1

Capitolo B20
piano sugli interi, numeri primi, numeri razionali

Contenuti delle sezioni

a. interi negativi e interi relativi p. 2
b. piano-ZZ, rette-ZZK e nozioni elementari collegate p. 6
c. somma e differenza di interi p. 13
d. prodotto di interi p. 16
e. permutazioni degli interi p. 19
f. nozioni di gruppo di simmetria e di gruppo in generale p. 24
g. numeri primi e fattorizzazione degli interi mediante primi p. 31
h. frazioni, numeri razionali e operazioni sui razionali p. 38

44 pagine

B20 0.01 Questo capitolo riprende l'introduzione dell'insieme $\mathbb{Z}$ degli interi relativi ottenuto come estensione dell'insieme dei naturali motivata dalla opportunità di avere un ambiente numerico nel quale l'operazione di differenza sia definita per ogni coppia di operandi.

Questo ampliamento dell'insieme numerico $\mathbb{N}$ all'insieme $\mathbb{Z}$ viene effettuato un po' paradossalmente passando attraverso l'insieme delle coppie di naturali $\mathbb{N} \times \mathbb{N}$ e l'opportunità di estendere $\mathbb{N} \times \mathbb{N}$ a $\mathbb{Z} \times \mathbb{Z}$, l'insieme delle coppie di interi.

In effetti ponendoci in due dimensioni si possono visualizzare meglio le caratteristiche e le esigenze delle operazioni binarie, le entità che maggiormente richiedono l'ampliamento.

A questo punto risulta opportuno approfondire l'esame di $\mathbb{Z}$ e $\mathbb{Z} \times \mathbb{Z}$ al fine di conoscere meglio la struttura di questi insiemi e definire vari strumenti per operare entro di essi, soprattutto perché essi costituiscono i primi ambienti nei quali conviene impostare fondamentali nozioni geometriche. Essi inoltre costituiscono il quadro nel quale è conveniente visualizzare molte entità e molte costruzioni matematiche.

Si mostra anche che per trattare questi ambienti è opportuno servirsi di un linguaggio che pone in collegamento formule matematiche, oggetti fisici e termini delle descrizioni visive.

Di $\mathbb{Z}$ e $\mathbb{Z} \times \mathbb{Z}$ si esaminano con cura le traslazioni e le riflessioni, endofunzioni biiettive che inducono a introdurre senza indugi la nozione di gruppo, struttura algebrica che si comincia a vedere nella versione dei gruppi di trasformazioni, prima di trattarla al livello generale dei cosiddetti gruppi astratti [B41b, T22]

I gruppi delle traslazioni e delle rotazioni consentono di presentare le prime proprietà di simmetria delle figure geometriche, ossia le simmetrie delle configurazioni che per prime possono essere illustrate proficuamente.

Alberto Marini

B20 a. interi negativi e interi relativi

B20 a.01 I numeri interi naturali sono stati introdotti al fine di esprimere quantità di entità di varia natura (oggetti materiali, esseri viventi, nozioni mentali, ...) caratterizzate dall'essere singolarmente bene individuabili.
Nella pratica i raggruppamenti delle entità valutabili mediante interi riguardano elementi dotati di caratteristiche simili.

Un'altra importante applicazione dei naturali riguarda la possibilità di esprimere spostamenti su posizioni allineate ed equidistanziate in una direzione scelta come primaria o nella direzione opposta per tratti che hanno lunghezze multiple della distanza tra due posizioni contigue, misura che si assume unica.

La somma di interi naturali è l'operazione che permette di esprimere sia l'accumularsi di oggetti individuabili che il succedersi di spostamenti nella unica direzione primaria.

In B04d, considerati due interi naturali m ed n con $m \leq n$, si è definita come differenza tra n ed m, e la si è denotata con $n - m$, l'intero naturale d tale che $m + d = n$.

Questa prima definizione della differenza permette di esprimere l'eliminazione da un raggruppamento di oggetti di una parte di esse e il succedersi di uno spostamento in una direzione seguito da uno spostamento non superiore nella direzione opposta.

La somma e la differenza di interi naturali si possono presentare molto intuitivamente mediante un modello cinematico che mostra i numeri naturali disposti su successivi punti allineati ed equidistanziati. La somma $n + m$ è rappresentata da due spostamenti: il primo verso destra di n unità dal punto 0 al punto n, il secondo anch'esso verso destra di m unità dal punto n al punto $n + m$. La differenza $n - m$ con $n > m$ si collega invece alla coppia di spostamenti formata ancora da quello verso destra di n unità dal punto 0 al punto n e da un secondo verso sinistra di m unità dal punto n al punto $n - m$.

Si rivela utile considerare anche una presentazione del tutto equivalente che raffigura gli spostamenti in verticale: questa è particolarmente significativa nel caso di interi utilizzati per operazioni finanziarie o attività di magazzino che comportano il sommarsi di crediti o l'accumularsi di beni materiali per l'espressione $n + m$ e il ridursi di un credito a causa di una restituzione o il diminuire di una scorta anche al di sotto di un livello di guardia in conseguenza di un asporto quantificato dall'espressione $n - m$.

B20 a.02 La varietà delle situazioni che si possono trattare con numeri interi al fine di descrivere spostamenti secondo una determinata direzione o la sua opposta e di descrivere scambi di denaro suggerisce che sia utile disporre di un'estensione dell'operazione differenza applicabile a numeri n ed m per i quali può accadere che sia $n \geq m$.

Questa operazione si vuole poterla utilizzare anche per spostamenti secondo una direzione che riguardano arretramenti superiori agli avanzamenti e per gli eventi finanziari nei quali un operatore ha debiti superiori ai crediti, ossia abbassamenti delle sue disponibilità maggiori degli innalzamenti.

Per effettuare una tale estensione delle operazioni si rende evidentemnte necessario disporre di un ambiente più ampio dell'insieme dei naturali.

Tale ampliamento risulta pienamente giustificato se porta a un ambiente operativo più versatile: è opportuno estendere ad esso, oltre alla differenza, le operazioni di somma e prodotto e fare in modo che le operazioni estese mantengano il più possibile le proprietà che si sono dimostrate utili.

Osserviamo che la differenza tra interi naturali $n - m$ con $n \geq m$ è una funzione del genere $\lceil\, \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \,\rceil$ avente come dominio il sottoinsieme "triangolare" di $\mathbb{N} \times \mathbb{N}$

$$\mathsf{T} \;:=\; \mathbf{Arc}(\mathbb{N}, \leq) \;:=\; \{n \in \mathbb{N} :|\ \ , m \in [\![n]\!] :|\ \langle n, m\rangle\} \;=\; \{\langle n, m\rangle \in \mathbb{N} \times \mathbb{N} \,\rceil\!\rceil\, n \geq m\}\ .$$

La differenza tra naturali viene significativamente presentata con la seguente tabella che, in linea di principio, può essere estesa quanto si vuole:

Da questa tabella risultano evidenti le classi della equivalenza associata canonicamente alla funzione differenza, relazione che denotiamo con $\mathsf{E}'_$ e che riguarda le caselle della T, cioè le coppie di naturali, caratterizzate dalla richiesta $\langle n, m\rangle \mathsf{E}'_ \langle p, q\rangle$ sse $n + q = m + p$.
Queste classi corrispondono agli insiemi delle caselle di T che sono allineate parallelamente alla diagonale principale.

Questa raffigurazione suggerisce di ampliare la $\mathsf{E}'_$ innanzi tutto all'intero $\mathbb{N} \times \mathbb{N}$ aggiungendole come nuove classi di equivalenza gli insiemi di coppie di naturali $\langle n, m\rangle$ con $m > n$ tali che sia costante $m - n$; questi insiemi relativi a valori diversi di $m - n$ sono disgiunti e costituiscono una partizione di $\mathbb{N} \times \mathbb{N} \;\setminus\; \mathsf{T}$. L'equivalenza così ottenuta la denotiamo con $\mathsf{E}''_$.

Gli elementi rappresentativi di maggiore evidenza delle nuove classi di equivalenza sono le coppie $\langle 0, m\rangle$ nelle posizioni più a sinistra nella tabella, come per le classi in T le più in evidenza sono le coppie più in basso $\langle n, 0\rangle$.
Viene spontaneo contraddistinguere le nuove classi servendosi degli interi m come secondi membri delle coppie $\langle 0, m\rangle$; questi interi positivi m non si possono però utilizzare direttamente, in quanto darebbero classi indistinguibili da quelle rappresentate dagli interi positivi n ricavati dalle caselle $\langle n, 0\rangle$. Utilizziamo quindi una loro variante tipografica associando a $\langle 0, m\rangle$ la scrittura $\overline{m}$.

B20 a.03 Per rendere utili le classi della equivalenza $\mathsf{E}''_$ non contenute in T si è indotti a trattare le coppie che le rappresentano $\langle 0, m\rangle$, per $m \in \mathbb{P}$ dei nuovi numeri, ovvero le scritture $\overline{m}$, come entità sottoponibili a operazioni come somma e prodotto che agiscono su due numeri nuovi oppure su un numero nuovo e un intero naturale.

Dati Diciamo che due numeri m e $\overline{m}$ sono l'uno l'**opposto** dell'altro.
In tal modo si ha una tabella della differenza, anch'essa estendibile quanto si vuole, che assume il seguente aspetto:

Definiamo come insieme dei **numeri interi negativi** $\mathbb{Z}_ \;:=\; \{m \in \mathbb{P} :|\ \overline{m} \in \mathbb{P}\}$ e come insieme dei **numeri interi [relativi]** $\mathbb{Z} \;:=\; \mathbb{Z}_ \dot\cup \{0\} \dot\cup \mathbb{P}$.

Riferendosi alla presentazione dei numeri naturali allineati orizzontalment e visitabili con spostamenti multipli di una unità, è ragionevole a collocare i numeri $\overline{m}$ a sinistra dello 0; questa operazione corrisponde a ridurre la tabella precedente alla sua prima riga e alla sua prima colonna e a ruotare questa in modo da disporla alla sinistra della suddetta riga.

Risultano utili due raffigurazioni dell'insieme $\mathbb{Z}$, la raffigurazione a punti e la raffigurazione a caselle:

Entrambe si possono chiamare **raffigurazioni della retta-Z**. La prima rappresenta più efficacemente $\mathbb{Z}$ come primo ambiente per la costruzione della geometria della retta. La seconda anticipa la presentazione sequenziale delle funzioni aventi come dominio $\mathbb{Z}$.

B20 a.04 Abbiamo introdotto la scrittura "-Z" [B20a04] da usare come suffisso del sostantivo retta. Si tratta di un esempio di quella che chiamiamo **specificazione sincopata**, elemento linguistico artificioso, ma che useremo spesso in quanto permette di esprimere concisamente caratteristiche anche dettagliate di molteplici termini i quali possono essere formati da sostantivi, aggettivi, verbi, avverbi e anche preposizioni che si vogliono individuabili nella suddetta specificazione sincopata.

In seguito incontreremo molte altre specificazioni sincopate, alcune come precisi sostituti di aggettivi, di avverbi e di complementi.
In particolare useremo "-N" per fare riferimento agli interi naturali, "-Z" per oggetti concernenti i numeri interi, "-NN" per richiamare l'insieme delle coppie di naturali, "-ZZ" per le coppie di interi relativi, le precisazioni di carattere geometrico della "-ZZ": "-ZZH", "-ZZV", "-ZZD1", "-ZZD2", "-ZZR", "-ZZB", "-ZZK", "-QQ" per riferirsi al piano razionale [B30 e B31], "-RR" concernente il piano cartesiano reale [B43], "-CC" riguardante il piano delle coppie di numeri complessi [B50].

Accadrà di trattare numerose nozioni di carattere geometrico collocandole di volta in volta in insiemi come quelli delle coppie degli interi, delle coppie dei razionali, delle coppie o delle terne dei reali, delle coppie dei numeri complessi e così via.

B20 a.05 Usiamo molte specificazioni sincopate ritenendo possano costituire precisazioni concise abbastanza efficaci e talora sistematiche; in particolare servono a distinguere esplicitamente le diverse ambientazioni nelle quali si collocano molte definizioni e vari enunciati che spesso sono lasciate implicite confidando nei riferimenti al contesto.

Specificazioni sincopate saranno utilizzate anche per oggetti geometrici in tre dimensioni. In particolare useremo

"-NNN" per oggetti in $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$,
"-ZZZ" per oggetti in $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$,
"-ZZN" per oggetti in $\mathbb{Z} \times \mathbb{Z} \times \mathbb{N}$,
"-ZZP" per oggetti in $\mathbb{Z} \times \mathbb{Z} \times \mathbb{P}$,
"-RRR" per oggetti in $\mathbb{R}^{\times 3}$ (lo spazio tridimensionale reale) ,
"-CCC" per oggetti in $\mathbb{C}^{\times 3}$ (lo spazio tridimensionale sui numeri complessi) .

Svariate specificazioni sincopate saranno inoltre usate per i moltissimi generi di funzioni che si possono comunemente incontrare. In particolare useremo JP

- "funzioni-NtN" per le funzioni del genere $\lceil \mathbb{N} \longrightarrow \mathbb{N} \rceil$,
- "funzioni-NNtN" per le funzioni del genere $\lceil \mathbb{N} \times \mathbb{N}\ funac\ \mathbb{N} \rceil$,
- "funzioni-NNtQ" per le funzioni del genere $\lceil \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{Q} \rceil$,
- "funzioni-PtP" per le funzioni del genere $\lceil \mathbb{P} \longrightarrow \mathbb{P} \rceil$,
- "funzioni-ZtZ" per le funzioni del genere $\lceil \mathbb{Z} \longrightarrow \mathbb{Z} \rceil$,
- "funzioni-ZZtN" per le funzioni del genere $\lceil \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{N} \rceil$,
- "funzioni-QtQ" per le funzioni del genere $\lceil \mathbb{Q} \longrightarrow \mathbb{Q} \rceil$,
- "funzioni-RtR" per le funzioni del genere $\lceil \mathbb{R} \longrightarrow \mathbb{R} \rceil$,
- "funzioni-RRtR" per le funzioni collocabili in $\lceil \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R} \rceil$,
- "funzioni-RRtRR" per le funzioni collocabili in $\lceil \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R} \times \mathbb{R} \rceil$,
- "funzioni-RRRtR" per le funzioni collocabili in $\lceil \mathbb{R}^{\times 3} \longrightarrow \mathbb{R} \rceil$,

- "funzioni-RdtRe" per le funzioni collocabili in $\lceil\, \mathbb{R}^{\times d} \longrightarrow \mathbb{R}^{\times e} \,\rceil$ per $d, c \in \mathbb{P}$,
- "funzioni-RRRtRRR" per le funzioni collocabili in $\lceil\, \mathbb{R}^{\times 3} \longrightarrow \mathbb{R}^{\times 3} \,\rceil$,
- "funzioni-CtC" per le funzioni del genere $\lceil\, \mathbb{C} \longrightarrow \mathbb{C} \,\rceil$,
- "funzioni-CCtC" per le funzioni collocabili in $\lceil\, \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C} \,\rceil$, ossia le funzioni di due variabili complesse che assumono valori complessi.

Segnaliamo anche che per varie argomentazioni nelle quali è opportuno distinguere i numeri reali, da definire mediante assiomi, dai numeri reali costruibili che si possono definire come i numeri approssimabili illimitatamente mediante liste.GI di numeri razionali, l'insieme di questi sarà denotato anche con $\mathbb{W}$.
Diamo quindi per scontato il significato degli insiemi delle funzioni-WtW, delle funzioni-WWtW, delle funzioni-WWWtW e delle funzioni-WWWtWWW.

Cogliamo l'occasione per introdurre anche la specificazione sincopata **semiretta-N** per la la raffigurazione di $\mathbb{N}$.

B20 a.06 Ricordiamo anche che l'insieme $\mathbb{Z}_-$ e l'insieme $\mathbb{Z}$ sono numerabili: infatti essi si possono porre in biiezione con $\mathbb{N}$, risp., ad esempio, con le seguenti funzioni:

$$\left\downarrow \begin{matrix} 0 & 1 & 2 & 3 & \cdots & n & \cdots \\ -1 & -2 & -3 & -4 & \cdots & -n-1 & \cdots \end{matrix} \right. \quad \text{e} \quad \left\downarrow \begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \cdots \\ 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & -4 & \cdots \end{matrix} \right. .$$

Ricordiamo anche che sono numerabili anche $\mathbb{N} \times \mathbb{N}$, $\mathbb{Z} \times \mathbb{Z}$ e $\mathbb{Q} \times \mathbb{Q}$.

B20 b. piano-ZZ, retta-ZZK e nozioni elementari collegate

B20 b.01 Per estendere le operazioni di somma, prodotto e differenza dagli interi naturali a tutti i numeri interi è opportuno fare riferimento all'insieme quadrato cartesiano $\mathbb{Z} \times \mathbb{Z}$ e di considerarlo un ben motivato ampliamento di $\mathbb{N} \times \mathbb{N}$.

In effetti $\mathbb{Z} \times \mathbb{Z}$ si rivela l'ambiente più conveniente per l'introduzione di molte nozioni matematiche basilari.
Nel seguito spesso lo chiameremo **piano-ZZ** e vedremo che costituisce l'importante ambiente nel quale vengono introdotte le prime nozioni geometriche.

In questa sezione introduciamo i primi termini e i primi fatti che lo riguardano; successivamente, dopo aver trattato somma, differenza e prodotto degli interi, inizieremo un suo studio sistematico che proseguirà in B21, B22, B23, D21 e nel tomo G.
Il piano-ZZ viene chiamato anche piano combinatorio, piano di Pólya, e piano cartesiano a coordinate intere.

B20 b.02 Ci proponiamo di introdurre il piano-ZZ servendoci di un suo modello osservabile che risulta utile e interessante per vari motivi:

- consente di servirsi, per matematica, fisica, programmazione e loro applicazioni, di un linguaggio visivo-cinematico che agevola la prima comprensione delle varie utili configurazioni che si collocano nel piano-ZZ e nei suoi prevedibili successivi ampliamenti consentendo di alternare argomentazioni formali e più sbrigative considerazioni intuitive;
- questo modello costituisce un primo passo verso i cosiddetti **modelli geometrico-fisici classici** dello spazio fisico, in sigla **modelli GFC**;
- costituisce un preliminare utile per il chiarimento della portata dei calcoli effettivi e dei loro rapporti con la geometria, la fisica matematica e varie loro applicazioni.

Come vedremo in seguito [:h], $\mathbb{Z} \times \mathbb{Z}$ può essere raffigurato in vari modi; qui presentiamo il suo modello mediante una sola delle sue raffigurazioni, la cosiddetta raffigurazione geografica mediante punti e successivamente otterremo le restanti raffigurazioni come sue varianti.

B20 b.03 Un modello GFC riguarda oggetti fisicamente idealizzati: punti senza estensione, segmenti e rette con sezioni trascurabili, piani privi di spessore e di estensione illimitata, figure perfettamente regolari e altre configurazioni idealizzate.

Va ricordato che la geometria classica ha trattato questi oggetti con termini e linguaggi i quali, nella storia delle idee, sono stati i primi utensili formali usati ampiamente per ottenere risultati di grande importanza scientifica e culturale.

Per maggiore facilità ed efficacia espositiva risulta conveniente descrivere anch questi modelli in termini di materiali idealizzati.
Dei modelli GFC non diamo descrizioni costruttive dettagliate, ma solo indicazioni di massima su modalità che possono essere seguite per ottenere oggetti tangibili in grado di rappresentarli con approssimazioni sufficienti per molti scopi.

Il modello GFC per il piano-ZZ deve potersi considerare ottenibile con strumenti e processi finiti con il consumo di risorse finite nel quale si possono sviluppare elaborazioni effettive con risultati chiaramente osservabili e valutabili secondo criteri condivisibili.

Alla base del modello poniamo un "postulato di estendibilità delle risorse": in relazione a ogni esigenza di elaborazioni effettive, u modello GFC può essere ulteriormente esteso quanto serve e la precisione dei suoi elementi può essere aumentata quanto si vuole [B18a].

Una sua costruzione effettiva preferirebbe estensione e precisione elevate; senza entrare in dettaglo, ci limitiamo a enunciare che il modell si potrebbe costruire servendosi di tecniche che permettono di ottenere un artefatto esteso e preciso tanto da poter essere utile per numerose applicazioni di rilievo e che, per il postulato di estendibilità delle risorse, abbia la possibilità di essere ulteriormente ampliato e raffinato.

B20 b.04 Vanno tuttavia subito segnalate le difficoltà che si incontrano per ottenere estensioni e precisioni sufficienti per applicazioni più esigenti di quelle collaudate, difficoltà che portano a limiti di applicabilità del modello a varie situazioni reali.

Questa dichiarazione sui limiti autorizza a procedere nello studio delle caratteristiche del modello al fine di ottenere risultati piùampiamente applicabili.

In particolare risulta opportuno servirsi di un linguaggio che presuppone che la estensione e la precisione ottenibili per il modello siano migliorabili quanto si vuole, salvo abbandonare tale presupposto ideale nelle situazioni applicative nelle quali non risulta attuabile. (va prevista la falsificazione del modello).

In effetti sappiamo dall'inizio del XX secolo, in seguito ai progressi della fisica dell'atomo e delle particelle elementari e agli sviluppi dell'astrofisica, che la presupposta ipotesi della estensione e della precisione illimitatamente aumentabili incontra limiti invalicabili che possono essere quantificati ricorrendo alle teorie meccanico-statistiche, relativistiche e quantistiche. [e.g.`moto browniano (wi)`, `raggi catodici (wi)`, modelli per la `spettroscopia (wi)`].

Tuttavia per la spiegazione di molti fenomeni la precisione del modello GFC risulta sufficiente, ossia è sensato assumerla sufficiente; in questi casi risulta accettabile esprimersi confondendo le componenti del modello, ossia gli oggetti osservabili idealizzati, con le entità formali che li rappresentano.
accade in molti contesti che l'assunzione del modello GFC consente argomentazioni scorrevoli, cosa molto vantaggioso sul piano della didattica.

B20 b.05 La prima fase costruttiva del modello GFC per $\mathbb{Z} \times \mathbb{Z}$ concerne una linea di riferimento equivalente a una retta-Z che nei fogli o negli schermi digitali che utilizziamo per comunicare raffiguriamo come orizzontale, senza tuttavia preoccuparci della collocazopme di questi fogli e schermi nello spazio fisico.

Si traccia dunque una linea "orizzontale" sufficientemente rettilinea, sottile ed estesa in grado di dare l'idea di una linea retta ideale "illimitatamente sottile ed estesa", servendosi di strumenti di elevata precisione, vuoi meccanici, vuoi costituiti da segnali luminosi o da altre radiazioni elettromagnetiche (ad esempio fornita da un dispositivo laser) peottenere quella che giudichiamo una buona rettilineità.

Questo è un modello osservabile per una linea ideale che chiamiamo **retta di riferimento orizzontale**; anticipando i discorsi che svilupperemo parlando del piano $\mathbb{R} \times \mathbb{R}$ [B43], in breve la denoteremo con Ox_{ZZ}; questo simbolo spessp (icsue) lo possiamo semplificare in Ox.

Nella seconda fase costruttiva si fissa, una unità di misura per le lunghezze che servirà per stabilire distanze tra i punti che stiamo per definire.
Per questo si sceglie un "regolo campione" costituito da un solido con proprietà meccaniche e termiche tali da assicurare una sua buona invariabilità allo scorrere del tempo, al variare della sua posizione e della sua orientazione e anche a contenute variazioni della temperatura; più modernamente potremmo servirci di un procedimento spettroscopico [`Metro (wi)`].

Si cura che la sua estensione possa essere riprodotta in tutti gli ambienti praticabili (nei quali possa servire) da compassi da costruire anch'essi con opportune tecniche di precisione.
Si trascura invece il fatto che la riproducibilità delle lunghezze incontra limiti che emergono nelle condizioni che richiedono di adottare la `relatività ristretta (wi)` [P60].

B20 b.06 Sulla retta di riferimento orizzontale si fissa un punto che si dice **origine del piano-ZZ** e a esso si associa l'elemento $\langle 0,0\rangle$ di $\mathbb{Z}\times\mathbb{Z}$.
Sulla destra dell'origine alla distanza unitaria fornita dal compasso si individua il punto che si associa alla coppia $\langle 1,0\rangle$.

Spostandosi sulla retta di riferimento verso destra con passi unitari determinati dal compasso, si individuano successivamente i punti $\langle i,0\rangle$ per $i=2,3,...,N$ e sulla sinistra i punti $\langle -1,0\rangle$, $\langle -2,0\rangle$, $\langle -3,0\rangle$, ... ,$\langle -N,0\rangle$.
In tal modo si può avvicinare la definizione del modello dell'insieme $\{i\in\mathbb{Z}:|\ \langle i,0\rangle\}$ quanto lo richiedono le applicazioni prospettate. Questo insieme viene chiamato **primo asse-Z di riferimento**, **asse-Z orizzontale**, **asse-ZZH** o **asse-ZZ delle ascisse**.
Esso lo si denota concisamente con Ox_{ZZ}, simbolo che spesso si può semplificare in Ox.

A questo punto conviene introdurre la notazione $+\infty$ con due significati: (a) come componente del costrutto $[h:+\infty)$ con il quale si individua l'insieme degli interi relativi superiori o uguali all'intero h; (b) come elemento di espressioni quale "tendere a $+\infty$ di un intero variabile che va assumendo valori sempre più elevati".

Simmetricamente si introduce la notazione $-\infty$, utile all'espressione $(-\infty:k]$ con il quale si individua l'insieme degli interi relativi inferiori o uguali all'intero k e una componente di espressioni quali "tendere a $-\infty$ di un intero variabile che va assumendo valor sempre più negativi".

Possiamo anche introdurre la notazione $\pm\infty$ per denotare un oggetto che può essere aut $-\infty$ aut $+\infty$. Essa in particolare può servire a caratterizzare un intero variabile che va assumendo valori sia positivi che negativi sempre più grandi in valore assoluto.

Conviene sottolineare, per il seguito, che sono state effettuate alcune scelte in modo arbitrario, senza curarsi di possibili vincoli pratici o di principio: le scelte dell'unità di misura, dell'origine delle coordinate e dell'orientazione dell'asse di riferimento.

B20 b.07 Utilizziamo ora un compasso dotato di una seconda punta in grado di tracciare curve sottili quanto serve; puntandolo successivamente nei punti $\langle 1,0\rangle$ e $\langle -1,0\rangle$ e apertura superiore ad 1 (ad esempio pari a 2) si tracciano due archi che si intersecano in due punti come in figura e si individua una retta materiale sufficientemente sottile ed estesa passante per questi due punti; questa retta viene chiamata "seconda retta di riferimento".

Su questa retta con il compasso si individuano i punti $\langle 0,1\rangle$, $\langle 0,2\rangle$, $\langle 0,3\rangle$, ... muovendosi al di sopra dell'origine e verso l'alto e i punti $\langle 0,-1\rangle$, $\langle 0,-2\rangle$, $\langle 0,-3\rangle$, ... muovendosi al di sotto dell'origine verso il basso.

In tal modo si viene a definire il modello dell'insieme $\{j\in\mathbb{Z}:|\ \langle 0,j\rangle\}$, insieme detto **secondo asse-ZZ di riferimento**, **asse-ZZ verticale**, **asse-ZZV** o **asse-ZZ delle ordinate**.
Esso lo si denota concisamente con Oy_{ZZ}, simbolo che spesso si può semplificare in Oy.

Si effettuano successivamente le costruzioni analoghe delle rette verticali passanti per i punti $\langle i,0\rangle$ di Ox servendosi del compasso con seconda punta tracciante imperniato nelle coppie di punti $\langle i-1,0\rangle$

e $\langle i+1, 0\rangle$. Su queste rette operando con il compasso con apertura unitaria si individuano quanti si vogliono punti $\langle i, j\rangle \in \mathbb{Z} \times \mathbb{Z}$.

B20 b.08 Sul piano-ZZ, aiutandoci con il linguaggio del modello GFC, si individuano varie nozioni di natura geometrica.

Due punti-ZZ della forma $\langle i, j\rangle$ e $\langle i, j+1\rangle$ si dicono **punti-ZZ adiacenti-ZZH**; due punti-ZZ della forma $\langle i, j\rangle$ e $\langle i+1, j\rangle$ si dicono **punti-ZZ adiacenti-ZZV**; due punti-ZZ della forma $\langle i, j\rangle$ e $\langle i+1, j+1\rangle$ si dicono **punti-ZZ adiacenti-ZZD1**; due punti-ZZ della forma $\langle i, j\rangle$ e $\langle i+1, j-1\rangle$ si dicono **punti-ZZ adiacenti-ZZD2**.

Abbiamo quindi individuate quattro relazioni tra elementi di $\mathbb{Z} \times \mathbb{Z}$: **adiacenza-ZZH**, **adiacenza-ZZV**, **adiacenza-ZZD1** e **adiacenza-ZZD2**.
L'unione delle due relazioni di adiacenza-ZZH e adiacenza-ZZV e si dice **adiacenza-ZZR**. La lettera R che caratterizza questa specificazioni e varie altre notazioni riguardanti $\mathbb{Z} \times \mathbb{Z}$ richiama i movimenti della torre del gioco degli scacchi, in inglese *rook*.

L'unione delle due relazioni di adiacenza-ZZD1 e adiacenza-ZZD2 e si dice **adiacenza-ZZB**. La lettera B che caratterizza questa specificazione e altre notazioni concernenti $\mathbb{Z} \times \mathbb{Z}$ richiama i movimenti dell'alfiere del gioco degli scacchi, in inglese *bishop*.

L'unione delle due relazioni di adiacenza-ZZR e adiacenza-ZZB e si dice **adiacenza-ZZK**. La lettera K che caratterizza questa relazione e altre nozioni di $\mathbb{Z} \times \mathbb{Z}$ richiama i movimenti del re del gioco degli scacchi, in inglese *king*.

Tutte queste relazioni sono banalmente decidibili a partire dalle due coordinate caratterizzanti ciascun punto da indagare.

B20 b.09 Chiamiamo **segmenti-ZZH elementari** i duetti di punti adiacenti-ZZH, cioè gli insiemi esprimibili come $\{\langle i, j\rangle, \langle i, j+1\rangle\}$; diciamo **segmenti-ZZV elementari** i duetti di punti adiacenti-ZZV, cioè gli insiemi aventi la forma $\{\langle i, j\rangle, \langle i+1, j\rangle\}$; collettivamente questi duetti di punti-ZZ si dicono **segmenti-ZZ1R elementari**.
Se $\{P, Q\}$ è uno di questi duetti, i punti P e Q si dicono **estremità del segmento**.

Diciamo **casella-ZZ** ogni entità individuata da un quartetto di punti-ZZ della forma

$$\{\langle i, j\rangle,\ \langle i+1, j\rangle,\ \langle i, j+1\rangle,\ \langle i+1, j+1\rangle\}\ .$$

Il termine "casella-ZZ" spesso si può semplificare in **casella**.
I quattro punti precedenti si dicono **vertici della casella**; tra questi punti con notazioni geografiche di evidente significato si distinguono il vertice SE, il vertice NE, il vertice NW e il vertice SW.
Si dicono invece **lati della casella** i duetti di punti

$$\{\langle i, j\rangle, \langle i+1, j\rangle\},\ \{\langle i+1, j\rangle, \langle i+1, j+1\rangle\},\ \{\langle i+1, j+1\rangle, \langle i, j+1\rangle\} \text{ e } \{\langle i, j+1\rangle, \langle i, j\rangle\}\ ,$$

cioè i duetti di vertici adiacenti della casella.
Tra questi quattro lati si distinguono, attraverso le lettere associate ai quattro punti cardinali, risp., il lato S, il lato E, il lato N e il lato W.

Due vertici di una casella-ZZ che non sono adiacenti-ZZR si dicono **vertici opposti** della casella; due tali punti-ZZ si dicono anche **punti adiacenti-ZZB**.

Gli insiemi di caselle-ZZ si dicono anche **insiemi-ZZC**.

Diciamo **segmenti-ZZD1 elementari** i duetti di punti-ZZ della forma $\{\langle i,j\rangle, \langle i+1, j+1\rangle\}$; chiamiamo **segmenti-ZZD2 elementari** i duetti di punti-ZZ della forma $\{\langle i,j\rangle, \langle i+1, j-1\rangle\}$; collettivamente i segmenti-ZZD1 elementari e i segmenti-ZZD2 elementari si dicono **segmenti-ZZB elementari**. Collettivamente i segmenti-ZZR elementari ed segment-ZZB elementari si dicono **segmenti-ZZK elementari**.

Due segmenti-ZZK elementari si dicono **segmenti-ZZK adiacenti** sse hanno un solo vertice in comune.

Due caselle-ZZ si dicono **caselle adiacenti-ZZR** sse hanno un (solo) lato-ZZ1R in comune; si dicono inoltre **caselle adiacenti-ZZB** sse hanno in comune un (solo) vertice; si parla invece di **caselle adiacenti-ZZK** sse sono adiacenti-ZZR o adiacenti-ZZB.

B20 b.10 La struttura costituita da punti-ZZ, caselle-ZZ e segmenti-ZZR elementari verrà chiamata **griglia combinatoria**. Per molti discorsi, per esempio per definire le nozioni di circuito-ZZ e di area con segno [B21r], risulta utile servirsi di questo arricchimento dell'insieme $\mathbb{Z} \times \mathbb{Z}$.

Nel modello osservabile GFC i lati si possono far corrispondere ad aste sottili che uniscono i loro punti estremità.
Si possono invece adottare come rappresentanti materiali delle caselle delle piastrelle quadrate ovvero delle tessere di un mosaico, che siano accuratamente intercambiabili e che abbiano i vertici fisici collocati in punti-ZZ.

Oltre a queste relazioni tra elementi delle varie nature della griglia combinatoria, risulta utile introdurre in una prima forma una relazione di portata generale, l'**incidenza**, che riguarda duetti di entità che tipicamente sono oggetti geometrici di natura diversa.

Cominciamo a definire l'incidenza tra un punto-ZZ e un segmento-ZZ elementare, tra un punto-ZZ e una casella-ZZ e tra un segmento-ZZ elementare e una casella-ZZ.

Si dice che un punto-ZZ e un segmento-ZZK elementare sono incidenti sse il punto è un'estremità del segmento.
Si dice che un punto-ZZ e una casella-ZZ sono incidenti sse il punto è un vertice della casella.
Si dice che un segmento-ZZR elementare e una casella-ZZ sono incidenti sse il segmento è lato della casella.

B20 b.11 Accanto all'asse Ox_{ZZ} e all'asse Oy_{ZZ}, introduciamo altri semplici sottoinsiemi di $\mathbb{Z} \times \mathbb{Z}$.

Si dice diagonale principale-ZZ, o semplicemente **diagonale-ZZ**, l'insieme evidentemente numerabile $\{i \in \mathbb{Z} :| \langle i,i\rangle\}$.

Si dice diagonale secondaria-ZZ o **codiagonale-ZZ** di $\mathbb{Z} \times \mathbb{Z}$ l'insieme numerabile $\{i \in \mathbb{Z} :| \langle i,-i\rangle\}$.

Si introducono senza difficoltà i sottoinsiemi di $\mathbb{Z} \times \mathbb{Z}$ infiniti, evidentemente numerabili, che generalizzano assi e diagonali:

Per ogni $k \in \mathbb{Z}$ si dice **retta-ZZ orizzontale** o **retta-ZZH** l'insieme $\{i \in \mathbb{Z} :| \langle i,k\rangle\}$.

Per ogni $h \in \mathbb{Z}$ si definisce **retta-ZZ verticale** o **retta-ZZV** l'insieme $\{j \in \mathbb{Z} :| \langle h,j\rangle\}$.
Collettivamente le rette-ZZH e le rette-ZZV si dicono **rette-ZZR**.

Per ogni $s \in \mathbb{Z}$ si dice **retta-ZZD1** o parallela-ZZ alla diagonale principale: $\{i \in \mathbb{Z} :| \langle i+s,i\rangle\}$;
Per ogni $s \in \mathbb{Z}$ si dice **retta-ZZD2** o parallela-ZZ alla diagonale secondaria: $\{i \in \mathbb{Z} :| \langle i+s,-i\rangle\}$.

Collettivamente le rette-ZZD1 e le rette-ZZD2 si dicono **rette-ZZB**.

Collettivamente le rette-ZZR e le rette-ZZB si dicono **rette-ZZK**.

Ancora le lettere R, B e K che distinguono le specificazioni sincopate attribuite alle precedenti entità derivano, risp., dai termini scacchistici *rook*, *bishop* e *king*.

B20 b.12 Sopra un modello osservabile fisico costruito con la adeguata accuratezza si possono verificare sperimentalmente e con buona approssimazione alcuni fatti.

(1) Due diverse rette verticali non hanno alcun punto in comune (in accordo con il fatto che per i e h interi diversi gli insiemi $\{j \in \mathbb{Z} :| \langle i, j\rangle\}$ e $\{j \in \mathbb{Z} :| \langle h, j\rangle\}$ sono disgiunti).
(2) Due diverse rette orizzontali non presentano punti in comune, similmente a quanto visto in (1).
(3) Due diverse retta-ZZD1 e due diverse retta-ZZD2 non presentano punti in comune, per motivi analoghi a quello visto in (1).
(4) Per ogni $i \in \mathbb{Z}$ i punti $\langle i, j\rangle$ al variare di $j \in \mathbb{Z}$, punti di ciascuna delle retta-ZZV, sono otticamente allineati;
(5) Similmente risultano otticamente allineati i punti di ciascuna delle rette-ZZH, di ciascuna delle rette-ZZD1 e di ciascuna delle rette-ZZD2.
(6) Muovendo una sagoma S quadrata di materiale con buone doti di indeformabilità inizialmente sovrapposta con buona precisione a una casella-ZZ C la si può similmente sovrapporre a una qualsiasi altra casella-ZZ C' avvicinando due dei propr vertici ai vertici rispettivi omologhi della C'. Questo è in accordo con la possibilità di individuare una corrispondenza biunivoca dell'insieme-ZZC con se stesso (ossia una permutazione dell'insieme-ZZC) che mantenga le relazioni di adiacenza-ZZH e di adiacenza-ZZV tra caselle, corrispondenza che alla C faccia corrispondere la C' [v.a. le considerazioni sulle traslazioni-ZZ in B21f].
(7) Analoga possibilità di sovrapporre caselle collocate opportunamente in seguito a a riflessioni rispetto a rette-ZZK e rispetto a rette-ZZB (queste verifiche saranno precisate in B22a.
(8) Analoga possibilità di sovrapporre caselle collocate opportunamente in seguito a rotazioni di 90°, di 180° e di 270° (queste verifiche saranno precisate in B22b e in B22d.

B20 b.13 Come accennato, il piano combinatorio $\mathbb{Z} \times \mathbb{Z}$ può essere raffigurato in vari modi, ciascuno dei quali presenta qualche vantaggio. Una distinzione riguarda le raffigurazioni che chiamiamo geografiche e quelle dette matriciali; un'altra contrappone le raffigurazioni mediante punti (o nodi) e quelle che si servono di caselle (o tessere).

Nella **raffigurazione geografica mediante punti** le rette orizzontali riguardano i nodi $\langle i, j\rangle \in \mathbb{Z} \times \mathbb{Z}$ con la prima componente variabile e crescente da sinistra a destra e con la seconda componente fissa; le rette verticali riguardano i nodi con la prima componente fissa e la seconda crescente dal basso verso l'alto.

Essa spesso viene considerate una riduzione della usuale raffigurazione del piano cartesiano, limitata ai soli punti con entrambe le coordinate intere. Questa raffigurazione è la più usata e sarà chiamata anche raffigurazione normale.

La **raffigurazione matriciale mediante punti** si può pensare ottenuta dalla precedente mediante una rotazione del foglio di un quarto di angolo giro, 90°, nel verso orario, ossia nel verso del movimento dalle lancette di un orologio a quadrante.

Nelle **raffigurazioni mediante caselle** i punti sono rimpiazzati da quadratini adiacenti. Questi quadratini, fin tanto che ci si limita a trattare $\mathbb{Z} \times \mathbb{Z}$, sono da considerare elementari, indivisibili, e i loro lati di lunghezza unitaria (grandezza che in linea di principio, va ricordato, si può scegliere in modo arbitrario).

B20 b.14 Per molte considerazioni la scelta della raffigurazione è poco rilevante, in quanto è facile passare dall'una all'altra.
Quando si devono trattare molti dettagli è comunque necessario precisare quale raffigurazione si adotta per evitare ambiguità: espressioni di largo uso come " orizzontale", "verticale", "più a destra", "immediatamente sotto", "altezza" e "larghezza" usate per la raffigurazione geografica da un lato e per la matriciale dall'altro individuano oggetti che si raffigurano ben diversamente.

Le raffigurazioni mediante caselle sono convenienti per la presentazione di molte funzioni aventi come dominio $\mathbb{Z} \times \mathbb{Z}$ o una sua parte. Questo accade per le matrici finite speciali che vengono presentate come schieramenti dei valori assunti da funzioni di un genere come $\{(m) \times (n)\}$ e per le matrici numerabili trattate inparticolare in D20.

Per le raffigurazioni matriciali alle rette-ZZH corrispondono colonne infinite, alle rette-ZZV righe infinite, alle rette-ZZD1 corrispondono gli allineamenti obliqui che vanno dall'alto a sinistra verso il basso a destra (da NW a SE), mentre alle rette-ZZD2 corrispondono gli allineamenti obliqui che vanno dal basso a sinistra all'alto a destra (da SW a NE).

Nella raffigurazione geografica mediante caselle:
una retta-ZZH si dice anche riga illimitata,
una retta-ZZV si dice anche colonna illimitata,
una retta-ZZD1 si dice anche scala crescente illimitata,
una retta-ZZD2 si dice anche scala decrescente illimitata.

Nelle raffigurazioni geografiche la diagonale principale si dice anche diagonale-ZZ crescente, mentre la secondaria si dice diagonale-ZZ decrescente.
I due aggettivi crescente e decrescente vanno scambiati quando si fa riferimento alla raffigurazione matriciale.

B20 c. somma e differenza di interi

B20 c.01 Procediamo a estendere a $\mathbb{Z}$ le operazioni di somma e differenza. Per questo conviene confrontare $\mathbb{Z}\times\mathbb{Z}$ a $\mathbb{N}\times\mathbb{N}$ e presentare considerazioni facilmente visualizzabili che, come vedremo, servono anche per introdurre altre nozioni geometriche.

Come vedremo, risulta opportuno mantenere per la differenza la proprietà di invarianza per incremento di una stessa quantità degli operandi espressa dall'enunciato

$$\forall k\in\mathbb{N}\ :\ (n+k)-(m+k)\ =\ n-m\ .$$

Iniziamo con considerazioni immediatamente visualizzabili. Chiamiamo **successore-N** la relazione, più precisamente la funzione, che collega un qualsiasi intero naturale al suo successivo, cioè l'insieme di coppie $\{z\in\mathbb{N}:|\ \langle z,z+1\rangle\}$.
Inoltre chiamiamo **predecessore-N** la relazione sua trasposta cioè l'insieme di coppie $\{z\in\mathbb{N}:|\ \langle z+1,z\rangle\}$ e **adiacenza-N** la relazione unione di successore-N e predecessore-N.

Ciascuna di queste tre relazioni, tra di loro biunivocamente collegate, fornisce la caratterizzazione strutturale di base della retta-Z.
Si osserva innanzi tutto che ogni elemento di $\mathbb{N}$ può essere raggiunto dall'elemento 0 mediante gli spostamenti associabili aut alle coppie di interi naturali costituenti la relazione successore-N, aut a quelle costituentipredecessore-N.

Le operazioni di somma e differenza tra interi naturali conservano la relazione successore-N: infatti se a e b sono interi naturali con $b=a+1$, per ogni $k\in\mathbb{N}$ sono nella stessa relazione, risp., $a+k$ con $b+k$ e $a-k$ con $b-k$ mentre $k-a$con $k-b$ sono nella relazione predecessore-N (ammesso che queste ultime coppie facciano parte di $\mathbb{N}\times\mathbb{N}$).

Queste conservazioni di relazioni corrisponde al fatto che i due corrispondenti insiemi di coppie in $\mathbb{N}\times\mathbb{N}$ costituiscono le due semirette-NND1 parallele alla diagonale principale che a essa sono le più vicine.

B20 c.02 Vogliamo ora estendere queste relazioni al piano $\mathbb{Z}\times\mathbb{Z}$ chiedendo che siano relazioni mantenute dalle operazioni di somma e differenza in $\mathbb{Z}\times\mathbb{Z}$.
Il mantenimento da parte della somma equivale a dire che questi insiemi di coppie siano invarianti per scorrimento parallelo alla diagonale principale.

Quindi definiamo relazione **successore-Z** l'insieme di coppie $\{z\in\mathbb{Z}:|\ \langle z,z+1\rangle\}$, relazione **predecessore-Z** l'insieme $\{z\in\mathbb{Z}:|\ \langle z+1,z\rangle\}$ e relazione **adiacenza-Z** l'unione di queste due relazioni.
Le relazioni successore-Z e predecessore-Z entro $\mathbb{Z}\times\mathbb{Z}$ consistono nelle due rette-ZZD1 adiacenti alla diagonale principale di $\mathbb{Z}\times\mathbb{Z}$, prolungamenti delle semirette-ZZ concernenti le relazioni omologhe per $\mathbb{N}\times\mathbb{N}$.

Si osserva che le relazioni predecessore-Z e successore-Z sono permutazioni di $\mathbb{Z}$. In quanto endofunzioni si possono denotare, risp., con le notazioni funzionali $\boldsymbol{prec}(n)$ e $\boldsymbol{succ}(n)$ e si possono interpretare come meccanismi che provocano spostamenti dei punti di $\mathbb{Z}$.

B20 c.03 Dopo avere esteso $\mathbb{N}$ illimitatamente sulla sua sinistra, si è indotti a estendere la differenza prolungando nella direzione SW le semirette-ZZD1 e mantenendo in esse i valori d o $\overline{d}$, ottenendo in definitiva la tavola di composizione:

$\overline{10}$	$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{\mathbf{5}}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$	0
$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{\mathbf{4}}$	$\overline{3}$	$\overline{2}$	$\overline{1}$	0	1
$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{\mathbf{3}}$	$\overline{2}$	$\overline{1}$	0	1	2
$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{\mathbf{2}}$	$\overline{1}$	0	1	2	3
$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{\mathbf{1}}$	0	1	2	3	4
$\overline{\mathbf{5}}$	$\overline{\mathbf{4}}$	$\overline{\mathbf{3}}$	$\overline{\mathbf{2}}$	$\overline{\mathbf{1}}$	**0**	**1**	**2**	**3**	**4**	**5**
$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$	0	**1**	2	3	4	5	6
$\overline{3}$	$\overline{2}$	$\overline{1}$	0	1	**2**	3	4	5	6	7
$\overline{2}$	$\overline{1}$	0	1	2	**3**	4	5	6	7	8
$\overline{1}$	0	1	2	3	**4**	5	6	7	8	9
0	1	2	3	4	**5**	6	7	8	9	10

Da questa tabella avente come dominio $\mathbb{Z} \times \mathbb{Z}$ si ricava, innanzi tutto, che scambiando i due operandi della differenza si passa da un valore positivo p al numero negativo opposto $\overline{p}$ e viceversa da un intero negativo $\overline{q}$ al suo opposto positivo q.
Il passaggio all'intero opposto risulta quindi una involuzione entro $\mathbb{Z}$ avente come unico punto fisso l'elemento 0.

Si osserva poi che:

$$(1) \qquad \forall\, m,n \in \mathbb{N} \;:\; \begin{array}{llll} n-\overline{m}=n+m & \overline{n}-m=\overline{n+m} & \overline{n}-\overline{m}=m-n & \\ 0-m=\overline{m} & n-0=n & 0-\overline{m}=m & \overline{n}-0=\overline{n} \end{array} .$$

Si può allora osservare che il numero opposto di un qualsiasi intero z si può esprimere come $\overline{z}$ o, più convenientemente, con $-z$.
Inoltre il carattere involutorio del passaggio all'opposto si esprime mediante l'identità $\overline{\overline{z}}=z$ e le 4 precedenti uguaglianze si riscrivono come segue:

$$(1) \qquad \forall z,w \in \mathbb{Z} \;:\; 0-z=\overline{z} \qquad z-0=z \qquad z-w=\overline{w}-\overline{z}=\overline{w-z} \;.$$

B20 c.04 Procediamo ora di estendere la somma a tutte le coppie di interi; anche per questo procediamo a una analoga estensione a $\mathbb{Z} \times \mathbb{Z}$ della presentazione geografica su $\mathbb{N} \times \mathbb{N}$ dell'operazione:

⋮	⋮	⋮	⋮	⋮	⋮	⋰
5	6	7	8	9	10	...
4	5	6	7	8	9	...
3	4	5	6	7	8	...
2	3	4	5	6	7	...
1	2	3	4	5	6	...
0	**1**	**2**	**3**	**4**	**5**	...

Per mantenere la proprietà espressa dalla $\forall\, k \in \mathbb{N} : m+n=(m+k)+(n-k)$ basta passare a $\mathbb{Z} \times \mathbb{Z}$ e attribuire lo stesso valore a tutte le caselle di $\mathbb{Z} \times \mathbb{Z}$ costituenti ciascuna delle rette-ZZD2, le parallele alla codiagonale: in una prima fase si estendono verso SE e NW i segmenti del primo quadrante e successivamente si procede ad assegnare i valori $\overline{p}$ per $p = 1, 2, 3, ...$ alle rette-ZZD2 via

via più spostate verso SW. Alla fine si ottiene:

0	1	2	3	4	**5**	6	7	8	9	10
$\overline{1}$	0	1	2	3	**4**	5	6	7	8	9
$\overline{2}$	$\overline{1}$	0	1	2	**3**	4	5	6	7	8
$\overline{3}$	$\overline{2}$	$\overline{1}$	0	1	**2**	3	4	5	6	7
$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$	0	**1**	2	3	4	5	6
5	**4**	**3**	**2**	**1**	**0**	**1**	**2**	**3**	**4**	**5**
$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	**$\overline{1}$**	0	1	2	3	4
$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	**$\overline{2}$**	$\overline{1}$	0	1	2	3
$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	**$\overline{3}$**	$\overline{2}$	$\overline{1}$	0	1	2
$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	**$\overline{4}$**	$\overline{3}$	$\overline{2}$	$\overline{1}$	0	1
$\overline{10}$	$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	**$\overline{5}$**	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$	0

Si nota che la precedente tavola di composizione si ottiene da quella per la differenza riflettendola rispetto alla retta orizzontale relativa ad $m = 0$, cioè scambiando i valori di m con gli opposti; questo fatto equivale all'uguaglianza $n + m = n - \overline{m}$.
Si osserva anche che l'estensione equivale alle scelte:

(1) $$n + \overline{m} := n - m \qquad \overline{n} + m := m - n \qquad \overline{n} + \overline{m} := \overline{n + m} .$$

Infine si osserva che estendendo la somma da $\mathbb{N} \times \mathbb{N}$ a $\mathbb{Z} \times \mathbb{Z}$ si mantengono le sue principali proprietà: la sua simmetria (ovvero la sua commutatività) e la sua associatività.

B20 d. prodotto di interi

B20 d.01 È evidentemente utile estendere a $\mathbb{Z}\times\mathbb{Z}$ il prodotto di naturali per ampliare la portata della operazione prodotto.
Anche per questa estensione si procede ad ampliare a $\mathbb{Z}\times\mathbb{Z}$ la presentazione tabellare su $\mathbb{N}\times\mathbb{N}$ dell'operazione:

⋮	⋮	⋮	⋮	⋮	⋮	⋰
0	5	10	15	20	25	...
0	4	8	12	16	20	...
0	3	6	9	12	15	...
0	2	4	6	8	10	...
0	1	2	3	4	5	...
0	**0**	**0**	**0**	**0**	**0**	...

Si trova utile mantenere per la moltiplicazione di un naturale n per un intero z il compito di esprimere la somma di n addendi uguali a z: quindi si chiede

$$\forall\, z\in\mathbb{Z}\ ,\ n\in\mathbb{N}\ \ :\ \ n\cdot z\ :=\ \underbrace{z+z+\cdots z}_{n-volte}\ . \tag{1}$$

In particolare, procedendo per induzione su m, si trova

$$\forall z\in\mathbb{Z}\ ,\ n\in\mathbb{N}\ \ :\ \ n\cdot\overline{m}\ =\ \underbrace{\overline{m}+\overline{m}+\cdots+\overline{m}}_{n-volte}\ =\ \overline{n\cdot m}\ . \tag{2}$$

La precedente richiesta consente applicazioni come quella riguardante il calcolo del debito complessivo di n debitori che devono a un creditore una stessa quantità di denaro m o quella riguardante la valutazione dell'arretramento complessivo dovuto all'applicazione di n arretramenti successivi, tutte della stessa estensione m.

Inoltre si trova decisamente vantaggioso chiedere di mantenere la simmetria dell'operazione definendo

$$\forall\, m\in\mathbb{Z}\ ,\ n\in\mathbb{N}\ :\ \overline{n}\cdot m\ :=\ \overline{n\cdot m}\ . \tag{3}$$

Seguendo lo stesso criterio di perseguire vantaggi operativi ed espositivi si richiede infine la completa simmetria della tabella del prodotto rispetto al centro $\langle 0,0\rangle$ ponendo

$$\forall m,n\in\mathbb{Z}\ :\ \overline{n}\cdot\overline{m}\ :=\ n\cdot m\ . \tag{4}$$

La presentazione tabellare geografica del prodotto di interi assume allora il seguente aspetto simmetrico (agevolmente controllabile):

$\overline{25}$	$\overline{20}$	$\overline{15}$	$\overline{10}$	$\overline{5}$	**0**	5	10	15	20	25
$\overline{20}$	$\overline{16}$	$\overline{12}$	$\overline{8}$	$\overline{4}$	**0**	4	8	12	16	20
$\overline{15}$	$\overline{12}$	$\overline{9}$	$\overline{6}$	$\overline{3}$	**0**	3	6	9	12	15
$\overline{10}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	**0**	2	4	6	8	10
$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$	**0**	1	2	3	4	5
0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
5	4	3	2	1	**0**	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
10	8	6	4	2	**0**	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{10}$
15	12	9	6	3	**0**	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{12}$	$\overline{15}$
20	16	12	8	4	**0**	$\overline{4}$	$\overline{8}$	$\overline{12}$	$\overline{16}$	$\overline{20}$
25	20	15	10	5	**0**	$\overline{5}$	$\overline{10}$	$\overline{15}$	$\overline{20}$	$\overline{25}$

Si osserva che la richiesta di mantenimento del prodotto da parte della simmetria rispetto all'origine equivale al mantenimento da parte della riflessione rispetto all'asse orizzontale seguita (o preceduta) dalla riflessione rispetto all'asse verticale.

L'opportunità della scelta della simmetria si rivelerà pienamente con l'introduzione delle aree con segno per figure-ZZ orientate [B24d, [B24h].

B20 d.02 La scrittura $\overline{z}$ si può considerare una semplificazione di una scrittura di forma esponenziale come z^{-e}, scrittura nella quale compare un operatore unario in posizione esponenziale.
Si può considerare come sua alternativa del tutto equivalente una scrittura che si serve di un operatore unario prefisso chiamato **meno unario**, che scriviamo $-_u$ esprime la involuzione $\mathsf{Mirr}_{0,\mathbb{Z}} := \lceil z \in \mathbb{Z} \mapsto \overline{z} \rceil$, cioè il passaggio all'intero opposto; la notazione Mirr_0 è stata scelta in vista della generalizzazione che introduciamo in e03.

La notazione $-_u z$ consente di esprimere le uguaglianze

$$(1)\quad \forall m,n\in\mathbb{Z}\ :\ -_u\, m \;=\; (-_u 1)\cdot m \qquad,\qquad n-m \;=\; n+(-_u m) \qquad,\qquad 0-m \;=\; -_u m\ .$$

In genere il segno meno unario viene scritto come il binario: questo apre la possibilità di scritture ambigue che però in genere il contesto consente di interpretare con la corretta distinzione.

B20 d.03 L'ordine totale $\leq$ si estende dagli interi naturali a tutti gli interi relativi in accordo con la raffigurazione di $\mathbb{Z}$ con gli interi negativi allineati alla sinistra dei numeri naturali.

Per due interi positivi qualsiasi si definisce quanto segue.

$$(1)\qquad \forall m,n\in\mathbb{P}\ :\ -_u\, n \;<\; 0 \;<\; m \qquad \text{e} \qquad -_u\, n \;<\; -_u m \iff m \;<\; n\ .$$

Le proprietà di antisimmetria e di transitività della relazione "<" si verificano facilmente.

Dopo questa definizione si estendono facilmente dai naturali a tutti gli interi, cioè da $\mathbb{N}$ all'intero $\mathbb{Z}$, le nozioni di intervallo e le funzioni massimo e minimo.

$$(2)\qquad \forall w,z\in\mathbb{Z}\ :\ \mathbf{[}w:z\mathbf{]} \;:=\; \begin{cases} \{w,w+1,...,z\} & \text{sse } w<z\ , \\ \{w\} & \text{sse } w=z\ , \\ \emptyset & \text{sse } w>z\ ; \end{cases}\ .$$

$$(3)\qquad \mathbf{(}w:z\mathbf{]} \;:=\; \mathbf{[}w:z\mathbf{]}\setminus\{w\} \quad,\quad \mathbf{[}w:z\mathbf{)} \;:=\; \mathbf{[}w:z\mathbf{]}\setminus\{z\} \quad,\quad \mathbf{(}w:z\mathbf{)} \;:=\; \mathbf{[}w:z\mathbf{]}\setminus\{w,z\}\ .$$

$$(4)\qquad \max(w,z) \;:=\; \begin{cases} z & \text{se } w\leq z\ , \\ w & \text{se } z\leq w\ ; \end{cases} \qquad \min(w,z) \;:=\; \begin{cases} w & \text{se } w\leq z\ , \\ z & \text{se } z\leq w\ ; \end{cases}\ .$$

Si dimostrano facilmente le seguenti proprietà

$$\max(w,z) \;=\; \max(z,w) \quad,\quad \min(w,z) \;=\; \min(z,w) \quad,\quad \max(w,z)=z \iff \min(w,z)=w\ .$$

Si introducono anche gli intervalli illimitati di interi:

$$(5)\quad \forall z\in\mathbb{Z}\ :\ \mathbf{(}-\infty:z\mathbf{]} \;:=\; \{k\in\mathbb{Z}\ \S\ k\leq z\} \;=\; \{...,z-1,z\}\ ,\mathbf{(}-\infty:z\mathbf{)} \;=\; \{...,z-1\}$$

$$(6)\quad \forall z\in\mathbb{Z}\ :\ \mathbf{[}w:+\infty\mathbf{)} \;:=\; \{k\in\mathbb{Z}\ \S\ w\leq k\} \;=\; \{w,w+1,...\}\ ,\mathbf{(}w:+\infty\mathbf{)} \;=\; \{w+1,...\}$$

$$(7)\qquad \mathbf{(}-\infty:+\infty\mathbf{)} \;:=\; \mathbb{Z}\ .$$

(8) Eserc. Per i cardinali degli intervalli finiti verificare le uguaglianze

(a) $[m,n]^{\#} \;=\; \max(m-n+1,0)$;
(b) $(m,n]^{\#} \;=\; [m,n)^{\#} \;=\; \max(m-n,0)$;
(c) $(m,n)^{\#} \;=\; \max(m-n-1,0)$.

B20 d.04 Spesso risultano utili due funzioni su $\mathbb{Z}$: il **valore assoluto** di $z \in \mathbb{Z}$ denotato con $\mathrm{abs}(z)$, oppure concisamente mediante delimitatori con $|z|$, ed la funzione **segno** di $z \in \mathbb{Z}$ denotata con $\mathrm{sign}(z)$, definite come segue.

(1) $$|z| \;:=\; \mathrm{abs}(z) \;:=\; \begin{cases} z & \text{se } z \geq 0 \ , \\ -z & \text{se } z \leq 0 \ ; \end{cases}$$

(2) $$\mathrm{sign}(z) \;:=\; \begin{cases} +1 & \text{sse } z > 0 \ , \\ 0 & \text{sse } z = 0 \ , \\ -1 & \text{sse } z < 0 \quad . \end{cases}$$

(3) Eserc. Verificare gli enunciati che seguono.

(a) $\forall z,w \in \mathbb{Z} \;:\; \mathrm{sign}(z\cdot w) \;=\; \mathrm{sign}(z)\cdot\mathrm{sign}(w) \quad , \quad \mathrm{sign}(-z) \;=\; -\mathrm{sign}(z) \quad , \quad |z\cdot w| \;=\; |z|\cdot|w|$.
(b) $\forall z,w \in \mathbb{Z} \;:\; z \;=\; \mathrm{sign}(z)\cdot|z| \ , \ |-z| \;=\; |z| \ , \ z^2 \;=\; |z|^2 \quad , \quad z^3 \;=\; \mathrm{sign}(z)\cdot|z|^3$.
(c) $\forall z,w \in \mathbb{Z} \;:\; \big||z|-|w|\big| \;\leq\; |z-w| \;\leq\; |z|+|w|$.

B20 d.05 Anche la definizione delle potenze intere naturali degli interi naturali si estende a tutti gli interi relativi.

(1) $$\forall z \in \mathbb{Z} \ , \ n \in \mathbb{N} \;:\; z^n \;:=\; \begin{cases} 1 & \text{sse } n = 0 \ , \\ z\cdot z^{n-1} & \text{sse } n \in \mathbb{P} \ . \end{cases}$$

Si dimostrano quindi le seguenti proprietà:

(2) $$\forall y,z \in \mathbb{Z} \ , \ m,n \in \mathbb{N} \;:\; \begin{array}{l} (y\cdot z)^n \;=\; y^n\cdot z^n \quad , \quad z^{m+n} \;=\; z^m\cdot z^n \quad , \quad z^{m\cdot n} \;=\; (z^m)^n \quad , \\ z^{2n} \;=\; |z|^{2n} \ , \ z^{2n+1} \;=\; \mathrm{sign}(z)\cdot|z|^{2n+1} \end{array} \quad .$$

B20 d.06 Si dice insieme dei multipli (interi) dell'intero z l'insieme $\{f \in \mathbb{Z} :|\ f\cdot z\}$; questo insieme si denota concisamente con $z\cdot\mathbb{Z}$.

Si osserva che

(1) $$1\cdot\mathbb{Z} \;=\; \mathbb{Z} \quad , \quad 0\cdot\mathbb{Z} \;=\; \{0\} \quad \text{e} \quad \forall z \in \mathbb{Z} \;:\; -z\cdot\mathbb{Z} = z\cdot\mathbb{Z} \ .$$

Fissato $f \in \mathbb{Z}$, si dice **dilatazione-Z** relativa al fattore f la trasformazione $\boldsymbol{Dil}_f \;:=\; \lceil\, z \in \mathbb{Z} \mapsto f\cdot z \,\rceil$.
Ciascuna di queste trasformazioni associa a ogni intero uno dei suoi multipli.

Mentre $\boldsymbol{Dil}_1$ non è che l'identità di $\mathbb{Z}$, $\boldsymbol{Dil}_{-1}$ si constata coincidere con la riflessione rispetto a 0, cioè con $\mathsf{Mirr}_{0.\mathbb{Z}}$.

Queste sono le due sole dilatazioni che sono anche permutazioni di $\mathbb{Z}$. in quanto le $\boldsymbol{Dil}_f$ con $|f| \geq 2$ sono endofunzioni non invertibili.

Inoltre evidentemente, $\boldsymbol{Dil}_0$ è la funzione collasso $\lceil\, z \in \mathbb{Z} \mapsto 0 \,\rceil$.

Per ogni $f \in (-\infty : 2] \cup [2 : +\infty)$ la trasformazione $\boldsymbol{Dil}_f$ ha come codominio l'insieme degli interi multipli di f, $f\cdot\mathbb{Z}$ e quindi è iniettiva e non è suriettiva (e non invertibile).

(1) Eserc. Verificare le seguenti relazioni, nelle quali si suppone che $\circ$ possa esprimere sia $\circ_{lr}$ che $\circ_{rl}$:

(a) $\forall f,g \in \mathbb{Z} \;:\; \boldsymbol{Dil}_f \circ \boldsymbol{Dil}_g = \boldsymbol{Dil}_{f\cdot g} = \boldsymbol{Dil}_g \circ \boldsymbol{Dil}_f$.
(b) $\forall f \in \mathbb{Z} \;:\; \boldsymbol{Dil}_f \;=\; \boldsymbol{Dil}_{|f|} \circ \boldsymbol{Dil}_{\mathrm{sign}(f)} \;=\; \boldsymbol{Dil}_{\mathrm{sign}(f)} \circ \boldsymbol{Dil}_{|f|}$.

B20 e. permutazioni degli interi

B20 e.01 Come avremo ampiamente modo di vedere, per approfondire la conoscenza di molte strutture matematiche e dei problemi che le riguardano (in particolare delle strutture esprimibili in termini geometrici) si rivela di grande utilità lo studio delle permutazioni dei loro insiemi terreno che lasciano invariate alcune relazioni e proprietà; esse forniscono forti caratterizzazioni delle strutture stesse.

In questa sezione prendiamo in esame le trasformazioni biiettive dell'insieme $\mathbb{Z}$ che conservano la relazione "successore-Z". Nella successiva parleremo più in generale degli insiemi di permutazioni di insiemi qualsiasi i quali costituiscono un cosiddetto **gruppo**.
Su tale termine ritorneremo spesso; per ora ci limitiamo a dire che un insieme di trasformazioni di un terreno T costituisce un gruppo quando comprende l'identità di T, se comp[rende una trasformazione deve contenere anche l'inversa e se contiene due trasformazioni deve contenere anche la loro composizione.

B20 e.02 Fissato un arbitrario $d \in \mathbb{Z}$, si dice **traslazione-Z** di spostamento d la trasformazione

$$\boldsymbol{Trsl}_{\,d} \;:=\; \ulcorner\, z \in \mathbb{Z} \mapsto z + d \,\urcorner \;. \tag{1}$$

L'effetto di una traslazione sopra il numero intero z è esprimibile con le scritture equivalenti

$$z \text{¸} \boldsymbol{Trsl}_{\,d} \;=\; \boldsymbol{Trsl}_{\,d}(z) \;:=\; z + d \;. \tag{2}$$

Ricordiamo che nella prima espressione compare una terna di unità lessicali: un argomento, il connettivo argomento-funzione "¸" e una funzione precisata da un parametro numerico.
Questa terna dice che la funzione esercita un'azione sull'argomento posto in prima posizione ed esprime il risultato di questa azione.

Conviene osservare che i costrutti della forma precedente possono essere utilizzati convenientemente per ogni endofunzione e più in generale per ogni funzione.
Più in generale costrutti analoghi si possono utilizzare convenientemente per ogni relazione [B53].

B20 e.03 Osserviamo alcune caratteristiche delle traslazioni-Z.

Le traslazioni-Z conservano la validità delle relazioni successore-Z, predecessore-Z e adiacenza-Z.

La composizione di due traslazioni-Z è un'altra traslazione-Z:

$$\begin{aligned} \boldsymbol{Trsl}_{\,e}(\boldsymbol{Trsl}_{\,d}(z)) \;&=\; (z \text{¸} \boldsymbol{Trsl}_{\,d}) \text{¸} \boldsymbol{Trsl}_{\,e} \;=\; z \text{¸} (\boldsymbol{Trsl}_{\,d} \circ_{lr} \boldsymbol{Trsl}_{\,e}) \;=\; (z + d) + e \\ &=\; z + (d + e) \;=\; z \text{¸} \boldsymbol{Trsl}_{\,d+e} \;=\; \boldsymbol{Trsl}_{\,d+e}(z) \end{aligned} \;. \tag{1}$$

La composizione di traslazioni-Z è commutativa; questa è una conseguenza della commutatività della somma di interi.

La composizione delle traslazioni $\boldsymbol{Trsl}_{\,d}$ e $\boldsymbol{Trsl}_{\,-d}$ lascia invariata $\mathbb{Z}$, cioè

$$\boldsymbol{Trsl}_{\,d} \circ_{lr} \boldsymbol{Trsl}_{\,-d} \;=\; \boldsymbol{Trsl}_{\,-d} \circ_{lr} \boldsymbol{Trsl}_{\,d} \;=\; \mathsf{Id}_{\mathbb{Z}} \;. \tag{2}$$

In altri termini le due traslazioni sono una la trasformazione inversa dell'altra,

$$\boldsymbol{Trsl}_{\,-d} \;=\; \boldsymbol{Trsl}_{\,d}^{\,-1} \;. \tag{3}$$

L'insieme delle traslazioni-Z si è comprensibilmente indotti a denotarlo con $\boldsymbol{Trsl}_{\,\mathbb{Z}}$.

Quando un gruppo è formato da permutazioni che commutano si parla di **gruppo di permutazioni commutativo** o di **gruppo di permutazioni abeliano**.

Per la commutatività delle traslazioni-Z possiamo affermare che il gruppo delle traslazioni-z $\boldsymbol{Trsl}_{\mathbb{Z}}$ è un gruppo abeliano.

$\boldsymbol{Trsl}_{\mathbb{Z}}$ è un sottoinsieme proprio dell'insieme delle permutazioni di $\mathbb{Z}$, $\boldsymbol{Trsl}_{\mathbb{Z}} \subset \mathsf{Perm}_{\mathbb{Z}}$.
Infatti nell'insieme $\mathsf{Perm}(\mathbb{Z}) \setminus \boldsymbol{Trsl}_{\mathbb{Z}}$ si trovano tutte le permutazioni che modificano solo un sottoinsieme finito di $\mathbb{Z}$ e permutazioni come

$$P_1 := \left\downarrow \begin{matrix} \cdots & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & \cdots \\ \cdots & -3 & -4 & -1 & -2 & 1 & 0 & 3 & 2 & \cdots \end{matrix} \right\downarrow \quad \text{e}$$

$$P_2 := \left\downarrow \begin{matrix} \cdots & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & \cdots \\ \cdots & -3 & -4 & -1 & -2 & 1 & 2 & 0 & 4 & 5 & 3 & \cdots \end{matrix} \right\downarrow .$$

Si osserva anche che la funzione $\ulcorner\, d \in \mathbb{Z} \mapsto \boldsymbol{Trsl}_{d} \,\urcorner$ pone in biiezione $\mathbb{Z}$ con l'insieme delle traslazioni-Z. La semplicità della corrispondenza induce a dire che $\mathbb{Z}$ e $\boldsymbol{Trsl}_{\mathbb{Z}}$ sono in biiezione naturale e rende veniale la identificazione dei due tipi di oggetti, cioè l'utilizzo nella presentazione dei termini "numero intero" e "traslazione di un intero" come termini equivalenti.

B20 e.04 Fissato $k \in \mathbb{Z}$ si dice **riflessione-Z** di parametro k la trasformazione

$$\mathsf{Mirr}_{[k]} := \ulcorner\, z \in \mathbb{Z} \mapsto k - z \,\urcorner \ . \tag{1}$$

Si osserva che abbiamo già incontrato $\mathsf{Mirr}_{[0]}$, la permutazione di $\mathbb{Z}$ che scambia il segno degli interi.

Conviene presentare più esplicitamente riflessioni come le seguenti:

$$\mathsf{Mirr}_{[4]} = \left\downarrow \begin{matrix} \cdots & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \cdots \\ \cdots & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & -1 & -2 & -3 & -4 & \cdots \end{matrix} \right\downarrow ,$$

$$\mathsf{Mirr}_{[3]} = \left\downarrow \begin{matrix} \cdots & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \cdots \\ \cdots & 6 & 5 & 4 & 3 & 2 & 1 & 0 & -1 & -2 & -3 & -4 & -5 & \cdots \end{matrix} \right\downarrow ;$$

$$\mathsf{Mirr}_{[-3]} = \left\downarrow \begin{matrix} \cdots & -7 & -6 & -5 & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & \cdots \\ \cdots & 4 & 3 & 2 & 1 & 0 & -1 & -2 & -3 & -4 & -5 & -6 & -7 & \cdots \end{matrix} \right\downarrow ;$$

Possono essere utili anche le corrispondenti figure.

Si osserva facilmente che le riflessioni sono tutte e sole le permutazioni di $\mathbb{Z}$ diverse dalla identità $\mathsf{Id}_{\mathbb{Z}}$ che mantengono l'adiacenza-Z; esse inoltre sono le permutazioni che scambiano le relazioni successore-Z e predecessore-Z.
Applicando due volte una riflessione si trasforma ogni $z \in \mathbb{Z}$ in se stesso, cioè $\mathsf{Mirr}_{[k]} \circ \mathsf{Mirr}_{[k]} = \mathsf{Id}_{\mathbb{Z}}$; quindi le riflessioni-Z sono involuzioni di $\mathbb{Z}$.
Si osserva che anche P_1 è una involuzione, mentre non lo è P_2; per questa si ha invece ${P_2}^6 = \mathsf{Id}_{\mathbb{Z}}$.

B20 e.05 Pensiamo a un modello osservabile di $\mathbb{Z}$ costituito da un'asta di materiale rigido soddisfacentemente rettilinea, sottile ed estesa nella quale i punti sono rappresentati da miniscole tacche (tali da ricordare le comuni righe da disegno).
Si osserva che per tale oggetto una riflessione-Z corrisponde a un capovolgimento dell'orientamento dell'asta ottenuto:

– se k è pari e scriviamo $k = 2\,c$, tenendo fissa la tacca in c e in tal caso si ha la trasformazione $\mathsf{Mirr}_c(\mathbb{Z})$;

– se k è dispari e scriviamo $k = 2\,c + 1$, tenendo fisso il punto a metà tra la tacca in c e quella in $c+1$ e in tal caso si ha la trasformazione che scriviamo $\mathsf{Mirr}_{c+1/2}(\mathbb{Z})$ la quale non lascia fisso alcun punto intero.

Abbiamo quindi individuato oggetti, i punti intermedi per le coppie di punti successivi di $\mathbb{Z}$, che sono utili per operare su $\mathbb{Z}$ ma non appartengano a tale insieme. Questo è un primo segnale del fatto che $\mathbb{Z}$, in quanto ambiente operativo, presenta delle carenze e suggerisce di ampliare $\mathbb{Z}$ per ottenere un insieme numerico più versatile.

B20 e.06 Per trattare più comodamente le riflessioni-Z e, come vedremo più avanti, varie altre entità geometriche, è opportuno introdurre i numeri semidispari, entità che formalizzano quelle che, sul modello materiale di $\mathbb{Z}$, abbiamo considerate come posizioni intermedie tra le posizioni di due interi consecutivi.
Questo insieme e il più esteso insieme dei numeri seminteri, insieme costituito dai numeri semidispari e dai numeri interi, consentiranno nei prossimi paragrafi di trattare le riflessioni e le rotazioni in $\mathbb{Z} \times \mathbb{Z}$ e successivamente le aree delle cosiddette figure-ZZ [B24].

Denotiamo con $n + 1/2$ l'entità numerica che rappresenta la posizione intermedia tra quella dell'intero n e quella di $n + 1$ e per esso chiediamo innanzi tutto che sia

$$\forall m, n \in \mathbb{Z} \;:\; (m + 1/2) + (n + 1/2) \;:=\; m + n + 1 \;.$$

Si definisce come **insieme dei numeri semidispari**

$$\mathbb{O}\mathsf{dd}/2 \;:=\; \mathbb{Z} + 1/2 \;:=\; \{n \in \mathbb{Z} :|\; n + 1/2\} \;. \tag{1}$$

Unendo questo insieme con l'insieme degli interi otteniamo quello che chiamiamo **insieme dei numeri seminteri**:

$$\mathbb{Z}/2 \;:=\; \mathbb{Z} \;\dot\cup\; \mathbb{O}\mathsf{dd}/2 \;. \tag{2}$$

Sopra $\mathbb{Z}/2$ chiediamo siano definite le operazioni somma e differenza dotate delle proprietà che seguono.

– esse estendono le corrispondenti sugli interi;
– la somma è commutativa e associativa ed ha 0 come elemento neutro;
– la differenza è l'operazione binaria inversa della somma, cioè $\forall a, b \in \mathbb{Z}/2 \;:\; (a + b) - b \;=\; a$.

Queste richieste sono soddisfatte se si chiede la validità delle seguenti uguaglianze

$$\forall n, m \in \mathbb{Z} \;:\; (n + 1/2) + m \;=\; n + (m + 1/2) \;,\; (n + 1/2) + (m + 1/2) \;=\; n + m + 1 \;,$$

$$(n + 1/2) - m \;=\; n - (m - 1 + 1/2) \;,\; n - (m + 1/2) \;=\; n - m - 1 + 1/2 \;, \tag{3}$$

$$(n + 1/2) - (m + 1/2) \;=\; n - m \;.$$

Può essere conveniente servirsi anche dell'uguaglianza $n - 1/2 \;:=\; (n - 1) + 1/2$.

B20 e.07 In termini algebrici potremo affermare che a $\mathbb{Z}/2$ la somma, la differenza e lo zero hanno dato una struttura di gruppo abeliano commutativo [B41b].
Per ora evitiamo invece di definire il prodotto tra due semidispari, in quanto questa operazione porterebbe a numeri intermedi tra due seminteri palesando una insufficienza di $\mathbb{Z}/2$, difetto cui porremo rimedio con un ampliamento più rilevante degli interi costituito dall'introduzione dei numeri razionali [B30].

Conviene invece prendere in considerazione fin d'ora le coppie di numeri seminteri, cioè gli elementi dell'insieme $(\mathbb{Z}/2) \times (\mathbb{Z}/2)$ che evidentemente è una estensione di $\mathbb{Z} \times \mathbb{Z}$. Queste coppie serviranno

per definire importanti permutazioni di $\mathbb{Z}\times\mathbb{Z}$, le riflessioni e le rotazioni (e dunque le simmetrie centrali). Osserviamo che queste coppie consentono di individuare sia i punti-ZZ, sia le caselle-ZZ, sia i segment-ZZR elementari.

B20 e.08 Mediante i numeri seminteri $h\in\mathbb{Z}/2$ le riflessioni-Z si possono esprimere come

$$\mathsf{Mirr}_h \;:=\; \lceil\, z\in\mathbb{Z} \mapsto 2\,h-z \,\rceil \;. \tag{1}$$

(1) Prop.: La composizione di due riflessioni-Z è una traslazione; più precisamente:

$$\forall h,k\in\mathbb{Z}/2 \;:\; \mathsf{Mirr}_h \circ_{lr} \mathsf{Mirr}_k \;=\; \boldsymbol{Trsl}_{\,2(k-h)} \;.$$

Dim.: $\lceil\, z\in\mathbb{Z} \mapsto 2\,h-z \,\rceil \circ_{lr} \lceil\, z\in\mathbb{Z} \mapsto 2\,k-z \,\rceil \;=\; \lceil\, z\in\mathbb{Z} \mapsto 2\,h-z \,\rceil \circ_{lr} \lceil\, 2\,h-z\in\mathbb{Z} \mapsto 2\,k-(2\,h-z) \,\rceil$
$= \;\lceil\, z\in\mathbb{Z} \mapsto z+2(k-h) \,\rceil \;=\; \boldsymbol{Trsl}_{\,2(k-h)}$ ∎

(2) Prop.: $\forall h,k\in\mathbb{Z}/2 \;:\; \mathsf{Mirr}_k \circ_{lr} \mathsf{Mirr}_h = \boldsymbol{Trsl}_{\,2(h-k)} = \big(\boldsymbol{Trsl}_{\,2(k-h)}\big)^{-1} = (\mathsf{Mirr}_h \circ_{lr} \mathsf{Mirr}_k)^{-1}$ ∎

(3) Prop.: $\forall k\in\mathbb{Z}/2\;,\; d\in\mathbb{Z} \;:\; \mathsf{Mirr}_k \circ_{lr} \boldsymbol{Trsl}_{\,d} \;=\; \mathsf{Mirr}_{k+d/2}$.

Dim.: $\mathsf{Mirr}_k \circ_{lr} \boldsymbol{Trsl}_{\,d} \;=\; \lceil\, z\in\mathbb{Z} \mapsto 2\,k-z \,\rceil \circ_{lr} \lceil\, 2\,k-z\in \mapsto :|\, 2\,k-z+d \,\rceil \;=$
$\lceil\, z\in\mathbb{Z} :|\, 2(k+d/2)-z \,\rceil \;=\; \mathsf{Mirr}_{k+d/2}$ ∎

(4) Prop.: $\forall k\in\mathbb{Z}/2\;,\; d\in\mathbb{Z} \;:\; \boldsymbol{Trsl}_{\,d} \circ_{lr} \mathsf{Mirr}_k \;=\; \mathsf{Mirr}_{k-d/2}$.

Dim.: $\boldsymbol{Trsl}_{\,d} \circ_{lr} \mathsf{Mirr}_k \;=\; \lceil\, z\in\mathbb{Z} \mapsto z+d \,\rceil \circ_{lr} \lceil\, z+d\in\mathbb{Z} \mapsto 2\,k-z-d \,\rceil \;=$
$\lceil\, z\in\mathbb{Z} \mapsto 2(k-d/2)-z \,\rceil \;=\; \mathsf{Mirr}_{k-d/2}$ ∎

B20 e.09 Dato che componendo due riflessioni non si ottiene una trasformazione dello stesso genere, le riflessioni-Z non costituiscono un gruppo di trasformazioni.
Si ottiene invece un gruppo di trasformazioni di $\mathbb{Z}$ considerando l'unione dell'insieme delle traslazioni-Z con quello delle riflessioni-Z; esso viene detto **gruppo delle trasloriflessioni-Z**.

Le composizioni degli elementi di questo gruppo vengono indicate dal seguente schema di tabella di composizione

$$\forall d,e\in\mathbb{Z}\;,\; h,k\in\mathbb{Z}/2 \;:\; \begin{array}{cc|cc} \circ_{lr} & & \boldsymbol{Trsl}_{\,e} & \mathsf{Mirr}_k \\ \hline \boldsymbol{Trsl}_{\,d} & & \boldsymbol{Trsl}_{\,d+e} & \mathsf{Mirr}_{k-d/2} \\ \mathsf{Mirr}_h & & \mathsf{Mirr}_{h+e/2} & \boldsymbol{Trsl}_{\,2(k-h)} \end{array} \;. \tag{1}$$

Questo schema evidenzia che il gruppo delle traslazioni-Z si distingue all'interno del gruppo delle traslo-riflessioni-Z; questo fatto viene chiarito dalla nozione di sottogruppo [B41b], mentre l'insieme delle riflessioni fornisce un esempio di laterale sinistro e di laterale destro.

B20 e.10 Tra le permutazioni di $\mathbb{Z}$ si possono anche considerare quelle che lasciano fissi tutti gli interi che non appartengono all'intervallo $[1:n]$ per qualche intero positivo n.

Di queste permutazioni di $\mathbb{Z}$ solo $\mathsf{Id}_{\mathbb{Z}}$ conserva l'adiacenza.
Consideriamo infatti una permutazione che conserva l'adiacenza π; dato che -2 e -1 vengono lasciati fissi, deve essere anche $\pi(0)=0$ e con considerazioni analoghe si vede che deve essere $\pi(1)=1$, $\pi(2)=2$, ..., $\pi(n)=n$.

Le suddette permutazioni si possono identificare con le permutazioni dell'insieme finito $\{1,2,...,n\}$ e quindi in questa ottica possiamo dire che tutti i gruppi simmetrici Sym_n e tutti i loro sottogruppi sono sottogruppi di $\mathsf{Perm}[\mathbb{Z}]$.

B20 e.11 Riprendiamo le operazioni di dilatazione-Z introdotte in d06. $\boldsymbol{Dil}_f := \lceil z \in \mathbb{Z} \mapsto f \cdot z \rceil$ per ogni $f \in \mathbb{Z}$.
Inoltre denotiamo con $\boldsymbol{Dil}_{\mathbb{Z}}$ l'insieme delle dilatazioni-Z.
Si è visto che $\forall f, g \in \mathbb{Z} \ : \ \boldsymbol{Dil}_f \circ \boldsymbol{Dil}_g = \boldsymbol{Dil}_{f \cdot g}$.

Accade dunque che quasi tutte le dilatazioni sono trasformazioni non invertibili entro l'intero $\mathbb{Z}$; sono invertibili solo $\boldsymbol{Dil}_1 = \mathsf{Id}_{\mathbb{Z}}$ e $\boldsymbol{Dil}_{-1} = \mathsf{Mirr}_0$.

In termini algebrici non si può quindi dire che $\boldsymbol{Dil}_{\mathbb{Z}}$ costituisca un gruppo di trasformazioni; costituisce invece un esempio di monoide di trasformazioni, specie di struttura che sarà introdotta in B41a.

B20 f. nozioni di gruppo di simmetria e di gruppo in generale

B20 f.01 Nella sezione precedente abbiamo incontrato insiemi di permutazioni dell'insieme numerabile $\mathbb{Z}$ che presentano caratteristiche che sono comuni a molti altri insiemi di permutazioni e che le rendono di grande interesse per molteplici scopi.

Questo conduce a individuare una specifica categoria di sistemi formali basati su insiemi di permutazioni alla quale conviene dedicare molta attenzione fin dai primi stadi dell'*esposizione*, in particolare prima dell'introduzione più sistematica delle svariate strutture algebriche che inizieremo in B41.

Consideriamo un insieme ambiente S, un insieme G di permutazioni di S, cioè un $G \subseteq \mathbf{Perm}_S$, e l'operazione binaria prodotto di composizione di tali endofunzioni che, per fissare le notazioni, consideriamo nella versione "$\circ_{lr}$" .

Alle permutazioni costituenti G chiediamo soddisfino le proprietà che seguono.

(1) Componendo due permutazioni di G si ottiene un'altra permutazione di tale insieme (chiusura di G per il prodotto di composizione).
(2) G contiene l'identità dell'ambiente S.
(3) Se G contiene una permutazione T, contiene necessariamente anche la sua inversa $T^{-\mathbf{1}}$.

La quaterna $\mathsf{G} := \langle G, \circ_{lr}, ^{-\mathbf{1}}, \mathsf{Id}_S \rangle$ si dice costituire un **gruppo di permutazioni**. Mentre l'insieme G si dice **terreno del gruppo**, l'insieme S, ricavabile da Id_S, si dice **campo d'azione del gruppo**.

L'insieme dei gruppi di permutazioni si può qualificare come insieme-P e viene detto **specie dei gruppi di permutazioni**.

I gruppi di permutazioni costituiscono un esempio dei sistemi formali che chiameremo **strutture algebriche** e la specie dei gruppi di permutazioni costituisce un esempio delle cosiddette **specie di strutture algebriche**.

Queste entità e le più generali **strutture matematiche** costituiscono delle classi di riferimento di primaria importanza per le nozioni della matematica e le incontreremo in vari punti di questa *esposizione*.
In particolare alle strutture algebriche dedicheremo il già citato capitolo introduttivo B41 e i successivi capitoli T15, T22, T23, T25.

I gruppi di permutazioni, come vedremo, sono una specie di struttura di particolare importanza in quanto aiuta a inquadrare molte sitazioni e in particolare molte collezioni di strutture.

B20 f.02 Per esemplificare cominciamo da due esempi già incontrati.

In B13 e abbiamo introdotto, per ogni n intero positivo, l'insieme delle $n!$ permutazioni dell'insieme finito $\mathsf{(n\,]} = \{1, 2, ..., n\}$ e quindi il gruppo di permutazioni che abbiamo denotato con $\mathsf{Sym}_n := \left\langle Sym_n, \circ_{lr}, ^{-\mathbf{1}}, \mathsf{Id}_{\mathsf{(n\,]}} \right\rangle$.
Nella precedente sezione :e abbiamo visto alcune permutazioni del terreno $\mathbb{Z}$ che mantengono l'adiacenza-ZZ, cioè le traslazioni-ZZ e le riflessioni-ZZ, e lo schema che stabilisce come queste trasformazioni si compongono e definiscono il **gruppo delle trasloriflessioni** di $\mathbb{Z}$.

B20 f.03 La nozione di gruppo simmetrico Sym_n si estende senza problemi a quella di gruppo simmetrico di un insieme finito qualsiasi. Inoltre si può introdurre un gruppo simmetrico costituito dalle permutazioni di un qualsiasi insieme ricorsivo come $\mathbb{Z}$ e anche un gruppo costituito dalle permutazioni di un qualsiasi insieme-P S.

Infatti le proprietà f01(1),(2),(3) sono evidentemente soddisfatte dalle permutazioni di S; quindi si può cercare di trattare il gruppo simmetrico di un qualsiasi insieme che possa presentare interesse.

Come abbiamo già osservato, si individuano varie relazioni interessanti tra gli elementi di potenziali campi d'azione, anche tra quelli elementari come (n]; per ciascuna di tali relazioni può essere utile stabilire quali permutazioni del campo d'azione la rispettano e quali la modificano.

Precisiamo questa situazione per una relazione binaria $R \subseteq$ (n] $\times$ (n]. Si dice che la permutazione P **rispetta una relazione** R o che **conserva una relazione** R sse

$$\forall \langle i,j\rangle \in R \ : \ \big\langle P(i),P(j)\big\rangle \in R \ . \tag{1}$$

Da questa richiesta segue che rispettano la R anche tutte le potenze di composizione di una permutazione che rispetta la R. Quindi rispetta la R anche la permutazione inversa di una permutazione che la rispetta.
Di conseguenza se $P \in \mathbf{Perm}_{(\mathrm{n}\ ]}$ rispetta la R e se $\langle h,k\rangle \notin R$ deve essere $\big\langle P(h),P(k)\big\rangle \notin R$: infatti in caso contrario, applicando la P^{-1} alla $\big\langle P(h),P(k)\big\rangle$ si avrebbe $\langle h,k\rangle \in R$.
Quindi a una permutazione P di $S =$ (n] che rispetta i nodi della relazione R è associata una permutazione di $S \times S$ che rispetta gli archi della R.

B20 f.04 Dati l'insieme S e la relazione $R \subset S \times S$, denotiamo con $Gcons_R$ il sottoinsieme di $\mathbf{Perm}_S$ comprendente tutte e sole le permutazioni che conservano la R.

(1) Prop.: $Gcons_R$ fa da campo d'azione a un gruppo di permutazioni.

Dim.: Evidentemente l'identità di S fa parte di $Gcons_R$ [f01(3)]; se T fa parte di $Gcons_R$ lo stesso accade alla T^{-1} [f01(2)]; se T_1 e T_2 fanno parte di $Gcons_R$, lo stesso accade per $T_1 \circ_{lr} T_2$ [f01(1)] ∎

Dunque a ogni relazione su S èquindi associato un gruppo di permutazioni di S e il suo terreno abbiamo denotato con $Gcons_R$.

In generale, dato un gruppo di permutazioni di un insieme S $\mathsf{G} = \big\langle G, \circ_{lr}, {}^{-1}, \mathsf{Id}_S\big\rangle$ si dice **sottogruppo di permutazioni** di G ogni gruppo di permutazioni di S della forma $\mathsf{H} = \big\langle H, \circ_{lr}, {}^{-1}, \mathsf{Id}_S\big\rangle$ con $H \subseteq G$. Prevedibilmente si parla di sottogruppo proprio sse $H \subset G$.

Chiaramente l'insieme dei gruppi di permutazioni di un insieme S coincide con l'insieme dei sottogruppi di permutazioni di Sym_S.

B20 f.05 Vediamo alcuni esempi di sottogruppi di Sym_n associati a relazioni su (n].
Lo stesso Sym_n si può considerare il gruppo delle permutazioni di (n] che conserva la relazione (n]$\times$(n], la relazione ovvia per (n].

Consideriamo le permutazioni che lasciano fisso n in quanto elemento del terreno; evidentemente esse costituiscono un gruppo di permutazioni identificabile con Sym_{n-1}. Questo sottogruppo risulta associato alla relazione di equivalenza su (n] corrispondente alla partizione $\{1,2,...,n-1\} \dot\cup \{n\}$, ossia alla corrispondente relazione di equivalenza.
Le matrici permutative dei suoi elementi sono quelle dominate dalla matrice binaria della suddetta relazione

$$\begin{bmatrix} 1 & 1 & \dots & 1 & 0 \\ 1 & 1 & \dots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix} .$$

Le permutazioni che lasciano fisso un altro intero di (n] si ottengono dalle precedenti mediante un semplice riordinamento di (n].

Più in generale a ogni relazione di equivalenza su $(\mathrm{n}\,]$, ossia a ogni partizione $(\mathrm{n}\,] = I_1 \dot\cup I_2 \dot\cup \cdots \dot\cup I_k$, corrisponde il gruppo delle permutazioni che mandano ogni intero appartenente a I_h $(h = 1, 2, ..., k)$ in un altro intero di tale sottoinsieme. Per esempio alla partizione $\{1, 2, ..., 8\} = \{1, 4, 6\} \dot\cup \{2, 7\} \dot\cup \{3, 5, 8\}$ è associato il gruppo delle permutazioni esprimibili come prodotto di una permutazione di $\{1, 4, 6\}$, di una permutazione di $\{2, 7\}$ e di una di $\{3, 5, 8\}$. Le corrispondenti matrici permutative sono quelle dominate dalla

$$\begin{bmatrix} 1&0&0&1&0&1&0&0\\ 0&1&0&0&0&0&1&0\\ 0&0&1&0&1&0&0&1\\ 1&0&0&1&0&1&0&0\\ 0&0&1&0&1&0&0&1\\ 1&0&0&1&0&1&0&0\\ 0&1&0&0&0&0&1&0\\ 0&0&1&0&1&0&0&1 \end{bmatrix} .$$

B20 f.06 Altre interessanti coppie $\langle$ relazione , gruppo di permutazioni $\rangle$ riguardano relazioni che esprimono digrafi simmetrici, ovvero grafi nonorientati; in ciascuno di questi casi il gruppo delle permutazioni individua le simmetrie di queste configurazioni combinatorie.

Un primo esempio è dato dal gruppo Sym_3 esaminato in B13e. Si vede che esso è il gruppo che lascia invariato il semplice grafo nonorientato a forma di triangolo (Δ).

Per un secondo esempio consideriamo il grafo nonorientato a forma di quadrato individuabile con la matrice delle adiacenze

$$\begin{bmatrix} 1&1&0&1\\ 1&1&1&0\\ 0&1&1&1\\ 1&0&1&1 \end{bmatrix} . \tag{1}$$

Le permutazioni dei suoi vertici che trasformano il grafo in se stesso sono: l'identità che denotiamo con e; le permutazioni circolari $c^k := \langle_{cy} 1, 2, 3, 4\rangle^k$ per $k = 1, 2, 3$, le riflessioni $h := (1, 4) \circ (2, 3)$, $v := (1, 2) \circ (3, 4)$, $d1 : (1, 3)$ e $d2 := (2, 4)$. La sua tavola di moltiplicazione è

$$\begin{array}{c|cccccccc} & e & c & c^2 & c^3 & h & v & d1 & d2\\ \hline e & e & c & c^2 & c^3 & h & v & d1 & d2\\ c & c & c^2 & c^3 & e & d1 & d2 & v & h\\ c^2 & c^2 & c^3 & e & c & v & h & d2 & d1\\ c^3 & c^3 & e & c & c^2 & d2 & d1 & h & v\\ h & h & d2 & v & d1 & e & c^2 & c^3 & c\\ v & v & d1 & h & d2 & c^2 & e & c^3 & c\\ d1 & d1 & h & d2 & v & c & c^3 & e & c^2\\ d2 & d2 & v & d1 & h & c^3 & c & c^2 & e \end{array} . \tag{2}$$

B20 f.07 Si osserva che un gruppo di permutazioni di un qualsiasi insieme finito di n oggetti $A := \{a_1, a_2, ..., a_n\}$ presenta una tavola di moltiplicazione che ricalca quella di Sym_n.

Questa situazione si esprime affermamdo che i due gruppi sono isomorfi.

In generale due gruppi di permutazioni $\mathsf{G} = \langle G, \circ_{lr}, {}^{-1}, \mathsf{Id}_S\rangle$ e $\mathsf{H} = \langle H, \circ_{lr}, {}^{-1}, \mathsf{Id}_T\rangle$ si dicono **gruppi di permutazioni isomorfi** sse esiste una biiezione tra il campo di azione del primo, S, e quello del secondo, T, che trasforma il prodotto del primo nel prodotto del secondo.

Vediamo la situazione nel caso di Sym_n e Sym_A con più dettagli formali. La biiezione

$$\beta \;:=\; \left\downarrow \begin{matrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{matrix} \right\downarrow \;\in\; \lceil\!(\mathrm{n}\,]\!\rceil \longleftrightarrow A \rceil \;, \tag{1}$$

consente di stabilire la seguente biiezione tra Sym_n e Sym_A

$$\overline{\beta} \;:=\; \left\lceil\!\!\left\lceil\; P \in \mathsf{Sym}_n \;\mapsto\; \left\downarrow \begin{matrix} a_1 & a_2 & \cdots & a_n \\ a_{P(1)} & a_{P(2)} & \cdots & a_{P(n)} \end{matrix} \right\downarrow \right\rceil\!\!\right\rceil \;=\; \lceil\!\lceil\; P \in \mathsf{Sym}_n \;\mapsto\; \beta^{-\mathbf{1}} \circ_{lr} P \circ_{lr} \beta \;\rceil\!\rceil \;, \tag{2}$$

tale che si abbia

$$\forall P, Q \in \mathsf{Perm}_n \;:\; \overline{\beta}(P \circ_{lr} Q) = \overline{\beta}(P) \circ_{lr} \overline{\beta}(Q) \;. \tag{3}$$

Queste espressioni dicono che gli elementi dei due gruppi di permutazioni si compongono in modi strettamente corrispondenti.

In altre parole, due gruppi di permutazioni $\mathsf{G} = \langle G, \circ_{lr}, {}^{-\mathbf{1}}, \mathsf{Id}_S \rangle$ e $\mathsf{H} = \langle H, \circ_{lr}, {}^{-\mathbf{1}}, \mathsf{Id}_T \rangle$ si dicono **gruppi di permutazioni isomorfi** sse si individua una biiezione

$$\overline{\beta} \in \lceil\!\lceil\, G \lhd\!\!\rightarrow\!\!\rhd H \,\rceil\!\rceil \quad \text{tale che} \quad \forall P, Q \in G \;:\; \overline{\beta}(P \circ_{lr} Q) \;=\; \overline{\beta}(P) \circ_{lr} \overline{\beta}(Q) \;. \tag{4}$$

Questa definizione vale quali che siano i campi d'azione dei due gruppi e in particolare se uno o entrambi i gruppi hanno campi d'azione infiniti.

Si trovano senza difficoltà anche coppie di gruppi di permutazioni isomorfi, l'uno con campo d'azione finito e l'altro con campo infinito.

In particolare sono isomorfi il gruppo delle permutazioni del grafo quadrato e il gruppo delle permutazioni del piano $\mathbb{Z} \times \mathbb{Z}$ che trasforma in se stesso il quadrato avente i vertici nei 4 punti $\langle 1, 1 \rangle$, $\langle 1, -1 \rangle$, $\langle -1, -1 \rangle$ e $\langle -1, 1 \rangle$.

B20 f.08 Il fatto che certe caratteristiche essenziali di due gruppi di permutazioni non dipendano dai rispettivi campi d'azione induce a considerare gruppi dei sistemi della forma $\langle G, *, j, e \rangle$ con G che denota un insieme, $*$ una operazione binaria su G, j una operazione unaria su G ed $e \in G$ tali da soddisfare le richieste seguenti:

(1) $*$ è operazione associativa, ossia $\forall g, h, k \in G \;:\; g * (h * k) \;=\; (g * h) * k$;
(2) e è elemento neutro per l'operazione $*$, ossia $\forall g \in G \;:\; e * g \;=\; g * e \;=\; g$;
(3) $\forall g \in G \;:\; g * j(g) \;=\; j(g) * g = e$.

Queste strutture risultano formalmente più maneggevoli. Per esse si possono definire con discorsi molto simili a quelli utilizzati per Sym_n e per i gruppi di permutazioni le nozioni di sottogruppo, carattere abeliano o commutativo della operazione binaria e isomorfismo.

La relazione di isomorfismo tra gruppi è chiaramente un'equivalenza. Le classi di equivalenza per isomorfismo le chiameremo **gruppi astratti**. Tali entità possono essere utili in vari momenti della organizzazione delle conoscenze sui gruppi e sulle simmetrie di molteplici tipi di entità matematiche.

B20 f.09 Dopo aver ricavato le strutture gruppi astratti dalle strutture gruppi di permutazioni, ora stabiliamo una sorta di collegamento inverso mostrando come da ogni gruppo astratto si può ricavare un gruppo di permutazioni.

Consideriamo un generico gruppo $\mathsf{G} = \langle G, *, j, e \rangle$; a ogni suo elemento $h \in G$ si associano le due endofunzioni di G:

$$h^{ltrsl} \;:=\; \lceil\, g \in G \;\mapsto\; h * g \,\rceil \qquad \textbf{traslazione da sinistra per } h \;, \tag{1}$$

(2) $$h^{rtrsl} := \ \lceil\!\lceil\, g \in G \mapsto g * h \,\rceil\!\rceil \qquad \textbf{traslazione da destra per } h\ .$$

Queste due endofunzioni in effetti sono permutazioni del terreno G del gruppo. Infatti sottoponendo alla traslazione da sinistra due elementi diversi g_1 e g_2 di G si ottengono due elementi di G diversi: se fosse $h * g_1 = h * g_2$, moltiplicando da sinistra per $j(h)$ i due membri dell'uguaglianza si otterrebbe l'uguaglianza $g_1 = g_2$. Stessa conclusione per la traslazione da destra.

Questa situazione si riscontra facilmente, per esempio, nella tavola di composizione del gruppo del grafo quadrato f06(1): tutte le righe della matrice si ottengono per traslazione a sinistra degli elementi di G e tutte le sue colonne si ottengono per traslazione a destra e sono evidentemente permutazioni della sequenza degli elementi di G che etichettano le righe e le colonne dalla tavola.
Osserviamo anche che le due traslazioni per un dato elemento $h \in G$ possono coincidere; questo evidentemente accade per ogni h per i gruppi abeliani, ma anche per particolari elementi h di vari gruppi nonabeliani.

B20 f.10 Se h e k sono due elementi di G per le rispettive traslazioni da sinistra si trova

(1) $$(h * k)^{ltrsl} = \lceil\!\lceil\, g \in G \mapsto (h * k) * g \,\rceil\!\rceil = \lceil\!\lceil\, g \in G \mapsto h * (k * g) \,\rceil\!\rceil = h^{ltrsl} \circ_{rl} k^{ltrsl}\ ;$$

Per le traslazioni da destra si ottiene similmente

(2) $$(h * k)^{rtrsl} = \lceil\!\lceil\, g \in G \mapsto g * (h * k) \,\rceil\!\rceil = \lceil\!\lceil\, g \in G \mapsto (g * h) * k) \,\rceil\!\rceil = h^{rtrsl} \circ_{lr} k^{ltrsl}\ ;$$

A questo punto accanto al gruppo $\mathsf{G} = \langle G, *, j, e\rangle$ possiamo considerare i due gruppi di permutazioni di G chiamati, risp., gruppo delle traslazioni da sinistra di G e gruppo delle traslazioni da destra di G:

(3) $$\left\langle G^{ltrsl},\, \circ_{rl}\,,\, \lceil\!\lceil\, h^{ltrsl} \in G^{ltrsl} \mapsto (j(h))^{ltrsl} \,\rceil\!\rceil\,, \mathsf{Id}_G \right\rangle\ ,$$

(4) $$\left\langle G^{rtrsl},\, \circ_{lr}\,,\, \lceil\!\lceil\, h^{rtrsl} \in G^{rtrsl} \mapsto (j(h))^{rtrsl} \,\rceil\!\rceil\,, \mathsf{Id}_G \right\rangle\ .$$

Grazie alle uguaglianze (1) e (2) si ha che i due gruppi di permutazioni precedenti sono isomorfi al gruppo G. Possiamo quindi concludere con il seguente classico enunciato.

(5) Teorema (**teorema di Cayley**) Ogni gruppo è isomorfo a un gruppo di permutazioni.

B20 f.11 Gruppi di grande importanza, come vedremo, sono dati da insiemi numerici di uso comune muniti di una delle ordinarie operazioni di somma e prodotto. Per ora consideriamo l'insieme dei numeri interi munito dell'operazione somma.

Si dice **gruppo additivo degli interi** la struttura

(1) $$\mathbb{Z}_{ag}\ := \langle \mathbb{Z}, +, -_u, 0\rangle\ ,$$

ricordando che con $-_u$ abbiamo denotato il meno unario, cioè l'operazione di passaggio di un intero al suo opposto. Questo è un esempio di gruppo commutativo con terreno numerabile.

Il suo carattere commutativo fa sì che a esso sia associato un solo gruppo delle traslazioni; questo evidentemente è dato da

(2) $$\left\langle \boldsymbol{Trsl}_{\,\mathbb{Z}} = \{k \in \mathbb{Z} :|\ \lceil\!\lceil\, n \in \mathbb{Z} \mapsto n + k \,\rceil\!\rceil\}\,,\, \lceil\!\lceil \forall k \in \mathbb{Z} :\ k^{\boldsymbol{Trsl}} \mapsto (-k)^{\boldsymbol{Trsl}} \,\rceil\!\rceil, 0^{\boldsymbol{Trsl}} = \mathsf{Id}_{\mathbb{Z}} \right\rangle\ .$$

È interessante individuare l'insieme dei sottogruppi propri di $\mathbb{Z}_{ag}$

(3) Prop.: Sia H un sottoinsieme di $\mathbb{Z}$; esso è terreno di un sottogruppo proprio di $\mathbb{Z}_{ag}$ sse si trova $m \in \{2, 3, 4, ...\}$ tale che Hè l'insieme dei multipli interi di m.

Dim.: È evidente che per ogni $m \in \{2,3,4,...\}$ l'insieme $m \cdot \mathbb{Z} = \{k \in \mathbb{Z} :| \, k\, m\}$ è terreno di un sottogruppo proprio di $\mathbb{Z}_{ag}$.
Per il viceversa, se H è un sottogruppo di $\mathbb{Z}_{ag}$ si individua il suo elemento positivo minimo m ed è evidente che l'insieme dei suoi multipli appartiene ad H; se in H si trovasse un intero q non multiplo di m lo si può scegliere positivo e dovrebbe appartenere ad H anche $q\%m$, intero positivo inferiore ad m, contro l'ipotesi su m ∎

Chiaramente i sottogruppi del sottogruppo $m \cdot \mathbb{Z}$ dei multipli di un intero positivo m sono tutti e soli i sottogruppi dei multipli di m $km \cdot \mathbb{Z}$.

Va segnalato che in molte descrizioni due gruppi isomorfi si identificano; questo accade in particolare per gruppi di permutazioni con lo stesso campo d'azione.

Questo può anche accadere per due gruppi di permutazioni con campi d'azione diversi che denotiamo con $\mathsf{G} = \langle G, *, j, \mathsf{Id}_S \rangle$ e $\mathsf{H} = \langle H, *, j, \mathsf{Id}_T \rangle$.
Questa identificazione è accettabile quando si presentano risultati che nelle formulazioni accurate che riguardano i due gruppi si possono trasformare gli uni negli altri mediante biiezioni tra S e T e biiezioni tra G e H facili da individuare, tanto da non rendere necessaria la loro segnalazione esplicita.

B20 f.12 Come si è già osservato, l'insieme delle trasloriflessioni di $\mathbb{Z}$ è l'insieme delle permutazioni di $\mathbb{Z}$ che conservano l'adiacenza tra gli interi. Anche questo gruppo si può quindi considerare un gruppo di permutazioni che conserva una relazione binaria concernente il suo campo d'azione.

Più in generale si osserva che ogni insieme $G_{\mathcal{P}}$ costituito da tutte e sole le permutazioni di S che conservano il sistema $\mathcal{P}$ di relazioni o proprietà concernenti S deve costituire un gruppo di permutazioni. Infatti se le trasformazioni T_1 e T_2 appartengono a $G_{\mathcal{P}}$, anche $T_1 \circ_{lr} T_2$ conserva $\mathcal{P}$ e quindi appartiene a $G_{\mathcal{P}}$. Se $T \in G_{\mathcal{P}}$, allora anche $T^{-\mathbf{1}}$ conserva $\mathcal{P}$ e quindi deve appartenere a $G_{\mathcal{P}}$. Ovvio poi che Id_S conserva $\mathcal{P}$ e quindi appartiene a $G_{\mathcal{P}}$.

B20 f.13 Ricordiamo la tavola di moltiplicazione del gruppo delle trasloriflessioni di $\mathbb{Z}$ [e09(1)].
Le traslazioni-Z fcostituiscono un suo sottogruppo commutativo; non è invece commutativo Sym_3.

Dato un gruppo di permutazioni $G_{\mathcal{P}}$ di un insieme S caratterizzato da un sistema $\mathcal{P}$ di proprietà degli elementi di S, se si riesce a individuare un sistema di proprietà $\mathcal{Q}$ che implica $\mathcal{P}$, cioè un sistema di proprietà più vincolante di $\mathcal{P}$, il gruppo $G_{\mathcal{Q}}$ delle trasformazioni di S che conservano $\mathcal{Q}$ è un sottogruppo di trasformazioni di $G_{\mathcal{P}}$, in quanto ogni permutazione che rispetta $\mathcal{Q}$ deve rispettare $\mathcal{P}$.

Per esempio il gruppo delle traslazioni di $\mathbb{Z}$ si ottiene richiedendo la conservazione della relazione di successore; questa proprietà di conservazione è più vincolante della proprietà di conservazione dell'adiacenza e in effetti il gruppo delle traslazioni è sottogruppo proprio del gruppo delle trasloriflessioni.

Chiamiamo rotazioni-ZZ le rotazioni di $\mathbb{Z} \times \mathbb{Z}$ intorno a un suo qualsiasi punto-ZZ di 0°, di 90°, di 180° e di 270°. Si osserva che si tratta di permutazioni di $\mathbb{Z} \times \mathbb{Z}$ che conservano l'adiacenza e che le 4 rotazioni-ZZ intorno a un determinato punto-ZZ costituiscono un gruppo abeliano.

Chiamiamo gruppo delle roto-traslo-riflessioni di $\mathbb{Z} \times \mathbb{Z}$ o **gruppo dei movimenti rigidi del piano-ZZ** il gruppo costituito dalle composizioni delle rotazioni-ZZ, delle traslazioni-ZZ e dalle riflessioni-ZZ.
Tra i suoi sottogruppi vi sono anche quelli costituiti dalle 4 rotazioni intorno a un puno-ZZ determinato; questi sottogruppi rispettano l'adiacenza-ZZ e il punto-ZZ centro delle rotazioni.
Altri sottogruppi del gruppo dei movimenti rigidi di $\mathbb{Z} \times \mathbb{Z}$ sono costituiti dalla riflessione rispetto una delle rette verticali, orizzontali, diagonali o codiagonali e dalla identità $\mathsf{Id}_{\mathbb{Z}}$.

Si ottengono altri sottogruppi componendo questi sottogruppi di riflessioni tra di loro con le traslazioni o con le rotazioni.

Tra tutti questi sottogruppi se ne trovano di abeliani sottogruppi di sottogruppi nonabeliani.

B20 f.14 Eserc. Individuare attraverso la rispettiva tavola di composizione i seguenti gruppi.

(a) Gruppo delle simmetrie di un foglio rettangolare di carta.

(b) Gruppo delle rotazioni in $\mathbb{Z} \times \mathbb{Z}$ con centro nell'origine per multipli di $90°$.

(c) Gruppo delle permutazioni di un triangolo regolare, da confrontare con Sym_3.

B20 g. numeri primi e fattorizzazione degli interi mediante primi

B20 g.01 Si dice **numero primo** un intero positivo che non possiede divisori diversi da 1 e da se stesso.

I numeri primi fin dall'antichità hanno sempre destato molto interesse e sono stati molto studiati, sia per il loro fascino numerologico, sia per la loro utilità perspiegare importanti quastioni matematiche, sia da qualche anno, per la loro utilità per recenti tecnologie avanzate (crittografia, telecomunicazioni).

Si possono definire varie MSRG, macchine sequenziali programmabili generatrici, in grado di procedere a generare la sequenza dei numeri primi crescenti.
Queste macchinein linea di massima procedono a generare i successivi interi a partire da 2 e per ciascuno di essi stabiliscono se possiede o meno un divisore proprio. Queste operazioni si possono effettuare in vari modi, dai più semplici e poco efficienti ai più complessi con le maggiori prestazioni.

L'elenco dei numeri primi può essere esteso quanto si vuole, fatto la cui dimostrazione compare nel classico testo *Elementi* di Euclide risalente al 300 a.C. circa.

(1) Prop.: La sequenza dei numeri primi può essere generata illimitatamente.

Dim.: Procediamo per assurdo supponendo che l'elenco dei numeri primi sia finito e denotiamo con n il loro numero.
Definiamo l'intero $N := 2\cdot 3\cdot 5\cdot ...\cdot p_{[n]}$. L'intero positivo $N+1$ non è divisibile per nessuno dei $p_{[i]}$: infatti ogni $N/p_{[i]} =: q_i$ è un intero e quindi per ciascuno dei $p_{[i]}$ abbiamo $(N+1)/p_{[i]} = q_i + 1/p_{[i]}$.
Quindi non si può individuare un numero primo maggiore di tutti gli altri ∎

B20 g.02 Per esaminare i numeri primi elencati per valori crescenti adottiamo le seguenti notazioni:

$$p_{[1]} := 2\ ,\quad p_{[2]} := 3\ ,\quad p_{[3]} := 5\ ,\quad p_{[4]} := 7\ ,\quad p_{[5]} := 11\ ,\quad p_{[6]} := 13\ ,\ \ldots\ .$$

Possiamo quindi fare riferimento alla successione dei numeri primi:

$$\mathsf{PRMseq}\ := \langle p_{[1]}, p_{[2]}, p_{[3]}, ..., p_{[j]}, ...\rangle\ = \langle 2, 3, 5, ..., p_{[j]}, ...\rangle\ .$$

Risulta inoltre utile definire $p_{[0]} := 1$ e considerare la successione del genere $\lceil\, \mathbb{N} \longmapsto \mathbb{P}\, \rceil$

$$\mathsf{PRMseq1}\ := \langle p_{[0>]}, p_{[1]}, p_{[2]}, p_{[3]}, ..., p_{[j]}, ...\rangle\ = \langle 1, 2, 3, 5, ..., p_{[j]}, ...\rangle\ .$$

Per l'insieme numerabile dei numeri primi useremo la notazione

$$\begin{aligned}\mathsf{PRM}\ :=\ \mathsf{SetY}(\mathsf{PRMseq})\ =\ \{&2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,\\ &71,73,79,83,89,97,101,103,107,109,113,127,131,137,139,\\ &149,151,157,163,167,173,179,181,191,193,197,199,...\}\end{aligned}\quad .$$

Scriviamo inoltre $\mathsf{PRM1}\ :=\ \mathsf{SetY}(\mathsf{PRMseq1})\ =\ \{1, 2, 3, 5, 7, 11, 13, ...\}$.

B20 g.03 Sia m un intero maggiore di 1 e diciamo **fattorizzazione mediante primi** di m ogni espressione che fornisce m come prodotto di potenza di numeri primi.
Esempi di fattorizzazione mediante primi: $12 = 2^2\cdot 3$; $1089 = 3^3\cdot 11^2$; $1836 = 2^2\cdot 3^3\cdot 17$.
Per la commutatività del prodotto di interi naturali ogni intero non primo possiede più fattorizzazioni mediante primi: per esempio $120 = 2\cdot 5\cdot 2\cdot 2\cdot 3 = 3\cdot 2\cdot 2\cdot 5\cdot 2$.
Possiamo limitarci a utilizzare le fattorizzazioni date da prodotti nelle quali i numeri primi compaiono in ordine noncrescente, come nella $5\,544 = 2\cdot 2\cdot 2\cdot 3\cdot 3\cdot 7\cdot 11$.

Diciamo più in particolare **fattorizzazione canonica** di m una sua fattorizzazione nella quale compaiono come fattori le potenze positive dei numeri primi presi in ordine crescente: un esempio è $5\,544 = 2^3\cdot 3^2\cdot 7\cdot 11$.

Prop. Ogni intero m maggiore di 1 si può esprimere come prodotto di fattori primi e possiede una unica fattorizzazione canonica.

Dim.: Procediamo per induzione.
La possibilità di esprimere un intero positivo come prodotto di numeri primi si constata senza difficoltà per gli interi maggiori di 1 di valore ridotto; la cosa è ovvia per i numeri primi, mentre per i non primi compresi tra 4 e 15 abbiamo:

$4 = 2^2$, $6 = 2 \cdot 3 = 3 \cdot 2$, $8 = 2^3$, $9 = 3^2$, $10 = 2 \cdot 5 = 5 \cdot 2$, $12 = 2^2 \cdot 3$, $14 = 2 \cdot 7$, $15 = 3 \cdot 5$.

Osserviamo che abbiamo presentato solo fattorizzazioni canoniche.

Supponiamo che a ogni positivo inferiore di m si possa dare la fattorizzazione canonica e denotiamo con p un primo che divide m e scriviamo per l'espressione di m/p come prodotto di fattori primi ordinati per valore crescente, ipotizzata per l'induzione (anticipando la notazione in g03)

$$\frac{m}{p} \;=:\; {p_{[i_1]}}^{e_1}\, {p_{[i_2]}}^{e_2} \ldots {p_{[i_h]}}^{e_h} \;.$$

Si ottiene quindi l'espressione per m

$$m \;=\; {p_{[i_1]}}^{e_1}\, {p_{[i_2]}}^{e_2} \ldots {p_{[i_h]}}^{e_h} \cdot p \;,$$

espressione trasformabile nella fattorizzazione canonica attraverso qualche scambio.

Se per m si potessero trovare due diverse fattorizzazioni canoniche darebbero

$$m \;=\; {p_{[i_1]}}^{e_1}\, {p_{[i_2]}}^{e_2} \ldots {p_{[i_k]}}^{e_k} = {p_{[j_1]}}^{f_1}\, {p_{[j_2]}}^{f_2} \ldots {p_{[j_k]}}^{f_k} \;.$$

Eliminando i fattori comuni delle due espressioni si avrebbe una uguaglianza di due prodotti di numeri primi con fattori diversi nei due membri dell'uguaglianza, cosa assurda; da qui l'unicità della fattorizzazione canonica ∎

B20 g.04 Per la fattorizzazione canonica mediante numeri primi dell'intero m maggiore di 1 usiamo scritture come

$$\mathsf{ftrprm}(m) \;=:\; {p_{[i_1]}}^{e_1}\, {p_{[i_2]}}^{e_2} \ldots {p_{[i_h]}}^{e_h} \quad , \text{ con } \; e_1, e_2, ..., e_h \in \mathbb{P} \;\text{ e }\; p_{[i_1]} < p_{[i_2]} < \cdots < p_{[i_h]} \;.$$

Accanto a questa può essere utile quella che chiamiamo **fattorizzazione canonica prolissa** nella quale compaiono come fattori tutti i numeri primi fino al massimo tra i divisori.

$$\mathsf{ftrprim}(m) \;:=\; 2^{\epsilon_1}\, 3^{\epsilon_2} \ldots {p_{[k]}}^{\epsilon_k} \quad , \quad \text{con } \; \epsilon_1, \epsilon_2, ..., \epsilon_{k-1} \in \mathbb{N} \quad \text{ed} \quad \epsilon_k \in \mathbb{P} \;.$$

Per esempio $\mathsf{ftrprm}(133\,848) \;=\; 2^3\, 3^2\, 11\, 13^2$, mentre $\mathsf{ftrprim}(5\,544) \;=\; 2^3\, 3^2\, 5^0\, 7^1\, 11^1$.

Evidentemente h, k, i numeri primi $p_{[i]}$, gli ϵ_i e gli e_i sono determinati univocamente da m.

Può servire anche la successione dei numeri dei numeri naturali esponenti dei successivi fattori della fattorizzazione canonica prolissa che scriviamo

$$\mathsf{ftrprimE}(m) \;:= \langle \epsilon_1, \epsilon_2, \epsilon_3, ..., \epsilon_j, ... \rangle \;\text{ con } \epsilon_j = 0 \text{ per } j > k \;.$$

Tutte le precedenti sequenze e successioni sono in corrispondenza biunivoca con m; si può quindi scrivere

$$m = \mathsf{ftrprimE}^{-1}\,(\mathsf{ftrprimE}(m)) \;.$$

Esempi: $\mathsf{ftrprm}(80) = 2^4 \cdot 5$, $\mathsf{ftrprm}(126) = 2 \cdot 3^2 \cdot 7$, $\mathsf{ftrprm}(1) = 1$,
$\mathsf{ftrprimE}(48) = \langle 4, 3, 0, ... \rangle$, $\mathsf{ftrprimE}(126) = \langle 1, 2, 0, 1, 0, ... \rangle$.

Si constata facilmente che $\mathsf{ftrprm}(m)$, h, $\mathsf{ftrprim}(m)$, $\mathsf{ftrprimE}(m)$ e k si possono ottenere da m con algoritmi ben definiti.

B20 g.05 Occorre segnalare che sono state cercate lungamente ma invano formule chiuse che si servono solo di operazioni algebriche e di operazioni loro derivate che consentissero di individuare costruttivamente l'intera successione dei numeri primi.
Si sono ottenute solo formule in grado di individuare sottoinsiemi di PRM, riuscendo più volte a trovare una formula più elaborata delle precedenti e in grado di individuare un sottoinsieme di numeri primi un poco più esteso di quello dei già noti.
In questa attività sono stati studiati vari compromessi tra estensione dei risultati e complessità della formula.

Vediamo un esempio.

(1) Prop.: Ogni numero intero positivo della forma n^4+8h^6 con n e h interi positivi qualsiasi non è un numero primo.

Dim.: Posto $N := n^2$, abbiamo:
$n^4+8h^6 = N^2+2N(2h^2)^3+8(h^3)^2-2N(2h^2)^3 = \left(N^2+(2h)^3\right)^2-2^2n^2h^6 = \left(n^4+8h^3\right)^2-(2^2nh^3)^2 = \left((n^4+8h^3)+2^2nh^3\right)\left((n^4+8h^3)-2^2nh^3\right)$ ∎

B20 g.06 Dato un intero positivo m, denotiamo con $\mathsf{Dvsr}(m)$ l'insieme dei suoi divisori, con $\mathsf{Dvsrp}(m)$ l'insieme dei suoi divisori propri e con $\mathsf{Sbmlt}(m)$ l'insieme dei suoi sottomultipli.

Ad esempio: $\mathsf{Dvsr}(220) = \{1,2,4,5,10,11,20,22,44,55,110,220\}$, $\mathsf{Dvsrp}(284) = \{1,2,4,71,142\}$, $\mathsf{Sbmlt}(1) = \mathsf{Sbmlt}(2) = \mathsf{Sbmlt}(7) = \emptyset$ e $\mathsf{Sbmlt}(342) = \{2,3,6,9,18,19,38,57,114,171\}$.

Consideriamo l'intero $m \in \{2,3,4,5,6,...\}$ e la sua fattorizzazione canonica

$$\mathsf{ftrprim}(m) =: {p_{[1]}}^{e_1}\,{p_{[2]}}^{e_2}\,...\,{p_{[h]}}^{e_h} \ .$$

L'insieme dei divisori di m è dato da $\left\{f_1 \in [\![\epsilon_1]\!], ..., f_h \in [\![\epsilon_h]\!] \ :|\ {p_{[1]}}^{f_1}\,{p_{[2]}}^{f_2}\,...\,{p_{[h]}}^{f_h}\right\}$.

Il loro numero è $\prod_{i=1}^{h}(e_i+1)$. Per esempio $180 = 2^2\,3^2\,5$ possiede $3\cdot 3\cdot 2 = 18$ divisori: 1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180.

Consideriamo due interi positivi m e n con le relative fattorizzazioni canoniche:

$$m = 2^{e_1}\,3^{e_2}\,5^{e_3}...{p_{[h]}}^{e_h} \qquad \text{e} \qquad n = 2^{g_1}\,3^{g_2}\,5^{g_3}...{p_{[k]}}^{g_k} \ .$$

Si dice **massimo comun divisore** di m ed n e si denota con $\mathrm{MCD}(m,n)$ o con $\mathsf{gcd}(m,n)$ il massimo degli interi che dividono sia m che n.
Per esempio: $\mathrm{MCD}(12,88) = 4$, $\mathrm{MCD}(225,165) = 15$, $\mathrm{MCD}(42,1001) = 7$.

Si dice **minimo comune multiplo** di m ed n e si denota con $\mathrm{mcm}(m,n)$ o con $\mathsf{lcm}(m,n)$ il minimo degli interi che sono multipli sia di m che di n.
Per esempio: $\mathrm{mcm}(12,88) = 264$, $\mathrm{mcm}(225,165) = 2475$, $\mathrm{MCD}(42,1001) = 6006$.
Evidentemente le due precedenti funzioni bivariate del genere $\lceil\, \mathbb{P}\times\mathbb{P} \longmapsto \mathbb{P}\,\rceil$ si possono considerare operazioni binarie su $\mathbb{P}$; inoltre esse sono funzioni simmetriche, ovvero operazioni commutative:

$$\forall m,n \in \mathbb{P} \ : \ \mathrm{MCD}(n,m) = \mathrm{MCD}(m,n) \quad \text{e} \quad \mathrm{mcm}(n,m) = \mathrm{mcm}(m,n) \ .$$

B20 g.07 Consideriamo ancora gli interi m ed n e le due operazioni introdotte sopra.

(1) Prop.: $\mathrm{MCD}(m,n) \ = \ 2^{\min(e_1,g_1)}\,3^{\min(e_2,g_2)}\,...\,{p_{[s]}}^{\min(e_s,g_s)}$ con $s := \min(h,k)$ ∎

(2) Prop.: $\mathrm{mcm}(m,n) \ = \ 2^{\max(e_1,g_1)}\,3^{\max(e_2,g_2)}\,...\,{p_{[t]}}^{\max(e_t,g_t)}$ con $t := \max(h,k)$ ∎

(3) Prop.: Valgono le seguenti fattorizzazioni:

$$m = \mathrm{MCD}(m,n)\cdot\frac{m}{\mathrm{MCD}(m,n)} \quad \text{ed} \quad n = \mathrm{MCD}(m,n)\cdot\frac{n}{\mathrm{MCD}(m,n)} \ .$$

I tre fattori precedenti si ottengono dalle due sequenze degli esponenti delle fattorizzazioni di m ed n

$$\begin{aligned}\mathrm{MCD}(m,n) &= \mathsf{ftrprimE}^{-1}\ Big(\min(\mathsf{ftrprim}(m),\mathsf{ftrprim}(n)\Big)\ ,\\ \frac{m}{\mathrm{MCD}(m,n)} &= \mathsf{ftrprimE}^{-1}\Big(\mathsf{ftrprim}(m)-\mathsf{ftrprim}(\mathrm{MCD}(m,n)\Big)\ ,\\ \frac{n}{\mathrm{MCD}(m,n)} &= \mathsf{ftrprimE}^{-1}\Big(\mathsf{ftrprim}(n)-\mathsf{ftrprim}(\mathrm{MCD}(m,n)\Big)\ \blacksquare\end{aligned}$$

Si dice che due interi positivi m ed n sono **interi positivi coprimi**, e si scrive $m \perp n$, sse non posseggono sottomultipli comuni.
Evidentemente la relazione "$\perp$" è simmetrica. Essa è stata definita entro $\mathbb{P}$, ma può estendersi a $\mathbb{Z}_{ne} := \mathbb{Z} \setminus \{0\}$ ponendo

$$\forall m,n \in \mathbb{Z}_{ne}\ :\ m \perp n\ \text{ sse }\ |m| \perp |n|\ .$$

Si hanno per esempio le relazioni $7 \perp 13$, $27 \perp 77$, $20 \perp -1001$.

Chiaramente $\mathrm{MCD}(m,n) = 1$ sse $\min(\mathsf{ftrprimE}(m),\mathsf{ftrprimE}(n)) = \langle 0,0,...,0,...\rangle$
sse $\mathsf{SbmIt}(m) \cap \mathsf{SbmIt}(n) = \emptyset$.

B20 g.08 Della fattorizzazione degli interi positivi mediante numeri primi e del massimo comun divisore e del minimo comune multiplo di due (e anche di tre, quattro, ...) interi positivi si può dare una presentazione grafica che può risultare efficace.
Consideriamo per esempio $m = 180\,180 = 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ ed $n = 204490 = 2 \cdot 5 \cdot 11^2 \cdot 13^2$; per essi $\mathrm{MCD}(m,n) = 2 \cdot 5 \cdot 11 \cdot 13 = 1\,430$ e $\mathrm{mcm}(m,n) = 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11^2 \cdot 13^2 = 25\,765\,740$.

Consideriamo in generale un intero positivo m per il quale sia $\mathsf{ftrprim}(m) =: 2^{e_1}\,3^{e_2}\,5^{e_3}\,...\,p_{[k]}{}^{e_k}$.
Si dice **istogramma di fattorizzazione** di m l'istogramma di $\mathbb{Z} \times \mathbb{Z}$ costituito da k barre verticali con le caselle minime adagiate sull'asse orizzontale e aventi come altezze, risp., e_1, e_2, ... e_k.

Dati gli istogrammi di due interi m ed n, è semplice tracciare gli istogrammi di fattorizzazione di $\mathrm{MCD}(m,n)$ e di $\mathrm{mcm}(m,n)$: il primo si ottiene con le barre verticali con le altezze minime, il secondo è costituito dalle barre verticali con le altezze massime.

B20 g.09 Vediamo come, con calcoli manuali molto semplici, si riesce a stabilire se un intero positivo m di cui si conosce la notazione decimale m_{10} è divisibile per alcuni piccoli numeri primi.

La divisibilità per 10^k è la più semplice da determinare.

(1) Prop.: m_{10} presenta k zeri finali sse m è divisibile per 10^k ma non per 10^{k+1} $\blacksquare$

In tal caso puòo essere utile scrivere $m = m_1 \cdot 10^k$.

Anche la divisibilità per 2 e per 5 si stabiliscono rapidamente.

(2) Prop.: Un intero positivo m è divisibile per 2 sse l'ultima cifra di m_{10} è 0, 2, 4, 6 o 8.

Dim.: Scriviamo $m = \left\lfloor \frac{m}{10} \right\rfloor \cdot 10 + u$ con $u := m\%10$. Chiaramente m divide 2 (oppure 5) sse u divide 2 [oppure 5] $\blacksquare$

Seguono subito due caratterizzazioni di m_{10} che equivalgono alla divisibilità di m per il quadrato, risp., di 2 e di 5.

(3) Prop.: Un intero positivo m è divisibile per 4 sse
aut la sua ultima cifra decimale è 0, 4 o 8 e la sua penultima cifra è pari
aut la sua ultima cifra decimale è 2 o 6 e la sua penultima cifra è dispari.

Dim.: Scriviamo $m = \left\lfloor \frac{m}{100} \right\rfloor \cdot 100 + u$ con $u := m\%100$ e osserviamo che m divide 4 sse u divide 4; la caratterizzazione della divisibilità per 4 dei numeri positivi esprimibili con due cifre si verifica facilmente ∎

(4) Prop.: Un intero positivo m è divisibile per 25 sse le due ultime cifre della sua notazione decimale sono 00, 25, 50 o 75.

Dim.: Basta scrivere ancora $m = \left\lfloor \frac{m}{100} \right\rfloor \cdot 100 + u$ e osservare i 4 numeri naturali inferiori a 100 e divisibili per 25 ∎

B20 g.10 Esaminiamo la divisibilità per 3 e per 9.

(1) Prop.: Un intero naturale m è divisibile per 3 sse la somma delle cifre decimali di m_{10} è divisibile per 3.

Dim.: Osserviamo preliminarmente che l'intero in esame si può esprimere come

$$m = \sum_{i=0}^{k} d_i \, 10^i = \sum_{i=0}^{k} d_i \, (10^i - 1) + \sum_{i=0}^{k} d_i$$

e che $\sum_{i=0}^{k} d_i \, (10^i - 1)$ è multiplo di 9 e di 3. Di conseguenza

$$3 \text{ divide } m \text{ sse } 3 \text{ divide } \sum_{i=0}^{k} d_i \; ∎$$

(2) Prop.: Un intero naturale m è divisibile per 9 sse la somma delle cifre decimali di m_{10} è divisibile per 9.

Dim.: Dalla osservazione iniziale della dimostrazione precedente si ricava che

$$9 \text{ divide } m \quad \text{sse} \quad 9 \text{ divide } \sum_{i=0}^{k} d_i \; ∎$$

I criteri precedenti si possono applicare più volte di seguito: se la somma delle cifre decimali di m_{10} fosse un intero molto grande, s, si potrebbe considerare la somma delle cifre di s_{10}, certamente molto inferiore ad s e spesso tale da rendere inutili altre manovre dello stesso genere.
Inoltre nella effettuazione della somma delle cifre di una notazione decimale si possono trascurare tutti gli addendi divisibili, risp., per 3 o per 9 e si possono ridurre a zero tutte le somme parziali divisibili, risp., per 3 o per 9.

B20 g.11 Non si conoscono criteri semplici per decidere la divisibilità per 7 e neppure per i primi superiori a 11. È invece semplice decidere la divisibilità per 11.
Per questa conveniamo per ogni $m \in \mathbb{N}$ di denotare con O_m l a somma delle cifre di m_{10} nelle posizioni dispari contate a partire dall'ultima, cioè dalla meno pesante, considerata nella posizione 1 e di denotare con E_m la somma delle cifre di m_{10} nelle posizioni pari rimanenti.
Per esempio abbiamo $O_{76} = 6 = E_{76} - 1$, $O_{77} = E_{77} = 7$, e $O_{78} = 8 = E_{78} + 1$, $O_{347} - E_{347} = 10 - 4 = 6$, $O_{1001} - E_{1001} = 1 - 1 = 0$, $O_{12221} - E_{12221} = 4 - 4 = 0$.

(1) Prop.: Un intero naturale m è divisibile per 11 sse la somma delle sue cifre decimali nelle posizioni pari e la somma delle sue cifre decimali nelle sue posizioni dispari differiscono per un multiplo di 11 o coincidono.

Dim.: Se si può scrivere $n = \sum_{i=0}^{k} d_i\, 10^i$ con $d_k \neq 0$, introdotti $d_{-1} := 0$ e $d_{k+1} := 0$ si ha l'espressione

$$n \cdot 11 \;=\; n + n \cdot 10 \;=\; \sum_{i=0}^{k+1} d_i\, 10^i + \sum_{i=0}^{k+1} d_{i-1}\, 10^i = \sum_{i=0}^{k+1} (d_i + d_{i-1})\, 10^i \;,$$

facilmente riconoscibile nell'usuale schema per la moltiplicazione di interi mediante le loro notazioni decimali [B10d].

Denotiamo ancora con O_n e con E_n, risp., le somme delle cifre che compaiono come fattori delle potenze pari e delle potenze dispari di 10, senza effettuare alcuna somma locale con riporto; per entrambe le somme otteniamo $O_n = E_n = \sum_{i=0}^{k} d_i$. I valori delle "somme competitive" E_n e O_n si possono ottenere trasformando i successivi addendi $d_i + d_{i-1}$, eventualmente aumentati di un riporto precedente r_{i-1}, nei resti della divisione per 10 e nei riporti da assegnare alla somma in competizione per la successiva potenza di 10.

Evidentemente se nessuna delle somme $d_i + d_{i-1}$ supera 9 si ha $O_n = E_n$ (questo accade in particolare se nessuna delle cifre d_i supera 4). Ciascuna modifica di $d_i + d_{i-1} + r_{i-1}$ comporta una diminuzione di 19 per la propria somma e un aumento di 1 per la somma in competizione dovuta al riporto; tutte queste modifiche trasformano la differenza tra le somme in competizione aumentandola o riducendola di 11.

A questo punto si può concludere affermando che per ogni m multiplo di 11, $m =: n \cdot 11$, si ha il corrispondente $|O_m - E_m|$ multiplo di 11, mentre a ogni m della forma $n \cdot 11 + h$ con $h \in [1 : 10]$ corrisponde il valore $|O_m - E_m|$ della forma $t\,11 \pm h$, cioè non multiplo di 11 ∎

B20 g.12 Alcuni esempi sulla divisibilità per 11.
Per $m := 1\,560\,383$ si ha $O_n = 13 = E_n$; deve quindi essere $m = n \cdot 11$ e per n si trova $n = 141\,853$. Viceversa non sono divisibili per 11, né $k := m + 4 = 1\,560\,387$, per il quale $O_k = 17$ ed $E_k = 13$, né $h = n - 6 = 1\,560\,377$, tale che $O_h = 17$ ed $E_h = 12$. Anche $j := m - 44 = 1\,560\,339$ deve dividere 11 e per esso $O_j = 19$ ed $E_j = 8 = 19 - 11$.

In relazione a quanto sopra si possono segnalare alcune curiosità numeriche.

Si osserva che $1001 = 7 \cdot 11 \cdot 13$ e quindi che sono divisibili per 7, 11 e 13 numeri come 835 835, 1 112 111 e 22 244 222. Anche 100 001 è divisibile per 11; quindi sono divisibili per 11 anche numeri come 1 234 512 345 e 3 333 366 633 333 .

Si osserva che $11 \cdot 11 = 121$, $111 \cdot 111 = 12\,321$, $1\,1111 \cdot 1\,111 = 1\,234\,321$, ..., $111\,111\,111 \cdot 111\,111\,111 = 12\,345\,678\,987\,654\,321$; ma non bisogna esagerare, in quanto $1\,111\,111\,111 \cdot 1\,111\,111\,111 = 1\,234\,567\,900\,987\,654\,321$.

B20 g.13 In linea di massima la divisibilità di un intero positivo m per un numero non primo d si decide stabilendo se esso è divisibile per un fattore primo p di d e in caso positivo esaminando la divisibilità di m/p per d/p.

Questo esame si può un poco semplificare evitando di effettuare i calcoli di m/p e d/p quando si tratta della divisibilità per alcuni piccoli multipli di 3, 5 e 11.

Per esempio per garantirsi la divisibilità per 6 basta stabilire con i criteri visti in precedenza, sia la divisibilità per 2 che quella per 3. Simili economie si possono realizzare per la divisibilità per numeri come 12, 15, 22, 24, 27, 30, 33, 40, 44, 45, 55, 60, 66, 90, 99.

B20 g.14 La proprietà di un intero positivo di essere un numero primo viene chiamata **primalità**.

La decisione se un dato intero positivo è un primo o meno serve in numerose circostanze. Per calcoli sistematici e/o su grandi numeri interi risulta necessario servirsi di procedure automatiche, talora in modo molto sofisticato.
Qui ci limitiamo a presentare un semplice procedimento per raggiungere la suddetta decisione.

Per stabilire se l'intero positivo m è primo disponendo di un elenco dei più ridotti numeri primi si può procedere a esaminare la divisibilità per i primi via via crescenti. Se si trova che un primo p divide m risulta stabilita la non primalità di m senza che si debbano esaminare i primi superiori.

Resta invece stabilito che m è primo sse nessuno dei primi p tali che $p^2 \leq m$ divide m. È infatti inutile chiedersi se m è divisibile per un primo q tale che $m < q^2$: infatti se così fosse si sarebbe trovato in precedenza che m è divisibile per $m/q(< q)$ o per un fattore primo di questo intero il cui quadrato m^2/q^2 non supera m.

Il problema della primalità si enuncia in modo semplice, ma è molto impegnativo nel caso di numeri interi positivi grandi.
Questo procedimento si dice avere una complessità più che polinomiale e questo, come vedremo in C47, dice che appartiene alla classe dei procedimenti di elevata complessità computazionale, manovre che possono rivelarsi infattibili se non si dispone di risorse molto molto grandi.

B20 g.15 Sia per lo sviluppo della teoria dei numeri che per applicazioni di grande rilievo economico come la crittografia delle telecomunicazioni digitali sono di notevole interesse i procedimenti per decidere se un dato intero positivo è primo e in caso contrario per trovare la sua fattorizzazione mediante fattori primi. In effetti fin dall'antichità si sono redatti elenchi i numeri primi e si è cercata una formula che consentisse di rappresentarli tutti e che, possibilmente, fosse valutabile con una certa rapidità. Questa formula non esiste e ci si deve accontentare di formule parziali e di procedimenti che consentono di individuare insiemi di primi molto estesi e anche completi, ma in tempi lunghi.

Un procedimento classico per la compilazione di elenchi di primi viene chiamato **crivello di Eratostene**, dal nome di uno dei più grandi scienziati greco-ellenistici, Eratostene di Cirene .
Si tratta di operare sopra le componenti di una lunga sequenza $S = \langle a_2, s_3, s_4, s_5, ..., s_N \rangle$ di valori binari che inizialmente sono posti uguali ad 1; l'intero N viene scelto in modo da essere sufficientemente elevato per gli scopi attuali. Si organizza una sequenza di manovre che fanno riferimento ai successivi numeri primi $p = 2, 3, 5, ...$; questi vengono individuati dalle successive posizioni della S occupate da 1. La manovra relativa al numero primo p consiste nel porre a 0 tutte le cifre nelle posizioni $k \cdot p$ della S, evidentemente relative a numeri non primi. Conclusa l'eliminazione dei multipli di p, si passa alla manovra analoga per il successivo primo che viene individuato dalla prima posizione della S a destra di quella occupata da p, evidentemente relativa a un intero non divisibile per alcun primo inferiore. Alla fine del processo si dispone di un elenco di primi utilizzabile sia come sequenza binaria sia come elenco di scritture decimali, queste ottenibili scorrendo la sequenza binaria e facendo crescere un contatore.

Oggi si usano sofisticati procedimenti che si servono dei sistemi di computers più potenti per far procedere la elencazione dei numeri primi in genere e di numeri primi con proprietà particolari.
Questi argomenti sono trattati in particolare in `Numeri di Mersenne (wi)` e `Numeri di Lucas (wi)`.

B20 h. frazioni, numeri razionali e operazioni sui razionali

B20 h.01 Ricordiamo le notazioni introdotte in :g per i numeri primi con le seguenti successioni:

$$\mathsf{PRMseq1} := \langle p_{[0]}, p_{[1]}, p_{[2]}, p_{[3]}, ..., p_{[j]}, ... \rangle = \langle 1, 2, 3, 5, ..., p_{[j]}, ... \rangle \ ,$$

$$\mathsf{PRM} := \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 91, 97, ...\} \ ,$$

$$\mathsf{PRM1} := \{1\} \dot\cup \mathsf{PRM} = \{1, 2, 3, 5, 7, 11, 13, 17, 19, 23, ...\} \ ,$$

la fattorizzazione mediante numeri primi di un intero positivo m

$$\mathsf{ftrprim}(m) = 2^{\epsilon_1} 3^{\epsilon_2} 5^{\epsilon_3} ... p_{[k]}^{\epsilon_k} \quad , \quad \text{con } \epsilon_1, \epsilon_2, ..., \epsilon_k \in \mathbb{N} \quad \text{ed} \quad \epsilon_k > 0 \text{ se } m > 1 \ ,$$

nonché la successione degli esponenti della fattorizzazione di m mediante primi

$$\mathsf{ftrprimE}(m) := \langle \epsilon_1, e_2, \epsilon_3, ... \epsilon_h, ... \rangle \ \text{ con } e_k = 0 \text{ per } k > h \ .$$

Ricordiamo poi che ftrprim, ftrprimE e k sono determinati univocamente da m e che m è determinato univocamente da $\mathsf{ftrprimE}(m)$ e può scriversi $m = \mathsf{ftrprimE}^{-1}(\mathsf{ftrprimE}(m))$.

Ricordiamo inoltre che, dati due interi positivi m ed n, sono univocamente individuati:
il loro massimo comun divisore $\mathrm{MCD}(m,n) := \max\left(d \in \mathbb{P} \ \S \ d \nmid m \ \wedge \ d \nmid n\right)$;
il loro minimo comune multiplo $\mathrm{mcm}(m,n) := \min\left(\mu \in \mathbb{P} \ \S \ m \nmid \mu \ \wedge \ n \nmid \mu\right)$;
le fattorizzazioni $m = \mathrm{MCD}(m,n) \cdot (m/\mathrm{MCD}(m,n))$, $n = \mathrm{MCD}(m,n) \cdot (n/\mathrm{MCD}(m,n))$
$m = \mathrm{mcm}(m,n)/(n/\mathrm{MCD}(m,n)$ ed $n = \mathrm{mcm}(m,n)/(m/\mathrm{MCD}(m,n)$.

B20 h.02 Se consideriamo due elementi $\langle i,j \rangle$ e $\langle h,k \rangle$ di $\mathbb{Z} \times \mathbb{Z}_{nz} := \mathbb{Z} \times (\mathbb{Z} \setminus \{\mathbf{0}_2\})$ come due vettori-ZZ, ovvero come estremi finali di due segmenti-ZZ orientati aventi il primo estremo nell'origine $\mathbf{0}_2$, viene spontaneo chiamarli **equinclinati** sse si trovano due interi nonnulli a e b tali che $a\,\langle i,j \rangle = b\,\langle h,k \rangle$; questa relazione entro $\mathbb{Z} \times \mathbb{Z}_{nz}$ la esprimiamo enunciando $\langle i,j \rangle \, \boldsymbol{AE}_{incl} \, \langle h,k \rangle$.

Per esempio sono equinclinati: $\langle 4,3 \rangle$ e $\langle 12,9 \rangle$ grazie ad $a = 3$ e $b = 1$; $\langle 10,2 \rangle$ e $\langle -15,-3 \rangle$ grazie ad $a = 3$ e $b = -2$; $\langle -5,5 \rangle$ e $\langle 3,-3 \rangle$ grazie ad $a = 3$ e $b = -5$.

Due punti-ZZ $\langle i,j \rangle$ e $\langle h,k \rangle$ diversi dall'origine sono detti **punti-ZZ allineati con l'origine** sse $i \cdot k = j \cdot h$.
Per esempio sono allineati con l'origine: $\langle 3,2 \rangle$ e $\langle 9,6 \rangle$; $\langle 14,-4 \rangle$ e $\langle 35,-10 \rangle$; $\langle -40,30 \rangle$ e $\langle 60,-45 \rangle$.

(1) Prop.: Due vettori-ZZ $\langle i,j \rangle$ e $\langle h,k \rangle$ sono equinclinati sse i corrispondenti punti sono allineati con l'origine.

Dim.: "$\Longrightarrow$": $\langle a\,i, a\,j \rangle = \langle b\,h, b\,k \rangle \implies a\,i\,k = a\,j\,h \implies i\,k = j\,h$.
"$\Longleftarrow$": $i\,k = j\,h \implies a\langle i,j \rangle - b\langle h,k \rangle$ [per $a := k, b := j$] $= \langle i\,k, j\,k \rangle - \langle j\,h, j\,k \rangle = 0$ ∎

Dunque la relazione tra vettori di $\mathbb{Z} \times \mathbb{Z}_{nz}$ che denotiamo con $\boldsymbol{AE}_{incl}$ si può chiamare **equiinclinazione** oppure **allineamento con l'origine**.

B20 h.03 Prop. La equiinclinazione è una equivalenza entro $\mathbb{Z} \times \mathbb{Z}_{nz}$.

Dim.: L'equiinclinazione-ZZ è evidentemente riflessiva e simmetrica; resta da dimostrare che sia transitiva. Consideriamo $\langle i,j \rangle, \langle h,k \rangle, \langle m,n \rangle \in \mathbb{Z} \times \mathbb{Z}_{nz}$ e si abbia equiinclinazione tra prima e seconda coppia ed equiinclinazione tra seconda e terza coppia; più precisamente siano a, b, c, d interi nonnulli tali che sia $a\,\langle i,j \rangle = b\,\langle h,k \rangle$ e $c\,\langle h,k \rangle = d\,\langle m,n \rangle$.
Si trova $a\,c\,\langle i,j \rangle = b\,c\,\langle h,k \rangle = b\,d\,\langle m,n \rangle$, quindi la equiinclinazione tra $\langle i,j \rangle$ e $\langle m,n \rangle$ ∎

Le classi di equivalenza della relazione $\boldsymbol{AE}_{incl}$, prevedibilmente, sono chiamate **classi di equiinclinazione**. Tra di esse si trovano:

l'asse-ZZ orizzontale privata dell'origine , $\mathsf{Ox}_{nz} := \{x \in \mathbb{Z}_{nz} :| \langle x, 0\rangle\}$,
l'asse-ZZ verticale privata dell'origine , $\mathsf{Oy}_{nz} := \{y \in \mathbb{Z}_{nz} :| \langle 0, y\rangle\}$,
la diagonale-ZZ privata dell'origine , $\{x \in \mathbb{Z}_{nz} :| \langle x, x\rangle\}$,
la codiagonale-ZZ privata dell'origine , $\{x \in \mathbb{Z}_{nz} :| \langle x, -x\rangle\}$.

Gli insiemi ottenuti aggiungendo l'origine $\langle 0, 0\rangle$ alle varie classi di equiinclinazione costituiscono l'insieme delle rette-ZZ passanti per l'origine, entità chiamata più specificamente **fascio delle rette-ZZ** passanti per l'origine.
Diciamo **classe-ZZ razionale** ogni classe di equiinclinazione diversa dall'asse-ZZ verticale privata dell'origine Oy_{nz}.

Introduciamo i seguenti termini:
punti-PP, i punti di $\mathbb{P} \times \mathbb{P}$;
punti-NN, i punti di $\mathbb{N} \times \mathbb{N}$;
punti-PN, i punti di $\mathbb{P} \times \mathbb{N}$;
punti-NP, i punti di $\mathbb{N} \times \mathbb{P}$;
punti-ZP, i punti di $\mathbb{Z} \times \mathbb{P}$;
punti-PZ, i punti di $\mathbb{N} \times \mathbb{Z}$;
punti-NZ, i punti di $\mathbb{N} \times \mathbb{Z}$;
punti-ZN, i punti di $\mathbb{Z} \times \mathbb{N}$.

Useremo inoltre i termini **semipiano-ZP** per l'insieme $\mathbb{Z} \times \mathbb{P}$, **semipiano-ZN** per $\mathbb{Z} \times \mathbb{N}$ e **semipiano-ZNeg** per $\{x \in \mathbb{Z}, y \in \mathbb{P} :| \langle x, -y\rangle\} = \mathbb{Z} \times \mathbb{N}_-$.

Chiaramente ogni classe-ZZ razionale si bipartisce nella sua intersezione con il semipiano-ZP, che viene detta **semiretta-ZP per l'origine**, e nella sua intersezione con il semipiano-ZZ- .

B20 h.04 Ricorrendo alla fattorizzazione mediante primi, ovvero all'algoritmo euclideo, si trova formalmente che ogni semiretta-ZP per l'origine, e quindi ogni classe-ZZ razionale, contiene una e una sola coppia $\langle n, d\rangle$ con $n \in \mathbb{Z}$ e $d \in \mathbb{P}$ tale che $|n| \perp d$. Tale coppia di interi privi di divisori comuni viene detta **coppia ridotta della classe-ZZ razionale**.
Per ogni punto-PZ, cioè per ogni coppia $\langle a, b\rangle \in \mathbb{P} \times \mathbb{Z}$, gli interi costituenti la corrispondente coppia ridotta si possono ottenere come

$$n = \frac{a}{\mathrm{MCD}(a, |b|)} \qquad \text{e} \qquad d = \frac{b}{\mathrm{MCD}(a, |b|)} \ . \tag{1}$$

L'insieme delle coppie ridotte costituisce un insieme di rappresentativi delle classi-ZZ razionali; ogni coppia ridotta corrisponde all'elemento di una semiretta-PZ per l'origine più vicino all'origine (e agli assi-ZZ). Si osserva anche che la classe razionale e la semiretta-PZ per l'origine rappresentate dalla coppia ridotta $\langle n, d\rangle$ sono esprimibili, risp., con

$$\{h \in \mathbb{Z}_{nz} \ : \ \langle h \cdot n, h \cdot d\rangle\} \qquad \text{e} \qquad \{h \in \mathbb{P} \ : \ \langle h \cdot n, h \cdot d\rangle\} \ . \tag{2}$$

B20 h.05 È utile osservare la raffigurazione dei punti-ZP che distingue le coppie ridotte marcandole con maggiore evidenza.

L'insieme dei punti-ZP in evidenza $\langle n, d\rangle \in \mathbb{Z} \times \mathbb{P}$ con i componenti coprimi è simmetrico rispetto all'asse verticale, cioè è invariante per la riflessione di $\mathbb{Z} \times \mathbb{Z}$ rispetto Oy_{ZZ} $\lceil \langle x, y\rangle \in \mathbb{Z} \times \mathbb{P} \mapsto \langle -x, y\rangle \rceil$.

Inoltre il suo sottoinsieme $\mathbb{P} \times \mathbb{P}$ è simmetrico rispetto alla diagonale (ossia alla bisettrice) di $\mathbb{Z} \times \mathbb{Z}$, cioè è invariante per la riflessione $\lceil \langle x, y \rangle \in \mathbb{P} \times \mathbb{P} \mapsto \langle y, x \rangle \rceil$.

Se si confrontano per i diversi $n \in \mathbb{Z}$ le semirette-ZP verticali, semirette della forma $\{y \in \mathbb{P} :| \langle n, y \rangle\}$, le rette-ZZ orizzontali $\{x \in \mathbb{Z} :| \langle x, n \rangle\}$ e i segmenti-ZZ appartenenti a rette-ZZD2, cioè i segmenti della forma $\{x \in (\mathrm{n}\,] :| \langle x, n - x \rangle\}$, si osservano rilevanti differenze tra questi insiemi caratterizzati da n numero primo e quelli relativi ad n numero fattorizzabile.

B20 h.06 Introduciamo l'**insieme dei numeri razionali**, come insieme delle entità ottenibili per soggettificazione collettivizzante dalle classi razionali; tale insieme si denota con $\mathbb{Q}$, simbolo introdotto da matematici tedeschi e richiamante il termine *quotient*.

Dalla figura precedente si osserva che i numeri (classi) razionali aventi coppie ridotte della forma $\langle z, 1 \rangle$ con $z \in \mathbb{Z}$, cioè costituenti la retta-ZP orizzontale $\{x \in \mathbb{Z} :| \langle x, 1 \rangle\}$ posta immediatamente al di sopra dell'asse-ZZ orizzontale, sono in evidente biiezione con i numeri interi relativi.

Un numero razionale r, in quanto associato biunivocamente ad una classe-ZZ razionale, può essere rappresentato da tutte le scritture h/k, o dalle equivalenti $\dfrac{h}{k}$, derivate dalle diverse coppie $\langle h, k \rangle$ di tale classe.
Le scritture h/k e $\dfrac{h}{k}$ vengono dette **forme frazionarie**, o in breve **frazioni**, esprimenti il razionale r; talora per denotare la relazione tra una forma frazionaria e il corrispondente numero razionale si usano scritture come $h/k \in r$. Di una frazione h/k l'intero h è detto **numeratore**, mentre k è chiamato **denominatore**.

Sono particolarmente utili le **forme frazionarie ridotte** n/d corrispondenti alle coppie ridotte rappresentative delle varie classi razionali: per tali classi si può proporre la scrittura $\mathrm{redfrac}(r) := \dfrac{n}{d}$.

Denotiamo con $\mathbb{Q}_{redfr}$ l'insieme delle forme frazionarie ridotte dei numeri razionali; si osserva che la funzione redfrac è una biiezione algoritmica tra $\mathbb{Q}$ e $\mathbb{Q}_{redfr}$.

B20 h.07 Il passaggio da una generica forma frazionaria alla equivalente forma ridotta si dice **riduzione della frazione ai minimi termini** e si effettua riferendosi alle fattorizzazioni mediante primi del numeratore e del denominatore richiamate in h01.

Si dice invece più genericamente **semplificazione di una frazione** la sua trasformazione in una forma frazionaria equivalente avente numeratore e denominatore minori e non necessariamente ridotta: una frazione $\dfrac{h}{k}$ si semplifica trovando un intero positivo c divisore comune ad h e k e sostituendola con $\dfrac{h/c}{k/c}$.
La frazione $\dfrac{100\,100}{214\,500}$ può essere immediatamente semplificata nella $\dfrac{1\,001}{2\,145}$, mentre le determinazione della sua forma ridotta, che è $\dfrac{7}{15}$, richiede qualche altro calcolo.

Le frazioni della forma $\dfrac{n \cdot f}{f}$ con $n \in \mathbb{Z}$ ed $f \in \mathbb{Z}_{nz}$ si dicono **frazioni apparenti** o **frazioni improprie**.
I numeri razionali dati da frazioni apparenti, cioè rappresentabili con frazioni ridotte della forma $z/1$, oltre a essere in evidente biiezione con i numeri interi, risultano equivalenti a essi logicamente e operativamente: quindi i numeri razionali dati da frazioni apparenti si possono identificare con gli interi.

A questo punto è pienamente accettabile affermare che $\mathbb{Q}$ è una estensione di $\mathbb{Z}$.

B20 h.08 Dobbiamo ora giustificare l'uso del termine "numeri" per i razionali, definendo sulle loro forme frazionarie le operazioni di somma, sottrazione e prodotto e introducendo una relazione d'ordine

in modo che queste entità estendano le omologhe definite sugli interi, cioè in modo che applicate alle frazioni apparenti siano strettamente simili a quelle definite su $\mathbb{Z}$; anche con questo ampliamento è importante che si mantenga la maggior parte delle proprietà che valgono per $\mathbb{Z}$.

Dobbiamo anche mostrare che questa estensione risulta effettivamente utile grazie al fatto che i razionali rendono disponibili procedimenti di calcolo di ampia utilità non praticabili nel più ridotto ambito degli interi.
A tal fine si introduce sopra i razionali una operazione di divisione che è l'inversa del prodotto e che si può effettuare su tutte le coppie di razionali con la sola esclusione di quelle con il secondo componente nullo. Essa si riduce al quoziente tra interi quando viene applicata a coppie di numeri interi dei quali il primo sia multiplo del secondo.

Si constata allora che la divisione costituisce un notevole potenziamento del passaggio al quoziente tra interi: la divisione tra razionali estende in misura notevole il quoziente tra un intero e un suo sottomultiplo, in quanto è applicabile a un insieme di coppie di interi molto più esteso delle coppie con il primo componente multiplo del secondo (nonnullo).
Vedremo inoltre che la divisione si può effettuare con algoritmi applicabili alle notazioni posizionali in qualsiasi base.

B20 h.09 Siano dunque $m, p \in \mathbb{Z}$ e $n, q, c, k \in \mathbb{Z}_{nz}$. Le seguenti due uguaglianze rispecchiano proprietà delle forme frazionarie.

(1) **regola dell'uguaglianza** (da a02): $\dfrac{m}{n} = \dfrac{p}{q} \iff m \cdot q = n \cdot p$.

(2) **regola di semplificazione** (da h07): $\dfrac{m \cdot c}{n \cdot c} = \dfrac{m}{n}$.

Estendiamo quindi le operazioni di somma, passaggio all'opposto e prodotto mediante le seguenti definizioni.

(3) **somma di razionali**: $\dfrac{m}{n} + \dfrac{p}{q} := \dfrac{m \cdot q + p \cdot n}{n \cdot q}$.

(4) **passaggio all'opposto di razionale**: $-\left(\dfrac{m}{n}\right) := \dfrac{-m}{n} = \dfrac{m}{-n}$.

(5) **prodotto di razionali**: $\dfrac{m}{n} \cdot \dfrac{p}{q} := \dfrac{m \cdot p}{n \cdot q}$.

Si osserva che quando $n = q = 1$ le definizioni si riducono a ben note uguaglianze concernenti gli interi.
Si vede inoltre che 1/1=1 è l'elemento neutro per il prodotto di numeri razionali, come accade per le operazioni di prodotto tra interi naturali e tra interi relativi.

B20 h.10 (1) Eserc. Dimostrare che la somma di frazioni è commutativa e associativa.

(2) Eserc. Dimostrare che la somma di una frazione e della opposta dà 0.

(3) Eserc. Dimostrare che il prodotto è commutativo e associativo e che 1/1 è elemento neutro per tale operazione.

(4) Eserc. Dimostrare la distributività del prodotto rispetto alla somma.

B20 h.11 Definiamo ora per i razionali il passaggio al reciproco e la divisione.

(1) **passaggio al reciproco di razionale**: $\forall m, n \in \mathbb{Z}_{nz} \ : \ \left(\dfrac{m}{n}\right)^{-1} := \dfrac{n}{m}$.

(2) **divisione tra razionali**: $\forall m \in \mathbb{Z}\ ,\ n, k, q \in \mathbb{Z}_{nz} \ : \ \left(\dfrac{m}{n}\right) : \left(\dfrac{k}{q}\right) := \dfrac{m}{n} \cdot \dfrac{q}{k} = \dfrac{m \cdot q}{n \cdot k}$.

Si osserva che il prodotto di un razionale per il proprio reciproco, in forza della regola di semplificazione, è uguale a 1. Inoltre la divisione è l'operazione inversa del prodotto per i razionali diversi da 0, grazie al fatto che

$$\left(\frac{m}{n} : \frac{k}{q}\right) \cdot \frac{k}{q} \;=\; \frac{(m \cdot q) \cdot k}{(n \cdot k) \cdot q} = \frac{m}{n} \;.$$

Questo giustifica l'utilizzo del termine **inverso di numero razionale** come sinonimo di "reciproco di numero razionale".
È evidente che la divisione non è commutativa: un controesempio è

$$(3/4) \;/\; (7/9) \;=\; 27/28 \;\neq\; (7/9) \;/\; (3/4) \;=\; 28/27 \;.$$

In generale lo scambio degli operandi della divisione equivale al passaggio al reciproco:

$$\left(\frac{m}{n}\right) : \left(\frac{k}{q}\right) \;=\; \frac{m \cdot q}{n \cdot k} \;=\; \left(\frac{k \cdot n}{q \cdot m}\right)^{-1} = \left(\left(\frac{k}{q}\right) : \left(\frac{m}{n}\right)\right)^{-1} \;.$$

Quindi si ha la commutatività della divisione sse si compongono un razionale nonnullo e il suo inverso. Inoltre, come la divisione esatta tra interi, anche la divisione tra razionali nonnulli non è associativa:

$$((12/5) \;/\; (3/2)) \;/\; (7/9) \;=\; 72/35 \;\neq\; (12/5) \;/\; ((3/2) \;/\; (7/9)) \;=\; 168/135.$$

Le operazioni di somma, differenza e prodotto sono dette **operazioni polinomiali** e le operazioni di somma, differenza, prodotto e divisione sono chiamate **operazioni razionali**.

B20 h.12 Estendiamo l'ordinamento canonico degli interi ai numeri razionali con una definizione operativa sulle forme frazionarie. Basta considerare le forme frazionarie con denominatori positivi, chiedendo che sia

$$\forall n, q \in \mathbb{P},\; m, p \in \mathbb{Z} \quad : \quad \frac{m}{n} \leq \frac{p}{q} \iff m \cdot q \leq p \cdot n \;.$$

La precedente richiesta nel caso $n = q = 1$, cioè quando si considerano solo frazioni apparenti, ossia solo numeri interi, si riduce alla `tautologia (wi)` dell'identità: questo fatto garantisce che la relazione introdotta con il simbolo "$\leq$" estende la omologa sugli interi e giustifica l'adozone del suo stesso simbolo.

Si osserva che date due forme frazionarie $\frac{m}{n}$ e $\frac{p}{q}$, possono verificarsi tre situazioni mutuamente esclusive:
se $m \cdot q = p \cdot n$ le due forme sono equivalenti, cioè individuano lo stesso numero razionale $\frac{m}{n} = \frac{p}{q}$;
se $m \cdot q < p \cdot n$ le due forme individuano due numeri razionali diversi per i quali $\frac{m}{n} < \frac{p}{q}$;
se $m \cdot q > p \cdot n$ le due forme individuano due numeri razionali diversi per i quali $\frac{m}{n} > \frac{p}{q}$.
Quindi dati due forme frazionarie qualsiasi si può effettivamente stabilire se la prima esprime un numero razionale minore, uguale o maggiore del numero espresso dalla seconda. Per una decisione (piuttosto frequente) come la precedente si usa il termine **decisione tricotomica**.

Evidentemente la relazione "$\leq$" è riflessiva; in effetti si osserva che se m/n e p/q sono forme frazionarie equivalenti, cioè appartenenti alla stessa classe-ZZ razionale, si ha $m \cdot q = p \cdot n$ e quindi $\frac{m}{n} \leq \frac{p}{q}$ e $\frac{p}{q} \leq \frac{m}{n}$.
È chiaro anche che la relazione è antisimmetrica, in quanto se valgono entrambe le relazioni precedenti, allora $m \cdot q \leq p \cdot n$ e $p \cdot n \leq m \cdot q$, cioè $m \cdot q = p \cdot n$, ovvero le due forme frazionarie sono equivalenti, cioè individuano lo stesso numero razionale.

Inoltre la relazione introdotta è transitiva in quanto:

$\forall m,p,r \in \mathbb{Z},\ n,q,s \in \mathbb{Z}_{nz}$:

$$\frac{m}{n} \le \frac{p}{q} \ \wedge\ \frac{p}{q} \le \frac{r}{s} \iff m\,q\,s \le p\,n\,s \le r\,n\,q \implies m\,s \le r\,n \iff \frac{m}{n} \le \frac{r}{s}\ .$$

Dunque la relazione "$\le$" tra numeri razionali è un ordinamento totale.

B20 h.13 È utile distinguere:
i **razionali positivi**, razionali maggiori di $0 = 0/1$, dati da frazioni con numeratore e denominatore dello stesso segno,
dal razionale 0 e
dai **razionali negativi**, i numeri razionali minori di 0 dati da frazioni con numeratore e denominatore di segni opposti.

Chiaramente se $m,n,k,q \in \mathbb{P}$ si ha $-\dfrac{m}{n} < 0 < \dfrac{k}{q}$.

Denotiamo: l'insieme dei numeri razionali positivi con $\mathbb{Q}_+$,
l'insieme dei razionali nonnegativi con $\mathbb{Q}_{0+}$, l'insieme dei numeri razionali negativi con $\mathbb{Q}_-$,
l'insieme dei razionali nonpositivi con $\mathbb{Q}_{-0}$,
l'insieme dei razionali nonnulli con $\mathbb{Q}_{nz}$.

Risulta necessario estendere da $\mathbb{Z}$ a $\mathbb{Q}$ anche le definizioni di valore assoluto e di funzione segno.
Si definisce **valore assoluto** del numero razionale r

$$|r| \ :=\ \mathrm{abs}(r) \ :=\ \begin{cases} -r & \text{sse } r \in \mathbb{Q}_- \\ r & \text{sse } r \in \mathbb{Q}_{0+} \end{cases}\ . \tag{1}$$

Questa funzione è del genere $\lceil\, \mathbb{Q} \longmapsto\!\triangleright\ \mathbb{Q}_{0+} \,\rceil$; essa non è invertibile, in quanto se si conosce un razionale positivo s e si sa che $|r| = s$, si può concludere solo che $r = s$ oppure $r = -s$.

Si estende a tutti i numeri razionali r la **funzione segno**

$$\mathrm{sign}(r) \ :=\ \begin{cases} -1 & \text{sse } r \in \mathbb{Q}_- \\ 0 & \text{sse } r = 0 \\ 1 & \text{sse } r \in \mathbb{Q}_+ \end{cases}\ . \tag{2}$$

B20 h.14 Eserc. Dimostrare che, se r ed s sono razionali qualsiasi, valgono le seguenti relazioni:

(1) $\quad |r\cdot s| = |r|\cdot|s|\ ;\ \ |r : s| = |r| : |s|\ \ (\text{ sse }\ s \neq 0)\ ;\ \ \big||r| - |s|\big| \le |r \pm s| \le \big||r| + |s|\big| = |r| + |s|\ .$

(2) $$r \ =\ \mathrm{sign}(r)\cdot|r|\ .$$

B20 h.15 Dimostriamo ora che l'ordinamento totale tra razionali rispetta la somma e il prodotto.

(1) Prop.: Consideriamo due razionali positivi m/n e h/k, con $h,k,m,n \in \mathbb{P}$.

$$h/k < m/n \iff (-1)\cdot m/n < (-1)\cdot h/k\ .$$

Dim.: $h/k < m/n \iff h\,n < k\,m \iff -k\,m < -h\,n \iff -m/n < -h/k$ ∎

(2) Prop.: $h/k < m/n\ ,\ u,v \in \mathbb{P} \implies (u/v)(h/k) < (u/v)(m/n)$.

Dim.: $h/k < m/n\ ,\ u,v \in \mathbb{P} \implies n\,h < m\,k\ ,\ u\,v > 0 \implies (u\,v)(n\,h) < (u\,v)(m\,k) \iff$
$(u\,h)(v\,n) < (v\,k)(u\,m) \iff (u\,h)/(v\,k) < (u\,m)/(v\,n) \implies (u/v)(h/k) < (u/v)(m/n)$ ∎

(3) Prop.: $0 < h_1/k_1 < m_1/n_1\ ,\ 0 < h_2/k_2 < m_2/n_2 \implies (h_1/k_1)(h_2/k_2) < (m_1/n_1)(m_2/n_2)$.
Dim.: Supponiamo per semplicità che siano $h_1,k_1,h_2,k_2 \in \mathbb{P}$. Applicando due volte (2) si trova

$(h_1/k_1)(h_2/k_2) < (m_1/n_1)(h_2/k_2) < (m_1/n_1)(m_2/n_2)$ ∎

B20 h.16 Introduciamo ora gli intervalli di razionali, come generalizzazioni degli intervalli di interi e servendoci di notazioni che sono evidenti varianti di quelle riguardanti $\mathbb{Z}$.

Cominciamo con le definizioni degli intervalli razionali limitati.

$\mathbf{[}m/n :: p/q\mathbf{]} := \{r \in \mathbb{Q} \S\ m/n \leq r \leq p/q\}$, intervallo razionale chiuso;

$\mathbf{[}m/n :: p/q\mathbf{)} := \{r \in \mathbb{Q} \S\ m/n \leq r < p/q\}$, intervallo razionale chiuso a sinistra e aperto a destra;

$\mathbf{(}m/n :: p/q\mathbf{]} := \{r \in \mathbb{Q} \S\ m/n < r \leq p/q\}$, intervallo razionale aperto a sinistra e chiuso a destra;

$\mathbf{(}m/n :: p/q\mathbf{)} := \{r \in \mathbb{Q} \S\ m/n < r < p/q\}$, intervallo razionale aperto.

Ancora similmente a quanto fatto per gli interi, definiamo gli intervalli illimitati di numeri razionali.

$\mathbf{[}m/n :: \mathbf{)} := \{r \in \mathbb{Q} \S\ m/n \leq r\}$, intervallo razionale chiuso illimitato superiormente;

$\mathbf{(}m/n :: \mathbf{)} := \{r \in \mathbb{Q} \S\ m/n \leq r\}$, intervallo razionale aperto illimitato superiormente;

$\mathbf{(} :: p/q\mathbf{]} := \{r \in \mathbb{Q} \S\ m/n \leq r\}$, intervallo razionale chiuso illimitato inferiormente;

$\mathbf{(} :: p/q\mathbf{)} := \{r \in \mathbb{Q} \S\ m/n \leq r\}$, intervallo razionale aperto illimitato inferiormente.

Lo stesso $\mathbb{Q}$ si può considerare intervallo di razionali illimitato inferiormente e superiormente.

Occorre segnalare che nelle precedenti locuzioni la qualifica “a sinistra” equivale alla qualifica “inferiormente” e la qualificca ’‘a destra” equivale alla qualifica ”superiormente”.

Evidentemente questi intervalli costituiscono strumenti di portata superiore di quella degli intervalli di numeri interi. Va tuttavia segnalato che servono intervalli numerici che risultino strumenti di maggiore efficacia dei precedenti e la cui definizione richiede entità che non sono numeri razionali.

Li vedremo più avanti in quanto si possono definire solo con procedimenti sostanzialmente diversi da quelli (finitistici) qui usati; in particolare vedremo come questi altri intervalli di razionali consentano una definizione costruttiva dell’insieme dei numeri reali [B38 e B42], insieme numerico che costituisce un ampliamento sostanziale di $\mathbb{Q}$.

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