ALGEBRA I: NUMERI INTERI, DIVISIBILITÀ E IL TEOREMA FONDAMENTALE DELL'ARITMETICA

1. Richiami sulle proprietà dei numeri naturali

Ho mostrato in un'altra dispensa come ricavare a partire dagli assiomi di Peano le principali strutture sull'insieme $\mathbb{N}$ dei numeri naturali. Qui mi limito a richiamare quelle che utilizzerò in seguito. Ricordo che $\mathbb{N}$ possiede un'operazione di *somma* $\mathbb{N} \times \mathbb{N} \ni (a, b) \mapsto a + b \in \mathbb{N}$ ed un'altra di *molriplicazione* $\mathbb{N} \times \mathbb{N} \ni (a, b) \mapsto a \cdot b$[1].

La somma e la moltiplicazione sono operazioni commutative ed associative, e la moltiplicazione è distributiva rispetto alla somma:

$$a + b = b + a, \qquad (a + b) + c = a + (b + c), \tag{1.1}$$

$$ab = ba, \qquad (ab)c = a(bc), \qquad a(b + c) = ab + ac, \qquad (a + b)c = ac + bc, \tag{1.2}$$

per ogni $a, b, c \in \mathbb{N}$. 0 e 1 sono gli elementi neutri di somma e moltiplicazione:

$$0 + a = a = a + 0, \qquad 1 \cdot a = a = a \cdot 1, \qquad 0 \cdot a = 0 = a \cdot a, \tag{1.3}$$

per ogni scelta di a in $\mathbb{N}$. Vale una regola di cancellazione per la somma:

$$a + c = b + c \Rightarrow a = b, \tag{1.4}$$

ed una corrispondente per il prodotto

$$ac = bc \Rightarrow a = b \qquad \text{se } c \neq 0. \tag{1.5}$$

Una facile conseguenza della proprietà di cancellazione per il prodotto è la *legge di annullamento del prodotto*:

$$ab = 0 \Rightarrow a = 0 \text{ oppure } b = 0. \tag{1.6}$$

L'insieme $\mathbb{N}$ possiede un buon ordinamento $\leq$, cioè una relazione d'ordine (totale) rispetto alla quale ogni sottoinsieme non vuoto possiede un elemento minimo. L'elemento minimo di $\mathbb{N}$ è lo 0, e di $\mathbb{N} \setminus \{0\}$ è 1. Le operazioni sono compatibili con l'ordinamento. In particolare, per ogni scelta di $a, b, c \in \mathbb{N}$ si ha:

$$a \leq b \Leftrightarrow a + c \leq b + c, \tag{1.7}$$

ed anche

$$a \leq b \Leftrightarrow ac \leq bc, \tag{1.8}$$

se $c \neq 0$. Di conseguenza da $a \leq c, b \leq d$ si ottiene $a + b \leq c + d$ come pure $ab \leq cd$. Poiché se $a \neq 0$, allora $1 \leq a$, abbiamo che $a \neq 0 \Rightarrow b \leq ab$. In particolare, da $ab = 1$ segue $a, b \leq 1$ e quindi $a = b = 1$. Questo fatto si può anche esprimere affermando che 1 è l'unico elemento *invertibile* di $\mathbb{N}$. E' importante ricordare che

$$a \leq b \Leftrightarrow b = a + c \text{ per qualche } c. \tag{1.9}$$

Tale elemento c è unico a causa della proprietà di cancellazione, e viene solitamente indicato con $b - a$.
E' probabilmente superfluo ricordare che $a \leq b$ si scrive anche $b \geq a$, che $a \leq b, a \neq b$ si scrive anche $a < b$ e che $a \not< b$ equivale a $a \geq b$.

Esercizi.

(1) Siano $a, b \leq c$. Mostrate allora che $a \leq b$ se e solo se $c - b \leq c - a$.
(2) Un sottoinsieme $X \subset \mathbb{N}$ è *limitato dall'alto* se esiste un *maggiorante* di X, cioè un elemento $n \in \mathbb{N}$ tale che ogni $x \in X$ soddisfi $x \leq n$. Mostrate che ogni sottoinsieme di $\mathbb{N}$ limitato dall'alto ammette elemento massimo. *[Sugg.: sfruttate l'esercizio precedente, e il buon ordinamento di $\mathbb{N}$]*
(3) Mostrate che in $\mathbb{N}$ vale la proprietà archimedea: per ogni scelta di $a, b \in \mathbb{N}$ tale che $a \neq 0$, esiste n tale che $b \leq na$.

2. Piccolo vocabolario di strutture algebriche

In matematica, una struttura algebrica è un insieme dotato di una o più operazioni, che soddisfano opportune proprietà o *assiomi*: ad esempio, l'insieme $\mathbb{N}$ dei numeri naturali, dotato delle operazioni di somma e moltiplicazione, è una struttura algebrica. Nella pratica, si preferisce studiare strutture algebriche con caratteristiche migliori di quelle di $\mathbb{N}$ - nelle quali ad esempio sia possibile anche sottrarre e dividere elementi.

In questo paragrafo farò un elenco dei principali tipi di strutture algebriche che incontreremo durante il corso. Ricordo che un'operazione $\circ : X \times X \to X$ si dice associativa se $(x \circ y) \circ z = x \circ (y \circ z)$ per ogni $x, y, z \in X$, e commutativa se $x \circ y = y \circ x$ per ogni $x, y \in X$.

Definizione 2.1. Un *gruppo* è un insieme G dotato di un'operazione associativa $\circ : G \times G \to G$ associativa, per la quale

- esiste un elemento $e \in G$ che soddisfa $e \circ g = g \circ e = g$ per ogni $g \in G$.
- Per ogni $g \in G$ esiste $h \in G$ tale che $g \circ h = h \circ g = e$.

[1] Spesso il punto tra i due argomenti della moltiplicazione viene dimenticato, e si scrive ab invece di $a \cdot b$.

Un gruppo è *abeliano* se la sua operazione è commutativa.

Si vede facilmente che esiste al più un elemento che soddisfa la prima proprietà. Effettivamente, se $e \circ g = g \circ e = g = e' \circ g = g \circ e'$ per ogni $g \in G$, allora in particolare $e = e \circ e' = e'$. L'elemento e è detto *elemento neutro* o *identità* del gruppo G.

Ogni elemento h tale che $g \circ h = h \circ g = e$ si dice *inverso* di g. Ogni elemento possiede al più un inverso: in effetti se h e h' sono entrambi inversi di g, si ha: $h = h \circ e = h \circ (g \circ h') = (h \circ g) \circ h' = e \circ h' = h'$. L'inverso di g in G è quindi univocamente determinato, ed è solitamente indicato con la notazione g^{-1}. Quando però l'operazione di gruppo è la somma $+$ è consigliabile indicare l'inverso con $-g$.

Esempi 2.2. (1) L'operazione $e \circ e = e$ definisce una struttura di gruppo sull'insieme $\{e\}$.

(2) Sull'insieme $X = \{P, D\}$ definiamo un'operazione di somma tale che $P + P = P, P + D = D + P = D, D + D = P$. E' facile mostrare (fatelo!) che $+$ definisce una struttura di gruppo abeliano su X, la cui identità è P.

(3) Né l'operazione di somma né quella di prodotto definiscono una struttura di gruppo sull'insieme $\mathbb{N}$ dei numeri naturali.

(4) Sia S_n l'insieme di tutte le applicazioni invertibili dell'insieme $\{1, 2, \ldots, n\}$ in se stesso. Allora l'operazione di composizione tra applicazioni definisce (mostratelo!) una struttura di gruppo non abeliano su S_n. S_n è detto *gruppo simmetrico su n elementi*.

Definizione 2.3. Un *anello* è un insieme A dotato di un'operazione di *somma* $+ : A \times A \to A$, che vi definisce una struttura di gruppo abeliano – il cui elemento neutro è indicato con 0; e di un'operazione associativa di moltiplicazione $\cdot : A \times A \to A$ distributiva rispetto alla somma, tale cioè che

- $a \cdot (b + c) = a \cdot b + a \cdot c$,
- $(a + b) \cdot c = a \cdot c + b \cdot c$,

per ogni scelta di $a, b, c \in A$. Un anello è *commutativo* se la moltiplicazione è commutativa, ed è *unitario* o *con unità* se A possiede un elemento neutro $1 \neq 0$ rispetto alla moltiplicazione.

Si vede facilmente che $0 \cdot a = a \cdot 0 = 0$ per ogni $a \in A$. Ad esempio, $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$, da cui si ottiene $0 = 0 \cdot a$ sommando ad entrambi i membri l'inverso di $0 \cdot a$ rispetto all'operazione di somma. Questo mostra che l'operazione di moltiplicazione non definisce mai una struttura di gruppo su un anello, perché l'elemento 0 non può possedere un inverso moltiplicativo. L'unità 1, se esiste, è unica. Infatti, se $1 \cdot a = a \cdot 1 = a = 1' \cdot a = a \cdot 1'$ per ogni $a \in A$, allora in particolare $1 = 1 \cdot 1' = 1'$.
Inoltre, se -1 indica l'inverso additivo di 1, si ha $1 + (-1) = 0$ e quindi $0 = 0 \cdot a = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a$. In modo simile si ottiene anche $(-1) \cdot a + a = 0$. In altre parole $(-1) \cdot a$ è l'inverso additivo di a, cioè: $-a = (-1) \cdot a$. In generale, gli anelli che saranno oggetto del nostro studio godranno di ulteriori proprietà:

Definizione 2.4. Un anello commutativo con unità è un *dominio d'integrità* se vale in esso la legge di annullamento del prodotto, cioè se $a \cdot b = 0$ è possibile solo quando almeno uno tra a e b è uguale a 0. Un anello con unità A si dice *corpo* se l'operazione di moltiplicazione definisce una struttura di gruppo sull'insieme $A \setminus \{0\}$, cioè se ogni elemento non nullo possiede un inverso moltiplicativo. Un corpo commutativo è detto *campo*.

Ogni campo è ovviamente un dominio d'integrità – mostratelo!

L'unica struttura algebrica che conosciamo finora – quella dei numeri naturali – non è un gruppo né un anello. Il nostro obiettivo è ora quello di costruire, a partire da $\mathbb{N}$, il più piccolo anello che lo contenga, estendendone le operazioni: l'anello $\mathbb{Z}$ dei numeri interi.

Esercizi.

(1) Una relazione d'ordine totale $\leq$ su un anello A definisce una struttura di *anello ordinato* se
- $a \leq b \iff a + c \leq b + c$,
- $a > 0, \quad b \leq c \Rightarrow ab \leq ac$,

per ogni $a, b, c \in A$. Mostrate che se $P = \{a \in A | a > 0\}$, allora A è unione disgiunta di P, $-P = \{-a | a \in P\}$ e $\{0\}$, e che $x, y \in P \Rightarrow x + y, xy \in P$. [$P$ è detto *cono positivo* dell'ordinamento $\leq$]

(2) Sia A un anello, e $P \subset A$ tale che A sia unione disgiunta di P, $-P$ e $\{0\}$. Supponiamo inoltre che se x e y sono elementi di P allora anche $x + y$ e xy giacciono in P. Mostrate che la relazione $\leq$ definita da $x \leq y \Leftrightarrow y - x \in P \cup \{0\}$ è una relazione d'ordine totale, che definisce una struttura di anello ordinato su A.

(3) Sia $(A, \leq)$ un anello ordinato con unità. Mostrate che $a^2 \geq 0$ per ogni $a \in A$, e in particolare che $1 > 0$.

(4) Sia $(A, \leq)$ un anello ordinato con unità. Mostrate che A non contiene elementi a tali che $a^2 = -1$.

(5) Sia $(A, \leq)$ un anello ordinato con unità, e $a \in A$ un elemento invertibile, tale cioè che esista un elemento $a^{-1} \in A$ con la proprietà che $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Mostrate che $a > 0 \Leftrightarrow a^{-1} > 0$.

(6) Sia F un *campo ordinato*, cioè un campo con una struttura di anello ordinato. Mostrate che se $x, y \in F$ soddisfano $x, y > 0$, allora $x < y \Leftrightarrow y^{-1} < x^{-1}$.

3. Costruzione dell'anello dei numeri interi

A lezione non ho costruito i numeri interi a partire dai numeri naturali. Abbiamo intenzione di presentare una costruzione molto simile più tardi nel corso: quella di campo delle frazioni di un dominio d'integrità. Per completezza di esposizione, vi riporto comunque la costruzione di $\mathbb{Z}$.

Nelle lezioni, ho dato per buone le principali proprietà algebriche di $\mathbb{Z}$, e cioè il fatto che sia un dominio d'integrità e possieda una struttura d'ordine compatibile con le operazioni. All'inizio del prossimo paragrafo riassumerò le proprietà di $\mathbb{Z}$ che verranno utilizzate in seguito.

3.1. **I numeri interi come classi di equivalenza.** Sull'insieme $\mathbb{N} \times \mathbb{N}$ consideriamo la relazione $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$.

Proposizione 3.1. *La relazione $\sim$ è di equivalenza.*

Dimostrazione. La relazione $\sim$ è riflessiva: $(a, b) \sim (a, b)$ dal momento che $a + b = b + a$.

E' anche simmetrica: $(a, b) \sim (c, d)$ se $a+d = b+c$, mentre $(c, d) \sim (a, b)$ se $c+b = d+a$; comunque $a+d = d+a$ e $b + c = c + b$.

La relazione è infine transitiva: se $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$, allora si ha $a + d = b + c, c + f = d + e$, da cui sommando membro a membro si ottiene $(a + d) + (c + f) = (b + c) + (d + e)$. Sfruttando la commutatività e l'associatività della somma, e cancellando $c+d$ da entrambi i membri, si ottiene $a+f = b+e$, cioè $(a, b) \sim (e, f)$. □

Definizione 3.2. L'insieme $\mathbb{Z}$ dei numeri interi è il quoziente $\mathbb{N} \times \mathbb{N} / \sim$.

L'idea intuitiva della definizione appena data è quella di dare alla coppia (a, b) il significato $a - b$. La relazione di equivalenza introdotta è quella che garantisce l'uguaglianza di tali differenze. L'interesse di $\mathbb{Z}$ sta nel fatto di poter definire operazioni analoghe a quelle di $\mathbb{N}$, ma che forniscano una struttura di anello.

3.2. **Buona definizione delle operazioni di somma e prodotto su $\mathbb{Z}$.**

Proposizione 3.3. *Le assegnazioni*

$$[(a, b)] + [(c, d)] = [(a + c, b + d)], \qquad [(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)]$$

danno operazioni ben definite sull'insieme $\mathbb{Z}$.

Dimostrazione. Stiamo definendo delle operazioni su un insieme quoziente: dobbiamo quindi sincerarci che siano *ben definite*, che non dipendano cioè dalla scelta dei rappresentanti delle classi di equivalenza. Questo è immediato per la somma: da $(a, b) \sim (a', b')$ e $(c, d) \sim (c', d')$ si ricava $a + b' = a' + b, c + d' = c' + d$. Sommando membro a membro si ottiene $a+c+b'+d' = a'+c'+b+d$, cioe $(a+c, b+d) \sim (a'+c', b'+d')$. La verifica per la moltiplicazione è invece più laboriosa, e la facciamo in due passi.

Sostituiamo prima $(a, b) \sim (a', b')$ e verifichiamo che $(ac + bd, ad + bc) \sim (a'c + b'd, a'd + b'c)$. Questo accade se $ac + bd + a'd + b'c = ad + bc + a'c + b'd$ cioè se $(a + b')c + (a' + b)d = (a' + b)c + (a + b')d$: questo segue facilmente da $a + b' = a' + b$. Se a questo punto sostituiamo (c, d) con l'elemento (c', d') appartenente alla stessa classe di $\sim$-equivalenza, verifichiamo alla stessa maniera che $(a'c+b'd, a'd+b'c) \sim (a'c' +b'd', a'd' +b'c')$ utilizzando il fatto che $c + d' = c' + d$. □

Proposizione 3.4. *Le operazioni di somma e moltiplicazione appena definite sono commutative ed associative, e la moltiplicazione è distributiva rispetto alla somma.*

Dimostrazione. La commutatività di entrambe le operazioni e l'associatività della somma sono di immediata e facile verifica. Per quanto riguarda l'associatività del prodotto abbiamo:

$$([(a, b)] \cdot [(c, d)]) \cdot [(e, f)] = [(ac + bd, ad + bc)] \cdot [(e, f)] = [((ac + bd)e + (ad + bc)f, (ac + bd)f + (ad + bc)e)],$$

mentre

$$[(a, b)] \cdot ([(c, d)] \cdot [(e, f)]) = [(a, b)] \cdot [(ce + df, cf + de)] = [(a(ce + df) + b(cf + de), a(cf + de) + b(ce + df))],$$

e si vede subito che i due risultati coincidono utilizzando le proprietà di commutatività, associatività e distributività delle due operazioni. La distributività si controlla alla stessa maniera. Ad esempio si ha:

$$[(a, b)] \cdot ([(c, d)] + [(e, f)]) = [(a, b)] \cdot [(c + e, d + f)] = [(a(c + e) + b(d + f), a(d + f) + b(c + e))]$$

mentre

$$[(a, b)] \cdot [(c, d)] + [(a, b)] \cdot [(e, f)] = [(ac + bd, ad + bc)] + [(ae + bf, af + be)] = [(ac + bd + ae + bf, ad + bc + af + be)],$$

che sono chiaramente uguali. □

3.3. **Proprietà delle operazioni di $\mathbb{Z}$.**

Lemma 3.5. *Gli elementi $[(0, 0)]$ e $[(1, 0)]$ sono gli elementi neutri rispetto alla somma e al prodotto di $\mathbb{Z}$ rispettivamente.*

Dimostrazione. Si vede facilmente che

$$[(0, 0)] + [(a, b)] = [(a, b)] = [(a, b)] + [(0, 0)],$$

e che

$$[(1, 0)] \cdot [(a, b)] = [(1 \cdot a + 0 \cdot b, 1 \cdot b + 0 \cdot a)] = [(a, b)] = [(a \cdot 1 + b \cdot 0, a \cdot 0 + b \cdot 1)] = [(a, b)] \cdot [(1, 0)].$$

□

Lemma 3.6. *Comunque si scelgano $a, b \in \mathbb{N}$, l'elemento $[(b, a)]$ è inverso di $[(a, b)]$ rispetto all'operazione di somma.*

Dimostrazione. Si ha: $[(a, b)] + [(b, a)] = [(a + b, a + b)]$, e si vede subito che $(a + b, a + b) \sim (0, 0)$. □

Teorema 3.7. *$(\mathbb{Z}, +, \cdot)$ è un anello commutativo con unità.*

Dimostrazione. Abbiamo verificato che $+$ è un'operazione commutativa ed associativa dotata di elemento neutro $[(0,0)]$ rispetto alla quale ogni elemento possiede un inverso, pertanto $(\mathbb{Z}, +)$ è un gruppo abeliano.

Inoltre l'operazione di moltiplicazione $\cdot$ è commutativa ed associativa, distribuisce rispetto alla somma e possiede l'elemento neutro $[(1,0)]$. □

Nell'uso comune di $\mathbb{Z}$ utilizzeremo una notazione diversa da quella finora sfruttata per indicare le classi di equivalenza: abbiamo già visto come $[(a,a)] = [(0,0)]$ sia l'elemento neutro rispetto alla somma. Se $a \neq b$, allora esattamente una tra $a < b$ e $b < a$ sarà valida. Nel primo caso $(a,b) \sim (0, b-a)$, mentre nel secondo $(a,b) \sim (a-b, 0)$. Pertanto oltre a $[(0,0)]$, gli elementi di $\mathbb{Z}$ sono solo del tipo $[(a,0)]$ oppure $[(0,a)]$, con $a > 0$.

Lemma 3.8. *Si hanno $(a,0) \sim (b,0)$ e $(0,a) \sim (0,b)$ se e solo se $a = b$. Inoltre $(a,0) \sim (0,b)$ se e solo se $a = b = 0$.*

Dimostrazione. Immediata. □

Possiamo quindi concludere che gli elementi $[(0,0)]$ e $[(a,0)], [(0,a)], a \neq 0$ sono tutti distinti in $\mathbb{Z}$, e che ogni elemento di $\mathbb{Z}$ è di tale tipo. La notazione che utilizzeremo[2] per tali elementi è: $\mathbf{0} = [(0,0)], \boldsymbol{a} = [(a,0)], \boldsymbol{-a} = [(0,a)]$. Il numero naturale a è detto *valore assoluto* sia dell'elemento $[(a,0)]$ che dell'elemento $[(0,a)]$. Il valore assoluto di $x \in \mathbb{Z}$ si indica con $|x|$. In altre parole $|\boldsymbol{a}| = |\boldsymbol{-a}| = a$, se $a \in \mathbb{N}$.

Proposizione 3.9. ***0*** *e* ***1*** *sono gli elementi neutri rispetto alla somma e al prodotto di $\mathbb{Z}$. Inoltre se $a, b \in \mathbb{N}$, si ha:*

- *Se $c = a + b$, allora $\boldsymbol{a} + \boldsymbol{b} = \boldsymbol{c}$, $\quad \boldsymbol{-a} + \boldsymbol{-b} = \boldsymbol{-c}$.*
- *Se $a \geq b$ e $c = a - b$, allora $\boldsymbol{a} + \boldsymbol{-b} = \boldsymbol{c}$.*
- *Se $a < b$ e $c = b - a$, allora $\boldsymbol{a} + \boldsymbol{-b} = \boldsymbol{-c}$.*
- *Se $c = ab$, allora $\boldsymbol{a} \cdot \boldsymbol{b} = \boldsymbol{c}$, $\quad \boldsymbol{a} \cdot \boldsymbol{-b} = \boldsymbol{-c}$, $\quad \boldsymbol{-a} \cdot \boldsymbol{-b} = \boldsymbol{c}$.*

In altre parole, gli elementi di $\mathbb{Z}$ si sommano e si moltiplicano come già sapete. Da questo momento in poi possiamo quindi evitare di indicarli in grassetto, e scriverli normalmente.

E' importante osservare come gli elementi $\boldsymbol{a}$, con $a \in \mathbb{N}$, si sommino e si moltiplichino esattamente come i corrispondenti elementi di $\mathbb{N}$, e questo evita confusione nel momento di rimuovere il grassetto. Possiamo considerare $\mathbb{Z}$ come un'*ampliamento* dell'insieme dei numeri naturali con una struttura di anello.

Corollario 3.10. *Siano $x, y \in \mathbb{Z}$. Se $xy = 0$, allora $x = 0$ oppure $y = 0$.*

Dimostrazione. Segue da (1.6), sfruttando le regole di moltiplicazione della proposizione precedente. □

Possiamo finalmente concludere:

Teorema 3.11. *L'anello $(\mathbb{Z}, +, \cdot)$ è un dominio di integrità.*

3.4. **Struttura d'ordine su $\mathbb{Z}$.** Una delle strutture intrinseche dell'insieme dei numeri naturali era data dalla relazione d'ordine. Si può estendere anch'essa all'anello $\mathbb{Z}$.

Definizione 3.12. $[(a,b)] \preceq [(c,d)] \Leftrightarrow a + d \leq b + c$

Notate che, per il momento, siamo costretti a usare la notazione nuova $\preceq$ per non confondere questa relazione su $\mathbb{Z}$ con la relazione d'ordine $\leq$ che già abbiamo su $\mathbb{N}$.

Proposizione 3.13. *$\preceq$ è una relazione d'ordine totale su $\mathbb{Z}$.*

Dimostrazione. La relazione $\preceq$ è riflessiva: in effetti $a+b \leq b+a$. E' inoltre antisimmetrica: da $[(a,b)] \preceq [(c,d)]$, $[(c,d)] \preceq [(a,b)]$ seguono $a + d \leq b + c$ e $b + c \leq a + d$. Ma allora per antisimmetria di $\leq$ su $\mathbb{N}$ si ottiene $a + d = b + c$, cioè $[(a,b)] = [(c,d)]$.

Infine, è transitiva: da $a+d \preceq b+c$ e $c+f \preceq d+e$ si ottiene, sommando membro a membro, $a+d+c+f \leq b+c+d+e$, da cui cancellando $c+d$ si ha $a+f \leq b+e$, cioè $[(a,b)] \preceq [(e,f)]$. Tale relazione d'ordine è totale, in quanto è definita per mezzo della relazione di ordine $\leq$ che è totale. □

Proposizione 3.14. *Siano a, b elementi di $\mathbb{N}$. Allora:*

- *$a \preceq b$ se e solo se $a \leq b$,*
- *$-a \preceq b$ per ogni scelta di a, b,*
- *$-a \preceq -b$ se e solo se $b \leq a$.*

Vediamo quindi che la relazione $\preceq$ coincide con $\leq$ sulla porzione di $\mathbb{Z}$ che abbiamo identificato con $\mathbb{N}$. Da questo momento in poi possiamo quindi rimuovere la doppia notazione, e interpretare la relazione $\leq$ su $\mathbb{Z}$ come un estensione della relazione d'ordine già definita su $\mathbb{N}$.

Osservazione 3.15. La relazione $\leq$ è di ordine totale su $\mathbb{Z}$, ma non è un buon ordinamento: infatti $\mathbb{Z}$ non ammette elemento minimo.

Esercizi.

[2]Stiamo sottolineando gli elementi per distinguerli dai corrispondenti elementi di $\mathbb{N}$, ma in generale eviteremo questo segno grafico, quando non ci siano rischi di confusione.

(1) Sia $X \subset \mathbb{Z}$ un sottoinsieme non vuoto *limitato dal basso*, che possiede cioè un elemento $n \in \mathbb{Z}$ tale che $n \leq x$ per ogni $x \in X$. Mostrate che X possiede un elemento minimo. *[Sugg.: osservate che un traslato di X è completamente contenuto in $\mathbb{N}$]*
(2) Mostrate che se $a, b \in \mathbb{Z}$ soddisfano $ab = 1$, allora $a = b = 1$ oppure $a = b = -1$. In altre parole, i soli due elementi invertibili di $\mathbb{Z}$ sono ± 1.
(3) Mostrate che $\leq$ definisce una struttura di anello ordinato su $\mathbb{Z}$.
(4) Sia $\preccurlyeq$ una relazione d'ordine che definisca una struttura di anello ordinato su $\mathbb{Z}$. Mostrare che $0 \leq a \Rightarrow 0 \preccurlyeq a$. Concludere che le relazioni $\preccurlyeq$ e $\leq$ coincidono, cioè che $\mathbb{Z}$ possiede un'unica struttura di anello ordinato.

4. Divisione euclidea e teorema fondamentale dell'aritmetica

4.1. **Divisione euclidea in $\mathbb{N}$ e in $\mathbb{Z}$.** Ricapitoliamo: $\mathbb{Z}$ è un dominio d'integrità dotato di una struttura di anello ordinato. I suoi elementi positivi[3] sono chiusi rispetto alle operazioni e costituiscono una copia dell'insieme dei numeri naturali. Gli unici elementi invertibili di $\mathbb{Z}$ sono 1 e -1.

Una struttura importante dell'anello dei numeri interi è l'esistenza della cosiddetta *divisione euclidea*. La dimostriamo prima per i numeri naturali, ed immediatamente dopo per tutti i numeri interi.

Proposizione 4.1. *Siano $a, b \in \mathbb{N}, b \neq 0$. Allora esistono $q, r \in \mathbb{N}$ tali che $a = qb + r$, con $0 \leq r < b$.*

Dimostrazione. Sia $X = \{n \in \mathbb{N} \,|\, nb > a\}$. L'insieme X contiene $a + 1$ ed è pertanto non vuoto: in effetti, $b \neq 0$ e quindi $b \geq 1$ e di conseguenza $ab \geq a$; ma allora $(a + 1)b = ab + b \geq a + b > a$. Osserviamo che 0 non appartiene all'insieme X, in quanto $0 \cdot b = 0$ non è maggiore di a.

Per la proprietà di buon ordinamento dei numeri naturali, X possiede un elemento minimo (diverso da 0) che possiamo indicare con $q + 1$. In altre parole, $q \notin X, q + 1 \in X$. Questo significa che $(q + 1)b > a$, ma $qb \not> a$, cioè $qb \leq a$; riassumendo: $qb \leq a < (q + 1)b = qb + b$.

Sottraendo da tutti e tre i membri la quantità qb si ottiene $0 \leq a - qb < b$. Se poniamo $r = a - qb$, abbiamo $a = qb + r$, con $0 \leq r < b$. □

Teorema 4.2. *Siano $a, b \in \mathbb{Z}, b \neq 0$. Allora esistono $q, r \in \mathbb{Z}$ tali che $a = qb + r, 0 \leq r < |b|$.*

Dimostrazione. Intanto, è sufficiente dimostrare l'enunciato quando $b > 0$. In effetti, se $a = qb + r$, allora chiaramente $a = (-q)(-b) + r$.

Se anche $a \geq 0$, basta invocare la proposizione precedente. Se invece $a < 0$, allora $-a > 0$ e quindi $-a = qb + r$, da cui $a = -qb - r = (-q)b - r$. Se $r = 0$, abbiamo concluso. Se invece $0 < r < b$, allora $-qb - r = -qb - b + b - r = (-q - 1)b + (b - r)$ e $r' = b - r$ soddisfa $0 < r' < b$. □

Osservazione 4.3. Gli elementi q, r che compaiono nell'enunciato del teorema precedente sono univocamente determinati da a e b, anche se non avremo mai bisogno di tale fatto.

4.2. **Divisibilità e massimo comun divisore.**

Definizione 4.4. Siano $a, b \in \mathbb{Z}$. Si dice che *a divide b*, e si scrive $a|b$, quando esiste $q \in \mathbb{Z}$ tale che $b = aq$.

Se $a|b$, si dice equivalentemente che *b è un multiplo di a*. La relazione di divisibilità gode di alcune ovvie proprietà.

Proposizione 4.5. *Valgono le seguenti proprietà:*

(1) *$a|a$ per ogni $a \in \mathbb{Z}$;* *(riflessività)*
(2) *se $a|b$ e $b|c$, allora $a|c$;* *(transitività)*
(3) *se $a|b$ allora $a|bc$ per ogni $c \in \mathbb{Z}$;*
(4) *se $a|b$ e $a|c$, allora $a|b \pm c$;*
(5) *se $a|b$ e $b|a$, allora $a = \pm b$;* *(anti-simmetria a meno del segno)*
(6) *$a|0$ per ogni $a \in \mathbb{Z}$;*
(7) $0|a \Rightarrow a = 0$;
(8) *$1|a$ per ogni $a \in \mathbb{Z}$;*
(9) *$a|1$ se e solo se a è invertibile in $\mathbb{Z}$, cioè $a = \pm 1$.*

Dimostrazione. Tutte le dimostrazioni sono molto semplici. Un cenno per ognuna: (1) $a = 1 \cdot a$; (2) $b = qa, c = rb \Rightarrow c = (qr)a$; (3) è una riformulazione di (2); (4) $b = qa, c = ra \Rightarrow b \pm c = (q \pm r)a$; (5) $b = qa, a = rb \Rightarrow a = (qr)a$. Se $a = 0$, allora anche $b = 0$. Se $a \neq 0$, allora $qr = 1$; (6) $0 = 0 \cdot a$; (7) $q \cdot 0 = 0$; (8) $a = a \cdot 1$; (9) $a|1$ se e solo se esiste $x \in \mathbb{Z}$ tale che $ax = 1$. □

Osservazione 4.6. Una conseguenza immediata della proposizione precedente è che se d divide sia a che b, divide allora ogni numero intero della forma $ha + kb, h, k \in \mathbb{Z}$. Un altro aspetto da sottolineare è che la relazione di divisibilità, sul sottoinsieme $\mathbb{N}$, è riflessiva, antisimmetrica e transitiva, ed è quindi una relazione d'ordine.

Una delle proprietà algebriche fondamentali dell'anello dei numeri interi è l'esistenza del massimo comun divisore. In generale si è soliti definire massimo comun divisore di due interi il più grande divisore comune. Questo ha lo svantaggio di non permettere la definizione del massimo comun divisore di 0 e 0. In effetti, tutti gli interi dividono 0, e non esiste un massimo elemento di $\mathbb{Z}$. La definizione che segue ha il vantaggio di fornire un massimo comun divisore (uguale a 0) anche per la coppia $(0, 0)$, e di descrivere una proprietà non immediata dei divisori comuni di due interi dati. Ha purtroppo la fastidiosa controindicazione di non garantire l'esistenza[4], e nemmeno l'unicità —

[3] Cioè ≥ 0.
[4] Per il momento...

che andranno entrambe verificate in seguito — del massimo comun divisore.

Definizione 4.7. Siano $a, b \in \mathbb{Z}$. Un elemento $d \in \mathbb{Z}$ si dice *massimo comun divisore* di a e b se $d|a, d|b$ ed ogni elemento $e \in \mathbb{Z}$ che soddisfi $e|a, e|b$, soddisfa anche $e|d$.

Osservazione 4.8. Se d e d' sono entrambi massimi comuni divisori di a e b, allora vale sia $d|d'$ che $d'|d$. Abbiamo visto come questo accada soltanto quando $d = \pm d'$, e si vede chiaramente che se d è un massimo comun divisore di a e b, anche $-d$ lo è. Pertanto il massimo comun divisore in $\mathbb{Z}$ è unico a meno del segno. Se d è un massimo comun divisore di a e b, scriveremo impropriamente $\mathrm{MCD}(a, b) = d$.

Ad esempio, $\mathrm{MCD}(26, -39) = 13$ significherà che esistono massimi comuni divisori di 26 e -39, e che 13 è uno di essi: in particolare, che ± 13 sono gli unici massimi comuni divisori di 26 e -39. Per pulizia di notazione, quando avremo bisogno di indicare il massimo comun divisore di due numeri, utilizzeremo sempre il valore non negativo tra i due disponibili.Dalla definizione segue immediatamente che $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, a)$[5] per ogni scelta di $a, b \in \mathbb{Z}$.

Potreste trovare altrove la notazione più compatta (a, b) al posto di $\mathrm{MCD}(a, b)$, che troverà una giustificazione una volta che avremo introdotto il concetto di ideali in un anello.

Lemma 4.9. *Il massimo comun divisore soddisfa le seguenti proprietà:*

(1) $\mathrm{MCD}(0, 0) = 0$;
(2) $\mathrm{MCD}(a, 0) = a$ *per ogni* $a \in \mathbb{Z}$;
(3) *siano* $a, b, q, r \in \mathbb{Z}$ *tali che* $a = bq + r$. *Allora, se esiste* $\mathrm{MCD}(b, r)$, *esiste anche* $\mathrm{MCD}(a, b)$, *e si ha* $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, r)$.

Dimostrazione. (1) ovvio, poiché ogni intero divide 0, e 0 è l'unico intero con la proprietà di essere diviso da tutti gli altri.
(2) i divisori comuni di a e 0 sono esattamente quelli di a. Tra tali elementi, $\pm a$ sono quelli con la proprietà di essere divisi da tutti gli altri. (3) Se d divide sia a che b, allora divide anche qb, ed anche $a - qb = r$, quindi ogni divisore comuni di a e b è anche un divisore comune di b ed r. Viceversa, se d divide sia b che r, allora divide anche qb e la somma $qb + r = a$. Pertanto ogni divisore comune di b ed r è anche un divisore comune di a e b. Questo mostra che se tra i divisori comuni di b ed r esiste un elemento che è diviso da tutti gli altri, lo stesso è vero per a e b, e tale elemento è lo stesso (a meno del segno). □

Il lemma appena dimostrato suggerisce una possibile strategia per trovare il massimo comun divisore di due numeri interi a, b. Eseguire la divisione euclidea $a = bq + r$ e sostituire la coppia (a, b) con quella (b, r). Questo ha il vantaggio di rendere il secondo elemento della nuova coppia più piccolo (in valore assoluto) del secondo nella coppia precedente: infatti $0 \leq r < |b|$. Reiterando questa procedura al più $|b|$ passi, otterremo una coppia del tipo $(n, 0)$ che possiede certamente un massimo comun divisore, la cui determinazione è immediata — è uguale ad n.

Ad esempio, per individuare il massimo comun divisore di 1001 e 273 si può effettuare la divisione euclidea tra 1001 e 273, ottenendo

$$1001 = 3 \cdot 273 + 182 \Rightarrow \mathrm{MCD}(1001, 273) = \mathrm{MCD}(273, 182).$$

Possiamo quindi continuare:

$$273 = 1 \cdot 182 + 91, \qquad 182 = 2 \cdot 91 + 0,$$

per ottenere $\mathrm{MCD}(1001, 273) = \mathrm{MCD}(273, 182) = \mathrm{MCD}(182, 91) = \mathrm{MCD}(91, 0) = 91$. In effetti, $1001 = 7 \cdot 11 \cdot 13$, mentre $273 = 3 \cdot 7 \cdot 13$, per cui il loro massimo comun divisore[6] è $7 \cdot 13 = 91$.

Questa procedura può essere percorsa alla rovescia per ottenere la cosiddetta *identità di Bézout*, che esprime il massimo comun divisore di due numeri come somma di loro multipli: vediamo come.
Sappiamo che $(1001, 273) = 91$. In effetti, da $273 = 1 \cdot 182 + 91$ segue $91 = 1 \cdot 273 - 1 \cdot 182$. La divisione euclidea precedente $1001 = 3 \cdot 273 + 182$ permette di ricavare $182 = 1 \cdot 1001 - 3 \cdot 273$. Sostituendo, si ottiene

$$91 = 1 \cdot 273 - 1 \cdot 182 = 1 \cdot 273 - 1 \cdot (1 \cdot 1001 - 3 \cdot 273) = -1 \cdot 1001 + 4 \cdot 273.$$

Teorema 4.10. $\mathrm{MCD}(a, b)$ *esiste per ogni scelta di* $a, b \in \mathbb{Z}$. *Inoltre, se* $d = \mathrm{MCD}(a, b)$, *allora esistono* $h, k \in \mathbb{Z}$ *tali che* $d = ha + kb$.

Dimostrazione. L'esistenza di $\mathrm{MCD}(a, b)$ si dimostra per induzione (forte) su $|b|$.
La base dell'induzione è chiara, in quanto se $|b| = 0$, allora $b = 0$, e sappiamo che $\mathrm{MCD}(a, 0)$ esiste ed è uguale ad a. Il passo induttivo è stato descritto sopra: se $b \neq 0$, la divisione euclidea ci garantisce l'esistenza di $q, r \in \mathbb{Z}$ tali che $a = qb + r, 0 \leq r < |b|$. Per ipotesi induttiva, esiste $\mathrm{MCD}(b, r)$; ma per il lemma precedente, esiste allora anche $\mathrm{MCD}(a, b)$ e coincide con $\mathrm{MCD}(b, r)$.

Per quanto riguarda l'identità di Bézout, fornisco varie dimostrazioni diverse, tutte istruttive. La prima, anche se non sembra, è quella data a lezione risalendo l'algoritmo euclideo e potete limitarvi a leggere quella.

- Per induzione su $|b|$. Se $|b| = 0$, non c'è nulla da dimostrare: $\mathrm{MCD}(a, 0) = a$, ed effettivamente $a = 1 \cdot a + 0 \cdot b$. Il passo induttivo è facile: se $b \neq 0$ possiamo trovare $q, r \in \mathbb{Z}$ tali che $a = qb + r, 0 \leq r < |b|$. Ma allora $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, r)$. Per ipotesi induttiva, se $d = \mathrm{MCD}(b, r)$, possiamo trovare $h, k \in \mathbb{Z}$ tali che $d = hb + kr$. Sostituendo $r = a - qb$ si ottiene $d = hb + k(a - qb) = ka + (h - qk)b$.

[5] Cioè che ogni massimo comun divisore di a e b è anche un massimo comun divisore di b e a.
[6] Calcolato con l'usuale procedimento di fattorizzazione, che presume la fattorizzazione unica, che non abbiamo però ancora dimostrato.

- Consideriamo l'insieme $X = \{ha + kb \,|\, h, k \in \mathbb{Z}\}$. X contiene $a = 1 \cdot a + 0 \cdot b$ e $b = 0 \cdot a + 1 \cdot b$, nonché $0 = 0 \cdot a + 0 \cdot b$. Inoltre soddisfa: $x \in X \Rightarrow -x \in X; x, y \in X \Rightarrow x + y \in X; x \in X, h \in \mathbb{Z} \Rightarrow hx \in \mathbb{Z}$. Con un linguaggio che sarà introdotto solo in seguito, X è un *ideale* dell'anello $\mathbb{Z}$. Basta ora osservare che eseguendo la divisione euclidea su due elementi x, y di X, anche il resto appartiene ad X: se $x = qy + r$, allora $r = x + (-q)y$; da $y \in X$ segue $(-q)y \in X$, e poiché anche $x \in X$, allora $r = x + (-q)y \in X$. Reiterando le divisione euclidee a partire da $a, b \in X$, tutti i resti che si ottengono appartengono ad X, e quindi anche l'ultimo resto non nullo, che è il massimo comun divisore di a e b.
- Possiamo supporre, senza perdere di generalità, che a e b non siano entrambi nulli. Come sopra, si dimostra che X è un ideale di $\mathbb{Z}$. Se d è il suo minimo elemento positivo — che esiste per buon ordinamento — allora ogni altro elemento di X è multiplo di d. Infatti, eseguendo la divisione euclidea tra $x \in X$ e d si ottiene $x = qd + r$, con $0 \leq r < d$, ed $r \in X$ come abbiamo già mostrato sopra. Se $r \neq 0$, si ottiene un assurdo, quindi $r = 0$ e d divide ogni elemento di X.
  Tra gli elementi di X ci sono anche a e b, quindi d è un divisore comune di a e b. Inoltre, d è automaticamente della forma $ha + kb$, quindi se e divide sia a che b, deve dividere anche $ha + kb = d$. In altre parole, d è un massimo comun divisore di a e b.

□

Quest'ultima dimostrazione utilizza un fatto che ha la sua indipendente utilità.

Proposizione 4.11. *Se d è un divisore di a e b della forma $d = ha + kb$, con $h, k \in \mathbb{Z}$, allora $d = \mathrm{MCD}(a, b)$.*

Dimostrazione. Se e è un divisore comune di a e b, deve dividere anche ha, kb e la loro somma $d = ha + kb$. □

Corollario 4.12. *Siano $a, b \in \mathbb{Z}$:*

(1) *se è possibile esprimere 1 nella forma $ha + kb$ con $h, k \in \mathbb{Z}$, allora $\mathrm{MCD}(a, b) = 1$;*
(2) *$\mathrm{MCD}(ab, ac) = a \cdot \mathrm{MCD}(b, c)$;*
(3) *se $d = \mathrm{MCD}(a, b)$, allora $\mathrm{MCD}(a/d, b/d) = 1$.*

Dimostrazione. (1) segue direttamente dalla proposizione precedente.
(2): se $d = \mathrm{MCD}(b, c)$, allora $d = hb + kc$; ma allora $ad = h \cdot ab + k \cdot ac$. Inoltre, se d divide sia b che c, ad divide chiaramente sia ab che ac. A questo punto basta applicare la proposizione precedente.
(3) è una riformulazione di (2). □

Quando $\mathrm{MCD}(a, b) = 1$, gli interi a e b si dicono *primi tra loro* o *relativamente primi* o *coprimi*. L'ultima delle affermazioni sostiene che dividendo due numeri per il loro massimo comun divisore si ottengono due quozienti primi tra loro.

4.3. **Elementi invertibili, primi e irriducibili in $\mathbb{N}$ e in $\mathbb{Z}$.** Per poter enunciare e dimostrare il teorema di fattorizzazione unica, abbiamo bisogno di un po' di terminologia.

Definizione 4.13.
- $a \in \mathbb{Z}$ si dice *invertibile* se $a|1$;
- $0 \neq p \in \mathbb{Z}$ non invertibile si dice *primo* se, ogni volta che $p|ab$, allora p divide almeno uno tra a e b;
- $0 \neq p \in \mathbb{Z}$ non invertibile si dice *irriducibile* se quando $p = ab$, allora uno tra a e b è invertibile.

Osservazioni 4.14.

(1) Abbiamo già visto come l'unico elemento invertibile di $\mathbb{N}$ sia 1, e vi siano esattamente due invertibili in $\mathbb{Z}$: ± 1.
(2) Se $p = ab$ è irriducibile, allora esattamente uno tra a e b è invertibile. Se fossero entrambi invertibili, infatti, anche il loro prodotto sarebbe invertibile, e questo è escluso dalla definizione.
(3) Se p è irriducibile e x è invertibile, allora anche px è irriducibile. In effetti, se $px = ab$, allora $p = abx^{-1} = a(bx^{-1})$. Quindi a è invertibile, oppure bx^{-1} è invertibile, e di conseguenza $b = (bx^{-1})x$ è invertibile perché prodotto di invertibili.
(4) Se $p \in \mathbb{Z}$ non è invertibile, $q \in \mathbb{Z}$ è irriducibile, e $p|q$, allora $q = px$. Di conseguenza, x è invertibile e $p = qx^{-1}$ è anch'esso irriducibile. In particolare, se p, q sono entrambi irriducibili, e $p|q$, allora $p = \pm q$.
(5) Se $p \in \mathbb{Z}$ è irriducibile, gli unici divisori di p sono $\pm 1, \pm p$ e sono tutti e quattro distinti. Se $p \in \mathbb{N}$ è irriducibile, gli unici divisori naturali di p sono 1 e p, e sono distinti[7].

Mi aspetto che vi sia sempre stato detto che un numero naturale p è primo se i suoi unici divisori naturali sono 1 e p. Questa è la definizione che diamo — dopo aver richiesto che p non sia invertibile — per gli interi *irriducibili*, non per quelli primi. In realtà i concetti di elemento primo ed irriducibile coincidono in $\mathbb{Z}$, e quindi anche in $\mathbb{N}$. Dimostrare questo fatto è il nostro prossimo obiettivo.

Lemma 4.15. *Se $a, b, c \in \mathbb{Z}$ soddisfano $a|bc$ e $\mathrm{MCD}(a, b) = 1$, allora $a|c$.*

Dimostrazione. Se $\mathrm{MCD}(a, b) = 1$, per l'identità di Bézout abbiamo $1 = ha + kb$ per un'opportuna scelta di $h, k \in \mathbb{Z}$. Ma allora $c = 1 \cdot c = hac + kbc$. Sia hac che kbc sono chiaramente multipli di a — il primo lo è esplicitamente, il secondo in quanto multiplo di bc — e quindi anche la loro somma è divisa da a. □

Osservazione 4.16. Senza l'ipotesi $\mathrm{MCD}(a, b) = 1$, l'enunciato è evidentemente falso. Ad esempio, $4|2 \cdot 6$, ma nè 2, né 6 sono multipli di 4.

[7] In altre parole, un naturale è primo quando ha **esattamente** due divisori naturali.

Proposizione 4.17. *Un elemento $p \in \mathbb{Z}$ è primo se e solo se è irriducibile.*

Dimostrazione. Se p è invertibile o uguale a 0, non è né primo, né irriducibile, quindi possiamo limitarci al caso di elementi non invertibili diversi da 0.
p primo $\Rightarrow$ p irriducibile: se $p = ab$, allora p divide ab. Essendo p primo, possiamo supporre (a meno di scambiare a con b) che p divida a. Allora $a = px$ e $p = ab = pbx$. Ma allora $bx = 1$, e quindi b è invertibile. Quindi le uniche fattorizzazioni di p hanno un fattore invertibile, e p è irriducibile.
p irriducibile $\Rightarrow$ p primo: se $p|ab$, dobbiamo dimostrare che p divide a oppure b. Il massimo comun divisore $\mathrm{MCD}(a, p)$ è un divisore di p. Essendo p irriducibile, il quinto punto delle Osservazioni 4.14 ci illustra che le sole due possibilità sono $\mathrm{MCD}(a, p) = p$ oppure $\mathrm{MCD}(a, p) = 1$. Se $\mathrm{MCD}(a, p) = p$, allora $p|a$; se invece $\mathrm{MCD}(a, p) = 1$, applicando il Lemma 4.15 si ottiene $p|b$. In conclusione, p è primo. □

Gli elementi primi di $\mathbb{N}$ sono detti anche *numeri primi*.

4.4. **Fattorizzazione unica in $\mathbb{N}$ e in $\mathbb{Z}$.** E' più semplice enunciare, e dimostrare, il teorema di fattorizzazione unica in $\mathbb{N}$ che in $\mathbb{Z}$. Il teorema di fattorizzazione unica in $\mathbb{N}$, meglio noto come *Teorema fondamentale dell'aritmetica* sostiene che ogni numero naturale (diverso da zero) si scrive in modo unico come prodotto di numeri primi. L'unicità della fattorizzazione consiste nel fatto che in due fattorizzazioni dello stesso numero compaiono gli stessi numeri primi, e ciascuno di essi compare lo stesso numero di volte.

L'enunciato si compone di due affermazioni: una sull'esistenza della fattorizzazione e l'altra sulla sua unicità, che si dimostra separatamente.

Teorema 4.18. *Ogni $0 \neq N \in \mathbb{N}$ può essere espresso come prodotto di numeri primi.*

Dimostrazione. Per induzione (forte) su N.
La base dell'induzione $N = 1$ è banale, in quanto 1 è prodotto di zero numeri primi — è il prodotto vuoto! Per quanto riguarda il passo induttivo, sia $N > 1$. Se N è primo, allora costituisce la propria fattorizzazione nel prodotto di un solo primo. Se invece N non è primo, allora non è irriducibile, e quindi $N = ab$, con a, b entrambi diversi da 1. Di conseguenza, $a, b < N$. Ma allora, per ipotesi induttiva, sia a che b sono prodotto di numeri primi. Moltiplicando tali espressioni tra loro, si esprime N come prodotto di numeri primi. □

Passiamo ora all'unicità

Teorema 4.19. *Se $0 \neq N \in \mathbb{N}$ ammette le due fattorizzazioni*

$$\begin{aligned} N &= p_1 p_2 \dots p_r \\ &= q_1 q_2 \dots q_s, \end{aligned}$$

dove tutti i p_i e tutti i q_j sono primi, allora $r = s$ e, a meno di riordinare i q_i, si ha $p_i = q_i$ per ogni $i = 1, \dots, r$.

Dimostrazione. Per induzione su N. Se $N = 1$ non c'è nulla da dimostrare, in quanto ogni divisore di 1 è invertibile, e quindi nessun primo può dividere 1. L'unica fattorizzazione in primi di 1 è quella vuota.
Sia ora $N > 1$. E' evidente che $p_1|N$. Poiché $N = q_1 \dots q_s$ e p_1 è primo, allora p_1 deve dividere almeno uno dei fattori q_i, che possiamo supporre essere q_1 a meno di riordinare i primi della seconda fattorizzazione. Se $p_1|q_1$, allora $p_1 = q_1$, poiché sono entrambi irriducibili. Dividendo per p_1 si ottiene allora

$$\begin{aligned} N/p_1 &= p_2 \dots p_r \\ &= q_2 \dots q_s, \end{aligned}$$

con $N/p_1 < N$. Dall'ipotesi induttiva si ha allora $r - 1 = s - 1$, e quindi $r = s$; inoltre, a meno di riordinare i primi della seconda fattorizzazione, $p_i = q_i$ per $i = 2, \dots, r$. □

Teorema 4.20. *Ogni $0 \neq N \in \mathbb{Z}$ si scrive come prodotto di un invertibile e di elementi primi di $\mathbb{Z}$. Tale fattorizzazione in primi è unica nel senso che comunque prese due fattorizzazioni di N, i primi che compaiono nella prima sono tutti e soli — a meno del segno — quelli che compaiono nella seconda; inoltre il numero di volte che i primi $\pm p$ compaiono (in totale) in una delle fattorizzazioni è uguale al numero di volte che compaiono nell'altra.*

Dimostrazione. A meno di sostituire ogni primo nella fattorizzazione di N col suo valore assoluto, il problema si riduce alla fattorizzazione unica di $|N|$ in $\mathbb{N}$. □

Esercizi.

(1) Calcolare con l'algoritmo euclideo il massimo comun divisore tra 233 e 144, e ricavare la corrispondente identità di Bézout.
(2) Stimare in funzione di a e b il numero di divisioni euclidee necessarie a calcolare il massimo comun divisore tra a e b.
(3) Mostrare che il minimo comune multiplo di $a, b \in \mathbb{N}$ è uguale ad $ab/(a, b)$.

5. APPLICAZIONI

5.1. **La divisibilità si controlla con la fattorizzazione.** Innanzitutto, prendiamo la decisione di utilizzare solamente elementi primi *positivi*, in modo da evitare le ridondanze di segno che avremmo altrimenti. In generale, è comodo raggruppare i primi che compaiono più di una volta in una fattorizzazione per sostituirli con una potenza. In questo modo, invece di $72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$, scriveremo $72 = 2^3 \cdot 3^2$. In generale, avremo

$$N = p_1^{n_1} \dots p_k^{n_k},$$

dove i p_i sono primi distinti e gli esponenti n_i sono tutti ≥ 1.

Se a, b sono interi non nulli tali che $a|b$, da $b = ax$ segue che ogni primo che compare nella fattorizzazione di a deve anche comparire nella fattorizzazione di b, e il numero di volte che appare in b deve essere almeno quello con cui appare nella fattorizzazione di a. In effetti, la fattorizzazione in primi di b si ottiene da quelle di a e x moltiplicandole.

E' vero anche il viceversa: se ogni primo che compare nella fattorizzazione di a compare anche in quella di b, con molteplicità maggiore o uguale, allora il rapporto b/a è ancora un intero, nella cui fattorizzazione ogni primo di b compare con esponente pari alla differenza tra quello di b e quello di a (o non compare se gli esponenti coincidono). Questo mostra che la conoscenza delle fattorizzazioni di a e b permette di verificare immediatamente se a divida b.

5.2. **Il** MCD **si calcola attraverso la fattorizzazione.** Per quanto detto nel punto precedente, se a, b, d sono non nulli e d divide sia a che b, allora nella fattorizzazione di d possono comparire solamente primi che compaiono sia nella fattorizzazione di a che in quella di b, e con molteplicità che non superi la molteplicità con cui compare in a e in b.

Tra tutti questi divisori, si ottiene il MCD scegliendo, come esponente di ciscun primo, il più grande intero possibile che non superi né l'esponente in a, né quello in b. Questo esponente è il minimo tra i due esponenti, e ritroviamo la tecnica ben nota per il calcolo di $\mathrm{MCD}(a, b)$ una volta note le fattorizzazione di a e b in primi.

5.3. **Il minimo comune multiplo.** Per il minimo comune multiplo di a, b vale il medesimo ragionamento, ma bisogna scegliere, per ciascun primo, un esponente che **superi** entrambi gli esponenti, e che sia il più piccolo possibile. Questo si ottiene scegliendo il massimo tra l'esponente in a e quello in b.

Poiché $m + n = \max(m + n) + \min(m + n)$, si ottiene facilmente che

$$\mathrm{MCD}(a, b)\,\mathrm{mcm}(a, b) = ab.$$

5.4. **Irrazionalità di** $\sqrt{n}$ **quando** n **non è un quadrato perfetto.** Per quali scelte di $0 \neq n \in \mathbb{N}$ la radice quadrata $\sqrt{n}$ è razionale? Il Teorema di fattorizzazione unica ci permette di rispondere facilmente. In effetti, se $\sqrt{n} = a/b$, dove a, b sono interi non nulli, allora $a^2 = b^2 n$. Ogni primo presente nella fattorizzazione di a^2 e b^2 compare un numero pari di volte e quindi, per differenza, questo è vero anche per la fattorizzazione di n. Allora n è un quadrato perfetto, e quindi $\sqrt{n}$ è un intero.

In conclusione, $\sqrt{n}$ è razionale solo quando n è un quadrato perfetto. In particolare, $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}$ sono tutti irrazionali.

5.5. **Irrazionalità di** $\sqrt[k]{N}$ **quando** N **non è una** k**-esima potenza perfetta.** Lo stesso ragionamente si ripete per radici superiori: se $\sqrt[k]{N} = a/b$, con a, b interi non nulli, allora $a^k = b^k N$ e confrontando le fattorizzazioni, si ricava subito che N deve essere necessariamente una k-esima potenza perfetta, se $\sqrt[k]{N}$ è razionale.

5.6. **L'accordatura perfetta di un pianoforte è impossibile.** Ogni nota pura corrisponde ad una determinata frequenza di vibrazione[8] e due note eseguite contemporaneamente producono un suono gradevole se le frequenze corrispondenti hanno un rapporto razionale che si esprime tramite una frazione con numeratore e denominatore piccoli. Un rapporto di frequenze vicino, ma non uguale, ad una frazione "piccola" può produrre dei fenomeni acustici fastidiosi, detti *battimenti*.

Ad esempio, l'intervallo di un'ottava corrisponde ad un raddoppio di frequenza, cioè ad un rapporto $2 = 2/1$, una quinta ad un rapporto $3/2$, una quarta a $4/3$ e una terza maggiore ad un rapporto $5/4$. Per identificare questi intervalli sulla tastiera di un pianoforte, bisogna contare 12 semitoni per un'ottava, 7 per una quinta, 5 per una quarta e 4 semitoni per una terza maggiore. Ci si può quindi aspettare che, con un'accordatura perfetta, tre terze maggiori forniscano un'ottava. Tuttavia $(5/4)^3 = 125/64 \neq 128/64 = 2$, pur essendo i due numeri molto vicini. Allo stesso modo si può pensare che dodici quinte forniscano esattamente sette ottave, ma anche questo è impossibile, poiché da $(3/2)^{12} = 2^7$ segue $2^{19} = 3^{12}$ che è vietato dall'unicità della fattorizzazione in primi. In effetti, $(3/2)^{12} \sim 129,75$ è lievemente di più di $2^7 = 128$.

La conseguenza di questo fatto è che un pianoforte accordato per suonare bene una scala di do stonerebbe inevitabilmente sulle altre intonazioni. La soluzione di compromesso che viene usata è quella di utilizzare un *temperamento* suddividendo l'ottava in dodici intervalli di rapporto identico, detti semitoni, pari a $\sqrt[12]{2}$. In questo modo la terza maggiore corrisponde al rapporto $2^{4/12} \simeq 1,260$, una quarta a $2^{5/12} = 1,335$ e una quinta a $2^{7/12} = 1,498$ che sono abbastanza vicini ai rapporti ideali $5/4, 4/3, 3/2$. Un orecchio non allenato non si accorge, probabilmente, della differenza.

La suddivisione dell'ottava in dodici intervalli uguali non è l'unica soluzione percorribile: ci sono temperamenti in $19, 29$ o 41 intervalli e anche soluzioni più esotiche.

[8]Ogni strumento musicale produce, oltre alla frequenza propria della nota, tutta una serie di altre *armoniche*, che corrispondono a modi di vibrazione di frequenza multipla.

5.7. **Esistono infiniti numeri primi.** Il fatto che esistano infiniti numeri primi segue da un argomento introdotto inizialmente da Euclide. L'idea è semplice: se $p_1, \dots, p_k$ sono primi distinti, allora il numero

$$N = p_1 \cdot \dots \cdot p_k + 1 > 1$$

deve essere, per il Teorema di fattorizzazione unica, divisibile per almeno un numero primo[9]. Tuttavia N si ottiene sommando 1 ad un multiplo di ciascun p_i, e quindi non è divisibile per nessuno dei p_i. Ciascun primo che lo divida è allora diverso dai p_i e questo mostra l'infinitezza dei primi[10].

5.8. **La dimensione di $\mathbb{R}$ come spazio vettoriale razionale.** Consideriamo i numeri reali $\log(2), \log(3), \log(5), \dots$ ottenuti prendendo il logaritmo — la base non importa — di tutti i numeri primi. Questi numeri devono essere $\mathbb{Q}$-linearmente indipendenti.

In effetti, una relazione di $\mathbb{Q}$-dipendenza lineare, una volta eliminati i denominatori moltiplicando per un intero opportuno, fornirebbe un'uguaglianza del tipo

$$n_1 \log(p_1) + n_2 \log(p_2) + \dots + n_k \log(p_k) = 0,$$

dove i p_i sono primi distinti e gli n_i appartengono a $\mathbb{Z}$. L'identità è equivalente a

$$p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} = 1.$$

Spostando, con una moltiplicazione, i primi di esponente negativo a secondo membro si ottiene allora un controesempio alla validità del Teorema fondamentale dell'aritmetica. Essendo i numeri primi in quantità infinita, concludiamo che $\mathbb{R}$ ha dimensione infinita come $\mathbb{Q}$-spazio vettoriale.

Ricordate che sappiamo già che $\mathbb{Q}^n$ è numerabile per ogni $0 \neq n \in \mathbb{N}$, mentre $\mathbb{R}$ ha la cardinalità del continuo; il fatto che $\mathbb{R}$ non abbia $\dim_{\mathbb{Q}}$ finita segue quindi anche da considerazioni di cardinalità. Con un minimo di attenzione in più ci si convince che una $\mathbb{Q}$-base di $\mathbb{R}$ non può essere numerabile.

5.9. **Il piccolo teorema di Fermat.** Nello sviluppo di Newton della potenza di un binomio

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

compaiono i *coefficienti binomiali*, che sono tutti interi e sono calcolabili per mezzo dell'espressione

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

In particolare, per fattorizzazione unica, quando p è primo il coefficiente binomiale

$$\binom{p}{k}$$

è multiplo di p per ogni $0 < k < p$, mentre quando $k = 0, p$ si ottiene, ovviamente, 1.

Teorema 5.1. *Se $a \in \mathbb{N}$ e p è un numero primo, allora $a^p - a$ è un multiplo di p.*

Dimostrazione. Per induzione su a, la base $a = 0$ dell'induzione essendo ovvia.

Per il passo induttivo, supponiamo di sapere che $n^p - n$ sia multiplo di p. Usando lo sviluppo di Newton si ottiene

$$(n+1)^p - (n+1) = (n^p - n) + \sum_{k=1}^{p-1} \binom{p}{k} n^k,$$

che è ancora multiplo di p in quanto somma di multipli di p. □

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI ROMA – "LA SAPIENZA"
E-mail address: dandrea@mat.uniroma1.it

[9] Ad esempio se stesso, nel caso in cui sia primo.
[10] Nella forma: *ciascun elenco finito di numeri primi è incompleto*.