_k$, dato che $[k(x)]_k = [0]_k$, si ottiene $[f(x)]_k[a(x)]_k = [1]_k$, cioè risulta che $f(x)$ è invertibile ∎

Come vedremo in seguito, per ogni p ed r si trova in $\mathbb{Z}_p[x]$ un polinomio irriducibile di grado r; quindi la proposizione precedente consente di concludere che esiste un campo finito di ogni ordine p^r.

T15 I.11 Un altro risultato sui campi finiti, generale e di grande semplicità, è il seguente.

(1) Prop.: Il gruppo moltiplicativo di ogni campo finito è ciclico.

Dim.: Sia $\boldsymbol{F}$ un campo di ordine q sul terreno F e introduciamo la notazione $F_{nz} := F \setminus \{0\}$.
Per ogni $f \in F_{nz}$ si ha che il suo periodo divide l'ordine del gruppo $q-1$ e $f^{q-1} = 1$; per l'arbitrarietà di f, si ricava che il polinomio $x^{q-1} - 1$ ha $q-1$ radici in F ∎

T15 I.12 Consideriamo un generico d divisore di $q-1$; posto $k := (q-1)/d$, si verifica l'uguaglianza

$$x^{q-1} - 1 = (x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + ... + x^d + 1) \ .$$

Dato che il numero delle radici del primo membro è pari al suo grado, il massimo possibile, deve essere massimo anche il numero delle radici di ciascuno dei due polinomi della fattorizzazione al secondo membro.
Quindi $x^d - 1$ ha d radici in F, cioè vi sono d elementi $f \in F_{nz}$ per i quali $f^d = 1$.
Ma un gruppo finito che gode della precedente proprietà per ogni divisore d del suo ordine è un gruppo ciclico ∎

T15 I.13 Si dice **elemento primitivo di un campo** $\boldsymbol{F}$ un suo elemento g in grado di generare l'intero F_{nz} e quindi in grado di rendere lecita la formula:

$$F_{nz} = \{1, g, g^2, ..., g^{q-2}\} \qquad \text{con} \quad g^{q-1} = 1 \ .$$

La proposizione precedente può dunque riformularsi come segue.

(1) Prop.: Ogni campo finito possiede un elemento primitivo ∎

T15 I.14 Può essere molto utile individuare un elemento primitivo di un campo finito, in quanto tale elemento consente di controllare agevolmente la struttura moltiplicativa del campo; purtroppo la soluzione di questo problema incontra notevoli difficoltà.

Dato che il numero degli elementi di periodo $q-1$ in $\boldsymbol{Cycl}_{q-1}$ è $\Phi_{eu}(q-1)$, può essere sensato procedere sperimentalmente. Si dispone anche di tavole piuttosto ampie, sia per i campi $\mathbb{Z}_p$ che per i campi di polinomi $\mathbb{Z}_q[x]$.

Sono particolarmente maneggevoli i campi di Galois individuati da un polinomio irriducibile $k(x)$ per i quali lo stesso polinomio x è elemento primitivo. In questo caso $k(x)$ viene detto **polinomio irriducibile primitivo**.
Per calcolare i prodotti di polinomi in questi campi risulta piuttosto utile la tavola delle potenze di x.

T15 I.15 Due polinomi di grado r irriducibili su $\mathbb{Z}_p$ generano due campi dello stesso ordine p^r. L'ultimo risultato di ampia portata sui campi finiti garantisce il loro isomorfismo.

(1) Prop.: Tra due campi finiti dello stesso ordine esiste una biiezione che è contemporaneamente isomorfismo per i due gruppi additivi, isomorfi a $\boldsymbol{Cycl}_p^{\,r}$, ed isomorfismo per i due gruppi moltiplicativi, isomorfi a $\boldsymbol{Cycl}_{p^r-1}$.

Si ha quindi la sostanziale unicità dei campi finiti di ciascuno degli ordini $q = p^r$ possibili. In astratto il campo di ordine q viene detto **campo di Galois di ordine** q e lo si denota con con $\mathcal{GF}(q)$.
Naturalmente per $r = 1$ si ha $\mathcal{GF}(1) = \mathbb{Z}_p$.

T15 m. semireticoli e reticoli

T15 m.01 In questa sezione, dopo aver presentata una specie di struttura che si colloca tra i monoidi, sono introdotti i reticoli come strutture algebriche dotate di due operazioni con proprietà molto simili, contrariamente a quelle degli anelli e alle strutture loro vicine.

I reticoli si possono considerare arricchimenti dei semireticoli, e risultano equivalenti a strutture d'ordine, cioè risultano criptomorfi a specifiche strutture d'ordine.

Anche grazie alla loro versatilità derivante da quanto sopra i reticoli sono strutture ampiamente utilizzate e sono riprese in vari momenti di questa *esposizione*, in particolare in B55.

T15 m.02 Si dice **semireticolo** un magma la cui operazione binaria è commutativa, associativa e idempotente; in altre parole si può affermare che un semireticolo è un semigruppo abeliano con l'operazione idempotente.

Un semireticolo spesso si denota con una scrittura del tipo $\boldsymbol{L} = \langle L, \wedge \rangle$ e la sua operazione si chiama **incontro**, in inglese *meet*.
In dettaglio per essa si chiedono le proprietà che seguono.

$\forall a, b, c \in L \quad :$

(1) $\quad a \wedge b \;=\; b \wedge a \quad$ (commutatività) ;

(2) $\quad a \wedge (b \wedge c) \;=\; (a \wedge b) \wedge c \quad$ (associatività) ;

(3) $\quad a \wedge a \;=\; a \quad$ idempotenza) .

T15 m.03 La classe dei semireticoli si denota con **Smlatt** e l'insieme dei semireticoli aventi l'insieme L come terreno con $\mathbf{Smlatt}_L$.

Ad ogni semireticolo $\boldsymbol{L} = \langle L, \wedge \rangle$ si associa una relazione entro L che denotiamo con:

$$\leq_{\boldsymbol{L}} := \bigcup_{a \in L} \Big\{ \langle a, b \rangle \; ST \; b \in L \wedge a \wedge b = a \Big\} \; ,$$

leggibile come **essere sottostruttura del semireticolo $\boldsymbol{L}$**.

(1) Prop.: La relazione $\leq_{\boldsymbol{L}}$ relativa ad $\boldsymbol{L} = \langle L, \wedge \rangle$ è una relazione d'ordine.

Dim.: Consideriamo a, b e c generici elementi di L.

Chiaramente $\forall a \in L \; : \; a \wedge a = a$, ossia $a \leq_{\boldsymbol{L}} a$, ovvero la relazione è riflessiva.

$a \leq_{\boldsymbol{L}} b$ e $b \leq_{\boldsymbol{L}} a$ implicano, risp., $a \wedge b = a$ e $b \wedge a = b$ e quindi, per m02, $a = b$; dunque la relazione è antisimmetrica.

$a \leq_{\boldsymbol{L}} b$ e $b \leq_{\boldsymbol{L}} c$ implicano $a \wedge b = a$ e $b \wedge c = b$ e quindi $a \wedge c = (a \wedge b) \wedge c \;=\; \lfloor_{\mathbb{N}}\, \mathsf{m01}(2) \,\rfloor_{\mathbb{N}} \;=\; a \wedge (b \wedge c) = a \wedge b = a$, cioè $a \leq_{\boldsymbol{L}} c$; dunque la relazione è transitiva ∎

L'insieme ordinato $\big\langle L, \leq_{\boldsymbol{L}} \big\rangle$ ha la seguente proprietà: ogni coppia $\langle a, b \rangle$ di suoi elementi possiede l'elemento infimo, cioè il massimo dei comuni minoranti; un tale ordine si dice **ordine reticolato inferiormente**.

T15 m.04 Ad ogni semireticolo si è associato un insieme reticolato inferiormente. Vale anche il procedimento inverso: ad ogni insieme reticolato inferiormente $\big\langle L, \leq \big\rangle$ si associa il semireticolo $\big\langle L, \wedge \big\rangle$, dove per ogni $a, b \in L$ si pone $a \wedge b := \inf(a, b)$.
Si mostra facilmente che le due trasformazioni da semireticolo a insieme reticolato inferiormente sono l'una l'inversa dell'altra. Quindi si ha criptomorfismo tra semireticoli e insieme reticolati inferiormente.

T15 m.05 La possibilità di trattare un semireticolo servendosi della relazione d'ordine associata può essere vantaggiosa. In particolare un semireticolo finito può essere trattato avvalendosi della raffigurazione del corrispondente digrafo.

Ogni controarborescenza, cioè ogni digrafo che presenta un nodo (radice) che può essere raggiunto da tutti i rimanenti con uno e un solo cammino fornisce un semireticolo, quello avente come terreno l'insieme dei nodi e per il quale l'operazione incontro porta da due nodi (nodi operandi) al primo nodo che hanno in comune i due cammini ciascuno dei quali porta da uno dei nodi operandi al nodo radice.

input pT15m04

Si osserva che la radice di questo digrafo corrisponde all'elemento neutro per l'operazione di incontro. Ogni semireticolo rappresentato da una controarborescenza, quindi, è dotato di unità (bilatera); quindi è un monoide. L'elemento neutro di un semireticolo viene chiamato anche zero o minimo.
Vedremo tra poco semireticoli privi di unità. I semireticoli dotati di unità sono detti **semireticoli uniferi**. Questi sono i monoidi abeliani idempotenti.

T15 m.06 Altri esempi di semireticoli si ottengono considerando un insieme G di punti del piano $\mathbb{R} \times \mathbb{R}$ e la sua estensione $\overline{G}$ ottenuta con successive operazioni di ampliamento del seguente genere: se $\langle a, b\rangle$ e $\langle a', b'\rangle$ appartengono a $\overline{G}$, gli si aggiunge anche il punto-RR $\langle \min(a, a'), \min(b, b')\rangle$.

Se G è finito si ottiene un semireticolo unifero finito, reticolo la cui unità è data dalla coppia costituita dalla minima delle prime coordinate degli elementi in G e dalla minima delle seconde coordinate.

G potrebbe anche essere infinito numerabile o più che numerabile.
Se i due insiemi delle prime e delle seconde coordinate sono entrambi dotati di minimo si ha un semireticolo unifero avente come elemento neutro la coppia dei due minimi. In caso contrario si ha un semireticolo privo di elemento neutro.

La costruzione precedente si può applicare, più in generale, a insiemi G di coppie di elementi appartenenti al prodotto cartesiano di due insiemi reticolati inferiormente $\boldsymbol{L}_1 = \langle L_1, \leq_1\rangle$ e $\boldsymbol{L}_2 = \langle L_2, \leq_2\rangle$‘ .
In questo caso l'ampliamento di G a $\overline{G}$ si ottiene aggiungendo, in presenza delle coppie $\langle a, b\rangle$ e $\langle a', b'\rangle$, la coppia $\big\langle \inf_1(a, a'), \inf_2(b, b')\big\rangle$, dove $\inf_i$ denota l'operazione di infimo per il semireticolo $\boldsymbol{L}_i$.

T15 m.07 Ricordiamo che a ogni insieme ordinato si può associare l'ordine opposto e osserviamo che si possono ottenere semireticoli a partire da insiemi ordinati utilizzando il passaggio al supremo invece che il passaggio all'infimo.

Talora è opportuno distinguere i semireticoli dell'incontro dai semireticoli della giunzione. Per questi ultimi si utilizzano le operazioni di massimo invece che di minimo e le operazioni di supremo invece che di infimo.
Per questi semireticoli invece che di elemento zero o minimo si parla di elemento unità o massimo.

Mentre in astratto i semireticoli dell'incontro e quelli della giunzione possono essere trattati come strutture equivalenti, interessano strutture che chiamiamo strutture ambiente entro e quali si individuano due semireticoli che condividono lo stesso terreno della struttura ambiente e che hanno i rispettivi operatori in stretta relazione.

T15 m.08 Torniamo alle raffigurazioni dei semireticoli introdotte all'inizio di m06 per suggerire che ruotando tali sistemi di punti di 90°, di 180° e di 270° si ottengono altri insiemi di coppie di punti-RR che si possono considerare semireticoli.

(1) Eserc. Precisare le definizioni delle operazioni binarie commutative, associative e idempotenti per i tre tipi di reticoli di punti-RR suggeriti in precedenza.

T15 m.09 Consideriamo un ambiente U e un suo sottoinsieme S. La collezione dei sottoinsiemi di S munita dell'operazione di intersezione costituisce un semireticolo.
Dualmente-UD costituisce un semireticolo la collezione dei sovrainsiemi di S munita dell'operazione di unione.

Degli interessanti sottosemireticoli dei semireticoli precedenti si individuano quando si considerano semireticolo di insiemi di vettori di uno spazio vettoriale.

(1) Eserc. Precisare il semireticolo costituito dagli insiemi di vettori indipendenti di uno spazio vettoriale.

(2) Eserc. Precisare il semireticolo costituito dagli insiemi di vettori dipendenti di uno spazio vettoriale.

T15 m.10 Definiamo **reticolo** una struttura algebrica che si può introdurre con una espressione della forma $\langle P, \wedge, \vee \rangle$ nella quale P è un insieme nonvuoto, mentre $\wedge$ e $\vee$ sono operazioni binarie che soddisfano le seguenti richieste:

$\forall a, b, c \in P \ :$

(1) $\quad a \wedge b \ = \ b \wedge a \quad , \quad a \vee b \ = \ b \vee a \quad , \quad$ (commutatività) ;

(2) $\quad a \wedge (b \wedge c) \ = \ (a \wedge b) \wedge c \quad , \quad a \vee (b \vee c) \ = \ (a \vee b) \vee c \quad , \quad$ (associatività) ; JP (3) $a \vee (a \wedge b) \ = \ a \quad , \quad a \wedge (a \vee b) = a \quad , \quad$ (proprietà di assorbimento) .

(4) Prop.: Dalle identità precedenti si derivano le due seguenti

$$\forall a \in P \ : \ a \wedge a \ = \ a \qquad , \qquad a \vee a \ = \ a \quad , \quad \text{(idempotenza)} \ .$$

Dim.: $a \vee a = \llcorner (3) II \lrcorner = a \vee (a \wedge (a \vee a)) = \llcorner (3) I \lrcorner = a$.
Similmente si trova $a \wedge a = a \wedge (a \vee (a \wedge a)) = a$ ∎

In italiano, oltre al termine reticolo, è stato utilizzato anche il termine traliccio. In inglese la struttura qui esaminata si chiama **lattice**; segnaliamo anche che in tedesco si dice *verband* e in francese **treilli**.

T15 m.11 In un reticolo $\langle L, \wedge, \vee \rangle$ si individuano i due semireticoli $\langle L, \wedge \rangle$ e $\langle L, \vee \rangle$.
Si osserva che le due relazioni ottenute da questi semireticoli sono l'una l'opposta dell'altra.
Data una relazione d'ordine sopra un insieme nonvuoto L (e quindi la sua opposta) non è detto che si giunga a un reticolo. Questo richiede anche che valgano le proprietà di assorbimento, proprietà che si possono considerare come regole per l'armonizzazione dei due semireticoli che si riconoscono entro il reticolo.
Le identità di assorbimento implicano che il poset $\langle L, \leq \rangle$ sia tale che per ogni coppia di suoi elementi $\langle a, b \rangle$ esistano il minimo dei loro maggioranti, cioè il loro supremo $\sup(a, b)$, ed il massimo dei loro minoranti, cioè il loro infimo $\inf(a, b)$.
Un tale poset si dice **poset reticolato**.

T15 m.12 Ad ogni reticolo $\boldsymbol{L} = \langle L, \wedge, \vee \rangle$ risulta associato il poset reticolato $\langle L, \leq_{\boldsymbol{L}} \rangle$ dove

$$\forall a, b \in L \ : \ a \leq_{\boldsymbol{L}} b \quad \text{sse} \quad a \wedge b = b \quad \text{sse} \quad a \vee b = a \ .$$

Viceversa a ogni poset reticolato $\langle L, \leq \rangle$ risulta associato il reticolo $\langle L, \sup, \inf \rangle$.
È ovvio che le due operazioni del precedente reticolo sono commutative ed idempotenti.
Si vede facilmente anche che esse sono associative: infatti, per ogni scelta $x, y, z \in P$, sia $x \wedge (y \wedge z)$ che $(x \wedge y) \wedge z$ individuano il minimo dei maggioranti di $\{x, y, z\}$.

Si constata inoltre che la specie dei reticoli e la specie dei poset reticolati sono criptomorfe.
Denotiamo con **PosetLatt** la classe dei posets reticolati.

T15 m.13 Osserviamo che un reticolo è limitato inferiormente sse è dotato di minimo.
Dualmente-UD un reticolo è limitato superiormente sse è dotato di massimo.
Inoltre il minimo, se esiste, è elemento neutro per l'operazione $\vee$ ed è elemento assorbente (lo zero) per l'operazione $\wedge$; dualmente il massimo, se esiste, è elemento neutro per l'operazione $\wedge$ ed è lo zero per la $\vee$.

In genere il minimo di un reticolo limitato inferiormente si denota con 0 o con segno simile; dualmente il massimo di un reticolo limitato superiormente si denota con 1 o con segno simile.

T15 m.14 Un insieme reticolato $\langle L, \preceq \rangle$ si dice **insieme reticolato completo** sse di ogni sottoinsieme di L esistono il supremo e l'infimo.
A sua volta di dice, prevedibilmente, **reticolo completo** ogni reticolo criptomorfo a un insieme reticolato completo. Denotiamo con **LattC** la classe dei reticoli completi.

Chiaramente un reticolo completo $\langle L, \wedge, \vee \rangle$ è limitato: infatti si possono individuare il suo massimo e il suo minimo, risp., con le espressioni

$$\bigwedge \{a \in L :| \ a\} \quad \text{e} \quad \bigvee \{a \in L :| \ a\} \ .$$

T15 m.15 In un poset due elementi x e y possono avere nessuno, uno o molti minoranti comuni e possono avere nessuno, uno o molti maggioranti comuni.

Si dice **poset reticolato** un poset in cui ogni coppia di elementi possiede un infimo e un supremo; ovviamente in un poset reticolato ogni insieme finito possiede un infimo e un supremo.
Si dice inoltre **poset completamente reticolato** un poset nel quale tutti i sottoinsiemi, anche gli infiniti, posseggono un infimo e un supremo.
Denotiamo con **PosetLatt** la classe dei posets reticolati e con **PosetLattC** la classe dei posets completamente reticolati.

I posets totali sono particolari posets reticolati, ossia **PosetT** $\subset$ **PosetLatt**.

T15 m.16 In un poset reticolato $\langle P, \preceq \rangle$ il passaggio da due elementi x e y al loro infimo $x \wedge y$ e il passaggio al loro supremo $x \vee y$ sono operazioni binarie.

Si osserva poi che $x \preceq y \iff x \wedge y = x \iff x \vee y = y$.
Da questo si deduce che valgono le cosiddette **proprietà di assorbimento**:

$$\forall x, y \in P \ : \ x \vee (x \wedge y) \ = \ x \qquad x \wedge (x \vee y) \ = \ x \ .$$

T15 m.17 Si può compiere ora un cammino opposto, definendo la nozione di reticolo in termini puramente algebrici e successivamente associando a un generico reticolo un poset che risulta essere reticolato.

Definiamo dunque **reticolo** una struttura algebrica della forma $\langle P, \wedge, \vee \rangle$, ove $\wedge$ e $\vee$ sono due operazioni binarie per le quali valgono le proprietà di
- commutatività,
- associatività e
- assorbimento.

Denotiamo con **Latt** la classe dei reticoli e con **LattF** la classe dei reticoli finiti.

Ad una tale struttura algebrica si associa la relazione $\preceq$ chiedendo:

$$x \preceq y \iff x \wedge y = x \iff x \vee y = y \ .$$

Si dimostra che $\preceq$ è una relazione riflessiva, antisimmetrica e transitiva e, più precisamente, che $\langle P, \preceq \rangle$ è un poset reticolato. Esso si dice **poset associato al reticolo**.

T15 m.18 Si verifica anche che passando da un poset reticolato $\boldsymbol{P} = \langle P, \preceq \rangle$ al reticolo associato e da questo al poset associato si ritorna al poset $\boldsymbol{P}$.
Si trova inoltre che trasformando un reticolo $\boldsymbol{L}$ nel corrispondente poset reticolato e passando da quest'ultimo al reticolo associato si riottiene $\boldsymbol{L}$.

Abbiamo quindi che le nozioni di poset reticolato e di reticolo sono **logicamente equivalenti**, cioè ogni affermazione vera per uno di queste strutture può essere trasformata in una affermazione vera per la struttura associata, previo cambiamento di alcuni costrutti (come scambiare una relazione d'ordine con una coppia di operazioni binarie).
Si ha quindi un interessante esempio di **criptomorfismo** tra le due specie di strutture.

T15 m.19 Si tratta di una situazione che consente di portare sistematicamente le costruzioni e le proprietà di una specie di struttura all'altra.
Quindi si può parlare di zero, unità, atomi e coatomi del reticolo.
Risulta anche naturale parlare di **passaggio al reticolo duale**: si tratta semplicemente della trasformazione in cui i due operatori di incontro e giunzione si scambiano i ruoli.

Quindi si può introdurre un principio di dualità anche per i reticoli. In particolare le operazioni giunzione e incontro vanno considerate nozioni duali.

T15 m.20 Un sottoinsieme M di un reticolo $\boldsymbol{L} = \langle L, .. \rangle$ é chiamato **terreno di un sottoreticolo** di $\boldsymbol{L}$ sse incontro e giunzione di elementi di N portano ad altri elementi di N, cioè sse M è chiuso rispetto alle due operazioni binarie.
Per la suddetta relazione essere **sottoreticolo** si usano le notazioni

$$\boldsymbol{M} \leq_{Latt} \boldsymbol{L} \qquad \text{e} \qquad \boldsymbol{M} <_{Latt} \boldsymbol{L} \ .$$

T15 m.21 Un reticolo $\boldsymbol{L} = \langle L, \wedge, \vee \rangle$ dotato di minimo $\underline{0}$ è chiamato **reticolo atomico** sse ogni elemento $a \in L$ è esprimibile come supremo di un insieme di elementi che coprono il minimo.

T15 m.22 Un reticolo $\boldsymbol{L} = \langle L, \wedge, \vee \rangle$ è chiamato **reticolo distributivo** sse per ogni terna $\langle x, y, z \rangle$ di suoi elementi valgono le seguenti identità:

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \ ,$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \ .$$

Entrambe le identità possono essere generalizzate a due arbitrari insiemi finiti di operandi:

$$\bigvee_{i=1}^{m} x_i \wedge \bigvee_{j=1}^{n} y_j = \bigvee_{i,j}^{m,n} (x_i \wedge y_j) \ ,$$

$$\bigwedge_{i=1}^{m} x_i \vee \bigwedge_{j=1}^{n} y_j = \bigwedge_{i,j}^{m,n} (x_i \vee y_j) \ .$$

T15 m.23 Un reticolo $\boldsymbol{L} = \langle L, \wedge, \vee \rangle$ è detto **reticolo modulare** sse per tutte le coppie di suoi elementi $\langle x, z \rangle$ avviene che:

$$z \leq x \implies \forall y \in P \ : \ x \wedge (y \vee z) = (x \wedge y) \vee c \ .$$

T15 m.24 Un reticolo $\boldsymbol{L} = \langle L, \wedge, \vee \rangle$ è chiamato **reticolo semimodulare** sse per tutte le coppie di suoi elementi $\langle x, z \rangle$ accade che :

$$x \wedge y \prec_{\mathtt{I}} x \implies \forall y \in P \ : \ y \prec_{\mathtt{I}} x \vee y \ .$$

T15 m.25 Consideriamo un reticolo dotato di minimo $\underline{0}$ e di massimo $\underline{1}$ e un suo elemento x.
Si dice **complemento nel reticolo di un suo elemento** x ogni x' tale che $x \wedge x' = \underline{0}$ e $x \vee x' = \underline{1}$.

Evidentemente $\underline{0}$ è complemento di $\underline{1}$ e viceversa; inoltre se x' è un complemento di x, allora x è un complemento di x'.

In un reticolo generico si hanno elementi con nessun complemento, elementi con un complemento ed elementi con più complementi.

Un reticolo limitato è chiamato **reticolo complementato** sse ciascuno dei suoi elementi è dotato di uno e un solo complemento.

Nella figura che segue accanto a ogni elemento è scritto il numero dei suoi complementi. /JU input pT15m25

T15 m.26 Consideriamo due posets $\boldsymbol{P} = \langle P, \preceq \rangle$ e $\boldsymbol{Q} = \langle Q, \leq \rangle$. Si dice **prodotto diretto dei reticoli** $\boldsymbol{P}$ e $\boldsymbol{Q}$ $\boldsymbol{P} \times \boldsymbol{Q} := \langle P \times Q, \preceq \times \leq \rangle$.
Osserviamo che

$$\preceq \times \leq = \left\{ \langle p_1, p_2 \rangle \in \preceq \ , \ \langle q_1, q_2 \rangle \in \leq \ \ : \middle| \ \left\langle \langle p_1, q_1 \rangle, \langle p_1, q_1 \rangle \right\rangle \right. .$$

Si verifica senza difficoltà che anche $\boldsymbol{P} \times \boldsymbol{Q}$ è un poset.

Semplici esempi di prodotti diretti di poset sono $\langle \mathbb{N} \times \mathbb{N}, \leq \times \leq \rangle$, $\langle \mathbb{Z} \times \mathbb{Z}, \leq \times \leq \rangle$ e $\langle \mathbb{R} \times \mathbb{R}, \leq \times \leq \rangle$.
Si osserva che questi prodotti di poset totali sono posets nontotali.

Più in generale si dimostra facilmente che il prodotto diretto di posets reticolati è un poset reticolato.

T15 m.27 Consideriamo i due insiemi delle potenze naturali dei due numeri primi 2 e 3 ordinati per divisibilità ed il loro prodotto diretto.

input pT15m26

Questo poset è isomorfo al poset degli interi naturali che sono potenze di 2 e 3 ordinati per divisibilità $\langle \{ i, j \in \mathbb{N} :| \ 2^i, 3^j \}, : \rangle$. Questo poset a sua volta è isomorfo a $\langle \mathbb{N} \times \mathbb{N} \ , \ \leq \times \leq \rangle$.

T15 m.28 Consideriamo l'insieme degli interi positivi e la relazione di divisibilità che intercorre tra i suoi elementi: evidentemente si tratta di una relazione d'ordine che ha la una seguente raffigurazione di Hasse:

input pT15m27

Osserviamo che si tratta di un digrafo graduato numerabile nel quale al livello più basso, livello 0, si trova il minimo 1 e al livello 1 degli atomi si trovano i numeri primi; al generico livello l si trovano i positivi dati dal prodotto di l fattori primi, da contare con la propria molteplicità.

Questo reticolo si può considerare il prodotto diretto degli infiniti reticoli totali delle potenze naturali dei numeri primi.
Esso è isomorfo al reticolo delle sequenze finite di numeri naturali con le operazioni di sup e inf che a due sequenze $\langle a_1, ..., a_r \rangle$ e $\langle b_1, ..., b_s \rangle$ associano le sequenze di lunghezza $m = \max(r, s)$ formate risp. dai $\max(a_i, b_i)$ e $\min(a_i, b_i)$, convenendo di assumere $a_j = 0$ per $r < j \leq m$ e $b_j = 0$ per $s < j \leq m$.

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