

Benedetto Scimemi

ALGEBRETTA

*un'introduzione al corso di algebra
per la laurea in matematica*



DECIBEL



ZANICHELLI

Benedetto Scimemi
*professore di Algebra
 nell'Università di Padova*

ALGEBRETTA

Nel primo corso per la laurea in Matematica molti studenti incontrano difficoltà nell'apprendere le nozioni astratte dell'Algebra se queste non si fanno precedere da un adeguato campionario di esempi concreti.

In questo volumetto, dopo una breve introduzione alla nomenclatura degli insiemi e delle funzioni, si trattano, in modo semplice ma rigoroso, certe strutture algebriche fondamentali (permuteazioni; numeri interi, razionali, reali e complessi; polinomi), in modo che la successiva introduzione dei concetti di gruppo, anello, ecc. sia resa più facile dalla familiarità con questi esempi.

Da molti anni (la prima edizione è del 1972) l'Algebretta viene adottata con un certo successo in varie sedi universitarie come premessa al corso di Algebra, nelle prime settimane di lezioni.

INDICE

§ 1 Insiemi	1
§ 2 Applicazioni	3
§ 3 Operazioni	5
§ 4 Analisi combinatoria	7
§ 5 Permutazioni	10
§ 6 Numeri interi: induzione	16
§ 7 Divisione	20
§ 8 Massimo Comune Divisore	22
§ 9 Fattorizzazione unica	26
§10 Scrittura b -adica	28
§11 Congruenze	29
§12 Numeri razionali	33
§13 Numeri reali	35
§14 Numeri complessi	37
§15 Funzioni razionali intere	44
Indice analitico e dei simboli	55

§ 1. Insiemi

1.1. Un *insieme* è una collezione di oggetti. Un oggetto di questa collezione si chiama un *elemento* dell'insieme. Gli insiemi ed i loro elementi si indicano per lo più con lettere latine, in generale maiuscole per gli insiemi, ad esempio $S, T, Z, \dots, X, Y, \dots$, minuscole per gli elementi, ad esempio $a, b, c, \dots, x, y, \dots$. Se l'insieme A è costituito dagli elementi a, b, c, \dots , lo si indicherà anche con $\{a, b, c, \dots\}$.

Invece di dire che x è un elemento dell'insieme X , diremo anche che x appartiene ad X oppure x sta in X e scriveremo $x \in X$ (oppure $X \ni x$).

$x \notin X$ sta a indicare che x non appartiene ad X .

1.2. Dati due insiemi S e T diremo che S è un *sottoinsieme* di T (espressioni equivalenti: T contiene S , S è *incluso in* T , S è *parte di* T) se ogni elemento di S è anche elemento di T . In questo caso scriveremo $S \subseteq T$ (oppure $T \supseteq S$). Ad esempio, l'insieme N dei numeri interi positivi è un sottoinsieme dell'insieme Z dei numeri interi. Risulta $N \subseteq Z$, ma $Z \not\subseteq N$, cioè Z non è parte di N , perché esistono numeri interi che non sono positivi. Se $S \subseteq T$ e $T \subseteq S$, i due insiemi si dicono *eguali* e si scrive $S = T$. Se però $S \subseteq T$, ma $S \neq T$ (leggi: S è *diverso* da T , S non è uguale a T) allora diremo che S è un *sottoinsieme proprio* di T (espressione equivalente: S è *contenuto propriamente in* T) e scriveremo $S \subset T$. Ad esempio $N \subset Z$. L'insieme A privo di elementi, cioè tale che $x \notin A$ qualunque sia x , si chiama l'insieme *vuoto* e si denota con il simbolo \emptyset .

1.3. Se S_1, S_2 sono insiemi, allora l'*intersezione* di S_1 ed S_2 , che si indica con $S_1 \cap S_2$, è l'insieme di quegli elementi che appartengono sia ad S_1 che ad S_2 . Ad esempio, se S_1 ed S_2 sono gli insiemi dei punti del piano che giacciono rispettivamente su due rette non parallele, allora $S_1 \cap S_2$ è costituito da un solo punto. L'insieme $S_1 \cap S_2$ può essere privo di elementi, perché esiste la possibilità che S_1 ed S_2 non abbiano elementi in comune (espressione equivalente: siano *disgiunti*). Ad esempio, se le due rette, di cui sopra, sono parallele e distinte, sarà $S_1 \cap S_2 = \emptyset$.

1.4. L'unione di S_1 ed S_2 , che si indica con $S_1 \cup S_2$, è l'insieme degli elementi che appartengono ad S_1 o ad S_2 (o ad entrambi). Ad esempio, se M è l'insieme costituito dai numeri interi negativi e dallo zero (non positivi) allora $M \cup N = \mathbf{Z}$. Ma anche $\mathbf{Z} \cup N = \mathbf{Z}$.

1.5. Per descrivere un insieme A si può usare una proprietà $P(x)$ di cui godono gli elementi $x \in A$. Allo scopo è molto usata la seguente notazione: $A = \{x | P(x)\}$, che si legge: A è l'insieme di tutti gli elementi che godono della proprietà P . Ad esempio, $A = \{x | x \in \mathbf{Z} \text{ e } 1 < x < 5\}$ è l'insieme dei numeri interi che sono maggiori di 1 e minori di 5, cioè l'insieme $\{2, 3, 4\}$. Oppure $A = \{x | x \in \mathbf{Z} \text{ e } 2 \text{ divide } x\}$ è l'insieme degli interi pari.

1.6. Un'altra utile nozione è quella di insieme differenza di S_1 ed S_2 , che si denota con $S_1 \setminus S_2$ ed è l'insieme di quegli elementi che appartengono al primo ma non al secondo insieme. Con i simboli sopra introdotti, $S_1 \setminus S_2 = \{x | x \in S_1, x \notin S_2\}$. Ad esempio $\mathbf{Z} \setminus \mathbf{N} = M$; $\mathbf{N} \setminus \mathbf{Z} = \emptyset$.

1.7. Alle volte si considerano insiemi i cui elementi sono a loro volta insiemi; così, ad esempio, l'insieme $\mathcal{P}(X)$ di tutti i sottoinsiemi di un dato insieme X . Qualunque sia X , si avrà sempre: $X \in \mathcal{P}(X)$, $\emptyset \in \mathcal{P}(X)$.

$\mathcal{P}(X)$ si chiama l'insieme delle parti di X .

1.8. Le definizioni di unione e intersezione di due insiemi si generalizzano ad un insieme F di insiemi mediante le posizioni:

$$\bigcap_{A \in F} A = \{x | x \in A \text{ per ogni } A \in F\};$$

leggi: insieme intersezione di tutti gli insiemi di F .

$$\bigcup_{A \in F} A = \{x | x \in A \text{ per qualche } A \in F\};$$

leggi: insieme unione di tutti gli insiemi di F .

1.9. L'insieme prodotto (cartesiano) di due insiemi S_1 ed S_2 è quello che consiste di tutte le coppie ordinate (x, y) in cui la prima componente x è un elemento di S_1 , la seconda y di S_2 . Lo si indica con $S_1 \times S_2$. Due coppie ordinate (x, y) , (x', y') sono eguali se e solo se $x = x'$, $y = y'$. Così, ad esempio, se $S_1 = \{1, 2\}$ e $S_2 = \{a, b, c\}$, allora

$$S_1 \times S_2 = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}.$$

Il prodotto $S \times S$ si dice il quadrato (cartesiano) di S e si indica talvolta con S^2 . Così, ad esempio, $S_1^2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$. Più in generale, $S_1 \times S_2 \times \dots \times S_n$ è l'insieme delle n -uple (leggì: ennuple) ordinate (s_1, s_2, \dots, s_n) la cui i -esima componente s_i è un elemento di S_i .

Esercizi

- 1) Elencare i sottoinsiemi di $\{1,2,3\}$.
- 2) Verificare che $R \cap (S \cup T) = (R \cap S) \cup (R \cap T)$, dove R, S, T sono insiemi qualsiasi.
- 3) Dimostrare che risulta $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ dove A, B, C sono insiemi qualsiasi.

§ 2. Applicazioni

2.1. Siano S, T insiemi. Si ha un'*applicazione* f (sinonimo: *funzione*) di S in T se è data una regola (sinonimo: *legge*) che ad ogni elemento di S associa (sinonimo: *assegna*) un unico elemento di T . Ad esempio, tra l'insieme dei segmenti del piano e l'insieme dei punti del piano si definisce un'applicazione associando ad ogni segmento il suo punto di mezzo. Per esprimere che f è un'applicazione di S in T , useremo di solito la notazione $f: S \rightarrow T$, oppure $S \xrightarrow{f} T$. Se $x \in S$, indicheremo con $f(x)$ quell'elemento $y \in T$ che è associato ad x da f , e scriveremo $f: x \mapsto y$; $f(x)$ si dirà il *valore di f in x* (sinonimo: *l'immagine* di x secondo f). Dati S e T , per assegnare un'applicazione f di S in T basta dunque assegnare il valore che f assume in ogni *punto* x di S . Ad esempio, tra le applicazioni di \mathbf{Z} in \mathbf{Z} (diremo anche di \mathbf{Z} *in sé*) la posizione $x \mapsto x^2$ individua quella che ad ogni numero intero associa il suo quadrato.

2.2. Se $f: S \rightarrow T$, gli insiemi S e T si dicono rispettivamente il *dominio* e il *codominio* di f . Due applicazioni f, g sono eguali se e solo se f e g hanno lo stesso dominio, lo stesso codominio, e si ha $f(x) = g(x)$ per ogni x del dominio. Se U è un sottoinsieme del dominio S , si indica con $f(U)$ l'*insieme degli elementi di T che sono immagine di qualche $x \in U$* . In particolare, $f(S)$ si chiama l'(insieme) *immagine* di f .

2.3. Dalla definizione di applicazione non consegue che $f(S)$ coincide con il codominio T (nell'esempio considerato, del *quadrato di un intero*, si ha $f(\mathbf{Z}) \subset \mathbf{Z}$). Nel caso che risulti $f(S) = T$, l'applicazione f si dice *suriettiva*

(espressione equivalente: f è su T). Dunque, se f è suriettiva, assegnato $y \in T$ esiste (almeno) un $x \in S$ tale che si abbia $y = f(x)$. Il precedente esempio del *punto medio* fornisce un caso di applicazione suriettiva; si noti che non si richiede ad x di essere l'unico elemento di S con $f(x) = y$.

2.4. Un'applicazione $f: S \rightarrow T$ si dice *iniettiva* se immagini di elementi distinti sono distinte, cioè se $f(x) \neq f(y)$ non appena $x \neq y$; o equivalentemente, se ogni elemento di T o non appartiene ad $f(S)$ oppure è immagine di un solo elemento di S (ovvero: se da $f(x) = f(y)$ segue $x = y$). Ad esempio, l'applicazione di \mathbf{Z} in \mathbf{Z} individuata da $x \mapsto 2x$ è iniettiva; invece l'applicazione di \mathbf{Z} in \mathbf{Z} individuata da $x \mapsto x^2$ non è iniettiva, perché assume lo stesso valore, ad esempio, in 1 e in -1.

2.5. Un'applicazione $f: S \rightarrow T$ si dice *biiettiva* se è iniettiva e suriettiva. Ciò significa che per ogni elemento $t \in T$ esiste uno ed un solo elemento $s \in S$ tale che $t = f(s)$. Ad esempio, l'applicazione di \mathbf{Z} in sé data da $x \mapsto x + 1$ è biiettiva (espressione equivalente: è una *bijezione*). Altro esempio: sia S una superficie sferica (come insieme di punti) di centro C , e sia T l'insieme delle semirette che hanno C come origine. Allora si ottiene un'applicazione biiettiva $f: S \rightarrow T$ associando ad ogni punto $x \in S$ la semiretta $f(x) \in T$ che contiene x . Ovviamente è una bijezione l'*identità* dell'insieme S (sinonimo: l'applicazione *identica* di S in sé) che è l'applicazione di S in S data da $x \mapsto x$. L'*identità* di S si indica talvolta con i_S .

2.6. Sia $f: S \rightarrow T$ biiettiva. L'applicazione $f^{-1}: T \rightarrow S$ inversa di f è l'applicazione il cui valore s nel punto t di T è quell'unico elemento $s \in S$ tale che $f(s) = t$. Ad esempio, se f è l'applicazione $x \mapsto x + 1$ di \mathbf{Z} in sé, allora f^{-1} è l'applicazione $x \mapsto x - 1$ di \mathbf{Z} in sé. Nell'altro esempio, l'inversa di f si ottiene associando ad ogni semiretta $t \in T$ quell'unico suo punto che sta sulla superficie sferica. L'*identità* i_S coincide con la sua inversa.

Se $f: S \rightarrow T$ non è biiettiva, la funzione inversa di f non si può definire; in effetti, preso $t \in T$ può non esserci alcun elemento $s \in S$ tale che $t = f(s)$ (se f non è suriettiva), oppure possono esistere più elementi con tale proprietà (se f non è iniettiva).

Se V è un sottoinsieme di T , si chiama *immagine inversa* (sinonimo: *controimmagine*) di V , e si indica con $f^{-1}(V)$ la totalità degli elementi di S la cui immagine sta in V . Si definisce cioè $f^{-1}(V) = \{x \mid x \in S; f(x) \in V\}$. Se V consiste di un solo elemento v , invece di $f^{-1}(\{v\})$ si scrive qualche volta $f^{-1}(v)$, ma è bene notare che si tratta di una notazione impropria; ad esempio, se f è l'applicazione $x \mapsto x^2$ di \mathbf{Z} in sé, risulta: $f^{-1}(0) = \{0\}$; $f^{-1}(1) = \{1, -1\}$; $f^{-1}(-1) = \emptyset$; $f^{-1}(\mathbf{N}) = \mathbf{Z} \setminus \{0\}$.

Esercizi

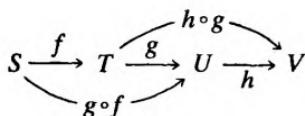
- 1) Se $f: S \rightarrow T$ e $A, B \subseteq S$, è vero che $f(A \cap B) = f(A) \cap f(B)$? È vero che $f(A \cup B) = f(A) \cup f(B)$?
- 2) Se f è l'applicazione di \mathbf{Z} in sé data da $x \mapsto 2 - x$, si scriva f^{-1} .
- 3) Se $f: S \rightarrow T$ e $C, D \subseteq T$, è vero che $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$? Analoga domanda per l'unione.

§ 3. Operazioni

3.1. Dati tre insiemi A, B, C un'operazione tra A e B a valori in C è un'applicazione $f: A \times B \rightarrow C$. Se $a \in A$, $b \in B$, il valore $c = f(a, b)$ si dice il risultato dell'operazione sulla (ovvero applicata alla) coppia (a, b) . Alle volte il risultato si denota con $a + b$ (e si dice somma) oppure con ab (prodotto) o più in generale con $a * b$, $a \circ b$ ecc. Tra gli esempi più ovvi di operazione sono note l'addizione, la sottrazione, la moltiplicazione dei numeri interi ($A = B = C = \mathbf{Z}$). Quando, come in questo caso, i tre insiemi coincidono, si parla di operazione nell'insieme A . Un altro esempio: assegnati due punti a, b nel piano, indichiamo con $a * b$ il loro punto medio (cioè il punto di mezzo del segmento che ha a, b per estremi). Qui $*$ è un'operazione nell'insieme dei punti del piano.

3.2. Date due applicazioni $f: S \rightarrow T$, $g: T \rightarrow U$ si definisce l'applicazione composta $g \circ f: S \rightarrow U$ (di f con g) ponendo $(g \circ f)(x) = g(f(x))$ per ogni $x \in S$. Ad esempio, siano $f: \mathbf{N} \rightarrow \mathbf{N}$ definita da $x \mapsto 1 + 2x$, $g: \mathbf{N} \rightarrow \mathbf{Z}$ definita da $x \mapsto 1 - x^2$. Allora $g \circ f: \mathbf{N} \rightarrow \mathbf{Z}$ è definita da $x \mapsto 1 - (1 + 2x)^2$.

Sia ora $h: U \rightarrow V$ una terza applicazione. Allora possiamo considerare le applicazioni composte $(h \circ g) \circ f$, $h \circ (g \circ f)$ e verificare che coincidono.



Infatti per ogni $x \in S$ si ha $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$; $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$. Si conclude che la *composizione di applicazioni gode della proprietà associativa*, nel senso che risulta $(h \circ g) \circ f = h \circ (g \circ f)$ per ogni scelta di h, g, f (purché sia lecito considerare tali applicazioni composte!). Ad esempio, se f, g sono come sopra ed $h: \mathbf{Z} \rightarrow \mathbf{Z}$ è definita da $x \mapsto -x$, allora

$$((h \circ g) \circ f)(x) = (h \circ g)(1 + 2x) = (1 + 2x)^2 - 1;$$

$$(h \circ (g \circ f))(x) = h(1 - (1 + 2x)^2) = (1 + 2x)^2 - 1.$$

3.3. Siano $f: S \rightarrow T$, $g: T \rightarrow U$ due applicazioni iniettive. Allora anche $g \circ f$ è iniettiva. Infatti, se $x, y \in S$ con $x \neq y$, allora $f(x) \neq f(y)$ perché f è iniettiva, e quindi $g(f(x)) \neq g(f(y))$ perché g è iniettiva; per definizione, questo significa che $g \circ f$ è iniettiva.

Siano $f: S \rightarrow T$, $g: T \rightarrow U$ due applicazioni suriettive. Allora anche $g \circ f$ è suriettiva. Infatti per ogni $z \in U$ esiste un $y \in T$ con $g(y) = z$, perché g è suriettiva. Inoltre, assegnato $y \in T$, esiste un $x \in S$ con $f(x) = y$, perché f è suriettiva. Ma allora, per ogni $z \in U$, esiste un elemento $x \in S$ tale che $(g \circ f)(x) = g(f(x)) = g(y) = z$, e quindi, per definizione, $g \circ f$ è suriettiva.

Segue che, se f, g sono entrambe biiettive, cioè iniettive e suriettive, allora anche $g \circ f$ lo è. Un caso particolare, che studieremo in seguito in dettaglio, si ha quando $S = T = U$, cioè quando si tratta di biezioni di un insieme S in sé; in questo caso le considerazioni precedenti ci dicono che componendo due biezioni di S in sé si ottiene ancora una biezione di S in sé e che la composizione (di applicazioni) è un'operazione associativa nell'insieme di tali biezioni.

3.4. Sia $f: S \rightarrow T$ un'applicazione biiettiva, e sia $f^{-1}: T \rightarrow S$ la sua inversa. Allora, per definizione di inversa, risulta $f(f^{-1}(x)) = x$ per ogni $x \in T$; $f^{-1}(f(x)) = x$ per ogni $x \in S$; in altre parole, risulta $f \circ f^{-1} = i_T$, $f^{-1} \circ f = i_S$.

Esercizi

- 1) Sia $*$ l'operazione del punto medio sull'insieme dei punti del piano. È associativa?
- 2) È la divisione un'operazione in \mathbf{Z} ?
- 3) Siano f, g applicazioni di \mathbf{Z} in sé definite da $x \mapsto 2x$, $x \mapsto x^2$ rispettivamente. Si trovino $g \circ f$ ed $f \circ g$. È vero che $f \circ g = g \circ f$?

§ 4. Analisi combinatoria

In questo paragrafo ci proponiamo di *contare* gli elementi di certi insiemi. Siano S e T due insiemi che contengono rispettivamente k ed n elementi:

$$S = \{x_1, x_2, \dots, x_k\}, \quad T = \{y_1, y_2, \dots, y_n\}.$$

4.1 *Gli elementi del prodotto cartesiano $S \times T$ sono $n \cdot k$.* Infatti ci sono evidentemente n coppie ordinate del tipo (x_1, \dots) , n del tipo (x_2, \dots) , ecc., e tutte queste coppie sono distinte.

4.2. *Le applicazioni di S in T sono n^k .* Infatti si hanno n scelte per il valore di $f(x_1)$; per ciascuna di queste abbiamo ancora n scelte per $f(x_2)$; ecc.. Si possono fare in totale $n \cdot n \cdot \dots \cdot n$ (k fattori) scelte, ed ogni scelta dà luogo ad una diversa applicazione. Ad esempio, se $k=2$, $n=3$ si hanno le seguenti 9 possibilità:

- | | | |
|---|---|---|
| 1) $\begin{cases} x_1 \mapsto y_1 \\ x_2 \mapsto y_1 \end{cases}$ | 2) $\begin{cases} x_1 \mapsto y_1 \\ x_2 \mapsto y_2 \end{cases}$ | 3) $\begin{cases} x_1 \mapsto y_1 \\ x_2 \mapsto y_3 \end{cases}$ |
| 4) $\begin{cases} x_1 \mapsto y_2 \\ x_2 \mapsto y_1 \end{cases}$ | 5) $\begin{cases} x_1 \mapsto y_2 \\ x_2 \mapsto y_2 \end{cases}$ | 6) $\begin{cases} x_1 \mapsto y_2 \\ x_2 \mapsto y_3 \end{cases}$ |
| 7) $\begin{cases} x_1 \mapsto y_3 \\ x_2 \mapsto y_1 \end{cases}$ | 8) $\begin{cases} x_1 \mapsto y_3 \\ x_2 \mapsto y_2 \end{cases}$ | 9) $\begin{cases} x_1 \mapsto y_3 \\ x_2 \mapsto y_3 \end{cases}$ |

4.3. *Sia $k \leq n$, allora il numero delle applicazioni iniettive di S in T è $n(n-1)(n-2)\dots(n-k+1)$.* Infatti gli elementi $f(x_1), f(x_2), \dots, f(x_k)$ devono essere distinti e quindi, fatta la prima scelta per $f(x_1)$ arbitrariamente (n possibilità) rimangono $n-1$ scelte possibili per $f(x_2)$, $n-2$ per $f(x_3)$ ecc. Nell'esempio precedente si ottengono 6 applicazioni: le 2), 3), 4), 6), 7), 8).

4.4. *Le applicazioni iniettive di S in sé ($T=S$, quindi $k=n$) sono anche suriettive e quindi bigettive.* Infatti le immagini $f(x_1), \dots, f(x_n)$ sono tutte

distinte e quindi esauriscono l'insieme S . Ma allora, con la formula precedente il loro numero è $n(n-1)\cdots 3 \cdot 2 \cdot 1$ che si indica con $n!$ e si chiama il *fattoriale* di n . Le biiezioni di S in sé si chiamano anche *permutazioni* di S . Il loro insieme si indica talvolta con Σ_S . Se, ad esempio, $S = \{1,2,3\}$, si trovano 6 permutazioni:

$$\begin{array}{ll} \left\{ \begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 2 \\ 3 \mapsto 3 \end{array} \right. & \left\{ \begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \end{array} \right. \quad \left\{ \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{array} \right. \quad \left\{ \begin{array}{l} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 1 \end{array} \right. \quad \left\{ \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{array} \right. \quad \left\{ \begin{array}{l} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \end{array} \right. \end{array}$$

che si scrivono anche nella forma

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

4.5. Se $k \leq n$, ci proponiamo di contare i sottoinsiemi U di T che contengono precisamente k elementi. Introdotto l'insieme $S = \{1,2,\dots,k\}$ osserviamo che ogni applicazione iniettiva $f: S \rightarrow T$ ha per immagine un tale sottoinsieme: $f(S) = U$. Viceversa, ogni $U \subseteq T$ è immagine di qualche applicazione iniettiva $f: S \rightarrow T$. Fissato U , quante sono le applicazioni iniettive f con $f(S) = U$? sono tante quante le applicazioni iniettive di S in U e quindi sono $k!$ per 4.3. e 4.4.. Se dunque m è il numero (che cerchiamo) dei sottoinsiemi del tipo di U , allora il numero delle funzioni iniettive di S in T è $m \cdot k!$. Per 4.3. si ottiene

$$m = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

e tale numero si indica con $\binom{n}{k}$. Per esempio $\binom{5}{3} = \frac{5 \cdot 4 \cdot 3}{1 \cdot 2 \cdot 3} = 10$; infatti i sottoinsiemi di $\{1,2,3,4\}$ che contengono 3 elementi sono: $\{1,2,3\}$, $\{1,2,4\}$, $\{1,2,5\}$, $\{1,3,4\}$, $\{1,3,5\}$, $\{1,4,5\}$, $\{2,3,4\}$, $\{2,3,5\}$, $\{2,4,5\}$, $\{3,4,5\}$.

4.6. È comodo attribuire significato a $k!$ e a $\binom{n}{k}$ anche quando $k = 0$, ponendo $0! = 1$, $\binom{n}{0} = 1$. Quest'ultima è conforme al fatto che ogni insieme contiene uno (ed un solo) sottoinsieme con 0 elementi, cioè \emptyset .

4.7. Un numero del tipo $\binom{n}{k}$ si dice *coefficiente binomiale* ed i sottoinsiemi di k elementi di un insieme di n elementi ($n \geq k$) si dicono le *combinazioni (semplici) di n oggetti a k a k* . Si ha

$$\binom{n}{0} = \binom{n}{n} = 1, \quad \binom{n}{1} = \binom{n}{n-1} = n, \quad \binom{n}{2} = \binom{n}{n-2} = \frac{n(n-1)}{2}$$

e, in generale

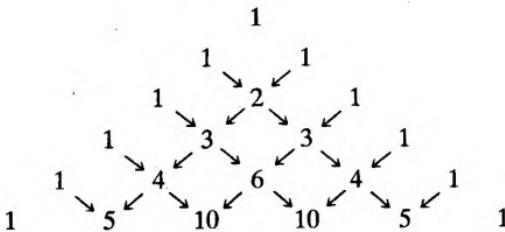
$$\binom{n}{k} = \binom{n}{n-k}$$

perché nella formula che definisce $\binom{n}{k}$ sostituire k con $n - k$ equivale soltanto allo scambio dei due fattori al denominatore. Risulta

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Tale eguaglianza si potrebbe verificare meccanicamente con la formula che definisce $\binom{n}{k}$, ma è più istruttivo rifarsi ai sottoinsiemi di un insieme $Y = \{y_1, y_2, \dots, y_n\}$ che contenga n elementi. Scegliamo un elemento in Y , sia y_1 . Allora i sottoinsiemi di Y che contengono k elementi si ripartiscono in due classi: I) quelli che non contengono y_1 , il cui numero è quello dei sottoinsiemi di $\{y_2, \dots, y_n\}$ che hanno k elementi, cioè a $\binom{n-1}{k}$; II) quelli che contengono y_1 il cui numero è quello dei sottoinsiemi di $\{y_2, \dots, y_n\}$ che hanno $k-1$ elementi, cioè $\binom{n-1}{k-1}$. Ne segue la formula.

4.8. La relazione di 4.7. permette di costruire tutti i coefficienti binomiali del tipo $\binom{n}{k}$, a partire da quelli del tipo $\binom{n-1}{k}$. Nel triangolo di Tartaglia (di Pascal per i francesi) qui riprodotto, $\binom{n}{k}$ occupa la $(k+1)$ -esima posizione della $(n+1)$ -esima riga. Esso si ottiene (se $0 < k < n$) sommando i due numeri che lo sovrastano.



4.9. L'insieme delle parti di $S = \{x_1, x_2, \dots, x_k\}$ contiene 2^k elementi. Per dimostrarlo, introduciamo l'insieme $T = \{0,1\}$ e consideriamo le applicazioni di S in T . Per ogni tale $f: S \rightarrow T$, la controimmagine $f^{-1}(1)$ è un sottoinsieme di S . Viceversa ogni sottoinsieme $V \subseteq S$ è controimmagine di una e una sola $f: S \rightarrow T$, definita da $f(x) = 1$ se $x \in V$, $f(x) = 0$ se $x \notin V$. Ma allora i sottoinsiemi di S sono tanti quante sono le applicazioni di S in T e quindi 2^k per 4.2..

4.10. Per contare i sottoinsiemi di S possiamo anche sommare il numero $\binom{n}{k}$ di quelli che contengono k elementi per $k = 0, 1, \dots, n-1, n$. Si ottiene la relazione:

$$\sum_{k=0}^n \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

Ad esempio

$$\binom{4}{0} + \binom{4}{1} + \binom{4}{2} + \binom{4}{3} + \binom{4}{4} = 1 + 4 + 6 + 4 + 1 = 16 = 2^4.$$

§ 5. Permutazioni

5.1. Per studiare le permutazioni di un insieme S di n oggetti supponiamo, per semplicità, che si tratti dell'insieme $S = \{1, 2, \dots, n-1, n\}$. Allora Σ_S (vedi 4.4.) si scrive talvolta Σ_n . Il suo generico elemento $f \in \Sigma_n$ si denoterà con

$$\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}.$$

5.2. Ricordando quanto detto, osserviamo che assegnate due permutazioni $f, g \in \Sigma_n$

- 1) ha significato considerare l'applicazione composta $g \circ f$ (vedi 3.2.),
- 2) $g \circ f$ è ancora una permutazione di S , cioè $g \circ f \in \Sigma_n$ (vedi 3.3.),
- 3) quindi la *composizione* \circ è un'operazione in Σ_n (vedi 3.1.),
- 4) questa operazione è *associativa* (vedi 3.2.).

5.3. Osserviamo inoltre che per ogni $f \in \Sigma_n$

- 5) ha significato considerare l'applicazione inversa f^{-1} ,
- 6) f^{-1} è una permutazione di S , cioè $f^{-1} \in \Sigma_n$,

- 7) $f^{-1} \circ f = f \circ f^{-1}$ è l'identità in S (che indichiamo semplicemente con i) anch'essa un elemento di Σ_n
 8) $f \circ i = i \circ f = f$,
 9) l'inversa di $g \circ f$ è il prodotto delle inverse nell'ordine scambiato: $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Verifichiamo soltanto quest'ultima affermazione: se $x \in S$, consideriamo $y = (g \circ f)^{-1}(x)$, $z = (f^{-1} \circ g^{-1})(x)$; basta provare che $y = z$. Ragioniamo per assurdo: se fosse $y \neq z$, sarebbe anche $(g \circ f)(y) \neq (g \circ f)(z)$ perché $g \circ f$ è iniettiva. Ora $(g \circ f)(y) = x$ per definizione di applicazione inversa. D'altra parte applicando la proprietà associativa si ha:

$$(g \circ f)(z) = (g \circ f)((f^{-1} \circ g^{-1})(x)) = (g \circ (f \circ f^{-1}) \circ g^{-1})(x) = \\ = (g \circ i \circ g^{-1})(x) = (g \circ g^{-1})(x) = i(x) = x.$$

Seguirebbe $x \neq x$, una contraddizione. Concludiamo che il caso $y \neq z$ non si può verificare, cioè $y = z$.

Esempi:

Sia $n = 4$ e si considerino le permutazioni

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

Per calcolare $g \circ f$ prepariamoci lo schema $1 \xrightarrow{f} 2 \xrightarrow{g} 3 \quad 2 \xrightarrow{f} 4 \xrightarrow{g} 2 \quad 3 \xrightarrow{f} 3 \xrightarrow{g} 4$
 $4 \xrightarrow{f} 1 \xrightarrow{g} 1$; dunque scriveremo

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \quad f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \neq g \circ f.$$

Per calcolare l'inversa di f , osserviamo che da $1 \xrightarrow{f} 2$ segue $2 \xrightarrow{f^{-1}} 1$, perché $f^{-1}(2)$ è quell'unico elemento la cui immagine secondo f è 2. Analogamente $4 \xrightarrow{f^{-1}} 2 \quad 3 \xrightarrow{f^{-1}} 3 \quad 1 \xrightarrow{f^{-1}} 4$ e quindi

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix},$$

che si ottiene da f scambiando le righe orizzontali e riordinando le quattro colonne verticali. Nello stesso modo si calcola

$$g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

e si verifica che

$$f^{-1} \circ g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

è l'inversa di $g \circ f$.

5.4. Se f è una permutazione sugli n oggetti $1, 2, \dots, n$ consideriamo successivamente gli elementi:

$$1 \xrightarrow{f} f(1) \xrightarrow{f} f(f(1)) \xrightarrow{f} f(f(f(1))) \xrightarrow{f} \dots;$$

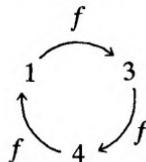
dopo un certo numero di passi ritroveremo l'elemento 1 e la successione si ripeterà *periodicamente*. Infatti prima o poi qualche elemento dovrà ripetersi (al più dopo n passi) ed il primo elemento che si ripete deve essere proprio 1, altrimenti esso sarebbe immagine secondo f di due elementi distinti contrariamente al fatto che f è iniettiva. Ad esempio in Σ_6 se

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}$$

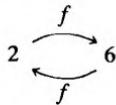
si ha

$$1 \xrightarrow{f} 3 \xrightarrow{f} 4 \xrightarrow{f} 1 \xrightarrow{f} 3 \xrightarrow{f} 4 \xrightarrow{f} \dots$$

Rappresenteremo tale situazione disegnando un'*orbita circolare*:



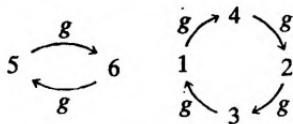
Ripetendo il procedimento a partire dagli altri elementi si trova:



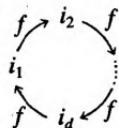
e l'orbita *banale* contenente il solo elemento 5. Analogamente

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 2 & 6 & 5 \end{pmatrix}$$

dà luogo alle due orbite *non banali*:



Una permutazione f si dice *ciclica* ovvero un *ciclo di lunghezza d* se possiede (al più) un'unica orbita non banale e in questo caso si usa per f anche il simbolo $(i_1 \ i_2 \dots i_n)$.



In Σ_4 ad esempio,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = (1 \ 4 \ 2), \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (1 \ 3) \text{ e } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1 \ 3 \ 2 \ 4)$$

sono cicli di lunghezza rispettivamente 3, 2, 4. Per convenzione l'identità

$$\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

si considera un ciclo di lunghezza 1. Invece, ad esempio

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

non è un ciclo perché dà luogo alle due orbite non banali



Se però costruiamo le permutazioni cicliche

$$(1 \ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \text{ e } (2 \ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

che corrispondono a queste due orbite singolarmente, è evidente che il loro prodotto coincide con la permutazione di partenza

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1 \ 3) \circ (2 \ 4).$$

Si è così sostanzialmente dimostrato che *ogni permutazione si può scrivere in modo unico come prodotto di cicli disgiunti*

$$(*) \quad f = (i_1 i_2 \dots i_d) \circ (j_1 j_2 \dots j_r) \circ \dots \circ (h_1 h_2 \dots h_s),$$

dove *disgiunti* significa che ogni oggetto compare in uno solo di questi cicli fattori (oppure in nessuno, se f lo lascia fisso), e *in modo unico* significa che questi cicli fattori sono individuati da f ; non è invece individuato l'ordine in cui essi compaiono. Infatti è facile convincersi che *due cicli disgiunti commutano* nel senso che sono permutabili

$$(i_1 i_2 \dots i_d) \circ (j_1 j_2 \dots j_r) = (j_1 j_2 \dots j_r) \circ (i_1 i_2 \dots i_d).$$

Ad esempio

$$\left(\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 2 & 4 \end{array} \right) = (1 \ 3) \circ (2 \ 5) \circ (4 \ 6) = (4 \ 6) \circ (2 \ 5) \circ (1 \ 3) = \text{ecc.}$$

5.5. Quando f è decomposta in cicli disgiunti come in (*) possiamo costruire il numero

$$(d-1) + (r-1) + \dots + (s-1) = N(f)$$

che si ottiene sommando la lunghezza dei suoi fattori ciclici, ciascuna diminuita di 1. Ad esempio

$$N\left(\left(\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{array} \right)\right) = N((1 \ 3) \circ (2 \ 4)) = (2-1) + (2-1) = 2,$$

$$N\left(\left(\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{array} \right)\right) = N((1 \ 3 \ 4)) = (3-1) = 2.$$

Si dice che f è di *classe pari* oppure *dispari* a seconda che sia pari o dispari $N(f)$.

5.6. I cicli di lunghezza 2 si chiamano *trasposizioni*. Ogni ciclo di lunghezza maggiore di 2 si può scrivere come prodotto di trasposizioni (non disgiunte) come segue $(i_1 i_2 \dots i_{d-1} i_d) = (i_1 i_d) \circ (i_1 i_{d-1}) \circ \dots \circ (i_1 i_3) \circ (i_1 i_2)$. E quindi anche ogni permutazione si può scrivere come prodotto di trasposizioni. Ad esempio

$$\left(\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 2 & 6 & 5 \end{array} \right) = (1 \ 3 \ 4 \ 2) \circ (5 \ 6) = (1 \ 2) \circ (1 \ 4) \circ (1 \ 3) \circ (5 \ 6),$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 6 & 1 & 3 \end{pmatrix} = (1\ 2\ 5) \circ (3\ 4\ 6) = (1\ 5) \circ (1\ 2) \circ (3\ 6) \circ (3\ 4).$$

Si osservi che la nostra costruzione dà luogo ad un numero di trasposizioni pari ad $N(f)$.

5.7. Per una stessa permutazione possono sussistere varie decomposizioni in prodotto di trasposizioni; ad esempio

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\ 3) \circ (2\ 4) = (1\ 4) \circ (1\ 2) \circ (4\ 3) \circ (1\ 4) = (4\ 2) \circ (4\ 1) \circ (4\ 3) \circ (4\ 1).$$

Però il numero di trasposizioni nelle varie fattorizzazioni è sempre pari oppure è sempre dispari, a seconda che sia pari o dispari $N(f)$: Ciò si può dimostrare così: osserviamo che se f si moltiplica per una qualsiasi trasposizione (ab) il valore di N cambia di ± 1 ; $N((ab) \circ f) = N(f) \pm 1$ a seconda che a e b compaiono in cicli diversi o nello stesso ciclo di una fattorizzazione di f in cicli disgiunti. Infatti valgono le formule:

$$(ab) \circ (ai_1 i_2 \dots i_h) \circ (bj_1 j_2 \dots j_k) = (ai_1 \dots i_h b j_1 \dots j_k),$$

$$(ab) \circ (ai_1 i_2 \dots i_h b j_1 \dots j_k) = (ai_1 \dots i_h) \circ (bj_1 \dots j_k).$$

Ma allora, se $f = (a_1 b_1) \circ (a_2 b_2) \circ \dots \circ (a_n b_n)$ è un prodotto di trasposizioni, applicando più volte le formule precedenti si ha

$$\begin{aligned} N(f) &= N((a_2 b_2) \circ (a_3 b_3) \circ \dots \circ (a_n b_n)) \pm 1 \\ &= N((a_3 b_3) \circ (a_4 b_4) \circ \dots \circ (a_n b_n)) \pm 1 \pm 1 \\ &\vdots \\ &= N(a_n b_n) \underbrace{\pm 1 \pm 1 \pm \dots \pm 1}_{n-1 \text{ addendi}} = \underbrace{1 \pm 1 \pm \dots \pm 1}_{n \text{ addendi}}, \end{aligned}$$

ed è chiaro che il secondo membro è pari o dispari in accordo con n .

5.8. Dunque, per determinare la classe di una permutazione f basta sapere il numero delle trasposizioni che appaiono in una (qualunque) fattorizzazione di f in trasposizioni. Ne segue che se f e g sono due permutazioni di classe pari, allora il prodotto $f \circ g$ è ancora di classe pari, poiché una fattorizzazione in trasposizioni di $f \circ g$ si ottiene semplicemente giustapponendo una fattorizzazione di f ed una di g .

Esercizi

- 1) Se $f = (a_1 a_2 \dots a_n)$, si scriva f^{-1} .

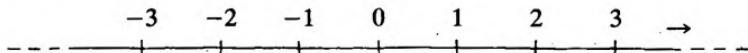
- 2) Cos'è $f \circ f$ se la permutazione f coincide con la propria inversa?
 3) Trovare la classe delle seguenti permutazioni

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 2 & 3 & 6 & 5 & 1 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 7 & 3 & 6 & 1 \end{pmatrix}$$

- 4) Quante sono le permutazioni di classe pari in Σ_4 ?
 5) Verificare che, se f è una permutazione, $(f^{-1})^{-1} = f$.
 6) Se f è una permutazione di classe dispari, che classe ha f^{-1} ?

§ 6. Numeri interi: induzione

6.1. L'insieme dei *numeri interi* $\mathbf{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ è il sistema numerico che si impara ad usare fin dalle scuole inferiori. Supporremo senz'altro note le proprietà delle operazioni fondamentali definite in \mathbf{Z} , cioè l'addizione e la moltiplicazione (proprietà che riassumeremo nel numero 12.) nonché la relazione $<$ (*minore di*) in base alla quale \mathbf{Z} viene *ordinato linearmente*. Qui $x < y$ (equivolentemente: $y > x$) significa che x precede y nel verso indicato.



6.2. I numeri interi maggiori di 0 si dicono positivi o *numeri naturali* e si denotano con il simbolo \mathbf{N} , ponendo cioè $\mathbf{N} = \{x \mid x \in \mathbf{Z}, x > 0\}$. Una importante proprietà degli interi positivi è il seguente

ASSIOMA DEL BUON ORDINAMENTO: *ogni insieme non vuoto di interi positivi possiede un elemento minimo.*

In altre parole: se $\emptyset \neq S \subseteq \mathbf{N}$, allora esiste $m \in S$ tale che $m \leq s$ per ogni $s \in S$. Si usa la parola *assioma* perché su questa proprietà (assieme a poche altre) si può fondare una precisa definizione di \mathbf{N} e di \mathbf{Z} (definizione cui abbiamo rinunciato di proposito a questo livello).

6.3. Come prima applicazione dell'assioma del buon ordinamento, deriviamo un'altra proprietà che porta il nome di *induzione* e sta alla base di molte dimostrazioni che incontreremo in seguito:

PRINCIPIO DI INDUZIONE O DI RICORRENZA (prima forma): *consideriamo, per ogni numero naturale n , un'asserzione $A(n)$ ad esso associata, e supponiamo di sapere che: 1) $A(1)$ è vera; 2) per ogni $k \in \mathbb{N}$, supposta vera $A(k)$, ne segue che è vera $A(k+1)$. Allora l'asserzione $A(n)$ è vera per ogni $n \in \mathbb{N}$.*

Dimostrazione: sia S l'insieme degli interi positivi per i quali l'asserzione non è vera $S = \{x \mid x \in \mathbb{N}, A(x) \text{ è falsa}\}$. Ci proponiamo di provare che S è vuoto. Supponiamo allora S non vuoto (ragionamento *per assurdo*) e proviamo che ne segue una contraddizione. Sia dunque $S \neq \emptyset$. Allora per l'assioma del buon ordinamento, S ha un minimo m . Dunque $A(m)$ è falsa (perché $m \in S$), mentre $A(1)$ è vera, ipotesi 1). Allora $m \neq 1$, quindi $m > 1$; poiché m è il minimo di S , $m-1 \notin S$ e perciò $A(m-1)$ è vera. Ma allora, per l'ipotesi 2), anche $A(m)$ è vera, perché $m = (m-1) + 1$. Così $A(m)$ sarebbe contemporaneamente vera e falsa; un controsenso. Si conclude che la eventualità $S \neq \emptyset$ non si può presentare, cioè S è vuoto, come volevamo.

6.4. Esempio di dimostrazione *per induzione*. Sia $A(n)$ l'asserzione: *la somma dei primi n numeri naturali dispari è uguale ad n^2* :

$$1 + 3 + 5 + \dots + (2n-1) = n^2.$$

Allora $A(1)$ è vera perché $1 = 1^2$, e dunque l'ipotesi 1) del principio di induzione è verificata. Supponiamo allora che $A(n)$ sia vera per un certo $n \in \mathbb{N}$; segue da ciò che anche $A(n+1)$ è vera? Osserviamo che la somma dei primi $n+1$ numeri naturali dispari si ottiene aggiungendo alla somma dei primi n il numero $2(n+1)-1 = 2n+1$; dunque questa somma vale $(1 + 3 + 5 + \dots + (2n-1)) + 2n+1 = n^2 + 2n + 1 = (n+1)^2$. Ma questa è proprio l'asserzione $A(n+1)$. Così anche l'ipotesi 2) del principio di induzione è verificata. Concludiamo *per induzione* che $A(n)$ è vera per ogni $n \in \mathbb{N}$.

6.5. Altro esempio: siano $x, y \in \mathbb{Z}$; dimostriamo che *per ogni $n \in \mathbb{N}$ si ha la FORMULA DEL BINOMIO*

$$(x+y)^n = x^n + nx^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \dots + nxy^{n-1} + y^n = \sum_{k=0}^n \binom{n}{k} x^{n-k}y^k.$$

Per $n=1$ l'asserzione è vera, perché $(x+y)^1 = x+y = \binom{1}{0}x + \binom{1}{1}y$.

Supponiamola vera per n . Allora risulta

$$\begin{aligned}(x+y)^{n+1} &= (x+y)^n(x+y) = \left(\sum_{k=0}^n \binom{n}{k} x^{n-k} y^k\right)(x+y) = \\ &= \sum_{k=0}^n \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^n \binom{n}{k} x^{n-k} y^{k+1}.\end{aligned}$$

Sostituendo l'indice k con l'indice $h = k+1$ e mettendo in evidenza l'ultimo addendo, la seconda sommatoria si può scrivere

$$\sum_{h=1}^n \binom{n}{h-1} x^{n-h+1} y^h + y^{n+1};$$

mettendo in evidenza il primo addendo, la prima sommatoria si può scrivere

$$x^{n+1} + \sum_{h=1}^n \binom{n}{h} x^{n-h+1} y^h.$$

Se ora usiamo la relazione $\binom{n}{h-1} + \binom{n}{h} = \binom{n+1}{h}$ che abbiamo dimostrato in 4.7., si ottiene:

$$\begin{aligned}(x+y)^{n+1} &= x^{n+1} + \sum_{h=1}^n \left[\binom{n}{h} + \binom{n}{h-1} \right] x^{n-h+1} y^h + y^{n+1} = \\ &= x^{n+1} + \sum_{h=1}^n \binom{n+1}{h} x^{n+1-h} y^h + y^{n+1} = \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} x^{(n+1)-k} y^k.\end{aligned}$$

Questo è l'asserto per $n+1$, quindi la formula è dimostrata *per induzione*, per qualsiasi $n \in \mathbb{N}$.

6.6. L'assioma del buon ordinamento vale, ovviamente, anche se al posto di \mathbb{N} si considera $\mathbb{N} \cup \{0\}$, l'insieme degli interi non negativi. Di conseguenza, nel principio di induzione, l'asserto rimane valido se si sostituiscono gli interi positivi con quelli non negativi; allora l'ipotesi $A(1)$ è *vera* va sostituita con $A(0)$ è *vera*.

6.7. PRINCIPIO DI INDUZIONE (seconda forma): *per ogni intero $n \geq 0$ consideriamo l'asserzione $A(n)$ e supponiamo di sapere che: 1) $A(0)$ è vera; 2) per*

ogni $m > 0$, se $A(k)$ è vera per ogni k soddisfacente a $0 \leq k < m$, allora anche $A(m)$ è vera. Allora $A(n)$ è vera per ogni $n \geq 0$.

Dimostrazione: Sia S l'insieme degli $s \geq 0$ per cui $A(s)$ è falsa. Supponiamo per assurdo $S \neq \emptyset$ e sia m il minimo. Allora $A(m)$ è falsa e quindi $m > 0$ perché per l'ipotesi 1) $A(0)$ è vera; mentre $A(k)$ è vera per ogni $k < m$ (perché m è il minimo di S). Ma allora, per l'ipotesi 2), $A(m)$ è vera: contraddizione.

6.8. Questa forma del principio di induzione, pur essendo una variazione della prima, fornisce un metodo di dimostrazione più potente: esistono cioè casi (vedi 6.9.) in cui è facile provare l'ipotesi 2) della seconda forma ma è meno facile provare l'ipotesi 2) della prima forma.

6.9. DIVISIONE: *Siano m, n numeri interi, con $m > 0$, $n \geq 0$. Allora esistono due interi q, r con $0 \leq r < m$ tali che: $n = mq + r$.*

Dimostrazione: Applichiamo il principio di induzione nella seconda forma (rispetto ad n). Se $n = 0$, basta porre $q = r = 0$: l'asserto $A(0)$ è vero. Sia $n > 0$. Vediamo se $A(n)$ segue dall'ipotesi che $A(k)$ sia vero per ogni k , con $0 \leq k < n$. Se $m > n$, basta porre $q = 0$, $r = n$. Se invece $m \leq n$, allora $0 \leq n - m < n$. Per l'ipotesi (*induttiva*) l'asserto $A(n - m)$ è vero: cioè esistono due numeri interi q_1, r_1 tali che $n - m = mq_1 + r_1$, $0 \leq r_1 < m$. Ma allora $n = m + mq_1 + r_1 = m(q_1 + 1) + r_1$ e questo è proprio $A(n)$. Per il principio di induzione $A(n)$ vale per ogni $n \geq 0$.

6.10. Il principio di induzione può essere usato per definire alcune applicazioni che abbiano per dominio l'insieme dei numeri naturali: precisamente, in base ad esso possiamo asserire di aver definito un'applicazione f di \mathbb{N} in un insieme X , se conosciamo $f(1)$ e abbiamo dato una regola che permette di calcolare $f(n)$ mediante i valori $f(k)$ con $k < n$. Ad esempio l'applicazione $f: \mathbb{N} \rightarrow \mathbb{N}$ che ad ogni n associa il suo fattoriale (vedi 4.4.) può essere definita da $f(1) = 1$, $f(n+1) = f(n) \cdot (n+1)$. Così la potenza (n -esima) di un numero intero z è (l'immagine di n secondo) l'applicazione $g: \mathbb{N} \rightarrow \mathbb{Z}$ definita da $g(1) = z$, $g(n+1) = g(n) \cdot z$.

Esercizi

- Usando il principio di induzione, si dimostri che se X è un insieme con un numero finito n di elementi, allora $\mathcal{P}(X)$ ha 2^n elementi.

§ 7. Divisione

7.1. Il *valore assoluto* (o *modulo*) è quell'applicazione $x \mapsto |x|$ di \mathbf{Z} in sé definita ponendo:

$$|x| = x \quad \text{se } x \geq 0; \quad |x| = -x \quad \text{se } x < 0.$$

Se $|x| = |y|$, allora $x = y$ oppure $x = -y$ (ciò si scriverà talvolta $x = \pm y$). In particolare, $|x| = 0$ se e solo se $x = 0$. Per ogni $x, y \in \mathbf{Z}$ valgono le relazioni

$$|x| + |y| \geq |x + y|; \quad |x| \cdot |y| = |x \cdot y|;$$

che si verificano esaminando tutte le possibili scelte di *segni* per x, y .

7.2. In 6.9. abbiamo già attribuito alla parola *divisione* di un numero intero positivo n per un altro m , il significato di determinazione di quel multiplo del divisore m che differisce dal dividendo n , per difetto, il meno possibile. Il seguente teorema precisa ed estende questa nozione ai numeri interi.

Siano $a, b \in \mathbf{Z}$, $b \neq 0$. Allora esistono due interi q, r tali che $a = bq + r$, $0 \leq r < |b|$. Gli interi q, r sono unici, nel senso che sono determinati univocamente dalle condizioni precedenti.

Dimostrazione dell'esistenza: Si potrebbe utilizzare con opportune modifiche la dimostrazione di 6.9., ma preferiamo rifarci direttamente al *principio del minimo*. Supponiamo anzitutto b positivo, quindi $|b| = b$. Consideriamo l'insieme $S = \{x \mid x = a - bz, z \in \mathbf{Z}, a - bz \geq 0\}$ cioè la totalità dei numeri interi non negativi della forma $a - bz$. Proviamo che S non è vuoto, facendo vedere che $S \ni a - b(-|a|) = a + b|a|$. Infatti è $b \geq 1$, quindi $b|a| \geq |a|$ e $a + b|a| \geq a + |a| \geq 0$. Ma allora S ammette minimo r che è del tipo $r = a - bq$. Abbiamo dunque già provato che $a = bq + r$, $r \geq 0$ e resta da provare $r < b$. Se infatti fosse, per assurdo, $r \geq b$, allora si avrebbe $0 \leq r - b = a - bq - b = a - b(q + 1) \in S$ ed $r - b < r$ contro l'ipotesi che r sia il minimo di S . Supponiamo adesso b negativo: allora osservando che $a = (-b)(-q) + r$, $-b = |b|$ il problema si riconduce al caso precedente:

si divide a per il numero positivo $-b$, si cambia segno al quoziente e si lascia inalterato il resto.

Unicità: proviamo che q, r sono gli unici interi che soddisfano alle condizioni poste. Sia infatti $a = bq + r = bq' + r'$, $0 \leq r, r' < |b|$, e supponiamo, ad esempio, $r' \geq r$. Allora $0 \leq r' - r = b(q - q')$. Passando ai valori assoluti, si ha $|b| \cdot |q - q'| = |b(q - q')| = r' - r \leq r' < |b|$. Ma ciò è possibile solo se $|q - q'| < 1$, e quindi $q = q'$. Sostituendo nelle equazioni iniziali si ottiene anche $r = r'$.

7.3. È bene guardarsi da un equivoco comune: sostituendo il dividendo a con il suo opposto $-a$, non è detto che si ottenga $-q$ come quoziente. Ad esempio

$$\begin{array}{lllll} 19 = 6 \cdot 3 + 1 & a = 19 & b = 6 & q = 3 & r = 1; \\ -19 = 6(-4) + 5 & a = -19 & b = 6 & q = -4 & r = 5. \end{array}$$

7.4. Se $a, b \in \mathbb{Z}$, diremo che b divide a (espressioni equivalenti: a è multiplo di b , b è divisore di a) e scriveremo $b \mid a$ se esiste un intero z tale che $a = bz$. Se b non divide a , si scriverà $b \nmid a$. Ad esempio: $5 \mid 15$, $-3 \mid 3$, $2 \nmid -3$. Se $b \neq 0$, allora $b \mid a$ se e soltanto se la divisione di a per b dà resto zero. Se invece $b = 0$, allora $b \mid a$ comporta $a = 0z = 0$.

7.5. Osserviamo che se $b_1, b_2, b_3 \in \mathbb{Z}$, da $b_1 \mid b_2$ e $b_2 \mid b_3$ segue che $b_1 \mid b_3$; infatti si ha $b_2 = b_1 z_1$, $b_3 = b_2 z_2$ e quindi $b_3 = b_1(z_1 z_2)$. Due interi che si dividono l'uno l'altro sono eguali o opposti; infatti, se $b_1 \mid b_2$, $b_2 \mid b_1$, allora $b_2 = b_1 z_1$, $b_1 = b_2 z_2$ e quindi $b_1 = b_1(z_1 z_2)$ cioè $b_1(1 - z_1 z_2) = 0$. Poiché il prodotto di due interi è nullo se e solo se è nullo almeno uno dei fattori, si presentano due possibilità: 1) $b_1 = 0$, dunque anche $b_2 = b_1 z_1 = 0$; 2) $(1 - z_1 z_2) = 0$, dunque $z_1 z_2 = 1$. Ma il prodotto di due interi vale 1 se e solo se i due fattori sono entrambi 1 oppure entrambi -1 : $z_1 = z_2 = \pm 1$. In ogni caso possiamo concludere $b_1 = \pm b_2$. Viceversa è chiaro che $x \mid x$, $-x \mid x$ per ogni $x \in \mathbb{Z}$.

7.6. Poiché gli interi $1, -1$ dividono ogni altro intero, tra i divisori di un intero a dobbiamo annoverare i numeri: $1, -1, a, -a$. Per qualche numero intero a l'elenco dei divisori termina qui. Ad esempio, se $a = -7$, i divisori sono soltanto $1, -1, 7, -7$. L'intero p si dice *primo* se $p \neq \pm 1$ e i suoi divisori sono soltanto $\pm 1, \pm p$. Ad esempio, 4 non è primo, perché $2 \mid 4$, $2 \neq \pm 1$, $2 \neq \pm 4$; 0 non è primo perché $x \mid 0$ qualunque sia x (infatti $0 = x \cdot 0$); -1 e 1 non sono primi per definizione. Sono numeri primi ± 2 , ± 3 , ± 5 , $\pm 7 \dots$. Lo studio dei numeri primi è l'obiettivo principale della teoria dei numeri.

Esercizi

- 1) Si provi, per induzione su n , che se $x_1, x_2, \dots, x_n \in \mathbf{Z}$, allora

$$|x_1 + x_2 + \dots + x_n| \leq |x_1| + |x_2| + \dots + |x_n|.$$

- 2) Si trovino quoziente q e resto r della divisione di $a = 630$ per $b = -132$.
Lo stesso per $a = -71$, $b = 36$.
- 3) Come si modificano q ed r se a, b si sostituiscono con i multipli ma, mb ?
- 4) Si trovino tre interi a, b, c tali che $a \nmid b$, $a \nmid c$, $a \mid bc$.

§ 8. Massimo comune divisore

8.1. Un intero d si dirà un *massimo comune divisore* (brevemente M.C.D.) degli interi a, b (non entrambi nulli) se e solo se

- 1) d divide entrambi: $d \mid a$, $d \mid b$;
- 2) d è multiplo di ogni intero che divida entrambi:

se $z \mid a$, $z \mid b$, allora $z \mid d$.

Ad esempio -8 è un M.C.D. di 24 e -32 . Infatti, osservato che i divisori comuni di 24 e -32 sono: ± 1 , ± 2 , ± 4 , ± 8 , si verifica che fra i divisori comuni di 24 e -32 c'è -8 e che tutti i divisori comuni dividono -8 . Notiamo che alle medesime condizioni soddisfa il numero 8 , ma nessun altro intero. Questo fatto è del tutto generale: se d, d' sono due M.C.D. di a, b , allora la condizione 1) per d' e la condizione 2) per d comportano $d' \mid d$ e scambiando i ruoli otteniamo $d \mid d'$. Ma allora per 7.5. otteniamo $d = d'$ oppure $d = -d'$. In conclusione possiamo sempre scegliere un M.C.D. positivo: questo particolare M.C.D. di a, b si denoterà con il simbolo (a, b) . Visto così che (a, b) se esiste, è unico, rimane da vedere che esiste. Per dimostrare l'esistenza consideriamo l'insieme $S = \{s \mid s = ax + by; x, y \in \mathbf{Z}, s > 0\}$, cioè la totalità degli interi positivi della forma $ax + by$. Poiché a, b non sono entrambi nulli, S non è vuoto, e perciò contiene un elemento minimo $d = at + bs$. Proviamo che risulta $d = (a, b)$. Dividendo a per d scriviamo $a = dp + r$, $0 \leq r < d$. Allora $r = a - dq = a - (at + bs)q = a(1 - tq) + b(-sq)$.

Dunque r è del tipo $ax + by$; se fosse $r > 0$ sarebbe $S \ni r < d$, in contrasto con la minimalità di d . Ne segue $r = 0$ e quindi $d \mid a$. Analogamente $d \mid b$, e la condizione 1) per il M.C.D. è soddisfatta. Quanto alla 2) si osservi che $z \mid a$, $z \mid b$ comportano $a = zc_1$, $b = zc_2$ e quindi

$$d = at + bs = zc_1t + zc_2s = z(c_1t + c_2s) \quad \text{ossia } z \mid d.$$

8.2. ALGORITMO DI EUCLIDE. Diamo ora un procedimento di calcolo che permette l'effettiva determinazione di (a, b) . Osserviamo intanto che nelle ultime righe abbiamo incidentalmente dimostrato che se $z \mid a$, $z \mid b$, allora $z \mid ax + by$ per ogni $x, y \in \mathbb{Z}$.

Si debba calcolare, ad esempio, $(72, 22)$. Dividiamo successivamente 72 per 22, poi 22 per il resto, il primo resto per il secondo resto e così via, fino a ottenere resto 0.

$$\begin{aligned} 72 &= 22 \cdot 3 + 6 \\ 22 &= 6 \cdot 3 + 4 \\ 6 &= 4 \cdot 1 + 2 \\ 4 &= 2 \cdot 2 + 0 \end{aligned}$$

Affermiamo che l'ultimo resto positivo è il M.C.D.: $(72, 22) = 2$; infatti, leggendo le divisioni precedenti dall'ultima alla prima, e tenendo conto della osservazione preliminare, si ottiene: $2 \mid 4$; $2 \mid 6$ perché $2 \mid 2$, $2 \mid 4$; $2 \mid 22$ perché $2 \mid 4$, $2 \mid 6$; $2 \mid 72$, perché $2 \mid 6$, $2 \mid 22$. Allora il numero 2 soddisfa alla condizione 1) per il M.C.D.. Inoltre se $z \mid 72$, $z \mid 22$, leggendo le divisioni dalla prima all'ultima, si ottiene rispettivamente: $z \mid 6$ perché $6 = 72 \cdot 1 + 22(-3)$, $z \mid 72$, $z \mid 22$; $z \mid 4$ perché $z \mid 22$, $z \mid 6$; $z \mid 2$ perché $z \mid 6$, $z \mid 4$. E la condizione 2) è provata.

Osserviamo che l'algoritmo euclideo è applicabile ad ogni coppia a, b di interi non entrambi nulli (si incomincerà col dividere a per b , oppure b per a) quindi fornisce un'ulteriore dimostrazione dell'esistenza del M.C.D.. Anzi, l'algoritmo risolve il problema di determinare gli interi t, s che in 8.1. fornivano $d = at + bs$. Infatti utilizzando le divisioni precedenti, dall'ultima alla prima, otteniamo:

$$\begin{aligned} 2 &= 6 + 4(-1) = 6 + (22 + 6(-3))(-1) = 22(-1) + 6(1 + (-3)(-1)) = \\ &= 22(-1) + (72 + 22(-3))4 = 22(-13) + 72(4). \end{aligned}$$

Si è trovato dunque $t = -13$, $s = 4$.

8.3. Due numeri interi si dicono *primi tra loro* (sinonimo: *coprimi*) se il loro M.C.D. è l'unità. Le considerazioni precedenti forniscono il seguente

criterio: *due interi a, b sono coprimi se e soltanto se $1 = ax + by$ per opportuni interi x, y .* Sia, ad esempio, $b = a + 1$; allora $1 = b - a = a(-1) + b(1)$ e quindi $(a, b) = 1$. Altra applicazione: dividendo due interi a, b per il loro M.C.D. si ottengono due numeri coprimi. Infatti se $a = (a, b)a_1$ e $b = (a, b)b_1$ dalla relazione $(a, b) = ax + by = (a, b)a_1x + (a, b)b_1y$ si ottiene, semplificando per (a, b) , $1 = a_1x + b_1y$.

8.4. Un'importante proprietà dei numeri primi è la seguente: *se un primo divide un prodotto, allora esso divide uno dei fattori.* Si otterrà questo risultato come caso particolare del seguente lemma:

$$\text{se } c \mid ab \text{ e } (a, c) = 1, \text{ allora } c \mid b.$$

Dimostrazione: Sappiamo che $1 = cx + ay$ per opportuni $x, y \in \mathbb{Z}$. Moltiplicando per b otteniamo $b = cbx + aby$. Ma, per ipotesi $ab = cz$ per qualche $z \in \mathbb{Z}$, quindi $b = c(bx + zy)$, ossia $c \mid b$. In particolare:

$$\text{se } p \text{ è primo allora } p \mid ab \text{ implica } p \mid a \text{ oppure } p \mid b.$$

Dimostrazione: Per definizione i divisori di p sono soltanto ± 1 e $\pm p$. Se allora $p \nmid a$, i divisori comuni di p ed a sono ± 1 . Allora $(p, a) = 1$ e si applica il lemma precedente.

Osserviamo infine che se $a \mid m$, $c \mid m$, e $(a, c) = 1$, allora $ac \mid m$.

Dimostrazione: Per ipotesi $m = ab$ per qualche b ; per il lemma precedente $c \mid b$ ossia $b = cz$ ed infine $m = ab = acz$.

8.5. Diciamo che m è un *minimo comune multiplo* (brevemente: m.c.m.) degli interi a, b (non entrambi nulli) se e solo se

- 1) m è multiplo di entrambi: $a \mid m$, $b \mid m$;
- 2) m è divisore di ogni intero che sia multiplo di entrambi:

$$\text{se } a \mid z, b \mid z, \text{ allora } m \mid z.$$

Ad esempio, 96 è un m.c.m. di 24 e -32: la 1) è subito verificata, ma la 2) si prova meno facilmente. Dimostriamo perciò un teorema che riconduce il calcolo del m.c.m. a quello del M.C.D. Osserviamo anzitutto che il m.c.m. è individuato a meno del segno: la dimostrazione è pressoché identica all'analogia per il M.C.D. Dopodiché si indicherà con il simbolo $[a, b]$ il m.c.m. non negativo dei numeri a, b . Il teorema che segue fornisce ad un tempo la dimostrazione dell'esistenza ed un metodo di calcolo.

$$\text{Se } a, b \in \mathbb{Z}, \text{ allora } (a, b) [a, b] = |ab|.$$

Dimostrazione: Dividendo ab per (a, b) otteniamo evidentemente resto 0:

$ab = (a,b)q$. Si tratta di provare che q soddisfa alle condizioni 1) e 2) della definizione di m.c.m.. Scriviamo infatti $a = (a,b)a_1$ e $b = (a,b)b_1$. Moltiplicando rispettivamente per b e per a otteniamo:

$$(a,b)q = ab = (a,b)a_1b = (a,b)ab_1.$$

Semplificando si ottiene la 1): $q = a_1b = ab_1$. Quanto alla 2), se $a|z$, $b|z$ possiamo scrivere $z = (a,b)z_1$. Si trova, come prima: $a_1|z_1$, $b_1|z_1$. Poiché a_1 , b_1 sono coprimi (cfr. 8.3.), l'osservazione prima di 8.5. fornisce $a_1b_1|z_1$ cosicché $q = a_1b_1 = (a,b)$ divide $z = z_1(a,b)$ e dunque la 2) è verificata.

8.6. La nozione di M.C.D. si estende facilmente a più di due numeri: l'intero d si dice un M.C.D. degli interi a_1, a_2, \dots, a_n (non tutti nulli) se

- 1) d divide ciascun a_i ($i = 1, 2, \dots, n$);
- 2) d è multiplo di ogni intero che divida ciascun a_i ($i = 1, 2, \dots, n$).

L'esistenza si può dimostrare ricorrendo al minimo dell'insieme $S = \{s \mid s = a_1x_1 + a_2x_2 + \dots + a_nx_n; x_i \in \mathbb{Z}; s > 0\}$ e procedendo in modo analogo a quanto abbiamo fatto al paragrafo 8.1. Il M.C.D. risulta ancora individuato a meno del segno e se ne indica con (a_1, a_2, \dots, a_n) il valore positivo. Si dimostra che risulta $(a_1, a_2, \dots, a_n) = ((a_1, a_2, \dots, a_{n-1}), a_n)$ (si svolga l'esercizio 3 e si applichi l'induzione su n), e quindi anche il M.C.D. di più di due numeri si può calcolare con successive applicazioni dell'algoritmo di Euclide.

Anche il m.c.m. $[a_1, a_2, \dots, a_n]$ si può definire per analogia. Per provare l'esistenza di un m.c.m., invece di parafrasare l'8.5., conviene ricorrere al minimo dell'insieme $S = \{s \mid s \in \mathbb{Z}, s \geq 0, a_i|s \text{ per ogni } i = 1, 2, \dots, n\}$.

Lasciamo agli esercizi i dettagli.

Esercizi

- 1) Si calcoli, con procedimento delle divisioni successive, $(630, 132)$.
- 2) Si trovino $s, t \in \mathbb{Z}$ tali che $1 = 54s + 19t$. Sono s, t individuati da questa condizione?
- 3) Si dimostri che $((a, b), c) = (a, b, c) = (a, (b, c))$ per ogni $a, b, c \in \mathbb{Z}$.

§ 9. Fattorizzazione unica

9.1. TEOREMA FONDAMENTALE DELL'ARITMETICA: *ogni intero maggiore di 1 si può esprimere come prodotto di numeri primi positivi. Questa espressione è unica a meno dell'ordine in cui compaiono i fattori.*

Dimostrazione: Proviamo anzitutto l'esistenza di una tale fattorizzazione. Supponiamo, per assurdo, che esistano interi > 1 che non si lasciano esprimere come prodotto di primi, e sia m il minimo di essi. Allora m non è primo, e quindi ammette divisori diversi da ± 1 , $\pm m$; dunque, per opportuni $q, n > 1$, risulta $m = nq$. Ma allora n, q sono minori di m , e quindi, per la minimalità di m , essi si esprimono come prodotti di primi: $n = p_1 p_2 \cdots p_r$, $q = p'_1 p'_2 \cdots p'_s$. Si ottiene $m = p_1 p_2 \cdots p_r p'_1 p'_2 \cdots p'_s$, una contraddizione. Concludiamo che per ogni $n > 1$ si ha $n = p_1 p_2 \cdots p_t$ per opportuni primi positivi p_i .

Quanto all'unicità, supponiamo che sia anche $n = p'_1 p'_2 \cdots p'_u$ una fattorizzazione in primi positivi. Allora p_1 divide $n = p'_1 (p'_2 \cdots p'_u)$. Per quanto si è visto in 8.4., $p_1 | p'_1$ oppure $p_1 | (p'_2 \cdots p'_u)$. Nel primo caso $p_1 = p'_1$ (perché si tratta di primi positivi); nel secondo caso si trova $p_1 | p'_2$ oppure $p_1 | (p'_3 \cdots p'_u)$. Così procedendo si arriva a trovare $p_1 = p'_j$ per qualche $j \leq u$. I fattori primi si possono riordinare in modo che p'_j sia al primo posto ($j = 1$); allora $n = p_1 p_2 \cdots p_t = p_1 p'_2 \cdots p'_u$ da cui $p_2 p_3 \cdots p_t = p'_2 p'_3 \cdots p'_u$. Si ripete il procedimento fintantoché non si esauriscono i fattori p_i . Allo stesso tempo si devono esaurire i p'_j . Si conclude che nelle due fattorizzazioni compare lo stesso numero di fattori ($t = u$), anzi compaiono i medesimi fattori primi, al più disposti in ordine diverso.

9.2. Nella fattorizzazione di n il medesimo primo può comparire più volte. È conveniente riordinare i fattori in modo da ravvicinare i primi eguali. Allora, se p_1, p_2, \dots, p_v sono i fattori primi distinti nella fattorizzazione di m , si scrive $m = p_1^{n_1} p_2^{n_2} \cdots p_v^{n_v}$ e gli interi positivi n_1, n_2, \dots, n_v sono individuati univocamente da m . Con riferimento a vari problemi di divisibilità, è conveniente scrivere tutti i numeri in questione (che supporremo per semplicità

positivi) a, b, \dots come prodotti di potenze dei medesimi numeri primi (distinti): $a = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$; $b = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ ecc. Ciò è sempre possibile purché si ammettano valori nulli per gli esponenti m_i, n_i ecc.

9.3. L'unicità della fattorizzazione ci garantisce che, facendo uso di questa rappresentazione per a, b , risulta $a|b$ se e solo se $m_i \leq n_i$ per ogni $i = 1, 2, \dots, t$. Questa osservazione sta alla base del metodo tradizionale di calcolo del M.C.D.: $(a, b) = p_1^{w_1} p_2^{w_2} \cdots p_t^{w_t}$ ove w_i è il minimo tra m_i e n_i . Inoltre $[a, b] = p_1^{z_1} p_2^{z_2} \cdots p_t^{z_t}$ ove z_i è il massimo fra m_i e n_i .

9.4. Ecco una classica applicazione del teorema fondamentale: *Esistono infiniti numeri primi.*

Dimostrazione Se infatti i primi fossero in numero finito: p_1, p_2, \dots, p_t , allora il numero $m = p_1 p_2 \cdots p_t + 1$ sarebbe coprimo con $p_1 p_2 \cdots p_t$ (cfr. 8.3), e dunque con ogni primo p_i . Ma allora m non potrebbe essere un prodotto di primi, in contrasto col teorema fondamentale.

9.5. Assegnato l'intero positivo n , quanti tra i numeri $1, 2, \dots, n$ sono primi con n ? Qual è, cioè, il numero $\varphi(n)$ degli $x \in \mathbb{N}$ tali che $1 \leq x \leq n$, $(x, n) = 1$? La funzione $\varphi: \mathbb{N} \rightarrow \mathbb{N}$ così definita si chiama *funzione φ (ovvero indicatore) di Eulero*. Ad esempio, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, ecc. In qualche caso il calcolo di $\varphi(n)$ è semplice. Ad esempio, se p è primo, allora $\varphi(p) = p - 1$; si vede anche subito che $\varphi(p^n) = p^n - p^{n-1}$: ciò si ottiene osservando che non sono primi con p^n i soli multipli di p : $p, 2p, \dots, p^n - p, p^n$. Per calcolare $\varphi(n)$ nel caso generale basta provare (e lo faremo nel paragrafo 11.12.) che $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$ se $(r, s) = 1$. Allora se $n = p_1^{n_1} \cdots p_r^{n_r}$ (p_i primi distinti) si calcola subito:

$$\varphi(n) = (p_1^{n_1} - p_1^{n_1-1}) (p_2^{n_2} - p_2^{n_2-1}) \cdots (p_r^{n_r} - p_r^{n_r-1}).$$

Ad esempio, $\varphi(72) = \varphi(2^3 \cdot 3^2) = \varphi(2^3) \varphi(3^2) = (2^3 - 2^2)(3^2 - 3) = 24$.

Esercizi

- 1) Si verifichi la regola data in 9.3. per il calcolo del M.C.D. e m.c.m. di due numeri, partendo dalla fattorizzazione in primi.
- 2) Si estenda la regola di cui sopra al caso di $n (> 2)$ numeri.
- 3) Se $a = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ (primi distinti), quanti sono i divisori di a ?

§ 10. Scrittura b -adica

La *notazione* che abbiamo sempre adoperato per gli interi è quella *decimale* o *10-adica* o *in base 10*. Con ciò intendiamo ad esempio che al simbolo 3502 si associa il numero $3 \cdot 10^3 + 5 \cdot 10^2 + 0 \cdot 10 + 2$; la notazione è cioè la seguente: se un numero si ottiene dalla somma

$$A_r \cdot 10^r + A_{r-1} \cdot 10^{r-1} + \dots + A_1 \cdot 10 + A_0 \quad \text{con } 0 \leq A_i < 10,$$

allora tale numero si scrive giustapponendo (non moltiplicando!) gli A_i nell'ordine $A_r A_{r-1} \dots A_1 A_0$. Ci proponiamo di illustrare come il ruolo del numero 10 in questa notazione possa essere svolto da ogni intero $b \geq 2$. Ad esempio, per $b = 7$ abbiamo

$$3502 = 1 \cdot 7^4 + 3 \cdot 7^3 + 1 \cdot 7^2 + 3 \cdot 7 + 2.$$

La notazione 7-adica per il decimale 3502 è dunque 13132. La determinazione delle cifre A_i si ottiene mediante successive divisioni per 7:

$$\begin{aligned} 3502 &= 7 \cdot 500 + 2 \\ 500 &= 7 \cdot 71 + 3 \\ 71 &= 7 \cdot 10 + 1 \\ 10 &= 7 \cdot 1 + 3 \\ 1 &= 7 \cdot 0 + 1. \end{aligned}$$

Si dividono cioè i quozienti successivi per 7 fino ad ottenere quoziente 0. I resti forniscono, nell'ordine inverso, le cifre della notazione 7-adica. Infatti sostituendo ciascuna eguaglianza nella precedente, si ottiene:

$$\begin{aligned} 3502 &= 7 \cdot 500 + 2 = 7(7 \cdot 71 + 3) + 2 = 7^2 \cdot 71 + 7 \cdot 3 + 2 = \\ &= 7^2(7 \cdot 10 + 1) + 7 \cdot 3 + 2 = 7^3 \cdot 10 + 7^2 \cdot 1 + 7 \cdot 3 + 2 = \\ &= 7^3(7 \cdot 1 + 3) + 7^2 \cdot 1 + 7 \cdot 3 + 2 = 7^4 \cdot 1 + 7^3 \cdot 3 + 7^2 \cdot 1 + 7 \cdot 3 + 2. \end{aligned}$$

Seguendo la falsariga di questo esempio si può provare la parte *esistenza* del seguente teorema:

Sia $b \geq 2$ un intero fissato. Allora ogni intero positivo m si scrive in modo unico nella forma

$$m = a_r b^r + a_{r-1} b^{r-1} + \dots + a_1 b + a_0$$

con $a_r \neq 0$, $0 \leq a_i < b$ per $i = 0, 1, \dots, r$.

Per dimostrare l'unicità, supponiamo che $m = a'_s b^s + \dots + a'_0$ sia pure una rappresentazione b -adica di m . Allora a'_0 è il resto della divisione di m per b è quindi $a_0 = a'_0$. Anche i quozienti devono coincidere $a'_s b^{s-1} + \dots + a'_1 = a_s b^{s-1} + \dots + a_1$ e così proseguendo $a'_1 = a_1$, $a'_2 = a_2$, ecc.

Particolare importanza ha recentemente assunto il sistema di numerazione 2-adica (detto anche *binario*), perchè l'uso delle sole cifre 0, 1 corrisponde alle esigenze dei dispositivi elettronici. Naturalmente il passaggio dalla notazione decimale a quella binaria comporta un aumento del numero delle cifre (precisamente: in base b hanno al più r cifre i primi b^r numeri interi). Ad esempio 3502 in base 2 si scrive 110110101110.

Anche in base b le somme e i prodotti si possono calcolare, mutatis mutandis, con le consuete regole: ad esempio le operazioni $7 + 5 = 12$ e $7 \cdot 5 = 35$ nella notazione binaria si scrivono:

$$\begin{array}{r} 111 + \\ 101 \\ \hline 1100 \end{array} \quad \begin{array}{r} 111 \times \\ 101 \\ \hline 111 \\ 111 \\ \hline 100011 \end{array}$$

§ 11. Congruenze

11.1 Assegnato un intero non nullo m , diremo che due interi x, y sono *congrui modulo m* e scriveremo $x \equiv y \pmod{m}$ se essi differiscono per un multiplo di m , cioè se $m | (x - y)$. Ad esempio $14 \equiv 2 \pmod{12}$, $-5 \equiv 55 \pmod{10}$. Se x non è congruo ad y modulo m , scriviamo $x \not\equiv y \pmod{m}$. Ad esempio $3 \not\equiv 5 \pmod{3}$. Naturalmente $x \equiv y \pmod{0}$ se e solo se $x = y$.

11.2 Un criterio per stabilire la congruenza di due numeri è il seguente:

due interi x, y sono congrui modulo m ($\neq 0$) se e solo se, divisi per m , danno luogo al medesimo resto. Sia infatti $x = mq_1 + r_1$, $y = mq_2 + r_2$, $0 \leq r_1, r_2 < m$. Se $r_1 = r_2$ allora $x - y = m(q_1 - q_2)$ cioè $x \equiv y \pmod{m}$. Viceversa da $x \equiv y \pmod{m}$ segue per qualche $z \in \mathbb{Z}$,

$$y = x + mz \quad \text{quindi} \quad y = mq_1 + r_1 + mz = m(q_1 + z) + r_1.$$

Per l'unicità del (quoziante e del) resto nella divisione euclidea, si conclude $q_1 + z = q_2$ e $r_2 = r_1$.

11.3 Per la congruenza, modulo un prefissato intero m , valgono proprietà che richiamano quelle delle uguaglianze: ad esempio, per ogni $x, y, z \in \mathbb{Z}$

- | | |
|---|--------------|
| a) $x \equiv x$, | RIFLESSIVITÀ |
| b) se $x \equiv y$ allora $y \equiv x$, | SIMMETRIA |
| c) se $x \equiv y$ e $y \equiv z$ allora $x \equiv z$, | TRANSITIVITÀ |
| d) se $x \equiv y$ allora $x + z \equiv y + z$, | |
| e) se $x \equiv y$ allora $xz \equiv yz$. | |

Tutte queste proprietà sono facili conseguenze della definizione: ad esempio, la transitività si prova osservando che se $m|(x - y)$ e se $m|(y - z)$ allora m divide $x - z = (x - y) + (y - z)$.

11.4 È bene osservare che l'ultima proprietà di 11.3 non si inverte. Ad esempio $7 \cdot 2 \equiv 1 \cdot 2 \pmod{12}$ non comporta $7 \equiv 1 \pmod{12}$. Questo avviene perché il fattore 2, che si vorrebbe cancellare in entrambi i membri, è un divisore del modulo. Vale però la seguente proprietà: se z è primo con m , allora da $xz \equiv yz \pmod{m}$ segue $x \equiv y \pmod{m}$. Infatti per ipotesi m divide $xz - yz = (x - y)z$ ed $(m, z) = 1$. Ma allora, come si è visto in 8.4, $m|(x - y)$ come si voleva.

11.5 PROBLEMA: assegnati $m, b, c \in \mathbb{Z}$ esiste un intero x tale che risulti $cx \equiv b \pmod{m}$? Proveremo che una soluzione x di questa congruenza esiste se e solo se $(m, c) | b$.

Dimostrazione: necessità. Se questa congruenza ha soluzione, allora, per qualche $y \in \mathbb{Z}$ si ha $cx - b = my$, e quindi $b = cx - my$ è un multiplo di (m, c) (cfr. 8.1.). *Sufficienza.* Viceversa supponiamo che (m, c) sia un divisore di b ; poiché (cfr. 8.1.) (m, c) si scrive nella forma $ct + ms$ (per opportune scelte di $t, s \in \mathbb{Z}$) allora, per qualche $z \in \mathbb{Z}$, si ha $b = (m, c)z = (ct + ms)z$, da cui risulta $c(tz) - b = -m(sz)$ e $c(tz) \equiv b \pmod{m}$. Ma allora tz è una soluzione.

11.6. Ad esempio, la congruenza $6x \equiv 5 \pmod{4}$ non ha soluzioni perché $2 = (4,6) \nmid 5$. Invece la congruenza $12x \equiv 15 \pmod{39}$ ha soluzioni perché $3 = (39,12) \mid 15$. Per determinare una soluzione si può seguire la dimostrazione di 11.5. (applicando l'algoritmo di Euclide). Si trova:

$$3 = 1 \cdot 39 + (-3) \cdot 12, \quad 15 = 5 \cdot 3 = 5 \cdot 39 + (-15) \cdot 12,$$

da cui si ottiene $12 \cdot (-15) \equiv 15 \pmod{39}$, cioè -15 è una soluzione.

11.7. Se x è una soluzione della congruenza $cx \equiv b \pmod{m}$ allora è una soluzione anche $x + zm/(m,c)$ per ogni scelta di $z \in \mathbb{Z}$. Infatti risulta $c(x + zm/(m,c)) = cx \pm z[m,c] = b + my \pm z[m,c]$ ove si è sfruttata la egualianza $[m,c] \cdot (m,c) = |mc|$ (cfr. 8.5.). Ora $z[m,c]$ è multiplo di m , e quindi $c(x + zm/(m,c)) \equiv b \pmod{m}$ come si voleva. Viceversa, se x, x' sono due soluzioni, allora $cx = b + my$ e $cx' = b + my'$ con $y, y' \in \mathbb{Z}$, quindi risulta $c(x - x') = m(y - y')$ e, infine, $(c/(m,c))(x - x') = (m/(m,c))(y - y')$. Ora $c/(m,c)$ e $m/(m,c)$ sono primi fra loro e quindi $m/(m,c) \mid (x - x')$. In altre parole $x' = x + zm/(m,c)$ per qualche $z \in \mathbb{Z}$. Si conclude che, una volta determinata una soluzione particolare, tutte le altre si ottengono da essa aggiungendole un arbitrario multiplo di $m/(m,c)$. Nell'esempio di 11.6 la soluzione generale è dunque

$$x = -15 + z \cdot 13, \quad \text{con } z \in \mathbb{Z}.$$

11.8. Un importante corollario è il seguente. Sia p un numero primo e sia c un intero non divisibile per p . Allora la congruenza $cx \equiv b \pmod{p}$ ammette soluzione; tutte le soluzioni differiscono per multipli di p . (Si usa dire perciò che la soluzione è unica modulo p). Se, ad esempio, $p = 7$, $b = 1$, allora si trovano le congruenze:

$$1 \cdot 1 \equiv 1 \quad 2 \cdot 4 \equiv 1 \quad 3 \cdot 5 \equiv 1 \quad 6 \cdot 6 \equiv 1 \pmod{7}$$

11.9 TEOREMA CINESE DEL RESTO: Siano r, s interi primi tra loro. Allora le congruenze $x \equiv a \pmod{r}$, $x \equiv b \pmod{s}$ hanno una soluzione comune. La soluzione generale si ottiene aggiungendo ad una soluzione particolare un arbitrario multiplo di rs .

Infatti, per ogni $y \in \mathbb{Z}$, $x = a + yr$ è una soluzione della prima congruenza. Tale x è soluzione anche della seconda se e solo se $a + yr \equiv b \pmod{s}$, cioè $yr \equiv b - a \pmod{s}$. Come si è visto in 11.5, un tale y esiste, perché per ipotesi $(r,s) = 1$. Infine, se anche x^* è soluzione delle due congruenze iniziali, allora $x - x^* \equiv 0 \pmod{r}$ e $x - x^* \equiv 0 \pmod{s}$. Ma allora $x - x^*$ è multiplo di r e di s , quindi anche di $[r,s] = rs$. Viceversa è chiaro che se x è soluzione, anche $x + rsz$ lo è per ogni $z \in \mathbb{Z}$.

Esempio. Per risolvere il sistema delle congruenze

$$x \equiv 1 \pmod{6} \quad x \equiv 5 \pmod{7}$$

si scrive $1 + 6y \equiv 5 \pmod{7}$, quindi $6y \equiv 4 \pmod{7}$. Si trovano ad esempio per x, y i valori particolari 19 e 3 e dunque la soluzione generale

$$x = 19 + 42z.$$

11.10. Per ogni $x, y \in \mathbb{Z}$ e per ogni primo p , $(x+y)^p \equiv x^p + y^p \pmod{p}$.

Per il teorema del binomio (cfr. 6.5.) sappiamo che

$$(x+y)^p = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k + y^p.$$

Perciò è sufficiente dimostrare che la sommatoria è divisibile per p . Ma dalla definizione di $\binom{p}{k}$ si vede che p divide $\binom{p}{k}$ per $1 \leq k \leq p-1$ e quindi p divide anche $\sum_{k=1}^{p-1} \binom{k}{p} x^{p-k} y^k$.

11.11. TEOREMA DI FERMAT: Se a è un intero e p un primo, allora
 $a^p \equiv a \pmod{p}$.

Dimostrazione: supponiamo anzitutto $a \geq 0$ e usiamo l'induzione. Se $a = 0$ il risultato è banale. Sia vero l'asserto per un certo intero a : $a^p \equiv a \pmod{p}$. Allora per 11.10. $(a+1)^p \equiv a^p + 1^p$; ma $1^p \equiv 1$ e $a^p \equiv a$ comportano $(a+1)^p \equiv a+1$, cioè l'asserto è vero per $a+1$. Per il principio di induzione il teorema è provato per ogni $a \geq 0$. Consideriamo adesso il caso $a < 0$. Allora risulta $0 \equiv 0^p \equiv (a+(-a))^p \equiv a^p + (-a)^p \pmod{p}$. Ora $-a > 0$, e quindi $(-a)^p \equiv -a$ per il risultato precedente. Si conclude $0 \equiv a^p - a$ come si voleva. Ad esempio $2 \equiv 2^5 = 32 \pmod{5}$; $3 \equiv 3^5 = 243 \pmod{5}$.

11.12. Applichiamo il teorema cinese del resto per dimostrare la seguente relazione per la funzione di Eulero: $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$ se $(r, s) = 1$, relazione che abbiamo anticipata al numero 9.5.

Sia $U = \{u_1, u_2, \dots, u_{\varphi(r)}\}$ l'insieme dei numeri interi x tali che $1 \leq x \leq r$, $(x, r) = 1$. Siano $V = \{v_1, v_2, \dots, v_{\varphi(s)}\}$ e $W = \{w_1, w_2, \dots, w_{\varphi(rs)}\}$ gli analoghi insiemi, relativi a s ed rs . Ci proponiamo di definire una biiezione $f: U \times V \rightarrow W$, e dunque di provare che W possiede $\varphi(r)\varphi(s)$ elementi.

Sia $(u, v) \in U \times V$; il teorema di 11.10. afferma allora che le congruenze $z \equiv u \pmod{r}$, $z \equiv v \pmod{s}$ hanno una soluzione comune, e anzi che ne esiste una (sola) che soddisfa all'ulteriore condizione $1 \leq z \leq rs$. Chiamia-

mo w questa soluzione; w è primo con r (perché lo è u , che è congruo a w ($\text{mod } r$)); w è primo con s (perché lo è v); dunque w è primo con rs (perché r,s sono coprimi) e in definitiva $w \in W$. Ponendo allora $f(u,v) = w$ si definisce un'applicazione $f: U \times V \rightarrow W$, f è iniettiva: se infatti risulta $f(u,v) = w = f(u',v')$, allora $u = w = u' \pmod{r}$, $v = w = v' \pmod{s}$ e dunque $u = u'$, $v = v'$. Infine f è suriettiva: partendo infatti da un qualunque $w \in W$ se lo si divide per r si ottiene un resto u che è primo con r (perché lo è w); analogamente, il resto v della divisione di w per s è il primo con s . Ma allora $(u,v) \in U \times V$, $w \equiv u \pmod{r}$, $w \equiv v \pmod{s}$, e dunque $f(u,v) = w$.

Esercizi

- 1) Si dimostrino le familiari *prove del 9* per la verifica delle addizioni e moltiplicazioni negli interi (si usi la scrittura decimale e si osservi che $10^n \equiv 1 \pmod{9}$ per ogni $n > 0$).
- 2) Si generalizzi il teorema cinese del resto, provando che: se m_1, m_2, \dots, m_r sono interi a due a due coprimi (cioè $(m_i, m_j) = 1$ se $i \neq j$), allora esiste una soluzione comune delle congruenze $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, ..., $x \equiv a_r \pmod{m_r}$.

§ 12. Numeri razionali

12.1. Denoteremo con il simbolo \mathbf{Q} l'insieme dei *numeri razionali*. Sono definite in \mathbf{Q} due operazioni: l'addizione e la moltiplicazione; tra le proprietà di queste operazioni, ricordiamo le seguenti:

A 1 ASSOCIAZIIVITÀ DELL'ADDIZIONE:

per ogni $x, y, w \in \mathbf{Q}$, $(x + y) + w = x + (y + w)$;

A 2 ELEMENTO NEUTRO ADDITIVO: esiste un unico elemento 0 (leggi zero) di \mathbf{Q} , tale che $0 + x = x = x + 0$ per ogni $x \in \mathbf{Q}$;

A 3 OPPOSTO: per ogni $x \in \mathbf{Q}$ esiste un unico elemento $-x$ di \mathbf{Q} (che si dice *opposto* di x) tale che $x + (-x) = 0 = (-x) + x$;

A 4 COMMUTATIVITÀ DELL'ADDIZIONE: per ogni $x, y \in \mathbf{Q}$, $x + y = y + x$;

M1 ASSOCIAZIVITÀ DELLA MOLTIPLICAZIONE:

per ogni $x,y,w \in \mathbb{Q}$, $(xy)w = x(yw)$;

M2 ELEMENTO NEUTRO MOLTIPLICATIVO: *esiste un unico elemento $1 \neq 0$ (leggi uno, o unità) di \mathbb{Q} , tale che $x1 = x = 1x$ per ogni $x \in \mathbb{Q}$;*

M3 DISTRIBUTIVITÀ:

per ogni $x,y,w \in \mathbb{Q}$, $x(y + w) = xy + xw$; $(x + y)w = xw + yw$;

M4 COMMUTATIVITÀ DELLA MOLTIPLICAZIONE: *per ogni $x,y \in \mathbb{Q}$, $xy = yx$.*

Le proprietà precedenti sono valide anche per l'addizione e la moltiplicazione in \mathbb{Z} . Ciò che di nuovo si acquisisce in \mathbb{Q} è la proprietà

M5 INVERSO: *per ogni $x \in \mathbb{Q}$, $x \neq 0$, esiste un unico elemento x^{-1} di \mathbb{Q} (che si dice inverso di x) tale che $x \cdot x^{-1} = 1 = x^{-1} \cdot x$.*

È quest'ultima proprietà che permette di risolvere in \mathbb{Q} ogni equazione del tipo $ax = b$, con $a,b \in \mathbb{Q}$, $a \neq 0$. (L'analogia equazione in \mathbb{Z} non ammette soluzioni, se non in casi particolari).

12.2. *I numeri razionali sono un insieme ordinato, nel senso che*

O1 TRICOTOMIA: *per ogni $x,y \in \mathbb{Q}$ si presenta uno ed un solo dei seguenti casi: $x > y$ (leggi: x è maggiore di y); $x = y$; $y > x$;*

O2 TRANSITIVITÀ: *se $x > y$, $y > z$, allora $x > z$.*

Un elemento $x > 0$ si dice *positivo*; si ha $x > y$ se e solo se $x - y$ è positivo. I legami tra l'ordinamento e le operazioni sono:

A O COMPATIBILITÀ DELL'ORDINE CON L'ADDITIONE: *se $x,y,w \in \mathbb{Q}$, $x > y$ se solo se $x + w > y + w$;*

M O COMPATIBILITÀ DELL'ORDINE CON LA MOLTIPLICAZIONE: *se $x,y,w \in \mathbb{Q}$, $w > 0$, $x > y$ se e solo se $xw > yw$.*

Proprietà analoghe alle precedenti sussistono anche in \mathbb{Z} . Esse equivalgono al fatto che somme e prodotti di positivi sono ancora positivi. La proprietà M5 comporta inoltre che in \mathbb{Q} ogni positivo ha inverso positivo. Da ciò segue l'ulteriore proprietà di *densità*; se $x,y \in \mathbb{Q}$, $x > y$, allora esiste $z \in \mathbb{Q}$ tale che $x > z > y$ (basta considerare il razionale $z = (x+y)/2$). Questa proprietà non vale ovviamente in \mathbb{Z} ; in compenso, non possiamo aspettarci in \mathbb{Q} un principio del minimo; ad esempio, non ammette minimo l'insieme \mathbb{Q}^+ dei numeri razionali positivi.

12.3. Utilizzando lo zero e l'unità di \mathbb{Z} e di \mathbb{Q} , possiamo definire un'applicazione $f: \mathbb{Z} \rightarrow \mathbb{Q}$ nel modo seguente: $f(0) = 0$, e, per induzione, per ogni

$n \in \mathbf{Z}$, $n \geq 0$: $f(n+1) = f(n) + 1$; per ogni $n \in \mathbf{Z}$, $n < 0$: $f(n) = -f(-n)$.

f è iniettiva e conserva le operazioni e l'ordine, cioè, per ogni $z_1, z_2 \in \mathbf{Z}$, $f(z_1 + z_2) = f(z_1) + f(z_2)$; $f(z_1 z_2) = f(z_1)f(z_2)$; $z_1 > z_2$ se e solo se $f(z_1) > f(z_2)$.

Ciò significa che tutte le proprietà di \mathbf{Z} che abbiamo messo in evidenza nei paragrafi precedenti si riproducono esattamente in $f(\mathbf{Z})$, cosicchè, a tutti gli effetti che ci interessano, il numero razionale $f(n)$ è identificabile con il numero intero n . Queste circostanze giustificano la consuetudine (impropria, ma economica) di considerare \mathbf{Z} , anzichè $f(\mathbf{Z})$, un sottoinsieme di \mathbf{Q} ; a questa consuetudine aderiamo senz'altro di qui in avanti. Si ha inoltre:

F FRAZIONI: *ogni numero razionale è soluzione di un'equazione del tipo*

$$sx = r, \text{ con } r, s \in f(\mathbf{Z}).$$

Tale soluzione, unica, è rs^{-1} , e si denota per lo più con il simbolo r/s . Se $p, q \in f(\mathbf{Z})$ sono tali che $qr = ps$, lo stesso numero razionale r/s è soluzione anche della equazione $qx = p$. Risulta perciò $r/s = p/q$. Viceversa, se le due equazioni $sx = r$, $qx = p$ hanno soluzione comune $r/s = p/q$, allora $qr = ps$.

Si deducono infine le ben note regole:

$$(r/s) + (m/n) = (rn + ms)/sn;$$

$$(r/s)(m/n) = rm/sn;$$

$$r/s > 0 \text{ se e soltanto se } rs > 0.$$

§ 13. Numeri reali

13.1. L'insieme \mathbf{R} dei *numeri reali* è un insieme su cui sono definiti un'addizione, una moltiplicazione e un ordinamento per cui valgono tutte le proprietà A 1,2,3,4, M 1,2,3,4,5, O 1,2, A O, M O che valevano per l'analogo in \mathbf{Q} . Utilizzando lo zero e l'unità di \mathbf{Q} ed \mathbf{R} , si definisce un'applicazione $f: \mathbf{Q} \rightarrow \mathbf{R}$ ponendo $f(0) = 0$; $f(x+1) = f(x) + 1$ per $x \in \mathbf{Q}$, x intero non negativo; $f(x) = -f(-x)$ per x intero negativo; e, in generale,

$$f(r/s) = f(r)(f(s))^{-1}.$$

f è iniettiva e conserva le operazioni e l'ordinamento di \mathbf{Q} , quindi rende possibile l'identificazione di \mathbf{Q} con il sottoinsieme $f(\mathbf{Q})$ di \mathbf{R} .

13.2. Un $S \subseteq \mathbf{R}$ si dice *limitato superiormente* se ammette *maggioranti*, vale a dire se esiste un elemento $a \in \mathbf{R}$ tale che $x \leq a$ per ogni $x \in S$. In \mathbf{R} sussiste la seguente proprietà (che non vale in \mathbf{Q}):

C **COMPLETEZZA:** se S è un sottoinsieme di \mathbf{R} , non vuoto e limitato superiormente, allora l'insieme dei maggioranti di S ha minimo.

Questo minimo si dice *l'estremo superiore* di S . Tra le conseguenze della completezza, citiamo le seguenti:

- 1) \mathbf{Q} è denso in \mathbf{R} , cioè: se $x, y \in \mathbf{R}$, $x > y$, allora esiste $z \in \mathbf{Q}$ tale che $x > z > y$.
- 2) Ogni numero reale è l'estremo superiore di un insieme di numeri razionali.
- 3) Ogni numero reale non negativo è un quadrato; cioè per ogni $a \in \mathbf{R}$, $a \geq 0$, esiste un $b \in \mathbf{R}$ tale che $b^2 = a$.

Poiché non esistono numeri razionali il cui quadrato è 2, si vede che $\mathbf{Q} \subset \mathbf{R}$ (gli elementi di $\mathbf{R} \setminus \mathbf{Q}$ si dicono *numeri irrazionali*).

13.3. Ogni $x \in \mathbf{R}$ si può approssimare quanto si vuole con numeri decimali, cioè con razionali del tipo $r/10^n$. Ci limitiamo agli x positivi; anzi, poiché ogni tale x è del tipo $x = m + y$ ($m \in \mathbf{Z}$, $m \geq 0$; $y \in \mathbf{R}$, $0 \leq y < 1$) e sappiamo associare ad m lo sviluppo decimale

$$m = A_r \cdot 10^r + \dots + A_1 \cdot 10 + A_0 \quad \text{con } 0 \leq A_i < 10 \quad (\text{vedi § 10.})$$

basterà considerare reali compresi tra 0 e 1. Per essi vale il seguente teorema (che si prova in modo analogo a quello del § 10.):

Sia $y \in \mathbf{R}$, $0 \leq y < 1$; prefissato un intero $n > 0$, esiste una ed una sola espressione del tipo

$$y = C_1 \cdot 10^{-1} + C_2 \cdot 10^{-2} + \dots + C_n \cdot 10^{-n} + r_n$$

con $C_i \in \mathbf{Z}$, $r_n \in \mathbf{R}$, $0 \leq C_i < 10$, $0 \leq r_n < 10^{-n}$.

Lo sviluppo (arrestato alla n -esima cifra decimale) di $x = m + y$ si ottiene in definitiva giustapponendo le cifre A_i (per m), C_j (per y) tra le quali si interpone la virgola; si scrive cioè

$$A_r A_{r-1} \dots A_1 A_0, C_1 C_2 \dots C_{n-1} C_n.$$

§ 14. Numeri complessi

14.1. Nell'insieme delle coppie ordinate di numeri reali $C = \mathbf{R} \times \mathbf{R}$ definiamo due operazioni di addizione e moltiplicazione ponendo, per ogni coppia di elementi di C , $z_1 = (x_1, y_1)$, $z_2 = (x_2, y_2)$

$$z_1 + z_2 = (x_1 + x_2, y_1 + y_2),$$

$$z_1 \cdot z_2 = (x_1 \cdot x_2 - y_1 \cdot y_2, x_1 \cdot y_2 + x_2 \cdot y_1).$$

È facile verificare che anche per queste operazioni in C valgono le proprietà A 1,2,3,4, M 1,2,3,4,5, del paragrafo 12. Ogni insieme K su cui siano definite una somma e un prodotto che soddisfano le condizioni A, M si dice *corpo*. Dunque $\mathbf{Q}, \mathbf{R}, C$ sono corpi, detti rispettivamente *il corpo razionale*, *reale* e *complesso*; gli elementi di C si chiamano i numeri complessi. In particolare, lo zero e l'unità di C sono rispettivamente $(0,0)$, $(1,0)$; l'opposto di $z = (x,y)$ è $-z = (-x,-y)$; l'inverso di $z = (x,y)$ purché $\neq (0,0)$ è $z^{-1} = (x/(x^2+y^2), -y/(x^2+y^2))$. A titolo di esempio, dimostriamo l'*associatività* della moltiplicazione. Siano:

$$z_1 = (x_1, y_1); \quad z_2 = (x_2, y_2); \quad z_3 = (x_3, y_3);$$

allora

$$\begin{aligned} (z_1 \cdot z_2) \cdot z_3 &= ((x_1, y_1) \cdot (x_2, y_2)) \cdot (x_3, y_3) = \\ &= (x_1 \cdot x_2 - y_1 \cdot y_2, x_1 \cdot y_2 + x_2 \cdot y_1) \cdot (x_3, y_3) = \\ &= ((x_1 \cdot x_2 - y_1 \cdot y_2) \cdot x_3 - (x_1 \cdot y_2 + x_2 \cdot y_1) \cdot y_3, \\ &\quad (x_1 \cdot x_2 - y_1 \cdot y_2) \cdot y_3 + (x_1 \cdot y_2 + x_2 \cdot y_1) \cdot x_3) = \\ &= (x_1 \cdot x_2 \cdot x_3 - y_1 \cdot y_2 \cdot x_3 - x_1 \cdot y_2 \cdot y_3 - y_1 \cdot x_2 \cdot y_3, \\ &\quad x_1 \cdot x_2 \cdot y_3 - y_1 \cdot y_2 \cdot y_3 + x_1 \cdot y_2 \cdot x_3 + y_1 \cdot x_2 \cdot x_3) = \\ &= (x_1 \cdot (x_2 \cdot x_3 - y_2 \cdot y_3) - y_1 \cdot (x_2 \cdot y_3 + y_2 \cdot x_3)), \\ &\quad x_1 \cdot (x_2 \cdot y_3 + y_2 \cdot x_3) + y_1 \cdot (x_2 \cdot x_3 - y_2 \cdot y_3)) = \\ &= (x_1, y_1) \cdot (x_2 \cdot x_3 - y_2 \cdot y_3, x_2 \cdot y_3 - y_2 \cdot x_3) = \\ &= (x_1, y_1) \cdot ((x_2, y_2) \cdot (x_3, y_3)) = z_1 \cdot (z_2 \cdot z_3). \end{aligned}$$

14.2. L'applicazione $f: \mathbf{R} \rightarrow \mathbf{C}$ definita da $x \mapsto (x, 0)$ è iniettiva e conserva le somme e i prodotti, come si verifica subito; ad esempio:

$$f(x_1 x_2) = (x_1 x_2, 0) = (x_1, 0) \cdot (x_2, 0) = f(x_1) f(x_2).$$

Ciò significa che (in analogia a quanto già fatto per \mathbf{Z} in \mathbf{Q} e per \mathbf{Q} in \mathbf{R}) possiamo identificare i numeri reali con i numeri complessi della forma $(x, 0)$, e pensare ad \mathbf{R} come sottoinsieme di \mathbf{C} .

14.3. Il numero complesso $(0, 1)$ si denota con il simbolo i ; esso gode della proprietà che il suo quadrato è l'opposto dell'unità:

$$i^2 = (0, 1)^2 = (0, 1) (0, 1) = (-1, 0) = -(1, 0) = -1.$$

L'elemento i si chiama l'unità immaginaria. Ogni numero complesso (x, y) si può scrivere nella forma $(x, 0) + (0, 1)(y, 0) = (x, 0) + (0, y) = (x, y)$. Qui $(x, 0)$ si dice la parte reale di $z = (x, y)$, e si indica con $\operatorname{Re}(z)$; $(y, 0)$ si dice il coefficiente dell'immaginario di $z = (x, y)$, e si indica con $\operatorname{Im}(z)$. Ogni $z \in \mathbf{C}$ si può dunque scrivere $z = \operatorname{Re}(z) + i \operatorname{Im}(z)$. Con l'identificazione di $(x, 0)$, $(y, 0)$ con i reali x, y , risulterà $z = x + iy$. Si ha $x + iy = x' + iy'$ ($x, x', y, y' \in \mathbf{R}$) se e solo se $x = x', y = y'$.

La scrittura $z = x + iy$ è particolarmente comoda perché le somme e i prodotti dei numeri complessi in questa forma si ottengono applicando le usuali regole del calcolo letterale e tenendo presente che $i^2 = -1$. Ad esempio, applicando formalmente le note proprietà (distributiva ecc.) si calcola

$$(x + iy)(x' + iy') = xx' + i^2yy' + i(xy' + x'y).$$

Sostituito -1 a i^2 , ciò equivale a scrivere

$$(x, y)(x', y') = (xx' - yy', xy' + x'y),$$

che è appunto la definizione del prodotto.

14.4. La coniugazione è l'applicazione di \mathbf{C} in sé definita ponendo $z = x + iy \mapsto \bar{z} = x - iy$. Si vede subito che la coniugazione è biettiva e conserva le somme e i prodotti, nel senso che il coniugato della somma (del prodotto) è la somma (il prodotto) dei coniugati:

$$\begin{aligned} \overline{z_1 + z_2} &= \overline{x_1 + iy_1 + x_2 + iy_2} = \overline{x_1 + x_2 + i(y_1 + y_2)} = x_1 + x_2 - i(y_1 + y_2) = \\ &= x_1 - iy_1 + x_2 - iy_2 = \overline{x_1 + iy_1} + \overline{x_2 + iy_2} = \bar{z}_1 + \bar{z}_2. \end{aligned}$$

$$\begin{aligned} \overline{z_1 z_2} &= \overline{x_1 x_2 - y_1 y_2 + i(x_1 y_2 + x_2 y_1)} = x_1 x_2 - y_1 y_2 - i(x_1 y_2 + x_2 y_1) = \\ &= (x_1 - iy_1)(x_2 - iy_2) = \bar{z}_1 \cdot \bar{z}_2. \end{aligned}$$

La coniugazione è un'applicazione involutoria, nel senso che $\bar{\bar{z}} = z$ per ogni $z \in \mathbf{C}$. Osserviamo inoltre che per ogni $z \in \mathbf{C}$ risulta

$$z + \bar{z} = x + iy + x - iy = 2x \in \mathbb{R}; \quad z \cdot \bar{z} = (x + iy)(x - iy) = x^2 + y^2 \in \mathbb{R}.$$

Il numero reale non negativo $z \cdot \bar{z}$ si chiama la *norma* di z . Esso è utile per calcolare l'inverso di un numero complesso. Infatti, se $z \neq 0$, allora $z^{-1} = \bar{z} \cdot (z \cdot \bar{z})^{-1}$, cioè è il prodotto del coniugato per l'inverso della norma. Ad esempio calcoliamo l'inverso di $2 - 3i$:

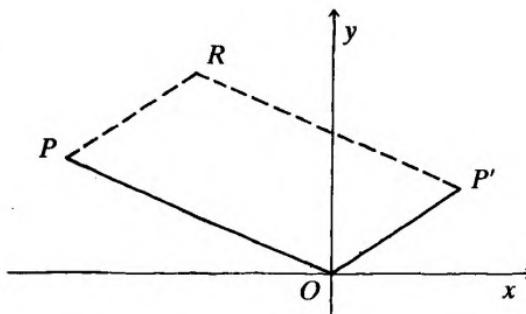
$$\begin{aligned}(2 - 3i)^{-1} &= \text{coniugato di } (2 - 3i) \text{ per inverso della norma di } (2 - 3i) = \\ &= (2 + 3i) (2^2 + 3^2)^{-1} = \frac{2}{13} + \frac{3}{13} i.\end{aligned}$$

Analogamente

$$\frac{1+i}{5+3i} = \frac{(1+i)(5-3i)}{25+9} = \frac{8+2i}{34} = \frac{4}{17} + \frac{1}{17} i.$$

14.5. L'introduzione nel piano \mathcal{P} di un sistema di coordinate cartesiane ortogonali unitarie definisce una biiezione tra \mathcal{P} e \mathbb{C} se al punto $P \in \mathcal{P}$ di ascissa x e ordinata y si associa il numero complesso $(x, y) = x + iy$, detto l'*affissa* di P . Tale biiezione si dice *rappresentazione geometrica dei numeri complessi* e \mathcal{P} il *piano di (Argand-) Gauss*: gli assi x e y si dicono rispettivamente *asse reale* e *asse immaginario*, in quanto luogo dei punti di affissa reale $(x, 0)$ e immaginaria $(0, y)$. Se $z, z' \in \mathbb{C}$ sono le affisse rispettivamente dei punti $P, P' \in \mathcal{P}$, allora $z + z'$ è l'affissa del punto R individuato dalla relazione vettoriale

$$OR = OP + OP'$$



14.6. Sia P il punto di affissa $z = x + iy$. Si dice *valore assoluto* (o *modulo*) di z , e si indica con $|z|$ il numero reale non negativo

$$\sqrt{z \cdot \bar{z}} = \sqrt{x^2 + y^2},$$

cioè la distanza di P dall'origine O . Siano $u, v \in \mathbb{C}$. Allora

$$|u \cdot v|^2 = (u \cdot v) \cdot (\overline{u \cdot v}) = u \cdot \bar{u} \cdot v \cdot \bar{v} = |u|^2 \cdot |v|^2$$

e quindi

$$|u \cdot v| = |u| \cdot |v|,$$

$$\begin{aligned} |u + v|^2 &= (u + v) \cdot (\overline{u + v}) = u \cdot \bar{u} + v \cdot \bar{v} + u \cdot \bar{v} + v \cdot \bar{u} = \\ &= |u|^2 + |v|^2 + 2\operatorname{Re}(u \cdot \bar{v}). \end{aligned}$$

Ma per ogni $z \in \mathbb{C}$ la parte reale $\operatorname{Re}(z) = x$ non può superare il modulo $|z| = \sqrt{x^2 + y^2}$; dunque $\operatorname{Re}(u \cdot \bar{v}) \leq |u \cdot \bar{v}| = |u| \cdot |\bar{v}| = |u| \cdot |v|$, e, sostituendo, $|u + v|^2 \leq |u|^2 + |v|^2 + 2|u| \cdot |v| = (|u| + |v|)^2$. Si conclude che valgono in \mathbb{C} le stesse relazioni che valgono per il valore assoluto in \mathbb{R}

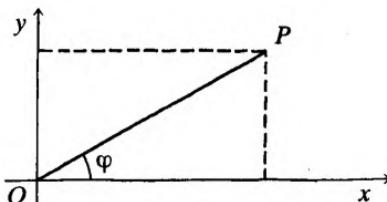
$$|u \cdot v| = |u| \cdot |v|; \quad |u + v| \leq |u| + |v|.$$

Quest'ultima si dice la *diseguaglianza triangolare*, perché, nella rappresentazione geometrica del paragrafo precedente, equivale al fatto che il lato di un triangolo non può misurare più della somma degli altri due.

14.7. Sia P il punto di affissa $z = x + iy \neq 0$. La misura φ dell'angolo orientato che ha per lati nell'ordine il semiasse delle x positive e la semiretta da O per P si dice l'*anomalia* di z . Se poniamo $q = |z|$, la trigonometria fornisce $x = q \cos \varphi$, $y = q \sin \varphi$; e dunque si scrive

$$z = x + iy = q(\cos \varphi + i \sin \varphi),$$

che si chiama *forma trigonometrica* del numero complesso non nullo z .



Esempi: per scrivere $z = 1 - i$ in forma trigonometrica, si calcola il modulo $q = |z| = \sqrt{1^2 + (-1)^2} = \sqrt{2}$ e quindi si cerca un valore φ tale che risulti $1 = \sqrt{2} \cos \varphi$, $-1 = \sqrt{2} \sin \varphi$; si trova $\varphi = 7\pi/4$ e una forma trigonometrica di z è

$$1 - i = \sqrt{2}(\cos(7\pi/4) + i \sin(7\pi/4)).$$

Altri esempi:

$$\begin{aligned} -3i &= 3(\cos(3\pi/2) + i \sin(3\pi/2)); \\ 2 + \sqrt{3} &= (2 + \sqrt{3})(\cos 0 + i \sin 0). \end{aligned}$$

Viceversa, assegnati $q^*, \varphi^* \in \mathbb{R}$, $q^* > 0$, si consideri il numero complesso $z = q^*(\cos \varphi^* + i \sin \varphi^*)$; allora $q^* \cos \varphi^* = \operatorname{Re}(z) = x$, $q^* \sin \varphi^* = \operatorname{Im}(z) = y$, da cui $(q^*)^2 = (q^* \cos \varphi^*)^2 + (q^* \sin \varphi^*)^2 = x^2 + y^2$ quindi $q^* = \sqrt{x^2 + y^2} = |z|$; inoltre $\cos \varphi^* = x/|z|$, $\sin \varphi^* = y/|z|$ cosicché φ^* è individuato da z , a meno di multipli di 2π . Conviene dunque assumere come forma trigonometrica di z ogni espressione del tipo

$$z = q(\cos(\varphi + 2k\pi) + i \sin(\varphi + 2k\pi))$$

dove φ è la anomalia e k un intero arbitrario.

14.8. Se $z = q(\cos \varphi + i \sin \varphi)$, $z' = q'(\cos \varphi' + i \sin \varphi')$ allora un semplice calcolo fornisce:

$$\begin{aligned} z \cdot z' &= q(\cos \varphi + i \sin \varphi) \cdot q'(\cos \varphi' + i \sin \varphi') = \\ &= q \cdot q' (\cos \varphi \cdot \cos \varphi' - \sin \varphi \cdot \sin \varphi') + \\ &\quad + i \cdot q \cdot q' (\sin \varphi \cdot \cos \varphi' + \cos \varphi \cdot \sin \varphi') = \\ &= qq'(\cos(\varphi + \varphi') + i \sin(\varphi + \varphi')). \end{aligned}$$

Si ottiene la **REGOLA**: *in forma trigonometrica, il prodotto di due numeri complessi si ottiene moltiplicando i moduli e sommando le anomalie.*

Ad esempio, se

$$\begin{aligned} z_1 &= 1 + i = \sqrt{2}(\cos \pi/4 + i \sin \pi/4), \quad z_2 = -1 + i = \sqrt{2}(\cos 3\pi/4 + i \sin 3\pi/4), \\ \text{allora,} \quad z_1 z_2 &= \sqrt{2}\sqrt{2}(\cos(\pi/4 + 3\pi/4) + i \sin(\pi/4 + 3\pi/4)) = \\ &= 2(\cos \pi + i \sin \pi) = -2. \end{aligned}$$

Dalla formula si deduce che l'inverso di $z (\neq 0)$ si ottiene sostituendo q con q^{-1} , φ con $-\varphi$. Ad esempio:

$$\begin{aligned} (1+i)^{-1} &= (1/\sqrt{2}) \cdot (\cos(-\pi/4) + i \sin(-\pi/4)) = \\ &= (1/\sqrt{2})(\sqrt{2}/2 - i\sqrt{2}/2) = (1/2) + i(-1/2). \end{aligned}$$

La regola si può usare, inversamente, per calcolare certi valori delle funzioni trigonometriche. Si voglia, ad esempio, calcolare $\cos(\pi/12)$. Si osserva che $\cos(\pi/12) = \cos(\pi/3 - \pi/4)$. Si considerano i due numeri complessi $\cos(\pi/3) + i \sin(\pi/3)$, $\cos(-\pi/4) + i \sin(-\pi/4)$ e si calcola il prodotto con la regola precedente:

$$\begin{aligned} \cos(\pi/12) + i \sin(\pi/12) &= \\ &= (\cos(\pi/3) + i \sin(\pi/3))(\cos(-\pi/4) + i \sin(-\pi/4)) = \\ &= (1/2 + i\sqrt{3}/2)(\sqrt{2}/2 - i\sqrt{2}/2) = [(\sqrt{2} + \sqrt{6})/4] + i\dots \end{aligned}$$

Quindi il valore cercato è $\cos(\pi/12) = (\sqrt{2} + \sqrt{6})/4$.

14.9. Il risultato precedente si estende al prodotto di più fattori:

$$\prod_{k=1}^n q_k (\cos \varphi_k + i \sin \varphi_k) = \left(\prod_{k=1}^n q_k \right) \left[\cos \left(\sum_{k=1}^n \varphi_k \right) + i \sin \left(\sum_{k=1}^n \varphi_k \right) \right].$$

In particolare, quando gli n fattori coincidono, si ottiene la

FORMULA DI DE MOIVRE:

$$z^n = (q (\cos \varphi + i \sin \varphi))^n = q^n (\cos n\varphi + i \sin n\varphi).$$

La formula si estende anche a valori negativi di n osservando che

$$z^n = (z^{-1})^{-n} = (q^{-1} (\cos(-\varphi) + i \sin(-\varphi)))^{-n} = q^n (\cos n\varphi + i \sin n\varphi)$$

Si può usare la stessa formula per calcolare $\cos(n\varphi)$, $\sin(n\varphi)$ a partire da $\cos \varphi$, $\sin \varphi$, per ogni n positivo. Infatti (ponendo $q = 1$) si ottiene

$$\cos(n\varphi) + i \sin(n\varphi) = (\cos \varphi + i \sin \varphi)^n = \sum_{k=0}^n \binom{n}{k} (\cos \varphi)^{n-k} (i \sin \varphi)^k.$$

Esempio:

$$\begin{aligned} \cos 4\varphi + i \sin 4\varphi &= (\cos \varphi + i \sin \varphi)^4 = \\ &= (\cos \varphi)^4 + 4(\cos \varphi)^3(i \sin \varphi) + 6(\cos \varphi)^2(i \sin \varphi)^2 + \\ &\quad + 4(\cos \varphi)(i \sin \varphi)^3 + (i \sin \varphi)^4. \end{aligned}$$

Isolando il reale dall'immaginario si ottiene:

$$\cos 4\varphi = (\cos \varphi)^4 - 6(\cos \varphi)^2(\sin \varphi)^2 + (\sin \varphi)^4; \quad \sin 4\varphi = \dots$$

14.10 Se $w, z \in \mathbb{C}$, si dice che w è una radice n -esima di z (n intero positivo) se $z = w^n$. Se $0 \neq z = q (\cos \varphi + i \sin \varphi)$, $0 \neq w = p (\cos \theta + i \sin \theta)$ sono forme trigonometriche, allora $z = w^n$ comporta $q = p^n$, $\cos(n\theta) = \cos \varphi$, $\sin(n\theta) = \sin \varphi$. Dalla prima si deduce $p = \sqrt[n]{q}$ (cioè l'unico numero reale positivo la cui potenza n -esima è q); dalle seconde si deduce $n\theta = \varphi + 2k\pi$, quindi $\theta = (\varphi + 2k\pi)/n$ per qualche $k \in \mathbb{Z}$. Viceversa, per

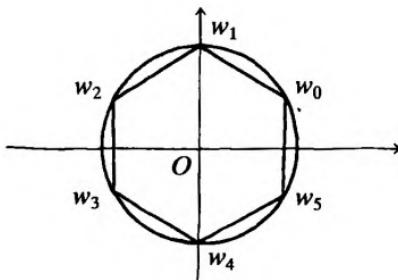
ogni $k \in \mathbb{Z}$, il numero complesso $w_k = q \left(\cos \frac{\varphi + 2k\pi}{n} + i \sin \frac{\varphi + 2k\pi}{n} \right)$ è una radice n -esima di z . Si vede facilmente che, al variare di k in \mathbb{Z} , w_k assume esattamente n valori distinti, che si ottengono, ad esempio, per $k = 0, 1, \dots, n-1$. Abbiamo così provato che **ogni numero complesso $z \neq 0$ ammette n radici n -esime distinte** (se $z = 0$, l'unica sua radice n -esima è 0). I numeri w_0, w_1, \dots, w_{n-1} sono le affisse dei vertici di un poligono regolare di

n lati iscritto nel cerchio di centro O e raggio $\sqrt[n]{|z|}$. Ad esempio, le radici seste di $-8 = 8(\cos \pi + i \sin \pi)$ sono:

$$w_0 = \sqrt{2}(\cos \pi/6 + i \sin \pi/6);$$

$$w_1 = \sqrt{2}(\cos (\pi + 2\pi)/6 + i \sin (\pi + 2\pi)/6);$$

$$w_2 = \sqrt{2}(\cos (\pi + 4\pi)/6 + i \sin (\pi + 4\pi)/6); \text{ ecc.}$$



Si trovano, in definitiva, i numeri:

$$w_0 = (\sqrt{2}/2)(\sqrt{3} + i), \quad w_1 = \sqrt{2}i, \quad w_2 = (\sqrt{2}/2)(-\sqrt{3} + i),$$

$$w_3 = \sqrt{2}/2)(-\sqrt{3} - i), \quad w_4 = -\sqrt{2}i, \quad w_5 = (\sqrt{2}/2)(\sqrt{3} - i).$$

In particolare, le *radici n-esime dell'unità* sono i numeri

$$e_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \quad k = 0, 1, \dots, n-1.$$

Esercizi

- 1) Esprimere nella forma $x+iy$ ($x, y \in \mathbb{R}$) i seguenti numeri complessi:
 $(4+2i)(1-i)$, i^{-1} , $(7-6i)/(2+3i)$, $(2+3i)^3$, $2i/(2+i)^2$.
- 2) Per quali $x \in \mathbb{R}$ è reale il numero $(x-2+ix)/(x-3-5i)$?
- 3) Per quali $x, y \in \mathbb{R}$ risulta $(x+iy)^2 = -5+12i$?
- 4) Si generalizzi la diseguaglianza triangolare: se $z_1, z_2, \dots, z_n \in \mathbb{C}$ allora
 $|z_1 + z_2 + \dots + z_n| \leq |z_1| + |z_2| + \dots + |z_n|$.
- 5) Se $z \in \mathbb{C}$ è dato in forma trigonometrica, come si ottiene quella del coniugato \bar{z} ?
- 6) Si trovino modulo e anomalia di: $2\sqrt{3}+2i$, $(2-2i)/(3+3i)$.
- 7) Si calcoli $(1+i)^6$ con la formula di De Moivre.
- 8) Si determinino tutti i numeri complessi w tali che $w^3 = i$. Lo stesso per $w^3 = -1$ e $w^2 = -i$.

- 9) Siano e_0, e_1, \dots, e_{n-1} le radici complesse n -esime dell'unità. Si provi che risulta $e_i \cdot e_j = e_k$ con $k \equiv i + j \pmod{n}$.
- 10) Si dimostri che $e_0 + e_1 + \dots + e_{n-1} = 0$.
- 11) La radice n -esima dell'unità e_i si dice *primitiva* se ogni altra radice e_j è una potenza di e_i . Si dimostri che esistono $\varphi(n)$ (funzione di Eulero) radici primitive.

§ 15 Funzioni razionali intere

In tutto il capitolo, salvo esplicita menzione in contrario, \mathbf{K} indicherà uno qualunque, fissato, dei seguenti corpi: $\mathbf{Q}, \mathbf{R}, \mathbf{C}$.

15.1. Chiameremo *funzione razionale intera* (o *funzione polinomiale*) in una variabile su \mathbf{K} (o in \mathbf{K}) ogni applicazione f di \mathbf{K} in sè, tale che esistano un intero $n \geq 0$ e degli elementi $a_0, a_1, \dots, a_n \in \mathbf{K}$, per cui risulti

$$f(x) = \sum_{h=0}^n a_h x^h \text{ per tutti gli } x \in \mathbf{K}.$$

Esempi di funzioni razionali intere in una variabile su \mathbf{Q} , \mathbf{R} e \mathbf{C} sono

$$f : \mathbf{Q} \rightarrow \mathbf{Q} \quad \text{con } f(x) = 3 + x^2,$$

$$g : \mathbf{R} \rightarrow \mathbf{R} \quad \text{con } g(x) = 1 + 2\sqrt{5}x + x^2,$$

$$h : \mathbf{C} \rightarrow \mathbf{C} \quad \text{con } h(x) = 1 + ix + x^3.$$

15.2. Indichiamo con $\mathbf{K}[x]$ l'insieme di tutte le funzioni razionali intere in una variabile su \mathbf{K} . Se $f, g \in \mathbf{K}[x]$, indichiamo con $f + g$ e chiamiamo *somma* di f e di g l'applicazione di \mathbf{K} in sè, definita ponendo

$$(f + g)(x) = f(x) + g(x) \quad \text{per ogni } x \in \mathbf{K}.$$

Indichiamo con fg e chiamiamo *prodotto* di f e g l'applicazione di \mathbf{K} in sè, definita ponendo

$$(fg)(x) = f(x)g(x) \quad \text{per ogni } x \in \mathbf{K}.$$

Ad esempio, se $f(x) = x^2$, $g(x) = 6 - 5x$,

$$\text{allora } (f+g)(x) = f(x) + g(x) = x^2 + (6 - 5x) = 6 - 5x + x^2,$$

$$(fg)(x) = f(x)g(x) = x^2(6 - 5x) = 6x^2 - 5x^3.$$

Notiamo che se

$$f(x) = \sum_{h=0}^n a_h x^h \quad \text{e} \quad g(x) = \sum_{k=0}^m b_k x^k,$$

allora, se è ad esempio $m \leq n$, possiamo scrivere $b_h = 0$ per $m < h \leq n$, e i valori $(f+g)(x)$ e $(fg)(x)$ sono dati da

$$(f+g)(x) = \sum_{h=0}^n (a_h + b_h)x^h; \quad (fg)(x) = \sum_{t=0}^{n+m} \left(\sum_{h+k=t} a_h b_k \right) x^t;$$

quindi $f+g, fg \in K[x]$. Abbiamo dunque definito due operazioni, l'addizione e la moltiplicazione in $K[x]$. Non è difficile verificare che queste operazioni soddisfano le proprietà A 1,2,3,4, e M 1,2,3,4 del 12.1. In particolare, l'elemento zero di $K[x]$ è la applicazione definita ponendo $x \mapsto 0$ per ogni $x \in K$, che si chiama l'applicazione nulla e si indica ancora con il simbolo 0; l'opposto $-f$ di f è definito ponendo $x \mapsto -f(x)$ per ogni $x \in K$; la unità di $K[x]$ è definita ponendo $x \mapsto 1$ per ogni $x \in K$, e si indica col simbolo 1.

15.3. Sia $f \in K[x]$, con $f(x) = \sum_{h=0}^n a_h x^h$; se u è un arbitrario elemento di K , allora esistono elementi $c_0, c_1, \dots, c_n \in K$ tali che $f(x) = \sum_{h=0}^n c_h (x-u)^h$.

Infatti poiché per ciascun intero h , con $0 \leq h \leq n$ possiamo scrivere $x^h = (u + (x-u))^h$, ricorrendo alla formula del binomio (numero 6.5.), $x^h = u^h + \dots + (x-u)^h$, e quindi $a_h x^h = a_h u^h + \dots + a_h (x-u)^h$ si può scrivere come somma di potenze di $(x-u)$, moltiplicate per opportuni elementi K . Sostituendo queste espressioni (per $h=0,1,\dots,n$) nella somma $\sum a_h x^h$, si trova la desiderata espressione per f .

Ad esempio, se f è definita da $f(x) = 6 - 5x + x^2$, e se $u = 1$, allora

$$x = 1 + (x-1), \quad x^2 = (1 + (x-1))^2 = 1 + 2(x-1) + (x-1)^2$$

e dunque

$$f(x) = 6 - 5(1 + (x-1)) + 1 + 2(x-1) + (x-1)^2 = 2 - 3(x-1) + (x-1)^2;$$

così

$$c_0 = 2, \quad c_1 = -3, \quad c_2 = 1.$$

15.4. L'elemento $u \in K$ si dice zero (o radice) di $f \in K[x]$ se $f(u) = 0$. Se u è uno zero di f , nell'espressione di $f(x) = \sum c_h (x-u)^h$ del numero precedente, è $c_0 = 0$. Otteniamo perciò

$$f(x) = (x-u) \left(\sum_{h=1}^n c_h (x-u)^{h-1} \right),$$

ossia $f(x) = (x-u) q(x)$, con $q \in \mathbf{K}[x]$.

15.5. TEOREMA: sia $f \in \mathbf{K}[x]$, con $f(x) = \sum_{h=0}^n a_h x^h$. Se non tutti gli elementi a_0, a_1, \dots, a_n sono nulli, allora esistono in \mathbf{K} al più n elementi distinti che sono zeri di f .

Dimostrazione: Poiché gli a_i non sono tutti nulli, possiamo supporre $a_n \neq 0$. Procediamo per induzione su n . Se $n=0$, il teorema è evidente ($a_0 \neq 0$ ed f non ha zeri). Supponiamolo vero per $n-1$, e vediamo di provarlo per n . Ammettiamo, per assurdo, che $u=u_1, u_2, \dots, u_n, u_{n+1}$ siano $n+1$ elementi distinti di \mathbf{K} che sono zeri di f . Allora, poiché $f(u)=0$, possiamo scrivere (cfr. 15.4.): $f(x) = (x-u) q(x)$ con

$$q(x) = c_1 + c_2(x-u) + \dots + c_n(x-u)^{n-1} = \sum_{h=0}^{n-1} a'_h x^h, \text{ con } a'_{n-1} = c_n = a_n \neq 0.$$

Poiché $0 = f(u_i) = (u_i - u) q(u_i)$ e $u - u_i \neq 0$

per ogni $i=2,3,\dots,n+1$, si conclude che q ammette più di $n-1$ zeri. Ma ciò contrasta con l'ipotesi induttiva. Dunque f ammette al più n zeri distinti. Per il principio di induzione, il teorema è vero per ogni $n \geq 0$.

COROLLARIO: se $f, g \in \mathbf{K}[x]$, con $f(x) = \sum_{h=0}^n a_h x^h$, $g(x) = \sum_{h=0}^m b_h x^h$ e, per ogni $x \in \mathbf{K}$, risulta $f(x) = g(x)$ allora $a_0 = b_0$, $a_1 = b_1, \dots, a_n = b_n$.

Possiamo dunque affermare che f è l'applicazione nulla se e solo se $a_0, a_1, \dots, a_n = 0$; in ogni altro caso, se $f(x) = \sum_{h=0}^n a_h x^h$ con $a_n \neq 0$, allora a_0, a_1, \dots, a_n sono individuati da f . Questi elementi si dicono i coefficienti di f ; a_0 è il termine costante di f , a_n il coefficiente direttivo di f , n il grado di f (e si scriverà $n = \deg f$). Se f è l'applicazione nulla, converremo che $\deg f$ è meno infinito e scriveremo $\deg f = -\infty$. Convenendo che $-\infty$ soddisfi queste condizioni:

$$-\infty + -\infty = -\infty, \quad -\infty + n = -\infty, \quad -\infty < n \quad \text{per ogni } n \in \mathbf{Z},$$

affermiamo che: se $f, g \in \mathbf{K}[x]$, allora $\deg(fg) = \deg f + \deg g$.

Infatti, supponiamo che

$$f(x) = \sum_{h=0}^n a_h x^h \text{ e } g(x) = \sum_{k=0}^m b_k x^k, \text{ con } a_n \neq 0 \text{ e } b_m \neq 0.$$

Allora $(fg)(x) = a_n b_m x^{n+m} + p(x)$, con $a_n b_m \neq 0$ e $p \in \mathbf{K}[x]$ di grado

$\varrho p < n + m$. Quindi $\varrho(fg) = n + m = \varrho f + \varrho g$. Se $f = 0$ o $g = 0$, allora $fg = 0$ e, per la convenzione fatta per $-\infty$, $\varrho(fg) = \varrho f + \varrho g$. Il risultato ora ottenuto ci assicura che: se $f, g \in \mathbf{K}[x]$, con $fg = 0$, allora o $f = 0$ oppure $g = 0$, poiché, in caso diverso, è $\varrho f \geq 0$, $\varrho g \geq 0$ e, quindi, $\varrho(fg) = \varrho f + \varrho g \geq 0$.

15.6. Per indicare l'elemento $f \in \mathbf{K}[x]$ definito ponendo $f(x) = \sum_{h=0}^n a_h x^h$ per ogni $x \in \mathbf{K}$, si usa talvolta scrivere $f = \sum_{h=0}^n a_h x^h$. In particolare $f = a_0$ indica l'elemento di $\mathbf{K}[x]$ definito da $x \mapsto a_0$ per ogni $x \in \mathbf{K}$, che diremo *costante*. Dunque f è costante se, e solo se, esso ha grado 0 oppure $-\infty$. Elementi distinti di \mathbf{K} danno luogo a costanti distinte di $\mathbf{K}[x]$, somme e prodotti in \mathbf{K} danno luogo a costanti che sono somme e prodotti in $\mathbf{K}[x]$. Ciò permette di *identificare* \mathbf{K} con l'insieme delle costanti, e pensare \mathbf{K} come un sottoinsieme di $\mathbf{K}[x]$.

15.7. DIVISIONE in $\mathbf{K}[x]$. Siano $f, g \in \mathbf{K}[x]$, con $\varrho g \geq 0$. Allora esistono $q, r \in \mathbf{K}[x]$, tali che

$$f = qg + r, \quad \varrho r < \varrho g.$$

Inoltre q, r sono univocamente determinati da queste condizioni.

Dimostrazione: esistenza. Se $\varrho f < \varrho g$, scriviamo $f = 0g + f$ per ottenere il nostro scopo. Supponiamo ora $\varrho f = n \geq m = \varrho g$ e siano a_n, b_m rispettivamente i coefficienti direttivi di f e di g . Allora, facendo induzione (nella seconda forma), possiamo supporre che il risultato sia vero per gli elementi di $\mathbf{K}[x]$ di grado minore di n . Definiamo h , e f_1 con le posizioni

$$h(x) = a_n b_m^{-1} x^{n-m} g(x) \quad f_1(x) = f(x) - h(x).$$

Poiché i coefficienti direttivi di f e h sono eguali, risulta $\varrho f_1 < \varrho f$.

Possiamo quindi supporre che esistano $q^*, r \in \mathbf{K}[x]$, con $\varrho r < \varrho g$, tali che $f_1 = q^* g + r$.

$$\text{Allora} \quad f(x) = a_n b_m^{-1} x^{n-m} g(x) + q^*(x) g(x) + r(x)$$

$$\text{quindi} \quad f = qg + r,$$

$$\text{dove} \quad q(x) = a_n b_m^{-1} \cdot x^{n-m} + q^*(x).$$

Unicità. Supponiamo che per $q, r, q', r' \in \mathbf{K}[x]$ risulti $qg + r = q'g + r'$, con $\varrho r < \varrho g$, $\varrho r' < \varrho g$. Allora $(q - q')g = r' - r$, da cui $\varrho((q - q')g) = \varrho(r' - r)$, cioè $\varrho g + \varrho(q - q') = \varrho(r' - r)$. Ma $\varrho(r' - r) < \varrho g$, per cui $\varrho(q - q') = -\infty$. Perciò $q - q' = 0$, e così $r' - r = 0$, ossia $q = q'$ ed $r = r'$.

Ad esempio, per $f(x) = 3 - 17x + x^2 + x^3 + x^5$, $g(x) = 5 + x^2$, risulta $q(x) = 1 - 4x + x^3$ e $r(x) = -2 + 3x$. L'esecuzione pratica della divisione euclidea si può organizzare in questo modo:

dividendo	$f(x) = x^5 + x^3 + x^2 - 17x + 3$	$x^2 + 5 = g(x)$	divisore
1° resto parziale	$-x^3g(x) = -x^5 - 5x^3$	x^3	
2° resto parziale	$f_1(x) = -4x^3 + x^2 - 17x + 3;$	$-4x$	
resto	$4xg(x) = 4x^3 + 20x$	$+1$	
	$f_2(x) = x^2 + 3x + 3;$	$x^3 - 4x + 1 = q(x)$	quoziente
	$(-1)g(x) = -x^2 - 5$		
	$r(x) = 3x - 2.$		

Ritroviamo, come corollario il **TEOREMA DI RUFFINI** (cfr. 15.4.): *Siano $f \in \mathbb{K}[x]$, $f \neq 0$, $u \in \mathbb{K}$; allora u è zero di f se, e soltanto se,*

$$f(x) = (x - u)q(x), \text{ per qualche } q \in \mathbb{K}[x].$$

Dimostrazione: Sia u zero di f . Allora dividendo f per $x - u$ troviamo $f(x) = (x - u)q(x) + r(x)$, $\varrho < \varrho(x - u) = 1$; r è allora costante. Poiché $0 = f(u) = (u - u)q(u) + r$, abbiamo $r = 0$ e così $f(x) = (x - u)q(x)$. Il viceversa è ovvio.

15.8. C'è un'evidente analogia tra l'algoritmo della divisione ora illustrata per $\mathbb{K}[x]$ e quello visto per \mathbb{Z} al 7.2.; infatti l'enunciato di 15.7. si ottiene formalmente da quello di 7.2. pur di sostituire *valore assoluto di un intero* con *grado della funzione polinomiale*. Ci proponiamo di estendere tale analogia a tutta la teoria della *fattorizzazione*, considerata nei numeri 7, 8 e 9. Poiché le dimostrazioni differiscono soltanto nei dettagli da quelle già viste per \mathbb{Z} , saremo brevi nelle definizioni e nelle dimostrazioni.

Siano $f, g \in \mathbb{K}[x]$ non entrambi nulli. Scriveremo $g | f$ (g divide f) se $f = qg$ per qualche $q \in \mathbb{K}[x]$.

Ad esempio, $x - 1 | x^3 - 1$ poiché risulta $x^3 - 1 = (x - 1)(x^2 + x + 1)$; invece $x - 1 \nmid x^3 + 1$.

Se $g \neq 0$ allora $g | f$ se e solo se è zero il resto della divisione di f per g .

Se $g | f$, $f | h$, allora $g | h$.

Se $f | g$ e $g | f$, allora $f = qg = qq'f$, $\varrho f = \varrho f + \varrho(q'q)$, e quindi (se $f \neq 0$), $0 = \varrho(q'q) = \varrho q' + \varrho q$. Allora $q, q' \in \mathbb{K}$, quindi f, g si ottengono uno dall'altro moltiplicando per un fattore costante.

Un elemento $d \in \mathbb{K}[x]$ si dirà M.C.D. degli elementi $f, g \in \mathbb{K}[x]$ se:

1°) $d | f$ e $d | g$;

2°) se $h \in \mathbb{K}[x]$, $h | f$ e $h | g$, allora $h | d$.

Per ogni $f, g \in \mathbb{K}[x]$ non entrambi nulli esiste un M.C.D. che anzi risulta individuato a meno di un fattore costante. La dimostrazione si ottiene considerando l'insieme $S = \{h \in \mathbb{K}[x]; 0 \neq h = fs + gt; s, t \in \mathbb{K}[x]\}$ e in esso un elemento d di grado minimo. Il ragionamento è identico a quello di 8.1. Anche in $\mathbb{K}[x]$ l'algoritmo di Euclide fornisce un M.C.D.

Esempio: $f = -1 - 2x + x^3 + x^4 + x^5; g = -1 + x^3$.

$$\begin{aligned} -1 - 2x + x^3 + x^4 + x^5 &= (-1 + x^3)(1 + x + x^2) - x + x^2 \\ -1 + x^3 &= (-x + x^2)(1 + x) - 1 + x \\ -x + x^2 &= (-1 + x)x + 0; \end{aligned}$$

allora M.C.D. di f, g è $= -1 + x$, cioè l'ultimo resto non nullo. Utilizzando le stesse divisioni nell'ordine inverso, si ha

$$-1 + x = f(-1 - x) + g(2 + 2x + 2x^2 + x^3),$$

cioè una (non unica) scrittura del tipo $d = fs + gt$.

15.9. Se $f \in \mathbb{K}[x]$ e c è una costante non nulla, allora risulta $cf | f, c | f$.

Si dice che $f \in \mathbb{K}[x]$ è *irriducibile* se f non è costante e gli unici divisori di f sono i *divisori impropri*, cioè le costanti e i multipli cf .

Esempi: 1) Se f ha grado 1, f è irriducibile. Infatti da $g | f$ segue $f = qg$, $1 = qf = qg + \varrho q$ da cui $\varrho q = 0$ oppure $\varrho q = 0$, quindi rispettivamente g è costante $\neq 0$ oppure $g = cf$, con c costante $\neq 0$.

2) $1 + x^2 \in \mathbb{Q}[x]$ è irriducibile in $\mathbb{Q}[x]$. Infatti un divisore proprio dovrebbe avere grado 1; ma allora (Ruffini) $x^2 + 1$ avrebbe uno zero in \mathbb{Q} .

3) $x^2 + 1$ è *riducibile* (cioè non è irriducibile) in $\mathbb{C}[x]$. Infatti se i è una radice quadrata di -1 , risulta $(x + i)(x - i) = x^2 + 1$.

4) $x^4 + 1$ è riducibile in $\mathbb{R}[x]$. Infatti $x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$.

5) $x^3 - 2$ è irriducibile in $\mathbb{Q}[x]$. Infatti altrimenti dovrebbe avere un fattore di grado 1, quindi (Ruffini) uno zero $u \in \mathbb{Q}$. Ma è $u^3 \neq 2$ per ogni $u \in \mathbb{Q}$.

Osserviamo che se c è una costante non nulla, allora $f = \mathbb{K}[x]$ è irriducibile se e solo se lo è cf .

15.10. Alcune proprietà dei numeri primi si possono riformulare per gli elementi irriducibili di $\mathbb{K}[x]$. In particolare: se $p, f, g \in \mathbb{K}[x]$, p irriducibile, $p | fg$, $p \nmid f$, allora $p | g$. Da questo segue, parafrasando la dimostrazione di 9.1., il

TEOREMA: *ogni $f \in \mathbb{K}[x]$, di grado ≥ 1 si può esprimere come prodotto di elementi irriducibili.* In questo prodotto, i fattori irriducibili sono *univocamente determinati, a meno dell'ordine e di fattori costanti*.

Esempi: 1) due tali fattorizzazioni in $\mathbf{Q}[x]$ per $3x^3 - x^2 - 15x + 5$ sono:

$$f = (3x - 1)(x^2 - 5) = (-x + 1/3)(-3x^2 + 15).$$

2) due fattorizzazioni in $\mathbf{R}[x]$ per $f = 3x^3 - x^2 - 15x + 5$ sono:

$$f = (x - 1/3)(3x - 3\sqrt{5})(x + \sqrt{5}) = (3x - 1)(-x + \sqrt{5})(-x - \sqrt{5}).$$

15.11. Gli elementi irriducibili di $\mathbf{C}[x]$ hanno grado 1. Ciò segue dalla seguente proprietà dei numeri complessi (non valida in \mathbf{Q}, \mathbf{R}), che ci limitiamo ad enunciare:

TEOREMA FONDAMENTALE DELL'ALGEBRA:

Ogni elemento non costante di $\mathbf{C}[x]$ ha uno zero in \mathbf{C} .

Per il teorema di Ruffini, ciò comporta che ogni $f \in \mathbf{C}[x]$ con $gf \geq 1$ ammette un fattore di grado 1. In definitiva, ogni tale f ammette una fattorizzazione del tipo $f = c_0(x - c_1)(x - c_2) \dots (x - c_n)$ dove i numeri complessi c_1, c_2, \dots, c_n sono gli zeri di f .

15.12. Proveremo che in $\mathbf{R}[x]$ gli elementi irriducibili hanno grado 1 oppure 2. Utilizzeremo il seguente lemma: se $c \in \mathbf{C}$ è uno zero di $f \in \mathbf{R}[x] \subseteq \mathbf{C}(x)$, allora anche il coniugato \bar{c} è zero di f .

Infatti sia $f = \sum_{k=0}^n a_k x^k$, $a_k \in \mathbf{R}$. Allora $f(c) = \sum a_k c^k = 0$. Sfruttando le proprietà della coniugazione, otteniamo $0 = \bar{0} = \overline{f(c)} = \sum \overline{a_k c^k} = \sum a_k \bar{c}^k = f(\bar{c})$, come si voleva. Proviamo che ogni $f \in \mathbf{R}[x]$, con $gf = n \geq 1$ è prodotto di elementi irriducibili in $\mathbf{R}[x]$, di grado 1 oppure 2:

$$f = r_0(x - r_1)(x - r_2) \dots (x - r_s)(x^2 + a_1x + b_1)(x^2 + a_2x + b_2) \dots (x^2 + a_t x + b_t)$$

per opportuni $r_i, a_i, b_i \in \mathbf{R}$; $s + 2t = n$. Poichè l'asserto è vero per $n = 1, 2$ procediamo per induzione su n . Consideriamo f come elemento di $\mathbf{C}[x] \supseteq \mathbf{R}[x]$; per il teorema fondamentale f ammette uno zero $c \in \mathbf{C}$; se $c \in \mathbf{R}$ (Ruffini) $f = f_1(x - c)$, con $f_1 \in \mathbf{R}[x]$, $gf_1 < gf$. Per l'ipotesi induttiva, l'asserto vale per f_1 , quindi anche per f . Se invece $c \notin \mathbf{R}$, allora, per il lemma precedente, anche \bar{c} è zero di f , quindi $x - c$, $x - \bar{c}$ dividono entrambi f in $\mathbf{C}[x]$. Poichè $c \neq \bar{c}$, i polinomi $x - c$ e $x - \bar{c}$ sono coprimi, quindi f è multiplo del prodotto $(x - c)(x - \bar{c}) = x^2 - (c + \bar{c})x + c\bar{c} = x^2 + ax + b$, che è un elemento di $\mathbf{R}[x]$, dato che $a = -c - \bar{c}$, $b = c\bar{c} \in \mathbf{R}$. Allora $f = (x^2 + ax + b)f_2$, con $f_2 \in \mathbf{R}[x]$, $gf_2 < gf$, e si riapplica l'ipotesi induttiva. Si osservi che $x^2 + ax + b$ è irriducibile in $\mathbf{R}[x]$, perché avendo già due zeri distinti $c, \bar{c} \in \mathbf{C} \setminus \mathbf{R}$, non può avere un terzo zero reale.

Esempio: per trovare i fattori irriducibili in $\mathbf{R}[x]$ di $f = x^5 - 1$, poichè ne conosciamo gli zeri complessi (le cinque radici quinte dell'unità: e_0, \dots, e_4 del 14.10.), scriviamo $f = (x - 1)(x - e_1)(x - e_2)(x - e_3)(x - e_4)$. Poichè

$e_4 = \bar{e}_1$, $e_3 = \bar{e}_2$, si ha $(x - e_2)(x - e_3) \in \mathbb{R}[x]$, $(x - e_1)(x - e_4) \in \mathbb{R}[x]$. Per calcolare i coefficienti reali, osservato che $e_2e_3 = e_1e_4 = 1$ (dalla forma trigonometrica), basterà determinare $a_1, a_2 \in \mathbb{R}$ tali che

$$f = (x - 1)(x^2 + a_1x + 1)(x^2 + a_2x + 1).$$

Dividendo per $x - 1$ si ottiene

$$x^4 + x^3 + x^2 + x + 1 = (x^2 + a_1x + 1)(x^2 + a_2x + 1),$$

ed eguagliando i termini di pari grado:

$$a_1 + a_2 = 2 + a_1a_2 = 1, \text{ da cui } a_{1,2} = (1/2)(1 \pm \sqrt{5}).$$

15.13. L'elemento $u \in \mathbb{K}$ si dice zero di *molteplicità r* per $f \in \mathbb{K}[x]$ se $(x - u)^r | f$, ma $(x - u)^{r+1} \nmid f$. Inoltre u si dice zero *semplice* se la sua molteplicità è 1, *multiplo* negli altri casi. Ad esempio, $x^5 - 1$ ha in \mathbb{R} un solo zero, $u = 1$, che è semplice; $x^5 - 1$ ha in \mathbb{C} 5 zeri, tutti semplici; invece per $x^4 - 2x^2 + 1 = (x - 1)^2(x + 1)^2$ gli zeri 1, -1 sono entrambi doppi ($r = 2$). Un criterio per determinare la molteplicità di uno zero f si ottiene introducendo la *derivata* f' : se $f = \sum_{h=0}^n a_h x^h$, allora la derivata $f' \in F(\mathbb{K})$ si definisce ponendo

$$f' = \sum_{h=1}^n h a_h x^{h-1} = a_1 + 2a_2 x + \dots + n a_n x^{n-1} \text{ se } qf > 0 \text{ e } f' = 0 \text{ se } qf \leq 0.$$

Se $f, g \in \mathbb{K}[x]$ e c è una costante, si verifica che è

$$(f + g)' = f' + g'; (fg)' = fg' + f'g; (cf)' = cf'.$$

In particolare, se $f = g^m$ ($m > 0$), $f' = m \cdot g^{m-1} \cdot g'$.

Proviamo che se $f \in \mathbb{K}[x]$, $qf > 1$, allora $u \in \mathbb{K}$ è zero multiplo di f se e solo se $(x - u)$ divide f ed f' .

Infatti, se u è zero multiplo di f , si ha $f = (x - u)^2 g$, $g \in \mathbb{K}[x]$, quindi

$$f' = 2(x - u)g + (x - u)^2 g' = (x - u)(2g + (x - u)g').$$

Viceversa, se u è zero di f e di f' , allora

$$f = (x - u)h, \quad h \in \mathbb{K}[x], \quad f' = (x - u)k, \quad k \in \mathbb{K}[x];$$

allora $((x - u)h)' = h + (x - u)h' = (x - u)k$, cosicché $(x - u) | h$, $(x - u)^2 | f$.

Esempi: 1) Gli zeri di $x^5 - 5x + 1$ sono semplici, perché se u è zero di $f' = 5(x^4 - 1)$, allora $u^4 = 1$, da cui $f(u) = u^5 - 5u + 1 = 1 - 4u \neq 0$ perché $(1/4)^4 \neq 1$.

2) $f = ax^2 + bx + c$ ($a \neq 0$) ha zeri multipli se e solo se il discriminante $d = b^2 - 4ac$ di f è zero. Infatti l'unico zero di $f' = 2ax + b$ è $-b/2a$, che risulta zero di f se e solo se $a(-b/2a)^2 + b(-b/2a) + c = -d/4a = 0$.

Esercizi

- 1) L'identità $i_K : K \rightarrow K$ è una funzione razionale intera?
- 2) Si scriva $f = \sum a_h x^h$ nella forma $f = \sum c_h (x - u)^h$ in ciascuno dei seguenti casi: $f = x^3 + x - 1$, $u = 1$; $f = x^2 - 5x + 6$, $u = -4$.
- 3) Siano $a, b, c \in C$, $a \neq 0$. Si determinino $u, d \in C$ in modo che sia $f = ax^2 + bx + c = a(x - u)^2 + d$. Si deduca che f possiede zeri in C , che hanno la forma $u + w$ dove $w^2 = -d \cdot a^{-1}$.
- 4) Si trovino gli zeri in C di $f = 4x^2 + 4ix - 1 - 4i \in C[x]$.
- 5) È l'applicazione *valore assoluto* $x \mapsto |x|$ di R in sè una applicazione razionale intera? Lo sono le applicazioni di R in sè definite da $x \mapsto \operatorname{sen} x$, $x \mapsto 1/(1+x^2)$?
- 6) Si calcolino quoziente e resto della divisione di f per g in ciascuno dei seguenti casi:
 - a) $f = x^2 - 2x + 1$, $g = x^2 + 1$;
 - b) $f = x^3 + 1$, $g = (2/3)x$;
 - c) $f = x^4 + 4$, $g = x^2 - 3x + 4$.
- 7) Si trovi per quali valori di n (> 0) sussistono le relazioni
 - a) $x - 1 \mid x^n - 1$;
 - b) $x + 1 \mid x^n + 1$;
 - c) $x + 1 \mid x^n - 1$;
 nei casi favorevoli, si trovino i quozienti.
- 8) Si trovino $f, h, k \in Q[x]$ tali che $f \nmid h$, $f \nmid k$, $f \mid hk$.
- 9) Si calcoli in $C[x]$ il M.C.D. $(x^4 - 1, (x+i)^3(x^3 - 1))$.
- 10) Si dimostri che in $Q[x]$ $f = x^2 - 1$, $g = x^3 + 2$ sono coprimi, e si trovino $h, k \in Q[x]$ tali che $fh + gk = 1$.
- 11) Si dimostri che $f = x^2 - x - 1$ è irriducibile in $Q[x]$.
- 12) Sia p un numero primo. Si dimostri che $f = x^n - p$ è irriducibile in $Q[x]$ per ogni $n \geq 1$.
- 13) Sia $f = \sum_{h=0}^n a_h x^h \in Q[x]$ e si supponga $a, a_1, \dots, a_n \in Z$. Si dimostri che se $u = r/s$ ($r, s \in Z$) è uno zero di f , allora $r \mid a_0$, $s \mid a_n$.
- 14) Sia $f \in K[x]$. Si dimostri che risulta $f' \mid f$ se e solo se $f = a(x - b)^n$ per convenienti $a, b \in K$, $n \in N$. (Per la *necessità*, si suggerisce di fare induzione sul grado di f).
- 15) Si scriva un $f \in R[x]$ che abbia -1 come zero doppio e 0 come zero triplo.
- 16) Si provi che $f = x^4 + x$ non ha zeri multipli in K .
- 17) Si dimostri che se $u \in C$ è uno zero di molteplicità r per $f \in R[x] \subseteq C[x]$, allora anche il coniugato \bar{u} è tale.
- 18) Si fattorizzi $f = x^4 + 4$ in fattori irriducibili in $Q[x]$.

INDICE ANALITICO e dei SIMBOLI

- Affissa 14.5.
 Algebra (teorema fondamentale dell'-) 15.11.
 Anomalia 14.7.
 Appartenenza $x \in S$, $S \ni x$ 1.1.
 Applicazione $f: S \rightarrow T$ 2.1.
 Aritmetica (teorema fondamentale dell'-) 9.1.
 Associativa (proprietà -) 3.2.
 b -adica (scrittura -) 10.
 Bigettiva (applicazione -) 2.5.
 Binomio (formula del -) 6.5.
 Cartesiano (prodotto -) $S \times T$ 1.9.
 Ciclica (permutazione -) (i_1, i_2, \dots) 5.4.
 Cinese (teorema - del resto) 11.9.
 Codominio 2.1.
 Coefficiente binomiale $\binom{n}{k}$ 4.6.
 Coefficiente direttivo 15.5.
 Combinazioni 4.7.
 Complessi (numeri -) C 14.1.
 Composta (applicazione -) $g \circ f$ 3.2.
 Congruenza (modulo m) $x \equiv y \pmod{m}$ 11.1.
 Coniugato (di un complesso z) \bar{z} 14.4.
 Controimmagine (di un insieme V) $f^{-1}(V)$ 2.6.
 Coppia ordinata (x, y) 1.9.
 Corpo K 14.1.
 De Moivre (formula di -) 14.9.
 Derivata 15.3.
 Differenza (insieme -) $S \setminus T$ 1.6.
 Disgiunti (insiemi -) 1.3.
 Divisibilità, Divisore $b | a$ 7.4., 15.8.
 Divisione 6.9., 15.7.
 Dominio 2.1.
 Ennupla (n -pla) (x_1, x_2, \dots, x_n) 1.9.
 Estremo superiore 13.2.
 Euclide (algoritmo di -) 8.2., 15.8.
 Eulero (funzione di -) $\varphi(n)$ 9.5.
 Fattoriale $n!$ 4.4.
 Fattorizzazione unica 9.1., 15.10.
 Fermat (teorema di -) 11.11.
 Forma trigonometrica (di un complesso) 14.6.
 Funzione (= applicazione) $f: x \mapsto f(x)$ 2.1.
 Funzioni razionali intere $K[x]$ 15.1.
 Gauss (piano di Argand-) 14.5.
 Grado (di una funzione razionale intera) 15.5.
 Identità (= applicazione identica) ~~is~~ 2.5.
 Immaginario (coefficiente dell'-; unità -) $Im(z)$; 14.3.
 Immagine (di un'applicazione ecc.) ~~f(S)~~ 2.2.
 Immagine (di un elemento) $f(s)$ 2.1.
 Inclusione (tra insiemi) $S \subseteq T$, $T \supseteq S$ 1.2.
 Inclusione propria $S \subset T$, $T \supset S$ 1.2.
 Induzione (principio di -; 1° forma) 6.3.
 Induzione (principio di -; 2° forma) 6.7.
 Iniettiva (applicazione -) 2.4.
 Insieme 1.1.
 Interi (numeri -) Z 6.1.
 Intersezione (insieme -) $S \cap T$ 1.3.
 Inversa (applicazione -; immagine -) f^{-1} , $f^{-1}(V)$ 2.6.
 Irrazionali (numeri -) 13.2.

Irriducibile 15.9.

Limitato (insieme - superiormente) 13.2.

Maggiorante 13.2.

Massimo comun divisore M.C.D. (a, b)
8.1., 15.8.

Minimo comune multiplo m.c.m. [a, b]
8.5., 15.8.

Modulo (di una congruenza) 11.1.

Modulo (di un numero) $|z|$ 7.1., 14.6.

Molteplicità (di uno zero) 15.3.

Multiplo 7.4.

Naturali (numeri -) N 6.2.

Norma 14.4.

n-pla (leggi: *ennupla*) (x_1, x_2, \dots, x_n) 1.9.

Operazione 3.1.

Ordinamento (assioma del buon -) 6.2.

Parti (insieme delle -) $\mathcal{P}(S)$ 1.7.

Permutazioni (di un insieme S) Σ_S 4.4.

Primi tra loro 8.3.

Primo (numero -) 7.6., 15.9.

Prodotto cartesiano $S \times T$ 1.8.

Proprio (divisore -) 15.9.

Proprio (sottoinsieme -) $S \subset T$ $T \supset S$ 1.2.

Radice n -esima dell'unità 14.10.

Radice (= zero) 15.4.

Razionali intere (funzioni -) $K[x]$ 15.1.

Razionali (numeri -) Q 12.1.

Reale (parte -) $Re(z)$ 14.3.

Reali (numeri -) R 13.1.

Ruffini (Teorema di -) 15.7.

Semplice (zero -) 15.13.

Sottoinsieme $S \subseteq T$, $T \supseteq S$ 1.2.

Sottoinsieme proprio $S \subset T$, $T \supset S$ 1.2.

Suriettiva (applicazione -) 2.3.

Tartaglia (triangolo di -) 4.8.

Trasposizione 5.6.

Triangolare (disuguaglianza -) 14.6.

Unione (insieme -) $S \cup T$ 1.4.

Valore assoluto $|z|$ 7.1., 14.6.

Vuoto (insieme -) \emptyset 1.2.

Zero (= radice) 15.4.

ALFABETO GRECO

A α	alfa	B β	beta	G γ	gamma
D δ	delta	E ε	epsilon	Z ζ	zeta
H η	eta	Θ ϑ, θ	theta	I ι	iota
K κ	kappa	Λ λ	lambda	M μ	mi (o mu)
N ν	ni (o nu) (e da distinguere da v epsilon e da v corsivo)				
Ξ ξ	xi (csi)	O \circ	òmicron	Π π	pi (greco)
P ρ	ro	Σ σ, ς	sigma	T τ	tau
Y υ	ipsilon (da distinguere da v ni e da v corsivo)			Φ φ, ϕ	fi
X χ	chi	Ψ ψ	psi	Ω ω	omega

Autore: Benedetto Scimemi - Dipartimento di Matematica - Università di Padova

Titolo: Algebrella *un'introduzione al Corso di Algebra*

Redazione, disegni, impostazione grafica: Giorgio Villella

Editore: Decibel editrice, ditta individuale di Giorgio Villella
via del Santo, 30 - 35123 Padova, tel. 049/36674

Distribuzione esclusiva: Zanichelli editore via Irnerio, 34 - 40126 Bologna,
tel. 051/293111 - telex 521587 Zaned I - telefax 051/249782 - 293224

Codice volume del catalogo Zanichelli per le ordinazioni: 93B.6580

Copyright © 1989 Decibel Editrice, Padova:

Il commercio di fotocopie di questo libro è vietato e verrà perseguito con tutti i mezzi consentiti dalla legge.

Fotocomposizione: Composizioni Grafiche - Via Pellizzo, 17A - 35123 Padova

Stampa: Grafiche TPM - Via Vigonese, 52A - 35127 Camin (Pd)

Prima edizione: 1972, **seconda edizione:** 1978, **terza edizione:** settembre 1989

Libri decibel di matematica per l'università, con codice volume del catalogo Zanichelli per le ordinazioni:

Per i corsi di algebra:

- B. SCIMEMI Gruppi (pp. 56) cod. 93B.6592
- C. PROCESI Elementi di teoria dei gruppi (pp. 48) cod. 93B.6582
- C. PROCESI Elementi di teoria degli anelli (pp. 40) cod. 93B.6584
- C. PROCESI Elementi di teoria di Galois (pp. 96) cod. 93B.6588
- R. PROCESI CIAMPI Elementi di algebra lineare (pp. 56) cod. 93B.6586
- A. FACCHINI Algebra × Informatica (pp. 120) cod. 93B.6594

Introduzione al corso di Analisi matematica:

- G. DE MARCO Analisi zero (pp. 80) cod. 93B.6590

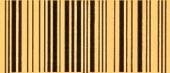
Per i biologi:

- A.C. CAPELO Modelli Matematici in Biologia (pp. 200) cod. 93B.6596

BENEDETTO SCIMEMI Algebrella

SCIMEMI*ALGEBRETTA (DB)

ISBN 978-88-08-06580-3



9 788808 065803

8 9 0 1 2 3 4 5 6 (60B)

Distribuzione esclusiva Zanichelli Editore S.p.A.

Al pubblico € 8,60***