Capitolo B41:
Strutture algebriche 1

B41:0.a In matematica hanno grande importanza, in particolare per il loro ruolo nella organizzazione formale dei risultati le **strutture algebriche**. Queste entità sono costituite da insiemi che chiamiamo **insiemi sostegno** (che possono essere finiti, numerabili, continui o di altra natura), e da operazioni tra gli elementi di questi insiemi caratterizzate da determinate proprietà formali. Due strutture che presentano la stessa organizzazione per i sostegni e le operazioni e con le stesse richieste per le operazioni, quale che sia la natura degli insiemi sostegno, si dicono appartenere alla stessa **specie di strutture**.
In questo capitolo si introducono solo specie di strutture algebriche che si servono di un solo insieme sostegno. Le prime due, i semigruppi e i gruppi, presentano una sola operazione binaria. Ai semigruppi si chiede solo di essere muniti di un'operazione associativa e questo consente di individuare facilmente semigruppi costituiti da enti matematici assai generici come stringhe, numeri, relazioni e funzioni. I gruppi si possono considerare semigruppi dotati di un'operazione dotata di inversa, proprietà che rende i gruppi in grado di affrontare e chiarire un gran numero di problemi: si noti in particolare che con le endofunzioni di un dato insieme si costituisce un semigruppo, mentre con le endofunzioni invertibili si costruisce un gruppo.
Vengono poi introdotti gli anelli, strutture più ricche delle precedenti in quanto basate sopre un solo insieme sostegno, ma munite di due operazioni di cui solo una dotata di inversa, le quali in particolare si concretizzano nella somma e nel prodotto per i numeri interi; la seconda operazione rende gli anelli strumenti di maggiore portata. Per ultimi si introducono i campi, strutture che si possono vedere come anelli particolarmente versatili, ancora grazie alla disponibilità di una inversa per entrambe le operazioni.

B41:1. Semigruppi

B41:1.a Diciamo **semigruppo** una [[struttura algebrica]] costituita da un insieme non vuoto munito di un'operazione binaria associativa. Formalmente un semigruppo è una coppia $\langle A, * \rangle$ con A insieme non vuoto ed $*$ operazione binaria associativa su A, cioè funzione del genere $* \in \{A \times A \longmapsto A\}$ tale che

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

Si incontrano molti semigruppi finiti e infiniti facilmente definibili.
(1) L'insieme dei numeri interi positivi munito dell'addizione (operazione notoriamente associativa); tale struttura viene detta **semigruppo additivo degli interi positivi**.
(2) L'insieme dei numeri interi naturali munito della moltiplicazione (anche questa operazione è notoriamente associativa); tale struttura viene detta **monoide moltiplicativo degli interi naturali**.
(3) L'insieme $\{1, 2, 3, 4\}$ munito della operazione "scelta del massimo tra due numeri" che possiamo scrivere $\max(m, n)$: per l'associatività basta osservare che, evidentemente, sia $\max(\max(m, n), p)$ che $\max(m, \max(n, p))$ individuano il maggiore dei tre numeri m, n e p; questo rende lecito denotare tale numero con $\max(m, n, p)$.

(4) L'insieme finito di tutte le endofunzioni definite entro un qualsiasi insieme S, ad esempio entro $\{1,2,3,4\}$, munito della composizione di funzioni; anche questa operazione è evidentemente associativa.
(5) L'insieme, numerabile, di tutte le stringhe di lunghezza positiva sopra un dato alfabeto $\mathcal{A}$ dotato della giustapposizione fra stringhe; questa struttura si chiama **semigruppo libero** su $\mathcal{A}$.
(6) La collezione dei sottoinsiemi di un qualsiasi insieme munita dell'operazione di unione (operazione evidentemente associativa).
(7) La collezione dei sottoinsiemi di un qualsiasi insieme munita dell'operazione di intersezione (operazione notoriamente associativa).

B41:1.b Il semigruppo (3) ha 4 elementi e la sua tavola di moltiplicazione consiste nella matrice

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

La simmetria della matrice rende evidente che si ha un'operazione commutativa. In un caso come questo si parla di **semigruppo commutativo** o **semigruppo abeliano**. Anche i semigruppi (1), (2) e (6) sono commutativi.
Non è invece commutativo il semigruppo libero (5), in quanto la giustapposizione non è commutativa. Non è commutativo neppure il semigruppo di tutte le endofunzioni di un qualsiasi insieme ambiente S formato da 2 o più elementi. Per questo basta considerare il controesempio di due endofunzioni che non commutano. consideriamo due elementi diversi di S x e y e le corrispondenti funzioni a valore costante x^{cstnt} e y^{cstnt} che conviene considerare come trasformazioni postfisse, da scrivere a destra dell'argomento e quindi definire mediante la $\forall z = 1,2,3,4 : z\, x^{cstnt} := x$ (equivalente alla $x^{cstnt}(z) := x$) . Con tale notazione risulta chiaro che per le due composizioni delle due endofunzioni si ha

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

B41:1.c Un semigruppo dotato di un elemento neutro, cioè un cosiddetto **semigruppo unitale**, viene chiamato **[[monoide]]**.
Sono monoidi: il semigruppo (2) (il numero 21 essendo l'elemento neutro), il semigruppo (3) (elemento neutro è il numeo minimo), il semigruppo (4) (elemento neutro è la funzione identità), il semigruppo (6) (elemento neutro è l'insieme vuoto), il semigruppo (7) (elemento neutro è l'insieme ambiente).

Ogni semigruppo S può venire associato ad un monoide semplicemente aggiungendogli un elemento e scelto fuori da S e definendo $e * e := e$, $e * s := s =: s * e$ per ogni $s \in S$.
Viceversa dato un monoide lo si riduce a semigruppo eliminando semplicemente l'elemento neutro, nonché la riga e la colonna corrispondenti della tavola di moltiplicazione. Dunque lo studio dei monoidi aggiunge ben poco allo studio dei semigruppi: le due specie di strutture sono sostanzialmente equivalenti.
Coppie semigruppo - monoide associato sono ad esempio:
Semigruppo additivo degli interi positivi – monoide additivo degli interi naturali.
Semigruppo libero delle stringhe su $\mathcal{A}$, non includente la μ – monoide libero delle stringhe su $\mathcal{A}$, μ inclusa.

B41:2. Gruppi

B41:2.a I gruppi possono considerarsi semigruppi molto particolari e la [[teoria dei gruppi]] è una parte della matematica particolarmente ricca di risultati che si rivela in grado di fornire efficaci strumenti a molte altre parti della matematica e delle sue applicazioni: in particolare ha un ruolo importante nella [[meccanica classica]], nella [[meccanica quantistica]], nella [[strutturistica chimica]] e nella [[cristallografia]].

Un efficace approccio costruttivo ai gruppi consiste nel considerarli come sottoinsiemi "privilegiati" di insiemi di trasformazioni in se di un insieme ambiente S per il quale non poniamo nessuna restrizione. Il primo "pregio" che richiediamo alle trasformazioni che costituiscono un gruppo consiste nel possedere inverso: si vede facilmente che questo pregio si mantiene con la composizione delle trasformazioni e di conseguenza le trasformazioni di un insieme S che sono invertibili si possono comporre senza restrizioni. Tra le endofunzioni di un insieme S qualsiasi sono le biiezioni tutte e sole quelle che posseggono inverso. Tra le biiezioni di S va considerata anche la trasformazione identità Id_S ottenibile come composizione di una qualsiasi biezione con la sua inversa. Siamo quindi indotti a considerare una struttura della forma $\langle \{S \lhd\!\!\rightarrow\!\!\rhd S\}, \circ, {}^{-\mathbf{1}}, \mathrm{Id}_S \rangle$ costituita da trasformazioni invertibili.
Esso è detto **gruppo totale delle permutazioni** di S o **gruppo simmetrico** di S e viene denotato $\mathrm{S}ym_S$.

B41:2.b Dei gruppi si possono dare varie definizioni formali; qui ne diamo una che non è la più compatta e presenta qualche ridondanza, ma che si può utilizzare abbastanza facilmente.
Si dice **gruppo** una struttura della forma $\boldsymbol{G} = \langle G, \odot, {}^{-1}, e \rangle$ dove

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

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

B41:2.c Vediamo ora alcuni gruppi costituiti da pochi elementi. Questi gruppi si possono individuare dando esplicitamente le loro **tavola di Cayley**, cioè la rappresentazione sotto forma di matrice dell'operazione prodotto.
I gruppi di due e tre elementi sostanzialmente si riducono ai due caratterizzati dalle seguenti tavole di Cayley

$$\begin{array}{cc|cc} & & 1 & -1 \\ \hline 1 & & 1 & -1 \\ -1 & & -1 & 1 \end{array} \qquad \begin{array}{c|ccc} & e & a & b \\ \hline e & e & a & b \\ a & a & b & e \\ b & b & e & a \end{array} .$$

Il primo si può considerare isomorfo a $\mathrm{S}ym_2$; il secondo è un gruppo ciclico di tre elementi (v. :2.p).

È assai interessante il gruppo $\mathrm{S}ym_3$ che consideriamo come gruppo delle permutazioni dell'insieme $\{1, 2, 3\}$.

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

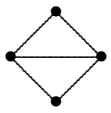
.

Questo gruppo può considerarsi il gruppo delle simmetrie del triangolo regolare.

B41:2.d Si dice **gruppo di Klein** o **Viergruppe** il gruppo di ordine 4 caratterizzato dalla seguente tavola di Cayley:

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

Questo gruppo abeliano si può interpretare come il gruppo costituito delle seguenti 4 trasformazioni del piano combinatorio $\mathbb{Z}\times\mathbb{Z}$ (o del piano cartesiano $\mathbb{R}\times\mathbb{R}$): identità e, riflessione rispetto l'asse orizzontale h, riflessione rispetto l'asse verticale v e riflessione rispetto all'origine c (riflessione centrale). Esso può anche vedersi come gruppo di simmetria del seguente grafo semplice



Il gruppo di Klein, oltre alla sua unità, contiene 3 involuzioni.

Per molti altri gruppi con pochi elementi v.a. [[en:Small groups]].

B41:2.e Tra le permutazioni di un insieme S si possono evidenziare quelle che non modificano determinate costruzioni B riguardanti S. Evidentemente la costruzione B viene conservata dalla applicazione successiva di due permutazioni che la conservano, dalla permutazione inversa di ogni permutazione che conserva B e dalla identità Id_S. Siamo quindi indotti a prendere in considerazione anche le strutture ottenute riducendo $\mathrm{S}ym_S$ alle trasformazioni che non modificano un determinato insieme di costruzioni B: ciascuna di queste strutture viene chiamata **sottogruppo** del gruppo $\mathrm{S}ym_S$.
Semplici esempi di richieste di conservazione sono i seguenti:

- non modificare determinati elementi di S;
- rispettare un sottoinsieme di S, cioè trasformare gli elementi di un $T \subset S$ in altri elementi di T;
- rispettare una data partizione di S, cioè trasformare gli elementi di ciascun blocco della partizione in altri elementi dello stesso blocco;
- mantenere determinate relazioni fra gli elementi di S;
- conservare i valori di determinate funzioni definite sugli elementi di S.

B41:2.f Diciamo **gruppo di permutazioni** ogni struttura della forma $\langle G, \circ, {}^{-\mathbf{1}}, \mathrm{Id}_S\rangle$ con G sottoinsieme della totalità delle permutazioni di un dato insieme S, sottoinsieme chiuso rispetto alla composizione di

tali permutazioni e rispetto al passaggio alla permutazione inversa. Come abbiamo visto molti gruppi di permutazioni si ottengono richiedendo la conservazione di una costruzione, ovvero il mantenimento di un invariante.
Mediante richieste di conservazione si ottengono gruppi di permutazioni di grande interesse. Ad esempio tra le permutazioni del piano si individuano quelle che mantengono le distanze tra i punti, le trasformazioni chiamate isometrie. Tra queste si individuano quelle che mantengono fisso un punto C e ruotano tutti i rimanenti di uno stesso angolo; queste trasformazioni sono chiamate **rotazioni** di centro C. Tra queste si possono scegliere quelle che trasformano in se un poligono regolare con centro in C, ad esempio un esagono regolare. Queste rotazioni costituiscono un gruppo di sei elementi. Tra queste si possono selezionare le rotazioni che trasformano in se uno dei due triangoli regolari individuati da tre dei vertici dell'esagono (in effetti conservano entrambi i due triangoli ottenibili in questo modo); con questa restrizione si individua un gruppo costituito solo da tre delle precedenti rotazioni e si ha un sottogruppo del precedente.
Da queste considerazioni emerge l'opportunità di definire come **sottogruppo** di un gruppo di permutazioni G una struttura ottenuta riducendo l'insieme delle permutazioni in G in modo da ottenere ancora un gruppo.

B41:2.g I gruppi di permutazioni rivestono grandissima importanza in quanto sopra di essi si basa lo studio delle simmetrie di numerosi oggetti presi in considerazione dalla matematica e dalle altre discipline scientifiche (v.o. e [[en:Symmetry]]).
Le simmetrie rivestono grande interesse, non solo estetico, ma anche pratico. Consideriamo il caso delle permutazioni che lasciano invariato l'esagono regolare. Oltre alle sei rotazioni viste in precedenza sono da considerare anche le riflessioni rispetto alle 3 rette definite dalle tre coppie di vertici opposti e le riflessioni rispetto alle 3 rette che sono bisettrici delle tre coppie di lati opposti. Questo gruppo di permutazioni si chiama **gruppo dell'esagono**. Supponiamo di dover studiare una costruzione che inizia con un vertice o un lato dell'esagono e prosegue con altri elementi (lati, vertici, bisettrici, segmenti, ...) considerati successivamente a partire dal primo elemento, fino ad ottenere un punto, un segmento, una distanza, una figura o un altro oggetto geometrico che goda di una particolare proprietà.
La conoscenza del gruppo delle simmetrie dell'esagono, cioè delle simmetrie della configurazione su cui è basata la costruzione, dice che esistono altre costruzioni che portano a risultati con la stessa proprietà ottenibili applicando una qualsiasi permutazione del gruppo a tutti i passi della costruzione. Quindi la conoscenza del gruppo di simmetria consente di controllare intere collezioni di costruzioni, cioè apre la strada ad una economia di elaborazioni e/o ad una economia di pensiero; queste economie possono risultare molto vantaggiose.
In seguito studieremo vari gruppi di permutazioni di configurazioni discrete e di procedure, a cominciare da gruppi di permutazioni di configurazioni finite monosostegno.

B41:2.h Procediamo ora a sviluppare i primi risultati generali riguardanti i gruppi. Facciamo riferimento ad un gruppo $\boldsymbol{G} = \langle G, \cdot, ^{-1}, e\rangle$ e adottiamo varie semplificazioni di scrittura: spesso trascuriamo le indicazioni infisse dell'operazione $\cdot$ e non distinguiamo fra gruppi e loro sostegni; se H e K sono sottoinsiemi di G, scriviamo $H \cdot K := \{h \in H, k \in K :| \ h \cdot k\}$ e $H^{-1} := \{h \in H :| \ h^{-1}\}$, cioè non distinguiamo le operazioni $\cdot$ e $^{-1}$ dalle rispettive estensioni booleane. Nell'attuale contesto, e in molti altri contesti, questo non porta ambiguità.

Per indicare che $\boldsymbol{H}$ è sottogruppo di $\boldsymbol{G}$ scriviamo $\boldsymbol{H} \leq_{Grp} \boldsymbol{G}$ o anche semplicemente $H \leq G$, se non si rischiano ambiguità. Nel caso in cui $\boldsymbol{H}$ sia sottogruppo proprio scriviamo $\boldsymbol{H} <_{Grp} \boldsymbol{G}$ o semplicemente $H < G$.

Ogni gruppo G possiede il sottogruppo banale $\{e\}$ ed il sottogruppo improprio G. Si dicono **gruppi semplici** i gruppi che presentano solo i due precedenti sottogruppi.

B41:2.i Prop. Sia $H \subset G$. $H < G \iff H \cdot H^{-1} \subseteq H$.
Dim.: "$\Longrightarrow$" $H < G$ equivale alle tre relazioni $e \in H$, $H^{-1} \subseteq H$ e $H \cdot H \subseteq H$. Di conseguenza $H \cdot H^{-1} \subseteq H \cdot H \subseteq H$.
"$\Longleftarrow$" Per ogni $a \in H$, $a \cdot a^{-1} \in H$, ovvero $e \in H$. $H^{-1} = e \cdot H^{-1} \subseteq H \cdot H^{-1} \subseteq H$. Per la terza relazione e per l'ipotesi $H \cdot H \subseteq H \cdot H^{-1} \subseteq H$. ∎

B41:2.j Introduciamo il gruppo additivo degli interi $\mathbb{Z}_{ag} := \langle \mathbb{Z}, +, -, 0 \rangle$ (ove $-$ denota il meno unario) e per ogni $z \in \mathbb{Z}$ consideriamo gli insiemi $z \cdot \mathbb{Z} := \{k \in \mathbb{Z} :| \; k \cdot z\}$. Si osserva che $0\mathbb{Z} = \{0\}$, cioè costituisce il sottogrupo banale di $\mathbb{Z}_{ag}$, che $-z \cdot \mathbb{Z} = z \cdot \mathbb{Z}$ e che $1 \cdot \mathbb{Z} = \mathbb{Z}$ costituisce il sottogruppo improprio di $\mathbb{Z}_{ag}$.

B41:2.k Prop. L'insieme dei sottogruppi di $\mathbb{Z}_{ag}$ è $\{m \in \mathbb{N} :| \; m \cdot \mathbb{Z}\}$
Dim.: Ciascuno di questi insiemi è sostegno di un sottogruppo di $\mathbb{Z}_{ag}$, in quanto contiene l'unità 0, coincide con l'insieme dei suoi inversi (numeri opposti) e $\forall z \in \mathbb{Z} \therefore \; z \cdot \mathbb{Z} + z \cdot \mathbb{Z} = z \cdot \mathbb{Z}$.
Viceversa ogni H sostegno di un sottogruppo di $\mathbb{Z}_{ag}$ deve avere la forma $z \cdot \mathbb{Z}$. Infatti, se non è il sottogruppo banale, deve contenere un intero non nullo ed il suo inverso, cioè deve contenere almeno un intero positivo; denotato con m il minimo di tali possibili interi positivi, per ogni altro $n \in H$ si può scrivere $n = qm + r$ con $r \in [m)$; ma $r = n - qm$ deve appartenere ad H e per la minimalità di m deve essere $r = 0$. ∎

Come vedremo in seguito, oltre a $\mathbb{Z}_{ag}$ presentano interesse vari altri gruppi numerici.
$\mathbb{Q}_{ag} := \langle \mathbb{Q}, +, -, 0 \rangle$, gruppo additivo dei razionali.
$\mathbb{R}_{ag} := \langle \mathbb{R}, +, -, 0 \rangle$, gruppo additivo dei reali.
$\mathbb{C}_{ag} := \langle \mathbb{C}, +, -, 0 \rangle$, gruppo additivo dei complessi.
$\mathbb{Q}_{mg} := \langle \mathbb{Q}_{np}, +, -, 0 \rangle$, gruppo moltiplicativo dei razionali.
$\mathbb{R}_{mg} := \langle \mathbb{R}_{np}, +, -, 0 \rangle$, gruppo moltiplicativo dei reali.
$\mathbb{C}_{mg} := \langle \mathbb{C}_{np}, +, -, 0 \rangle$, gruppo moltiplicativo dei complessi.

B41:2.l Consideriamo un gruppo $\langle \boldsymbol{G}, \cdot, ^{-1}, e \rangle$, un suo sottogruppo H e un suo elemento a. Si dice **laterale destro** o **coset destro** di H in G rappresentato da a l'insieme $Ha := \{h \in H :| \; ha\}$.
Simmetricamente si definisce **laterale sinistro** o **coset sinistro** di H in G rappresentato da a l'insieme $aH := \{h \in H :| \; ah\}$.

È possibile descrivere ogni laterale destro come una classe d'equivalenza rispetto alla relazione d'equivalenza $\sim$ definita in G ponendo per $a, b \in G$:

$$a \sim b \Longleftrightarrow ba^{-1} \in H \Longleftrightarrow b \in aH \; .$$

La classe di equivalenza contenente l'elemento g è proprio Hg: infatti $g = ge$ e quindi $e \in H$ perché H è un sottogruppo.
Simmetricamente ogni laterale sinistro può essere definito con una relazione di equivalenza analoga:

$$a \sim b \Longleftrightarrow a^{-1}b \in H \Longleftrightarrow b \in Ha \; .$$

Evidentemente per un gruppo abeliano i laterali sinistri di un sottogruppo H coincidono con i laterali destri di H; nel caso di un gruppo non abeliano questo in genere non avviene, se non per particolari sottogruppi.

Consideriamo il gruppo additivo degli interi $\mathbb{Z}$ e il suo sottogruppo $m\mathbb{Z}$, con $m = 2, 3, ...$ I laterali (sinistri e destri) di tale sottogruppo sono gli insiemi numerici $m\mathbb{Z}$, $m\mathbb{Z}+1$, $m\mathbb{Z}+2$, ..., $m\mathbb{Z}+m-1$; il loro numero è m.

B41:2.m Si verifica che in ogni gruppo, sia esso finito o infinito, i laterali sinistri possono essere facilmente messe in corrispondenza biunivoca con i laterali destri e quindi la cardinalità dei primi coincide con la cardinalità dei secondi. Tale cardinalità è detta **indice** del sottogruppo H nel gruppo G e talora si denota con $i(H)$.
In particolare, se G è finito ed ha n elementi e ogni classe laterale ha m elementi, si ha $n = m \cdot i(H)$: quindi l'indice del sottogruppo H e la cardinalità delle sue classi laterali sono divisori della cardinalità di G. In particolare questo è vero per il sottogruppo H, comunque esso venga scelto, perché esso corrisponde alla classe laterale eH.
Un sottogruppo N di un gruppo G (non abeliano) che definisce una unica partizione, cioè tale che $\forall g \in G : gN = Ng$, si dice **sottogruppo normale** di G; esso consente la definizione di un **gruppo quoziente** G/N i cui elementi sono le classi laterali sinistre ovvero destre.

B41:2.n Consideriamo un elemento a di un gruppo $\boldsymbol{G}$ e le sue successive potenze a, a^2, a^3, ... Se $\boldsymbol{G}$ è finito queste potenze non possono essere tutte diverse e scorrendole si trova un primo intero naturale m per il quale $a^m = e$; per ogni altro intero positivo n si può scrivere $n = qm + r$ con $r \in \mathbf{[}m\mathbf{)}$ e si ha $a^n = a^r$.
Se invece $\boldsymbol{G}$ è infinito si possono avere elementi con un numero finito di potenze diverse ed elementi b con infinite potenze diverse, della forma b^z con $z \in \mathbb{Z}$.
Si dice **periodo** dell'elemento a del gruppo G e si denota $\mathrm{prd}(a)$ il minimo intero positivo m per il quale $a^m = e$ se questo esiste, mentre in caso contrario si pone $\mathrm{prd}(a) = +\infty$.
Ovviamente in un gruppo finito tutti gli elementi hanno periodo finito ed in ogni gruppo l'unità è l'unico elemento di periodo 1.
Gli elementi di periodo 2, cioè gli elementi a t.c. $a^2 = e$, sono tutti e soli gli elementi che coincidono con il proprio inverso: essi si dicono **involuzioni**. Ogni involuzione è caratterizzata anche dalla uguaglianza $a = a^{-1}$. La scelta del termine involuzione, nel caso di un gruppo di permutazioni è coerente con il termine usato per le endofunzioni che applicate due volte danno l'identità, o, equivalentemente, con le endofunzioni coincidenti con la propria inversa.
Nel gruppo $\mathbb{Z}_{ag}$ tutti gli elementi diversi dall'elemento neutro, cioè da 0, hanno periodo infinito.
Nel gruppo moltiplicativo dei razionali $\mathbb{Q}_{mg} := \langle \mathbb{Q}_{np}, \cdot, ^{-1}, 1 \rangle$ l'elemento -1 ha periodo 2 e tutti gli elementi diversi da 1 e -1 hanno periodo infinito.

B41:2.o Consideriamo il gruppo i cui elementi sono le successioni infinite le cui componenti sono 1 o -1 e la cui operazione binaria è la moltiplicazione componente a componente; l'unità di questo gruppo è la successione costante $1^{\mathbb{Z}} = \langle z \in \mathbb{Z} :| \ 1 \rangle$ avente tutte le componenti uguali ad 1. Tutti gli elementi di questo gruppo diversi dall'unità hanno periodo 2.
Un gruppo si dice **gruppo di torsione** sse tutti i suoi elementi hanno periodo finito; tutti i gruppi finiti sono banalmente gruppi di torsione; il gruppo precedente è un gruppo di torsione infinito. Un gruppo si dice **gruppo privo di torsione** sse tutti i suoi elementi diversi dall'unità hanno periodo infinito; Sono gruppi privi di torsione $\mathbb{Z}_{ag}$, $\mathbb{Q}_{ag}$, $\mathbb{R}_{ag}$. Un gruppo si dice **gruppo misto** sse possiede sia elementi diversi dall'unità di periodo finito, che elementi di periodo infinito. Il gruppo moltiplicativo $\mathbb{Q}_{mg}$ considerato in precedenza è un gruppo misto; le stesse considerazioni mostrano che è misto anche il gruppo moltiplicativo dei reali $\mathbb{R}_{mg}$. Un gruppo misto con infiniti elementi di periodo finito e infiniti

elementi di periodo infinito è il gruppo moltiplicativo dei complessi $\mathbb{Q}_{mg}$: per ogni $n = 3, ...$ si trovano radici n-esime dell'unità che hanno periodo n.

B41:2.p Esercizio Consideriamo il gruppo G, due suoi elementi diversi dall'unità a e b ed un intero positivo k. Dimostrare che:
(1) $a^k = e \implies \lceil k \in \mathrm{prd}(a)\mathbb{P} \ \wedge \ a^{-1} = a^{k-1} \rceil$.
(2) $\mathrm{prd}(a) = \mathrm{prd}(a^{-1})$.
(3) $\mathrm{prd}(a), \mathrm{prd}(b) \in \mathbb{P} \ \wedge \ ab = ba \implies \mathrm{prd}(ab) \mid \mathrm{mcm}(\mathrm{prd}(a), \mathrm{prd}(b))$.
(4) $\mathrm{prd}(ab) = \mathrm{prd}(ba)$.

B41:2.q L'insieme delle potenze di un elemento a di un gruppo G, $P := \{z \in \mathbb{Z} :| \ a^z\}$, costituisce un sottogruppo di G: infatti per due elementi generici di questo sottoinsieme P $g := a^q$ ed $h := a^r$ si ottiene $g \cdot h^{-1} = a^{q-r}$, cioè un altro elemento di P.
Questo sottogruppo, finito o infinito, si dice **sottogruppo ciclico generato da** a e spesso si individua con la notazione locale $\langle a \rangle$. Ogni gruppo esprimibile nella forma $\langle a \rangle$ si dice **gruppo ciclico**. Evidentemente ogni gruppo ciclico è abeliano.
Si distinguono gruppi ciclici finiti della forma $\{a, a^2, a^3, ..., a^m = e\}$ generati da elementi di periodo finito coincidente con l'ordine del gruppo, e gruppi ciclici infiniti come $\mathbb{Z}_{ag}$.

B41:2.r Due elementi g ed h di un gruppo G si dicono **coniugati** sse esiste un altro elemento x del gruppo t.c. $xgx^{-1} = h$.

(1) Prop. La relazione di coniugio fra gli elementi di un gruppo è una equivalenza.
Dim.: Infatti $ege^{-1} = g$, quindi la relazione è riflessiva; da $xgx^{-1} = h$ segue $x^{-1}hx = g$, cioè che il coniugio è una relazione simmetrica; da $xgx^{-1} = h$ e $yhy^{-1} = k$ segue $yxgx^{-1}y^{-1} = (yx)g(yx)^{-1} = k$, cioè che il coniugio è transitivo ∎

La partizione del sostegno di un gruppo in classi di coniugio spesso presenta aspetti interessanti. Per ogni gruppo finito di permutazioni gli elementi di una classe di coniugio sono caratterizzati da un tipo di fattorizzazione in cicli. Questo invece non è il caso dei gruppi abeliani, in quanto in essi ogni elemento è coniugato solo di sé stesso: $xgx^{-1} = xx^{-1}g = g$.

B41:2.s Esercizio Dimostrare che, per ogni elemento x di un gruppo G l'applicazione $\lceil g \in G \mapsto xgx^{-1} \rceil$ è un automorfismo di G.

B41:2.t Esercizio Dimostrare che gli elementi di una classe di coniugio di un gruppo hanno tutti lo stesso periodo. Più in generale mostrare che due elementi di un gruppo collegati da un automorfismo hanno lo stesso periodo.

B41:2.u Consideriamo due gruppi $\boldsymbol{G}_i = \langle G_i, \otimes_i, j_i, e_i \rangle$ per $i = 1, 2$. Si dice **prodotto diretto** dei due gruppi $\langle \boldsymbol{G}_1 \times \boldsymbol{G}_2, \otimes_1 \times \otimes_2, j_1 \times j_2, \langle e_1, e_2 \rangle \rangle$. Esplicitiamo le operazioni di questo gruppo considerando, per $i = 1, 2$, g_i e h_i due elementi generici di G_i:
$\langle g_1, g_2 \rangle (\otimes_1 \times \otimes_2) \langle h_1, h_2 \rangle = \langle g_1 \otimes_1 h_1, g_2 \otimes_2 h_2 \rangle$,
$\langle g_1, g_2 \rangle (j_1 \times j_2) = \langle g_1 j_1, g_2 j_2 \rangle$,
$\langle g_1, g_2 \rangle (\otimes_1 \times \otimes_2) \langle g_1 j_1, g_2 j_2 \rangle = \langle e_1, e_2 \rangle$.
Questa costruzione consente di definire molti gruppi di interesse pratico. Esempi piuttosto semplici sono costituiti dagli insiemi delle coppie, oppure delle terne, o in generale delle sequenze di d numeri reali. Questi sono i gruppi additivi e abeliani dei vettori del piano, dello spazio tridimensionale e in generale dello spazio d-dimensionale.

B41:3. Anelli

B41:3.a Nelle attività matematiche ed elaborative, a partire dalle più elementari riguardanti stringhe, numeri naturali e insiemi, risulta necessario disporre di almeno due operazioni binarie ben distinte. In questo paragrafo introdurremo le più importanti tra le specie di strutture algebriche monosostegno munite di due operazioni.

B41:3.b Si dice **semianello** una struttura $\langle R, \oplus, \mathbf{0}, \otimes, \mathbf{1}\rangle$ per la quale valgano le seguenti proprietà:
$\langle R, \oplus, \mathbf{0}\rangle$ è un monoide abeliano;
$\langle R, \otimes, \mathbf{1}\rangle$ costituisce un monoide;
$\forall a, b, c \in R \ : \ (a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$ e $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$.

Si dice **anello** una struttura $\langle R, \oplus, \ominus, \mathbf{0}, \otimes, \mathbf{1}\rangle$ per la quale valgano le seguenti proprietà:
$\langle R, \oplus, \ominus, \mathbf{0}\rangle$ è un gruppo abeliano;
$\langle R, \otimes, \mathbf{1}\rangle$ costituisce un monoide;
$\langle R, \oplus, \otimes, \mathbf{1}\rangle$ è un semianello.
Un **anello** si dice **abeliano** o **commutativo** sse è commutativo il suo prodotto.
Denotiamo, rispettivamente, con **Rng** ed **RngAb** le classi degli anelli e degli anelli abeliani.

B41:3.c Un esempio fondamentale di anello commutativo è dato dall'insieme degli interi munito delle usuali operazioni di somma, differenza e prodotto, $\mathbb{Z}_{rng} := \langle \mathbb{Z}, +, -, 0, \cdot, 1\rangle$.
Altri anelli commutativi numerici sono costituiti similmente dai numeri razionali, dai reali e dai complessi:
$\mathbb{Q}_{rng} := \langle \mathbb{Q}, +, -, 0, \cdot, 1\rangle$, $\mathbb{R}_{rng} := \langle \mathbb{R}, +, -, 0, \cdot, 1\rangle$, $\mathbb{C}_{rng} := \langle \mathbb{C}, +, -, 0, \cdot, 1\rangle$.
Altri importanti anelli unitali commutativi sono costituiti dalle classi di resti $\mathbb{Z}_m$ modulo un qualsiasi intero $m \geq 2$.
Osserviamo che non si fa alcuna richiesta sull'esistenza di elementi inversi per il prodotto. Questa è assicurata solo all'elemento unità. Nel caso di $\mathbb{Z}_r$ degli elementi diversi da 1, solo -1 possiede elemento inverso. Nel caso degli altri tre anelli numerici tutti gli elementi ad esclusione dello 0 posseggono inverso. solo l'elemento unità, com chiede che

B41:3.d Un sottoinsieme S del sostegno R di un anello $\boldsymbol{R}$ si dice **sostegno di un sottoanello** di $\boldsymbol{R}$ sse è chiuso rispetto alle operazioni di somma e prodotto, cioè sse $\forall a, b \in S \ : \ a + b \in S$ e $a \cdot b \in S$.
In questo caso scriviamo $S \leq_{Rng} R$ o anche, se il contesto consente di evitare ambiguità, $S \leq R$. Se in particolare S è sottoinsieme proprio di R siscrive $S <_{Rng} R$.
Si constata facilmente che $\mathbb{Z}_{rng} <_{Rng} \mathbb{Q}_{rng} <_{Rng} \mathbb{R}_{rng} <_{Rng} \mathbb{C}_{rng}$.

B41:3.e Esercizio Dimostrare che per $m, k = 2, 3, ...$ si ha $m \cdot k\mathbb{Z} <_{Rng} m\mathbb{Z} <_{Rng}$.

B41:3.f Le matrici quadrate di ordine finito (v. G40:3) le cui componenti sono elementi di un anello costituiscono anelli ricchi di applicazioni.
A partire dall'anello $\boldsymbol{R} = \langle R, \oplus, \ominus, \mathbf{0}, \otimes, 1\rangle$ per ogni intero positivo d si può considerare l'anello delle matrici quadrate di un dato ordine

$$\langle \mathsf{Mat}_{d,\boldsymbol{R}}, \oplus_{mat}, \ominus_{mat}, MatZr_{d,\boldsymbol{R}}, \otimes_{mat}, MatId_{d,\boldsymbol{R}}\rangle \ .$$

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

B41:3.g 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.

$$\begin{bmatrix}0 & 1\\1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix} = \begin{bmatrix}0 & 1\\1 & 2\end{bmatrix} \neq \begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}\begin{bmatrix}0 & 1\\1 & 1\end{bmatrix} = \begin{bmatrix}1 & 2\\1 & 1\end{bmatrix}$$
$$\begin{bmatrix}1 & 2\\3 & 4\end{bmatrix}\begin{bmatrix}5 & 6\\7 & 8\end{bmatrix} = \begin{bmatrix}19 & 43\\22 & 50\end{bmatrix} \neq \begin{bmatrix}5 & 6\\7 & 8\end{bmatrix}\begin{bmatrix}1 & 2\\3 & 4\end{bmatrix} = \begin{bmatrix}23 & 31\\34 & 46\end{bmatrix}$$

B41:3.h In un anello $\langle R, +, -, 0, \cdot, 1\rangle$ può accadere che presi due elementi $r, s \in R$, diversi dallo zero, il loro prodotto rs sia uguale allo stesso elemento zero. Tali elementi si dicono **divisori dello zero**.

Consideriamo l'anello $\langle \mathbb{Z}_6, +_6, -_6, 0, \cdot_6, 1\rangle$; in esso $2 \cdot_6 3 = 0_6$, cioè 2_6 e 3_6 sono divisori dello zero. In ogni anello $\mathbb{Z}_m$ con m numero non primo si trovano divisori dello zero, in quanto si può scrivere $m = r \cdot s$ con $r, s \neq 0, 1$ ed $r \cdot_m s = 0_m$.

B41:3.i Esercizio Dimostrare che nell'anello $\mathbb{Z}_m$ l'insieme dei divisori dello zero coincide con gli interi in $\{2, ..., m-1\}$ non primi con m.
Concludere che ogni anello $\mathbb{Z}_p$ con p numero primo è privo di divisori dello zero.

B41:3.j Si trovano molte coppie di matrici 2×2 sui reali che costituiscono divisori dello zero $\mathbf{0}_{2,2}$: in particolare:

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

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

B41:3.k Si dice **corpo** un anello $\boldsymbol{R}$, in cui gli elementi diversi dallo zero formano gruppo rispetto all'operazione prodotto.
Perché questa definizione abbia senso è necessario che $\boldsymbol{R}$ possegga almeno due elementi. Il corpo più piccolo ha come sostegno $\mathbb{B} = \{0, 1\}$.
L'insieme degli elementi del corpo $\boldsymbol{R}$ diversi dallo zero, prende il nome di **gruppo moltiplicativo** di $\boldsymbol{R}$ e si denota solitamente con $\boldsymbol{R}^{\times}$.
Un corpo in cui il prodotto è commutativo viene detto **corpo commutativo** o **campo**. Un corpo non commutativo viene anche chiamato **corpo sghembo** (*skewfield*).
Denotiamo **Krp** la classe dei corpi, **Fld** la classe dei campi e **KrpNab** la classe dei corpi sghembi.

B41:4. Campi

B41:4.a Un campo è una struttura della forma $\boldsymbol{F} = \langle F, +, -, 0, \cdot, ^{-1}, 1\rangle$ t.c. $\langle F, +, -, 0\rangle$ e $\langle F \setminus 0, \cdot, ^{-1}, 1\rangle$ sono gruppi commutativi e il prodotto $\cdot$ è distributivo rispetto alla somma $+$. I due gruppi citati sono detti **gruppo additivo** e **gruppo moltiplicativo** del campo $\boldsymbol{F}$.
Vi sono importanti campi finiti e importanti campi infiniti.

B41:4.b Campi infiniti si ottengono munendo con le usuali operazioni di somma e prodotto l'insieme $\mathbb{Q}$ dei numeri razionali relativi, l'insieme $\mathbb{RA}$ dei numeri algebrici, l'insieme $\mathbb{RC}$ dei numeri reali costruibili,

l'insieme $\mathbb{R}$ dei numeri reali relativi e l'insieme $\mathbb{CA}$ dei numeri complessi algebrici, l'insieme $\mathbb{CC}$ dei numeri complessi costruibili e l'insieme $\mathbb{C}$ dei numeri complessi.
Un altro interessante campo infinito è costituito dalle funzioni razionali, funzioni esprimibili come quoziente di due polinomi.

B41:4.c Sono molto importanti anche i campi finiti che, come vedremo, si possono classificare completamente con relativa facilità. Denotiamo con **FldF** la classe dei campi finiti.
In particolare sono campi finiti gli anelli della forma $\mathbb{Z}_p$ con p numero primo.
Si dimostra che nell'insieme degli anelli $\mathbb{Z}_m$ con $m = 2, 3, 4, ...$ essi sono i soli che costituiscon dei campi.

B41:4.d Una importante proprietà dei campi riguarda la non esistenza di divisori dello 0 diversi da tale elemento.
B41:1 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 $b = 0$; similmente 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 efficaci piattaforme computazionali.

B41:4.e Segnaliamo alcune proprietà dei corpi.

B41:1 Teorema Ogni corpo è privo di divisori dello zero.

B41:2 Teorema Ogni anello finito $\boldsymbol{R}$ privo di divisori dello zero, cioè ogni dominio di integrità finito è un corpo.

B41:3 Teorema Ogni corpo finito è un campo.