Capitolo D15:
Strutture algebriche monosostegno

D15:0.01 Questo è i primo di due capitoli nei quali è presentata con una certa sistematicità una gamma abbastanza estesa di specie di strutture algebriche seguendo modalità espositive che intendono permettere nell'ambito di considerazioni generali la precisa individuazione delle componenti delle specie di strutture e delle strutture specifiche e nell'ambito di considerazioni specifiche la possibilità di servirsi di notazioni e dizioni semplificate ma riconducibili senza sostanziali ambiguità alle più complete.
Vengono anche presentate le composizioni di strutture della stessa specie (a cominciare dai prodotti diretti), le relazioni fra strutture e sottostrutture e le funzioni fra strutture della stessa specie che rispettano le loro operazioni.

D15:A. Magmi e loro elementi particolari

D15:A.01 Consideriamo un insieme M non vuoto; si dice **legge di composizione (interna)** su M ogni funzione del genere $M \times M \longmapsto M$. 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 l'**insieme sostegno**; si dice anche il magma $\boldsymbol{M}$ si ottiene **munendo** l'insieme M di una sua legge di composizione C.
Il termine magma è stato introdotto con il trattato di [[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]] introdotta da [[Heinrich Brandt]].
Un magma $\boldsymbol{M}$ si dice, rispettivamente, finito, infinito, numerabile, contabile, più che numerabile, ... sse il suo sostegno è un insieme finito, infinito, numerabile, contabile, più che numerabile, ...
Si dice **ordine di un magma** $\boldsymbol{M}$ la cardinalità del suo sostegno; essa si può denotare con $|\boldsymbol{M}|$

D15:A.02 Un esempio di magma di ordine 4 è $\langle\{1,2,3,4\}, \min\rangle$, 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 $i+2j$ e $\langle\mathbb{Z}, -\rangle$, dove "–" denota la differenza di interi. Un magma infinito più che numerabile è dato dall'insieme dei numeri reali e dalla funzione che ad ogni coppia di reali associa il loro prodotto.

D15:A.03 Noi studieremo soprattutto i **magmi discreti**, magmi con insieme sostegno finito o costruibile e con **legge di composizione interna** C **calcolabile**, cioè t.c. si conosca qualche meccanismo che, a partire da due elementi qualsiasi a e b di M, consenta di individuare effettivamente $C(a,b)$.
Tipicamente per tali magmi la legge di composizione si può individuare con una matrice le cui righe e le cui colonne sono caratterizzate da elementi di M; questi a loro volta sono sequenzializzati e posti in corrispondenza con gli interi di insiemi come $[n)$, $(n]$, $\mathbb{N}$ o $\mathbb{Z}$; la componente della matrice relativa alla riga r ed alla colonna c fornisce $C(r,c)$.

Le matrici dei primi due magmi in :A.02 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** o anche **tavole pitagoriche** dei rispettivi magmi.

D15:A.04 Spesso per le indicazioni sulla legge di composizione si usa la **notazione infissa**, secondo la quale in luogo di $C(a,b)$ o dell'equivalente $\langle a,b\rangle{}_{\scriptscriptstyle\backslash}C$ si scrive $a{}_{\scriptscriptstyle\backslash}C{}_{\scriptscriptstyle\backslash}b$ o ancor più semplicemente aCb.
In questo caso la legge di composizione C viene chiamata **operazione binaria** o **operatore binario** del magma; in una scrittura come aCb si dice che a e b costituiscono risp. il **primo operando** ed il **secondo operando** dell'operatore C, oppure l'**operando sinistro** e l'**operando destro** di C.
Quando si utilizzano notazioni infisse per gli operatori si preferiscono simboli non letterali come "+" , "$\cdot$", "$_\perp$" o "$\odot$". L'esempio del magma più che numerabile, solitamente, si denota $\langle\mathbb{R},\cdot\rangle$.
In certi discorsi denotare un magma con una scrittura del tipo $\boldsymbol{M}=\langle M,\odot\rangle$ risulta piuttosto pesante, mentre il contesto rende possibile non distinguere fra $\boldsymbol{M}$ ed M in modo da rendere l'esposizione più scorrevole.

D15:A.05 La classe dei magmi si denota **Mgm**; essa costituisce un primo esempio di **specie di struttura algebrica** (v. :D).
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 dotate di opportune proprietà.

I magmi finiti aventi come sostegno un $A_n=\{a_1,...,a_n\}$ corrispondono 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]] 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 indicazioni per calcoli effettivi siano indotti a giudicare un perdigiorno chi si soffermasse più di tanto su un elenco come il precedente che dovrebbe contenere pi'u matrici di quante sono le molecole dell'universo.

D15:A.06 Per $n=2$ si hanno 16 magmi che possono essere facilmente individuati; assumiamo per questo $M=\mathbb{B}=\{0,1\}$.

$$\begin{array}{cccc} 0&0 & 0&0 & 0&0 & 0&0 \\ 0&0 & 0&1 & 1&0 & 1&1 \end{array} \qquad \begin{array}{cccc} 0&1 & 0&1 & 0&1 & 0&1 \\ 0&0 & 0&1 & 1&0 & 1&1 \end{array}$$

$$\begin{array}{cccc} 1&0 & 1&0 & 1&0 & 1&0 \\ 0&0 & 0&1 & 1&0 & 1&1 \end{array} \qquad \begin{array}{cccc} 1&1 & 1&1 & 1&1 & 1&1 \\ 0&0 & 0&1 & 1&0 & 1&1 \end{array}$$

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

$$\cdot \;=\; \wedge \;=\; \begin{array}{cc} 0&0 \\ 0&1 \end{array} \qquad \vee \;=\; \begin{array}{cc} 0&1 \\ 1&1 \end{array} \qquad +_2 \;=\; \begin{array}{cc} 0&1 \\ 1&0 \end{array} \qquad \Longrightarrow = \begin{array}{cc} 1&1 \\ 0&1 \end{array}.$$

(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 A50: .

D15:A.07 In un magma $\boldsymbol{M} = \langle M, \odot \rangle$ si possono individuare elementi con caratterizzazioni algebriche interessanti.

Si dice **elemento neutro a sinistra**, o anche **unità a sinistra**, ogni $u_l \in M$ t.c. $\forall a \in M : u_l \odot a = a$.
Si dice **elemento neutro a destra**, o anche **unità a destra**, ogni $u_r \in M$ t.c. $\forall a \in M : a \odot u_r = a$.
Si dice **elemento neutro bilatero**, o tout court **elemento neutro**, o anche **unità bilatera** o **unità**, ogni $u \in M$ t.c. $\forall a \in M : u \odot a = a \odot u = a$.

Si dice **elemento assorbente a sinistra**, o anche **zero a sinistra**, ogni $z_l \in M$ t.c. $\forall a \in M : z_l \odot a = z_l$.
Si dice **elemento assorbente a destra**, o anche **zero a destra**, ogni $z_r \in M$ t.c. $\forall a \in M : a \odot z_r = z_r$.
Si dice **elemento assorbente bilatero**, o semplicemente **elemento assorbente** o zero bilatero o **zero**, ogni $z \in M$ t.c. $\forall a \in M : z \odot a = a \odot z = z$.

Si dice **elemento idempotente** ogni $j \in M$ t.c. $j \odot j = j$.

D15:A.08 Le matrici di Cayley dei precedenti elementi hanno caratterizzazioni piuttosto evidenti. Vediamo il caso dei magmi finiti aventi come supporto un insieme dato dalla sequenza della forma $\langle x, a, b, c, d \rangle$. Assumendo per x rispettivamente i precedenti elementi u_l, u_r, u, z_l, z_r, z, j abbiamo i seguenti schemi di matrice di Cayley:

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

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

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

D15:A.09 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, rispettivamente, le matrici di Cayley con forme come le seguenti:

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

Esistono anche magmi con elementi neutri a sinistra ed elementi assorbenti a sinistra, anche magmi con elementi neutri a destra ed elementi assorbenti a destra, magmi con un elemento assorbente bilatero e un elemento neutro bilatero, quelli caratterizzati, rispettivamente, da matrici di Cayley 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 rispettivamente le matrici di Cayley con forme come le seguenti:

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

D15:A.10 (1) Prop. In un magma non possono coesistere un elemento neutro a sinistra e un elemento neutro a destra; di conseguenza non possono coesistere due elementi neutri bilateri: in altre parole, se un elemento neutro è presente, esso è unico.

Dim.: Se M contenesse un u_l e un u_r t.c. $\forall a \in M \ : \ u_l \odot a = a \odot u_r = a$, 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 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 t.c. $\forall a \in M \ : \ z_l \odot a = z_l$ 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 ∎

D15:A.11 Un magma dotato di unità si dice **magma unitale**; talora si usa l'espressione **magma unifero**. Talvolta si usa anche l'aggettivo *unitario*: questo però viene usato anche per qualificazioni ben diverse, come per gli operatori unitari (v. G48?:).

Vediamo alcuni esempi di magmi unitali.
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 $\langle \mathbb{N}, \cdot \rangle$, $\langle \mathbb{Z}, \cdot \rangle$, $\langle \mathbb{Q}, \cdot \rangle$, $\langle \mathbb{RA}, \cdot \rangle$, $\langle \mathbb{RC}, \cdot \rangle$, $\langle \mathbb{R}, \cdot \rangle$ $\langle \mathbb{Q}_+, \cdot \rangle$, $\langle \mathbb{R}_+, \cdot \rangle$ e $\langle \mathbb{C}, \cdot \rangle$.
Non posseggono invece elemento neutro i semigruppi $\langle \mathbb{P}, + \rangle$ e $\langle k\mathbb{Z}, \cdot \rangle$ per $k = 2, 3, 4, \ldots$.

D15:A.12 In generale si può ampliare un qualsiasi magma $\langle M, \odot \rangle$ con un oggetto non appartenente ad M in modo da farlo diventare unitale. Questo oggetto si può considerare un'entità formale introdotta ad hoc; denotata con ν tale entità, basta estendere $\odot$ ponendo

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

In termini di matrice di Cayley si tratta semplicemente di aggiungerle una nuova riga ed 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 quanto si vuole. Ad esempio il magma di cui si è presentata la matrice di Cayley (v. :A.02 ed :A.03) 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 al contrario, da un qualsiasi magma unitale, attraverso l'eliminazione dell'elemento neutro si ricava un altro magma; in casi particolari questa riduzione può essere reiterata.
Si verifica facilmente che queste estensioni e riduzioni mantengono caratteristiche dell'operazione $\odot$ di essere commutative (:A.16) o associative (:B.01), caratteristiche espresse da uguaglianze che mantengono la loro validità.

D15:A.13 L'endofunzione cha ad 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 ad ogni x di tale magma associa $x \odot a$ si dice **traslazione a destra** di a e si denota con a^{trslRt}. Quindi

$$a^{trslLt} = \lceil\!\lceil x \in M \mapsto a \odot x \rceil\!\rceil \qquad\qquad a^{trslRt} = \lceil\!\lceil x \in M \mapsto x \odot a \ .$$

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

D15:A.14 (S) Eserc.piegare le seguenti affermazioni per 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 $\lceil\!\lceil a \in M \mapsto z_l \rceil\!\rceil = {z_l}^{cnst}$.
(iv) La traslazione a destra associata a un elemento assorbente a destra z_r è $\lceil\!\lceil a \in M \mapsto z_r \rceil\!\rceil = {z_r}^{cnst}$.
(v) Ogni traslazione associata ad elementi idempotenti possiede almeno un punto fisso.

D15:A.15 Si dice **magma trasposto** o **magma duale** del magma $\langle M, \odot \rangle$ il magma $\langle M, \lceil\!\lceil \langle a, b \rangle \mapsto b \odot a \rceil\!\rceil \rangle$
In altre parole il magma trasposto di un dato magma è il magma avente come matrice 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 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.

D15:A.16 Si ottengono collezioni di magmi più maneggevoli e utili della media chiedendo che la loro operazione binaria goda di proprietà specifiche.
Vediamo dunque le proprietà che si possono proficuamente richiedere ad un'operazione binaria $\odot \ : \ M \times M \longmapsto M$.

L'operazione $\odot$ si dice **operazione commutativa** o **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 **abeliano**. Sono abeliani il primo magma presentato in :A.02, $\langle \mathbb{R}, \cdot \rangle$ e $\langle \mathbb{R}, + \rangle$; non lo è $\langle \mathbb{N}, g \rangle$ con $g = \ulcorner \langle i, j \rangle \in \mathbb{N} \times \mathbb{N} \mapsto i + 2j \urcorner$, dato che $i \neq j \Longrightarrow g(i, j) = i + 2j \neq g(j, i) = 2i + j$.

Chiaramente un magma è abeliano sse la sua tavola di Cayley è una matrice simmetrica. Di conseguenza i magmi abeliani aventi un sostegno di n elementi $\{a_1, ..., a_n\}$ sono $n^{n(n+1)/2}$.
Denotiamo **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 $\langle \mathbb{C}_{nz}, / \rangle$.

D15:B. Semigruppi e monoidi

D15:B.01 Un'operazione binaria $\odot$ su M si dice **associativa** sse $\forall a, b, c \in M \ : \ a \odot (b \odot c) = (a \odot b) \odot c$; in questo caso $\langle M, \odot \rangle$ si dice **semigruppo**; sapendo che si tratta con un semigruppo, nelle espressioni come le due precedenti che individuano un elemento di M mediante ripetute composizioni di elementi di M, le parentesi sono inutili: possiamo quindi scrivere $a \odot b \odot c := a \odot (b \odot c) = (a \odot b) \odot c$.
Denotiamo con **Sgrp** la classe dei semigruppi.

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). Questa varietà di esempi induce a pensare che l'associatività sia una proprietà importante e che convenga esaminarla con cura.

D15:B.02 Un semigruppo si dice **abeliano** sse è abeliano come magma, cioè sse la sua operazione binaria è commutativa. Denotiamo **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 del minimo o 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: $c \neq 0 \Longleftrightarrow a - (b - c) \neq (a - b) - c$. Similmente il magma $\langle \mathbb{Q}_+, / \rangle$ non è semigruppo, dato che, supposto che $b, c \neq 0$, si ha $c \neq 1 \Longleftrightarrow a/(b/c) \neq (a/b)/c$.

D15:B.03 Un semigruppo dotato di elemento neutro si dice **monoide**.
Denotiamo **Mnd** la loro classe e **MndAb** la specie dei monoidi abeliani, cioè dei monoidi commutativi.

Con l'estensione per aggiunta di un elemento neutro, in particolare, da un qualsiasi semigruppo si ricava un monoide. Ad es. 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 0. Similmente dal semigruppo libero delle stringhe su un alfabeto A munite di giustapposizione $\langle \mathsf{A}^*, \cdot \rangle \in$ **Sgrp** si ottiene il monoide libero $\langle A^*, \cdot, \mu \rangle \in$ **Mnd** .
Le due specie di strutture sono quindi assai vicine: studio dei semigruppi e studio dei monoidi sono sostanzialmente inscindibili.

D15:B.04 È conveniente sul piano formale individuare un monoide come terna $\langle M, \odot, u\rangle$ con M insieme sostegno, $\odot$ operazione binaria su M associativa e $u \in M$ t.c. $\forall a \in M : u \odot a = a \odot u = a$.
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 talora risulta piuttosto pesante. Si possono avere discorsi pesanti anche se si vuole mantenere costantemente la distinzione fra una struttura come un monoide ed il suo insieme sostegno. In molti casi interessanti non è necessario insistere su queste distinzioni, in quanto il contesto permette di evitare ambiguità. Nel seguito quindi spesso adotteremo degli "abusi di linguaggio" come quello consistente nel parlare di elementi di una struttura invece che di elementi del sostegno di tale struttura.

D15:B.05 È opportuno segnalare altri monoidi. 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: $\langle \mathcal{B}(S \times S), \circ, \mathrm{Id}_S\rangle$.
Accanto ad un tale monoide si può considerare quello costituito dalle matrici binarie quadrate di aspetto $S \times S$, dal loro prodotto $*$ basato sulle due operazioni $\cdot$ e $+_2$ e dalla matrice unità di aspetto $S \times S$ Idm_S: questo monoide $\langle \mathbf{Mat}_{S;\mathbb{B}}, *, Idm_S\rangle$ 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 $\langle \mathbb{Z}_m, \cdot_m, 1\rangle$ (v. A18:).

D15:B.06 Consideriamo un monoide $\boldsymbol{M}$=$\langle M, \odot, \mathbf{1}\rangle$ ed un suo elemento $a \in M$. Si dice **inverso** di a un elemento $a' \in M$ t.c. $a \odot a' = a' \odot a = \mathbf{1}$.

(1) Prop. Un elemento inverso 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 $a' = a''$ ∎

D15:B.07 Un elemento a di un monoide si dice **invertibile** sse possiede l'inverso.
Indichiamo $Invelm(\boldsymbol{M})$ l'insieme degli elementi invertibili del monoide $\boldsymbol{M}$. Evidentemente $\imath(\mathbf{1}) = \mathbf{1}$ cioè $\mathbf{1} \in Invelm(\boldsymbol{M})$.
Il passaggio all'inverso è una funzione dell'insieme $\{Invelm(\boldsymbol{M}) \longmapsto M\}$ che indicheremo con $\imath$; inoltre denotiamo l'inverso di un elemento a con la notazione funzionale $\imath(a)$.

Riscriviamo $a \odot \imath(a) = \imath(a) \odot a = \mathbf{1}$ le due uguaglianze che individuano l'inverso. Esse dicono che anche $\imath(a)$ è invertibile e che il suo inverso è a; quindi $(\imath(\imath(a)) = a$.
Dunque possiamo scrivere $\imath \in \{Invelm(\boldsymbol{M}) \lhd\!\!\longrightarrow\!\!\rhd Invelm(\boldsymbol{M})\}$; 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**.

D15:B.08 Prop. Il prodotto di due elementi invertibili di un monoide a e b è anch'esso invertibile e si ha $\imath(a \odot b) = \imath(b) \odot \imath(a)$.
Dim.: Se a e b sono invertibili $(a \odot b) \odot (\imath(b) \odot \imath(a)) = a \odot \mathbf{1} \odot \imath(a) = \mathbf{1}$, e $(\imath(b) \odot \imath(a)) \odot (a \odot b) = \imath(b) \odot \mathbf{1} \odot b = \mathbf{1}$ ∎
Spesso per indicare l'operazione binaria di un semigruppo, anche generico, si usa il simbolo "$\cdot$" e la si chiama prodotto; inoltre nelle espressioni si adotta l'abbreviazione consistente nel trascurare lo stesso segno "$\cdot$" scrivendo ab invece di $a \cdot b$; in questi casi di solito l'inverso di a si denota con a^{-1}.

D15: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 $i \in \mathbb{Z}$ è $-i$, mentre l'inverso di $r \in \mathbb{C}_{nz}$ è $1/r$; in $\mathbb{R}_+$ ed 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 (v. A18:) si ricava che per ogni $m \in \mathbf{[}2 : +\infty\mathbf{)}$ la struttura $\langle \mathbb{Z}_m, \cdot_m, 1\rangle$ costituisce un momoide chiamato **monoide moltiplicativo delle classi di resti** modulo m. Gli elementi invertibili di tale monoide sono gli interi r primi con m, cioè t.c. $r \perp m$.
Ad esempio $\mathit{Invelm}(\mathbb{Z}_7) = \{1, 2, 3, 4, 5, 6\}$, $\mathit{Invelm}(\mathbb{Z}_8) = \{1, 3, 5, 7\}$ e $\mathit{Invelm}(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$. In generale la cardinalità di $\mathit{Invelm}(\mathbb{Z}_m)$ è dato dal valore $\Phi_{eu}(m)$ della funzione totient di Euler (v.s.).

D15:C. Gruppi

D15:C.01 Per l'invertibilità della composizione di due elementi invertibili, per ogni monoide $\boldsymbol{M}$ si ha che $\mathit{Invelm}(\boldsymbol{M})$ costituisce un sottomonoide (v. :E.05).
Per tale sottomonoide il passaggio all'inverso è una funzione definita su tutto l'insieme sostegno e più particolarmente una permutazione coincidente con la propria inversa, cioè una involuzione.

Per qualsiasi insieme S una funzione del genere $\{S \longmapsto S\}$, come l'inversione in un insieme $\mathit{Invelm}(\boldsymbol{M})$, viene detta anche **operazione unaria** o **operatore unario**; questo operatore nelle espressioni degli elementi della struttura può essere indicato:
- con una **notazione funzionale usuale**, ad esempio con $\imath(a)$;
- con un segno che precede il relativo operando, cioè con una cosiddetta **notazione prefissa**;
- con un segno che lo segue, cioè con una cosiddetta **notazione suffissa**.

La precedente scrittura $-i$ costituisce un esempio di notazione prefissa, la r^{-1} un esempio di notazione suffissa.

D15:C.02 Un monoide $\boldsymbol{M}$ nel quale ogni elemento è invertibile, cioè t.c. $M = \mathit{Invelm}(\boldsymbol{M})$, si dice costituire un **gruppo**.
Definiamo ora la specie delle strutture di gruppo basandola esplicitamente sopra una operazione binaria, una unaria ed una nullaria.

Diciamo **gruppo** una quaterna $\boldsymbol{G} = \langle G, \cdot, ^{-1}, e\rangle$ nella quale: G è un insieme (il sostegno del gruppo), $\cdot$ è una operazione binaria su G, e è un particolare elemento di 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 **abeliano** sse la sua operazione binaria è commutativa, cioè se il corrispondente monoide è abeliano.
Denoteremo **Grp** la classe dei gruppi e **GrpAb** quella dei gruppi abeliani.

D15:C.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

$\langle \mathbb{Z}, +, -, 0\rangle$, $\langle \mathbb{Q}, +, -, 0\rangle$, $\langle \mathbb{R}\mathsf{A}, +, -, 0\rangle$, $\langle \mathbb{R}\mathsf{C}, +, -, 0\rangle$, $\langle \mathbb{R}, +, -, 0\rangle$, $\langle \mathbb{C}, +, -, 0\rangle$,
$\langle \mathbb{Q}_+, \cdot, ^{-1}, 1\rangle$, $\langle \mathbb{R}\mathsf{A}_+, \cdot, ^{-1}, 1\rangle$, $\langle \mathbb{R}\mathsf{C}_+, \cdot, ^{-1}, 1\rangle$, $\langle \mathbb{R}_+, \cdot, ^{-1}, 1\rangle$, $\langle \mathbb{C}_+, \cdot, ^{-1}, 1\rangle$,
$\langle \mathbb{Q}_{nz}, \cdot, ^{-1}, 1\rangle$, $\langle \mathbb{R}\mathsf{A}_{nz}, \cdot, ^{-1}, 1\rangle$, $\langle \mathbb{R}\mathsf{C}_{nz}, \cdot, ^{-1}, 1\rangle$, $\langle \mathbb{R}_{nz}, \cdot, ^{-1}, 1\rangle$, $\langle \mathbb{C}_{nz}, \cdot, ^{-1}, 1\rangle$.

D15:C.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 fatorizzabile dal monoide moltiplicativo delle classi di resti modulo m si ricava un gruppo di ordine $\Phi_{eu}(m)$ (v. A18:D.04) 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

D15:C.05 Eserc. Trovare le tavole di moltiplicazione di *Invelm*$(\mathbb{Z}_7)$ e *Invelm*$(\mathbb{Z}_9)$.

D15:C.06 Per un generico insieme S, dal monoide delle endofunzioni, riducendo il sostegno $\{S \longmapsto S\}$ all'insieme delle funzioni invertibili si ricava il gruppo delle biiezioni di S, cioè il **gruppo delle permutazioni** dell'insieme S, detto anche **gruppo simmetrico** dell'insieme S e denotato con Sym_S.
A partire dai gruppi di permutazioni, come vedremo, si individuano vari altri gruppi di grande interesse limitandosi alle permutazioni che conservano 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 come π^{-1} e le loro composizioni come $\pi \circ \rho$.
Dai monoidi liberi non si ricavano gruppi interessanti, in quanto presentano come unico elemento invertibile la stringa muta.

D15:C.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 $\boldsymbol{G} = \langle G, \cdot, ^{-1}, e\rangle$ t.c. $\langle G, \cdot, e\rangle \in$ **Mnd** e $^{-1}$ è una operazione unaria su G t.c.

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

D15:D. Specie di strutture algebriche

D15:D.01 Magmi, semigruppi, monoidi e gruppi sono esempi di **strutture algebriche monosostegno**. 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 **insieme sostegno** di $\boldsymbol{S}$, i β_i denotano operazioni binarie su S, gli y_i individuano operatori unari di S ed i ν_i sono elementi particolari di S. Questa definizione comprende una vastissima varietà di oggetti matematici, la gran parte dei quali di 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).

D15:D.02 Può essere utile anche studiare strutture algebriche muniti di operazioni che richiedono 3, 4, ... operandi, cioè, se con S denotiamo il sostegno, muniti di funzioni dei tipi $\{S^3 \longmapsto S\}$, $\{S^4 \longmapsto S\}$, ...; in questi casi, non molto studiati, si parla di **operazioni ternarie**, **quaternarie**, ...
Il numero degli operandi richiesti da una operazione viene chiamata **arietà** della stessa.
Incontreremo anche importanti strutture basate su più insiemi, cioè **strutture algebriche multisostegno**.

Una struttura algebrica è quindi un sistema formale individuato da uno o più insiemi sostegno, 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 insieme sostegno o di loro determinati sottoinsiemi.

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

D15:D.03 Si possono trattare anche sistemi algebrici muniti di operazioni definite in sottoinsiemi dei propri sostegni o dei loro prodotti cartesiani. Ad es. una struttura dotata di un solo sostegno S si può dotare di operatori unari definiti su un sottinsieme proprio di S e/o di operazioni binarie definite su un sottinsieme proprio di $S \times S$. In uno di questi casi si parla di **struttura dotata di operazioni parziali**.
Si considerano anche strutture dotate di operazioni che forniscono non singoli elementi ma insiemi di elementi degli insiemi sostegno. In uno di questi casi si parla di **struttura dotata di operazioni larghe**.
Alcune di queste strutture vengono munite anche di relazioni. Per trattare molti problemi combinatorici, computazionali e di elaborazione delle informazioni, e quindi per affrontare molte applicazioni, risultano utili strutture nelle quali compaiono relazioni, eventualmente accanto ad 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 tipicamente costituiscono arricchimenti delle più semplici strutture relazionali, cioè dei digrafi (Cap. D27:). Una distinzione importante fra le specie di strutture riguarda le cosiddette **strutture equazionali**, strutture i cui assiomi sono espressi esclusivamente da equazioni.
Alcune di queste strutture sono caratterizzate da sottoinsiemi degli insiemi sostegno e da proprietà espresse da relazioni ed in genere per esse le equazioni non svolgono ruoli di primo piano. Talora però fra 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 (v. D5?, ...).

D15:D.04 Diciamo **schema costitutivo** 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 sostegno, sono munite di operazioni delle stesse arietà e soddisfano richieste formalmente uguali, fornite dalle stesse equazioni o da enunciati equivalenti. Le collezioni dei magmi, dei semigruppi, dei monoidi, dei quasigruppi, dei gruppi, dei magmi abeliani, ... dei gruppi abeliani costituiscono esempi di specie di strutture algebriche monosostegno.

Più in generale si considerano le **specie di strutture matematiche**, collezioni di strutture che seguono uno stesso schema costitutivo e soddisfano agli stessi assiomi. Si possono ad es. considerare 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, specie delle involuzioni, specie delle involuzioni su insiemi di n elementi. Le specie su insiemi di cardinalità finita sono gli oggetti centrali per le indagini combinatoriche.

D15:D.05 Una **specie di struttura** $\mathcal{S}_1$ si dice **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 più povera** della $\mathcal{S}_1$. Nel primo schema potrebbero intervenire più insiemi sostegno e/o più operazioni su tali insiemi che nello schema costruttivo della seconda specie. La specie dei gruppi è più ricca della specie dei monoidi e questa è più ricca di quella dei semigruppi.

Si dice invece che una **specie di struttura** è **più stringente** di una seconda sse deve ubbidire ad un insieme di assiomi più forte, ovvero ad un sistema di assiomi equivalente ad uno più esteso.
Ad es. 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.

D15:D.06 Naturalmente tra le strutture di ogni specie è importante distinguere tra **strutture finite**, aventi insiemi sostegno finiti e quindi operazioni finite e le **strutture infinite**; tra queste si distinguono le **strutture numerabili** aventi sostegni 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 sostegno ed 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 sostegno e delle leggi di composizione, ovvero delle tavole di Cayley.

D15:E. Prodotti di strutture e sottostrutture

D15:E.01 Introduciamo ora una costruzione che consente di ricavare nuove strutture da strutture note. 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 tali magmi il sistema
$\boldsymbol{M}_1 \times \boldsymbol{M}_2 := \langle M_1 \times M_2, \odot_1 \times \odot_2 \rangle$,
il cui secondo membro è l'operazione binaria definita da

$$\langle a_1, a_2 \rangle (\odot_1 \times \odot_2) \langle b_1, b_2 \rangle := \langle a_1 \odot_1 b_1, a_2 \odot_2 b_2 \rangle \quad \text{per } a_1, b_1 \in S_1 \ , \ a_2, b_2 \in S_2.$$

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 risulta 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

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

Si ha ad esempio il magma dato dall'insieme delle successioni di numeri razionali $\{\mathbb{N} \longmapsto \mathbb{Q}\}$ e dalla somma termine a termine delle successioni.

D15:E.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 vedere che $\langle \mathbf{1}_1, \mathbf{1}_2\rangle$ 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 $\langle \mathbb{N}^2, \mathsf{+}, \langle 0, 0\rangle\rangle$, dove $\mathsf{+}$ denota la somma termine a termine delle coppie di numeri o in generale la somma componente per componente delle sequenze numeriche della stessa lunghezza.

D15:E.03 Si dice **prodotto diretto** di due gruppi $\boldsymbol{G}_1 = \langle G_1, \odot_1, \imath_1, e_1\rangle$ e $\boldsymbol{G}_2 = \langle G_2, \odot_2, \imath_2, e_2\rangle$ la struttura

$$\boldsymbol{G}_1 \times \boldsymbol{G}_2 := \big\langle G_1 \times G_2, \odot_1 \times \odot_2, \imath_1 \times \imath_2, \langle e_1, e_2\rangle\big\rangle \ ,$$

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

$$\imath_1 \times \imath_2 := \ulcorner\, \langle a_1, a_2\rangle \in G_1 \times G_2 \mapsto \langle \imath_1(a_1), \imath_2(a_2)\rangle \,\urcorner \ .$$

Si verifica che questa costruzione porta ad un nuovo gruppo.
In particolare si hanno i gruppi $\big\langle \mathbb{Z}^2, \mathsf{+}, \mathsf{-}, \langle 0, 0\rangle\big\rangle$, $\big\langle \mathbb{R}^2, \mathsf{+}, \mathsf{-}, \langle 0, 0\rangle\big\rangle$ e $\big\langle \mathbb{C}^2, \mathsf{+}, \mathsf{-}, \langle 0, 0\rangle\big\rangle$, dove $\mathsf{-}$ è l'operatore unario per coppie di numeri definito da $\mathsf{-}\langle z_1, z_2\rangle := \langle -z_1, -z_2\rangle$; questi si possono chiamare **gruppo additivo dei vettori piani a coordinate**, rispettivamente, **intere**, **reali** e **complesse**.

D15:E.04 Le diverse generalizzazioni di prodotto diretto si possono applicare anche a monoidi e gruppi. Si hanno ad es. monoidi come $\langle \mathbb{N}^n, \mathsf{+}, \langle 0, ..., 0\rangle\rangle$ e gruppi come il **gruppo additivo dei vettori n–dimensionali reali** $\big\langle \mathbb{R}^n, \mathsf{+}, \mathsf{-}, \langle 0, ..., 0\rangle\big\rangle$.

Visto come si possono comporre "cartesianamente" le operazioni delle diverse arietà, si intuisce 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 sostegno un insieme costruibile e sono dotati di operazioni costruibili, e di conseguenza costituiscono anch'essi strutture algebriche costruibili.

D15:E.05 Introduciamo altre nozioni di portata generale per le strutture considerate in precedenza.
Relativamente ad un magma $\boldsymbol{M} = \langle M, \odot\rangle$, un sottinsieme $N \subseteq M$ si dice **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 $\langle N, \odot'\rangle$ con N sottoinsieme di M chiuso rispetto alla operazione $\odot$ e ad $\odot' := \odot_{\mathrm{R}_N}$, riduzione ad N dell'operazione $\odot$. La richiesta di chiusura di N si può anche esprimere scrivendo $N \odot N \subseteq N$; qui si è considerata la cosiddetta **estensione booleana** dell'operazione $\odot$, operazione definita per due sottoinsiemi N e P di M ponendo $N \odot^{be} P := \{a \in N, b \in P | a \odot b\}$.
Ogni sottomagma di un magma è esso stesso un magma. Per indicare che N è sottomagma di M, ovvero che è sostegno di un sottomagma del magma avente M come sostegno, si scrive $N \leq_{Mgm} M$; per indicare che N è sottomagma proprio di M, cioè che $N \leq_{Mgm} M$ e che $N \subset M$, si scrive $N <_{Mgm} M$.
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**.
Si dice **sottomonoide** di un monoide $\langle M, \cdot, \mathbf{1}\rangle$ ogni suo sottosemigruppo N (cioè ogni suo sottomagma) contenente l'unità. N viene quindi caratterizzato dalle relazioni $N \odot N \subseteq N$ e $\mathbf{1} \in N$; da queste si ricava facilmente $N \odot N = N$.

D15:E.06 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 ad un certo insieme S, $\langle\{S \longmapsto S\}, \circ, \mathrm{Id}_S\rangle$ è sottomonoide del monoide delle relazioni su S, $\langle\mathcal{B}(S \times S), \circ, \mathrm{Id}_S\rangle$.

Dal fatto che l'insieme delle biiezioni di un certo insieme S è chiuso rispetto alla composizione si deduce che $\langle\{S \lhd\!\!\longrightarrow\!\!\rhd S\}, \circ, \mathrm{Id}_S\rangle$ 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 ha $\langle(A^k)^*, \cdot, \mu\rangle <_{Mnd} \langle A^*, \cdot, \mu\rangle$.

D15:E.07 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 sottinsieme di G chiuso rispetto alle operazioni $\odot$, ${}^{-1}$ ed e. Essere chiuso rispetto ad un'operazione unaria come ${}^{-1}$ corrisponde all'essere invariante rispetto al passaggio all'inverso; questo fatto, servendosi della estensione della funzione ${}^{-1}$ ai sottoinsiemi di G, si esprime efficacemente scrivendo $H^{-1} \subseteq H$); essere chiuso rispetto ad una operazione nullaria come $e \in G$ significa contenere tale elemento, $e \in G$.

Da $HH^{-1} = H$ discende $e \in H^{-1}$ e quindi $e \in H$ e $H^{-1} \supseteq H$; ma essendo $|H| = |H^{-1}|$ deve essere $H^{-1} = H$.

D15:E.08 In generale per ogni struttura algebrica monosostegno si dice **sottostruttura** ogni sottoinsieme dell'insieme sostegno chiuso rispetto alle operazioni che caratterizzano la struttura stessa.

Un modo di procedere per individuare sottostrutture di una struttura monosostegno $\boldsymbol{M} = \langle M, ...\rangle$ consiste nel considerare un sottoinsieme $H \subset M$ e nel procedere ad ampliarlo aggiungendogli le operazioni nullarie eventualmente non appartenenti ad H ed i risultati delle operazioni unarie e binarie su operandi facenti parte di H e dei suoi successivi ampliamenti. Se si riesce ad 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 una sottostruttura. Osserviamo che queste indicazioni conducono ad un procedimento costruttivo solo quando le manovre indicate si sanno effettuare concretamente e questo dipende dalle caratteristiche costruttive della struttura $\boldsymbol{M}$ e del sottoinsieme H.

D15:E.09 La precedente costruzione di ampliamento di un generico sottoinsieme K dell'insieme G sostegno di una struttura algebrica che fornisce una sottostruttura che denotiamo $\overline{K}$, 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.

La chiusura algebrica è stata definita solo per le strutture monosostegno, ma può introdursi anche per altre strutture algebriche. Peraltro essa costituisce un caso particolare della nozione generale di funzione di chiusura, funzione di insieme che risulta ampliante, isotona ed idempotente (A42:D) .

Dalle considerazioni generali sulle funzioni di chiusura, seghe 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. Essa ha come sostegno il minimo nel reticolo dei sottoinsiemi di G dei sovrainsiemi di K.

D15:F. Morfismi di strutture

D15:F.01 Introduciamo ora delle particolari funzioni tra due strutture della stessa specie monosostegno che indichiamo con $\boldsymbol{S}_j = \langle S_j, \odot_j, ..., \imath_j, ..., \nu_j, ... \rangle$ per $j = 1, 2$, dove ogni $\odot_j^{(h)}$ individua un'operazione binaria, ogni $\imath_j^{(h)}$ un'operazione unaria e ogni $\nu_j^{(h)}$ un'operazione nullaria.
Consideriamo anche una funzione $\varphi \in \{S_1 \longmapsto S_2\}$; si dice che essa **trasporta l'operazione binaria** $\odot_1^{(h)}$ sse $\quad \forall a, b \in S_1 \ : \ \varphi(a \odot_1^{(h)} b) = \varphi(a) \odot_2^{(h)} \varphi(b)$;
si dice che φ **trasporta l'operazione unaria** $\imath_1(h)$ sse $\quad \forall a \in S_1 \ : \ \varphi(\imath_1(h)(a)) = \imath_2(h)(\varphi(a))$;
si dice che φ **trasporta l'operazione nullaria** $\nu_1(h)$ sse $\quad \varphi(\nu_1(h)) = \nu_2(h)$.
Una funzione come la precedente φ si dice **morfismo di $\boldsymbol{S}_1$ in $\boldsymbol{S}_2$** sse trasporta tutte le operazioni di $\boldsymbol{S}_1$ 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; si dice **isomorfismo di $\boldsymbol{S}_1$ ed $\boldsymbol{S}_2$** un morfismo che sia una applicazione biiettiva fra S_1 ed S_2; infine si dice **automorfismo** un endomorfismo dato da una permutazione, cioè un morfismo che è sia endomorfismo che automorfismo.
Talora invece che di trasporto delle operazioni si parla di *rispetto* delle operazioni.

D15:F.02 È semplice vedere che il codominio $\varphi(S_1)$ di un morfismo φ di $\boldsymbol{S}_1$ in $\boldsymbol{S}_2$ conduce ad una sottostruttura di $\boldsymbol{S}_2$. Infatti tale insieme munito delle riduzioni delle operazioni che caratterizzano S_2 costituisce una struttura 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 $\boldsymbol{S}_2$.

D15:G. Semianelli e matrici

D15:G.01 Nelle attività matematiche ed elaborative, a partire dalle più elementari riguardanti insiemi espliciti e numeri naturali, risulta necessario disporre di almeno due operazioni binarie ben distinte. In questo paragrafo introdurremo le più generali tra le specie di strutture algebriche monosostegno munite di due operazioni.

D15:G.02 Si dice **semianello** una struttura della forma $\langle R, \oplus, \otimes \rangle$, dove $\langle R, \oplus \rangle$ è un semigruppo commutativo, $\langle R, \otimes \rangle$ è un semigruppo e la operazione $\otimes$ è **distributiva** rispetto alla $\oplus$, cioè:

$$\forall a, b, c \in R \ : \ a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c \ ,$$

$$(a \oplus b) \otimes c = a \otimes c \oplus b \otimes c \ .$$

Dopo il caso del **semianello banale** formato da un solo elemento, il più ridotto semianello è il cosiddetto **semianello binario** o **semianello dei bits**, $\langle \mathbb{B}, +_2, \cdot \rangle$, dove $\mathbb{B}$ è l'insieme dei numeri binari o bits $\{0, 1\}$ e $+_2$ è la somma booleana.
Per ogni insieme S si ha poi il **semianello booleano** $\langle \mathcal{B}(S), \cup, \cap \rangle$. Si ottengono poi semianelli numerici munendo delle ordinarie operazioni di somma e prodotto insiemi come $\mathbb{P}$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{RA}$, $\mathbb{RC}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}_+$, $\mathbb{Q}_{0,+}$, $\mathbb{R}_+$, $\mathbb{R}_{0,+}$, ...

D15:G.03 Un **semianello** si dice **commutativo** sse il suo prodotto è commutativo.
Tutti i semianelli precedenti sono commutativi.

Si dice **semianello-zerounitale** una struttura della forma $\langle R, \oplus, \mathbf{0}, \otimes, \mathbf{1}\rangle$ che costituisce un arricchimento di un semianello $\langle R, \oplus, \otimes\rangle$ con due elementi diversi del sostegno R: $\mathbf{0}$ elemento neutro per $\oplus$ e elemento assorbente bilatero per l'operazione $\otimes$, cioè t.c.

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

e $\mathbf{1}$ elemento neutro per $\otimes$. $\mathbf{0}$ e $\mathbf{1}$ sono detti, rispettivamente, **zero** e **unità** del semianello-zerounitale.
Ogni semianello booleano $\langle \mathcal{B}(S), \cup, \cap\rangle$ si può arricchire al semianello-zerounitale $\langle \mathcal{B}(S), \cup, \emptyset, \cap, S\rangle$.
Si possono arricchire a semianelli-zerounitali anche i precedenti semianelli numerici dotati di insieme sostegno contenente 0.
Altri importanti semianelli-zerounitali commutativi sono costituiti, per qualsiasi m intero $m \geq 2$, dalla classe di resti modulo m $\mathbb{Z}_m$ munita delle operazioni somma modulo m $+_m$, prodotto modulo m $\cdot_m$ dello zero $[0]_m = m\mathbb{Z}$ e dell'unità $[1]_m = m\mathbb{Z} + 1$.

D15:G.04 Denotiamo con **Srng** la classe dei semianelli, con **Srngzu** quella dei semianelli-zerounitali e con **SrngAb** e **SrngzuAb** le classi dei semianelli e dei semianelli-zerounitali commutativi.
Un sottoinsieme S del sostegno di un semianello si dice **sottosemianello** sse è chiuso rispetto alle operazioni di somma e prodotto. Un sottoinsieme S del sostegno di un semianello-zerounitale si dice **sottosemianello-zerounitale** sse è chiuso rispetto alle operazioni di somma e prodotto e contiene zero e unità.

D15:G.05 Le matrici le cui componenti sono elementi di un semianello presentano notevole interesse algebrico e computazionale. Consideriamo gli interi positivi d, e, f e g, un semianello $\boldsymbol{R} = \langle R, \oplus, \otimes\rangle$, e matrici di estensioni finite le cui linee etichettiamo con intervalli di interi come $\mathbf{(}d\mathbf{]} = \{1, ..., d\}$, $\mathbf{(}e\mathbf{]}$, $\mathbf{(}f\mathbf{]}$ o $\mathbf{(}g\mathbf{]}$. Indichiamo con $\mathbf{Mat}_{d,e}(\boldsymbol{R})$ l'insieme delle matrici di aspetto $d \times e$ su $\boldsymbol{R}$.

D15:G.06 Si definisce **somma** di due matrici di tale insieme, $A = [i \in \mathbf{(}d\mathbf{]}, j \in \mathbf{(}e\mathbf{]} :| a_{i,j}]$ e $B = [i \in \mathbf{(}d\mathbf{]}, j \in \mathbf{(}e\mathbf{]} :| b_{i,j}]$, come

$$A \oplus_{\mathsf{M}} B := \left[i \in \mathbf{(}d\mathbf{]}, j \in \mathbf{(}e\mathbf{]} :| a_{i,j} \oplus b_{i,j}\right] .$$

La somma di due matrici dello stesso aspetto, ad es. $d \times e$, non è una costruzione del tutto nuova: si può vedere come caso particolare di una somma componente per componente sulla potenza cartesiana $d \cdot e$–esima del semigruppo abeliano $\langle R, \oplus\rangle$. Accade quindi che $\mathbf{Mat}_{d,e}(\boldsymbol{R})$ munito della suddetta somma costituisce un semigruppo abeliano.

D15:G.07 Si dice **coppia di matrici conformabili** o anche **coppia di matrici moltiplicabili** sul semianello $\boldsymbol{R}$ una coppia (ordinata) di matrici t.c. le colonne della prima e le righe della seconda sono individuate dagli stessi indici.
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]** di A per B

$$A \otimes_{\mathsf{M}} B := [i \in \mathbf{(}d\mathbf{]}, k \in \mathbf{(}f\mathbf{]} :| a_{i,1} \otimes b_{1,k} \oplus ... \oplus a_{i,d} \otimes b_{d,k}] .$$

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

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

$$\forall A, B \in \mathbf{Mat}_{d,e}, \ C \in \mathbf{Mat}_{e,f} \ : \ (A \oplus_{\mathsf{M}} B) \otimes_{\mathsf{M}} C = (A \otimes_{\mathsf{M}} C) \oplus_{\mathsf{M}} (B \otimes_{\mathsf{M}} C) ,$$

$$\forall A \in \mathbf{Mat}_{d,e}, \ B, C \in \mathbf{Mat}_{e,f} \ : \ A \otimes_{\mathsf{M}} (B \oplus_{\mathsf{M}} C) = (A \otimes_{\mathsf{M}} B) \oplus_{\mathsf{M}} (A \otimes_{\mathsf{M}} C) .$$

La nozione di matrice su semianelli generalizza la nozione classica di matrice a componenti numeriche e, come vedremo, rende possibile effettuare calcoli su matrici di bits, di insiemi, di linguaggi e di matrici. Può essere utile considerare il significato del prodotto di matrici sul fondamentale semianello binario (v B4:C.).

D15:G.08 Consideriamo la collezione delle matrici sul semianello $\boldsymbol{R}$ quadrate di aspetto $d \times d$ che indichiamo, oltre che con $\mathsf{Mat}_{d,d}(\boldsymbol{R})$, con la più semplice scrittura $\mathsf{Mat}_d(\boldsymbol{R})$.
Munendo questo insieme della somma e del prodotto fra matrici sopra definiti si ottiene un semianello. Questo è detto **semianello delle matrici quadrate** $d \times d$ sul semianello $\boldsymbol{R}$.
Osserviamo che il prodotto di matrici $d \times d$ con $d > 1$, anche se definite su un semianello commutativo, non è commutativo. Ad es. si hanno le seguenti differenze per matrici booleane 2×2:

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot_{\mathsf{M}} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \cdot_{\mathsf{M}} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} ,$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot_{\mathsf{M}} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot_{\mathsf{M}} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} .$$

D15:G.09 Consideriamo un semianello-zerounitale $\boldsymbol{R} = \langle R, \oplus, \mathbf{0}, \otimes, \mathbf{1} \rangle$ la collezione delle matrici $\mathsf{Mat}_d(R)$ e tra queste la **matrice zero** $MatZr_d(\boldsymbol{R}) := [i, j \in (d] :| \mathbf{0}]$ e la **matrice unità** $MatId_d(\boldsymbol{R}) := [i, j \in (d] :| \delta_{\boldsymbol{R}}(i, j)]$; qui si è utilizzata la funzione **delta di Kronecker sul semianello-zerounitale** $\boldsymbol{R}$ definita da

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

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

$$\mathsf{Mat}_d(\boldsymbol{R}) := \big\langle \mathsf{Mat}_d(R), \oplus_{\mathsf{M}}, MatZr_d(\boldsymbol{R}), \otimes_{\mathsf{M}}, MatId_d(\boldsymbol{R}) \big\rangle \ .$$

Si dimostra che questa struttura costituisce effettivamente un semianello-zerounitale.

D15:G.10 Sulle matrici quadrate è definita un'importante involuzione, la trasposizione:

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

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

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

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

(2) Eserc. Dimostrare che la trasposta di un prodotto di matrici è il prodotto dei fattori trasposti ma nell'ordine opposto: $(A \otimes B)^{\mathsf{T}} = B^{\mathsf{T}} \otimes A^{\mathsf{T}}$.
In una tale situazione si dice che la trasposizione costituisce un **antimorfismo** dell'anello delle matrici.

D15:G.11 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 identità del semianello-zerounitale delle matrici 2×2 sul semianello-zerounitale booleano $\langle \mathcal{B}(S), \cup, \emptyset, \cap, S \rangle$.

D15:H. Anelli

D15:H.01 I semianelli si possono arricchire richiedendo che contengano uno o due elementi con proprietà ben determinate in modo da fornire strutture più stringenti e decisamente più utili. Più precisamente chiedendo la presenza di un elemento zero neutro per l'operazione commutativa somma ed assorbente per l'operazione prodotto si ottiene una struttura che, chiamiamo pseudoanello. Chiedendo anche la prezenza 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 unitale invece di anello.

Diciamo dunque **pseudoanello** una struttura $\langle R, \oplus, \ominus, \mathbf{0}, \otimes\rangle$ nella quale dove $\langle R, \oplus, \ominus, \mathbf{0}\rangle$ è un gruppo abeliano e $\langle R, \oplus, \otimes\rangle$ un semianello.
Prevedibilmente uno **pseudoanello** si dice **abeliano** o **commutativo** sse è tale il suo prodotto.
Quando il prodotto di uno pseudoanello possiede unità $\mathbf{1}$, cioè quando la terna $\langle \boldsymbol{R}, \otimes, \mathbf{1}\rangle$ costituisce un monoide, risulta utile considerare il corrispondente arricchimento della struttura precedente chiamato **anello**, struttura della forma $\langle R, \oplus, \ominus, \mathbf{0}, \otimes, \mathbf{1}\rangle$.
Un **anello** si dice **abeliano** o **commutativo** sse è tale il suo pseudoanello sottostante.
Denotiamo, rispettivamente, **Psrng**, **PsrngAb**, **Rng** e **RngAb** le classi degli pseudoanelli, degli pseudoanelli abeliani, degli anelli e degli anelli abeliani.
Osserviamo che ogni anello è costituito da almeno due elementi.

D15:H.02 Gran parte dei semianelli visti in precedenza forniscono pseudoanelli e gran parte dei semianelli zerounitali visti in precedenza forniscono 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 ottenuti similmente da $\mathbb{Q}$, $\mathbb{RA}$, $\mathbb{RC}$, $\mathbb{R}$ e $\mathbb{C}$.
Altri importanti anelli commutativi sono costituiti, per un qualsiasi intero $m \geq 2$, dalle classi di resti $\mathbb{Z}_m$ modulo m.
Per ogni intero $m = 2, 3, \ldots$ $\langle m\mathbb{Z}, +, -, 0, \cdot\rangle$ è uno pseudoanello commutativo che non può essere dotato di una unità.

D15:H.03 Un sottoinsieme S del sostegno R di uno pseudoanello $\boldsymbol{R}$ si dice **sostegno 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 sottinsieme del sostegno di un anello che, oltre ad essere chiuso rispetto a somma e prodotto, contenga l'elemento unità.
In questo caso scriviamo $S \leq_{Rng} R$.

D15:H.04 Eserc. (i) Dimostrare che per $m, k = 2, 3, \ldots$ si ha $m \cdot k \cdot \mathbb{Z} <_{Psrng} m \cdot \mathbb{Z} <_{Rng}$.
(ii) Dimostrare che $\mathbb{Z} <_{Rng} \mathbb{Q} <_{Rng} \mathbb{RA} <_{Rng} \mathbb{RC} <_{Rng} \mathbb{R} <_{Rng} \mathbb{C}$.

D15:H.05 Le matrici quadrate di ordine finito le cui componenti sono elementi di un anello costituiscono anelli ricchi di applicazioni.

A partire da un anello $\boldsymbol{R} = \langle R, \oplus, \ominus, \mathbf{0}, \otimes, \mathbf{1} \rangle$ per ogni intero positivo d si può considerare

$$\langle \mathbf{Mat}_d(\boldsymbol{R}), \oplus, \ominus, MatZr_d(\boldsymbol{R}), \otimes_{\mathsf{M}}, MatId_d(\boldsymbol{R}) \rangle \ .$$

Infatti 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 $\boldsymbol{R}$.

D15:H.06 Come si è osservato per i semianelli, gli anelli di matrici di ordine maggiore di 1 sono non commutativi anche se costruiti a partire da un anello commutativo; controesempi alla commutatività si trovano facilmente con piccole matrici con componenti intere. Ad es.

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

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

D15:H.07 Come per i monoidi, anche per i più ricchi anelli $\boldsymbol{R} = \langle R, \oplus, \ominus, \mathbf{0}, \otimes, \mathbf{1} \rangle$ hanno grande importanza gli **elementi invertibili**, cioè gli elementi invertibili per il sotostante monoide $\langle R, \otimes, \mathbf{1} \rangle$; il gruppo che essi formano si indica $Invelm(\boldsymbol{R})$.

D15:H.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**.

Consideriamo 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. In ogni pseudoanello $\mathbb{Z}_m$ con m intero naturale fattorizzabile si trovano divisori dello zero, in quanto se si può scrivere $m = r \cdot s$ con $r, s \neq 0, 1$, si ha $[r]_m \cdot_m [s]_m = [0]_m = [m]_m$.

D15:H.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 ogni anello $\mathbb{Z}_p$ con p numero primo è privo di divisori dello zero.

D15:H.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.

D15:H.11 Come per un magma $\langle R, \cdot \rangle$, per uno pseudoanello $\langle R, +, -, 0, \cdot \rangle$ si dice che vale la **legge di cancellazione** sse

$$\forall r, x, y \in R \ : \ r \neq 0 \ , \ r \cdot x = r \cdot y \Longrightarrow x = y \ .$$

Vi sono pseudoanelli nei quali la legge di cancellazione non vale. Ad esempio in $\mathbb{Z}_4$ si ha $2 \cdot_4 3 = 2 \cdot_4 1 = 2 \implies 3 = 1$.

(1) Prop. Sia $\boldsymbol{R}$ un anello abeliano. $\boldsymbol{R}$ è un dominio di integrità $\Longrightarrow$ per $\boldsymbol{R}$ 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 nei quali sono possibili elaborazioni di rilevante utilità.

D15:H.12 Come per un magma dotato di uno zero 0, un elemento q diverso dallo zero di uno pseudoanello $\boldsymbol{R}$ viene chiamato **elemento nilpotente** sse si trova un intero positivo h t.c. 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 unitale o 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** h (talora si dice che 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, 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.

D15:H.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. In formule:

$$\mathbf{Krp} := \{\boldsymbol{R} = \langle R, \oplus, \ominus, \mathbf{0}, \otimes, \mathbf{1}\rangle \in \mathbf{Rng} \;\; t.c. \;\; \langle R \setminus 0, \otimes, inv(\otimes), \mathbf{1}\rangle \in \mathbf{Grp}\}$$

$$\boldsymbol{R} = \langle R, \oplus, \ominus, \mathbf{0}, \otimes, \mathbf{1}\rangle \in \mathbf{Rng} \;,\; \langle R \setminus 0, \otimes, inv(\otimes), \mathbf{1}\rangle \in \mathbf{Grp} \implies \boldsymbol{R} \in \mathbf{Krp} \;.$$

L'anello binario $\langle \mathbb{B}, +_2, +_2, 0, \cdot, 1\rangle$, oltre ad essere l'anello più piccolo, è il corpo più piccolo.
L'insieme degli elementi del corpo $\boldsymbol{R}$ diversi dallo zero, prende il nome di **gruppo moltiplicativo** di $\boldsymbol{R}$; spesso si denota localmente con $\boldsymbol{R}^\times$.
Un corpo in cui il prodotto sia commutativo viene detto **corpo commutativo** o **campo**. Un corpo non commutativo viene anche chiamato **corpo sghembo** (*skewfield*).
Denotiamo con **Fld** la classe dei campi e con **KrpNab** la classe dei corpi sghembi.

C4:I. Ideali

D15:I.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 di un anello** $\boldsymbol{R}$ un sottoinsieme I che soddisfa queste condizioni:
(I1) I è sottogruppo del gruppo additivo $\boldsymbol{R}_{ag}$;
(I2) è chiuso rispetto alla sottrazione, cioè $\forall a, b \in I \;:\; a - b \in I$;
(I3) $\forall a \in I,\ \forall r \in R \;:\; a \cdot r \in I \;,\; r \cdot a \in I$.
La stessa definizione vale per gli pseudoanelli.

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 costituiti l'uno costituito dal solo zero di R e l'altro coincidente con l'intero sostegno; essi sono detti rispettivamente **ideale nullo** e **ideale improprio** di $\boldsymbol{R}$. Ogni altro ideale, ammesso che esista, viene chiamato **ideale proprio**.
Denotiamo $Idl(\boldsymbol{R})$ la collezione degli ideali dell'anello $\boldsymbol{R}$.

D15:I.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 $< p(x) >:= \{q(x)p(x) \ \ |: \ q(x) \in \boldsymbol{F}[x]\}$, è un ideale in $\boldsymbol{F}[x]$.

D15:I.03 Prop. Ogni ideale I di uno pseudoanello o di un anello $\boldsymbol{R}$ contiene lo zero di questa struttura.
Dim.: Questo discende subito da (I2) ∎

D15:I.04 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 $\boldsymbol{R}$ ed un qualsiasi elemento $r \in R$ non contenuto in I, se $\mathbf{1}$ è 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 ∎

D15:I.05 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 l'inverso di i, i^{-1} e quindi anche $i^{-1} \cdot i = i \cdot i^{-1} = \mathbf{1}$, fatto in contrasto con la precedente proposizione ∎

D15:I.06 Prop. Consideriamo un anello $\boldsymbol{R}$, un suo sottoinsieme $S = \{s_1, ..., s_n >\}$ ed il sottoinsieme
$$< S >:= \cup_{\{s_1,...,s_n>\} \subseteq S} \{r_1, ..., r_n \in R :| \ r_1 s_1 + ... + r_n s_n\} \ .$$
Questo è 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, si ha $< S > \supseteq S$; inoltre dalla sua espressione si ricava facilmente che soddisfa le tre richieste (I1), (I2) ed (I3) ∎

Il precedente ideale è chiamato **ideale generato** da S

D15:I.07 Prop. Sono particolarmente interessanti gli ideali generati da un singoletto, cioè da un solo elemento s dell'anello $\boldsymbol{R}$, ideali aventi la forma $< s >= \{r \cdot s \ \ |: \ r \in R\}$ per qualche elemento $s \in R$; un tale ideale è chiamato **ideale principale**.

D15:I.08 (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 (I1) è soddisfatta in quanto anche l'intersezione di due sottogruppi è sottogruppo. Per la richiesta (I2) 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 (I3) ∎

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

(2) Prop. Consideriamo una famiglia di ideali di $\boldsymbol{R}$ pseudoanello o anello 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 $\boldsymbol{R}$ ∎

D15:I.09 Prop. Sia $I_1 \subset I_2 \subset ...$ è una successione ascendente di ideali, ognuno dei quali contenuto nel successivo; anche la loro unione $\bigcup\{j \in J \ :| \ I_j\}$ è un ideale.
Dim.: . . . . .

D15:I.10 Un dominio di integrità $\boldsymbol{R}$ in cui ogni ideale è principale è detto **dominio ad ideali principali**.

D15:I.11 Prop. Un qualunque campo $\boldsymbol{F}$ è un anello ad ideali principali.
Dim.: $\boldsymbol{F}$ è un anello commutativo che possiede soltanto i due ideali impropri 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 ad ideali principali. Infatti, ogni ideale I è generato dal più piccolo intero positivo m che è contenuto in I, cioè ha la forma $< m >$.
Anche l'anello $\boldsymbol{F}[x]$ è un dominio ad ideali principali. Infatti ogni ideale I è generato dall'unico polinomio monico contenuto in I eed avente grado minimo.

D15:I.12 Si dice **ideale massimale di un anello $\boldsymbol{R}$** un suo ideale I che soddisfa le due seguenti condizioni:
(IM1) I è incluso propriamente in R;
(IM2) I non è incluso propriamente in alcun ideale proprio di $\boldsymbol{R}$ diverso da I.

Ad es., se $\boldsymbol{K}$ è un corpo, l'ideale $< 0 >$ costituito dal solo zero di K è massimale, perché un corpo non possiede ideali propri.

D15:I.13 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 sta in I.

D15:I.14 Prop. Sia I un ideale di un anello commutativo $\boldsymbol{R}$. Se I è ideale massimale, esso è anche un ideale primo.

D15:I.15 Si chiama **radicale di un ideale** I di un anello $\boldsymbol{R}$, e lo si indica con $\mathsf{Rdcl}(I)$, il sottoinsieme di $\boldsymbol{R}$ costituito dagli elementi b di R, tali che $b^h \in I$ per qualche esponente intero positivo h.
Il radicale di I contiene I, in quanto per ogni $b \in I$, risulta $b^1 \in I$.

D15:I.16 Prop. Il radicale di un ideale I di un anello $\boldsymbol{R}$ commutativo è anch'esso un'ideale di $\boldsymbol{R}$.

D15:I.17 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, cioè b appartiene al radicale di I.

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

D15:J. Campi

D15:J.01 Un campo è una struttura della forma $\boldsymbol{F} = \langle F, +, -, 0, \cdot, ^{-1}, 1\rangle$ t.c. $\langle F, +, -, 0\rangle$ e $\langle F \backslash 0, \cdot, ^{-1}, 1\rangle$ sono gruppi commutativi e il prodotto $\cdot$ è distributivo rispetto alla somma $+$. I due gruppi citati sono detti **gruppo additivo** e **gruppo moltiplicativo** del campo $\boldsymbol{F}$.
Denotiamo **FldF** la classe dei campi finiti.

D15:J.02 Campi numerabili sono forniti dagli insiemi $\mathbb{Q}$ dei numeri razionali relativi, $\mathbb{RA}$ dei numeri algebrici e $\mathbb{RC}$; 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:

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

D15:J.03 Sono molto importanti anche i campi finiti che, come vedremo, si possono classificare completamente con relativa facilità.
In particolare sono campi finiti gli anelli della forma $\mathbb{Z}_p$ con p numero primo; tra gli anelli $\mathbb{Z}_m$ con $m = 2, 3, 4, ...$ essi sono i soli campi.

D15:J.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 t.c. $a \cdot b = 0$, allora o $a = 0$ o $b = 0$.

Dim.: Se fosse $a \neq 0$ esisterebbe a^{-1}; quindi sarebbe $a^{-1} \cdot (a \cdot b) = 0$, cioè $b = 0$; simmetricamente si 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 gli elementi fanno dei campi delle piattaforme computazionali molto efficaci.

D15:J.05 Segnaliamo alcune proprietà dei corpi.

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

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

(3) Teorema Ogni corpo finito è un campo.

C4:.K Campi finiti

D15:K.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 individuati algoritmi piuttosto complessi.

D15:K.02 Vediamo ora quali possono essere le cardinalità 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 indichiamo $\langle 1 \rangle_+$

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 $\boldsymbol{F}$**. Ad es. 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 $k \cdot 1 = 0$.

D15:K.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 $c \cdot 1 = \underbrace{1 + \cdots + 1}_{c-volte} = 0$. Ad 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 indicare la caratteristica di $\boldsymbol{R}$ si usa la scrittura $char(\boldsymbol{R})$.
Se $char(\boldsymbol{R}) = c$, allora $\forall r \in R$, si ha che: $c \cdot r = \underbrace{r + \cdots + r}_{c-volte} = \underbrace{(1 + \cdots + 1)}_{c-volte} \cdot r = 0 \cdot r = 0$.

D15:K.04 Sia $\boldsymbol{F}$ un campo dotato di almeno due elementi. Se gli elementi di $\boldsymbol{F}$ hanno tutti caratteristica maggiore di zero, e se l'insieme di dette caratteristiche ammette un massimo finito n, si dice che $\boldsymbol{F}$ è un **campo di caratteristica** n; in caso contrario si dice che $\boldsymbol{F}$ è un **campo di caratteristica zero**.

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

D15:K.05 Prop. Un campo F di caratteristica zero è infinito.
Dim.: ∎

D15:K.06 Prop. Ogni anello finito ha caratteristica diversa da zero.
Dim.: ∎

D15:K.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 $m_1 = 0$ o $m_2 = 0$, contro la minimalità richesta per la caratteristica ∎

D15:K.08 Prop. Il gruppo additivo di un campo finito di caratteristica p è isomorfo ad 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 F, $\langle a \rangle_+ := \{a, 2a, 3a, ...\}$; dato che $p = 0$ in 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 $\langle h_1, h_2, ..., h_s \rangle \in F^s$. Un generatore individuabile banalmente è F stesso; naturalmente tra i generatori sono più pregevoli i minimali rispetto all'inclusione; sia $\{f_1, ..., f_r\}$ 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 $f_i = (a_i - b_i)^{-1}((b_{i+1} - a_{i+1}) f_{i+1} + ... + (b_n - a_n) f_n)$, contro l'ipotesi di minimalità di $\{f_1, ..., f_r\}$. Quindi vi è una biiezione fra 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 delle r–uple di ${\mathbb{Z}_p}^r$, si ha un isomorfismo fra il gruppo additivo di F e ${\boldsymbol{Cycl}_p}^r$ ∎

(1) Cor. Ogni campo finito ha come cardinalità una potenza di un numero primo ∎

D15:K.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 $\sim_k$ chiedendo:

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

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

$$f_1(x) \sim_k g_1(x),\ f_2(x) \sim_k g_2(x) \implies f_1(x) + f_2(x) \sim_k g_1(x) + g_2(x),\ f_1(x) \cdot f_2(x) \sim_k g_1(x) \cdot g_2(x)$$

In questo caso si parla di **congruenza** sul campo $\mathbb{Z}_p$. Si può quindi considerare l'insieme quoziente $\mathbb{Z}_p/\sim_k$; ogni suo elemento, cioè ogni classe dell'equivalenza $\sim_k$, si può denotare $[f(x)]_k$ servendosi di un qualsiasi polinomio $f(x)$ che le appartiene.
Su $\mathbb{Z}_p/\sim_k$ si possono definire le operazioni di somma $+_k$ e prodotto $\cdot_k$ ponendo

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

D15:K.10 Prop. Il sistema $\langle \mathbb{Z}_p/\sim_k, +_k, -_k, [0], \cdot_k, [1] \rangle$ 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 poi routinario dimostrare che $\mathbb{Z}_p[x]/\sim_k$ munito di somma e prodotto costituisce un anello commutativo unitale.
Questi risultati non dipendono dalla irriducibilità di $k(x)$. Resta quindi da mostrare 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 $\mathrm{MCD}(f(x), k(x)) = 1$; quindi, per C4:1.10, si trovano $a(x), b(x) \in \mathbb{Z}_p[x]$ t.c. $f(x)a(x) + k(x)b(x) = 1$; passando 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.

D15:K.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 e scriviamo $F_g := F \setminus \{0\}$. Per ogni $f \in F_g$ 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 ∎
D15:K.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 $f \in F_g$ 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 ∎

D15:K.13 Si dice **elemento primitivo di un campo $\boldsymbol{F}$** un suo g in grado di generare l'intero F_g:

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

La proposizione precedente può dunque riformularsi come segue.

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

D15:K.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 questo problema non è risolvibile senza 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 per tentativi. Si dispone anche di tavole piuttosto ampie, sia per i campi $\mathbb{Z}_p$ che per i campi $\mathbb{Z}_q[x]$.

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.

D15:K.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 si indica con $\mathbb{F}_q$ o con $GF(q)$. Naturalmente per $r = 1$ si ha $\mathbb{F}_p = \mathbb{Z}_p$.