

CAPITOLO 1

Gli insiemi

*O sol che sani ogni vista turbata,
tu mi contenti sì quando tu solvi,
che, non men che saver, dubbiar m'aggrata.*
Dante, Inferno, XI, 91–93.

In questo capitolo vengono introdotte le nozioni di insieme, relazione, relazione di equivalenza, applicazione, nozioni che sono alla base non solo di tutta l'algebra ma di tutta la matematica. È quindi da considerarsi come un capitolo che fornisce il linguaggio base della matematica (e di questo testo in particolare). Viene poi data una definizione assiomatica dell'insieme \mathbb{N} dei numeri naturali, attraverso i postulati di Peano. Negli ultimi paragrafi inoltre vengono date le definizioni fondamentali di cardinalità di insiemi e di calcolo combinatorio.

1.1. Insiemi e operazioni tra insiemi

Un *insieme* è semplicemente una collezione di oggetti. Ad esempio, sono insiemi i seguenti:

- (a) L'insieme di tutti gli studenti di una scuola;
- (b) L'insieme di tutti i ragazzi nati nel 1978;
- (c) L'insieme \mathbb{N} di tutti i numeri $0, 1, 2, 3, \dots$;
- (d) L'insieme di tutte le circonferenze del piano.

Il concetto di insieme verrà assunto come *primitivo*, nel senso che non può essere definito in termini di altre nozioni più elementari. D'altra parte ognuno ha un'idea intuitiva di tale concetto, che corrisponde all'attività elementare di "raggruppare". Generalmente un insieme si indica con una lettera maiuscola. Gli oggetti che compongono un insieme S prendono il nome di *elementi* di S , e si indicano con una lettera minuscola. Per indicare che un elemento s appartiene ad un insieme S si scrive $s \in S$. Per indicare che un elemento s non

appartiene a S si scrive $s \notin S$. L'insieme vuoto, ossia l'insieme che non contiene nessun elemento, si indica con il simbolo \emptyset . Si dice *sottoinsieme* di S un insieme T tale che ogni elemento t di T è anche elemento di S : si scrive $T \subseteq S$. Per indicare che la inclusione è propria, ossia che esiste almeno un elemento di S che non appartiene a T , si scrive $T \subset S$ o $T \not\subseteq S$. Per indicare che un insieme T non è un sottoinsieme di S si scrive $T \not\subseteq S$. L'insieme vuoto è un sottoinsieme di ogni insieme. Si faccia attenzione alla differenza tra il simbolo \in di *appartenenza* (di un *elemento* ad un *insieme*) e il simbolo \subseteq di *essere contenuto* (di un *insieme* in un altro). Due insiemi A e B si dicono *uguali* se $A \subseteq B$ e $B \subseteq A$. Per dimostrare che due insiemi sono uguali, rifacendosi alla definizione, si deve quindi provare la doppia inclusione. Un insieme S si può definire o elencando tra parentesi graffe i suoi elementi, oppure specificando una sua proprietà caratteristica. Ad esempio, se indichiamo con \mathbb{N} l'insieme dei numeri naturali $0, 1, 2, 3, \dots$, l'insieme A costituito dai numeri naturali minori di 10 può scriversi in uno dei due modi che seguono:

$$A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

oppure

$$A = \{n \in \mathbb{N} \mid n < 10\}$$

che si legge: A è l'insieme degli elementi n in \mathbb{N} tali che n è minore di 10.

Si osservi che si è parlato dell'insieme \mathbb{N} dei numeri naturali senza che se ne sia stata data una definizione. D'altra parte c'è pur bisogno di fare qualche esempio, e tutti conoscono questi numeri. Per il momento quindi li diamo per noti: nel §1.4 se ne darà una definizione assiomatica attraverso i Postulati di Peano. Daremo per noti per il momento anche l'insieme \mathbb{Z} degli interi, gli insiemi \mathbb{Q} dei razionali, \mathbb{R} dei numeri reali e \mathbb{C} dei numeri complessi.

Qui di seguito vengono elencati i principali simboli, che sono fondamentali nel linguaggio matematico, perché permettono di scrivere in forma compatta frasi che altrimenti sarebbero lunghe.

SIMBOLO	DA LEGGERSI
\forall	per ogni, qualsiasi
\exists (\nexists)	esiste (non esiste)
$\exists!$	esiste uno e un solo
\in (\notin)	appartiene (non appartiene)
\subseteq ($\not\subseteq$)	è contenuto (non è contenuto)
\subset , $\not\subseteq$	è contenuto propriamente
\Rightarrow (\nRightarrow)	implica (non implica)
\Leftrightarrow	se e solo se
tale che	

Così, ad esempio, la frase *A è contenuto propriamente in B se e solo ogni elemento a in A appartiene a B ed esiste almeno un elemento b di B che non appartiene ad A* si può scrivere:

$$A \subset B \iff [\forall a. a \in A \implies a \in B] \text{ ed } \exists b \in B \mid b \notin A]$$

Dati due insiemi A e B , si definisce loro intersezione, e si indica con $A \cap B$, l'insieme di tutti gli elementi che appartengono ad A e a B . In simboli,

$$A \cap B \stackrel{\text{def}}{=} \{x \mid x \in A \text{ e } x \in B\}.$$

L'unione di due insiemi A e B , che si indica con $A \cup B$, è l'insieme degli elementi che appartengono ad A o a B . In simboli,

$$A \cup B \stackrel{\text{def}}{=} \{x \mid x \in A \text{ o } x \in B\}.$$

L'unione e l'intersezione di due insiemi corrispondono ai connettivi logici "o" ed "e". Il connettivo "o" ha il significato di "o/e" in italiano, o al latino "vel". Dire quindi che $x \in A$ o $x \in B$ non esclude che x possa stare in entrambi.

1.1.1 ESEMPIO. Siano $A = \{a, b, c, d, e, f\}$ e $B = \{a, d, g, h\}$. Allora

$$A \cap B = \{a, d\}, \quad A \cup B = \{a, b, c, d, e, f, g, h\}. \quad \square$$

L'unione e l'intersezione di due insiemi si possono generalizzare al caso di una famiglia non vuota $\{A_\alpha\}_{\alpha \in I}$ di insiemi:

$$\bigcup_{\alpha \in I} A_\alpha \stackrel{\text{def}}{=} \{x \in A_\alpha \text{ per qualche } \alpha \in I\}$$

$$\bigcap_{\alpha \in I} A_\alpha \stackrel{\text{def}}{=} \{x \in A_\alpha \text{ per ogni } \alpha \in I\}$$

Sia ora U un fissato universo, ossia un insieme che contiene tutti gli oggetti che ci possono interessare. Si definisce complemento di un insieme A (rispetto all'universo U) l'insieme di tutti gli elementi di U che non appartengono ad A . Esso si indica con \complement{A} . Quindi:

$$\complement{A} \stackrel{\text{def}}{=} \{x \in U \mid x \notin A\}.$$

Il complemento di un insieme A corrisponde al connettivo "non". Il complemento relativo di un insieme A in un insieme B è costituito da tutti gli elementi di B che non stanno in A . Si indica con $B \setminus A$ e prende anche il nome di insieme differenza di B ed A :

$$B \setminus A \stackrel{\text{def}}{=} \{x \in B \mid x \notin A\}.$$

I disegni di figura 1.1, noti come diagrammi di Venn, rappresentano le varie definizioni date.

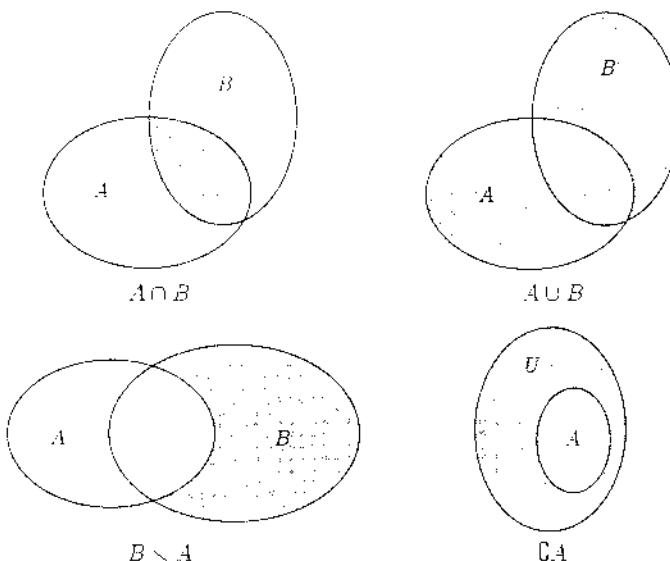


FIGURA 1.1

Negli esercizi vengono riportate le relazioni che legano tali insiemi. Lo studente è invitato a dimostrarle, utilizzando la doppia inclusione tra insiemi per dimostrarne l'uguaglianza.

Un altro concetto che si può definire a partire da due insiemi A e B è il loro *prodotto cartesiano*, che si indica con $A \times B$. Esso consiste di tutte le coppie ordinate (a, b) , dove il primo elemento varia in A e il secondo varia in B :

$$A \times B \stackrel{\text{def}}{=} \{(a, b) \mid a \in A, b \in B\}.$$

Ad esempio, se $A = \{3, 4\}$ e $B = \{2, 5\}$, allora

$$A \times B = \{(3, 2), (3, 5), (4, 2), (4, 5)\}.$$

Un importante insieme associato ad un dato insieme A è infine l'*insieme delle parti* (o dei sottoinsiemi) di A , che si indica con $\mathcal{P}(A)$. Risulta:

$$\mathcal{P}(A) \stackrel{\text{def}}{=} \{B \mid B \subseteq A\}.$$

Si noti che gli *elementi* di $\mathcal{P}(A)$ sono *sottoinsiemi* (o parti) di A . Il *sottoinsieme* di A che contiene il solo elemento a si chiama *singleton* e viene indicato

con $\{a\}$, per distinguerlo dall'elemento di A , a . Quindi, $a \in A$, ma $a \notin \underline{\mathcal{P}(A)}$. Invece, $\{a\} \in \mathcal{P}(A)$, e $\{a\} \subseteq A$.

Ad esempio, se $A = \{\bar{a}, \bar{b}, \bar{c}\}$, sarà

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

1.1.2 OSSERVAZIONE. Sia $U = \{a_1, a_2, a_3, \dots, a_n\}$ un fissato *universo*, costituito da un numero finito di elementi numerati da 1 a n . È utile, per impostare al calcolatore un problema riguardante gli insiemi, la seguente notazione per i sottoinsiemi di U . Ogni sottoinsieme A di U viene indicato sotto forma di n -pla (i_1, i_2, \dots, i_n) , dove i_j vale 1 o 0 a seconda che il corrispondente elemento a_j stia o non stia in A . Ad esempio, se

$$U = \{a_1, a_2, a_3, a_4, a_5, a_6\}, \quad A = \{a_2, a_4, a_5\}$$

A si scriverà nella forma:

$$A : (0, 1, 0, 1, 1, 0). \quad \square$$

ESERCIZI.

1. Si provi che $(A \cup B) \cup C = A \cup (B \cup C)$ (proprietà associativa dell'unione).
2. Si provi che $(A \cap B) \cap C = A \cap (B \cap C)$ (proprietà associativa dell'intersezione).
3. Si provi che $A \cup B = A$ se e solo se $B \subseteq A$.
4. Si provino le seguenti proprietà distributive:

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$

(distributività dell'intersezione rispetto all'unione):

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$

(distributività dell'unione rispetto all'intersezione):

5. Si provi che $\complement(A \cap B) = \complement A \cup \complement B$ e che $\complement(A \cup B) = \complement A \cap \complement B$.

ESERCIZI DI PROGRAMMAZIONE.

1. Utilizzando la notazione dei sottoinsiemi di un dato universo

$$U = \{a_1, a_2, \dots, a_n\}$$

sotto forma di n -ple di 0 e 1 come suggerito alla fine di questo paragrafo, si scriva un programma che trovi unione, intersezione, complementari, ecc., di sottoinsiemi di U .



CONTROLLO.

1. L'unione di due insiemi è ...
2. Gli elementi del prodotto cartesiano di due insiemi sono ...
3. L'insieme delle parti di un insieme A ha come elementi ...

1.2. Relazioni

Il concetto di relazione è legato, come mostra la seguente definizione, alla nozione di prodotto cartesiano, introdotta nel paragrafo precedente.

1.2.1 DEFINIZIONE. Una *relazione* ϱ da un insieme A ad un insieme B è un sottoinsieme del prodotto cartesiano $A \times B$. Quando $A = B$, allora si parla di relazione ϱ (*definita*) su A .

Invece che scrivere che la coppia (a, b) sta in ϱ (ossia che $(a, b) \in \varrho$), si usa scrivere $a \varrho b$. \square

1.2.2 ESEMPI DI RELAZIONI.

- (a) La relazione \leq , definita su \mathbb{N} .
- (b) La relazione di *essere amico*, definita su un dato insieme A di persone.
- (c) La relazione ϱ costituita da tutte le coppie (a, b) di $\mathbb{R} \times \mathbb{R}$ tali che $a + b = 1$: geometricamente, questa relazione coincide con la retta $x + y = 1$ del piano $\mathbb{R} \times \mathbb{R}$. \square

Ci sono diversi modi per rappresentare una relazione. Il primo consiste nel collegare con una freccia il primo con il secondo elemento di una coppia appartenente ad una relazione ϱ . Quindi

$$\boxed{(a, b) \in \varrho \iff a \xrightarrow{\varrho} b}.$$

Spesso in luogo della scrittura $a \varrho b$ si scrive $b = \varrho(a)$.

La relazione \leq definita su $S = \{1, 2, 3\}$, ossia

$$\{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\},$$

si potrà quindi rappresentare come in figura 1.2.

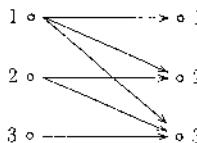


FIGURA 1.2

Un altro modo di rappresentare una relazione ϱ da A a B è il seguente: si costruisce una *matrice* (ossia una *tavella*) che ha tante righe quanti sono gli elementi di A e tante colonne quanti sono gli elementi di B , e che nella posizione (a, b) , ossia all'incrocio tra la riga che contiene l'elemento $a \in A$ e la b -esima colonna, ossia la colonna che contiene l'elemento $b \in B$, contiene 1 o 0

a seconda che la coppia (a, b) appartenga o no a ϱ . La matrice rappresentativa della relazione di cui sopra è la seguente:

ϱ	1	2	3
1	1	1	1
2	0	1	1
3	0	0	1

1.2.3 DEFINIZIONE. Se ϱ è una relazione da A a B , la *relazione inversa* ϱ^{-1} è la relazione da B ad A definita da

$$b \varrho^{-1} a \iff a \varrho b. \quad \square$$

1.2.4 ESEMPIO. Sia ϱ la relazione da $A = \{1, 2, 3, 4\}$ a $B = \{2, 5, 6, 7, 8\}$ data da

$$\varrho = \{(1, 2), (1, 5), (2, 5), (3, 5), (3, 2), (3, 7), (3, 8)\}.$$

La relazione inversa (da B ad A) è data da

$$\varrho^{-1} = \{(2, 1), (2, 3), (5, 1), (5, 2), (5, 3), (7, 3), (8, 3)\}.$$

Graficamente, la situazione è rappresentata in figura 1.3. \square

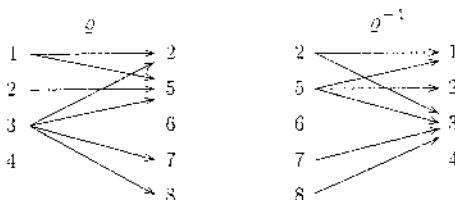


FIGURA 1.3

Esistono relazioni che verificano ulteriori proprietà: un importante esempio di tali relazioni è dato dalle relazioni di equivalenza.

1.2.5 DEFINIZIONE. Una relazione ϱ definita su un insieme A si dice *relazione di equivalenza* se verifica le seguenti proprietà:

1. *Proprietà riflessiva*: $a \varrho a \quad \forall a \in A$;
2. *Proprietà simmetrica*: $a \varrho b \implies b \varrho a \quad \forall a, b \in A$;
3. *Proprietà transitiva*: $a \varrho b \text{ e } b \varrho c \implies a \varrho c \quad \forall a, b, c \in A$.

Se ϱ è una relazione di equivalenza e $a \varrho b$, allora si dice che a è *equivalente* a b . \square

1.2.6 ESEMPI DI RELAZIONI DI EQUIVALENZA.

- (a) La relazione di *uguaglianza* definita su un insieme A ;

- (b) la relazione ϱ definita su un insieme A , che dichiara in relazione tutti gli elementi, ossia $a \varrho b \forall a, b \in A$;
- (c) la relazione di *avere la stessa età* definita su un insieme A di persone;
- (d) la relazione di *similitudine* definita nell'insieme A di tutti i triangoli del piano. \square

Nei capitoli seguenti si incontreranno molti altri esempi di relazioni di equivalenza.

1.2.7 ESEMPI DI RELAZIONI CHE NON SONO DI EQUIVALENZA.

- (e) La relazione \leq definita su \mathbb{N} ;
- (f) la relazione di *essere amico*, definita su un insieme A di persone;
- (g) la relazione di *perpendicolarità* definita sull'insieme A di tutte le rette del piano. \square

1.2.8 DEFINIZIONE. Sia ϱ una relazione di equivalenza definita su A . Si definisce *classe di equivalenza modulo ϱ* di un elemento $a \in A$, e si denota con $[a]$, l'insieme di tutti gli elementi di A che sono equivalenti ad a , ossia

$$[a] \stackrel{\text{def}}{=} \{b \in A \mid b \varrho a\}.$$

Ad esempio, nella relazione di equivalenza (a) data dall'uguaglianza, le classi di equivalenza sono costituite dai *singletons* (cioè dai sottoinsiemi ridotti ad un solo elemento) $\{a\}$ al variare di $a \in A$. Nella relazione (b) di cui sopra, esiste un'unica classe di equivalenza, data dall'intero insieme A . Nella relazione (c), in ogni classe di equivalenza ci sono tutte e sole le persone che hanno la stessa età: ogni classe può quindi essere *etichettata* con il numero corrispondente alla età comune a tutte le persone che appartengono a quella classe.

Una classe di equivalenza $[a]$ verrà anche denotata con \bar{a} . \square

La seguente proposizione spiega come il passaggio dagli *elementi* di A alle *classi di equivalenza* di A trasforma la *equivalenza (tra elementi)* in *uguaglianza (tra classi)*. Gli esempi di cui sopra mostrano chiaramente questo passaggio.

1.2.9 PROPOSIZIONE. *Sia ϱ una relazione di equivalenza definita su un insieme A . Allora,*

$$[a] = [b] \iff a \varrho b.$$

Dimostrazione. Sia $[a] = [b]$. Per la riflessività di ϱ , $\forall b \in A$ è $b \varrho b$, onde $b \in [b]$. Essendo per ipotesi $[a] = [b]$, segue che $b \in [a]$, da cui, per definizione di classe di equivalenza, $b \varrho a$ e, per la simmetria, $a \varrho b$.

Viceversa, si supponga $a \varrho b$. Faremo vedere la doppia inclusione $[a] \subseteq [b]$ e $[b] \subseteq [a]$. Sia $c \in [a]$. Allora $a \varrho c$. Quest'ultima relazione, assieme alla $b \varrho a$

implicano (transitività) $b \varrho c$ e quindi (per definizione di $[b]$), $c \in [b]$. Abbiamo dimostrato che $[a] \subseteq [b]$. La dimostrazione dell'altra inclusione è analoga (scambiando il ruolo di a e b). Quindi $[a] = [b]$. \square

1.2.10 DEFINIZIONE. Sia ϱ una relazione di equivalenza definita su un insieme A . Si definisce *insieme quoziente* di A rispetto a ϱ , e si indica con A/ϱ , l'insieme di tutte le classi di equivalenza modulo ϱ . In simboli,

$$A/\varrho \stackrel{\text{def}}{=} \{[a] \mid a \in A\}.$$

La proposizione precedente dice che elementi a che erano *equivalenti* in A si trasformano in un unico elemento, $[a]$, di A/ϱ . \square

La definizione e il teorema seguenti sono di fondamentale importanza.

1.2.11 DEFINIZIONE. Dicesi *partizione* di un insieme A una collezione di parti (o sottoinsiemi) A_α non vuoti di A tali che:

1. $\bigcup_\alpha A_\alpha = A$ (le parti *ricoprono* A);
2. $A_\alpha \cap A_\beta \neq \emptyset \iff A_\alpha = A_\beta$ (le parti o *coincidono* o sono *disgiunte*). \square

Una partizione di un insieme A è quindi un insieme Π di sottoinsiemi non vuoti di A tali che ogni elemento di A appartiene ad uno e un solo dei sottoinsiemi dati.

1.2.12 TEOREMA. *Sia ϱ una relazione di equivalenza in A . Le classi di equivalenza di A modulo ϱ costituiscono una partizione di A .*

Dimostrazione. (1) *Ricoprono A :* infatti, essendo $a \varrho a$ per ogni $a \in A$, ogni $a \in A$ appartiene alla sua classe di equivalenza.

(2) *Le classi di equivalenza o coincidono o sono disgiunte:* sia $z \in [a] \cap [b]$, cioè siano $[a]$ e $[b]$ non disgiunte. Allora $z \varrho a$ e $z \varrho b$, da cui, per simmetria e transitività, $a \varrho b$. In base alla Proposizione 1.2.9, $[a] = [b]$, ossia le due classi coincidono. \square

1.2.13 TEOREMA. *Ogni partizione di un insieme A determina su A una relazione di equivalenza, per la quale i sottoinsiemi della partizione sono le classi di equivalenza.*

Dimostrazione. Indicati con A_α i sottoinsiemi della partizione, basta definire la seguente relazione:

$$a \varrho b \iff \exists A_\alpha \mid a, b \in A_\alpha.$$

Si tratta ovviamente di una relazione di equivalenza, le cui classi sono le parti A_α . \square

I due teoremi precedenti asseriscono che i due concetti di relazione di equivalenza su di un insieme A e di partizione di A coincidono.

In definitiva, le proprietà di riflessività, simmetria e transitività, proprie delle relazioni di equivalenza, caratterizzano oggetti che *non sono (necessariamente) uguali*, ma che tali possono *venir considerati* limitatamente a particolari scopi. Esistono invece altre proprietà che confrontano oggetti tra loro diversi, e dicono ad esempio quando uno dei due oggetti è "più grande" o "più piccolo" di un altro. Precisiamo tali proprietà e le relazioni ad esse legate.

1.2.14 DEFINIZIONE. Una relazione ϱ definita su un insieme A si dice *antisimmetrica* se

$$a \varrho b, b \varrho a \rightarrow a = b. \quad \square$$

1.2.15 DEFINIZIONE. Una relazione ϱ definita su di un insieme A si dice *relazione di ordine parziale* se è riflessiva, antisimmetrica e transitiva. L'insieme A dicesi allora *insieme parzialmente ordinato* dalla relazione ϱ . \square

1.2.16 ESEMPI DI RELAZIONI DI ORDINE PARZIALE.

- (a) Nell'insieme $\mathcal{P}(X)$ la relazione \subseteq .
- (b) Nell'insieme \mathbb{N} l'ordinamento "naturale" \leq , quello cioè per cui $a \leq b$ se e solo se esiste un $c \in \mathbb{N}$ tale che $b = a + c$, è una relazione d'ordine.
- (c) La relazione \supseteq in $\mathcal{P}(X)$ e la relazione \geq in \mathbb{N} sono ancora relazioni d'ordine parziale, inverse rispettivamente della \subseteq e della \leq . \square

L'aggettivo *parziale* nella definizione di relazione d'ordine sta a significare che non si richiede che tutte le coppie (a, b) di elementi di un insieme A siano tra loro confrontabili, tali cioè che $a \varrho b$ o $b \varrho a$ per ogni $a, b \in A$. Se avviene che *tutte* le coppie sono confrontabili si dice che l'insieme A è *totalmente ordinato* o una *catena*. La relazione \subseteq è un ordinamento parziale, mentre la relazione \leq dell'esempio 1.2.16(b) è un ordinamento totale.

In genere, per indicare che una relazione ϱ definita su un insieme A è una relazione d'ordine (totale o parziale) si usa il simbolo \preccurlyeq . Nel caso in cui l'insieme A parzialmente (o totalmente) ordinato sia finito possiamo rappresentarlo graficamente congiungendo fra loro con una linea spezzata due elementi a e b dal basso verso l'alto se e solo se risulta $a \preccurlyeq b$. Tale linea spezzata si ridurrà ad un segmento di estremi a e b se non esistono elementi intermedi c tali che $a \preccurlyeq c \preccurlyeq b$. Ad esempio, sia $A = \mathcal{P}(X)$ dove $X = \{a, b, c\}$ e si consideri ordinato rispetto alla relazione \subseteq . Allora

$$\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

e la sua rappresentazione grafica è data in figura 1.4.

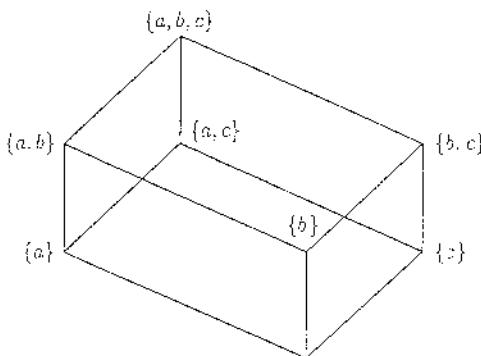


FIGURA 1.1

ESERCIZI.

1. Fissato $n \in \mathbb{N}$, sia ϱ la seguente relazione definita su \mathbb{Z} :

$$a \varrho b \pmod{n} \iff a - b = kn, \text{ } k \text{ intero.}$$

Si provi che ϱ è una relazione di equivalenza. Si studino le classi di equivalenza. Tale relazione prende il nome di *congruenza modulo n*, e si indica col simbolo \equiv_n . Si esamini in dettaglio il caso $n = 5$.

2. Si provi che le condizioni che definiscono una relazione di equivalenza sono indipendenti, dando
- un esempio di relazione riflessiva e simmetrica, ma non transitiva;
 - un esempio di relazione riflessiva e transitiva, ma non simmetrica;
 - un esempio di relazione simmetrica e transitiva, ma non riflessiva.
3. Sia ϱ la relazione su \mathbb{N} definita al modo seguente per ogni $a, b \in \mathbb{N}$:

$$a \varrho b \iff \exists c \in \mathbb{N} \mid b = ac.$$

Si dica se si tratta di una relazione d'ordine. E se tale relazione si pensa definita sugli interi \mathbb{Z} ?

Negli esercizi che seguono si consiglia di scrivere una relazione sotto forma di matrice.

ESERCIZI DI PROGRAMMAZIONE.

- Scrivere un programma che determini se una relazione definita su un insieme A di n elementi è riflessiva.
- Scrivere un programma che determini se una relazione definita su un insieme A di n elementi è simmetrica.
- Scrivere un programma che determini se una relazione definita su un insieme A con n elementi è transitiva.
- Scrivere un programma che determini se una relazione definita su un insieme A con n elementi è antisimmetrica.

5. Scrivere un programma che determini se una relazione definita su un insieme A è una relazione di equivalenza, o se è una relazione d'ordine (e in questo caso riconoscere se si tratta di un ordinamento parziale o totale).



CONTROLLO.

1. Un sottoinsieme arbitrario del prodotto cartesiano $A \times B$ è sempre una relazione da A a B ?
2. Quali sono le condizioni cui deve soddisfare un sottoinsieme di $A \times A$ per essere un relazione di equivalenza?
3. Gli elementi dell'insieme quoziente di A rispetto ad una relazione di equivalenza sono ...
4. Come si può associare ad una partizione di un insieme A una relazione di equivalenza e viceversa?

1.3. Funzioni

Tra le relazioni tra due insiemi A e B hanno particolare importanza le applicazioni (o funzioni).

1.3.1 DEFINIZIONE. Una *funzione* (o *applicazione*) f da un insieme A ad un insieme B è una legge che associa ad *ogni* elemento a di A *un ben determinato* elemento $b \in B$. Si scrive

$$f : A \longrightarrow B .$$

In questo testo useremo anche il termine di *corrispondenza* come sinonimo di applicazione e funzione, anche se a volte in letteratura tale termine viene usato come sinonimo di relazione. L'insieme A dicesi *dominio* della funzione f , l'insieme B *codominio* di f , e l'elemento $b = f(a)$ si dice l'*immagine* di a mediante la f .

Il sottoinsieme F di $A \times B$ (ossia la *relazione* F da A a B) dato da $F = \{(a, f(a)) \mid a \in A\}$ prende il nome di *grafico* della funzione f . Per essere il grafico di una *funzione* f da A a B pertanto, un sottoinsieme F di $A \times B$ deve essere tale che *ogni* elemento di A compaia come primo elemento di *una e una sola* coppia di F . Si noti quindi che una funzione è una (particolare) relazione, mentre non è vero che una qualunque relazione è una funzione. \square

Ad esempio, la relazione ϱ dell'esempio 1.2.4 non è una funzione da A a B , perché l'elemento 4 non compare come primo elemento di una coppia, e inoltre, ad esempio, l'elemento 1 compare come primo elemento di due coppie distinte. Il grafico di una funzione potrà quindi essere come quello in figura 1.5 (b), ma non come quello in figura 1.5 (a).

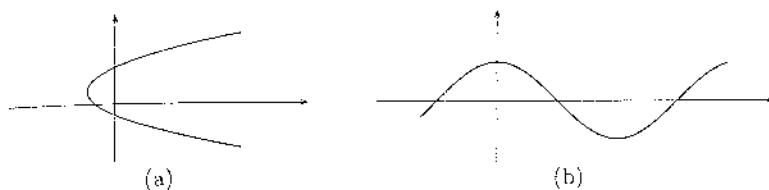


FIGURA 1.5

Sia f una funzione da A a B , e siano S e T due sottoinsiemi di A e B rispettivamente. L'immagine $f(S)$ di S mediante f è il sottoinsieme

$$f(S) \stackrel{\text{def}}{=} \{b \in B \mid b = f(s) \text{ per qualche } s \in S\}$$

L'immagine $f(A)$ si indica anche con $\text{Im } f$.

L'immagine inversa o controimmagine di T mediante la f è il sottoinsieme

$$f^{-1}(T) \stackrel{\text{def}}{=} \{a \in A \mid f(a) \in T\}.$$

Nel caso in cui T sia ridotto ad un solo elemento t , cioè sia $T = \{t\}$, spesso anziché $f^{-1}(\{t\})$ scriveremo $f^{-1}(t)$.

1.3.2 DEFINIZIONE. Una funzione f da A a B si dice *iniettiva* se, per ogni $a, a' \in A$, $f(a) = f(a')$ implica $a = a'$, ossia se elementi distinti di A hanno immagini distinte in B .

In altre parole, un'applicazione iniettiva è tale che la controimmagine di ogni elemento di B o è ridotta al sottoinsieme vuoto \emptyset o ad un solo elemento. In modo espressivo si può dire che un'applicazione è iniettiva quando frecce che partono da punti distinti non colpiscono mai uno stesso bersaglio. \square

1.3.3 DEFINIZIONE. Una funzione f da A a B si dice *suriettiva* se $\text{Im } f = B$, ossia se per ogni $b \in B$ esiste un $a \in A$ tale che $f(a) = b$.

Per restare nel linguaggio delle frecce, un'applicazione è suriettiva quando ogni elemento del codominio è colpito da almeno una freccia. □

1.3.4 DEFINIZIONE. Una funzione f da A a B si dice *biiettiva* (o *biunivoca*) se è contemporaneamente iniettiva e suriettiva. \square

1.3.5 DEFINIZIONE. Si considerino le due applicazioni $f : A \rightarrow B$ e $g : B \rightarrow C$. Si definisce *applicazione composta* di f con g l'applicazione

$$g \circ f : A \longrightarrow C$$

data da

$$(g \circ f)(a) \stackrel{\text{def}}{=} g(f(a)) \quad \forall a \in A . \quad \square$$

1.3.6 ESEMPIO. Siano $A = B = C = \mathbb{Z}$. Sia $f : \mathbb{Z} \rightarrow \mathbb{Z}$ data da $f(x) = 2 - x^3$, e sia $g : \mathbb{Z} \rightarrow \mathbb{Z}$ data da $g(x) = 3 + x$. Allora

$$(g \circ f)(x) = g(f(x)) = g(2 - x^3) = 3 + (2 - x^3) = 5 - x^3.$$

In generale non ha senso considerare l'applicazione composta $f \circ g$ (se il codominio di g non coincide con il dominio di f). Ma, anche se avesse senso, come nell'esempio ora fatto, in genere è $g \circ f \neq f \circ g$. Infatti

$$(f \circ g)(x) = f(g(x)) = f(3 + x) = 2 - (3 + x)^3 \neq (g \circ f)(x).$$

L'operazione di composizione tra applicazioni è *associativa*, nel senso che se f , g e h sono applicazioni rispettivamente da A a B , da B a C e da C a D , allora risulta (cfr. esercizio 1.3.3)

$$h \circ (g \circ f) = (h \circ g) \circ f. \quad \square$$

ATTENZIONE. Si è visto che *ogni* relazione ϱ da A a B determina una relazione inversa da B ad A . Questo non vale per le funzioni, perché la relazione inversa di una funzione in genere non è una funzione. Tuttavia, nel caso in cui f sia un'applicazione *biettiva* da A a B , allora l'immagine inversa di *ogni* singleton $\{b\}$ di B , $f^{-1}(\{b\})$, è un singleton, $\{a\}$, dove a è quell'*unico* elemento tale che $f(a) = b$. Ogni applicazione *biettiva* f da A a B determina quindi una (*unica*) *applicazione* da B ad A , che si indica con f^{-1} , e che prende il nome di *applicazione inversa* della f , definita, per ogni $b \in B$, da

$$f^{-1}(b) \stackrel{\text{def}}{=} a \quad \text{dove } a \text{ è quell'}\text{'unico} \text{ elemento } \in A \text{ tale che } f(a) = b.$$

L'applicazione i_X da X in X tale che $i_X(x) = x$ per ogni $x \in X$ prende il nome di *applicazione identica di X* . Se f è un'applicazione biettiva da A a B , allora risulta

$$f^{-1} \circ f = i_A, \quad f \circ f^{-1} = i_B. \quad \square$$

1.3.7 TEOREMA. *Sia X un insieme e sia $2 \stackrel{\text{def}}{=} \{0, 1\}$. Esiste una corrispondenza biunivoca tra $\mathcal{P}(X)$ e l'insieme 2^X di tutte le funzioni da X a $\{0, 1\}$.*

Dimostrazione. Sia A un sottoinsieme di X . Ad esso possiamo associare la sua *funzione caratteristica*, $\chi_A : X \rightarrow 2$ che è così definita:

$$\chi_A(x) = \begin{cases} 0 & \text{se } x \in X \setminus A \\ 1 & \text{se } x \in A. \end{cases}$$

Ebbene, l'applicazione $\chi : \mathcal{P}(X) \rightarrow 2^X$ che associa ad ogni elemento A di $\mathcal{P}(X)$ la sua funzione caratteristica χ_A è biunivoca (si provi!). \square

Chiudiamo questo paragrafo con un importante legame tra il concetto di relazione di equivalenza definita su un insieme A e il concetto di applicazione.

Sia f un'applicazione tra due insiemi A e B . Si può definire una relazione ϱ_f in A al modo seguente:

$$a \varrho_f b \iff f(a) = f(b).$$

È facile vedere che si tratta di una relazione di equivalenza. Per ogni $b \in B$ risulta $f^{-1}(\{b\}) = \emptyset$ se $b \notin \text{Im } f$, altrimenti $f^{-1}(\{b\}) = [a]$, dove a è un qualunque elemento di A tale che $f(a) = b$, e $[a]$ è la classe di equivalenza di a modulo ϱ_f . Se $b \in \text{Im } f$, il sottoinsieme $f^{-1}(\{b\})$ di A prende il nome di *fibra* sull'elemento b . L'insieme delle fibre è pertanto la partizione di A determinata dalla relazione di equivalenza ϱ_f , cioè le fibre sono gli elementi del quoziente A/ϱ_f .

Se viceversa partiamo da una relazione di equivalenza ϱ definita su un insieme A , detto A/ϱ l'insieme quoziente, resta individuata un'applicazione (suriettiva) π detta *proiezione canonica* sul quoziente:

$$\begin{aligned}\pi : A &\longrightarrow A/\varrho \\ a &\mapsto [a]\end{aligned}$$

tal che $\varrho_\pi = \varrho$. Questo legame tra applicazioni e relazioni di equivalenza indotte da queste giocherà un ruolo importante in molti teoremi fondamentali.

ESERCIZI.

1. Siano $A = \{1, 2, 3\}$, $B = \{0, 1\}$. Si determinino tutte le funzioni da A a B e quelle da B ad A . Quali tra queste sono suriettive, quali iniettive, quali biiettive?
2. Siano f e g due funzioni entrambe iniettive (suriettive) rispettivamente da A a B e da B a C . Si provi che $g \circ f$ è anch'essa iniettiva (suriettiva). Se ne deduca che la composizione di due applicazioni biiettive è biiettiva.
3. Siano f , g e h applicazioni rispettivamente da A a B , da B a C e da C a D . Si provi che

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

4. Posto $A = B = \mathbb{Z}$, si dica quali delle seguenti relazioni sono grafici di applicazioni:
 - (a) $\{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b = 2\}$;
 - (b) $\{(a, 3) \mid a \in \mathbb{Z}\}$;
 - (c) $\{(1, b) \mid b \in \mathbb{Z}\}$;
 - (d) $\{(a, a^2) \mid a \in \mathbb{Z}\}$;
 - (e) $\{(a+1, a) \mid a \in \mathbb{Z}\}$;
 - (f) $\{(a, |a|) \mid a \in \mathbb{Z}\}$;
 - (g) $\{(|a|, a) \mid a \in \mathbb{Z}\}$.

5. Di ciascuna delle relazioni precedenti che sono applicazioni si determini l'immagine, e si dica se è iniettiva e/o suriettiva. Nel caso in cui una sia biiettiva si determini l'inversa.
6. Siano A e B due insiemi non vuoti e sia f un'applicazione da A a B . Una funzione g da B ad A si dice inverso sinistro (destro) di f se $g \circ f = i_A$ ($f \circ g = i_B$). Si provi che f ammette inverso sinistro se e solo se f è iniettiva, f ammette inverso destro se e solo se f è suriettiva.
7. Sia $f : \mathbb{C} \rightarrow \mathbb{R}^+$ l'applicazione dai complessi ai reali positivi così definita: $f(a + ib) \stackrel{\text{def}}{=} a^2 + b^2$. Si dica se esiste una $g : \mathbb{R}^+ \rightarrow \mathbb{C}$ tale che $f \circ g = \text{id}_{\mathbb{R}^+}$ o una $g' : \mathbb{C} \rightarrow \mathbb{R}^+$ tale che $g' \circ f = \text{id}_{\mathbb{C}}$. Nel caso in cui una tale g o una tale g' esista, la si determini.
8. Sia f un'applicazione tra A e A' . Indicati con X e Y sottoinsiemi di A e con X' , Y' sottoinsiemi di A' , si provino le seguenti uguaglianze o inclusioni:
 - (a) $f(X \cup Y) = f(X) \cup f(Y)$;
 - (b) $f(X \cap Y) \subseteq f(X) \cap f(Y)$;
 - (c) $f^{-1}(X' \cup Y') = f^{-1}(X') \cup f^{-1}(Y')$;
 - (d) $f^{-1}(X' \cap Y') = f^{-1}(X') \cap f^{-1}(Y')$.

Si diano esempi che provino che nel punto (b) può valere l'inclusione propria.



ESEMCI DI PROGRAMMAZIONE.

1. Si scriva un programma che calcoli le funzioni caratteristiche di tutti i sottoinsiemi di un insieme finito X . Si verifichi che la funzione caratteristica di un insieme coincide con la notazione introdotta nell'osservazione 1.1.2, quando non avevamo ancora a disposizione la nozione di applicazione.



CONTROLLO.

1. Quali sono le condizioni perché una relazione da un insieme A ad un insieme B sia una funzione da A a B ?
2. Un'applicazione è iniettiva quando ...
3. Un'applicazione è suriettiva quando ...
4. Cosa si intende per controimmagine di un sottoinsieme mediante un'applicazione?
5. Cosa è la funzione caratteristica di un sottoinsieme di un insieme X ?

1.4. I numeri naturali e il principio di induzione matematica

Sia $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ l'insieme dei numeri naturali. Attraverso i seguenti assiomi, noti come postulati di Peano, verrà data una definizione di \mathbb{N} che, come avviene comunemente in algebra, *prescinde dalla natura degli elementi* di \mathbb{N} . La definizione formale di \mathbb{N} è la seguente:

L'insieme dei numeri naturali è costituito da una terna $(\mathbb{N}, \sigma, 0)$ dove \mathbb{N} è un insieme, σ è un'applicazione da \mathbb{N} in \mathbb{N} e 0 è un elemento di \mathbb{N} tali che

\mathbb{N}_1 σ è iniettiva;

\mathbb{N}_2 $0 \notin \text{Im } \sigma$:

\mathbb{N}_3 ogni sottoinsieme U di \mathbb{N} tale che

(a) $0 \in U$,

(b) $k \in U \implies \sigma(k) \in U \quad \forall k$

coincide con tutto \mathbb{N} .

Dato un elemento $n \in \mathbb{N}$, l'elemento $\sigma(n)$ si dice il *successivo* di n . Resta definita in \mathbb{N} allora in modo naturale una *relazione d'ordine*, \leq . Il postulato \mathbb{N}_3 è noto come il *principio di induzione matematica*. Si può dimostrare che se $(A, \sigma, 0)$ e $(A', \sigma', 0')$ sono due terne che verificano i postulati precedenti, allora esse sono "sostanzialmente identiche", nel senso che esiste una corrispondenza biiunivoca ϕ tra A e A' tale che $\sigma'(\phi(n)) = \phi(\sigma(n))$, cioè il successivo del trasformato è il trasformato del successivo. Quindi si può dire che i *postulati di Peano caratterizzano i numeri naturali*. Quello che si deve *postulare* (cioè accettare senza dimostrazione) è l'*esistenza* di un insieme \mathbb{N} verificante gli assiomi di Peano. L'intero edificio matematico è pertanto basato sull'accettazione dell'esistenza dei numeri naturali. Kronecker espresse questo fatto con la famosa frase: Dio creò i numeri naturali, tutto il resto è opera dell'uomo. Ora, dai soli postulati di Peano è possibile ricavare tutte le proprietà ben note dei numeri naturali. Ci serviranno alcune definizioni.

1.4.1 DEFINIZIONE. Una *operazione binaria* in un insieme S è un'applicazione da $S \times S$ in S , ossia una legge che associa ad ogni coppia di elementi di S un ben determinato elemento di S . \square

Ad esempio, l'unione tra sottoinsiemi di un insieme X è un'operazione binaria definita in $\mathcal{P}(X)$:

$$\begin{aligned} \cup : \mathcal{P}(X) \times \mathcal{P}(X) &\longrightarrow \mathcal{P}(X) \\ (A, B) &\longmapsto A \cup B. \end{aligned}$$

L'ordinaria addizione tra interi è un'operazione binaria definita in \mathbb{Z} :

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (a, b) &\longmapsto a + b. \end{aligned}$$

Il risultato dell'operazione di addizione, ossia l'elemento $a + b \in \mathbb{Z}$, prende il nome di *somma* di a e b .

Si parla anche di operazioni n -arie, definite per vari $n = 1, 2, \dots$. Si tratta di applicazioni da $\underbrace{S \times S \times \dots \times S}_{n \text{ copie}}$ in S . Per $n = 1$ un'operazione 1-aria definita su

S è un'applicazione da S ad S . Se $S = \mathcal{P}(X)$, un esempio di applicazione 1-aria è l'applicazione che associa ad ogni sottoinsieme di X il suo complementare.

1.4.2 DEFINIZIONE. Una *struttura algebrica* è un insieme S dotato di una o più operazioni n -arie definite su S che soddisfano ad eventuali assiomi. \square

In genere saremo interessati solo ad operazioni *binarie*, che chiameremo senza altro operazioni, omettendo la specificazione "binarie".

Ebbene, gli assiomi di Peano permettono di definire in \mathbb{N} due operazioni, di addizione e moltiplicazione, secondo le seguenti definizioni.

1.4.3 DEFINIZIONE. Si definisce *somma* di due numeri naturali n ed m il numero naturale $n + m$ dove

$$n + m \stackrel{\text{def}}{=} \begin{cases} \underbrace{\sigma(\sigma(\cdots\sigma(n)))}_{m \text{ volte}} & \text{se } m > 0 \\ n & \text{se } m = 0. \quad \square \end{cases}$$

Da questa definizione risulta ovviamente $\sigma(n) = n + 1$, dove $1 = \sigma(0)$.

1.4.4 DEFINIZIONE. Si definisce *prodotto* di due numeri naturali n e m il numero naturale $n \cdot m$ dove

$$n \cdot m \stackrel{\text{def}}{=} \begin{cases} \underbrace{n + n + \cdots + n}_{m \text{ volte}} & \text{se } m > 0 \\ 0 & \text{se } m = 0. \quad \square \end{cases}$$

Tali operazioni verificano tutte le ordinarie proprietà dell'aritmetica ordinaria (commutatività, associatività di addizione e moltiplicazione, proprietà distributive, esistenza di un elemento neutro rispetto all'addizione e uno neutro rispetto alla moltiplicazione, cfr. esercizio 1.4.1).

Soffermiamoci ora sul principio di induzione matematica, \mathbb{N}_3 . Esso sostanzialmente dice che se un sottoinsieme U di \mathbb{N} è tale che contiene lo zero e, accanto ad ogni elemento, contiene anche il successivo, allora necessariamente U coincide con tutto \mathbb{N} . L'accettazione di questo assioma fornisce "gratuitamente" un metodo di dimostrazione per induzione che è di fondamentale importanza in matematica. Vediamo in che cosa consiste. Supponiamo che per ogni intero $n \geq 0$ si possa formulare una proposizione $P(n)$ dipendente dall'intero n , ad esempio la proposizione seguente: "se un insieme finito S ha n elementi, allora l'insieme delle parti di S ha 2^n elementi". Supponiamo di voler provare che la proposizione $P(n)$ è vera per ogni n : si tratta di dimostrare infinite proposizioni! Ebbene, il metodo di dimostrazione per induzione permette di ottenere questi *infiniti* risultati con due soli passi. Si procede al modo seguente:

(1) *Base dell'induzione:* Dimostrare che è vera $P(0)$;

(2) *Passo induttivo:* Dimostrare che per ogni k dall'essere vera $P(k)$ segue che è vera $P(k+1)$.

Allora si può concludere di avere dimostrato che $P(n)$ è vera per ogni n .

Infatti, posto $U = \{n \in \mathbb{N} \mid P(n) \text{ è vera}\}$, risulta $0 \in U$ perché è stato provato che $P(0)$ è vera. Inoltre, se $k \in U$, cioè se $P(k)$ è vera, allora $P(k+1)$ è vera (passo induttivo) e quindi $k+1 \in U$, da cui segue, in virtù di \mathbb{N}_3 , $U = \mathbb{N}$, ossia $P(n)$ è vera per ogni n .

Si noti che se vogliamo dimostrare una proposizione $P(n)$ non per tutti gli n , ma per tutti gli $n \geq n_0$, basta provare come base dell'induzione $P(n_0)$ anziché $P(0)$.

Diamo qui di seguito un esempio di dimostrazione per induzione.

1.4.5. Provare che per ogni intero positivo n la somma dei cubi dei primi n numeri pari è data da

$$(1.4.1) \quad \underbrace{2^3 + 4^3 + 6^3 + \cdots + (2n)^3}_{n \text{ addendi}} = 2n^2(n+1)^2$$

Dimostrazione. Dovremo provare:

- (1) *La base dell'induzione:* $P(1)$ è verificata perché per $n=1$ entrambi i membri di (1.4.1) si riducono a 2^3 .
- (2) *Il passo induttivo:* Supposta vera $P(n-1)$, dimostriamo $P(n)$. La $P(n-1)$ (che stiamo supponendo vera) è:

$$(1.4.2) \quad \underbrace{2^3 + 4^3 + 6^3 + \cdots + (2(n-1))^3}_{n-1 \text{ addendi}} = 2(n-1)^2n^2$$

Aggiungendo ad ambo i membri della (1.4.2) il termine $(2n)^3$ si ha

$$\begin{aligned} 2^3 + 4^3 + 6^3 + \cdots + 2(n-1)^3 + (2n)^3 &= 2(n-1)^2n^2 + (2n)^3 \\ &= 2n^2[(n-1)^2 + 4n] \\ &= 2n^2(n+1)^2 \end{aligned}$$

che è esattamente $P(n)$. \square

Diamo qui di seguito delle formulazioni *equivalenti* del principio di induzione \mathbb{N}_3 , perché, a seconda dei casi che si presentano, può essere conveniente utilizzare una formulazione invece di un'altra. Consideriamo le seguenti due asserzioni, I e M:

I Ogni sottoinsieme V di \mathbb{N} tale che

- (a) $0 \in V$,
- (b) $n \in V$ ogniqualvolta $k \in V \quad \forall k$ tale che $0 \leq k < n$

coincide con tutto \mathbb{N} .

M (*Principio del buon ordinamento, o del minimo*) Ogni sottoinsieme non vuoto T contenuto in \mathbb{N} contiene un elemento minimo, cioè esiste un elemento $t \in T$ tale che $t \leq x$ per ogni $x \in T$.

Un insieme parzialmente ordinato X si dice *bene ordinato* se ogni sottoinsieme non vuoto di X ha un elemento minimo. In questa terminologia M afferma che l'insieme \mathbb{N} dei numeri naturali è bene ordinato.

Utilizzando M, si può provare che non esiste alcun intero c compreso tra 0 e 1.

Supponiamo per assurdo che esista un $c \in \mathbb{N}$ tale che $0 < c < 1$. Allora l'insieme $T = \{c \in \mathbb{N} \mid 0 < c < 1\}$ è non vuoto e pertanto possiede minimo m . Moltiplicando per $m > 0$ ogni membro della

$$0 < m < 1$$

si ottiene

$$0 < m^2 < m < 1$$

che contraddice la minimalità di m .

1.4.6 PROPOSIZIONE. Le tre asserzioni N₃, I e M sono equivalenti.

Dimostrazione. Basta provare che I \Rightarrow N₃ \Rightarrow M \Rightarrow I.

I \Rightarrow N₃. Osserviamo che le ipotesi (a) e (b) dell'asserzione I sono più deboli delle corrispondenti ipotesi contenute nell'asserzione N₃, quindi, se è vera la I, ossia se riusciamo a concludere che un insieme U che verifica le (a) e (b) di I necessariamente coincide con tutto \mathbb{N} , a maggior ragione coinciderà con tutto \mathbb{N} un insieme U che verifica le corrispondenti ipotesi di N₃, che sono più forti.

N₃ \Rightarrow M. Supponiamo per assurdo che esista un sottoinsieme $T \neq \emptyset$ di \mathbb{N} privo di elemento minimo. Allora, $0 \notin T$, per cui, posto $U = \complement T$, risulta

$$(a) 0 \in U \quad \text{e} \quad (b) k \in U \Rightarrow k + 1 \in U.$$

Quindi, per N₃, $U = \mathbb{N}$, che è un assurdo.

M \Rightarrow I. Sia U un sottoinsieme di \mathbb{N} verificante le ipotesi (a) e (b) di I, e supponiamo per assurdo che sia $U \neq \mathbb{N}$. Allora, detto $V = \complement U$, risulta $V \neq \emptyset$. Per la M, esiste un minimo m in V , che sarà maggiore di zero, perché $0 \in U$. Essendo m minimo per V , ogni k tale che sia $0 \leq k < m$ sta in U . Ma allora, per la (b) di I, $m \in U$, che è un assurdo. \square

Mettiamo subito in pratica questi metodi di dimostrazione, per provare la seguente proposizione riguardante la divisione in \mathbb{N} .

1.4.7 PROPOSIZIONE. *Siano $a, b \in \mathbb{N}$, $b \neq 0$. Allora esistono due numeri naturali q, r tali che*

$$a = bq + r, \quad 0 \leq r < b.$$

Dimostrazione. Utilizziamo l'assioma \mathbb{M} del buon ordinamento: sia $q+1$ il più piccolo intero positivo tale che $b(q+1) > a$ (tale minimo esiste sicuramente, considerando l'insieme [non vuoto!] $T = \{x \in \mathbb{N} \mid bx > a\}$) (si veda la figura 1.6).



FIGURA 1.6

Sarà pertanto

$$bq \leq a < b(q+1),$$

da cui

$$0 \leq a - bq < b.$$

Posto $r = a - bq$, si ha $a = bq + r$, $0 \leq r < b$. \square

Nel prossimo paragrafo avremo modo di dare una ulteriore dimostrazione di questo teorema, utilizzando il principio di induzione nella forma \mathbb{I} .

Terminiamo accennando al concetto di *relazione ricorsiva* che ci sarà utile in seguito. Partiamo da qualche semplice esempio.

1.4.8 ESEMPI DI RELAZIONI RICORSIVE.

(a) Determinare la somma $s_n = \sum_{i=1}^n \alpha_i$ di n numeri $\alpha_1, \alpha_2, \dots, \alpha_n$. Basta porre

$$(1.4.3) \quad s_1 = \alpha_1, \quad s_n = s_{n-1} + \alpha_n.$$

(b) Le relazioni seguenti:

$$(1.4.4) \quad a_1 = a, \quad a_n = a_{n-1} + d$$

definiscono una progressione aritmetica a_1, a_2, a_3, \dots in cui la differenza tra un termine e il precedente è d . \square

Le formule (1.4.3) e (1.4.4) prendono il nome di *relazioni ricorsive*. Le condizioni $s_1 = \alpha_1$ e $a_1 = a$ sono le cosiddette *condizioni iniziali*. Negli esempi dati il termine n -esimo dipende esclusivamente dal precedente (e da una costante). In generale in una relazione ricorsiva il termine n -esimo dipenderà da un certo numero r di termini precedenti e da una funzione nota di n . In tal

caso serviranno generalmente r condizioni iniziali (ad esempio i valori dei primi r termini). Il seguente è un esempio di successione definita ricorsivamente:

$$a_0 = 0, \quad a_1 = 1, \quad a_n = a_{n-1} + a_{n-2}.$$

I primi termini della successione sono i seguenti:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \dots$$

Si tratta della successione dei numeri di Fibonacci, che studieremo più in dettaglio fra breve, e della quale studieremo varie importanti proprietà.

Anche se una relazione ricorsiva ci permette di trovare il valore del termine n -esimo a_n per ogni n , tuttavia è importante trovare una *soluzione* per una relazione ricorsiva, o, come anche si dice, una *formula chiusa* che esprima *direttamente* a_n in termini di un numero di operazioni ben note di n e non in termini dei precedenti elementi della successione. Una soluzione permette di capire esattamente il valore di ogni a_n , mentre una relazione ricorsiva dà solo una informazione *locale*.

Una tale formula per il caso della progressione aritmetica (1.4.4) è data, come è immediato provare, da

$$a_n = a + (n - 1)d.$$

Il metodo di dimostrazione per induzione può venire in aiuto per trovare una tale formula. Si consideri ad esempio la seguente relazione ricorsiva:

$$a_0 = 0, \quad a_n = 2a_{n-1} + 1.$$

Cerchiamo di "indovinare" la soluzione. Dall'esame dei primi casi sembra che la soluzione possa essere

$$(1.4.5) \qquad a_n = 2^n - 1.$$

Occorre ora provare che è effettivamente soluzione per ogni n . Procediamo per induzione. Per $n = 0$, $a_0 = 0 = 2^0 - 1$, e la base dell'induzione è verificata. Supposta vera la $a_{n-1} = 2^{n-1} - 1$, si tratta di provare che vale (1.4.5). Infatti

$$a_n = 2a_{n-1} + 1 = 2(2^{n-1} - 1) + 1 = 2^n - 1.$$

e la dimostrazione è conclusa.

ESERCIZI.

- Si provi che l'addizione definita in \mathbb{N} è commutativa, associativa ed esiste un elemento neutro. Si provi inoltre che la moltiplicazione definita in \mathbb{N} è anch'essa commutativa e associativa, ed esiste un elemento neutro rispetto ad essa. Si provi inoltre la validità della seguente legge distributiva:

$$a(b + c) = ab + ac.$$

2. Si provi per induzione che, per ogni intero positivo n , risulta

$$\sum_{k=0}^n (4k+1) = (2n+1)(n+1).$$

3. Si provi per induzione che, per ogni intero positivo n , risulta

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

4. Si provi per induzione che, per ogni intero positivo n , l'insieme delle parti $\mathcal{P}(X)$ di un insieme finito X con n elementi ha 2^n elementi.
 5. Tutti gli studenti prendono gli stessi voti agli esami. Dimostriamo questo fatto per induzione sul numero n di studenti. Se $n = 1$ è ovvio che uno studente ha gli stessi voti di se stesso. Siano $1, \dots, n$ gli studenti: in virtù dell'induzione, gli $n - 1$ studenti $1, \dots, n - 1$ hanno tutti gli stessi voti, e così anche gli $n - 1$ studenti $2, \dots, n$. Ma allora gli studenti che si trovano a metà, ossia quelli dal numero 2 al numero $n - 1$ e che appartengono a due gruppi diversi di studenti, avranno gli stessi voti degli studenti del primo gruppo e anche gli stessi voti degli studenti del secondo gruppo. Quindi tutti gli n studenti hanno gli stessi voti.

Dove fa acqua questo ragionamento?

6. Si provi che il numero di regioni nel piano formate da n rette in posizione generica (tali cioè che non ci siano rette parallele e tali che tre rette non si incontrino mai in uno stesso punto) è $n(n+1)/2 + 1$.
7. Si provi che è possibile colorare le regioni formate da un qualunque numero di rette del piano (anche in posizione particolare, e non generica) con solo due colori. Si noti che per *colorare* si intende assegnare dei colori alle regioni in modo tale che regioni *confinanti* (ossia che hanno un *lato* in comune) abbiano colori diversi.
8. Si calcoli il numero di regioni del piano che si formano intersecando n cerchi in posizione generica (tali cioè che tre cerchi non si intersechino in un punto e due cerchi si intersechino in esattamente due punti).
9. *Il gioco della Torre di Hanoi* (inventato dal matematico E. Lucas nel 1883). La Torre di Hanoi consiste di n dischi circolari infilati in un'asticella verticale A , con diametri decrescenti dal basso verso l'alto (figura 1.7). Scopo del gioco è di trasferire tutti i dischi, nello stesso ordine di prima (ossia con diametri decrescenti dal basso verso l'alto), su cui un'altra asticella C , seguendo le seguenti regole:
- (a) I dischi devono essere trasferiti uno alla volta, utilizzando un'asticella intermedia B :
 - (b) in nessun momento del gioco un disco di diametro maggiore può trovarsi su di un disco di diametro minore.

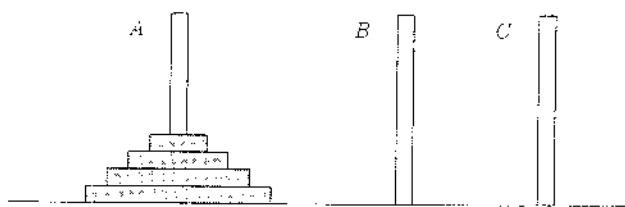


FIGURA 1.7

Pare che il gioco abbia la seguente origine. I sacerdoti del tempio di Brahma avevano il compito di fare in continuazione questi trasferimenti partendo da 64 dischi d'oro posti su tre aste d'oro poggiate su basi di diamante. La leggenda vuole che nell'istante stesso in cui il trasferimento fosse avvenuto il mondo sarebbe terminato!

- (α) Si trovi una relazione ricorsiva per il minimo numero m_n di mosse necessarie per trasferire n dischi;
 - (β) si trovi una formula chiusa, che esprima tale numero m_n in funzione di n ;
 - (γ) si deduca il numero di mosse nel caso $n = 64$ dei sacerdoti, e si veda quanto lontana era la fine del mondo!
10. Si provi che un insieme bene ordinato è totalmente ordinato (secondo la definizione del §1.2).



ESERCIZI DI PROGRAMMAZIONE.

1. Si consideri la seguente relazione ricorsiva:

$$a_n = h_1 a_{n-1} + h_2 a_{n-2} + \dots + h_r a_{n-r} + f(n),$$

dove gli h_i sono costanti e $f(n)$ una funzione arbitraria di n , con le seguenti condizioni iniziali:

$$a_1 = \alpha_1, a_2 = \alpha_2, \dots, a_r = \alpha_r.$$

Si scriva un programma che calcoli il termine a_n .

2. Si scriva un programma che attraverso la relazione ricorsiva trovata nell'esercizio (1.4.9) calcoli il numero m_n di mosse necessarie per risolvere il gioco della torre di Hanoi con n dischi. Si confrontino i tempi di calcolo rispetto ad un programma che utilizzi la formula chiusa.



CONTROLLO.

1. Enunciare il principio di induzione matematica, cercando di spiegarlo anche in termini non matematici.
2. Dare varie formulazioni equivalenti del principio di induzione matematica.
3. Cosa si intende per operazione binaria definita su di un insieme?

1.5. Cardinalità di insiemi

Il concetto di corrispondenza biunivoca (cfr. definizione 1.3.4) permette di confrontare quantitativamente due insiemi: per sapere se le caramelle in un sacchettino sono tante quanti i bambini, basta dare ad ogni bambino una caramella: se ogni bambino riceve una caramella e se nel pacchetto non restano caramelle, vuol dire che le caramelle sono tante quanti i bambini. Questo procedimento è indipendente dalla nozione di numero e dalla capacità di contare: l'uomo primitivo, pur essendo incapace di *contare*, era capace di vedere *se due insiemi A e B avevano lo stesso numero di elementi*, o se l'insieme A aveva più elementi dell'insieme B. Era questo sistema di confronto tra insiemi il suo modo di contare. Ebbene, noi utilizzeremo questo stesso metodo per *contare* gli elementi di un insieme arbitrario.

1.5.1 DEFINIZIONE. Si dice che due insiemi A e B hanno la stessa cardinalità (o la stessa potenza) o sono equivalenti se è possibile stabilire tra di essi una corrispondenza biunivoca. \square

È facile provare che la relazione di *avere la stessa cardinalità* (o di *equipotenza*) è una relazione di equivalenza tra insiemi. Due insiemi equipotenti verranno indicati con

$$A \sim B.$$

1.5.2 DEFINIZIONE. Si definisce *cardinalità* o *numero cardinale* o *potenza* di un insieme A la classe di equipotenza a cui A appartiene. Si indica con $\text{Card}(A)$. \square

1.5.3 DEFINIZIONE. Un insieme A si dice *finito* se per qualche $n \in \mathbb{N}$, $n \neq 0$, A è equipotente ad $I_n = \{0, 1, 2, \dots, n-1\}$. Un insieme che non è finito si dice *infinito*. \square

Nel caso di insiemi *finiti* la nozione di cardinalità coincide con la nozione di *numero di elementi* dell'insieme e la cardinalità di I_n viene chiamata n . In altre parole, i numeri naturali $0, 1, 2, \dots$ diventano numeri cardinali (finiti): 0 è il numero cardinale dell'insieme vuoto \emptyset , 1 è il numero cardinale di $\{\emptyset\}$ (e di qualunque altro insieme appartenente alla stessa classe di equipotenza), 2 è il numero cardinale di $\{\emptyset, \{\emptyset\}\}$ (e di qualunque altro insieme della stessa classe), 3 è il numero cardinale di $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, e così via. In conclusione, i numeri naturali non sono altro che particolari cardinalità. La potenza dell'insieme \mathbb{N} di tutti i numeri naturali prende il nome di \aleph_0 (che si legge "alef-zero") e dicesi la potenza del *numerabile*. Quindi si ha la seguente definizione:

1.5.4 DEFINIZIONE. Un insieme si dice avere la *potenza del numerabile* (o che è *numerabile*) se si può porre in corrispondenza biunivoca con \mathbb{N} . \square

Questo significa che un insieme numerabile S si potrà scrivere al modo seguente:

$$S = \{a_1, a_2, a_3, \dots, a_i, \dots\}$$

ossia i suoi elementi si possono per l'appunto *numerare* con degli indici $0, 1, 2, \dots$ oppure $1, 2, 3, \dots$

Non è difficile provare (cfr. esercizio 1.5.1) che un sottoinsieme di un insieme numerabile o è finito, oppure è numerabile anch'esso.

Il seguente teorema ci offre la possibilità di trovare molti insiemi numerabili.

1.5.5 TEOREMA. *L'unione di un numero finito o di una infinità numerabile di insiemi numerabili ha la potenza del numerabile.*

Dimostrazione. Dimostreremo il teorema nel caso di una infinità numerabile di insiemi numerabili a due a due disgiunti: gli altri casi sono conseguenza di questo. Sia $A_1, A_2, \dots, A_j, \dots$ una infinità numerabile di insiemi numerabili. Gli elementi di A_j saranno pertanto

$$a_{j,1}, a_{j,2}, a_{j,3}, \dots, a_{j,i} \dots$$

Si tratta ora di *numerare* anche gli elementi dell'insieme $A = A_1 \cup A_2 \cup A_3 \cup \dots$. Per far ciò, disponiamo gli elementi di tale unione in una tabella dove sulla riga j -esima vengono disposti gli elementi $a_{j,i}$ dell'insieme A_j .

A_1	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	\dots	$a_{1,i}$	\dots
A_2	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	\dots	$a_{2,i}$	\dots
A_3	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	\dots	$a_{3,i}$	\dots
\dots						
A_j	$a_{j,1}$	$a_{j,2}$	$a_{j,3}$	\dots	$a_{j,i}$	\dots
\dots						

Si consideri la diagonale j -esima D_j , cioè

$$D_j = \{a_{j,1}, a_{j+1,2}, a_{j+2,3}, \dots\} = \{a_{h,k} \in A \mid h + k = j + 1\}.$$

Ogni elemento $a_{h,k} \in A$ appartiene ad una e una sola diagonale, precisamente alla diagonale D_{h+k-1} . Possiamo stabilire la seguente corrispondenza tra A ed \mathbb{N} :

$$a_{h,k} \longmapsto 1 + 2 + 3 + \dots + (h + k - 2) + k$$

cioè

$$\begin{aligned}
 a_{11} &\mapsto & (1+1-2)+1 &= 1 \\
 a_{21} &\mapsto & (2+1-2)+1 &= 2 \\
 a_{12} &\mapsto & (1+2-2)+2 &= 3 \\
 a_{31} &\mapsto & 1+(3+1-2)+1 &= 4 \\
 a_{22} &\mapsto & 1+(2+2-2)+2 &= 5 \\
 a_{13} &\mapsto & 1+(1+3-2)+3 &= 6 \\
 a_{41} &\mapsto & 1+2+(4+1-2)+1 &= 7 \\
 &\dots
 \end{aligned}$$

Gli elementi di A vengono quindi numerati al modo seguente:

$$\begin{array}{ccccccccc}
 a_{11} & a_{21} & a_{12} & a_{31} & a_{22} & a_{13} & a_{41} & \dots \\
 1 & 2 & 3 & 4 & 5 & 6 & 7 & \dots
 \end{array}$$

Si può visualizzare con delle frecce l'operazione che stiamo facendo, che prende il nome di *procedimento diagonale di Cantor*:

$$\begin{array}{ccccccccc}
 A_1 & a_{1,1} & a_{1,2} & a_{1,3} & \dots & a_{1,i} & \dots \\
 & \nearrow & \nearrow & \nearrow & & & & \\
 A_2 & a_{2,1} & a_{2,2} & a_{2,3} & \dots & a_{2,i} & \dots \\
 & \nearrow & \nearrow & \nearrow & & & & \\
 A_3 & a_{3,1} & a_{3,2} & a_{3,3} & \dots & a_{3,i} & \dots \\
 & \nearrow & & & & & & \\
 & \dots & & & & & & \\
 A_j & a_{j,1} & a_{j,2} & a_{j,3} & \dots & a_{j,i} & \dots
 \end{array}$$

Si ottiene in tal modo una corrispondenza biunivoca tra A e \mathbb{N} , e pertanto l'insieme A è numerabile. \square

1.5.6 COROLLARIO. L'insieme \mathbb{Z} degli interi è numerabile, e così anche $\mathbb{N} \times \mathbb{N}$.

Dimostrazione. Basta scrivere questi insiemi come unione di un numero finito o una infinità numerabile di insiemi numerabili. Infatti

$$\mathbb{Z} = \mathbb{N} \cup \{-1, -2, -3, \dots\},$$

$$\mathbb{N} \times \mathbb{N} = \bigcup_{h=1}^{\infty} A_h$$

dove

$$A_h = \{(h, 1), (h, 2), (h, 3), \dots\}$$

è ovviamente numerabile per ogni h . \square

1.5.7 DEFINIZIONE. Si dice che un insieme A ha *cardinalità inferiore o uguale* a quella di un insieme B se esiste un'applicazione iniettiva $f : A \rightarrow B$. Si scrive allora

$$\text{Card}(A) \leq \text{Card}(B).$$

Se risulta $\text{Card}(A) \leq \text{Card}(B)$ e $\text{Card}(A) \neq \text{Card}(B)$, allora si scrive

$$\text{Card}(A) < \text{Card}(B). \quad \square$$

Il problema ora è vedere se *esistono* cardinalità superiori al numerabile. La risposta è positiva, come ci dice il teorema seguente.

1.5.8 TEOREMA. *Dato comunque un insieme numerabile A , risulta*

$$\text{Card}(A) < \text{Card}(\mathcal{P}(A)).$$

Dimostrazione. Chiaramente l'applicazione $h : A \rightarrow \mathcal{P}(A)$ data da $h(x) = \{x\}$ per ogni $x \in A$ è un'applicazione iniettiva da A a $\mathcal{P}(A)$, quindi $\text{Card}(A) \leq \text{Card}(\mathcal{P}(A))$. Dato che (cfr. Teorema 1.3.7)

$$\mathcal{P}(A) \cong 2^A = \{f : A \rightarrow \{0, 1\}\},$$

basta provare che non è possibile disporre in una successione numerabile $A_1, A_2, A_3, \dots, A_k, \dots$ l'insieme 2^A delle successioni composte di 0 e 1. Supponiamo per assurdo che esista una corrispondenza biunivoca tra 2^A e \mathbb{N} . Ciò significa che ad *ogni* successione di simboli 0 e 1 possiamo associare un indice $k \in \mathbb{N}$. Siano quindi

$$A_1 = a_{11}a_{12}a_{13}\dots$$

$$A_2 = a_{21}a_{22}a_{23}\dots$$

$$A_3 = a_{31}a_{32}a_{33}\dots$$

...

$$A_k = a_{k1}a_{k2}a_{k3}\dots$$

...

tutte le successioni di 0 e 1. Se riusciamo a trovare una successione di 0 e 1 che non compare in quella lista, saremo arrivati ad un assurdo. Basta a questo scopo definire una successione $S = s_1s_2s_3\dots$ al modo seguente:

$$s_k = \begin{cases} 0 & \text{se } a_{kk} = 1 \\ 1 & \text{se } a_{kk} = 0. \end{cases}$$

Chiaramente risulta $S \neq A_i$ per ogni i e il teorema è concluso. \square

1.5.9 DEFINIZIONE. Dicesi *potenza del continuo* la potenza dell'insieme $2^{\mathbb{N}}$. \square

Per quanto ora visto, la potenza del continuo è *strettamente maggiore* della potenza del numerabile. Essa coincide con la potenza dell'insieme \mathbb{R} dei numeri reali. La cosiddetta *ipotesi del continuo* afferma che non esistono *potenze intermedie* tra la potenza del numerabile e quella del continuo. È stato provato che l'ipotesi del continuo è indipendente dagli altri postulati sui quali si basa la teoria degli insiemi, il che significa che a partire dagli assiomi ordinari della teoria degli insiemi non si riuscirà né a dimostrare che la congettura è vera né a dimostrare che è falsa. L'insieme delle parti di un insieme che abbia la potenza del continuo è un insieme che ha una potenza strettamente superiore a quella del continuo. Con successivi passi si possono costruire insiemi di potenza via via crescente. Analogamente l'*ipotesi generalizzata del continuo* afferma che per ogni insieme infinito X non esistono insiemi di potenza *intermedia* tra quella di X e quella di $\mathcal{P}(X)$.

 ATTENZIONE. È opportuno notare che nel teorema 1.5.5 si è tacitamente utilizzato il cosiddetto *assioma di Zermelo o della scelta*. Tale assioma si enuncia al modo seguente: data una classe non vuota X di insiemi non vuoti I_α , esiste una funzione f che associa ad ogni $I_\alpha \in X$ un elemento $x_\alpha \in I_\alpha$. Sostanzialmente, l'assioma di Zermelo ci dice che a partire da una qualunque classe non vuota di insiemi non vuoti è possibile scegliere un rappresentante per ogni insieme della classe. Tale assioma è equivalente al *teorema del buon ordinamento*, in base al quale ogni insieme può essere bene ordinato.

Non intendiamo soffermarci oltre su questi argomenti, per i quali si rimanda ai corsi di Logica Matematica. □



ESERCIZI.

1. Si provi che un sottoinsieme di un insieme numerabile o è finito oppure è numerabile.
2. Si provi che un insieme numerabile possiede parti proprie numerabili.
3. Si provi che un insieme finito ha potenza minore di ogni insieme che lo contenga propriamente.
4. Si provi che un insieme è infinito se e solo se è equipotente ad un suo sottoinsieme proprio. Si diano esempi esplicativi di insiemi siffatti e delle relative corrispondenze biunivoche.
5. In \mathbb{R} si definisca la seguente relazione:

$$x \varrho y \iff x - y \in \mathbb{Q}.$$

- (a) Si provi che si tratta di una relazione di equivalenza;
- (b) si dica se il quoziente \mathbb{R}/ϱ è numerabile.



CONTROLLO.

1. Si definisca la nozione di equipotenza.
2. Si diano esempi di insiemi numerabili.
3. Si diano esempi di insiemi non numerabili.

1.6. Calcolo combinatorio

Scopo di questo paragrafo è di rispondere alla domanda: *quanti sono?* Ossia saremo interessati a *contare* gli oggetti di certi insiemi finiti. Diamo alcuni esempi.

1.6.1 ESEMPI.

- (a) Uno studente vuole usare durante i cinque giorni di lezione settimanali cinque penne diverse, senza mai riutilizzare la stessa penna. Quali sono i possibili modi con cui può utilizzare le sue penne?
 Ovviamente il primo giorno ha cinque possibilità di scelta, il secondo giorno ne ha quattro, il terzo ne ha tre, e così via fino all'ultimo giorno, in cui ha un'unica possibilità. In totale il numero di possibili scelte è

$$5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120 .$$

- (2) Quante targhe si possono formare utilizzando quattro cifre seguite da tre lettere (scelte tra 26)?

Ci sono $10 \cdot 10 \cdot 10 \cdot 10$ possibili numeri a quattro cifre. Ci sono $26 \cdot 26 \cdot 26$ possibili modi di utilizzare tre lettere. In tutto quindi il numero di targhe che si possono ottenere è

$$10^4 \cdot 26^3 = 17576 \cdot 10^4 . \quad \square$$

Per risolvere questo genere di problemi è conveniente introdurre alcune notazioni.

Dato un intero positivo n , si indica con $n!$, e si legge *n fattoriale*, il seguente intero:

$$n! \stackrel{\text{def}}{=} n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1, \quad 0! \stackrel{\text{def}}{=} 1 .$$

Ad esempio, $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$. Si osservi che la funzione fattoriale cresce molto rapidamente. Nei calcoli, quando si ha a che fare ad esempio con quozienti di fattoriali, conviene procedere alla loro cancellazione, tenendo conto del fatto che

$$n! = n(n-1)!$$

Ad esempio, se si deve dividere $1000!$ per $997!$ conviene scrivere

$$\frac{1000!}{997!} = \frac{1000 \cdot 999 \cdot 998 \cdot 997!}{997!} = 1000 \cdot 999 \cdot 998 .$$

Dati due insiemi A e B con n elementi ciascuno, il numero di corrispondenze biunivoche tra A e B è precisamente $n!$. Infatti, per individuare un'applicazione f basta assegnare i valori $f(x_1), f(x_2), \dots, f(x_n)$, dove x_1, x_2, \dots, x_n sono gli n elementi di A . Data quindi un'applicazione biiettiva arbitraria f da A a B , $f(x_1)$ può essere uno qualunque degli n elementi di B , cioè può assumere n valori, $f(x_2)$ può coincidere con uno qualunque degli elementi di B , purché diverso da $f(x_1)$ (per l'iniettività), quindi può assumere $n - 1$ valori, e così via. Si possono fare quindi in tutto $n \cdot (n - 1) \cdot (n - 2) \cdots 2 \cdot 1 = n!$ scelte, e scelte diverse danno luogo ad applicazioni biunivoche diverse tra A e B .

Nel caso in cui sia $A = B$, le corrispondenze biunivoche di A in sé prendono il nome di *permute*. L'insieme di tutte le permutazioni di un insieme X si indica con $S(X)$. Se si prende in considerazione la composizione di applicazioni, per quanto visto negli esercizi del §1.3, la composizione di elementi di $S(X)$ è ancora un elemento di $S(X)$. Inoltre tale composizione è associativa, esiste un elemento i_X neutro rispetto alla composizione, tale cioè che $i_X \circ f = f \circ i_X = f$ per ogni $f \in S(X)$. Inoltre, dato comunque un elemento $f \in S(X)$ esiste l'applicazione inversa f^{-1} , che sta ancora in $S(X)$, tale che $f \circ f^{-1} = f^{-1} \circ f = i_X$. L'insieme $S(X)$ rispetto alla composizione di applicazioni ha una struttura algebrica che prende il nome di *gruppo*. Tale insieme rivestirà un'importanza fondamentale nel seguito, quando studieremo in dettaglio i gruppi.

Dati due insiemi A e B di n e m elementi rispettivamente, il numero di applicazioni tra A e B è m^n (cfr. esercizio 1.6.1). Ad esempio, se $A = \{a_1, a_2, a_3\}$, $B = \{b_1, b_2\}$, tutte le possibili applicazioni tra A e B sono le seguenti 2^3 :

$$\begin{array}{ll}
 f_1 : \begin{array}{l} a_1 \rightarrow b_1 \\ a_2 \rightarrow b_1 \\ a_3 \rightarrow b_1 \end{array} & f_2 : \begin{array}{l} a_1 \rightarrow b_1 \\ a_2 \rightarrow b_1 \\ a_3 \rightarrow b_2 \end{array} \\
 f_3 : \begin{array}{l} a_1 \rightarrow b_1 \\ a_2 \rightarrow b_2 \\ a_3 \rightarrow b_2 \end{array} & f_4 : \begin{array}{l} a_1 \rightarrow b_2 \\ a_2 \rightarrow b_1 \\ a_3 \rightarrow b_1 \end{array} \\
 f_5 : \begin{array}{l} a_1 \rightarrow b_2 \\ a_2 \rightarrow b_2 \\ a_3 \rightarrow b_2 \end{array} & f_6 : \begin{array}{l} a_1 \rightarrow b_2 \\ a_2 \rightarrow b_2 \\ a_3 \rightarrow b_1 \end{array} \\
 f_7 : \begin{array}{l} a_1 \rightarrow b_2 \\ a_2 \rightarrow b_1 \\ a_3 \rightarrow b_2 \end{array} & f_8 : \begin{array}{l} a_1 \rightarrow b_1 \\ a_2 \rightarrow b_2 \\ a_3 \rightarrow b_2 \end{array}
 \end{array}$$

Supponiamo di voler contare quanti sono i sottoinsiemi con k elementi di un insieme A con n elementi ($k \leq n$). Conviene contare prima quante sono

le k -ple (ordinate) di elementi distinti di A : si noti che due k -ple che hanno gli stessi elementi ma in ordine diverso, sono da considerarsi diverse. Ora, il primo elemento della k -pla si può scegliere in n modi, il secondo in $n - 1$, l'ultimo, ossia il k -esimo, in $n - k + 1$ modi. Le k -ple ordinate sono quindi in numero di $n \cdot (n - 1) \cdots (n - k + 1)$. Ora, ogni sottoinsieme di A con k elementi ha esattamente $k!$ ordinamenti, quindi corrisponde a $k!$ k -ple distinte. Se si vuole pertanto il numero di sottoinsiemi di A con k elementi, si deve dividere per $k!$ il numero totale di k -ple. In conclusione, il numero di sottoinsiemi con k elementi di un insieme con n elementi è dato da

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

Ebbene, tale numero, che conta il numero di sottoinsiemi con k elementi di un insieme con n elementi e che rappresenta anche le combinazioni di n elementi a k a k , prende il nome (per un motivo che vedremo fra breve) di *coefficiente binomiale* e si suole indicare con il seguente simbolo:

$$\binom{n}{k}.$$

Quindi, per quanto detto,

$$\boxed{\binom{n}{k} \stackrel{\text{def}}{=} \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!} \quad n, k \in \mathbb{N}, k \leq n}.$$

Dalla definizione e dal significato di $\binom{n}{k}$ appare chiaro che

$$\binom{n}{0} = 1, \quad \binom{n}{1} = n, \quad \binom{n}{n} = 1$$

e che

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

Vale inoltre la seguente utile relazione (cfr. esercizio 1.6.4)

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

Tale formula ci permette di calcolare $\binom{n+1}{k}$ a partire dai valori $\binom{n}{k}$ e $\binom{n}{k-1}$. In tal modo si costruisce il cosiddetto *triangolo di Tartaglia* (o di *Pascal*):

n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$	$\binom{n}{7}$
0	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	4	6	4	1			
5	1	5	10	10	5	1		
6	1	6	15	20	15	6	1	
7	1	7	21	35	35	21	7	1

Il motivo per cui gli interi $\binom{n}{k}$ prendono il nome di coefficienti binomiali è che essi compaiono come coefficienti nella formula che dà lo sviluppo della potenza di un binomio $(x+y)^n$:

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k.$$

Per capire come vanno le cose, esaminiamo i primi valori di n :

$$(x+y)^0 = 1x^0y^0$$

$$(x+y)^1 = 1x^1y^0 + 1x^0y^1$$

$$(x+y)^2 = 1x^2y^0 + 2x^1y^1 + 1x^0y^2$$

$$(x+y)^3 = 1x^3y^0 + 3x^2y^1 + 3x^1y^2 + 1x^0y^3.$$

In generale, sviluppando la potenza

$$(x+y)^n = \underbrace{(x-y)(x+y) \cdots (x+y)}_{n \text{ fattori}}$$

si ottiene una somma di termini, ciascuno dei quali è un prodotto di n fattori ciascuno dei quali è x o y . Se in un fattore y compare k volte, allora in quello stesso fattore x compare $n-k$ volte. Il numero di fattori in cui y è ripetuto k volte (e quindi x è ripetuto $n-k$ volte) sarà il coefficiente di $x^{n-k}y^k$, e tale numero è precisamente il numero di modi di scegliere k degli n binomi $(x+y)$, ossia $\binom{n}{k}$.

ESERCIZI.

1. Siano A e B due insiemi con n e m elementi rispettivamente. Si contano le applicazioni tra A e B .
2. Si contano tutte le applicazioni *iniettive* tra due insiemi A e B con n elementi ciascuno. E quelle *suriettive* quante sono?

3. Siano A e B due insiemi con n e m elementi rispettivamente. Se è $n \leq m$ (perché?), si contano tutte le applicazioni iniettive di A in B .
4. Siano n, k interi positivi tali che $n \geq k$. Si provi che

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



ESERCIZI DI PROGRAMMAZIONE.

1. Scrivere un programma che calcoli $n!$ per ogni intero non negativo n .
2. Scrivere un programma che calcoli $\binom{n}{k}$.
3. Scrivere un programma che generi il triangolo di Tartaglia per vari valori di n .



CONTROLLO.

1. Fare gli esercizi proposti.

CAPITOLO 2

I numeri

*E poi rinvenni, a lor vantaggio, il numero,
somma fra le scienze, e le compagni
di lettere, ove la Memoria sorbasi,
che madre operatrice è delle Muse.*

Eschilo, Prometeo Legato, trad. E. Romagnoli.

La maggior parte dei concetti che verranno studiati nel corso di Algebra sono basati sul concetto di numero o, meglio, sono una evoluzione di tale concetto. Nel capitolo precedente abbiamo già introdotto l'insieme numerico per eccellenza, \mathbb{N} . A partire da tale insieme verranno definiti gli altri insiemi numerici $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e \mathbb{C} rispettivamente dei numeri interi, razionali, reali e complessi. Si passerà successivamente ad altri tipi di insiemi numerici, ad esempio gli *intervi modulo n*. Verranno via via esaminate le proprietà di questi insiemi numerici, e si vedrà nei capitoli successivi come queste proprietà si presteranno ad essere generalizzate, dando luogo a vari tipi di *strutture algebriche* che saranno l'oggetto di studio per questo corso.

2.1. I numeri interi

È ben noto che, mentre l'equazione $x - 5 = 0$ è risolubile in \mathbb{N} , l'equazione $x + 3 = 0$ non lo è. In questi casi allora si cerca di ampliare l'insieme numerico in modo da includere tutte le soluzioni di equazioni del tipo $x + n = 0$, $n \in \mathbb{N}$. Si giunge quindi all'insieme $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ degli interi relativi. Per dare significato agli interi negativi utilizzando solo nozioni già definite in precedenza, si procede al modo seguente. Si parta dal prodotto cartesiano $\mathbb{N} \times \mathbb{N}$, cioè l'insieme delle coppie ordinate di numeri naturali, e vi si introduca la seguente relazione:

$$\boxed{(n, m) \varrho (n', m') \iff n + m' = m + n'}.$$

Si tratta di una relazione di equivalenza (cfr. esercizio 2.1.1). L'insieme $\mathbb{N} \times \mathbb{N}$ viene pertanto ripartito in classi $(\overline{n}, \overline{m})$ rappresentate nella figura 2.1.

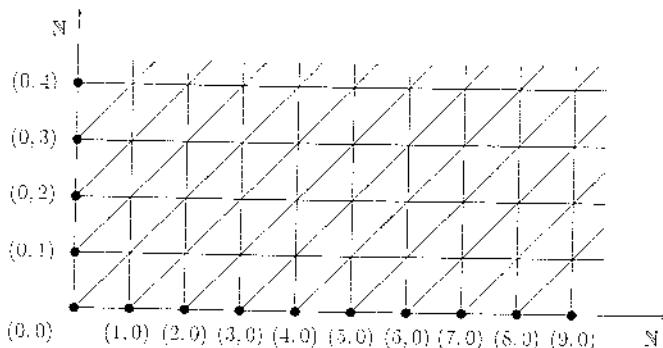


FIGURA 2.1

Come rappresentanti di ogni classe si possono scegliere coppie privilegiate, quelle in cui *almeno uno degli elementi è zero*. Geometricamente, si tratta delle coppie che si trovano sugli assi coordinati. È facile controllare che due coppie in cui il secondo elemento è zero sono equivalenti se e solo se sono uguali, e così coppie in cui il primo elemento è uguale a zero. *Ogni classe sarà rappresentabile con uno dei seguenti rappresentanti privilegiati distinti:*

$$\begin{aligned} &(0,0) \\ &(1,0), (2,0), (3,0), \dots, (n,0), \dots \\ &(0,1), (0,2), (0,3), \dots, (0,n), \dots \end{aligned}$$

Ebbene, poniamo per definizione

$$\boxed{\mathbb{Z} \stackrel{\text{def}}{=} (\mathbb{N} \times \mathbb{N}) / \varrho}:$$

\mathbb{Z} risulta decomposto nei seguenti sottoinsiemi:

$$\mathbb{Z} = \mathbb{Z}^+ \cup \{0\} \cup \mathbb{Z}^-$$

dove

$$\mathbb{Z}^+ \stackrel{\text{def}}{=} \{ \overrightarrow{(n,0)} \mid n \in \mathbb{N}, n \neq 0 \},$$

$$0 \stackrel{\text{def}}{=} \overrightarrow{(0,0)},$$

$$\mathbb{Z}^- \stackrel{\text{def}}{=} \{ \overrightarrow{(0,n)} \mid n \in \mathbb{N}, n \neq 0 \}.$$

Gli elementi di \mathbb{Z}^+ prendono il nome di *intervi positivi*, quelli di \mathbb{Z}^- di *intervi negativi*.

L'insieme \mathbb{Z} è un'estensione di \mathbb{N} nel senso che contiene al suo interno un sottoinsieme $\mathbb{Z}^+ \cup \{0\}$ identificabile con \mathbb{N} mediante l'applicazione iniettiva da \mathbb{N} in \mathbb{Z} che associa ad ogni naturale n la classe $(n, 0)$.

Nell'insieme \mathbb{Z} si possono definire un'operazione di addizione e una di moltiplicazione al modo seguente:

$$(n, m) + (n', m') \stackrel{\text{def}}{=} (n + n', m + m')$$

$$(n, m) \cdot (n', m') \stackrel{\text{def}}{=} (nn' - nm', n'm + nm') .$$

2.1.1 OSSERVAZIONI.

- (a) Tali operazioni sono *ben poste*, nel senso che, pur essendo definite attraverso i *rappresentanti* delle classi, non dipendono dalla *scelta* di tali rappresentanti (cfr. esercizio 2.1.2).
- (b) D ora in poi indicheremo gli elementi di \mathbb{Z} al modo seguente:

$$\overline{(n, 0)} \stackrel{\text{def}}{=} n, \quad \overline{(0, 0)} \stackrel{\text{def}}{=} 0, \quad \overline{(0, n)} \stackrel{\text{def}}{=} -n .$$

- (c) \mathbb{Z} rispetto alle due operazioni di addizione e moltiplicazione ora definite gode delle seguenti proprietà:

- (i) $a - b = b + a, \forall a, b \in \mathbb{Z}$
(proprietà commutativa dell'addizione);
- (ii) $(a + b) + c = a + (b + c), \forall a, b, c \in \mathbb{Z}$
(proprietà associativa dell'addizione);
- (iii) esiste un unico elemento $0 \in \mathbb{Z}$ tale che $a + 0 = 0 + a = a, \forall a \in \mathbb{Z}$
(esistenza dell'elemento neutro rispetto all'addizione);
- (iv) per ogni $a \in \mathbb{Z}$ esiste un unico elemento, $-a$, tale che $a + (-a) = (-a) + a = 0$
(esistenza dell'opposto);
- (v) $a \cdot b = b \cdot a, \forall a, b \in \mathbb{Z}$
(proprietà commutativa della moltiplicazione);
- (vi) $(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall a, b, c \in \mathbb{Z}$
(proprietà associativa della moltiplicazione);
- (vii) esiste in \mathbb{Z} un unico elemento, 1, tale che $a \cdot 1 = 1 \cdot a = a, \forall a \in \mathbb{Z}$
(esistenza dell'elemento neutro rispetto alla moltiplicazione);
- (viii) $a \cdot (b + c) = a \cdot b + a \cdot c, (a + b) \cdot c = a \cdot c + b \cdot c, \forall a, b, c \in \mathbb{Z}$
(distributività della moltiplicazione rispetto all'addizione). \square

Vedremo in seguito che un insieme dotato di due operazioni che verificano gli assiomi sopra riportati si dice avere la struttura di *anello commutativo con unità*. Pertanto $\mathbb{Z} (+, \cdot)$ è un esempio di anello commutativo con unità.

2.1.2 LEMMA. Siano a, b elementi di \mathbb{Z} . Allora

- (i) $a \cdot 0 = 0 \cdot a = 0$:

- (ii) $(-a) \cdot b = -(a \cdot b)$;
 (iii) $(-a)(-b) = ab$.

Dimostrazione. (i) Risulta $0 + (a \cdot 0) = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, da cui $a \cdot 0 = 0$.

(ii) $0 - 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$, da cui $(-a) \cdot b = - (a \cdot b)$.
 (iii) $(-a)(-b) = (\text{per (ii)}) = -(a(-b)) = -(-(ab)) = ab$. \square

2.1.3 PROPOSIZIONE. Siano a e b due numeri interi. Allora $ab = 0$ se e solo se $a = 0$ o $b = 0$.

Dimostrazione. Si osservi innanzitutto che se a e b sono entrambi positivi o entrambi negativi, il loro prodotto è sempre positivo (se sono entrambi positivi, basta ricordare la definizione di prodotto in \mathbb{N} , se sono entrambi negativi basta ricordare (iii) della proposizione precedente). Se invece è $a > 0$ e $b < 0$, allora $-b$ è positivo, quindi $a(-b) = -ab$ è positivo, per cui ab è negativo. Quindi se $ab = 0$ deve necessariamente essere uno dei due fattori a o b uguale a zero. Il viceversa è ovvio per la (i) del lemma precedente. \square

2.1.4 DEFINIZIONE. Si definisce *valore assoluto* di un intero a il numero intero positivo

$$|a| = \begin{cases} a & \text{se } a \geq 0 \\ -a & \text{se } a < 0. \end{cases} \quad \square$$

Dati comunque $a, b \in \mathbb{Z}$, valgono le seguenti relazioni:

$$|a| + |b| \geq |a + b|; \quad |a| \cdot |b| = |a \cdot b|.$$

Uno dei concetti fondamentali in \mathbb{Z} è il concetto di *divisibilità*.

2.1.5 DEFINIZIONE. Dati due interi a, b , si dice che a divide b (o che a è un *divisore* di b), e si scrive $a \mid b$, se esiste un $c \in \mathbb{Z}$ tale che $b = ac$. Se a non divide b , si scrive $a \nmid b$. \square

Ad esempio, $2 \mid 12, 3 \mid -27, 24 \mid 0$, ma $4 \nmid 2$ e $0 \nmid a$ se $a \neq 0$.

2.1.6 DEFINIZIONE. In un anello commutativo si dice che un elemento $a \neq 0$ è un *divisore dello zero* se esiste un $b \neq 0$ tale che $ab = 0$. \square

2.1.7 DEFINIZIONE. Un *dominio di integrità* è un anello commutativo privo di divisori dello zero. \square

La proposizione 2.1.3 dice che \mathbb{Z} è un dominio di integrità.

2.1.8 DEFINIZIONE. Si chiama *divisore comune* degli elementi a e b di \mathbb{Z} un elemento $c \in \mathbb{Z}$ tale che $c \mid a$ e $c \mid b$. \square

2.1.9 LEMMA. Se c è un divisore comune di a e b , allora c divide ogni intero della forma $sa + tb$, con s e t in \mathbb{Z} , cioè $c \mid a$ e $c \mid b \implies c \mid sa + tb \forall s, t \in \mathbb{Z}$.

Dimostrazione. $c \mid a \implies a = ch$ per qualche $h \in \mathbb{Z}$; $c \mid b \implies b = ck$ per qualche $k \in \mathbb{Z}$. Allora, per ogni $s, t \in \mathbb{Z}$, $sa + tb = s(ch) + t(ck) = c(sh + tk)$, da cui $c \mid sa + tb$. \square

Prima di proseguire e dare la fondamentale definizione di massimo comun divisore, conviene premettere alcune definizioni che apparentemente sono inutili, perché in \mathbb{Z} o sono poco significative o sono diversi modi per indicare la stessa cosa, ma delle quali capiremo il valore e il significato quando studieremo gli anelli in generale. Tanto vale quindi introdurlle già da ora.

2.1.10 DEFINIZIONE. Un elemento $u \in \mathbb{Z}$ che divide 1 si dice una *unità* (o elemento *invertibile*) di \mathbb{Z} . \square

È immediato riconoscere che le sole unità di \mathbb{Z} sono 1 e -1.

2.1.11 DEFINIZIONE. Due elementi a e b di \mathbb{Z} tali che $a \mid b$ e $b \mid a$ si dicono *associati*. \square

Dalla definizione è immediato vedere che due elementi a e b sono associati se e solo se $a = bu$, dove u è un'unità. Quindi, in \mathbb{Z} due elementi sono associati se e solo se differiscono per il segno. La relazione di "essere associati" è una relazione di equivalenza.

2.1.12 DEFINIZIONE. Un elemento $a \in \mathbb{Z}$ che sia diverso da zero e non sia una unità si dice *irriducibile* se ogni volta che a si scrive come prodotto $a = bc$ con $b, c \in \mathbb{Z}$ allora o b o c sono delle unità. \square

2.1.13 DEFINIZIONE. Un elemento $a \in \mathbb{Z}$ che non sia lo zero e non sia una unità si dice *primo* se ogni volta che a divide un prodotto bc , con $b, c \in \mathbb{Z}$, allora a divide almeno uno dei due fattori. \square

ATTENZIONE. In realtà la definizione che abbiamo appena dato di elemento irriducibile corrisponde alla definizione che comunemente si attribuisce ai numeri primi in \mathbb{Z} : infatti si dice normalmente che i numeri primi sono quegli interi positivi che non hanno altri divisori all'infuori di se stessi e l'unità. Si noti tuttavia che in questo caso si parla di *numeri* primi e non di *elementi* primi. Tuttavia non dobbiamo preoccuparci troppo di questa possibilità di confusione in \mathbb{Z} , perché vedremo comunque alla fine del prossimo paragrafo che le due nozioni di elemento irriducibile ed elemento primo coincidono in \mathbb{Z} ; in questo senso sembra futile dare due definizioni diverse quando in \mathbb{Z} questi due concetti coincidono, ma, lo ripetiamo, questo non sarà la situazione generale. Con i mezzi che abbiamo a disposizione, siamo in grado immediatamente di provare che un elemento primo è necessariamente irriducibile. Per provare che

in \mathbb{Z} anche ogni elemento irriducibile (ossia un ordinario numero primo) è primo occorrerà aspettare il prossimo paragrafo. \square

2.1.14 PROPOSIZIONE. *Ogni elemento primo in \mathbb{Z} è un elemento irriducibile.*

Dimostrazione. Sia a un elemento primo in \mathbb{Z} . Per provare che esso è irriducibile, dobbiamo provare che dall'essere $a = bc$ con $b, c \in \mathbb{Z}$ segue che b o c sono delle unità. Sia dunque $a = bc$; in particolare $a \mid bc$. Allora (essendo a primo per ipotesi) $a \mid b$ oppure $a \mid c$, cioè $b = ah$ o $c = ak$, con $h, k \in \mathbb{Z}$; ma allora la $a = bc$, assieme ad una di queste relazioni comportano che o b o c sono delle unità. \square

ESERCIZI.

- Si provi che la relazione

$$(n, m) \varrho (n', m') \iff n + m' = m + n'$$

definita su $\mathbb{N} \times \mathbb{N}$ è una relazione di equivalenza.

- Si provi che le operazioni di addizione e moltiplicazione definite in \mathbb{Z} sono *ben poste*.
- Si provi che in \mathbb{Z} valgono le seguenti *leggi di cancellazione*:

$$ac = bc, \quad c \neq 0 \implies a = b$$

$$ca = cb, \quad c \neq 0 \implies a = b$$

- Sia p un elemento primo in \mathbb{Z} (cfr. definizione 2.1.13). Si provi che se p divide un prodotto di n fattori $a_1 a_2 a_3 \cdots a_n$, allora p divide almeno uno dei fattori.



CONTROLLO.

- Spiegare perché gli interi si possono pensare come elementi di un insieme quoziante. Di quale insieme?
- Un elemento primo è ... Un elemento irriducibile è ...

2.2. Massimo comun divisore e l'algoritmo euclideo

2.2.1 DEFINIZIONE. *Siano $a, b \in \mathbb{Z}$. Un elemento $d \in \mathbb{Z}$ si dice un massimo comun divisore tra a e b se*

- (i) $d \mid a, d \mid b$;
- (ii) se $d' \mid a, d' \mid b$, allora $d' \mid d$. \square

ATTENZIONE. Si parla di *un* massimo comun divisore e non *del* massimo comun divisore tra due elementi, perché se d gode delle proprietà (i) e (ii), anche ogni associato di d (e quindi $\pm d$ nel caso di \mathbb{Z}) gode delle stesse proprietà. In generale, quando si parla *del* massimo comun divisore in \mathbb{Z} , si intende il

massimo comun divisore *positivo*. Esso si indica indifferentemente nei seguenti modi:

$$\text{MCD}(a, b), \quad \text{oppure} \quad (a, b).$$

Ad esempio, $\text{MCD}(3, -10) = 1$, $\text{MCD}(a, b) = \text{MCD}(b, a) = \text{MCD}(|a|, |b|)$, $\text{MCD}(ab, ac) = |a| \text{ MCD}(b, c)$, $\text{MCD}(0, a) = |a| \forall a \in \mathbb{Z}, a \neq 0$. Non è invece definito il $\text{MCD}(0, 0)$, in quanto *ogni* $x \in \mathbb{Z}$ divide lo zero, onde non esiste un divisore *massimo*. \square

2.2.2 DEFINIZIONE. Due interi a e b tali che $\text{MCD}(a, b) = 1$ si dicono *coprimi o relativamente primi*. \square

Abbiamo dato la *definizione* di massimo comun divisore tra due interi, ma nessuno ci garantisce che un tale elemento *esista* per ogni coppia di interi. La risposta a questo problema sarà una conseguenza del teorema che segue. Abbiamo visto che non è sempre vero che un intero divida un altro: vale tuttavia il seguente teorema.

2.2.3 PROPOSIZIONE (DIVISIONE IN \mathbb{Z}). *Siano a e b interi, $b \neq 0$. Allora esistono e sono univocamente individuati due interi q ed r tali che*

$$a = bq + r, \quad 0 \leq r < |b|.$$

Dimostrazione. *Esistenza:* Esaminiamo separatamente i due casi che si possono presentare, cioè $a \geq 0$ oppure $a < 0$.

$a \geq 0$. Possiamo applicare il principio di induzione nella forma I rispetto ad a . Se $a = 0$, basta porre $q = r = 0$, e quindi $P(0)$ è vera. Sia $a > 0$. Vediamo se dall'ipotesi che $P(k)$ sia vera per ogni k tale che $0 \leq k < a$ si può dedurre che è vera $P(a)$. Se è $|b| > a$, basta porre $q = 0$ e $r = a$. Possiamo pertanto supporre $a \geq |b|$. Allora $a > a - |b| \geq 0$, e per l'ipotesi induttiva $P(a - |b|)$ è vera. Ciò significa che esistono due interi q', r' tali che $a - |b| = bq' + r'$, $0 \leq r' < |b|$, da cui si deduce $a = |b| + bq' + r'$. Quindi, a seconda che sia $b > 0$ o $b < 0$ si avrà rispettivamente $a = b(q' + 1) + r'$ oppure $a = b(q' - 1) + r'$, con $0 \leq r' < |b|$, ossia $P(a)$ è vera, con $q = q' \pm 1$, $r = r'$, nel caso $b > 0$, e $q = q' - 1$, $r = r'$ se è $b < 0$. Per il principio di induzione, $P(a)$ è vera per ogni a .

$a < 0$. In questo caso risulta $-a > 0$. Esistono pertanto, per quanto provato nella prima parte, due interi \bar{q} e \bar{r} tali che $-a = b\bar{q} + \bar{r}$, con $0 \leq \bar{r} < |b|$. Se $\bar{r} = 0$, allora $a = b(-\bar{q})$, per cui basta porre $q = -\bar{q}$ e $r = 0$. Se è $\bar{r} > 0$, allora $a = b(-\bar{q}) + (-\bar{r}) = b(-\bar{q}) + |b| + |b| - \bar{r} = b(-\bar{q} + 1) + (|b| - \bar{r})$ con $0 < |b| - \bar{r} < |b|$. In ogni caso (cioè a seconda che sia $b > 0$ o $b < 0$) si riescono a trovare due interi q ed r (quali?) che risolvono il problema.

Unicità: Sia $a = bq + r = bq' + r'$, $0 \leq r, r' < |b|$. Supponiamo ad esempio $r' \geq r$. Allora $0 \leq r' - r = b(q - q')$, da cui, passando ai valori assoluti,

$$|b||q - q'| = |b(q - q')| = r' - r \leq r' < |b|.$$

Ciò è possibile solo se $|q - q'| < 1$ e cioè $|q - q'| = 0$, da cui $q = q'$ e $r = r'$. \square

2.2.4 ESEMPIO. $29 = 4 \cdot 7 - 1$, $-29 = 4 \cdot (-7 + 1) + (4 - 1) = 4 \cdot (-8) + 3$, $29 = (-4) \cdot (-7) + 1$, $-29 = -4 \cdot (7 + 1) - (4 - 1)$. \square

Proviamo ora l'esistenza del massimo comun divisore tra due interi non entrambi nulli.

2.2.5 TEOREMA (ESISTENZA DEL MASSIMO COMUN DIVISORE IN \mathbb{Z}). *Dati comunque $a, b \in \mathbb{Z}$ e non entrambi nulli, esiste il loro massimo comun divisore $d = \text{MCD}(a, b)$. Inoltre si possono trovare due interi s e t in \mathbb{Z} tali che $d = sa + tb$.*

Dimostrazione. Sia $S = \{xa + yb ; x, y \in \mathbb{Z}, xa + yb > 0\} \subseteq \mathbb{N}$. S è sicuramente non vuoto, perché a e b non sono entrambi nulli e quindi, se ad esempio a è diverso da zero, sarà certamente $a > 0$ o $-a > 0$ e quindi in S . Esisterà pertanto un minimo: sia esso $d = x_0a + y_0b$. Vogliamo provare che tale elemento è un massimo comun divisore di a e b . La (ii) è ovviamente verificata. Resta da provare che $d \mid a$ e $d \mid b$. Dividendo a per d si ha: $a = dq + r$, con $0 \leq r < d$. Ora, $0 \leq r = a - dq = a - (x_0a + y_0b)q = (1 - x_0)a - (-y_0)q \leq d$; per non contraddirre la minimalità di d , deve essere $r = 0$, e quindi $d \mid a$. Analogamente si prova che $d \mid b$. Abbiamo dimostrato in questo modo contemporaneamente l'esistenza del $\text{MCD}(a, b)$ e la sua scrittura nella forma $d = sa + tb$. \square

La scrittura del massimo comun divisore d di due interi a e b nella forma $d = sa + tb$ si dice *identità di Bézout*. Si noti che tale espressione non è unica. Ad esempio, $1 = 3 \cdot 7 + (-4) \cdot 5 = (-2) \cdot 7 + 3 \cdot 5$.

L'algoritmo che proponiamo, detto *algoritmo di Euclide*, o *algoritmo euclideo delle divisioni successive*, ci offre un metodo per il calcolo effettivo del massimo comun divisore di due interi a e b , che sappiamo esistere in virtù della proposizione precedente, e ci permette di determinare una identità di Bézout. Si osservi che se vogliamo determinare il $\text{MCD}(a, b)$, possiamo senz'altro supporre $a \geq b > 0$.

2.2.6 L'ALGORITMO. In quel che segue scriveremo in neretto gli elementi che dovranno essere divisi nella divisione successiva, in modo da evidenziarli: essi verranno quindi spostati a sinistra nella divisione successiva. Siano dunque $a, b \in \mathbb{Z}$ e sia $a \geq b > 0$. Operiamo le seguenti divisioni:

$$\begin{aligned} (1) \quad a &= bq_1 + r_1 & 0 < r_1 < b \\ (2) \quad b &= r_1q_2 + r_2 & 0 < r_2 < r_1 \\ (3) \quad r_1 &= r_2q_3 + r_3 & 0 < r_3 < r_2 \\ &\dots \\ (i+2) \quad r_i &= r_{i+1}q_{i+2} + r_{i+2} & 0 < r_{i+2} < r_{i+1} \end{aligned}$$

$$\begin{aligned} (n-1) \quad r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1} \quad 0 < r_{n-1} < r_{n-2} \\ (n) \quad r_{n-2} &= r_{n-1}q_n + \boxed{r_n} \quad 0 < r_n < r_{n-1} \\ (n+1) \quad r_{n-1} &= r_nq_{n+1} + 0. \end{aligned}$$

Allora

$$\boxed{\text{MCD}(a, b) = r_n \quad (= \text{ultimo resto non nullo})}.$$

Il procedimento si deve certamente fermare (in meno di b passi), dato che $b > r_1 > r_2 > r_3 \dots$ è una successione strettamente decrescente di interi positivi. Ora, dall'ultima divisione $(n+1)$, si vede che r_n divide r_{n-1} , per cui $\text{MCD}(r_n, r_{n-1}) = r_n$. Inoltre, guardando dal basso all'alto, dalla divisione n -esima si vede che r_n divide r_{n-2} , e inoltre, un intero c divide r_n e r_{n-1} se e solo se c divide r_{n-1} e r_{n-2} . Quindi $\text{MCD}(r_{n-1}, r_{n-2}) = \text{MCD}(r_n, r_{n-1}) = r_n$. Proseguendo verso l'alto, si ha $r_n = \text{MCD}(a, b)$.

Inoltre, queste relazioni ci offrono un modo di scrivere il $\text{MCD}(a, b)$ nella forma $\alpha a + \beta b$, cioè ci danno una identità di Bézout. Basta far vedere che tutti i resti delle divisioni si possono scrivere come combinazioni di a e b . Risulta

$$\begin{aligned} r_1 &= a - bq_1 \\ r_2 &= b - r_1q_2 \\ &\dots \\ r_{i+2} &= r_i - r_{i-1}q_{i+2} \\ &\dots \end{aligned}$$

Ora,

$$r_2 = b - r_1q_2 = b - (a - bq_1)q_2 = (-q_2)a + (1 + q_1q_2)b$$

cioè r_1 e r_2 si scrivono come combinazione di a e b . Supposto allora che r_i e r_{i+1} si possano scrivere come combinazione di a e b , allora r_{i+2} si può scrivere come combinazione di a e b . Ma allora ogni resto si può scrivere nel modo richiesto, e in particolare r_n che è il massimo comun divisore.

Diamo ora, attraverso un esempio, una notazione che aiuta i conti e che si presta ad essere programmata. Supponiamo di voler determinare una identità di Bézout per il $\text{MCD}(3522, 321)$. Allora, $a = 3522$, $b = 321$. Si ha

$$\begin{aligned} 3522 &= 321 \cdot 10 + 312 \\ 321 &= 312 \cdot 1 + 9 \\ 312 &= 9 \cdot 34 + 6 \\ 9 &= 6 \cdot 1 + \boxed{3} \\ 6 &= 3 \cdot 2 + 0. \end{aligned}$$

Risulta $\text{MCD}(3522, 321) = 3$. Vogliamo ora esprimere 3 nella forma $\alpha\mathbf{a} + \beta\mathbf{b}$. Conviene introdurre la seguente notazione per esprimere tale combinazione lineare:

$$\alpha\mathbf{a} + \beta\mathbf{b} \equiv (\alpha, \beta)$$

dimenticando cioè \mathbf{a} e \mathbf{b} e scrivendo solo i coefficienti della combinazione lineare all'interno della coppia. All'elemento \mathbf{a} resta associata la coppia $(1, 0)$, mentre a \mathbf{b} resta associata la coppia $(0, 1)$. La somma tra coppie è data da

$$\begin{aligned} (\alpha, \beta) + (\alpha', \beta') &\stackrel{\text{def}}{=} (\alpha + \alpha', \beta + \beta'), \\ \gamma(\alpha, \beta) &\stackrel{\text{def}}{=} (\gamma \cdot \alpha, \gamma \cdot \beta) \end{aligned}$$

$\forall \alpha, \beta, \gamma, \alpha', \beta' \in \mathbb{Z}$. In questo modo le operazioni che portano alla identità di Bézout si possono riassumere nella seguente tabella:

$$\begin{aligned} r_1 &= 312 = \mathbf{a} + \mathbf{b} \cdot (-10) &\equiv (1, 0) + (0, 1)(-10) &= (1, -10) \\ r_2 &= 9 = \mathbf{b} + 312 \cdot (-1) &\equiv (0, 1) + (1, -10)(-1) &= (-1, 11) \\ r_3 &= 6 = 312 + 9 \cdot (-34) &\equiv (1, -10) + (-1, 11)(-34) &= (35, -384) \\ r_4 &= 3 = 9 + 6 \cdot (-1) &\equiv (-1, 11) - (35, -384)(-1) &= (-36, 395). \end{aligned}$$

Quindi

$$3 = (-36) \cdot 3522 + (395) \cdot 321.$$

Si osservi che nella determinazione della coppia associata ad un resto r_i si utilizzano le due coppie associate rispettivamente ai due resti precedenti, cioè r_{i-1} ed r_{i-2} , come è evidente dall'algoritmo. Si può quindi lavorare direttamente con le coppie, senza passare attraverso la scrittura intermedia.

Si consideri ora la seguente equazione, detta equazione diofantea:

$$ax + by = c,$$

dove a, b, c sono in \mathbb{Z} , della quale cerchiamo soluzioni intere. Geometricamente l'equazione rappresenta una retta, della quale stiamo cercando soluzioni intere. Ad esempio, la $2x + 3y = 1$ è rappresentata in figura 2.2.

La seguente proposizione dà una condizione necessaria e sufficiente perché l'equazione $ax + by = c$ ammetta soluzioni intere.

2.2.7 PROPOSIZIONE. *L'equazione $ax + by = c$, $a, b, c \in \mathbb{Z}$, possiede una soluzione intera (x, y) se e solo se $\text{MCD}(a, b) = d$ divide c .*

Dimostrazione. Sia (\bar{x}, \bar{y}) una soluzione intera dell'equazione. Allora il $\text{MCD}(a, b)$, dividendo a e b , dividerà anche tutto il primo membro dell'equazione e quindi anche c .

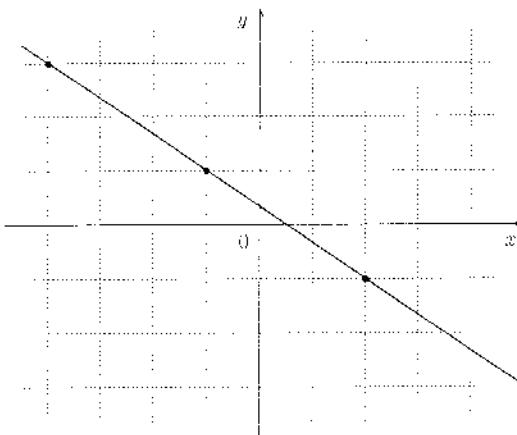


FIGURA 2.2

Viceversa, supponiamo che d divida c . Scriviamo d nella forma $d = \alpha a + \beta b$. Allora, essendo $c = d \cdot h$, sarà

$$c = \alpha ha + \beta hb$$

cioè $(\bar{x} = \alpha h, \bar{y} = \beta h)$ rappresenta una soluzione intera dell'equazione. \square

Ad esempio, la

$$(*) \quad 2x + 5y = 3$$

è risolubile in \mathbb{Z} , perché $(2, 5) = 1$ divide 3. Allora, essendo $1 = (-2)2 + (1)5$, si ha $3 = (-6)2 + (3)5$. Una soluzione intera della $(*)$ è quindi $(-6, 3)$. Si osservi che tale soluzione non è unica. Ad esempio, un'altra soluzione intera di $(*)$ è $(9, -3)$.

Siamo finalmente in grado di provare l'*equivalenza* in \mathbb{Z} delle nozioni di elemento irriducibile ed elemento primo. (Si vedano le definizioni 2.1.12 e 2.1.13, con relativi commenti a proposito della nozione di *numero* primo.) Abbiamo già provato (proposizione 2.1.14) che ogni elemento primo in \mathbb{Z} è irriducibile. Dobbiamo ora provare che ogni elemento irriducibile in \mathbb{Z} è primo.

2.2.8 PROPOSIZIONE. *Ogni elemento irriducibile in \mathbb{Z} è primo.*

Dimostrazione. Dobbiamo provare che dall'essere p un elemento irriducibile in \mathbb{Z} segue che se p divide un prodotto ab , allora p divide a o b . Sia dunque $ab = ph$ e supponiamo che p non divida a . Allora, dato che l'unico divisore di p che divide a è 1, segue che $\text{MCD}(a, p) = 1$. Ma allora esistono s, t tali che $1 = sa + tp$. Moltiplicando per b entrambi i membri, si ottiene $b = sab + tpb$: dato che $p \mid ab$ e $p \mid p$, si conclude che $p \mid b$. \square

 **ESERCIZI.**

- Sia (\bar{x}, \bar{y}) una soluzione intera della $ax + by = c$, $a, b, c \in \mathbb{Z}$. Si provi che tutte e sole le soluzioni intere di tale equazione si ottengono aggiungendo alla (\bar{x}, \bar{y}) una soluzione intera (x_0, y_0) dell'equazione omogenea associata $ax + by = 0$.

 **ESERCIZI DI PROGRAMMAZIONE.**

- Scrivere un programma che calcoli il massimo comun divisore di due interi a e b utilizzando l'algoritmo euclideo delle divisioni successive.
- Scrivere un programma che esprima il massimo comun divisore di a e b nella forma $sa + tb$ per opportuni s e t in \mathbb{Z} , (identità di Bézout), esprimendo ogni resto trovato nelle divisioni dell'algoritmo euclideo come combinazione di a e b .
- Scrivere un programma che dica se una data equazione

$$ax + by = c, \quad a, b, c \in \mathbb{Z}$$

ammette soluzioni in \mathbb{Z} , e che in caso positivo ne calcoli una.


CONTROLLO.

- Chi ci garantisce che ogni coppia di elementi non entrambi nulli di \mathbb{Z} ammette MCD?
- Dare le condizioni perché un'equazione $ax + by = c$ con $a, b, c \in \mathbb{Z}$ sia risolvibile in \mathbb{Z} .

2.3. Fattorizzazione in \mathbb{Z} e alcune conseguenze

2.3.1 TEOREMA FONDAMENTALE DELL'ARITMETICA. *Sia n un intero > 1 . Allora n si può fattorizzare nel prodotto di un numero finito di elementi irriducibili (o numeri primi) $p_j > 1$:*

$$n = p_1^{h_1} p_2^{h_2} p_3^{h_3} \cdots p_s^{h_s}$$

dove i p_j , $j = 1, \dots, s$, sono tutti distinti, gli esponenti h_j sono positivi e $s \geq 1$. Inoltre tale fattorizzazione è unica, nel senso che se n può essere fattorizzato anche al modo seguente

$$n = q_1^{k_1} q_2^{k_2} \cdots q_t^{k_t}$$

con i q_i elementi irriducibili distinti maggiori di 1, allora il numero dei fattori nella prima fattorizzazione coincide con il numero dei fattori della seconda e i q_i coincidono con i p_j a meno dell'ordine.

Dimostrazione. Esistenza della fattorizzazione. Procederemo per induzione sull'intero n da fattorizzare, utilizzando il principio di induzione II (cfr. §1.4). Se $n = 2$, $2 = 2$ è una fattorizzazione in elementi irriducibili > 1 . Supponiamo allora di avere provato l'esistenza di una tale fattorizzazione per ogni intero positivo $k < n$, $k \geq 2$ e dimostriamolo per n . Se n è irriducibile, non c'è nulla da dimostrare. Sia quindi n riducibile, e sia $n = ab$ una fattorizzazione propria, nel senso che a e b sono entrambi ≥ 2 e $< n$. Allora, per l'ipotesi induttiva, a e b sono fattorizzabili in un prodotto di irriducibili maggiori di 1:

$$a = p_1 p_2 \cdots p_r \quad b = \bar{p}_1 \bar{p}_2 \cdots \bar{p}_s .$$

Quindi

$$n = p_1 p_2 \cdots p_r \bar{p}_1 \bar{p}_2 \cdots \bar{p}_s .$$

Per il principio di induzione II ogni intero positivo si può fattorizzare in un prodotto di irriducibili maggiori di 1. Basta poi raggruppare fra loro i numeri primi fra loro uguali nella fattorizzazione per ottenere il risultato nella forma voluta.

Unicità della fattorizzazione. Per dimostrare l'unicità della fattorizzazione per ogni intero positivo n , procederemo per induzione sul numero m di fattori irriducibili di una fattorizzazione di lunghezza minima. Se $m = 1$, significa che il numero n che ha quella come fattorizzazione è un irriducibile (quindi primo) $p > 1$: supponiamo che $n = p$ abbia un'altra fattorizzazione $q_1^{k_1} q_2^{k_2} \cdots q_t^{k_t}$; allora

$$p = q_1^{k_1} q_2^{k_2} \cdots q_t^{k_t}, \quad q_i > 1 .$$

Essendo p un primo che divide il secondo membro, p dividerà uno dei fattori del secondo membro; sia $p \mid q_i$. Anche q_i è irriducibile, quindi non ha fattori propri, da cui $p = q_i$. Per la legge di cancellazione, valida in \mathbb{Z} , si ottiene

$$1 = q_1^{k_1} q_2^{k_2} \cdots q_i^{k_i-1} \cdots q_t^{k_t} .$$

Questa relazione implica che tutti gli esponenti a secondo membro sono nulli, altrimenti avremmo un prodotto di interi maggiori di 1 il cui prodotto dà 1. Allora il secondo membro si riduce a q_i e quindi $p = q_i$ è l'unica fattorizzazione di n . Abbiamo così provato la base dell'induzione. Supponiamo ora che la unicità della fattorizzazione sia stata provata per ogni fattorizzazione in $m - 1$ fattori irriducibili. Sia n un intero che ha una fattorizzazione in m fattori irriducibili. Siano allora

$$n = p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s} = q_1^{k_1} q_2^{k_2} \cdots q_t^{k_t} \quad p_i, q_j > 1$$

due fattorizzazioni di n in fattori irriducibili, la fattorizzazione di sinistra avendo m fattori irriducibili, cioè $h_1 + h_2 + \cdots + h_s = m$. Ora, p_1 è un primo che

divide il secondo membro, quindi dividerà un q_i . Come prima, risulta $p_1 = q_i$, onde si possono cancellare da ambo i membri. Ma allora si resta con

$$p_1^{h_1+1} p_2^{h_2} \cdots p_s^{h_s} = q_1^{k_1} q_2^{k_2} \cdots q_i^{k_i-1} \cdots q_t^{k_t}$$

dove a primo membro il numero di fattori irriducibili è $m - 1$. Per l'ipotesi induktiva vale in questo caso la unicità della fattorizzazione, onde i q_j coincidono con i p_i , a meno dell'ordine. Ma allora anche la fattorizzazione di n è unica. \square

 ATTENZIONE. Si noti come nel corso della dimostrazione si sia utilizzata pesantemente la equivalenza in \mathbb{Z} tra l'essere primo e l'essere irriducibile. \square

Il teorema precedente vale anche per interi arbitrari.

2.3.2 PROPOSIZIONE. *Preso comunque un intero z diverso da zero e da ± 1 , esso ha una unica scrittura della forma*

$$z = \pm p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s}, \quad p_i \text{ irriducibili} > 1.$$

Diamo ora alcune conseguenze di questo importante teorema.

2.3.3 DEFINIZIONE. Siano $a, b \in \mathbb{Z}$. Si definisce *minimo comune multiplo* tra a e b un intero m tale che

(a) m è un multiplo di a e di b ;

(b) se m' è un multiplo comune di a e b , allora m' è un multiplo anche di m . \square

Indicheremo con $\text{mcm}(a, b)$ o con $[a, b]$ il minimo comune multiplo *positivo*.

Il teorema fondamentale dell'aritmetica ci fornisce un metodo ulteriore per il calcolo del massimo comun divisore ed uno per il calcolo del minimo comune multiplo tra due interi. Si tratta sostanzialmente del metodo che si impara a scuola. Si decompiono a e b in fattori primi (e ora sappiamo che è sempre possibile e tale fattorizzazione è unica). Sia

$$a = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r}, \quad b = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}.$$

Si noti che il numero dei primi distinti è uguale in entrambe le fattorizzazioni, perché ammettiamo che gli esponenti possano essere nulli. In questo modo "costringiamo" ad entrare nella fattorizzazione anche dei primi che in realtà non compaiono. Allora è facile vedere che

$$\text{MCD}(a, b) = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

c

$$\text{mcm}(a, b) = p_1^{M_1} p_2^{M_2} \cdots p_r^{M_r}$$

dove $m_i = \min\{h_i, k_i\}$, $M_i = \max\{h_i, k_i\}$. Si noti tuttavia che questo metodo per la ricerca del massimo comun divisore e del minimo comune multiplo

non è molto efficiente. Conviene osservare che vale la seguente relazione tra $\text{MCD}(a, b)$ e $\text{mcm}(a, b)$:

$$\text{mcm}(a, b) = \frac{|a \cdot b|}{\text{MCD}(a, b)}.$$

Allora, per calcolare il minimo comune multiplo di due interi a e b conviene utilizzare l'algoritmo euclideo delle divisioni successive per la determinazione del massimo comune divisore e poi utilizzare la relazione ora detta.

Il teorema fondamentale dell'aritmetica ci permette anche di provare in un batter d'occhio il famoso risultato di Euclide sulla infinità dei numeri primi.

2.3.4 PROPOSIZIONE. *Esistono infiniti numeri primi.*

Dimostrazione. Supponiamo i numeri primi siano in numero finito: siano essi p_1, p_2, p_N . Si consideri l'elemento $a = p_1 \cdot p_2 \cdots p_N + 1$. Esso è un numero intero maggiore di 1, per cui il teorema fondamentale dell'aritmetica ci garantisce che è fattorizzabile in primi. Tuttavia non esiste nessun numero primo che lo divida, perché a diviso per ogni primo p_i dà come resto 1. Questo assurdo ci assicura che i numeri primi sono necessariamente infiniti. \square

Un'altra conseguenza del teorema fondamentale dell'aritmetica è il fatto che, ad esempio, $\sqrt{3}$ non è un numero razionale. Se infatti fosse $\sqrt{3} = r/s$ con r ed s interi, si avrebbe

$$3s^2 = r^2.$$

Ma questo contraddice la unicità della fattorizzazione in \mathbb{Z} perché a sinistra il fattore (irriducibile) 3 compare un numero dispari di volte, mentre a destra o non compare oppure compare un numero pari di volte.

ESERCIZI.

- Utilizzando il teorema fondamentale dell'aritmetica, provare che se p è un numero primo in \mathbb{Z} , allora \sqrt{p} è irrazionale.

CONTROLLO.

- Enunciare con precisione il teorema fondamentale dell'aritmetica.
- Dare alcune applicazioni di tale teorema.

2.4. I numeri razionali

L'esigenza di introdurre nuovi numeri, da "aggiungere" agli interi, sorge quando si voglia risolvere un'equazione del tipo

$$3x = 5$$

che chiaramente non ha soluzione in \mathbb{Z} . Tutti sanno che l'ampliamento da operare corrisponde all'introduzione dei numeri razionali, che sono esattamente le soluzioni di equazioni del tipo

$$ax = b, \quad a, b \in \mathbb{Z}, \quad a \neq 0.$$

Già nei paragrafi precedenti, abbiamo *informalmente* parlato dei numeri razionali. In questo paragrafo tuttavia vogliamo dare una costruzione di tali numeri, procedendo in modo simile a quanto fatto per la costruzione degli interi a partire dai naturali. Si consideri il prodotto cartesiano $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$, ossia l'insieme delle coppie ordinate di interi, in cui il secondo elemento della coppia è diverso da zero. Si introduca in tale insieme la seguente relazione:

$$(a, b) \varrho (c, d) \iff ad = bc.$$

Si tratta di una relazione di equivalenza. Dimostriamo solamente la transitività, dato che le altre due condizioni sono banali. Siano $(a, b) \varrho (c, d)$, e $(c, d) \varrho (e, f)$. Si deve provare che $(a, b) \varrho (e, f)$. Dalle

$$ad = bc, \quad cf = de,$$

moltiplicando la prima uguaglianza a destra per l'elemento (non nullo!) f e la seconda a sinistra per b (anch'esso non nullo) si ottiene per confronto

$$adf = bde.$$

La commutatività della moltiplicazione e la legge di cancellazione, che valgono in \mathbb{Z} (si ricordi che $d \neq 0$), ci permettono di concludere che $af = be$, ossia $(a, b) \varrho (e, f)$.

Ebbene, poniamo

$$\boxed{\mathbb{Q} \stackrel{\text{def}}{=} (\mathbb{Z} \times \mathbb{Z} \setminus \{0\})/\varrho}.$$

Gli elementi di \mathbb{Q} sono quindi le classi di equivalenza, che indicheremo con

$$\overline{(a, b)}.$$

La figura 2.3 mostra alcuni elementi di \mathbb{Q} , ossia alcune classi di equivalenza in $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$.

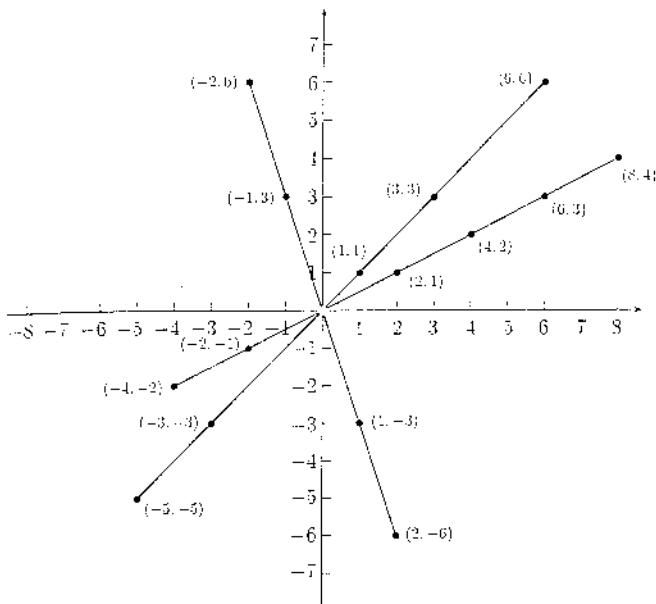


FIGURA 2.3

Introduciamo in \mathbb{Q} le seguenti operazioni:

$$\overline{(a, b)} + \overline{(c, d)} \stackrel{\text{def}}{=} \overline{(ad + bc, bd)}$$

$$\overline{(a, b)} \cdot \overline{(c, d)} \stackrel{\text{def}}{=} \overline{(ac, bd)}.$$

Osserviamo innanzitutto che le coppie $(ad + bc, bd)$ e (ac, bd) stanno entrambe in $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$, dato che in \mathbb{Z} non ci sono divisori dello zero. Resta da provare che tali definizioni sono *ben poste*, ossia che, pur essendo definite attraverso dei rappresentanti delle classi, non dipendono da questi.

Siamo

$$(a, b) \not\sim (a', b'), \quad (c, d) \not\sim (c', d').$$

Si tratta di provare che

$$(ad + bc, bd) \not\sim (a'd' - b'c', b'd'). \quad \text{ossia} \quad (ad + bc)b'd' = bd(a'd' + b'c').$$

Ricordando che $ab' = ba'$ e $cd' = dc'$ si vede immediatamente che tale relazione è verificata. Analoga dimostrazione per la moltiplicazione.

Le classi

$$0 \stackrel{\text{def}}{=} \overline{(0, 1)} = \overline{(0, b)}$$

$$1 \stackrel{\text{def}}{=} \overline{(1, 1)} = \overline{(a, a)}$$

sono elementi neutri rispettivamente per l'addizione e per la moltiplicazione. Rispetto a queste operazioni \mathbb{Q} è un anello commutativo con unità. Tuttavia vale una proprietà ulteriore. Risulta

$$\overline{(a, b)} \cdot \overline{(b, a)} = \overline{(ab, ba)} = \overline{(1, 1)}, \quad \forall \overline{(a, b)}, \text{ tale che } a \neq 0, b \neq 0.$$

Si noti che (b, a) sta in $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ perché si è supposto $a \neq 0$. L'elemento (b, a) prende il nome di *inverso* dell'elemento (a, b) . Un anello comunitativo con unità in cui ogni elemento non nullo ammette inverso moltiplicativo prende il nome di *campo*. Abbiamo così provato il seguente risultato.

2.4.1 PROPOSIZIONE. *L'insieme*

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z} \setminus \{0\})/\varrho$$

è un campo.

Vogliamo ora mostrare il seguente ulteriore risultato.

2.4.2 PROPOSIZIONE. *Il campo \mathbb{Q} è un'estensione di \mathbb{Z} . Inoltre ogni elemento di \mathbb{Q} è della forma uv^{-1} , con $u, v \in \mathbb{Z}$, $v \neq 0$.*

Dimostrazione. Dobbiamo trovare dentro \mathbb{Q} una *copia* di \mathbb{Z} . Basta a tal fine notare che l'applicazione

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow \mathbb{Q} \\ a &\longmapsto \overline{(a, 1)} \end{aligned}$$

è iniettiva (si provi). Inoltre il trasformato mediante φ della somma di due elementi di \mathbb{Z} è la somma (in \mathbb{Q}) dei trasformati, e così per il prodotto. Questo ci garantisce che l'immagine di \mathbb{Z} in \mathbb{Q} è la *copia* di \mathbb{Z} che cercavamo dentro \mathbb{Q} .

Infine, ogni elemento $(a, b) \in \mathbb{Q}$, si può scrivere nella forma

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)},$$

dove $\overline{(a, 1)}$ e $\overline{(1, b)}$ sono identificabili mediante la φ a elementi di \mathbb{Z} e quindi $\overline{(1, b)}$ è l'inverso di un elemento di \mathbb{Z} . Ogni elemento di \mathbb{Q} è quindi della forma uv^{-1} , $u, v \in \mathbb{Z}$, $v \neq 0$. \square

Dato che ogni elemento di \mathbb{Q} si può scrivere nella forma uv^{-1} , $u, v \in \mathbb{Z}$, $v \neq 0$, si dice che \mathbb{Q} è *campo dei quozienti* di \mathbb{Z} .

Siamo autorizzati allora a scrivere gli elementi di \mathbb{Q} nella forma più usuale

$$\overline{(a, b)} = \overline{(a, 1)} \overline{(1, b)} = \frac{a}{b}$$

ossia sotto forma di frazione.

In particolare, ogni equazione del tipo

$$ax = b, \quad a, b \in \mathbb{Z}, \quad a \neq 0$$

è risolubile in \mathbb{Q} (si provi). Abbiamo così risolto il nostro problema iniziale.

ESERCIZI.

- Si provino in dettaglio tutti i punti per dimostrare che \mathbb{Q} è un campo.
- Si verifichi che le operazioni di addizione e moltiplicazione definiti in $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z} \setminus \{0\})/\varrho$, ristrette agli elementi di \mathbb{Z} (o meglio alla *copia* di \mathbb{Z} che si trova in \mathbb{Q}) coincidono con le operazioni definite in \mathbb{Z} .
- Si controlli che addizione e moltiplicazione definiti in $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z} \setminus \{0\})/\varrho$ coincidono con le ordinarie operazioni tra frazioni.
- Si provi che ogni equazione del tipo $ax = b$, $a, b \in \mathbb{Z}$, $a \neq 0$, è risolubile in \mathbb{Q} .

CONTROLLO.

- Fare gli esercizi proposti.

2.5. I numeri di Fibonacci

Abbiamo parlato nel §1.4 di relazioni ricorsive e di una particolare successione definita ricorsivamente, la successione dei numeri di Fibonacci. Dedicheremo questo paragrafo allo studio di qualche notevole proprietà di questa successione, dato che giocherà un ruolo importante in molti campi, apparentemente slegati. Ricordiamo la definizione della successione $\{F_n\}$ dei *numeri di Fibonacci*:

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2} \quad \text{per } n > 1.$$

Ogni termine della successione è quindi somma dei due termini precedenti. I primi termini della successione sono, come si è visto, a partire da F_1 ,

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \dots$$

I numeri di Fibonacci sorgono in molte situazioni e compaiono spesso in natura (ad esempio nei petali di certi fiori o in qualche specie di pigna). Sono stati introdotti da Leonardo Fibonacci come soluzione del problema delle *coppie di conigli*. Il problema era quello di modellare la crescita di una popolazione di conigli. Più precisamente, supponiamo che ogni coppia di conigli impieghi un

mese per diventare adulta e un secondo mese per procreare un'altra coppia. Se al primo mese si ha una sola coppia e se si fa l'ipotesi ulteriore che nessun animale muoia, allora quante coppie si avranno dopo n mesi? Indicando con \circ una coppia non ancora adulta e con \bullet una coppia capace di procreare, e con a_n il numero di coppie dopo n mesi, la situazione che si presenta è illustrata in figura 2.4.

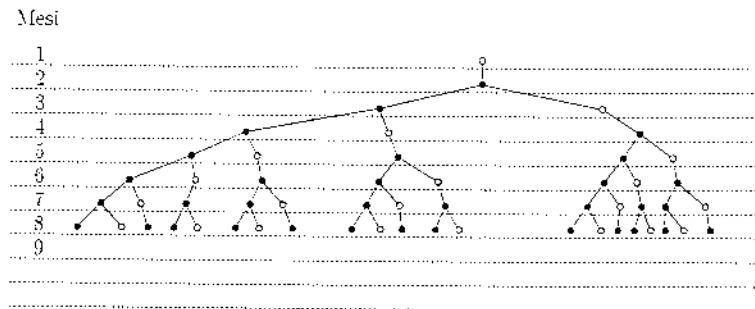


FIGURA 2.4. Schema di riproduzione.

Dallo schema si deduce quanto segue:

- Dopo la prima riproduzione, il ramo destro riproduce lo stesso schema dell'intero albero (il tutto traslato di due mesi). Cioè la situazione in questo ramo all' n -mo mese è quella che si aveva nell'intero albero due mesi prima, cioè a_{n-2} .
- Nel ramo sinistro la situazione dell'intero albero si riproduce dopo solo un mese. Quindi all' n -mo mese la situazione è come quella del mese precedente. Quindi risulta

$$a_n = a_{n-1} + a_{n-2}, \quad a_0 = 0, \quad a_1 = 1.$$

Diamo qui di seguito alcune delle proprietà dei numeri di Fibonacci.

2.5.1 PROPOSIZIONE. *Se F_n sono i numeri di Fibonacci, per ogni $n > 0$ vale la seguente identità (di Cassini):*

$$C(n) \quad F_{n+1}F_{n-1} - F_n^2 = (-1)^n.$$

Dimostrazione. Procederemo per induzione su n . Per $n = 1$ si ha $F_2F_0 - F_1^2 = 1 \cdot 0 - 1 = -1$, quindi $C(1)$ è vera. Supposta vera $C(n-1)$, ossia

$$C(n-1) \quad F_nF_{n-2} - F_{n-1}^2 = (-1)^{n-1},$$

si tratta di provare $C(n)$. Ora, sostituendo nella $C(n-1)$ (che stiamo supponendo vera) $F_{n-2} = F_n - F_{n-1}$, si ottiene

$$F_n(F_n - F_{n-1}) - F_{n-1}^2 = (-1)^{n-1}, \quad \text{cioè} \quad F_n^2 - F_nF_{n-1} - F_{n-1}^2 = (-1)^{n-1}$$

che coincide con la $C(n)$ cambiata di segno, a seguito della sostituzione $F_{n-1} = F_n - F_{n-1}$. Quindi $C(n)$ è vera e l'identità di Cassini è stata provata per ogni n . \square

Vogliamo ora trovare una "soluzione" della relazione ricorsiva, ossia una "formula chiusa" che ci permetta di determinare il termine n -esimo della successione direttamente come funzione di n e non dei termini precedenti. Prendendo come esempio il caso di una progressione geometrica

$$a_n = r \cdot a_{n-1}, \quad a_0 = k$$

in cui la "soluzione" è

$$a_n = k \cdot r^n \quad n \geq 0,$$

cerchiamo *una* soluzione della relazione ricorsiva

$$(2.5.1) \quad F_n = F_{n-1} + F_{n-2}$$

che non tenga per il momento conto delle condizioni iniziali e che sia della forma

$$F_n = x^n$$

per qualche x costante reale, da determinare. Sostituendo allora la soluzione x^n nella (2.5.1) si ottiene

$$x^n - x^{n-1} - x^{n-2} = x^{n-2}(x^2 - x - 1) = 0.$$

Ora, tale equazione è soddisfatta per $x = 0$, soluzione che scartiamo perché banale, oppure per x soluzione dell'equazione

$$x^2 - x - 1 = 0$$

che prende il nome di *equazione caratteristica* della relazione ricorsiva $F_n = F_{n-1} + F_{n-2}$. Le radici di $x^2 - x - 1 = 0$ sono

$$\alpha = \frac{1 + \sqrt{5}}{2}, \quad \beta = \frac{1 - \sqrt{5}}{2}.$$

Si osservi che nessuna delle due soluzioni $F_n = \alpha^n$ o $F_n = \beta^n$ soddisfa le condizioni iniziali $F_0 = 0$, $F_1 = 1$. Tuttavia è facile vedere (si provi) che se α^n e β^n sono entrambe soluzioni di (2.5.1), allora anche una qualunque loro combinazione lineare del tipo

$$(2.5.2) \quad A_1 \alpha^n + A_2 \beta^n$$

è soluzione di (2.5.1).

Cerchiamo quindi soluzioni di tipo (2.5.2)

$$(2.5.3) \quad F_n = A_1 \alpha^n + A_2 \beta^n$$

(dove α e β sono le due soluzioni dell'equazione $x^2 - x - 1 = 0$) che soddisfano le condizioni iniziali

$$0 = A_1\alpha^0 + A_2\beta^0, \quad 1 = A_1\alpha + A_2\beta.$$

Si tratta di risolvere il sistema seguente:

$$\begin{cases} 0 = A_1 + A_2 \\ 1 = A_1 \cdot \left(\frac{1 + \sqrt{5}}{2}\right) + A_2 \cdot \left(\frac{1 - \sqrt{5}}{2}\right). \end{cases}$$

Si trovano le soluzioni $A_1 = 1/\sqrt{5}$ e $A_2 = -A_1 = -1/\sqrt{5}$, che, sostituiti in (2.5.3), danno la forma chiusa dell' n -esimo numero di Fibonacci:

$$(2.5.4) \quad F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right].$$

2.5.2 DEFINIZIONE. Il numero

$$\frac{1 + \sqrt{5}}{2}$$

prende il nome di *rapporto aureo* o *proporzione divina*. □

Il rapporto più armonioso tra due lunghezze a e b era considerato infatti dai Greci quello tale che

$$\frac{a}{b} = \frac{a+b}{a},$$

tanto che la facciata del Partenone è stata inscritta in un rettangolo avente queste proporzioni. Risolvendo la proporzione, si ottiene

$$\frac{a}{b} = \frac{1 + \sqrt{5}}{2} \approx 1.61803.$$

La costruzione geometrica che permette, dato un segmento di lunghezza a , di costruire il segmento di lunghezza b tale che a/b sia il rapporto aureo, è illustrata nella figura 2.5: si costruisce il quadrato $ABCD$ di lato a , e dal punto medio M del segmento AB si traccia il segmento (di lunghezza $\sqrt{5}a/2$) MC . Il punto E intersezione della retta per A e B con la circonferenza di centro M e raggio MC è tale che \overline{BE} è la lunghezza b richiesta.

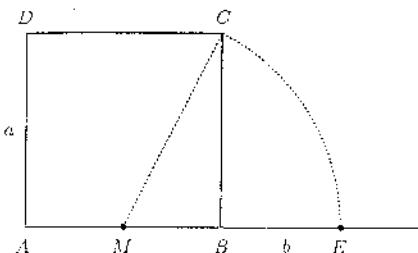


FIGURA 2.5

Spesso il numero $(1 + \sqrt{5})/2$ si indica con la lettera Φ , dal nome dell'artista greco Fidia, che nelle sue sculture utilizzò spesso questo rapporto. Anche l'altra radice

$$\frac{1 - \sqrt{5}}{2} = -\frac{1}{\Phi} \cong -.61803$$

gode di molte delle proprietà di Φ , e spesso si indica con $\widehat{\Phi}$.

La (2.5.4) ci dice che, quando n è grande, F_n è molto vicino al numero irrazionale $\Phi^n/\sqrt{5}$. Infatti, per n grande, essendo $|\widehat{\Phi}| < 1$, $\widehat{\Phi}^n$ diventa esponenzialmente piccolo, quindi trascurabile.

La successione dei numeri di Fibonacci è legata anche all'algoritmo euclideo per la determinazione del massimo comun divisore tra due interi a e b . Infatti esiste il seguente risultato.

2.5.3 PROPOSIZIONE. *Dato comunque un $n > 0$ esistono due interi positivi a e b tali che nel calcolo del $\text{MCD}(a, b)$ con l'algoritmo euclideo, il numero delle divisioni necessarie è esattamente n .*

Dimostrazione. Basta scegliere $a = F_{n+2}$, $b = F_{n+1}$, rispettivamente l' $(n+2)$ -esimo e l' $(n+1)$ -esimo numero di Fibonacci. Infatti

$$\begin{aligned}
 F_{n+2} &= F_{n+1} \cdot 1 + F_n & 0 < F_n < F_{n+1} \\
 F_{n+1} &= F_n \cdot 1 + F_{n-1} & 0 < F_{n-1} < F_n \\
 F_n &= F_{n-1} \cdot 1 + F_{n-2} & 0 < F_{n-2} < F_{n-1} \\
 F_{n-1} &= F_{n-2} \cdot 1 + F_{n-3} & 0 < F_{n-3} < F_{n-2} \\
 &\dots \\
 F_4 &= F_3 \cdot 1 + F_2 & 0 < F_2 < F_3 \\
 F_3 &= F_2 \cdot 2 + 0
 \end{aligned}$$

Sono esattamente n divisioni (F_{n-k} è diverso da zero fin quando $k = n-1$). \square

Questa proposizione ci permette di determinare un limite superiore per il numero di divisioni necessarie per completare l'algoritmo euclideo partendo da due interi arbitrari a e b . Dalla proposizione infatti si può dedurre che per

ogni coppia di interi positivi a e b tali che $a > b$ e $b < F_n$ (dove F_n è l' n -esimo numero di Fibonacci), il numero $D(a, b)$ di divisioni necessarie per ottenere un resto nullo mediante l'algoritmo di Euclide è minore di n (cfr. esercizio 2.5.12). Si noti che il numero di divisioni nell'algoritmo euclideo può essere ridotto se, anziché scegliere come resto il più piccolo resto *positivo*, si scelgono i resti soggetti alla condizione

$$-\frac{1}{2}r_{i-1} \leq r_i \leq \frac{1}{2}r_{i-1}$$

Un'altra interpretazione dei numeri di Fibonacci è la seguente. Si consideri il sottoinsieme $S = \{1, 2, \dots, n\}$ di \mathbb{N} , e si supponga di voler contare i sottoinsiemi di S che *non* contengono due numeri consecutivi di S . Ciò significa che se X è un tale sottoinsieme e $i \in X$, allora $i-1$ ed $i+1$ non appartengono ad X . Se identifichiamo un sottoinsieme di S con la sua funzione caratteristica, ossia lo rappresentiamo come una parola di n lettere, ciascuna delle quali può essere 1 o 0 a seconda che l'elemento corrispondente stia in X o no, allora contare tali sottoinsiemi equivale a contare le parole che non hanno mai due simboli 1 consecutivi. Fissiamo l'attenzione sui sottoinsiemi con k elementi; allora la parola che li rappresenterà conterrà k volte il simbolo 1. Per contare quante sono queste parole, partiamo da $n - k$ simboli 0:

$$\underbrace{0 \ 0 \ 0 \ \dots \ 0}_{n-k}.$$

In quanti modi si possono inserire k cifre 1 in modo che due di loro non siano mai adiacenti? Essendo i posti vuoti disponibili in numero di $n - k + 1$, le k cifre 1 si possono sistemare in

$$s(n, k) = \binom{n - k + 1}{k}$$

modi. Quindi le parti di S non contenenti due interi consecutivi sono $s(n)$, dove

$$(2.5.5) \quad s(n) = \sum_k s(n, k) = \sum_{\substack{h+k=n+1 \\ k \leq h}} \binom{h}{k}.$$

D'altra parte (cfr. esercizio 2.5.10), vale la seguente relazione:

$$F_n = \sum_{\substack{h+k=n-1 \\ k \leq h}} \binom{h}{k},$$

che è anche messa in luce dalla seguente figura:

n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$	$\binom{n}{7}$
0	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	4	6	4	1			
5	1	5	10	10	5	1		
6	1	6	15	20	15	6	1	
7	1	7	21	35	35	21	7	1

Si può quindi concludere dando un significato “geometrico” ai numeri di Fibonacci. In virtù di (2.5.5) l’ $(n+2)$ -esimo numero di Fibonacci

$$F_{n+2} = \sum_{\substack{h+k=n+1 \\ k \leq h}} \binom{h}{k} = s(n)$$

rappresenta il numero di sottoinsiemi dell’insieme $S := \{1, 2, 3, \dots, n\} \subset \mathbb{N}$ che non contengono due numeri consecutivi di S .



ESERCIZI.

1. Si provi per induzione che due numeri di Fibonacci consecutivi sono coprimi.
2. Si determinino i valori di n per i quali F_{n+1}/F_n è un intero.
3. Si provi che per ogni n e ogni k in \mathbb{N} risulta

$$F_{n+k} = F_k F_{n+1} + F_{k-1} F_n.$$

Se ne deduca che F_{kn} è un multiplo di F_n .

4. Si provi che il massimo comun divisore di due numeri di Fibonacci è ancora un numero di Fibonacci. Precisamente

$$\text{MCD}(F_n, F_m) = F_d, \quad d = \text{MCD}(m, n).$$

5. Si provi che F_k divide F_n se e solo se k divide n .
6. Si provi induttivamente che ogni intero positivo si può scrivere come somma di un numero finito di numeri di Fibonacci distinti.
7. Si provi per induzione che per ogni $n \geq 1$ risulta

$$F_n \geq \left(\frac{1 + \sqrt{5}}{2} \right)^{n-2}.$$

8. Si provi che

$$\lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n} = \frac{1 + \sqrt{5}}{2}.$$

9. Si provi che per ogni n risulta

$$F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}.$$

10. Si provi che per ogni n risulta

$$F_{n+2} = \sum_{\substack{h+k=n+1 \\ k \leq h}} \binom{h}{k}.$$

(Si suggerisce di procedere per induzione su n , utilizzando la relazione ricorsiva dei numeri di Fibonacci e la $\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$.)

11. Si provi per induzione su k che se r_n è il primo resto nullo nell'algoritmo euclideo, allora

$$r_{n-k} \geq F_k.$$

12. Si sfrutti il risultato dell'esercizio precedente per dimostrare che se $b < F_n$, allora, per ogni $a \geq b$, il numero $D(a, b)$ di divisioni necessarie per ottenere un resto nullo nell'algoritmo euclideo è

$$D(a, b) < n.$$

13. Si chiamano *numeri di Euclide* gli interi e_i definiti per ricorrenza al modo seguente:

$$e_1 = 2, \quad e_n = e_1 e_2 \cdots e_{n-1} + 1 \quad n \geq 1.$$

Si calcoli il $\text{MCD}(e_n, e_m)$ per ogni n e ogni m , e si determini $D(e_n, e_m)$, ossia il numero di divisioni per ottenere un resto nullo nell'algoritmo euclideo.



ESERCIZI DI PROGRAMMAZIONE.

1. Si scriva un programma che determini se un dato intero n è un numero di Fibonacci. Si utilizzi tale programma per verificare gli esercizi 2.5.2, 2.5.3, 2.5.5 e 2.5.7.
2. Si scriva un programma che calcoli il MCD di due numeri di Fibonacci, e si verifichino con tale programma gli esercizi 2.5.1 e 2.5.4.
3. Si scriva un programma che esprima ogni intero n come somma di numeri di Fibonacci distinti (cfr. esercizio 2.5.6).
4. Si scriva un programma che permetta, dati due interi a e b , $a \geq b$, di calcolare il numero di divisioni necessarie per portare a termine l'algoritmo euclideo (cfr. esercizio 2.5.12).



CONTROLLO.

1. Dare alcune proprietà dei numeri di Fibonacci e alcune loro applicazioni.
2. Il rapporto aureo è ... In che modo è legato ai numeri di Fibonacci?

2.6. Congruenze: prime proprietà e applicazioni

In questo paragrafo definiremo un'importante relazione in \mathbb{Z} , la *relazione di congruenza modulo un intero positivo n* . In sostanza questa relazione identifica tra loro due interi se la loro differenza è un multiplo di n . Tale relazione quindi si può pensare come un'uguaglianza a meno di multipli di n . Si pensi ad esempio alla lettura delle ore sull'orologio: alle quattro del pomeriggio (ossia 16 ore dopo la mezzanotte) noi "leggiamo" la cifra 4. Ai fini del computo delle ore della giornata, quindi, la cifra 16 "uguaglia" la cifra 4. Stiamo lavorando *modulo 12*. Diamo la definizione precisa.

2.6.1 DEFINIZIONE. Sia n un fissato intero positivo. Si dice *relazione di congruenza modulo n* la relazione su \mathbb{Z} definita al modo seguente:

$$\boxed{a \equiv_n b \text{ ovvero } a \equiv b \pmod{n} \iff a - b = nh \text{ per qualche } h \in \mathbb{Z}}. \quad \square$$

2.6.2 PROPOSIZIONE. *Ogni intero a è congruo modulo n ad un intero r tale che $0 \leq r < n$.*

Dimostrazione. Basta osservare che ogni intero a è congruo modulo n al resto r della divisione di a per n (cfr. proposizione 2.2.3). \square

Per illustrare meglio la situazione, possiamo pensare gli interi disposti su di una circonferenza di lunghezza n . In tal modo appare chiaro che tutti i multipli interi di n vengono a coincidere con 0, gli interi che divisi per n danno per resto 1 vengono a coincidere con 1, quelli che divisi per n danno come resto 2 vengono a coincidere con 2, ecc.

La relazione di congruenza gode di molte delle proprietà dell'uguaglianza tra numeri interi. Il simbolo di \equiv è stato introdotto da Gauss, proprio per l'analogia con la relazione di uguaglianza.

2.6.3 PROPOSIZIONE. *Sia $n > 0$ un intero fissato. La relazione di congruenza modulo n è una relazione di equivalenza. Inoltre, se a, b, c, d sono elementi di \mathbb{Z} , allora valgono le seguenti proprietà:*

$$(2.6.1) \quad a \equiv b \pmod{n}, \quad c \equiv d \pmod{n} \implies \begin{cases} a - c \equiv b - d \pmod{n} \\ ac \equiv bd \pmod{n}. \end{cases}$$

Dimostrazione. La relazione è di equivalenza: si veda esercizio 1.2.1. Dimostriamo la (2.6.1): $a \equiv b \pmod{n} \iff a - b = hn, c \equiv d \pmod{n} \iff c - d = kn$, da cui $a + c - (b + d) = (h+k)n$ cioè $a + c \equiv b + d \pmod{n}$. Analogamente,

$ac - bd = ac - ad + ad - bd = a(c - d) + (a - b)d = akn + hnd = (ak + hd)n$ e quindi $ac \equiv bd \pmod{n}$. \square

Le classi di equivalenza sono:

$$\bar{0} = \{\text{interi che divisi per } n \text{ danno per resto } 0\} = \{kn \mid k \in \mathbb{Z}\}$$

$$\bar{1} = \{\text{interi che divisi per } n \text{ danno per resto } 1\} = \{kn + 1 \mid k \in \mathbb{Z}\}$$

...

$$\overline{n-1} = \{\text{interi che divisi per } n \text{ danno per resto } n-1\}$$

$$= \{kn + n - 1 \mid k \in \mathbb{Z}\}.$$

Indicheremo con \mathbb{Z}_n l'insieme quoziente di \mathbb{Z} rispetto alla congruenza modulo n :

$$\boxed{\mathbb{Z}_n \stackrel{\text{def}}{=} \mathbb{Z}/\equiv_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}}.$$

La proposizione 2.6.3 ci dice che la relazione di congruenza definita su \mathbb{Z} è *compatibile con le due operazioni definite in \mathbb{Z}* . Questo ci assicura che se si definiscono in \mathbb{Z}_n le seguenti due operazioni:

$$\boxed{\bar{a} + \bar{b} \stackrel{\text{def}}{=} \overline{a+b}, \quad \bar{a} \cdot \bar{b} \stackrel{\text{def}}{=} \overline{a \cdot b}},$$

queste sono *ben poste*, cioè, pur essendo definite attraverso i rappresentanti, non dipendono da questi. Rispetto a queste due operazioni, è facile vedere che \mathbb{Z}_n è un anello commutativo con unità. Esso prende il nome di *anello delle classi resto modulo n*. Diamo qui sotto la tavola additiva e moltiplicativa di \mathbb{Z}_n nei casi $n = 4$ e $n = 5$.

-	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$$n = 4$$

-	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

-	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$$n = 5$$

-	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Si noti il diverso comportamento di \mathbb{Z}_4 rispetto a \mathbb{Z}_5 : il primo possiede divisori dello zero (cfr. definizione 2.1.6), mentre il secondo no. Quindi, \mathbb{Z}_4 non è un dominio di integrità, mentre \mathbb{Z}_5 lo è. Si provi a generalizzare questa osservazione (cfr. esercizio 2.6.1).

2.6.1 COROLARIO. *Sia n un fissato intero positivo. Allora per ogni $a, b, c \in \mathbb{Z}$ se $a \equiv b \pmod{n}$ si ha*

$$(2.6.2) \quad a + c \equiv b + c \pmod{n}$$

$$(2.6.3) \quad ac \equiv bc \pmod{n}$$

$$(2.6.4) \quad a^i \equiv b^i \pmod{n} \quad \forall i \in \mathbb{N}.$$

Dimostrazione. Le congruenze (2.6.2) e (2.6.3) sono casi particolari di (2.6.1), mentre (2.6.4) si ottiene da (2.6.1) per induzione. \square

Non bisogna pensare però che tutto quello che vale per l'uguaglianza valga automaticamente anche per la congruenza. Ad esempio, la legge di cancellazione $ac = bc \implies a = b$, che vale in \mathbb{Z} purché sia $c \neq 0$, non si trasporta alle congruenze, ad esempio

$$3 \cdot 5 \equiv 3 \cdot 8 \pmod{9}$$

ma non è vero che $5 \equiv 8 \pmod{9}$. Vale tuttavia il seguente risultato.

2.6.5 PROPOSIZIONE. *Se $ac \equiv bc \pmod{n}$ e $(c, n) = 1$, allora $a \equiv b \pmod{n}$.*

Dimostrazione. La $ac \equiv bc \pmod{n}$ ci dice che $n \mid (a - b)c$. Ora, la $(c, n) = 1$ implica che esistono s, t tali che $1 = sc + tn$: moltiplicando per $a - b$ ambo i membri, si ottiene

$$a - b = (a - b)sc + (a - b)tn = (a - b)c \cdot s + (a - b)tn$$

da cui risulta che n deve dividere $(a - b)$ dato che divide il secondo membro e quindi $a \equiv b \pmod{n}$. \square

Si osservi che nell'esempio che abbiamo dato prima *non* era verificata l'ipotesi richiesta, perché $(3, 9) = 3 \neq 1$.

In realtà questa proposizione è una conseguenza del seguente risultato più generale.

2.6.6 PROPOSIZIONE. *Se $ac \equiv bc \pmod{n}$, allora $a \equiv b \pmod{n/d}$, dove $d = (c, n)$.*

Dimostrazione. La proposizione sostanzialmente dice che si può sempre semplificare una congruenza cancellando un fattore comune, *purché si cambi opportunamente il modulo*: $ac \equiv bc \pmod{n} \iff (a - b)c \equiv 0 \pmod{n}$, da cui, dividendo per $d = (c, n)$, $(a - b)(c/d) \equiv 0 \pmod{n/d}$ (si osservi che le frazioni c/d e n/d sono dei numeri interi). Ma allora n/d divide il prodotto $(a - b) \cdot (c/d)$ e $(c/d, n/d) = 1$, quindi (si provi!) $n/d \mid (a - b)$, cioè $a \equiv b \pmod{n/d}$. \square

Riprendendo l'esempio precedente, $5 \not\equiv 8 \pmod{9}$, ma $5 \equiv 8 \pmod{9/3}$. La proposizione appena dimostrata collega fra loro due congruenze rispetto a moduli diversi. Raccogliamo nella seguente proposizione altre proprietà utili, che legano fra loro congruenze relative a moduli diversi.

2.6.7 PROPOSIZIONE. Sussistono le seguenti proprietà:

- (a) Se $a \equiv b \pmod{n}$ e $d \mid n$, allora $a \equiv b \pmod{d}$;
- (b) se $a \equiv b \pmod{r}$ e $a \equiv b \pmod{s}$, allora $a \equiv b \pmod{[r, s]}$.

Dimostrazione. Basta ricordare la definizione di congruenza. \square

Diamo qui di seguito alcune congruenze notevoli.

2.6.8 PROPOSIZIONE. Per ogni numero primo p e ogni x, y in \mathbb{Z} vale la seguente congruenza:

$$(x + y)^p \equiv x^p + y^p \pmod{p}.$$

Dimostrazione. Risulta

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

Si tratta di provare che la sommatoria è divisibile per p . Ma questo è vero, perché nella sommatoria risulta $k < p$ e $p - k < p$, onde ogni $\binom{p}{k}$ che compare nella sommatoria è un intero che ha p a fattore. \square

2.6.9 TEOREMA (PICCOLO TEOREMA DI FERMAT). Sia a un intero e p un numero primo. Allora

$$a^p \equiv a \pmod{p}.$$

Dimostrazione. Supponiamo $a \geq 0$, per cui possiamo procedere per induzione prendendo come variabile di induzione a stessa. Se $a = 0$ il risultato è ovvio. Supponiamo allora vero il risultato per a , cioè

$$a^p \equiv a \pmod{p},$$

e dimostriamolo per $a + 1$. Per la proposizione precedente

$$(a + 1)^p \equiv a^p + 1^p.$$

Ma $1^p = 1$ e $a^p \equiv a$ per l'ipotesi induttiva. Quindi

$$(a + 1)^p \equiv a + 1$$

che è quanto volevano provare.

Supponiamo ora $a < 0$. Allora $0 \equiv 0^p = (a + (-a))^p \equiv a^p + (-a)^p \pmod{p}$. Dato che è $-a > 0$, per quanto provato al punto precedente è $(-a)^p \equiv -a$, quindi $0 \equiv a^p - a$ cioè $a^p \equiv a$. \square

2.6.10 COROLLARIO. Se è $(a, p) = 1$, allora

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dimostrazione. Nelle ipotesi attuali possiamo semplificare per a il risultato della proposizione precedente. \square

Chiediamo questo paragrafo con alcune utili applicazioni delle congruenze. Ricordiamo la cosiddetta "prova del nove" per controllare l'esattezza di una moltiplicazione tra interi. Supponiamo di voler moltiplicare fra loro due interi, 2356 e 431, e supponiamo di avere trovato come risultato 1015436. Vogliamo controllarne l'esattezza. Allora si procede al modo seguente: si scrive la somma delle cifre dei fattori e si fa la moltiplicazione di questi due numeri; questa deve coincidere con la somma delle cifre del risultato da controllare. Quindi nel nostro caso

$$\begin{array}{rcl} 2356 \times & 2 + 3 + 5 + 6 = 16, & 1 + 6 = 7 \\ 431 = & 4 + 3 + 1 = 8, & 8 = 8 \\ 1015436 & 1 + 0 + 1 + 5 + 4 + 3 + 6 = 20, & 2 + 0 = \boxed{2}. \end{array}$$

A questo punto si fa il prodotto $7 \cdot 8 = 56$, la cui somma delle cifre è $5 + 6 = 11$. $1 + 1 = 2$ che coincide con la somma delle cifre del risultato della moltiplicazione dei due numeri originari. Se anziché 2 avessimo trovato un altro numero, voleva dire che *sicuramente* avevamo commesso un errore nella moltiplicazione. Il fatto di aver superato il controllo positivamente *non garantisce* però che la moltiplicazione sia corretta. Cerchiamo di capire cosa c'è dietro questa "prova del nove", in particolare vediamo cosa c'entra il nove. Il numero 2356 corrisponde a scrivere $2 \cdot 10^3 + 3 \cdot 10^2 + 5 \cdot 10 + 6$. Ora, qualsunque sia $n > 0$, $10^n - 1 = \underbrace{999 \cdots 9}_{n \text{ volte}} = 9 \cdot \underbrace{111 \cdots 1}_{n \text{ volte}}$, cioè

$$10^n \equiv 1 \pmod{9}.$$

Ritornando al nostro esempio e utilizzando le proprietà delle congruenze,

$$2356 \Rightarrow 2 \cdot 10^3 + 3 \cdot 10^2 + 5 \cdot 10 + 6 \equiv 2 + 3 + 5 + 6 \pmod{9}$$

ossia 2356 è congruo modulo 9 alla somma delle sue cifre. Ecco dove interviene il nove e la spiegazione della "prova del nove". Questo è un fatto generale: se z è il numero intero

$$z = a_n a_{n-1} a_{n-2} \cdots a_1 a_0 = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$$

allora

$$z \equiv a_n + a_{n-1} + \cdots + a_0 \pmod{9}.$$

cioè ogni numero intero, scritto in base 10, è congruo modulo 9 alla somma delle sue cifre.

 ATTENZIONE. Nella prova del nove il test che deve essere superato è che un numero e la somma delle sue cifre siano congrui modulo nove, ossia stiano nella stessa classe modulo 9 (figura 2.6). È chiaro quindi che si tratta di una condizione necessaria, ma non sufficiente per l'esattezza dei calcoli. □

8	431
7	2356
6	
5	
4	
3	
2	56 1015436
1	
0	

FIGURA 2.6

Utilizzando ancora le proprietà delle congruenze, siamo in grado di offrire alcuni criteri di divisibilità, senza svolgere nessuna divisione.

I numeri interi saranno scritti in forma decimale, ossia nella forma

$$z = a_n a_{n-1} \cdots a_0 = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_0.$$

2.6.11 CRITERIO DI DIVISIBILITÀ PER 3 E PER 9. Un numero intero è divisibile per 3 (per 9) se e solo se la somma delle sue cifre è divisibile per 3 (per 9).

Dimostrazione. $z \equiv a_n + a_{n-1} + \cdots + a_0$ sia modulo 3 sia modulo 9. □

2.6.12 CRITERIO DI DIVISIBILITÀ PER 2 E PER 5. Un numero intero è divisibile per 2 o per 5 se e solo se l'ultima cifra di destra, a_0 , è divisibile per 2 o per 5.

Dimostrazione. Per ogni $n \geq 1$, $10^n \equiv 0$ sia modulo 2 sia modulo 5. Quindi $z \equiv a_0$ sia modulo 2 sia modulo 5. □

2.6.13 CRITERIO DI DIVISIBILITÀ PER 4. Un intero z è divisibile per 4 (o per 25) se e solo se il numero $a_1 a_0$ formato dalle sue ultime due cifre è divisibile per 4 (o per 25).

Dimostrazione. $100 = 2^2 5^2 \equiv 0$ sia modulo 4 sia modulo 25. Allora ogni intero è congruo modulo 4 o modulo 25 all'intero costituito dalle sue ultime due cifre di destra. In particolare, vale il criterio di divisibilità richiesto. □

2.6.14 CRITERIO DI DIVISIBILITÀ PER 2^k . Un intero z è divisibile per 2^k se e solamente se 2^k divide il numero costituito dalle ultime k cifre di z .

Dimostrazione. Infatti

$$10^n = 2^n \cdot 5^n \equiv 0 \pmod{2^k} \text{ per ogni } n \geq k.$$

Quindi, ad esempio, per vedere se un numero è divisibile per 8 basta vedere se sono divisibili per 8 le ultime tre cifre. \square

2.6.15 CRITERIO DI DIVISIBILITÀ PER 11. Un intero è divisibile per 11 se e solo se

$$a_0 - a_1 + a_2 - \cdots + (-1)^n a_n$$

è divisibile per 11.

Dimostrazione. Basta osservare che

$$10 \equiv -1 \pmod{11} \implies \begin{cases} 10^{2p} \equiv 1 \pmod{11} \\ 10^{2p+1} \equiv -1 \pmod{11}. \end{cases} \quad \square$$

Le proprietà delle congruenze ci permettono di risolvere anche altri tipi di problemi.

2.6.16 PROBLEMA. Al variare di $h \in \mathbb{N}$, trovare il resto della divisione per 9 di 74^{6h} . Si ha

$$74 \equiv 2 \pmod{9} \implies 74^{6h} \equiv 2^{6h} \pmod{9}.$$

Inoltre,

$$2^{6h} = (2^6)^h \quad \text{e} \quad 2^6 \equiv 1 \pmod{9}$$

quindi, per ogni $h \in \mathbb{N}$

$$74^{6h} \equiv 1^h \equiv 1 \pmod{9}.$$

e il resto cercato è 1.

2.6.17 PROBLEMA. Trovare il resto della divisione per 10 del numero

$$43816^{20321}.$$

Si ha $43816 \equiv 6 \pmod{10}$, e inoltre $6^2 \equiv 6 \pmod{10}$ e quindi $6^k \equiv 6 \pmod{10}$ per ogni $k > 0$. Ne segue che

$$43816^{20321} \equiv 6 \pmod{10}.$$

 ESERCIZI.

1. Si studi la struttura additiva e quella moltiplicativa di \mathbb{Z}_n per vari n . Per quali n \mathbb{Z}_n è un dominio di integrità?
2. Si determini il resto della divisione per 9 del numero

$$57432^{1142}$$

e il resto della divisione per 3 del numero

$$89741^{527}.$$

3. Si determinino le ultime due cifre del numero 302^{46} e del numero 7^{506} .
4. Si provi che per ogni $n \in \mathbb{N}$ il numero

$$2n^{17} + 2n^{15} + 3n^3 + 3n$$

è divisibile per 5.

5. Si dica se è vera o no la seguente affermazione:

$$a^k \equiv 1 \pmod{n}, \quad a^l \equiv 1 \pmod{n} \implies a^{\text{MCD}(k,l)} \equiv 1 \pmod{n}.$$

Se è vera, dimostrarla.

6. Si provi che $2^n \not\equiv 1 \pmod{n}$, se $n > 1$.
7. Si provi che il numero

$$z = a_n a_{n-1} a_{n-2} \cdots a_1 a_0 = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$$

è divisibile per 7 se e solo se 7 divide $a_3 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \cdots$.

Si provi che questo stesso criterio vale per la divisibilità per 11 e per 13 (ossia z è divisibile per 11 (o per 13) se e solo se è divisibile per 11 (o per 13) il numero $a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \cdots$).

8. Si calcoli il MCD delle seguenti coppie di numeri:

$$(4096, 13\,456\,791\,245\,321), \quad (1296, 3\,422\,573\,248\,525\,122).$$

9. Si provi che nessun numero naturale della forma $4n + 3$ può scriversi come somma di due quadrati.



ESERCIZI DI PROGRAMMAZIONE.

1. Si scriva un programma che verifichi se un dato intero è divisibile per 2, 3, 4, 5, 7, 9, 11, 2^k .
2. Si scriva un programma che stampi la tavola additiva di \mathbb{Z}_n e quella moltiplicativa.



CONTROLLO.

1. Proprietà delle congruenze.
2. In cosa consiste la prova del nove?
3. Spiegare i criteri di divisibilità. Tali criteri sono necessari e sufficienti?

2.7. Risoluzione di congruenze lineari e il teorema cinese del resto

Iniziamo con la seguente definizione.

2.7.1 DEFINIZIONE. Si definisce *congruenza lineare* nell'incognita x ogni equazione della forma

$$ax \equiv b \pmod{n}$$

con $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$. \square

Ci poniamo il problema di vedere se e quando una congruenza di questo tipo ammette soluzioni, dove per soluzione si intende ogni intero x_0 tale che $ax_0 \equiv b \pmod{n}$. Già dai seguenti esempi si vede come si possano presentare sia casi in cui la congruenza è risolubile, sia casi in cui non è risolubile.

2.7.2 ESEMPIO. La $4x \equiv 5 \pmod{6}$ non ammette soluzioni, perché altrimenti dovrebbe essere risolubile in \mathbb{Z} l'equazione $4x + 6y = 5$, mentre sappiamo che questa equazione non ammette soluzioni intere perché $(4, 6) = 2 \nmid 5$ (cfr. proposizione 2.2.7). \square

2.7.3 ESEMPIO. La $2x \equiv 6 \pmod{8}$ ammette invece ad esempio la soluzione $x = 3$. Ma anche $x = 7$ è soluzione. \square

Si tratta quindi di dare delle risposte generali riguardanti la risoluzione di una congruenza lineare. Daremo prima una risposta riguardante la *compatibilità* di una congruenza lineare, cioè l'esistenza o meno di soluzioni. Poi ci occuperemo, per congruenze che siano compatibili, del problema di contare le soluzioni.

2.7.4 PROPOSIZIONE. *La congruenza*

$$ax \equiv b \pmod{n}$$

ammette soluzioni se e solo se $(a, n) \mid b$.

Dimostrazione. La risoluzione della congruenza equivale alla risoluzione in interi della equazione

$$ax + ny = b$$

che sappiamo ammettere soluzioni intere se e solo se $(a, n) \mid b$ (cfr. proposizione 2.2.7). \square

La proposizione che segue ci dice *quante* sono le soluzioni di una congruenza che ammetta una soluzione.

2.7.5 PROPOSIZIONE. *Sia $ax \equiv b \pmod{n}$ una congruenza tale che sia $(a, n) \mid b$. Indicata con x_0 una sua soluzione, tutte e sole le soluzioni sono del tipo*

$$x_0 + h \cdot \frac{n}{(a, n)}, \quad h \in \mathbb{Z}.$$

Tra queste, le soluzioni

$$x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + 2 \cdot \frac{n}{d}, \quad \dots, \quad x_0 + (d-1) \cdot \frac{n}{d}$$

sono tutte non congruenti tra di loro e ogni altra è congruente ad una di queste. Quindi la congruenza ammette esattamente $d = (a, n)$ soluzioni non congruenti modulo n .

Dimostrazione. Proviamo innanzitutto che per ogni $h \in \mathbb{Z}$ $x_0 + h \cdot n/(a, n)$ è una soluzione. Infatti

$$a \left(x_0 + h \cdot \frac{n}{(a, n)} \right) = ax_0 \pm h[a, n] = b \pm \text{multiplo di } n.$$

Proviamo ora che *ogni* soluzione è di questo tipo. Siano x_0 e x'_0 due soluzioni; allora risulta

$$ax_0 = b + hn, \quad ax'_0 = b + kn,$$

da cui

$$a(x_0 - x'_0) = (h - k)n.$$

Dividendo ambo i membri per (a, n) si ottiene

$$\frac{a}{(a, n)}(x_0 - x'_0) = (h - k)\frac{n}{(a, n)}.$$

Essendo $a/(a, n)$ e $n/(a, n)$ coprimi, $n/(a, n)$ divide $x_0 - x'_0$, cioè $x_0 - x'_0 = z \cdot n/(a, n)$.

Resta da far vedere che tra le soluzioni $x_0 + h \cdot n/(a, n)$, al variare di h in \mathbb{Z} , ce ne sono esattamente $d = (a, n)$ non congruenti modulo n . Faremo vedere che le soluzioni

$$(2.7.1) \quad x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + 2 \cdot \frac{n}{d}, \quad \dots, \quad x_0 + (d-1) \cdot \frac{n}{d}$$

sono incongrue modulo n e ogni altra soluzione è congruente ad una di queste.

Supponiamo per assurdo che due delle soluzioni (2.7.1) siano congruenti modulo n , cioè

$$x_0 + h_1 \cdot \frac{n}{d} \equiv x_0 + h_2 \cdot \frac{n}{d} \pmod{n}$$

con $h_1, h_2 \in \mathbb{Z}$ e $0 \leq h_1 < h_2 \leq d - 1$. Allora si avrebbe

$$h_1 \cdot \frac{n}{d} \equiv h_2 \cdot \frac{n}{d} \pmod{n}$$

da cui, dividendo per n/d (che è il MCD($n/d, n$)),

$$h_1 \equiv h_2 \pmod{n/(n/d)}$$

e quindi

$$h_1 \equiv h_2 \pmod{d}$$

che è assurdo perché $0 < h_2 - h_1 < d$.

Per provare che *ogni* soluzione del tipo $x_0 + h \cdot (n/d)$, al variare di h in \mathbb{Z} è congruente ad una delle (2.7.1), basta dividere h per d : $h = dq + r$, con $0 \leq r \leq d - 1$, da cui

$$x_0 + h \cdot \frac{n}{d} = x_0 - (dq + r) \frac{n}{d} = x_0 + qn + \frac{n}{d}r \equiv x_0 + \frac{n}{d}r, \quad 0 \leq r \leq d - 1. \quad \square$$

La congruenza $2x \equiv 6 \pmod{8}$ del secondo esempio dato in questo paragrafo ammette infatti esattamente $2 = \text{MCD}(2, 8)$ soluzioni incongrue modulo 8, $x = 3$ e $x = 7$.

2.7.6 COROLLARIO. *Se $(a, n) = 1$ (in particolare se $n = p$ è un numero primo e a non è un multiplo di n), allora la congruenza $ax \equiv b \pmod{n}$ ammette un'unica soluzione modulo n .*

Vogliamo ora risolvere un *sistema* di congruenze

$$(2.7.2) \quad \begin{cases} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \\ \dots \\ a_sx \equiv b_s \pmod{n_s}. \end{cases}$$

in cui supporremo $(n_i, n_j) = 1$ per $i \neq j$. Una soluzione di un tale sistema è un intero che soddisfa contemporaneamente *tutte* le congruenze del sistema. Questo implica naturalmente che se anche una sola delle congruenze non è risolubile, allora il sistema non potrà ammettere soluzioni.

2.7.7 LEMMA. *Sia*

$$\begin{cases} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \\ \dots \\ a_sx \equiv b_s \pmod{n_s}. \end{cases}$$

con $(n_i, n_j) = 1$ per $i \neq j$ un sistema di congruenze tali che ogni congruenza del sistema ammetta soluzioni. Allora la risoluzione di (2.7.2) equivale a risolvere un sistema del tipo

$$(2.7.3) \quad \begin{cases} x \equiv c_1 \pmod{n'_1} \\ x \equiv c_2 \pmod{n'_2} \\ \dots \\ x \equiv c_s \pmod{n'_s} \end{cases}$$

con $(n'_i, n'_j) = 1$ per $i \neq j$.

Dimostrazione. Perché il sistema (2.7.2) ammetta soluzioni è necessario che, per ogni $k = 1, \dots, s$, $d_k = \text{MCD}(a_k, n_k)$ divida b_k . Una volta che siano soddisfatte queste condizioni, si può dividere la k -esima congruenza per d_k , ottenendo il nuovo sistema equivalente al precedente (nel senso che ammette le stesse soluzioni):

$$(2.7.2') \quad \begin{cases} a'_1 x \equiv b'_1 \pmod{n'_1} \\ a'_2 x \equiv b'_2 \pmod{n'_2} \\ \dots \\ a'_s x \equiv b'_s \pmod{n'_s} \end{cases}$$

dove $a'_k = a_k/d_k$, $b'_k = b_k/d_k$ e $n'_k = n_k/d_k$; inoltre, vale ancora la condizione $(n'_i, n'_j) = 1$ per $i \neq j$. Ora, si noti che per ogni $k = 1, \dots, s$ si ha $(a'_k, n'_k) = 1$ per cui, in base al corollario 2.7.6, ciascuna delle congruenze del sistema ammette *un'unica* soluzione c_k modulo n'_k . Possiamo allora sostituire nuovamente il sistema (2.7.2') con il seguente sistema:

$$(2.7.3) \quad \begin{cases} x \equiv c_1 \pmod{n'_1} \\ x \equiv c_2 \pmod{n'_2} \\ \dots \\ x \equiv c_s \pmod{n'_s} \end{cases}$$

Abbiamo così provato che ogni sistema di congruenze di tipo (2.7.2) si può ridurre ad un sistema di tipo (2.7.3). \square

Passiamo quindi a studiare sistemi di congruenze di tipo (2.7.3). La risoluzione di questo tipo di sistemi appare nella letteratura cinese del primo secolo d.C., e da qui il nome del teorema.

2.7.8 TEOREMA CINESE DEL RESTO. Siano r_1, r_2, \dots, r_s interi positivi tali che $(r_i, r_j) = 1$ per ogni $i \neq j$. Allora il sistema di congruenze

$$\begin{cases} x \equiv c_1 \pmod{r_1} \\ x \equiv c_2 \pmod{r_2} \\ \dots \\ x \equiv c_s \pmod{r_s} \end{cases}$$

ammette una soluzione che è unica modulo $r_1 r_2 \cdots r_s$.

Dimostrazione. Se $R = r_1 r_2 \cdots r_s$, e $R_k = R/r_k$, allora è $(R_k, r_k) = 1$, come è facile provare dall'ipotesi $(r_i, r_j) = 1$. Quindi la congruenza k -esima

$$R_k x \equiv c_k \pmod{r_k}$$

ammette un'unica soluzione, \bar{x}_k , modulo r_k . Il numero

$$\bar{x} = R_1 \bar{x}_1 + R_2 \bar{x}_2 + \cdots + R_s \bar{x}_s$$

è una soluzione simultanea del sistema dato: infatti, essendo R_i multiplo di r_k per $i \neq k$, sarà $R_i \equiv 0 \pmod{r_k}$ per $i \neq k$. Ne segue che

$$\begin{cases} \bar{x} \equiv R_1 \bar{x}_1 \equiv c_1 \pmod{r_1} \\ \bar{x} \equiv R_2 \bar{x}_2 \equiv c_2 \pmod{r_2} \\ \dots \\ \bar{x} \equiv R_s \bar{x}_s \equiv c_s \pmod{r_s}, \end{cases}$$

ossia \bar{x} è una soluzione del sistema.

Per quanto riguarda l'unicità modulo $r_1 r_2 \cdots r_s$, sia \bar{y} un'altra soluzione del sistema, cioè

$$\bar{x} \equiv c_k \equiv \bar{y} \pmod{r_k} \quad \forall k = 1, \dots, s.$$

Allora $\bar{x} - \bar{y} \equiv 0 \pmod{r_k}$ $\forall r_k$, da cui $\bar{x} - \bar{y} \equiv 0 \pmod{r_1 r_2 \cdots r_s}$. \square

2.7.9 OSSERVAZIONE. Se si vuole risolvere un sistema del tipo

$$\begin{cases} a_1 x \equiv b_1 \pmod{r_1} \\ a_2 x \equiv b_2 \pmod{r_2} \\ \dots \\ a_s x \equiv b_s \pmod{r_s} \end{cases}$$

con $(a_i, r_i) = 1$ e $(r_i, r_j) = 1$ per $i \neq j$, allora la soluzione sarà

$$\bar{x} = R_1 \bar{x}_1 + R_2 \bar{x}_2 + \cdots + R_s \bar{x}_s$$

dove, per ogni $k = 1, \dots, s$, \bar{x}_k è tale che $a_k R_k \bar{x}_k \equiv b_k \pmod{r_k}$. \square

Il teorema cinese del resto ha diverse applicazioni, come avremo modo di vedere. Cominciamo con una sua utilizzazione molto particolare. Supponiamo di dover contare un folto gruppo di ragazzi che si trovano radunati in un cortile, senza doverli chiamare uno per uno. Si sa che i ragazzi sono meno di 1000. Allora basta che si chieda loro di allinearsi per 7, per 11 e per 13, e ogni volta che si sono allineati, si contano i ragazzi che restano fuori: tali resti r_i , ($i = 1, 2, 3$) saranno rispettivamente minori di 7, di 11 e di 13. Dopo di che si risolve la congruenza:

$$\begin{cases} x \equiv r_1 \pmod{7} \\ x \equiv r_2 \pmod{11} \\ x \equiv r_3 \pmod{13} \end{cases}$$

che, in virtù del teorema cinese del resto, ammette un'unica soluzione modulo $7 \cdot 11 \cdot 13 = 1001$. Tale soluzione rappresenta il numero totale dei ragazzi.

Il seguente risultato è anch'esso conseguenza del teorema cinese del resto.

Sia $\mathbb{Z}_r \times \mathbb{Z}_s$ l'insieme prodotto cartesiano di \mathbb{Z}_r e \mathbb{Z}_s (cfr. §1.1). Si possono introdurre in $\mathbb{Z}_r \times \mathbb{Z}_s$ le seguenti due operazioni componente per componente:

$$\begin{aligned} (\bar{a}_r, \bar{b}_s) + (\bar{a}'_r, \bar{b}'_s) &\stackrel{\text{def}}{=} (\bar{a}_r + \bar{a}'_r, \bar{b}_s + \bar{b}'_s) \\ (\bar{a}_r, \bar{b}_s) \cdot (\bar{a}'_r, \bar{b}'_s) &\stackrel{\text{def}}{=} (\bar{a}_r \cdot \bar{a}'_r, \bar{b}_s \cdot \bar{b}'_s). \end{aligned}$$

Ebbene, si ha la seguente proposizione.

2.7.10 PROPOSIZIONE. *Siano r ed s due interi maggiori o uguali a 2 e relativamente primi. Allora la corrispondenza*

$$f : \mathbb{Z}_{rs} \longrightarrow \mathbb{Z}_r \times \mathbb{Z}_s$$

definita ponendo

$$f(\bar{x}_{rs}) = (\bar{x}_r, \bar{x}_s)$$

dove con \bar{x}_k si intende la classe resto modulo k , è una corrispondenza biunivoca e conserva le operazioni, è tale cioè che

$$f(\bar{x}_{rs} + \bar{y}_{rs}) = f(\bar{x}_{rs}) + f(\bar{y}_{rs})$$

c

$$f(\bar{x}_{rs} \cdot \bar{y}_{rs}) = f(\bar{x}_{rs}) \cdot f(\bar{y}_{rs}).$$

Dimostrazione. In virtù del teorema cinese del resto il sistema di congruenze

$$\begin{cases} x \equiv a \pmod{r} \\ x \equiv b \pmod{s} \end{cases} .$$

ammette una ed una sola soluzione modulo rs . Questo ci garantisce la suriettività e l'iniettività della applicazione. Il fatto che tale applicazione conservi le operazioni viene lasciato come esercizio (cfr. esercizio 2.7.7). \square

2.7.11 ESEMPIO. Scriviamo esplicitamente la corrispondenza f nel caso in cui sia $r = 2$, $s = 3$.

$$\begin{aligned} \mathbb{Z}_6 &\longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 \\ \bar{0}_6 &\longmapsto (\bar{0}_2, \bar{0}_3) \\ \bar{1}_6 &\longmapsto (\bar{1}_2, \bar{1}_3) \\ \bar{2}_6 &\longrightarrow (\bar{0}_2, \bar{2}_3) \\ \bar{3}_6 &\longrightarrow (\bar{1}_2, \bar{0}_3) \\ \bar{4}_6 &\longmapsto (\bar{0}_2, \bar{1}_3) \\ \bar{5}_6 &\longmapsto (\bar{1}_2, \bar{2}_3) . \end{aligned}$$

In generale tale corrispondenza si ottiene rapidamente con il seguente metodo. Si scrivono sulla prima colonna tutti gli elementi di \mathbb{Z}_{rs} . Sulla seconda tutti gli elementi di \mathbb{Z}_r , ripetuti s volte, sulla terza colonna tutti gli elementi di \mathbb{Z}_s , ripetuti r volte. La corrispondenza f è quella che associa al k -esimo elemento di \mathbb{Z}_{rs} la coppia costituita rispettivamente dal k -esimo elemento di \mathbb{Z}_r e dal k -esimo elemento di \mathbb{Z}_s , come appare dallo schema sotto riportato:

$$\begin{aligned} \bar{0}_6 &\longmapsto (\bar{0}_2, \bar{0}_3) \\ \bar{1}_6 &\longrightarrow (\bar{1}_2, \bar{1}_3) \\ \bar{2}_6 &\longmapsto (\bar{0}_2, \bar{2}_3) \\ \bar{3}_6 &\longrightarrow (\bar{1}_2, \bar{0}_3) \\ \bar{4}_6 &\longmapsto (\bar{0}_2, \bar{1}_3) \\ \bar{5}_6 &\longmapsto (\bar{1}_2, \bar{2}_3) . \end{aligned}$$

Questa proposizione ha un'applicazione importante nel campo dei calcolatori, perché permette di trasportare calcoli in \mathbb{Z}_n a calcoli *indipendenti* in vari \mathbb{Z}_{n_i} , $i = 1, \dots, r$, se $n = n_1 n_2 \cdots n_r$, con $(n_i, n_j) = 1$ se $i \neq j$. Illustriamo questa affermazione con un esempio da cui si possa già capire il vantaggio di questa possibilità. Supponiamo di dover fare delle operazioni in \mathbb{Z}_{21} , in particolare di dover moltiplicare la classe $\bar{17}$ per la classe $\bar{19}$ in \mathbb{Z}_{21} . Anziché lavorare in \mathbb{Z}_{21} , essendo $21 = 3 \cdot 7$, dove $(3, 7) = 1$, potremo utilizzare la corrispondenza f

della proposizione 2.7.10:

$$\begin{aligned}
 Z_{21} &\longleftrightarrow Z_3 \times Z_7 \\
 \bar{0}_{21} &\longleftrightarrow (\bar{0}_3, \bar{0}_7) \\
 \bar{1}_{21} &\longleftrightarrow (\bar{1}_3, \bar{1}_7) \\
 \bar{2}_{21} &\longleftrightarrow (\bar{2}_3, \bar{2}_7) \\
 \bar{3}_{21} &\longleftrightarrow (\bar{0}_3, \bar{3}_7) \\
 \bar{4}_{21} &\longleftrightarrow (\bar{1}_3, \bar{4}_7) \\
 \bar{5}_{21} &\longleftrightarrow (\bar{2}_3, \bar{5}_7) \\
 \bar{6}_{21} &\longleftrightarrow (\bar{0}_3, \bar{6}_7) \\
 \bar{7}_{21} &\longleftrightarrow (\bar{1}_3, \bar{0}_7) \\
 \bar{8}_{21} &\longleftrightarrow (\bar{2}_3, \bar{1}_7) \\
 \bar{9}_{21} &\longleftrightarrow (\bar{0}_3, \bar{2}_7) \\
 \overline{10}_{21} &\longleftrightarrow (\bar{1}_3, \bar{3}_7) \\
 \overline{11}_{21} &\longleftrightarrow (\bar{2}_3, \bar{4}_7) \\
 \overline{12}_{21} &\longleftrightarrow (\bar{0}_3, \bar{5}_7) \\
 \overline{13}_{21} &\longleftrightarrow (\bar{1}_3, \bar{6}_7) \\
 \overline{14}_{21} &\longleftrightarrow (\bar{2}_3, \bar{0}_7) \\
 \overline{15}_{21} &\longleftrightarrow (\bar{0}_3, \bar{1}_7) \\
 \overline{16}_{21} &\longleftrightarrow (\bar{1}_3, \bar{2}_7) \\
 \overline{17}_{21} &\longleftrightarrow (\bar{2}_3, \bar{3}_7) \\
 \overline{18}_{21} &\longleftrightarrow (\bar{0}_3, \bar{4}_7) \\
 \overline{19}_{21} &\longleftrightarrow (\bar{1}_3, \bar{5}_7) \\
 \overline{20}_{21} &\longleftrightarrow (\bar{2}_3, \bar{6}_7)
 \end{aligned}$$

Dalla tavola risulta che $\overline{17}$ è identificabile con la coppia $(\bar{2}_3, \bar{3}_7)$, mentre $\overline{19}$ è identificabile con $(\bar{1}_3, \bar{5}_7)$. Allora, anziché fare il prodotto $\overline{17} \cdot \overline{19}$ in Z_{21} basta fare separatamente il prodotto $\bar{2} \cdot \bar{1}$ in Z_3 e il prodotto $\bar{3} \cdot \bar{5}$ in Z_7 . Si ottiene la coppia $(\bar{2}_3, \bar{1}_7)$, che corrisponde all'elemento $\bar{8}$ di Z_{21} , che ovviamente è la stessa classe che si sarebbe ottenuto operando dentro Z_{21} . Il fatto che le operazioni in Z_3 e in Z_7 si possono fare *separatamente*, ossia sono indipendenti le une dalle altre, permette ad esempio di poter utilizzare due diversi calcolatori. \square



ESERCIZI.

1. Si trovino tutte le soluzioni (se esistono) delle seguenti congruenze:

- | | |
|------------------------------|------------------------------|
| (a) $3x \equiv 5 \pmod{4}$, | (b) $3x \equiv 9 \pmod{6}$ |
| (c) $4x \equiv 7 \pmod{9}$, | (d) $6x \equiv 8 \pmod{9}$. |

2. Si costruisca una congruenza lineare del tipo

$$ax \equiv b \pmod{319}$$

che ammetta esattamente 11 soluzioni non congruenti tra loro modulo 319.
Scrivere tale congruenza, si determinino tutte le soluzioni.

3. Dire se il seguente sistema di congruenze

$$\begin{cases} x \equiv 7 \pmod{9} \\ x \equiv 3 \pmod{5} \end{cases}$$

ammette soluzioni, e in caso positivo determinarle.

4. Si risolva il seguente sistema di congruenze:

$$\begin{cases} 1025x \equiv 5312065 \pmod{8} \\ 36x \equiv 322 \pmod{5} \\ 4x \equiv 7 \pmod{3} \end{cases}$$

5. Si consideri il seguente sistema di congruenze:

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$$

nel quale non si chiede che sia $(n, m) = 1$. Si diano le condizioni affinché tale sistema sia risolubile.

6. Se da un sacchetto di caramelle si tolgoano le caramelle a due a due, a tre a tre, a quattro a quattro, a cinque a cinque, a sei a sei, nel sacchetto resta sempre una caramella. Se si tolgoano a sette a sette, non ne resta nessuna. Si determini il minimo numero di caramelle che potevano trovarsi nel sacchetto.
7. Si provi che la corrispondenza di cui alla proposizione 2.7.10 conserva le operazioni.
8. Si risolva la congruenza

$$4x \equiv 3 \pmod{385}.$$



ESERCIZI DI PROGRAMMAZIONE.

1. Fare un programma che determini se una data congruenza lineare

$$ax \equiv b \pmod{n}$$

ammette soluzioni, e, in caso positivo, determini tutte le d soluzioni non congruenti mod n , dove $d = \text{MCD}(a, n)$.

2. Fare un programma che risolva un sistema di congruenze del tipo

$$\begin{cases} x \equiv c_1 \pmod{r_1} \\ x \equiv c_2 \pmod{r_2} \\ \dots \\ x \equiv c_s \pmod{r_s} \end{cases}$$

con $(r_i, r_j) \neq 1$ per $i \neq j$. Si utilizzi il teorema cinese del resto.

3. Si scriva un programma che trovi esplicitamente, per r e s tali che $(r, s) = 1$, la corrispondenza biunivoca tra \mathbb{Z}_{rs} e $\mathbb{Z}_r \times \mathbb{Z}_s$ garantita dal teorema cinese del resto, quella cioè che associa ad ogni \bar{a}_{rs} la coppia (\bar{a}_r, \bar{a}_s) (dove \bar{a}_k rappresenta la classe resto modulo k). Si consiglia di utilizzare il seguente metodo efficiente che permette, noto (\bar{x}_r, \bar{x}_s) , di ricavare \bar{x}_{rs} :

- (i) Si risolve prima il problema per $(\bar{1}_r, \bar{0}_s)$ e per $(\bar{0}_r, \bar{1}_s)$: si tratta di risolvere i seguenti due sistemi di congruenze:

$$\begin{cases} x \equiv 1 \pmod{r}, \\ x \equiv 0 \pmod{s}, \end{cases} \quad \begin{cases} y \equiv 0 \pmod{r}, \\ y \equiv 1 \pmod{s}. \end{cases}$$

Per risolvere questi sistemi si può utilizzare l'algoritmo di Euclide, ed esprimere 1 nella forma $1 = r\alpha + s\beta$, per opportuni α e β in \mathbb{Z} e poi prendere $x = s\beta$, $y = r\alpha$, eventualmente ridotti modulo rs .

- (ii) Una volta che si conosca il corrispondente di $(\bar{1}_r, \bar{0}_s)$ e $(\bar{0}_r, \bar{1}_s)$, la determinazione del corrispondente di (\bar{x}_r, \bar{x}_s) in \mathbb{Z}_{rs} è immediata. Infatti, se \bar{a}_{rs} e \bar{b}_{rs} sono gli elementi di \mathbb{Z}_{rs} corrispondenti rispettivamente a $(\bar{1}_r, \bar{0}_s)$ e a $(\bar{0}_r, \bar{1}_s)$, allora l'elemento di \mathbb{Z}_{rs} corrispondente alla coppia (\bar{x}_r, \bar{x}_s) è $(ax + by)_{rs}$ (si verifichi).



COSTROLLO.

1. Risolvere una congruenza lineare significa ...
2. Quante sono le soluzioni di una congruenza lineare (che sia compatibile)?
3. Come viene utilizzato il teorema cinese del resto per provare che se $(r, s) = 1$, allora $\mathbb{Z}_{rs} \simeq \mathbb{Z}_r \times \mathbb{Z}_s$?

2.8. La funzione di Eulero e il teorema di Eulero

Abbiamo visto (corollario 2.6.10) che se p è un numero primo e a non è un multiplo di p , allora

$$a^{p-1} \equiv 1 \pmod{p}.$$

In questo paragrafo dimostreremo il teorema di Eulero, che è una generalizzazione di questo risultato, perché si riferisce a moduli arbitrari n e non solamente

a moduli primi. Il risultato è del tipo

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Si tratta di scoprire chi è questa funzione $\varphi(n)$, che nel caso in cui n sia un numero primo p deve coincidere con $p - 1$.

2.8.1 DEFINIZIONE. Sia $n \geq 1$. Si definisce $\varphi(n)$ la funzione di n che rappresenta il numero di interi positivi $< n$ e relativamente primi con n . Essa prende il nome di *funzione di Euler* o anche *funzione φ* . \square

Ad esempio, $\varphi(20) = 8$ perché i numeri minori di 20 e relativamente primi con 20 sono 1, 3, 7, 9, 11, 13, 17, 19.

Le proposizioni che seguono ci permettono di calcolare la funzione di Euler per ogni intero n del quale si conosca la fattorizzazione. Nel prossimo paragrafo parleremo della difficoltà di fattorizzare interi grandi.

2.8.2 PROPOSIZIONE. Sia $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ la fattorizzazione di n , con i p_i ($i = 1, \dots, s$) primi distinti. Allora risulta

$$(2.8.1) \quad \varphi(n) = \varphi(p_1^{k_1}) \varphi(p_2^{k_2}) \cdots \varphi(p_s^{k_s}).$$

Dimostrazione. Si tratta di dimostrare che la funzione di Euler è *moltiplicativa*, cioè

$$\varphi(r \cdot s) = \varphi(r)\varphi(s) \quad \forall r, s \text{ tali che } (r, s) = 1.$$

Sia $n = rs$, $(r, s) = 1$. I numeri m tali che $0 \leq m < n$ si possono (cfr. proposizione 2.7.10) rappresentare come coppie del tipo

$$(m \bmod r, m \bmod s)$$

e si ha (si provi!)

$$(m, rs) = 1 \iff (m \bmod r, r) = 1 \text{ e } (m \bmod s, s) = 1.$$

Il numero totale $\varphi(rs)$ degli $m \bmod rs$ coprimi con rs è quindi $\varphi(r) \cdot \varphi(s)$, perché gli elementi $\bmod r$ coprimi con r nel primo elemento della coppia sono in numero di $\varphi(r)$ e quelli $\bmod s$ coprimi con s nel secondo elemento della coppia sono in numero di $\varphi(s)$. \square

Con questo risultato a disposizione, siamo ridotti a dover calcolare il valore di φ sulle potenze di un primo, ossia $\varphi(p^h)$.

2.8.3 PROPOSIZIONE. Se p è un numero primo, allora

$$\varphi(p^h) = p^h - p^{h-1}.$$

Dimostrazione. Basta osservare che non sono primi con p^h solo i multipli di p e questi sono del tipo:

$$p \cdot i, \quad 1 \leq i \leq p^{h-1}$$

e quindi sono in numero di p^{h-1} . Per $h = 1$ si ottiene $\varphi(p) = p - 1$. \square

Siamo quindi in grado di calcolare $\varphi(n)$ per ogni $n \in \mathbb{N}$ del quale si conosca la fattorizzazione. Ad esempio, $\varphi(72) = \varphi(2^3 \cdot 3^2) = \varphi(2^3)\varphi(3^2) = (2^3 - 2^2)(3^2 - 3) = 24$.

Abbiamo insistito nel dire che siamo in grado di calcolare $\varphi(n)$ per ogni intero n del quale si conosca la fattorizzazione: infatti è vero che il teorema fondamentale dell'aritmetica (§2.3) ci garantisce che ogni $n \in \mathbb{N}$ si fattorizza nel prodotto di un numero finito di fattori primi, ma per trovare questa fattorizzazione si devono trovare i primi che dividono n , e, per n grande, questo è un problema difficile: nel prossimo paragrafo ritorneremo su questo argomento.

Proviamo ora il preannunciato teorema di Eulero. La dimostrazione che daremo non è certo delle più eleganti: tuttavia, con le nozioni che abbiamo a disposizione fino a questo momento, dobbiamo accontentarci. Facciamo tuttavia notare che successivamente, quando avremo a disposizione alcuni risultati sui gruppi, si potrà dare di questo teorema una dimostrazione ben più rapida ed elegante. È istruttivo tuttavia presentare anche questa dimostrazione, perché dal confronto tra le due dimostrazioni si possano apprezzare i vantaggi dell'astrazione. Si invita pertanto lo studente a ricordarsi di questo fatto al momento opportuno.

2.8.4 TEOREMA DI EULERO. Se $(a, n) = 1$, allora

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dimostrazione. Procederemo per gradi: proveremo innanzitutto che se p è un numero primo che non divide a , allora

$$(2.8.2) \quad a^{\varphi(p^k)} \equiv 1 \pmod{p^k}.$$

Per induzione su k . Per $k = 1$

$$a^{\varphi(p)} = a^{p-1} \equiv 1 \pmod{p}$$

non è altro che il piccolo teorema di Fermat, che abbiamo già provato. Supponiamo che (2.8.2) sia vera per k e dimostriamola per $k + 1$. La (2.8.2) si può scrivere come

$$a^{\varphi(p^k)} \equiv 1 - hp^k$$

per qualche $h \in \mathbb{Z}$. Si noti anche che

$$\varphi(p^{k+1}) = p^{k+1} - p^k = p(p^k - p^{k-1}) = p \cdot \varphi(p^k).$$

Allora

$$\begin{aligned} a^{\varphi(p^{k+1})} &= a^{p \cdot \varphi(p^k)} = (1 + hp^k)^p \\ &= 1 + \binom{p}{1} hp^k + \binom{p}{2} \underbrace{(hp^k)^2}_{\equiv 0 \pmod{p^{k+1}}} + \dots \\ &\quad + \binom{p}{p-1} \underbrace{(hp^k)^{p-1}}_{\equiv 0 \pmod{p^{k+1}}} + \underbrace{(hp^k)^p}_{\equiv 0 \pmod{p^{k+1}}} \\ &\equiv 1 + \binom{p}{1} hp^k \equiv 1 \pmod{p^{k+1}} \end{aligned}$$

perché $\binom{p}{1} hp^k$ è un multiplo di p^{k+1} .

Dimostriamo ora il caso generale. Sia $(a, n) = 1$, e sia

$$n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}.$$

Per quanto provato, per ogni i risulta

$$(2.8.3) \quad a^{\varphi(p_i^{k_i})} \equiv 1 \pmod{p_i^{k_i}}, \quad i = 1, 2, \dots, s$$

Dato che abbiamo già mostrato la moltiplicatività della funzione φ , risulta

$$\varphi(p_i^{k_i}) \mid \varphi(n) \quad \forall i$$

per cui, elevando entrambi i membri di (2.8.3) alla potenza $\varphi(n)/\varphi(p_i^{k_i})$ si ottiene

$$a^{\varphi(n)} \equiv 1 \pmod{p_i^{k_i}}$$

per ogni $i = 1, \dots, s$. Ma allora

$$a^{\varphi(n)} \equiv 1 \pmod{p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}}$$

e quindi

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \quad \square$$

Chiudiamo questo paragrafo con un'importante applicazione della funzione di Eulero. Abbiamo visto che l'insieme \mathbb{Z}_n delle classi resto modulo n è stato dotato di due operazioni:

$$\bar{a} + \bar{b} \stackrel{\text{def}}{=} \overline{a + b}, \quad \bar{a} \cdot \bar{b} \stackrel{\text{def}}{=} \overline{a \cdot b}$$

rispetto alle quali \mathbb{Z}_n ha la struttura di anello commutativo con unità. Vogliamo ora studiare più a fondo questo anello, in particolare vogliano determinare gli elementi invertibili di \mathbb{Z}_n .

Faremo vedere quanto segue.

2.8.5 PROPOSIZIONE. In \mathbb{Z}_n gli unici elementi invertibili sono quelle classi \bar{a} tali che $(a, n) = 1$. Esse sono in numero di $\varphi(n)$. In particolare, in \mathbb{Z}_p con p primo, ogni classe non nulla è invertibile.

Dimostrazione. La determinazione delle classi \bar{a} invertibili in \mathbb{Z}_n equivale a risolvere la congruenza

$$ax \equiv 1 \pmod{n}.$$

Ora, tale congruenza ammette soluzione (ed unica!) se e solo se $(a, n) = 1$. Le classi invertibili sono pertanto le classi \bar{a} con $1 \leq a < n$ e $(a, n) = 1$; sono quindi in numero di $\varphi(n)$. Se in particolare $n = p$, allora ogni classe \bar{a} non nulla è tale che $(a, p) = 1$, quindi invertibile: le classi invertibili sono in questo caso $p - 1 = \varphi(p)$. \square

Ricordando che un campo è un anello commutativo con unità in cui ogni elemento non nullo è invertibile, si ha immediatamente il seguente risultato.

2.8.6 COROLLARIO. Se p è un numero primo, l'anello \mathbb{Z}_p è un campo.

L'insieme degli elementi invertibili di un anello commutativo con unità R si indica in genere con $U(R)$. Diamo qualche esempio di $U(\mathbb{Z}_n)$ per qualche n :

$$\begin{aligned}\mathbb{Z}_4 &= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}, & U(\mathbb{Z}_4) &= \{\bar{1}, \bar{3}\}; \\ \mathbb{Z}_6 &= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}, & U(\mathbb{Z}_6) &= \{\bar{1}, \bar{5}\}; \\ \mathbb{Z}_8 &= \{\bar{0}, \bar{1}, \dots, \bar{7}\}, & U(\mathbb{Z}_8) &= \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}.\end{aligned}$$

Si noti che $\varphi(4) = 2$, $\varphi(6) = \varphi(2)\varphi(3) = 1 \cdot 2$, $\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$.

ESERCIZI.

- Si provi che, per ogni intero positivo $n \geq 1$ vale la seguente relazione

$$n = \sum_{d|n} \varphi(d)$$

dove la somma si intende estesa a tutti i divisori positivi di n .

- Determinare le ultime due cifre della rappresentazione decimale dei numeri

$$9^{202} \quad \text{e} \quad 3^{950}.$$

- Si provi che il prodotto di elementi di $U(\mathbb{Z}_n)$ è ancora un elemento di $U(\mathbb{Z}_n)$ e che l'inverso di elementi di $U(\mathbb{Z}_n)$ è ancora un elemento di $U(\mathbb{Z}_n)$.
- Si provi che \mathbb{Z}_n è un campo se e solo se n è un numero primo.
- Si determini l'inverso della classe $\bar{8}$ in \mathbb{Z}_{15} .

6. Siano dati n punti P_1, P_2, \dots, P_n equidistanti su di una circonferenza (vertici di un n -gono regolare). Supponiamo di volere disegnare una stella ad n punte P_1, P_2, \dots, P_n , tracciando n segmenti senza mai staccare la penna dal foglio: per fare questo occorre collegare ogni P_i con uno degli $n - 3$ punti non adiacenti (altrimenti si ottiene un poligono e non una stella) saltando ogni volta lo stesso numero di punti. Ad esempio, nel caso $n = 5$ si parte da 1, si collega 1 con 3, 3 con 5, 5 con 2, 2 con 4 e 4 con 1, ottenendo la figura 2.7.

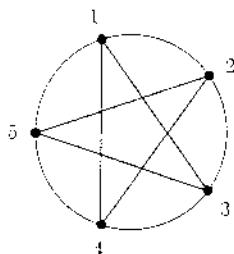


FIGURA 2.7

Si provi che per ogni n il numero di stelle distinte che si possono così ottenere è

$$\frac{\varphi(n) - 2}{2}$$

essendo $\varphi(n)$ la funzione di Eulero. Se ne deduca che è impossibile disegnare con queste regole stelle a 6 punte, mentre una stella a 7 punte si può disegnare in due modi diversi (cfr. [41] per ulteriori problemi di questo tipo).



ESERCIZI DI PROGRAMMAZIONE.

1. Si scriva un programma che calcoli $\varphi(n)$ per ogni intero n .
2. Si scriva un programma che calcoli gli elementi invertibili di \mathbb{Z}_n e dei loro inversi modulo n .
3. Stampare la tavola moltiplicativa $(\text{mod } n)$ di $U(\mathbb{Z}_n)$.



CONTROLLO.

1. Definire la funzione di Eulero di un intero positivo n . Quali sono le sue proprietà?
2. Dove si è utilizzata l'ipotesi $(a, n) = 1$ nel teorema di Eulero? È essenziale tale ipotesi?
3. Le classi invertibili di \mathbb{Z}_n sono in numero di ... Perché?

2.9. Applicazioni: numeri primi, fattorizzazioni, crittografia

In questo paragrafo vedremo alcune interessanti applicazioni degli argomenti finora trattati. Molti di questi saranno applicazioni delle congruenze, della funzione di Eulero e del teorema di Eulero.

2.9.1 TEST DI NON PRIMALITÀ. Abbiamo visto che se p è un numero primo allora *qualunque sia* a deve valere la

$$a^p \equiv a \pmod{p}.$$

Quindi vale il seguente risultato.

2.9.2 PROPOSIZIONE. *Se n è un numero tale che esista un $a \in \mathbb{Z}$ verificante la*

$$a^n \not\equiv a \pmod{n},$$

allora n non è primo.

Ad esempio, $n = 6$ è tale che $2^6 \not\equiv 2 \pmod{6}$, quindi 6 non è primo.

Si noti che questo test, pur assicurandoci che il numero non è primo, non ci permette di trovare una fattorizzazione di n . In genere si cerca un a piccolo, in modo da tenere sotto controllo i calcoli, ad esempio si prova con $a = 2$.

2.9.3 TEOREMA DI WILSON. *Se p è un numero primo, allora*

$$(p-1)! \equiv -1 \pmod{p}.$$

Dimostrazione. Per $p = 2$ e $p = 3$ il teorema è evidente. Supponiamo quindi $p > 3$. Se a è uno degli interi $1, 2, \dots, p-1$, si consideri la congruenza $ax \equiv 1 \pmod{p}$. Dato che $(a, p) = 1$, questa congruenza ammette una e una sola soluzione a' modulo p , $1 \leq a' < p$. Per quali valori di a risulta $a = a'$? Questo corrisponde a risolvere la $a^2 \equiv 1 \pmod{p}$, che equivale a dire che p divide $(a+1)(a-1)$ e quindi o p divide $a+1$ oppure divide $a-1$. Ne segue che $a-1 \equiv 0 \pmod{p}$ cioè $a = 1$, oppure $a+1 \equiv 0$, ossia $a = p-1$. Tralasciando questi due valori estremi, gli altri elementi $2, 3, \dots, p-2$ si possono raggruppare in $(p-3)/2$ coppie $\{a, a'\}$ con $a \neq a'$ tali che $aa' \equiv 1 \pmod{p}$. Moltiplicando tra loro le corrispondenti congruenze, si ottiene

$$2 \cdot 3 \cdots (p-2) = (p-2)! \equiv 1 \pmod{p}.$$

Ma allora, moltiplicando ambo i membri per $p-1 \equiv -1$, si ha che $(p-1)! \equiv -1 \pmod{p}$. \square

Vale anche il viceversa di questo teorema.

2.9.4 PROPOSIZIONE. *Se $(n-1)! \equiv -1 \pmod{n}$, allora n è un numero primo.*

Dimostrazione. Se n non fosse primo, avrebbe un divisore c , $1 < c < n$, che, in quanto divisore di n , dividerà anch'esso $(n-1)! + 1$. Ma, dato che $1 < c < n$, c comparirà tra i fattori di $(n-1)!$ e quindi $c \mid (n-1)!$. Dalle due relazioni ottenute si ottiene l'assurdo che c divide 1. \square

Il teorema di Wilson, assieme al suo inverso, ci offrono pertanto la seguente caratterizzazione dei numeri primi:

$$\boxed{n \text{ è primo} \iff (n-1)! + 1 \text{ è divisibile per } n} .$$

Si potrebbe essere tentati di utilizzare questo criterio come test per vedere se un numero è primo. Tuttavia tale criterio è inutilizzabile in pratica, dato che $(n-1)!$ cresce troppo rapidamente e non si conosce un algoritmo per un calcolo rapido della funzione fattoriale.

2.9.5 ALCUNI METODI DI FATTORIZZAZIONE. (i) Per fattorizzare un intero n si può procedere al modo seguente: si prova a vedere se è divisibile per $2, 3, 4, 5, \dots, \sqrt{n}$, ossia per tutti i numeri $\leq \sqrt{n}$: se non è divisibile per nessuno di questi, allora n è un numero primo (perché basta fermarsi a \sqrt{n} ?), altrimenti, detto n_1 un numero che divide n e posto $n = n_1 n_2$, si ripete con n_1 e n_2 lo stesso procedimento e alla fine si arriverà alla fattorizzazione completa di n .

(ii) *Il metodo del crivello di Eratostene.* Tale metodo permette di trovare tutti i primi $\leq n$. Si tratta di un metodo più efficiente del precedente, basato sull'osservazione che se un intero $n > 1$ non è divisibile per nessun $primo \leq \sqrt{n}$, allora n è necessariamente primo (cfr. esercizio 2.9.1). Il metodo consiste nei punti seguenti: si scrivono tutti i numeri $\leq n$, a partire da 2, che viene sottolineato; poi si cancellano tutti i multipli di 2. Si sottolinea poi il primo numero non cancellato (ossia 3) e si cancellano tutti i multipli di 3, e così via, finché non ci siano numeri non cancellati $\leq \sqrt{n}$. Ebbene, tutti i numeri sottolineati, assieme a tutti quelli che non sono stati cancellati, forniscono la lista completa di tutti i numeri primi $\leq n$.

(iii) *Il metodo di fattorizzazione di Fermat.* Per fattorizzare un numero n in molti casi è più efficiente il seguente metodo dovuto a Fermat. Esso si basa sui seguenti punti:

- (a) Si può supporre senz'altro n dispari.
- (b) Nel caso in cui n sia dispari fattorizzare n equivale a determinare due interi x e y tali che

$$n = x^2 - y^2 .$$

Infatti, se $n = x^2 - y^2$, allora $n = (x+y)(x-y)$ è una fattorizzazione di n . Viceversa, se $n = ab$, allora, supposto $a \geq b \geq 1$, si può scrivere

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

dove $(a+b)/2$ e $(a-b)/2$ sono interi non negativi, perché, essendo n dispari, anche a e b saranno dispari, e quindi $a \pm b$ è pari.

- (c) Determinare x e y tali che $n = x^2 - y^2$ equivale a determinare x tali che $x^2 - n$ sia un quadrato ($= y^2$). Si determina innanzitutto il più piccolo intero positivo k tale che $k^2 \geq n$, dopodiché si calcolano successivamente le seguenti differenze:

$$k^2 - n, \quad (k+1)^2 - n, \quad (k+2)^2 - n, \dots$$

fino a che si trova un valore $t \geq \sqrt{n}$ tale che $t^2 - n$ sia un quadrato. Si noti che tale processo *termina*, perché sicuramente si ha

$$\left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2$$

che si ottiene quando il numero n è primo, e quindi ha una fattorizzazione banale

$$n = \left(\frac{n+1}{2} + \frac{n-1}{2}\right) \left(\frac{n+1}{2} - \frac{n-1}{2}\right) = n \cdot 1 .$$

2.9.6 ESEMPIO. Si fattorizzi il numero 194333 in fattori primi. In questo caso $k = 441$:

$(441)^2 - 194333 = 148$	non quadrato
$(442)^2 - 194333 = 1031$	non quadrato
$(443)^2 - 194333 = 1916$	non quadrato
$(444)^2 - 194333 = 2803$	non quadrato
$(445)^2 - 194333 = 3692$	non quadrato
$(446)^2 - 194333 = 4583$	non quadrato
$(447)^2 - 194333 = 5426 = (74)^2$	quadrato.

Quindi

$$194333 = (447 - 74)(447 + 74) = 373 \cdot 521$$

e tali fattori sono numeri primi (si verifichi). \square

2.9.7 I NUMERI DI FERMAT. Accenniamo qui ad una classe di numeri che vedremo ricomparire quando parleremo di costruzioni con riga e compasso. Vale la pena di definirli già da ora, tanto più che siamo in tema, essendo stati introdotti da Fermat, del quale abbiamo appena finito di studiare la fattorizzazione. Consideriamo i numeri della forma $2^k + 1$. Se si chiede ad un numero di questa forma di essere un primo, l'esponente k non può contenere nessun fattore dispari: se infatti contenesse un fattore dispari $d = 2h + 1$ si avrebbe

$$\begin{aligned} 2^k + 1 &= 2^{dt} + 1 = (2^t)^d + 1 \\ &= (2^t + 1)((2^t)^{2h} - (2^t)^{2h-1} + \cdots + (2^t)^2 - 2^t + 1) \end{aligned}$$

ossia il numero avrebbe una fattorizzazione propria. Quindi, se vogliamo che un numero della forma $2^k + 1$ sia primo, l'esponente k deve avere la forma 2^n . Ebbene, si dà la seguente definizione.

2.9.8 DEFINIZIONE. Un numero di Fermat è un intero della forma

$$N_n = 2^{2^n} + 1. \quad \square$$

Spesso i numeri di Fermat vengono indicati con F_n , F iniziale del loro inventore. Purtroppo noi abbiamo già utilizzato questa lettera per indicare i numeri di Fibonacci: dovremo quindi ripiegare su un'altra lettera. I numeri di Fermat corrispondenti ai primi valori di n sono

$$N_0 = 3, \quad N_1 = 5, \quad N_2 = 17, \quad N_3 = 257, \quad N_4 = 65537.$$

Non è difficile verificare che tutti questi cinque numeri sono numeri primi. Era convinzione di Fermat che *tutti* i numeri della forma $2^{2^n} + 1$ fossero primi. La sua congettura fu confutata da Eulero, che provò che il successivo numero di Fermat, N_5 , non è primo, esibendo la fattorizzazione

$$N_5 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$$

Il problema della ricerca dei numeri di Fermat che siano primi è tuttora aperto. Il più grande numero di Fermat primo conosciuto è N_4 . Il più grande numero di Fermat non primo conosciuto è N_{23471} . Si conoscono le fattorizzazioni di N_5 , N_6 , N_7 , N_8 , N_9 e N_{11} . Si sa che N_{10} non è primo, ma non si conosce la fattorizzazione completa. Rimane un problema aperto se i numeri primi di Fermat sono in numero finito o infinito, e così se sono finiti o infiniti i numeri di Fermat composti. I numeri di Fermat primi interverranno, come abbiamo accennato all'inizio, nella soluzione del problema della costruzione (con riga e compasso) di poligoni regolari.

2.9.9 CRITTOLOGIA. Un'importante applicazione del teorema di Eulero si ha nel campo della crittologia. La crittologia è la scienza dei messaggi segreti *sicuri*, tali cioè che possano essere decifrati solo da destinatari selezionati: è chiara a tutti infatti la necessità della segretezza nell'invio di certi messaggi (in campo

bellico, finanziario, di spionaggio, ecc.). Giulio Cesare aveva già utilizzato un sistema di codice segreto traslando di tre lettere ogni lettera di un messaggio ($A \rightarrow D$, $B \rightarrow E$, ecc.). È chiaro che un tale messaggio in codice può essere facilmente decifrato anche da un estraneo, dall'esame della distribuzione delle lettere, la loro frequenza, le doppie, le lettere finali, ecc. Indipendentemente dalle tecniche usate per crearlo, un messaggio in codice deve essere tale da non potere essere decifrato da estranei e al tempo stesso deve essere rapidamente decifrato dai veri destinatari. La scrittura di codici segreti prende il nome di *crittografia*. Un grande progresso si è avuto con l'avvento (1976) del *sistema di crittografia con chiave pubblica*, chiamato comunemente *sistema RSA*, dai nomi dei suoi inventori Rivest, Shamir e Adleman. Lo illustreremo qui di seguito brevemente.

Stabilendo una corrispondenza biunivoca che assegna ad ogni lettera dell'alfabeto e ad ogni segno di interpunkzione un numero a tre cifre, un messaggio M può considerarsi un numero intero positivo.

Se ad esempio (come nell'*American Standard Code for Information Interchange*) alle lettere da a a z corrispondono nell'ordine i numeri da 065 a 090, allora ad esempio il messaggio *algebra* verrà letto come l'intero

065076071069066082065 .

Ogni utente U del sistema consegna una coppia di interi positivi, (n_U, e_U) , da inserire accanto al suo nome in un elenco pubblico. Il primo intero n_U deve essere il prodotto di due numeri primi, p_U, q_U che devono essere grandi e tenuti segreti (conosciuti cioè solamente dall'utente U), il secondo numero deve essere scelto da U in modo tale che $(e_U, p_U - 1) = 1$ e $(e_U, q_U - 1) = 1$. Sottolineiamo quindi che la coppia (n_U, e_U) è di dominio pubblico, ossia un qualunque utente che lo desideri può consultarla, mentre non è di dominio pubblico la fattorizzazione di n_U , nota solamente a U .

Supponiamo che l'utente A debba mandare un messaggio M all'utente B . Consultando l'elenco ufficiale, l'utente A controlla innanzitutto la coppia di numeri relativa all'utente B , cioè la coppia (n_B, e_B) . Se il messaggio M da inviare è maggiore del numero n_B , allora A spezzerà M in vari blocchi che risultino minori di n_B , che verranno inviati separatamente. Inoltre, aggiungendo, se necessario, una lettera finale al messaggio M , si può supporre $(M, n_B) = 1$. Quindi, senza perdita di generalità si può supporre che il messaggio M soddisfi alle seguenti due condizioni:

$$\boxed{M < n_B, \quad (M, n_B) = 1} .$$

Per codificare il messaggio M da inviare a B , l'utente A procede ora al modo seguente: eleva M alla potenza e_B e poi la riduce modulo n_B . Il messaggio M'

che viene ricevuto da B è quindi M' dove

$$M' \equiv M^{e_B} \pmod{n_B}.$$

Per decodificare il messaggio M' e scoprire il messaggio originario M , B determina innanzitutto d_B .

$$1 \leq d_B < \varphi(n_B) = (p_B - 1)(q_B - 1).$$

tale che d_B sia soluzione della

$$(2.9.1) \quad [e_B d_B \equiv 1 \pmod{\varphi(n_B)}]$$

dove φ è la funzione di Eulero. Si noti che questa congruenza ammette una e una sola soluzione modulo $\varphi(n_B)$, perché il coefficiente e_B è tale che

$$(e_B, p_B - 1) = 1, \quad (e_B, q_B - 1) = 1$$

per la scelta di e_B e quindi anche $(e_B, (p_B - 1)(q_B - 1)) = 1$.

 ATTENZIONE. Si noti che l'utente B è l'unico che può risolvere la congruenza (2.9.1), perché è l'unico a conoscere la funzione di Eulero di n_B , conoscendo i fattori primi p_B e q_B . □

Ebbene, la possibilità di risolvere la congruenza (2.9.1) (e quindi la conoscenza di d_B) è la *chiave segreta* che consente a B di conoscere M . Vale infatti la seguente proposizione.

2.9.10 PROPOSIZIONE. *Il messaggio originario M è tale che*

$$M \equiv M'^{d_B} \pmod{n_B}.$$

Dimostrazione. Risulta

$$M'^{d_B} \equiv (M^{e_B})^{d_B} \equiv M^{e_B \cdot d_B} \pmod{n_B};$$

ora, $e_B d_B \equiv 1 \pmod{\varphi(n_B)}$ $\implies e_B d_B - 1$ è un multiplo di $\varphi(n_B)$. Quindi,

$$M^{e_B d_B} = M^{1 + \varphi(n_B) \cdot k} = M \cdot (M^{\varphi(n_B)})^k.$$

Essendo $(M, n_B) = 1$, per il teorema di Eulero è $M^{\varphi(n_B)} \equiv 1 \pmod{n_B}$, da cui

$$M^{e_B d_B} \equiv M \pmod{n_B}.$$

Quindi

$$M \equiv M'^{d_B} \pmod{n_B}$$

e pertanto B riesce a leggere il messaggio M . □

Ripetiamo che B ha potuto decifrare il messaggio M perché era in possesso della fattorizzazione di n_B (che è equivalente alla conoscenza di $\varphi(n_B)$, cfr esercizio 2.9.4). La sicurezza di questo sistema risiede nel fatto che B non ha dovuto mandare la chiave ad A , ha semplicemente pubblicato una coppia di numeri. Ora, mentre, per inviare il messaggio la conoscenza di questa coppia è sufficiente, per decifrare il messaggio ciò non è sufficiente: occorre conoscere la fattorizzazione di n_B , che solo B conosce. Se un estraneo tentasse di decifrare il messaggio M' , dovrebbe trovare la fattorizzazione di n_B : ora per trovarla, nel caso ad esempio in cui n_B sia prodotto di due primi ciascuno di 60 cifre, anche utilizzando i più sofisticati algoritmi e i calcolatori più veloci, occorrerebbero molti mesi, se non addirittura anni, di calcoli. Se poi si scelgono i due primi con 100 o più cifre, la fattorizzazione di n è addirittura, in generale, impossibile. Diciamo *in generale*, perché nel 1994 è stato decodificato dal matematico Lenstra (con un'equipe di persone dei cinque continenti e con migliaia di calcolatori al lavoro) un messaggio relativo ad un modulo di 129 cifre (a seguito di una sfida fatta nell'agosto 1977, poco dopo la loro invenzione, dagli inventori del sistema a chiave pubblica Rivest, Shamir e Adleman che avevano offerto una ricompensa di 100 dollari a chi avesse decodificato una frase, che secondo loro avrebbe richiesto qualcosa come 10^{15} anni!). Questo episodio sta ad indicare che un sistema ritenuto sicuro oggi può non esserlo più domani.

Resta un problema: come fa ogni utente a trovare due numeri primi con, ad esempio, 100 cifre? Rispondiamo facendo solo una osservazione: per numeri n grandi il numero $\pi(n)$ dei numeri primi minori di n è dell'ordine di $n/\log n$. Se quindi n è un numero della grandezza voluta, la probabilità che esso sia primo è $1/\log n$. Con circa $\log n$ tentativi si potrà quindi ottenere un numero primo. Tuttavia esistono altri metodi, che non intendiamo sviluppare a questo livello.

Facciamo un esempio concreto. Supponiamo di dover mandare il messaggio $M = 4$ ad un utente B la cui coppia di numeri (che abbiamo trovato nell'elenco ufficiale) è

$$n_B = 221, \quad e_B = 7.$$

Il messaggio verrà inviato elevando M alla potenza e_B e riducendola modulo n_B . B riceverà quindi il messaggio $M' = 30$: infatti

$$M' = 4^7 \pmod{221} \equiv 30 \pmod{221}.$$

Per decodificarlo, B ha a disposizione la sua chiave segreta, che è il numero d_B soluzione della congruenza (2.9.1). Ovviamente tale numero l'utente B se l'è calcolato al momento in cui ha dato in dominio pubblico la coppia (n_B, e_B) , altrimenti corre il rischio di ricevere messaggi che non sa decifrare. Si è visto che il segreto per la determinazione di d_B è la conoscenza della fattorizzazione di n_B , che lui solo conosce. Ora, B aveva scelto $n_B = 221$ come prodotto dei due fattori primi 13 e 17 (speriamo che in questo caso semplice non sia solo B

conoscere la fattorizzazione di questo numero!), quindi

$$\varphi(221) = \varphi(13)\varphi(17) = 12 \cdot 16 = 192$$

da cui $d_B = 55$. Per decifrare il messaggio ricevuto, B deve elevare M' alla potenza d_B e ridurlo modulo 221. Facendo qualche riduzione che omettiamo, ma che è fattibile abbastanza rapidamente, B riesce a leggere il messaggio originario

$$30^{55} \pmod{221} \equiv \boxed{4} = M.$$

Missione compiuta!

Questo procedimento serve anche per risolvere il *problema dell'autenticazione di una firma*. Se Bruno riceve un messaggio da una persona che si firma Alberto, come può essere certo che sia stato proprio Alberto a spedirgliela? La garanzia si ottiene procedendo come segue:

Alberto scrive il suo messaggio M_1 , (in fondo al quale comparirà la sua firma F); per poter far sì che Bruno sia certo che il messaggio è autentico, in fondo al messaggio M_1 aggiunge il seguente messaggio M_2

$$M_2 \equiv F^{d_A} \pmod{n_A}$$

dove d_A è la sua chiave segreta, ossia quella che lui solo conosce, conoscendo la fattorizzazione della chiave pubblica n_A . Poi manda a Bruno l'intero messaggio $M = M_1 + M_2$ al solito modo, ossia elevando l'intero messaggio alla potenza e_B e riducendolo modulo n_B . Nel ricevere il messaggio, Bruno legge il messaggio (utilizzando la propria chiave segreta d_B). Dalla decifrazione del messaggio M_1 , Bruno capisce che il messaggio gli è stato inviato da Alberto. Dopo la lettura della firma F di Alberto, seguono dei caratteri illeggibili, che però contengono la prova della autenticità della firma. Infatti ora Bruno deve procedere al modo seguente: per decifrare questa parte M_2 del messaggio non deve utilizzare la *propria chiave segreta* d_B , perché il messaggio originario che deve leggere, ossia F , è già stato alterato, cioè elevato alla chiave segreta del *vero* Alberto. Utilizza allora la chiave pubblica e_A di Alberto. In tal modo gli viene fuori la firma F di Alberto, perché

$$M_2^{e_A} \equiv (F^{d_A})^{e_A} = F^{d_A e_A} \equiv F \pmod{n_A}.$$

Tale firma non può essere che quella autentica, perché solamente Alberto è a conoscenza della propria chiave segreta. Nel caso in cui non fosse comparsa la firma F di Alberto, il messaggio sarebbe stato un falso. In sostanza, per l'autenticazione di una firma è il *mittente* che utilizza la *propria chiave segreta*, anziché il *ricevente*.

La figura 2.8 mostra i vari stadi del processo di invio di un messaggio segreto e del controllo di autenticità della firma. Non è stato ovviamente visualizzata la traduzione in cifre del messaggio.

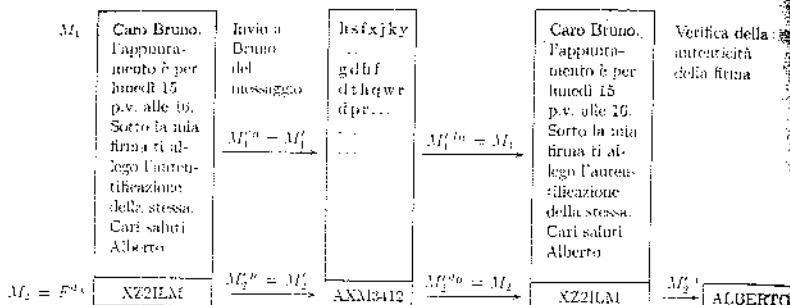


FIGURA 2.8

Chiudiamo con un esempio. Supponiamo che Alberto abbia la coppia $(n_A = 77, e_A = 13)$. Essendo $77 = 11 \cdot 7$, la chiave segreta di Alberto è (3 controlli) $d_A = 37$. Nell'inviare un messaggio a Bruno, Alberto ha autenticato la sua firma (che è $F = 70$) elevando 70 alla potenza d_A :

$$70^{37} \equiv 49 \pmod{77}.$$

Bruno verifica l'autenticità della firma elevando 49 alla potenza $e_A = 13$:

$$49^{13} \equiv 70 \pmod{77}$$

e in tal modo è sicuro che il messaggio proviene da Alberto.

ESERCIZI.

- Si provi che se un numero n non è primo, allora possiede un divisore primo $\leq \sqrt{n}$.
- Si fattorizzino in \mathbb{Z} i seguenti numeri in fattori primi:

 - 4084223, 2773, 3041, 1044541, 1643 .
 - 3. Si provi che il numero di Fermat $N_5 = 2^{32} + 1$ è divisibile per 641.
 - 4. Si provi che, se un intero positivo n è prodotto di due primi, la conoscenza di $\varphi(n)$ equivale a sapere fattorizzare n .
 - 5. Sia $n = 2279$. Supponiamo di sapere che $n = pq$, con p, q primi e che $\varphi(2279) = 2184$. Trovare la fattorizzazione di n . Si determini la fattorizzazione di n anche con il metodo di fattorizzazione di Fermat.
 - 6. Stesso esercizio del numero precedente con $n = 3053$ e $\varphi(3053) = 2940$.
 - 7. Si provi che vale la seguente relazione tra i numeri di Fermat:

$$N_{r+1} - 2 = N_0 N_1 \cdots N_{r-1} \quad \forall r .$$

Se ne deduca che N_{r-i} divide $N_r - 2$ per ogni $i = 2, \dots, n$. Si provi inoltre che i numeri di Fermat sono a due a due coprimi.

 ESERCIZI DI PROGRAMMAZIONE.

1. Fare un programma che, utilizzando il metodo del crivello di Eratostene, determini tutti i numeri primi minori o uguali ad un dato intero n .
2.
 - (a) Fare un programma che trovi una fattorizzazione per un intero n dispari calcolando tutti i primi minori o uguali a \sqrt{n} .
 - (b) Fare un programma che trovi una fattorizzazione di un intero dispari utilizzando il metodo di fattorizzazione di Fermat.
 - (c) Si confrontino i due metodi.
3. Fare un programma che decifri un codice a chiave pubblica, secondo le indicazioni date.

 CONTROLLO.

1. Fare gli esercizi proposti.

2.10. Numerazioni in basi diverse

Nei paragrafi precedenti abbiamo parlato di rappresentazione in base dieci di un numero: essa corrisponde alla ordinaria scrittura *decimale* di un numero è quella che si ottiene prendendo come *base* il numero 10. Questo significa che in questa scrittura ogni numero intero $a_n a_{n-1} a_{n-2} \cdots a_1 a_0$ deve intendersi come

$$a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$$

dove gli a_i sono interi tali che $0 \leq a_i < 10$. Ad esempio, il significato della scrittura 5342 è il seguente:

$$5342 = 5 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10 + 2.$$

Dividendo 5342 per 10 otteniamo

$$5342 = 10 \cdot 534 + 2$$

cioè 2 (ossia l'ultima cifra a destra) rappresenta il resto della divisione per 10 dell'intero numero. Proseguendo, dividiamo ora il quoziente ottenuto nuovamente per 10. Si ottiene

$$534 = 10 \cdot 53 + 4$$

la seconda cifra da destra rappresenta ancora il resto di una divisione, e quindi è univocamente individuata, ecc. Quindi, i coefficienti a_i della rappresentazione decimale di un numero sono univocamente individuati. Ora, il ruolo svolto dal numero 10 può essere svolto da un qualunque altro intero ≥ 2 . Ad esempio, scegliendo 9 come base, un numero

$$r_n r_{n-1} \cdots r_1 r_0$$

dovrà intendersi con il significato seguente:

$$r_n r_{n-1} \cdots r_1 r_0 = r_n 9^n + r_{n-1} 9^{n-1} + \cdots + r_1 9 + r_0$$

con gli r_i tali che $0 \leq r_i < 9$. In generale vale la seguente proposizione.

2.10.1 PROPOSIZIONE. *Si fissi un intero $b \geq 2$. Allora ogni intero $a \geq 0$ può essere rappresentato in base b , cioè a può essere scritto in modo unico come*

$$a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_2 b^2 + r_1 b + r_0$$

con gli r_i tali che $0 \leq r_i < b \forall i$.

Dimostrazione. Procederemo per induzione sull'intero positivo a . Per $a = 0$ non c'è nulla da dimostrare; supponiamo quindi di avere dimostrato il teorema per ogni intero minore di a , e dimostriamolo per a . Dividiamo a per la base b . Si ottiene

$$a = b \cdot q + r_0, \quad 0 \leq r_0 < b.$$

Ora, il quoziente q è minore di a , quindi, per l'ipotesi induttiva, q è rappresentabile in modo unico come

$$q = r_n b^{n-1} + r_{n-1} b^{n-2} + \cdots + r_2 b + r_1$$

con gli r_i univocamente individuati e tali che $0 \leq r_i < b \forall i$. Ma allora

$$\begin{aligned} a &= bq + r_0 = b(r_n b^{n-1} + r_{n-1} b^{n-2} + \cdots + r_2 b + r_1) + r_0 \\ &= r_n b^n + r_{n-1} b^{n-1} + \cdots + r_2 b^2 + r_1 b + r_0. \end{aligned}$$

Tale espressione è unica perché il quoziente q e il resto r_0 della prima divisione sono univocamente individuati, e la scrittura di q è unica per l'ipotesi induttiva. \square

Ogni numero strettamente inferiore alla base b è rappresentato da un unico "simbolo" o "cifra". Per rappresentare un numero in base b occorrono b simboli diversi. Le basi più comunemente usate (oltre ovviamente alla base 10) sono $b = 2$, $b = 8$ e $b = 16$, utilizzate soprattutto nel campo dei calcolatori elettronici. Nel sistema a base 2 (o *sistema binario*) ogni cifra contiene un bit di informazione: il simbolo 0 è interpretato dal calcolatore come il comando *off* e il simbolo 1 come *on*.

Per passare ad esempio dalla base 10 alla base 2, basta dividere il numero dato per 2, e successivamente ogni quoziente che si ottiene ancora per due, fino ad arrivare ad un *quoziente nullo*. I resti così ottenuti, letti dal basso all'alto,

danno la rappresentazione in base 2 del numero dato. Supponiamo ad esempio di volere scrivere il numero 5342 in base 2:

$$\begin{array}{ll}
 5342 = 2 \cdot 2671 + 0 & r_0 = 0 \\
 2671 = 2 \cdot 1335 + 1 & r_1 = 1 \\
 1335 = 2 \cdot 667 + 1 & r_2 = 1 \\
 667 = 2 \cdot 333 + 1 & r_3 = 1 \\
 333 = 2 \cdot 166 + 1 & r_4 = 1 \\
 166 = 2 \cdot 83 + 0 & r_5 = 0 \\
 83 = 2 \cdot 41 + 1 & r_6 = 1 \\
 41 = 2 \cdot 20 + 1 & r_7 = 1 \\
 20 = 2 \cdot 10 + 0 & r_8 = 0 \\
 10 = 2 \cdot 5 + 0 & r_9 = 0 \\
 5 = 2 \cdot 2 + 1 & r_{10} = 1 \\
 2 = 2 \cdot 1 + 0 & r_{11} = 0 \\
 1 = 1 \cdot 0 + 1 & r_{12} = 1 .
 \end{array}$$

Ebbene, il numero che si scrive come 5342 in base 10; in base 2 si scrive

$$(5342)_{10} = (r_{12}r_{11}r_{10}r_9r_8r_7r_6r_5r_4r_3r_2r_1r_0)_2 = (1010011011110)_2 .$$

Per fare il viceversa, cioè per passare ad esempio da base 2 a base 10, basta svolgere le somme e le potenze: per esempio, per ripassare dal numero $(1010011011110)_2$ alla sua rappresentazione decimale, basta scrivere

$$\begin{aligned}
 (1010011011110)_2 &= 1 \cdot 2^{12} + 0 \cdot 2^{11} + 1 \cdot 2^{10} + 0 \cdot 2^9 + 0 \cdot 2^8 + 1 \cdot 2^7 \\
 &\quad + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 \\
 &= 2^{12} + 2^{10} + 2^7 + 2^6 + 2^4 + 2^3 + 2^2 + 2 = 5342
 \end{aligned}$$

utilizzando, nello sviluppo delle potenze di 2, le 10 cifre da 0 a 9.

La scrittura di un numero in base 2 richiede ovviamente più spazio che non quella ad esempio in base 10. Per ovviare a questo inconveniente si può considerare l'insieme (costituito da 16 elementi) di tutte le stringhe formate da 4 cifre appartenenti a $\{0, 1\}$. Ognuna di queste stringhe rappresenta un numero in base 2, e ne diamo qui di seguito la lista completa. Accanto a ciascuna viene data la sua rappresentazione in base 10:

$$\begin{array}{llll}
 0000 = 0 & 0001 = 1 & 0010 = 2 & 0011 = 3 \\
 0100 = 4 & 0101 = 5 & 0110 = 6 & 0111 = 7 \\
 1000 = 8 & 1001 = 9 & 1010 = 10 & 1011 = 11 \\
 1100 = 12 & 1101 = 13 & 1110 = 14 & 1111 = 15 .
 \end{array}$$

Ebbene, se poniamo $1010 = A$, $1011 = B$, $1100 = C$, $1101 = D$, $1110 = E$, $1111 = F$, abbiamo 16 simboli $0, \dots, 9, A, B, C, D, E, F$ che possiamo prendere come cifre di un *sistema esadecimale*. Il passaggio da un numero scritto in base 2 ad uno scritto in base 16 è molto semplice: basta suddividere il numero binario, a partire da destra, in gruppi di quattro cifre (quattro bits = mezzo byte dato che 1 byte corrisponde a 8 bits). Diamo un esempio:

$$\begin{aligned}
 & (\underbrace{100}_{8} \underbrace{1110}_{E} \underbrace{1101}_{D} \underbrace{0110}_{6} \underbrace{0001}_{1})_2 = (8ED61)_{16} \\
 & = 8 \cdot (16)^4 + 14 \cdot (16)^3 + 13 \cdot (16)^2 + 6 \cdot 16 + 1 \\
 & = (585057)_{10}.
 \end{aligned}$$

Se si vuole invece passare da un sistema binario ad un sistema a base 8 bastano radunare le cifre a tre a tre, partendo da destra.

Osserviamo che, qualunque sia la base b , la scrittura 10 rappresenta sempre il numero b , la scrittura 100 il numero b^2 , in generale la scrittura $\underbrace{1000\dots0}_n$ il numero b^n .

Le quattro operazioni fondamentali tra numeri si possono fare in qualunque base. Basta conoscere le tavole di addizione e moltiplicazione dei numeri ad una sola cifra e seguire le ordinarie regole dei riporti. Diamo qui di seguito un esempio esplicativo. Se quindi si lavora in base 3, si devono tenere presenti le seguenti tavole additive e moltiplicative:

$+$	0	1	2
0	0	1	2
1	1	2	10
2	2	10	11

\cdot	0	1	2
0	0	0	0
1	0	1	2
2	0	2	11

e per fare ad esempio $(212)_3 + (21)_3$ e $(212)_3 \cdot (21)_3$ basta procedere al modo seguente: $2 + 1 = 10$, quindi si scrive 0 e si riporta 1. Poi si fa $1 + 1 + 2 = 11$. Si scrive 1 e si riporta 1. Infine $1 + 2 = 10$. In definitiva

$$\begin{array}{r}
 \boxed{1} \quad \boxed{1} \\
 2 \quad 1 \quad 2 \quad + \\
 \hline
 1 \quad 0 \quad 1 \quad 0
 \end{array}$$

Nel caso della moltiplicazione, $(212)_3 \cdot (21)_3 = (12222)_3$ (si verifichi).

Ovviamente si possono trattare anche numeri razionali allo stesso modo: in tal caso la rappresentazione in base b è la seguente:

$$\begin{aligned} a_{n-1}a_{n-2}\dots a_1a_0.c_1c_2\dots c_m\dots \\ = a_nb^n + a_{n-1}b^{n-1} + a_{n-2}b^{n-2} + \dots \\ + a_1b + a_0 + c_1b^{-1} + c_2b^{-2} + \dots + c_mb^{-m} + \dots \end{aligned}$$

ESERCIZI.

1. Scrivere in base 3 il numero $(2345)_{10}$, in base 8 il numero $(234)_{10}$, in base 2 il numero $(456)_8$.
2. Si addizionino e si moltiplichino tra loro i seguenti due numeri in base 2:

$$10010111 \quad \text{e} \quad 11101$$

e i seguenti numeri in base 4:

$$(12323)_4 \quad \text{e} \quad (321)_4.$$

3. Si consideri una numerazione in base b dove $b = n^2 + 1$, $n \in \mathbb{N}$.
 (i) Scrivere in base b i numeri seguenti:

$$n^2 + 2, \quad n^2 - 2n, \quad (n^2 + 2)^2, \quad n^4.$$

- (ii) Se $\alpha = n(n^2 + 2)$, si calcoli α^2 .

ESERCIZI DI PROGRAMMAZIONE.

1. Fare un programma che faccia passare dalla scrittura decimale alla scrittura binaria (base 2) un intero n e viceversa.
2. Fare un programma che trasformi un intero da una base ad un'altra per varie basi.
3. Fare un programma che trasformi un numero razionale da una base ad un'altra.
4. Fare un programma che addizioni e moltipichi fra loro due numeri scritti in base arbitraria.
5. Utilizzazione della scrittura in base 2 per il calcolo di potenze elevate, modulato un intero m . Riprendiamo, come esempio esplicativo, la congruenza già studiata nel §2.9

$$30^{55} \pmod{221}.$$

Ovviamente risulta, dividendo via via l'esponente,

$$\begin{aligned} (2.10.1) \quad 30^{55} &= (30^{27})^2 \cdot 30 = ((30^{13})^2 \cdot 30)^2 \cdot 30 = \dots \\ &= \left(\left(\left((30^2 \cdot 30)^2 \cdot 30 \right)^2 \cdot 30 \right)^2 \cdot 30 \right)^2 \cdot 30. \end{aligned}$$

Nel fare le singole operazioni si riduce modulo $m = 221$. Scriviamo ora in base 2:

$$(2.10.2) \quad 55 = (110111)_2 .$$

Si tratta di un numero a 6 cifre. Scriviamo allora le cinque (= 6 - lettere E

$E E E E E$

e partendo da sinistra inseriamo tra di esse una M per ogni cifra 1 che incontriamo in (2.10.2) e per ogni 0 che incontriamo avanziamo semplicemente di un posto. Il risultato finale sarà

$$(2.10.3) \quad MEMEEMEMEM .$$

Diamo ora il seguente significato alle lettere M e E . M indichi la moltiplicazione per 30 (e sua riduzione modulo 221), E l'elevamento al quadrato (riduzione modulo 221). Applichiamo allora l'operatore (2.10.3) al numero 1 (partendo da sinistra), cioè valutiamo

$$(1)MEMEEMEMEM$$

Il risultato è esattamente l'ultimo membro delle uguaglianze (2.10.1). La scrittura binaria dell'esponente 55 ha quindi permesso il calcolo di 30^{55} . Tale algoritmo è ovviamente utilizzabile ogni volta che si debba calcolare una potenza del tipo $n^e \pmod{m}$.

Si implementi tale algoritmo al calcolatore.



CONTROLLO.

1. Cosa significa rappresentare un numero in una data base?
2. Si può rappresentare in base b un numero razionale? Come?

2.11. I numeri complessi

Chindiamo questo capitolo introducendo i numeri complessi, e le loro principali proprietà.

Nell'insieme $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ delle coppie ordinate di numeri reali, definiamo le seguenti due operazioni:

$$(a, b) + (c, d) \stackrel{\text{def}}{=} (a + c, b + d)$$

$$(a, b) \cdot (c, d) \stackrel{\text{def}}{=} (ac - bd, ad + bc)$$

Tale insieme è un campo: la coppia $(0, 0)$ è l'elemento neutro rispetto all'addizione, $(1, 0)$ è l'elemento neutro rispetto alla moltiplicazione, e la coppia

$$\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$$

è l'inverso della coppia (a, b) . L'insieme delle coppie $(a, 0)$, $a \in \mathbb{R}$, è identificabile con l'insieme dei numeri reali, perché l'applicazione

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{C} \\ r &\longmapsto (r, 0) \end{aligned}$$

è iniettiva ed è tale che $f(r + r') = f(r) + f(r')$, e $f(r \cdot r') = f(r) \cdot f(r')$ per ogni $r, r' \in \mathbb{R}$.

2.11.1 DEFINIZIONE. Un *numero complesso* è una coppia ordinata di numeri reali, cioè un elemento di $\mathbb{C} = \mathbb{R} \times \mathbb{R}$. Rispetto alle operazioni sopra definite \mathbb{C} è un campo, che contiene il campo reale. \square

Se indichiamo la coppia $(0, 1)$ con il simbolo i , possiamo scrivere

$$\begin{aligned} (a, b) &= (a, 0) + (0, b) = (a, 0) + (0, 1)(b, 0) = a + ib, \\ i^2 &= (0, 1)(0, 1) = -1. \end{aligned}$$

L'elemento $i \in \mathbb{C}$ prende il nome di *unità immaginaria*. In questa notazione si ha

$$\begin{aligned} (a - ib) + (c + id) &= (a + c) + i(b + d) \\ (a + ib) \cdot (c + id) &= (ac - bd) + i(ad + bc). \end{aligned}$$

Il *conjugato* del numero complesso $z = x + iy$ è il numero complesso $\bar{z} = x - iy$. Dati comunque i numeri complessi z , z_1 e z_2 , si hanno le seguenti uguaglianze:

1. $\overline{(z)} = z$;
2. $\overline{(z_1 + z_2)} = \bar{z}_1 + \bar{z}_2$;
3. $\overline{(z_1 z_2)} = \bar{z}_1 \bar{z}_2$;
4. $z = \bar{z} \iff z \in \mathbb{R}$;
5. $z\bar{z} = x^2 + y^2$ è un numero reale ≥ 0 ; se $z \neq 0$, $z\bar{z} > 0$.

Il numero reale $z\bar{z}$ si chiama *norma* del numero complesso z , e la sua radice quadrata $\sqrt{z\bar{z}} = \sqrt{x^2 + y^2}$ prende il nome di *modulo* di z ; si indica con $|z|$. Vengono le seguenti proprietà:

1. $|z_1 z_2| = |z_1| |z_2|$;
2. $|z_1 + z_2| \leq |z_1| + |z_2|$.

Quest'ultima diseguaglianza si chiama *diseguaglianza triangolare*. Infatti indicando il numero complesso $z = x + iy$ con il punto $P(x, y)$ del piano euclideo allora il modulo di z rappresenta la lunghezza del segmento OP e la diseguaglianza triangolare dice semplicemente (ricordando la regola del parallelogramma) che la lunghezza di un lato di un triangolo è minore o uguale alla somma delle lunghezze degli altri due lati: si veda la figura 2.9.

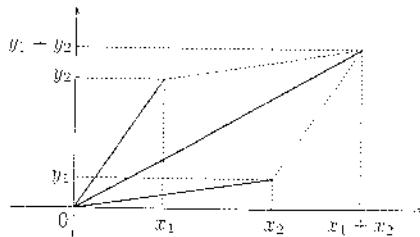


FIGURA 2.9

Se pensiamo alla rappresentazione geometrica dei numeri complessi (figura 2.10) osserviamo che, detto ϑ l'angolo che la semiretta OP forma con il semiasse positivo delle ascisse, e posto $r = \sqrt{x^2 + y^2}$, si hanno le seguenti relazioni:

$$x = r \cos \vartheta, \quad y = r \sin \vartheta.$$

Possiamo quindi rappresentare il numero complesso $x + iy$ nella seguente *forma trigonometrica*:

$$x + iy = r(\cos \vartheta + i \sin \vartheta).$$

L'angolo ϑ si dice l'*argomento* del numero complesso z .

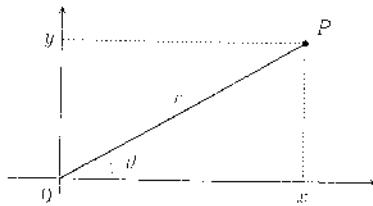


FIGURA 2.10

Se z e z' hanno le rappresentazioni $z = r(\cos \vartheta + i \sin \vartheta)$ e $z' = r'(\cos \vartheta' + i \sin \vartheta')$, allora, come è facile verificare, risulta

$$z \cdot z' = rr'(\cos(\vartheta + \vartheta') + i \sin(\vartheta + \vartheta'))$$

che ci dice che il prodotto di due numeri complessi scritti sotto forma trigonometrica è il numero complesso che ha come argomento la somma degli argomenti e come modulo il prodotto dei moduli. La forma trigonometrica di un numero complesso si presta quindi molto bene al calcolo delle potenze, perché per ogni intero $n \geq 0$ si ha la seguente formula di de Moivre:

$$(2.11.1) \quad z^n = r^n(\cos n\vartheta + i \sin n\vartheta).$$

Risulta

$$[r(\cos \vartheta + i \sin \vartheta)]^{-1} = r^{-1}(\cos(-\vartheta) + i \sin(-\vartheta))$$

quindi la (2.11.1) si estende anche ad esponenti interi arbitrari.

Siano ora z ed α due numeri complessi. Si dice che z è una radice n -esima di α (n intero positivo) se $z^n = \alpha$. Se $\alpha = r(\cos \vartheta + i \sin \vartheta)$ e $z = \rho(\cos \varphi + i \sin \varphi)$, allora dalla $z^n = \alpha$ si deduce che $r = \rho^n$, cioè $\rho = \sqrt[n]{r}$, ossia ρ è l'unico numero reale positivo la cui potenza n -esima è r . Inoltre, sempre dalla $z^n = \alpha$, si deduce $\cos n\varphi = \cos \vartheta$ e $\sin n\varphi = \sin \vartheta$, da cui $n\varphi = \vartheta + 2k\pi$ cioè

$$\varphi = \frac{\vartheta + 2k\pi}{n},$$

per qualche $k \in \mathbb{Z}$, ottenendo in definitiva il numero complesso

$$z_k = r^{1/n} \left(\cos \frac{\vartheta + 2k\pi}{n} + i \sin \frac{\vartheta + 2k\pi}{n} \right).$$

Per $k = 0, 1, \dots, n-1$ gli z_k sono tutti distinti e rappresentano n radici n -esime distinte di α . Per $\alpha = 0$ esiste una sola radice n -esima, che è lo zero. Tutte le radice n -esime di α si trovano sui vertici di un poligono regolare di n lati inscritto in un cerchio di lato $r^{1/n}$.

Se $\alpha = 1$, si hanno le radici n -esime dell'unità, $\zeta_{n,k}$, che si trovano sui vertici dell' n -gono regolare inscritto su di una circonferenza di lato 1. Esse sono

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

Se si ponе $\zeta_{n,1} = \zeta = \cos(2\pi/n) + i \sin(2\pi/n)$, ogni radice n -esima dell'unità, $\zeta_{n,k}$, ugualia, in virtù della formula di de Moivre, la potenza k -esima di ζ , ossia

$$\zeta_{n,k} = \zeta^k, \quad k = 0, 1, \dots, n-1.$$

È facile vedere che, indicata con z_0 una radice della

$$(2.11.2) \quad z^n = \alpha,$$

tutte le altre si ottengono da z_0 moltiplicandola per le n radici n -esime dell'unità, ossia tutte le soluzioni di (2.11.2) sono le seguenti

$$z_0, z_0\zeta, z_0\zeta^2, \dots, z_0\zeta^{n-1}.$$



ESERCIZI.

1. Calcolare il modulo dei seguenti numeri complessi:
 - (a) $1 + i + i^2 + i^3 + i^4 + i^5$;
 - (b) $(1 + i)^2$;
 - (c) $(1 + i)(1 - i)$.
2. Calcolare
 - (a) le radici quarte di i ;
 - (b) le radici terze dell'unità;
 - (c) le radici seste primitive dell'unità.

CAPITOLO 3

I polinomi

La mente non ha bisogno, come un vaso, di essere riempita, ma piuttosto, come legna, di una scintilla che l'accenda vi infonda l'impulso della ricerca e un amore ardente per la verità.

Plutarco, L'arte di ascoltare.

Questo capitolo è dedicato allo studio dei polinomi in una indeterminata a coefficienti in un campo. La scelta di questo argomento immediatamente dopo avere studiato gli interi è dovuta al fatto che la struttura dell'insieme dei polinomi a coefficienti in un campo è simile a quella degli interi, nel senso che gran parte delle definizioni e proprietà che abbiamo dato nel caso degli interi si possono dare in modo pressoché invariato nel caso dei polinomi. Vengono studiate le equazioni di terzo e quarto grado ed i polinomi ciclotomici. Nell'ultimo paragrafo vengono presentati i polinomi simmetrici in n variabili e viene dimostrato il teorema fondamentale per tali polinomi.

3.1. Funzioni polinomiali e polinomi

Abbiamo già visto vari esempi di *campi* ossia anelli comunitativi con unità in cui ogni elemento non nullo è invertibile: il campo \mathbb{Q} dei razionali, il campo \mathbb{R} dei reali o \mathbb{C} dei complessi o anche campi finiti come ad esempio \mathbb{Z}_p , con p primo. In quel che segue indicheremo con \mathbb{K} un qualunque campo. I teoremi che dimostreremo valgono quindi per un *qualunque* campo (salvo i casi in cui si parlerà esplicitamente di campi specifici come i razionali o i reali o i complessi). Se lo studente ha difficoltà a lavorare con elementi di un campo qualunque, senza avere di fronte un campo ben preciso, può tranquillamente pensare gli elementi come appartenenti ad un campo che conosce bene (ad esempio i razionali o i reali) salvo, ripetiamo, quando si parlerà di campi specifici.

3.1.1 DEFINIZIONE. Una *funzione polinomiale* o *funzione razionale intera* campo \mathbb{K} è una funzione p di \mathbb{K} in sé tale che esistano un intero $n \geq 0$ elementi $a_i \in \mathbb{K}$ in modo che

$$p : x \in \mathbb{K} \longmapsto \sum_{i=0}^n a_i x^i \in \mathbb{K} \quad \forall x \in \mathbb{K}. \quad \square$$

Una funzione polinomiale p è pertanto una *funzione* da \mathbb{K} in sé di natura particolare e verrà indicata al modo seguente:

$$p(x) = \sum_{i=0}^n a_i x^i.$$

Sia \mathcal{F} l'insieme di tutte le funzioni polinomiali di \mathbb{K} in sé. Trattandosi di *funzioni da un campo \mathbb{K} in sé*, possiamo definire addizione e moltiplicazione di tali funzioni al modo solito, cioè utilizzando nella definizione l'addizione e la moltiplicazione del campo \mathbb{K} :

$$\boxed{(p+q)(x) \stackrel{\text{def}}{=} p(x) + q(x), \quad (p \cdot q)(x) \stackrel{\text{def}}{=} p(x) \cdot q(x) \quad \forall x \in \mathbb{K}.}$$

Quindi, se $p(x)$ e $q(x)$ sono le funzioni polinomiali

$$p(x) = \sum_{i=0}^n a_i x^i, \quad q(x) = \sum_{j=0}^m b_j x^j, \quad m \geq n$$

allora risulterà, tenendo presenti le proprietà soddisfatte da addizione e moltiplicazione di elementi di un campo,

$$(p+q)(x) = p(x) + q(x) = \sum_{h=0}^{n+m} (a_h + b_h) x^h$$

c

$$(p \cdot q)(x) = p(x)q(x) = \sum_{h=0}^{n+m} \left(\sum_{i+j=h} a_i b_j \right) x^h.$$

L'insieme \mathcal{F} costituito dalle funzioni polinomiali di \mathbb{K} in sé, dotato delle due operazioni, $+$ e \cdot , ora introdotte, è, come è facile vedere, un *anello commutativo con unità*. L'elemento neutro rispetto alla prima operazione, $+$, ossia lo zero, è la funzione polinomiale che associa ad ogni $x \in \mathbb{K}$ l'elemento 0 di \mathbb{K} , la funzione polinomiale *opposta* della funzione polinomiale p è la funzione polinomiale, che indicheremo con $-p$, tale che $(-p)(x) = -p(x)$ per ogni $x \in \mathbb{K}$. Infine, l'*unità* di \mathcal{F} è quella funzione polinomiale che associa l'elemento 1 (unità del campo \mathbb{K}) ad ogni $x \in \mathbb{K}$, ossia la funzione costante uguale ad 1.

3.1.2 DEFINIZIONE. Un *polinomio* $p(x)$ a coefficienti in un campo \mathbb{K} è una espressione *formale* del tipo

$$(3.1.1) \quad p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad a_i \in \mathbb{K}$$

dove x è una indeterminata. \square

Dalla definizione segue che due polinomi $p(x) = \sum_{i=0}^n a_i x^i$ e $q(x) = \sum_{i=0}^m b_i x^i$, $a_i, b_j \in \mathbb{K}$, sono uguali se e solo se $a_i = b_j$, $\forall i$ (in particolare, se $m > n$, allora $b_{n+1} = b_{n+2} = \cdots = b_m = 0$).

L'insieme di tutti i polinomi a coefficienti in \mathbb{K} si indica con $\mathbb{K}[x]$.

ATTENZIONE. A questo punto è essenziale fare una precisazione. Spesso, e lo abbiamo fatto anche noi, le funzioni polinomiali e i polinomi vengono indicati allo stesso modo, cioè con $p(x) = \sum_{i=0}^n a_i x^i$, ma si tratta di due concetti diversi, come appare ad esempio dal confronto tra la nozione di uguaglianza tra funzioni polinomiali e uguaglianza tra polinomi. Due funzioni polinomiali, per loro natura, sono uguali quando assumono gli stessi valori in corrispondenza di ogni $x \in \mathbb{K}$, cioè se si "comportano" allo stesso modo. Due polinomi invece sono uguali se e solo se hanno la stessa scrittura formale, ed in effetti un polinomio altro non è che una espressione formale del tipo (3.1.1). Vediamo che tipo di legame esiste tra funzioni polinomiali e polinomi. È ovvio che un polinomio $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, $a_i \in \mathbb{K}$, definisce un funzione polinomiale, quella che associa ad ogni $c \in \mathbb{K}$ l'elemento (appartenente a \mathbb{K}) $p(c) = a_0 + a_1c + a_2c^2 + \cdots + a_nc^n$. Resta quindi definita la seguente applicazione Ψ :

$$\begin{aligned} \Psi : \mathbb{K}[x] &\longrightarrow \mathcal{F} \\ \sum_{i=0}^n a_i x^i &\longmapsto f : \mathbb{K} \longrightarrow \mathbb{K} \\ x &\longmapsto \sum_{i=0}^n a_i x^i \end{aligned}$$

Tale applicazione è senz'altro suriettiva, ma può non essere iniettiva, cioè può succedere che due polinomi diversi, cioè due espressioni polinomiali diverse diano luogo alla stessa funzione polinomiale. Ad esempio, se $\mathbb{K} = \mathbb{Z}_3$, le due espressioni polinomiali diverse x^2 , e $x^3 + x^2 - x$ danno luogo alla stessa funzione polinomiale da \mathbb{Z}_3 in \mathbb{Z}_3 . Quando il campo \mathbb{K} è finito, la Ψ non è mai iniettiva: infatti $\mathbb{K}[x]$ è un insieme infinito, perché infinite sono le espressioni polinomiali che si possono scrivere (anche se i coefficienti variano in un insieme finito, l'intero n può assumere valori arbitrari in \mathbb{N}). Invece, se \mathbb{K} è finito, \mathcal{F} è finito: infatti le possibili applicazioni tra due insiemi finiti A e B , se $|A| = s$ e $|B| = t$, sono in numero di t^s . Mostriremo fra breve che, nel caso in cui il campo \mathbb{K} sia infinito, la Ψ è biunivoca, quindi si possono confondere le funzioni polinomiali con i polinomi. \square

D'ora in poi saremo interessati allo studio dei polinomi, anche se sarà utile pensarli come funzioni polinomiali. Era però opportuno capire la differenza tra i due concetti.

Siano $p(x) = \sum_{i=0}^n a_i x^i$ e $q(x) = \sum_{j=0}^m b_j x^j$ due elementi di $\mathbb{K}[x]$. Possiamo utilizzare per $\mathbb{K}[x]$ le stesse definizioni di addizione e moltiplicazione di \mathcal{F} (se $m \geq n$)

$$p(x) + q(x) \stackrel{\text{def}}{=} \sum_{h=0}^m (a_h + b_h) x^h$$

e

$$p(x)q(x) \stackrel{\text{def}}{=} \sum_{h=0}^{n+m} \left(\sum_{i+j=h} a_i b_j \right) x^h.$$

È facile vederc che, rispetto a queste operazioni, $\mathbb{K}[x]$ diventa un anello commutativo con unità. Si noti però la differenza rispetto ad \mathcal{F} : qui il polinomio nullo non viene definito come quello che associa ad ogni elemento di \mathbb{K} lo zero di \mathbb{K} , ma come il polinomio con tutti i coefficienti nulli; così l'opposto di polinomio $p(x) = \sum_{i=0}^n a_i x^i$ è il polinomio che ha come coefficienti gli opposti dei coefficienti a_i , ecc.

3.1.3 DEFINIZIONE. Si definisce *grado* del polinomio $p(x) = \sum_{i=0}^n a_i x^i$ l'intero n , se $a_n \neq 0$. Si indica con $\deg p(x)$ oppure con $\partial p(x)$. Il coefficiente a_n prende il nome di *coefficiente direttivo* di $p(x)$. \square

Si noti che il grado di un polinomio $p(x) = a_0$, cioè di una costante, è zero. Al polinomio nullo non si attribuisce in genere un grado (oppure, convenzionalmente, gli si attribuisce il grado $-\infty$).

Vale la seguente proposizione.

3.1.4 PROPOSIZIONE. *L'anello $\mathbb{K}[x]$ è un dominio di integrità.*

Dimostrazione. Basta provare che è privo di divisori dello zero. Siano $p(x) = \sum_{i=0}^n a_i x^i$ e $q(x) = \sum_{j=0}^m b_j x^j$ due polinomi non nulli (cioè che abbiano almeno un coefficiente non nullo). Supponiamo che $\partial p(x) = n$ e $\partial q(x) = m$; ciò significa che $a_n \neq 0$ e $b_m \neq 0$. Dalla definizione di polinomio prodotto $p(x)q(x)$ risulta che il coefficiente di x^{m+n} è $a_n b_m$, che è diverso da zero perché a_n e b_m sono diversi da zero e sono elementi di un campo, in cui non esistono divisori dello zero (perché?). Quindi $p(x)q(x)$ non può essere il polinomio nullo. \square

Notiamo esplicitamente le seguenti relazioni tra i gradi di due polinomi a coefficienti in un campo e i gradi della loro somma e del loro prodotto:

$$\partial(p(x) + q(x)) \leq \max(\partial p(x), \partial q(x)), \quad \partial(p(x)q(x)) = \partial p(x) + \partial q(x).$$

ella definizione di polinomio come nelle proprietà dei polinomi la indetermina x non interviene, nel senso che non importa assolutamente il valore che essa assumere. Visto quindi che ne possiamo fare a meno, vediamo di liberarci una volta per tutte della indeterminata x nella definizione di polinomio. Diamo quindi la seguente definizione di polinomio.

3.1.5 DEFINIZIONE. Un *polinomio a coefficienti in un campo K* è una successione infinita

$$(a_0, a_1, a_2, \dots, a_i, \dots)$$

di elementi di K soddisfacenti la condizione che tutti gli a_n da un certo punto in poi sono uguali a zero. \square

Nell'insieme di tutte queste successioni definiamo addizione e moltiplicazione di successioni al modo seguente:

$$(a_0, a_1, a_2, \dots, a_i, \dots) + (b_0, b_1, b_2, \dots, b_i, \dots)$$

$$\stackrel{\text{def}}{=} (a_0 + b_0, a_1 - b_1, \dots, a_i + b_i, \dots)$$

$$(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots)$$

$$\stackrel{\text{def}}{=} (a_0 b_0, a_0 b_1 + a_1 b_0, \dots, \underbrace{\sum_{i+j=k} a_i b_j}_{\text{posizione } (k+1)-\text{ma}}, \dots).$$

L'identificazione tra una successione così definita ed un polinomio è data dalla corrispondenza, ovviamente biunivoca:

$$(a_0, a_1, a_2, \dots, a_n, \underbrace{0, 0, 0, 0, 0, \dots}_{\text{d'ora in poi tutti } = 0}) \longleftrightarrow \sum_{i=0}^n a_i x^i.$$

In particolare si hanno le seguenti identificazioni:

$$(1, 0, 0, 0, 0, \dots) \equiv 1$$

$$(0, 1, 0, 0, 0, \dots) \equiv x$$

$$(0, 0, 1, 0, 0, \dots) \equiv x^2$$

...

$$(0, 0, 0, \dots, \underbrace{1}_{\text{posizione } i+1-\text{ma}}, \dots, 0, 0, \dots) \equiv x^i.$$

Si capisce ora il significato dell'indeterminata x e delle sue potenze: sono specie di segnaposto. È chiaro anche che la definizione di addizione è un'applicazione tra successioni corrisponde alle definizioni delle analoghe operazioni sui corrispondenti polinomi.

Per comodità di scrittura, tuttavia, ed anche di calcolo, continueremo a scrivere i polinomi nella vecchia forma.

ESERCIZI.

- Scrivere in termini di successioni i polinomi a coefficienti in \mathbb{Q}

$$x^7 - 2x^3 + x - 1, \quad x + x^2 - 3x^5$$

e si scriva anche il loro prodotto come successione.



ESERCIZI DI PROGRAMMAZIONE.

- Si scriva un programma che esegua addizione e moltiplicazione di polinomi.



CONTROLLO.

- La nozione di polinomio a coefficienti in un campo.
- Proprietà dell'anello $\mathbb{K}[x]$.

3.2. Divisione tra polinomi, MCD e fattorizzazione

Come avevamo preannunciato, molte delle definizioni e proprietà degli interi possono estendere ai polinomi.

3.2.1 PROPOSIZIONE (L'ALGORITMO DELLA DIVISIONE TRA POLINOMI). Siano $f(x), g(x) \in \mathbb{K}[x]$ due polinomi, con $g(x) \neq 0$. Allora esistono, e sono univocamente individuati, due polinomi $q(x)$ e $r(x)$ in $\mathbb{K}[x]$ tali che

$$f(x) = g(x) \cdot q(x) + r(x) \quad \partial r(x) < \partial g(x) \quad \text{oppure} \quad r(x) = 0.$$

Dimostrazione. Se $f(x) = 0$ o $\partial f(x) < \partial g(x)$ basta porre $q(x) = 0$ e $r(x) = f(x)$. Supponiamo quindi senz'altro $\partial g(x) \leq \partial f(x)$. Procederemo per induzione su $\partial f(x)$. Se $\partial f(x) = 0$ (e quindi anche $\partial g(x) = 0$), significa che $f(x) = a_0$, $g(x) = b_0$, $a_0, b_0 \in \mathbb{K}$, da cui

$$f(x) = a_0 = \underbrace{(a_0 \cdot b_0^{-1})}_{q(x)} b_0 + \underbrace{0}_{r(x)}.$$

Si osservi l'importanza che i coefficienti si trovino in un campo!

Supponiamo vero il teorema per polinomi di grado $< n$ e dimostriamolo quando $\partial f = n$. Allora $\partial f = n \geq \partial g = m$. Siano

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \quad a_n \neq 0$$

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m, \quad b_m \neq 0.$$

Il polinomio

$$\tilde{f}(x) = f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x)$$

appartiene a $\mathbb{K}[x]$ e ha grado minore di n . Per l'ipotesi induttiva esistono $\tilde{q}(x)$ e $\tilde{r}(x)$ tali che

$$\tilde{f}(x) = g(x)\tilde{q}(x) + \tilde{r}(x), \quad \partial\tilde{r}(x) < m \quad \text{oppure} \quad \tilde{r}(x) = 0.$$

Allora

$$\begin{aligned} f(x) &= \tilde{f}(x) + a_n b_m^{-1} x^{n-m} g(x) \\ &= g(x)\tilde{q}(x) + \tilde{r}(x) + a_n b_m^{-1} x^{n-m} g(x) \\ &= g(x) \underbrace{[\tilde{q}(x) + a_n b_m^{-1} x^{n-m}]}_{q(x)} + \underbrace{\tilde{r}(x)}_{r(x)}. \end{aligned}$$

Abbiamo così trovato i polinomi $q(x)$ e $r(x)$ richiesti. Per quanto concerne l'unicità, supponiamo che sia

$$\begin{aligned} f(x) &= g(x)q(x) + r(x) = g(x)q'(x) + r'(x) \\ \partial r(x) &< \partial g(x), \quad \partial r'(x) < \partial g(x). \end{aligned}$$

Allora

$$r(x) - r'(x) = g(x)(q'(x) - q(x)),$$

dove il primo membro o è il polinomio nullo, oppure ha grado minore di $\partial g(x)$; il secondo membro o è zero, oppure ha grado $\geq \partial g(x)$. Quindi l'uguaglianza si può avere solo se $r(x) = r'(x)$ e $q(x) = q'(x)$. \square

3.2.2 DEFINIZIONE. Si dice che un polinomio $g(x) \in \mathbb{K}[x]$ divide un polinomio $f(x) \in \mathbb{K}[x]$, e si scrive $g(x) | f(x)$, se esiste un $q(x) \in \mathbb{K}[x]$ tale che

$$f(x) = g(x) \cdot q(x). \quad \square$$

3.2.3 DEFINIZIONE. Un elemento $f(x)$ in $\mathbb{K}[x]$ si dice invertibile se esiste un polinomio $g(x)$ in $\mathbb{K}[x]$ tale che $f(x)g(x) = 1$. \square

È ovvio, date le relazioni tra i gradi di un prodotto e quelli dei singoli fattori, che gli unici elementi invertibili di $\mathbb{K}[x]$ sono le costanti non nulle (cioè gli elementi non nulli del campo \mathbb{K}).

3.2.4 DEFINIZIONE. Siano $f(x)$ e $g(x)$ due polinomi appartenenti a $\mathbb{K}[x]$ entrambi nulli. Si definisce *massimo comun divisore* tra $f(x)$ e $g(x)$, o indica con $\text{MCD}(f(x), g(x))$ o semplicemente con $(f(x), g(x))$, un polinomio $d(x) \in \mathbb{K}[x]$ tale che

- (a) $d(x) \mid f(x)$, $d(x) \mid g(x)$,
- (b) se $d'(x) \mid f(x)$, $d'(x) \mid g(x)$, allora $d'(x) \mid d(x)$. \square

Lo stesso procedimento che ci garantiva l'esistenza del MCD tra interi, ossia l'algoritmo euclideo delle divisioni successive, vale per i polinomi, e ci garantisce quindi l'esistenza di un massimo comun divisore di due polinomi non entrambi nulli.

3.2.5 L'ALGORITMO EUCLIDEO DELLE DIVISIONI SUCCESSIVE PER LA RICERCA DEL MCD. Siano $f(x)$ e $g(x)$ polinomi di $\mathbb{K}[x]$, non entrambi nulli. Svolgano le seguenti divisioni:

$$f(x) = g(x)q_0(x) + r_0(x) \quad \partial r_0(x) < \partial g(x)$$

$$g(x) = r_0(x)q_1(x) + r_1(x) \quad \partial r_1(x) < \partial r_0(x)$$

...

$$r_i(x) = r_{i+1}(x)q_{i+2}(x) + r_{i+2}(x) \quad \partial r_{i+2}(x) < \partial r_{i+1}(x)$$

...

$$r_{n-2}(x) = r_{n-1}(x)q_n(x) + r_n(x) \quad \partial r_n(x) < \partial r_{n-1}(x)$$

$$r_{n-1}(x) = r_n(x)q_{n+1}(x) + 0.$$

Ebbene, con una dimostrazione identica a quella svolta nel caso degli interi, l'ultimo resto non nullo rappresenta il MCD tra $f(x)$ e $g(x)$.

3.2.6 DEFINIZIONE. Due elementi $f(x)$ e $g(x) \in \mathbb{K}[x]$ si dicono *associati* se esiste un elemento invertibile a di $\mathbb{K}[x]$ tale che $f(x) = g(x) \cdot a$. \square

La relazione di "essere associati" è una relazione d'equivalenza e in ogni classe di polinomi tra loro associati se ne può sempre scegliere uno *monico*, tale cioè che il suo coefficiente direttivo sia uguale ad 1. Per esempio, $4x^2 + 12x - 4$ in $\mathbb{Q}[x]$ è associato al polinomio monico $x^2 + 3x - 1$.

Siano $d(x)$ e $\tilde{d}(x)$ due elementi che rispondano entrambi alla definizione di massimo comun divisore tra $f(x)$ e $g(x)$. È facile vedere che essi sono associati. Allora si può (per convenzione) dire che il massimo comun divisore tra $f(x)$ e $g(x)$ è l'unico massimo comun divisore *monico*.

Vale inoltre anche per i polinomi la cosiddetta identità di Bézout. Se $f(x)$ e $g(x)$ stanno in $\mathbb{K}[x]$, detto $d(x)$ il loro massimo comun divisore, esistono $h(x)$ e $k(x)$ in $\mathbb{K}[x]$ tali che

$$d(x) = h(x)f(x) + k(x)g(x).$$

Si dimostra allo stesso modo dell'analogo risultato per gli interi.

3.2.7 DEFINIZIONE. Due polinomi $f(x)$ e $g(x)$ si dicono *coprimi* se

$$\text{MCD}(f(x), g(x)) = 1. \quad \square$$

3.2.8 DEFINIZIONE. Un polinomio $f(x)$ in $\mathbb{K}[x]$ che non sia il polinomio nullo e non sia invertibile si dice *irriducibile su \mathbb{K}* se

$$f(x) = g(x)h(x), \quad g(x), h(x) \in \mathbb{K}[x] \rightarrow g(x) \circ h(x) \text{ è invertibile}.$$

Se non è irriducibile, il polinomio si dice *riducibile*. \square

Nei casi attuali (ossia \mathbb{K} campo), un polinomio è irriducibile se, ogni volta che si fattorizza, uno dei due fattori è una costante non nulla.

3.2.9 DEFINIZIONE. Un polinomio $f(x)$ in $\mathbb{K}[x]$ che non sia il polinomio nullo e non sia invertibile si dice *primo* se, ogni volta che $f(x)$ divide un prodotto $g(x)h(x)$ (con $g(x)$ e $h(x)$ in $\mathbb{K}[x]$), allora divide uno dei due fattori. \square

La dimostrazione della proposizione seguente è pressoché identica a quella fatta negli interi, quindi viene tralasciata. Ciò non significa che non si debba sapere la dimostrazione in questo caso!

3.2.10 PROPOSIZIONE. Un polinomio in $\mathbb{K}[x]$ è irriducibile se e solo se è primo.

Vale un teorema di fattorizzazione unica, analogo a quello degli interi. Anche in questo caso si invita lo studente a ripercorrere la dimostrazione fatta, adattandola alla situazione attuale.

3.2.11 TEOREMA DI FATTORIZZAZIONE UNICA. Ogni polinomio $f(x)$ di grado ≥ 1 in $\mathbb{K}[x]$ si fattorizza in un prodotto di un numero finito di polinomi irriducibili. Tale fattorizzazione è unica nel senso che se

$$f(x) = p_1(x)p_2(x) \cdots p_s(x) = q_1(x)q_2(x) \cdots q_t(x),$$

$p_i(x), q_j(x)$ irriducibili in $\mathbb{K}[x]$, allora $s = t$ ed esiste una corrispondenza biunivoca tra $\{p_1(x), p_2(x), \dots, p_s(x)\}$ e $\{q_1(x), q_2(x), \dots, q_t(x)\}$ tale che se $q_j(x)$ corrisponde a $p_i(x)$, allora $p_i(x)$ è associato a $q_j(x)$.

3.2.12 TEOREMA DI RUFFINI. Se $f(x) \in \mathbb{K}[x]$ e $\alpha \in \mathbb{K}$ è tale che $f(\alpha) = 0$, allora $(x - \alpha) \mid f(x)$.

Dimostrazione. Si noti che in questo momento stiamo pensando al polinomio $f(x)$ come funzione polinomiale, visto che lo stiamo valutando in α . Dividiamo $f(x)$ per $(x - \alpha)$. Si ha

$$(3.2.1) \quad f(x) = (x - \alpha)q(x) + r(x), \quad \partial r(x) < \partial(x - \alpha) = 1.$$

Quindi $r(x)$ deve essere un elemento r di \mathbb{K} . Valutando la (3.2.1) per $x = \alpha$, si ottiene $f(\alpha) = 0 = (\alpha - \alpha)q(x) + r$, da cui segue che la costante r è uguale a zero, cioè $f(x)$ è divisibile per $x - \alpha$. \square

3.2.13 DEFINIZIONE. Sia $f(x) \in \mathbb{K}[x]$. Un elemento $\alpha \in \mathbb{K}$ tale che $f(\alpha) = 0$ si dice *radice o zero* di $f(x)$. \square

Il teorema di Ruffini ci dice che se α è una radice per $f(x)$, allora $x - \alpha$ divide $f(x)$. Ha senso allora la seguente definizione.

3.2.14 DEFINIZIONE. Una radice $\alpha \in \mathbb{K}$ di $f(x) \in \mathbb{K}[x]$ si dice *semplice* se $(x - \alpha) \mid f(x)$ ma $(x - \alpha)^2 \nmid f(x)$. Si dice di *molteplicità m* se $(x - \alpha)^m \mid f(x)$, ma $(x - \alpha)^{m+1} \nmid f(x)$. Una radice con molteplicità $m > 1$ si dice radice *multipla*. \square

3.2.15 PROPOSIZIONE. Sia \mathbb{K} un campo e $f(x)$ un polinomio non nullo in $\mathbb{K}[x]$ di grado n . Allora $f(x)$ ammette al più n radici in \mathbb{K} , contate con la loro molteplicità.

Dimostrazione. Procederemo per induzione sul grado n di $f(x)$. Se $n = 0$, $f(x)$ è una costante non nulla, che è priva di radici, quindi il teorema è vero. Supponiamo vero il teorema per ogni polinomio di grado $< n$. Sia $f(x)$ di grado n . Se $f(x)$ ha una radice α di molteplicità $m \geq 1$, $m \leq n$, allora

$$f(x) = (x - \alpha)^m q(x), \quad \deg q(x) = n - m.$$

Sia $\beta \neq \alpha$ un'altra radice di $f(x)$. Allora, $0 = f(\beta) = (\beta - \alpha)^m q(\beta)$. Dato che è $\beta \neq \alpha$, si deve avere $q(\beta) = 0$, perché \mathbb{K} è privo di divisori dello zero. Quindi le uniche radici di $f'(x)$ sono α (con molteplicità m) e le radici di $q(x)$. Ora, per l'ipotesi induttiva, $q(x)$ ha al più $n - m$ (= grado di $q(x)$) radici. In definitiva, $f(x)$ può avere al massimo $m + (n - m) = n$ radici in \mathbb{K} . \square

Questo teorema ha una conseguenza importante.

3.2.16 COROLLARIO. Sia \mathbb{K} un campo con infiniti elementi. Se $f(x)$ e $g(x)$ sono due polinomi di $\mathbb{K}[x]$, allora $f(x) = g(x)$ come polinomi se e solo se $f(x) = g(x)$ come funzioni polinomiali su \mathbb{K} .

Dimostrazione. Se $f(x) = g(x)$ come polinomi, ovviamente saranno uguali come funzioni polinomiali. Dobbiamo quindi provare il viceversa. Supponiamo che $f(\alpha) = g(\alpha)$ per ogni $\alpha \in \mathbb{K}$. Allora il polinomio $h(x) = f(x) - g(x)$ è un polinomio tale che $h(\alpha) = 0$ per ogni $\alpha \in \mathbb{K}$. Ora, se fosse $h(x)$ diverso dal polinomio nullo, $h(x)$ avrebbe un grado $n \in \mathbb{N}$. Dato che \mathbb{K} ha infiniti elementi, verremmo ad avere un polinomio con più radici del suo grado. Quindi $h(x)$ deve essere il polinomio nullo, cioè $f(x) = g(x)$ come polinomi. \square

Quindi per campi infiniti le due nozioni di polinomio e funzione polinomiale coincidono.

 **ESERCIZI.**

1. Si provi che un campo non può possedere divisori dello zero.
2. Si determinino i MCD delle seguenti coppie di polinomi a coefficienti in \mathbb{Q} :

$$(x^4 + x - 1, x^3 - 2)$$

$$(x^5 - x^3 + x^2 - 2x + 1, x^4 - x^3 + 2x^2 + x + 1)$$

e dei seguenti a coefficienti in \mathbb{Z}_7 :

$$(x^3 + x^2 - 6x - 1, x^4 - 2x^3 - 2x - 1).$$

3. Si determinino $h(x)$ e $k(x)$ in $\mathbb{Q}[x]$, se esistono, tali che

$$h(x)(x^2 + 1) + k(x)(x^3 - 3) = 20.$$

4. Siano f_1 e f_2 polinomi a coefficienti in un campo \mathbb{K} e sia $\alpha \in \mathbb{K}$. Se α è una radice di f_1 e f_2 con molteplicità rispettive k_1 e k_2 , si mostri che α è radice di $f_1 f_2$ con molteplicità $k_1 + k_2$. Se k è la molteplicità di α come radice di $f_1 + f_2$, si mostri che $k \geq \min(k_1, k_2)$ e che se $k_1 \neq k_2$, allora $k = \min(k_1, k_2)$.

 **ESERCIZI DI PROGRAMMAZIONE.**

1. Si scriva un programma che esegua la divisione tra due polinomi.
2. Si scriva un programma che calcoli il MCD $d(x)$ tra due polinomi f e g mediante l'algoritmo euclideo delle divisioni successive, ed esprima il MCD nella forma $d(x) = h(x)f(x) + k(x)g(x)$ (identità di Bézout).


CONTROLLO.

1. Differenza tra polinomi e funzioni polinomiali. Quando si possono identificare tali nozioni e perché?
2. Irriducibilità di polinomi a coefficienti in un campo \mathbb{K} : definizione. Tale definizione dipende dal campo? In che senso?
3. Cosa significa "fattorizzazione unica"? Enunciare con precisione il relativo teorema.

3.3. Questioni di irriducibilità

Abbiamo visto la definizione di polinomio irriducibile su di un campo \mathbb{K} , dalla quale appare chiaro che tale definizione *dipende dal campo* \mathbb{K} . Infatti, ad esempio, il polinomio $x^2 - 2$ (che è a coefficienti in \mathbb{Q} , e quindi anche in \mathbb{R}) è riducibile su \mathbb{R} , perché $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$, essendo $x + \sqrt{2}$ e $x - \sqrt{2}$ polinomi a coefficienti in \mathbb{R} , mentre è irriducibile su \mathbb{Q} , dato che $\sqrt{2} \notin \mathbb{Q}$ e quindi $x \pm \sqrt{2} \notin \mathbb{Q}[x]$. Vogliamo allora vedere come si fa a decidere se un polinomio è riducibile o irriducibile almeno quando \mathbb{K} è uguale a \mathbb{C} , \mathbb{R} o \mathbb{Q} .

3.3.1 POLINOMI IRRIDUCIBILI SU \mathbb{C} . Il seguente teorema è di capitale importanza in tutta la matematica, e anche per lo studio della riducibilità o irriducibilità di un polinomio su \mathbb{C} o su \mathbb{R} . Quindi a buon diritto gli è stato attribuito il nome di fondamentale.

3.3.2 TEOREMA FONDAMENTALE DELL'ALGEBRA. *Ogni polinomio $f(x) \in \mathbb{C}[x]$ di grado $n \geq 1$ ammette una radice in \mathbb{C} .*

Di questo teorema esistono diverse dimostrazioni, di varia natura. Noi desideriamo scegliere tra tutte le dimostrazioni una puramente algebrica. Non avendo però al momento gli strumenti necessari, dobbiamo posporne la dimostrazione all'ultimo capitolo. Da questo teorema discende il seguente corollario.

3.3.3 COROLLARIO. *Ogni polinomio $f(x) \in \mathbb{C}[x]$ di grado n ammette in \mathbb{C} esattamente n radici.*

Dimostrazione. Detta $\alpha_1 \in \mathbb{C}$ una radice di $f(x)$ (che esiste per il teorema fondamentale), per il teorema di Ruffini (§2) risulta

$$f(x) = (x - \alpha_1)q(x), \quad \partial q(x) = n - 1$$

con $q(x)$ ancora a coefficienti in \mathbb{C} . Quindi $q(x)$, ancora per il teorema fondamentale, ammette una radice $\alpha_2 \in \mathbb{C}$, ecc. Proseguendo allo stesso modo, si arriverà alla fine ad una fattorizzazione di $f(x)$ in

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

se $n = \partial f(x)$. \square

Conclusioni:

Tutti e soli i polinomi in $\mathbb{C}[x]$ irriducibili su \mathbb{C} sono i polinomi di grado 1.

Quindi ogni polinomio a coefficienti in \mathbb{C} si fattorizza su \mathbb{C} in fattori lineari.

3.3.4 POLINOMI IRRIDUCIBILI SU \mathbb{R} . Sia $f(x)$ un polinomio appartenente a $\mathbb{R}[x]$, di grado > 1 . Sia $\alpha \in \mathbb{C}$ una radice di $f(x)$ pensato come polinomio a coefficienti complessi (α esiste per il teorema fondamentale dell'algebra). Ora, essendo $f(x)$ a coefficienti reali, anche il numero $\bar{\alpha}$ complesso coniugato di α soddisfa al polinomio $f(x)$. Sia infatti $f(x) = \sum_{k=0}^n a_k x^k$; allora

$$0 = f(\alpha) = \sum_{k=0}^n a_k \alpha^k,$$

da cui, coniugando entrambi i membri, e osservando che i numeri reali sono autoconiugati,

$$0 = \bar{0} = \overline{f(\alpha)} = \overline{\sum_{k=0}^n a_k \alpha^k} = \sum_{k=0}^n a_k \bar{\alpha}^k = f(\bar{\alpha})$$

cioè $\bar{\alpha}$ è radice anch'essa di $f(x)$.

Ciò premesso, supponiamo $f(x)$ (di grado > 1) irriducibile su \mathbb{R} . Allora non avrà radici reali. La sua decomposizione in fattori lineari su \mathbb{C} sarà pertanto

$$f(x) = a_n(x - \alpha_1)(x - \bar{\alpha}_1)(x - \alpha_2)(x - \bar{\alpha}_2) \cdots (x - \alpha_t)(x - \bar{\alpha}_t)$$

con $\partial f(x) = n = 2t$. Ora, $\forall i = 1, \dots, t$

$$(x - \alpha_i)(x - \bar{\alpha}_i) = x^2 - (\alpha_i + \bar{\alpha}_i)x + \alpha_i\bar{\alpha}_i, \quad \alpha_i + \bar{\alpha}_i, \alpha_i\bar{\alpha}_i \in \mathbb{R}.$$

Quindi $f(x)$ si scrive come prodotto di t polinomi di secondo grado a coefficienti reali. Essendo per ipotesi $f(x)$ irriducibile su \mathbb{R} , tali fattori si dovranno ridurre ad uno solamente, quindi necessariamente $f(x)$ è di secondo grado e privo di radici reali (cioè si tratta di un polinomio di secondo grado con discriminante $\Delta < 0$). Dato che ovviamente un polinomio di *secondo* grado privo di radici reali è irriducibile, possiamo concludere dicendo:

Tutti e soli i polinomi $\in \mathbb{R}[x]$ irriducibili su \mathbb{R} sono i polinomi di primo grado e quelli di secondo grado con $\Delta < 0$.

 ATTENZIONE. Abbiamo messo in corsivo la parola *secondo*, perché il fatto di essere privo di radici nel campo \mathbb{K} non comporta che il polinomio sia irriducibile. \square

Ad esempio, il polinomio a coefficienti reali

$$x^4 - 3x^2 + 2$$

è privo di radici reali, ma è fattorizzabile nel modo seguente:

$$x^4 - 3x^2 + 2 = (x^2 + 1)(x^2 + 2).$$

Quando però il polinomio $f(x) \in \mathbb{K}[x]$ è di grado 2 o 3, allora la mancanza di radici nel campo \mathbb{K} assicura la irriducibilità di $f(x)$. Infatti, se $f(x)$ si fattorizzasse, uno almeno dei suoi fattori sarebbe di grado 1, e quindi questo comporterebbe l'esistenza di una radice in \mathbb{K} .

Riassumendo: *se un polinomio $f(x)$ di grado > 1 a coefficienti in un campo \mathbb{K} possiede una radice in \mathbb{K} , allora $f(x)$ è fattorizzabile (un fattore è lineare). Tuttavia un polinomio può essere fattorizzabile anche se non possiede nessuna radice nel campo (ad eccezione dei polinomi di grado 2 o 3 per i quali l'esistenza di una radice equivale alla riducibilità).*

3.3.5 POLINOMI IRRIDUCIBILI SU \mathbb{Q} . Siamo riusciti a caratterizzare i polinomi irriducibili su \mathbb{C} e su \mathbb{R} . Non saremo in grado di fare altrettanto per \mathbb{Q} . Dovremo accontentarci di stabilire dei criteri che ci permettano di dire se un dato polinomio è irriducibile su \mathbb{Q} e delle indicazioni per affrontare il problema della irriducibilità su \mathbb{Q} di un polinomio.

Premettiamo alcuni lemmi, dai quali vedremo come la fattorizzazione di un polinomio su \mathbb{Q} sia strettamente collegata alla sua fattorizzazione su \mathbb{Z} . Questo stretto legame è dovuto al fatto che \mathbb{Q} è il campo dei quozienti di \mathbb{Z} (cfr. §2.4).

Per studiare la fattorizzazione di polinomi a coefficienti in \mathbb{Q} dovremo considerare polinomi a coefficienti in \mathbb{Z} e studiarne alcune proprietà. Si noti che finora abbiamo definito solo polinomi a coefficienti in un campo K e abbiamo dimostrato molte loro proprietà. Nessuno ci vieta tuttavia di definire anche polinomi a coefficienti in un anello comutativo con unità (come \mathbb{Z}). L'importante è non pretendere che valgano per tali polinomi i risultati che valevano per il caso in cui i coefficienti appartenevano ad un campo.

3.3.6 LEMMA. *Sia $f(x) \in \mathbb{Q}[x]$. Allora*

$$f(x) = \frac{d}{m} f^*(x)$$

dove $f^*(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$, $(a_0, a_1, \dots, a_n) = 1$ e $d, m \in \mathbb{Z}$, $(d, m) = 1$.

Dimostrazione. Sia $f(x) = q_0 + q_1 x + q_2 x^2 + \dots + q_n x^n$, $q_i = b_i/c_i \in \mathbb{Q} \forall i$, e $b_i, c_i \in \mathbb{Z}$. Quindi

$$f(x) = \frac{b_0}{c_0} + \frac{b_1}{c_1} x + \dots + \frac{b_n}{c_n} x^n.$$

Indicato con m' il mcm(c_0, c_1, \dots, c_n), il polinomio $m'f(x) = b'_0 + b'_1 x + \dots + b'_n x^n$ è un polinomio a coefficienti interi. Posto $d' = \text{MCD}(b'_0, b'_1, \dots, b'_n)$, risulterà $m'f(x) = d'(a_0 + a_1 x + \dots + a_n x^n)$ con $a_i \in \mathbb{Z}$ e $\text{MCD}(a_0, a_1, \dots, a_n) = 1$. Dividendo, se necessario, per il MCD(d', m') entrambi i membri, si ottiene

$$mf(x) = d \sum_{k=0}^n a_k x^k$$

che è la relazione richiesta. \square

3.3.7 DEFINIZIONE. Sia $f(x) \in \mathbb{Z}[x]$. Si definisce *divisore* o *contenuto* di $f(x)$ il massimo comun divisore dei suoi coefficienti. \square

3.3.8 DEFINIZIONE. Un polinomio $f(x) = \sum_{k=0}^n a_k x^k \in \mathbb{Z}[x]$ si dice *primitivo* se il massimo comun divisore dei suoi coefficienti (cioè il suo contenuto) è 1. \square

Il lemma precedente mostra che se $f(x) \in \mathbb{Q}[x]$ allora esiste in $\mathbb{Z}[x]$ un polinomio $f^*(x)$ associato a $f(x)$ che è primitivo.

3.3.9 ESEMPIO. Sia

$$f(x) = \frac{3}{2} + \frac{6}{7}x - \frac{3}{8}x^2.$$

Allora $m' = \text{mcm}(2, 7, 8) = 56$ e $56f(x) = 84 + 48x - 21x^2 = 3(28 + 16x - 7x^2)$. Il polinomio primitivo $f^*(x)$ associato a $f(x)$ è pertanto $28 + 16x - 7x^2$. \square

Quanto ora detto ci permette di concludere che, quando si è interessati alla fattorizzazione di un polinomio $f(x)$ a coefficienti in \mathbb{Q} , si può sempre supporre che il polinomio sia a coefficienti interi (primitivo o no a seconda dei casi).

Vale il seguente risultato, che non è assolutamente ovvio.

3.3.10 LEMMA DI GAUSS. *Il prodotto di due polinomi primitivi è ancora un polinomio primitivo.*

Dimostrazione. Siano

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \quad g(x) = b_0 + b_1x + \cdots + b_mx^m, \quad a_i, b_i \in \mathbb{Z}$$

i due polinomi primitivi. Supponiamo per assurdo $f(x)g(x)$ non primitivo. Allora esiste un numero primo p che divide tutti i coefficienti di $f(x)g(x)$. Tale primo p non potrà dividere tutti i coefficienti di $f(x)$ e di $g(x)$ per l'ipotesi di primitività. Siano a_h e b_k i coefficienti rispettivamente di $f(x)$ e di $g(x)$ con indici più bassi non divisi da p . Andiamo ad esaminare il coefficiente di indice $h+k$ in $f(x)g(x)$. Risulta

$$c_{h+k} = a_h b_k - (a_{h-1} b_{k+1} - \cdots + a_0 b_{h+k}) + (a_{h+1} b_{k-1} + \cdots + a_{h+k} b_0).$$

Ora, p divide c_{h+k} , divide anche entrambe le quantità dentro le parentesi come è facile verificare, quindi divide anche $a_h b_k$. Ma allora divide uno dei due fattori, il che contraddice l'ipotesi. \square

3.3.11 COROLLARIO. *Il contenuto del prodotto di due polinomi uguaglia il prodotto dei contenuti dei due polinomi fattori.*

Dimostrazione. Sia $f(x) = g(x)h(x)$, $f(x), g(x), h(x) \in \mathbb{Z}[x]$. Estraiamo il contenuto dei singoli polinomi:

$$f(x) = df^*(x) = d_1 g^*(x) d_2 h^*(x) = d_1 d_2 \cdot g^*(x) h^*(x).$$

Essendo $g^*(x)h^*(x)$ primitivo, risulta $d = d_1 d_2$, che dice esattamente che il contenuto del prodotto è il prodotto dei contenuti dei singoli fattori. \square

3.3.12 TEOREMA DI GAUSS. *Se un polinomio $f(x) \in \mathbb{Z}[x]$ si decompone nel prodotto di due polinomi a coefficienti razionali, allora si decompone anche nel prodotto di due polinomi degli stessi gradi a coefficienti interi.*

Dimostrazione. Dimostreremo il teorema supponendo dapprima che $f(x)$ sia primitivo. Sia quindi $f(x) = g(x)h(x)$, $g(x), h(x) \in \mathbb{Q}[x]$. Ora, in virtù del lemma 3.3.6, sarà

$$g(x) = \frac{d_1}{m_1} g^*(x) \quad \text{e} \quad h(x) = \frac{d_2}{m_2} h^*(x),$$

con $g^*(x), h^*(x) \in \mathbb{Z}[x]$ primitivi e d_i e m_i interi. In definitiva, $f(x) = (d/m)g^*(x)h^*(x)$, $d = d_1d_2$, $m = m_1m_2$. In virtù del lemma di Gauss, il polinomio $f^*(x) = g^*(x)h^*(x)$ è primitivo, e risulta

$$(3.3.1) \quad mf(x) = df^*(x), \quad f(x) \text{ e } f^*(x) \text{ primitivi.}$$

I due polinomi del primo e secondo membro devono avere lo stesso contenuto: ma questo è rispettivamente m e d (essendo $f(x)$ e $f^*(x)$ primitivi). Quindi $m = d$ e la (3.3.1) diventa

$$f(x) = g^*(x)h^*(x)$$

che è una fattorizzazione su \mathbb{Z} con i fattori dello stesso grado della fattorizzazione originaria su \mathbb{Q} .

Nel caso in cui $f(x) \in \mathbb{Z}[x]$ non sia primitivo, sia ancora $f(x) = g(x)h(x)$ una sua fattorizzazione su \mathbb{Q} . Allora, posto $f(x) = df^*(x)$ (cioè posto $f(x)$ come prodotto del suo contenuto per un polinomio primitivo), sarà $df^*(x) = g(x)h(x)$, da cui

$$f^*(x) = d^{-1}g(x)h(x).$$

Ora, $f^*(x)$ è *primitivo*, quindi, per quanto dimostrato nella prima parte, avendo una fattorizzazione su \mathbb{Q} , ne avrà una anche su \mathbb{Z} , cioè

$$f^*(x) = \bar{g}(x)\bar{h}(x), \quad \bar{g}(x), \bar{h}(x) \in \mathbb{Z}[x].$$

Ma allora, tornando all'espressione originale di $f(x)$, la

$$f(x) = df^*(x) = d\bar{g}(x)\bar{h}(x)$$

è una fattorizzazione di $f(x)$ su \mathbb{Z} . \square

3.3.13 ESEMPIO. $f(x) = x^4 + 10x^2 + 24$ è un polinomio in $\mathbb{Z}[x]$ primitivo. Risulta fattorizzabile su \mathbb{Q} , come è facile controllare, ad esempio al modo seguente: $f(x) = (\frac{2}{3}x^2 + \frac{16}{9})(\frac{3}{2}x^2 + 9)$. Allora, procedendo come nel corso della dimostrazione del teorema,

$$f(x) = \frac{d_1}{m_1} g^*(x) \frac{d_2}{m_2} h^*(x) = \frac{4}{6} (x^2 + 4) \frac{3}{2} (x^2 + 6) = (x^2 + 4)(x^2 + 6),$$

che è una fattorizzazione su \mathbb{Z} . Se fossimo partiti ad esempio dal polinomio non primitivo $f(x) = 3x^4 + 30x^2 + 72$, una cui fattorizzazione su \mathbb{Q} è ad esempio $f(x) = (2x^2 + \frac{16}{3})(\frac{3}{2}x^2 + 9)$, per trovare una sua fattorizzazione su \mathbb{Z} si scrive $f(x) = df^*(x) = 3(x^4 + 10x^2 + 24)$. Quindi $f^*(x) = \frac{1}{3}f(x) = \frac{1}{3}(2x^2 + \frac{16}{3})(\frac{3}{2}x^2 + 9)$; dato che $f^*(x)$ è primitivo, si ripete quanto fatto prima, cioè $f^*(x) = \frac{1}{3}2(x^2 + 4)\frac{3}{2}(x^2 + 6) = (x^2 + 4)(x^2 + 6)$, che è una fattorizzazione di $f^*(x)$ su \mathbb{Z} . Allora sarà $f(x) = 3f^*(x) = 3(x^2 + 12)(x^2 + 6) = (3x^2 + 12)(x^2 + 6)$. \square

ATTENZIONE. Il teorema di Gauss ci dice che se un polinomio a coefficienti in \mathbb{Z} è fattorizzabile su \mathbb{Q} , allora esso è fattorizzabile anche su \mathbb{Z} , o, equivalentemente, se è irriducibile su \mathbb{Z} , allora è irriducibile anche su \mathbb{Q} . Sembra essere allora di poter concludere che un polinomio a coefficienti in \mathbb{Z} è irriducibile su \mathbb{Z} se e solo se esso è irriducibile su \mathbb{Q} . Infatti, dato che ad esempio, un polinomio in $\mathbb{Q}[x]$ irriducibile su \mathbb{R} è ovviamente irriducibile anche su \mathbb{Q} , si potrebbe pensare che debba valere anche la analoga proprietà che un polinomio a coefficienti in \mathbb{Z} irriducibile su \mathbb{Q} debba necessariamente essere irriducibile su \mathbb{Z} . Ma si pensi alla definizione di polinomio irriducibile: un polinomio $f(x)$ è irriducibile se, potendosi scrivere come prodotto di due polinomi, allora *uno dei due è invertibile*. Allora, esaminiamo ad esempio il seguente polinomio, $f(x) = 3x^2 + 6$: esso è irriducibile su \mathbb{Q} , perché è associato al polinomio $x^2 + 2$ che è chiaramente irriducibile su \mathbb{Q} . Tuttavia $f(x)$ è riducibile su \mathbb{Z} , perché la fattorizzazione $3(x^2 + 2)$ è una fattorizzazione non banale su \mathbb{Z} , perché 3 non è invertibile su \mathbb{Z} ! In altri termini, i due polinomi $3x^2 + 6$ e $x^2 + 2$ non sono associati in $\mathbb{Z}[x]$. Gli elementi invertibili di $\mathbb{Z}[x]$ non sono le costanti non nulle, ma sono gli elementi invertibili di \mathbb{Z} , ossia ± 1 . Quindi, la riducibilità su \mathbb{Z} non implica la riducibilità su \mathbb{Q} ! Dato che \mathbb{Z} non è un campo, non si possono estendere a $\mathbb{Z}[x]$ risultati del tipo: se un polinomio è riducibile su \mathbb{Q} , che è contenuto in \mathbb{R} , allora è riducibile su \mathbb{R} ; infatti \mathbb{Q} ed \mathbb{R} sono entrambi campi, l'uno contenuto nell'altro e un elemento di \mathbb{Q} è invertibile in \mathbb{Q} se e solo se è invertibile in \mathbb{R} . Si noti infine che volutamente, quando abbiamo dato (cfr. definizione 3.2.8) la definizione di irriducibilità di un polinomio a coefficienti in un campo, non abbiamo detto che un polinomio è irriducibile se ogni volta che si fattorizza, uno dei due fattori è una costante non nulla (cosa che peraltro avremmo potuto fare, dato che nel caso di polinomi a coefficienti in un campo le due nozioni di polinomio invertibile e di costante non nulla coincidono). Il motivo per cui abbiamo fatto ciò è che in questo modo la definizione data si può applicare ad anelli più generali, come vedremo. \square

A questo punto però possiamo affermare:

$f(x) \in \mathbb{Z}[x]$ è primitivo e irriducibile su \mathbb{Z} se e solo se è irriducibile su \mathbb{Q} .

Infatti, nel caso in cui il polinomio sia primitivo, non potrà avere una fattorizzazione in cui uno dei fattori è un elemento di \mathbb{Z} diverso da ± 1 .

Per decidere la riducibilità o irriducibilità di un polinomio $f(x) \in \mathbb{Z}[x]$ di grado > 1 su \mathbb{Q} è utile innanzitutto avere un metodo che permetta di stabilire se il polinomio ha o no radici razionali; se le avesse, sarebbe senz'altro riducibile. La seguente proposizione ci offre una utile informazione in questo senso.

3.3.14 PROPOSIZIONE. *Sia $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x]$. Sia $\alpha = r/s$ una radice di $f(x)$, con $r, s \in \mathbb{Z}$, $(r, s) = 1$. Allora $r \mid a_0$ e $s \mid a_n$.*

Dimostrazione. Se $\alpha = r/s$ è una radice di $f(x)$, risulterà $0 = f(r/s) = a_0 + a_1(r/s) + \cdots + a_n(r/s)^n$. Moltiplicando ambo i membri per s^n si ottiene

$$\begin{aligned} 0 &= s^n a_0 + s^{n-1} a_1 r + \cdots + a_n r^n \\ &= s(s^{n-1} a_0 + s^{n-2} a_1 r + \cdots + a_{n-1} r^{n-1}) + a_n r^n \\ &= s^n a_0 + r(s^{n-1} a_1 + \cdots + a_n r^{n-1}). \end{aligned}$$

Dalla $0 = s(s^{n-1} a_0 + \cdots + a_{n-1} r^{n-1}) + a_n r^n$ segue che $s \mid a_n r^n$, e dalla $0 = s^n a_0 + r(s^{n-1} a_1 + \cdots + a_n r^{n-1})$ segue $r \mid a_0 s^n$. Essendo $(r, s) = 1$, possiamo concludere che $s \mid a_n$ e $r \mid a_0$. \square

3.3.15 COROLLARIO. *Se un polinomio monico a coefficienti interi ha una radice razionale, questa è un numero intero.*

La proposizione ci dice che le possibili radici razionali di un polinomio $f(x) \in \mathbb{Z}[x]$ sono da ricercarsi tra i numeri razionali della forma r/s , dove r varia tra i divisori del termine noto a_0 e s tra i divisori del coefficiente direttivo a_n .

3.3.16 ESEMPIO. *Se il polinomio $3x^3 - 4x^2 + 2$ ha radici razionali, queste devono trovarsi nel seguente insieme: $\{\pm 1, \pm 2, \pm 1/3, \pm 2/3\}$. Basta allora controllare se queste sono radici di $f(x)$. Come è facile verificare, nessuno dei numeri razionali elencati è radice di $f(x)$, quindi si può essere certi che $f(x)$ non possiede radici razionali.* \square

Esiste poi un criterio che permette di stabilire se un polinomio a coefficienti interi è irriducibile su \mathbb{Q} .

3.3.17 CRITERIO DI IRRIDUCIBILITÀ DI EISENSTEIN. *Sia $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ un polinomio in $\mathbb{Z}[x]$. Sia p un numero primo tale che*

- (a) $p \nmid a_n$;
- (b) $p \nmid a_i \forall i = 0, \dots, n-1$;
- (c) $p^2 \nmid a_0$.

Allora $f(x)$ è irriducibile su \mathbb{Q} .

Dimostrazione. Per il teorema di Gauss basta provare che è irriducibile su \mathbb{Z} . Supponiamo per assurdo che sia $f(x) = g(x)h(x)$, con

$$g(x) = b_0 + b_1 x + \cdots + b_r x^r, \quad h(x) = c_0 + c_1 x + \cdots + c_s x^s, \quad b_i, c_i \in \mathbb{Z}$$

polinomi di gradi $r < n$ e $s < n$, se $n = \deg f(x)$. Allora $r+s=n$ e $b_0 c_0 = a_0$: $p \mid a_0$, per cui $p \mid b_0$ o $p \mid c_0$. Non può dividere entrambi (altrimenti sarebbe $p^2 \mid a_0$). Supponiamo quindi, ad esempio, che p divida b_0 ma non divida c_0 . Sia b_i il coefficiente con indice più basso non diviso da p (p non può dividere tutti i b_i , altrimenti p dividerebbe tutti gli a_i , contro l'ipotesi). Allora per $i \leq r < n$

$$a_i = b_i c_0 + b_{i-1} c_1 + \cdots + b_0 c_i$$

da cui $p \mid c_0$: infatti p divide a_i ($i < n$), p divide tutti i b_k con $k = 0, \dots, i-1$, da cui p deve dividere $b_i c_0$: non potendo p dividere b_i , deve necessariamente dividere c_0 . L'assurdo nasce dall'aver supposto $f(x)$ riducibile. \square

ATTENZIONE. Si noti che il criterio di Eisenstein offre una condizione *sufficiente* di irriducibilità, ma non una condizione *necessaria!* \square

Spesso ad un polinomio non è applicabile direttamente il criterio di Eisenstein. Può succedere però che modificando opportunamente il polinomio si ottenga un polinomio al quale invece si possa applicare il criterio. Tuttavia occorre essere certi che la irriducibilità del polinomio modificato sia equivalente alla irriducibilità del polinomio originario. A questo scopo ci vengono in aiuto le seguenti osservazioni.

3.3.18 OSSERVAZIONI.

(a) Sia $p(x)$ un fissato polinomio in $\mathbb{K}[x]$. L'applicazione

$$\begin{aligned} T_p : \mathbb{K}[x] &\longrightarrow \mathbb{K}[x] \\ f(x) &\longmapsto f(p(x)) \end{aligned}$$

che sostituisce ad x il polinomio $p(x)$ conserva le operazioni tra polinomi (cfr. esercizio 3.3.3).

(b) Nel caso in cui come $p(x)$ si prenda un polinomio lineare del tipo $x - \alpha$, allora la T_p è *biunivoca*, e $f(x)$ e il polinomio trasformato $f(x - \alpha)$ hanno lo stesso grado. Quindi, come è facile vedere,

$$\boxed{f(x) \text{ è irriducibile su } \mathbb{K} \iff f(x - \alpha) \text{ è irriducibile su } \mathbb{K}}.$$

Analogamente risulta, per $\alpha \neq 0$,

$$\boxed{f(x) \text{ è irriducibile su } \mathbb{K} \iff f(x/\alpha) \text{ è irriducibile su } \mathbb{K}}.$$

Si noti che la (a) vale anche nel caso in cui il polinomio appartenga a $\mathbb{Z}[x]$. Utilizzando queste proprietà, si riesce a volte a trasformare un polinomio in un nuovo polinomio al quale si può applicare il criterio di Eisenstein. \square

3.3.19 ESEMPIO.

Dimostrare che, se p è un numero primo, il polinomio

$$x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$$

è irriducibile su \mathbb{Q} .

Osserviamo innanzitutto che

$$x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1 = \frac{x^p - 1}{x - 1}.$$

Ora, facendo la sostituzione $x \rightarrow x+1$, si ottiene

$$\begin{aligned} & (x+1)^{p-1} + (x+1)^{p-2} + \cdots + (x+1)^2 + (x+1) + 1 \\ & \quad = \frac{(x+1)^p - 1}{(x+1) - 1} \\ & \quad = \frac{\sum_{k=0}^p \binom{p}{k} x^{p-k} - 1}{x} \\ & \quad = x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + p. \end{aligned}$$

A questo punto si può applicare il criterio di Eisenstein, con il primo p , ed è così provato che il polinomio originario è irriducibile. \square

Vorremmo però trovare altri metodi che permettano, dato un polinomio a coefficienti interi, di decidere se si tratta di un polinomio riducibile o no su \mathbb{Q} . Un metodo possibile (che però si può utilizzare solo nei casi in cui il grado del polinomio non è troppo elevato) è quello di cercare direttamente una fattorizzazione del polinomio dato. Se ad esempio $f(x)$ è un polinomio (che si può sempre supporre a coefficienti interi e primitivo) di grado 5 e se abbiamo preventivamente controllato che il polinomio è privo di radici razionali, allora, se $f(x)$ si spezza, esso potrà fattorizzarsi solo nel prodotto di un polinomio di secondo grado per uno di terzo. Uguagliando allora i coefficienti, si ottiene un sistema, per il quale cerchiamo soluzioni *intero*: infatti, come sappiamo, ci si può sempre ridurre ad una fattorizzazione in $\mathbb{Z}[x]$. Se il sistema è incompatibile, allora il polinomio originario è irriducibile.

3.3.20 ESEMPIO. Si provi che $x^4 + 1$ è irriducibile su \mathbb{Q} .

Il polinomio non ha radici razionali, quindi si può spezzare solo nel prodotto di due polinomi di secondo grado. Ricordando che il coefficiente direttivo del prodotto è il prodotto dei coefficienti direttivi, e il termine noto del prodotto è il prodotto dei termini noti dei fattori, si può scrivere

$$x^4 + 1 = (x^2 + ax \pm 1)(x^2 + bx \pm 1)$$

dove verranno scelti o entrambi i segni + o entrambi i segni -. I sistemi che si ottengono uguagliando i coefficienti sono

$$\begin{cases} a + b = 0 \\ ab = \mp 2 \end{cases}$$

nessuno dei quali ammette soluzioni intere. Si noti che su \mathbb{R} $x^4 + 1$ si fattorizza come $x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$.

Questo metodo però può diventare impraticabile non appena il grado del polinomio cresce. \square

Il metodo che presenteremo qui di seguito è assai utile per il controllo della irriducibilità di un dato polinomio a coefficienti interi.

Sia $f(x) = \sum_{i=0}^n a_i x^i$ un polinomio a coefficienti in \mathbb{Z} e primitivo. Riduciamo i coefficienti modulo un numero primo p (cioè pensiamo il polinomio $f(x)$ in $\mathbb{Z}_p[x]$). Indichiamo con $\bar{f}(x)$ il nuovo polinomio. Ebbene, se p è scelto in modo da non dividere a_n , allora $f(x)$ e $\bar{f}(x)$ hanno lo stesso grado. Se $f(x) = g(x)h(x)$, $g(x)$ e $h(x)$ in $\mathbb{Z}[x]$, allora risulta anche $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$, quindi se $f(x)$ è riducibile su \mathbb{Q} , allora è riducibile anche $\bar{f}(x)$ in $\mathbb{Z}_p[x]$. Possiamo quindi concludere al modo seguente:

$$\boxed{\bar{f}(x) \text{ irriducibile su } \mathbb{Z}_p \text{ per qualche } p \nmid a_n \implies f(x) \text{ irriducibile su } \mathbb{Q}}.$$

 ATTENZIONE. Si noti che non è vero il viceversa, cioè non è vero che se per qualche p $\bar{f}(x)$ è riducibile su \mathbb{Z}_p , allora $f(x)$ è riducibile su \mathbb{Q} . Ad esempio, abbiamo visto che $x^4 + 1$ è irriducibile su \mathbb{Q} , tuttavia, $x^4 + 1$ è riducibile su \mathbb{Z}_2 , infatti $x^4 + 1 = (x^2 + 1)(x^2 + 1)$ in $\mathbb{Z}_2[x]$. \square

Ora, dato che il test di irriducibilità in $\mathbb{Z}_p[x]$ è un test finito, la possibilità di lavorare modulo p è molto comoda.

3.3.21 ESEMPIO. Diamo un esempio per mostrare come funziona questo metodo. Si provi che il polinomio $3x^4 - 4x^3 + 5x - 7$ è irriducibile su \mathbb{Q} .

Pensato come polinomio a coefficienti in \mathbb{Z}_2 , il polinomio è $x^4 + x + 1$. Ora, questo polinomio non ha radici in \mathbb{Z}_2 , quindi, se si fattorizza, si fattorizza nel prodotto di due fattori di secondo grado, precisamente

$$x^4 + x + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$$

tenendo conto del modo in cui si trovano coefficiente direttivo e termine noto del prodotto (e del fatto che siamo in \mathbb{Z}_2). È facile vedere che questa fattorizzazione non è possibile. Quindi $x^4 + x + 1$ è irriducibile su \mathbb{Z}_2 , per cui il polinomio originario è irriducibile su \mathbb{Q} .

Si noti che possiamo anche concludere che $x^4 + x + 1$ è irriducibile su \mathbb{Q} , dato che abbiamo appena mostrato che è irriducibile su \mathbb{Z}_2 (i coefficienti in questo caso sono gli stessi, dato che sono già ridotti modulo 2). \square

Per comodità, riassumiamo qui di seguito i metodi visti per decidere se un polinomio è irriducibile su \mathbb{Q} , senza che questo significhi che questi sono tutti i modi possibili per affrontare questo problema, né che vadano eseguiti nell'ordine dato.

3.3.22 METODI PER STUDIARE LA IRRIDUCIBILITÀ DI UN POLINOMIO SU \mathbb{Q} .

- Ridursi ad un polinomio $f(x) \in \mathbb{Z}[x]$ e primitivo.
- Se $f(x)$ è di grado 2 o 3, $f(x)$ è irriducibile su \mathbb{Q} se e solo se è privo di radici in \mathbb{Q} .

- (c) Utilizzare il test dell'esistenza di radici razionali per poter concludere che $f(x)$ è riducibile (esistenza di radici implica polinomio riducibile).
- (d) Se esiste un p primo tale che siano verificate le condizioni del criterio di Eisenstein, applicare il criterio per concludere che $f(x)$ è irriducibile su \mathbb{Q} .
- (e) Fare eventuali trasformazioni del tipo $x \rightarrow x + \alpha$ per potere utilizzare il criterio di Eisenstein.
- (f) Per gradi non eccessivamente alti, vedere se esiste una fattorizzazione in polinomi a coefficienti interi. Combinare questo metodo col test di esistenza di radici razionali, per eliminare fattorizzazioni con un fattore lineare.
- (g) Passaggio da $f(x) \in \mathbb{Z}[x]$ a $\bar{f}(x) \in \mathbb{Z}_p[x]$: se esiste un p che non divide a_n tale che $\bar{f}(x)$ sia irriducibile su \mathbb{Z}_p , allora $f(x)$ è irriducibile sui \mathbb{Q} . \square



ESERCIZI.

- Si decompongano in fattori irriducibili su \mathbb{C} , \mathbb{R} , \mathbb{Q} e \mathbb{Z}_2 i seguenti polinomi

$$\begin{aligned}x^5 + 2x^4 - 5x^3 - 10x^2 + 6x + 12 \\x^5 + 2x^4 - x^3 - 2x^2 - 2x - 4 \\x^5 + 3x^4 - x^3 - 3x^2 - 2x - 6.\end{aligned}$$

- Si dica per quali valori $a \in \mathbb{Z}$ il polinomio

$$3x^3 + 20ax^2 + 50a^2x + 60$$

è irriducibile rispettivamente su \mathbb{Q} , \mathbb{R} e \mathbb{C} .

- Sia $p(x)$ un fissato polinomio appartenente a $\mathbb{K}[x]$. Si provi che l'applicazione T_p definita dalla $T_p(f(x)) = f(p(x))$ per ogni $f(x) \in \mathbb{K}[x]$ conserva le due operazioni di $\mathbb{K}[x]$.
- Si decida se il polinomio $x^5 - 7x^4 + 2x^3 + 6x^2 - x + 8$ è irriducibile su \mathbb{Q} .
- Si provi la irriducibilità su \mathbb{Q} dei seguenti polinomi:

$$\begin{aligned}x^5 - x - 1 \\x^4 - x^3 + x^2 + 1 \\x^4 - x^2 - 1 \\x^5 + 4x + 1.\end{aligned}$$

- Si fattorizzino su \mathbb{Z}_5 i seguenti polinomi:

$$\begin{aligned}x^5 + x^4 + x^3 + x + 1 \\x^4 + 2x + 3 \\x^6 + 4x + 1 \\x^4 - 1 \\x^4 + 1.\end{aligned}$$



ESERCIZI DI PROGRAMMAZIONE.

- Scrivere un programma che ricerchi le radici razionali di un polinomio a coefficienti interi.
- Scrivere un programma che testi la irriducibilità di un polinomio a coefficienti interi con il criterio di irriducibilità di Eisenstein.
- Scrivere un programma che controlli la irriducibilità su \mathbb{Q} di un polinomio a coefficienti in \mathbb{Z} pensandolo come polinomio a coefficienti in \mathbb{Z}_p per vari primi p .



CONTROLLO.

- Chi sono tutti e soli i polinomi irriducibili su \mathbb{C} ? e su \mathbb{R} ?
- Un polinomio a coefficienti in \mathbb{Z} irriducibile su \mathbb{Q} è anche irriducibile su \mathbb{Z} ? e viceversa?
- Se non esiste nessun primo p che soddisfa le condizioni richieste dal criterio di Eisenstein, si può concludere che il polinomio è riducibile?
- L'irriducibilità di un polinomio su \mathbb{Q} implica la sua irriducibilità su ogni \mathbb{Z}_p ?

3.4. I polinomi ciclotomici

Un'interessante classe di polinomi a coefficienti in \mathbb{Z} e irriducibili su \mathbb{Q} è rappresentata dai cosiddetti polinomi ciclotomici. Tali polinomi nascono in collegamento con il problema della ciclotomia, ossia della divisione del cerchio in parti uguali con riga e compasso. L'equazione di partenza è la $x^n - 1 = 0$, le cui soluzioni sono le radici n -esime dell'unità (cfr. §2.11). Sul problema della ciclotomia, e quindi della costruzione di poligoni regolari, avremo modo di parlare quando tratteremo la teoria di Galois. È opportuno però iniziare a parlare dei polinomi ciclotomici e delle loro proprietà, primo, perché si tratta di polinomi, e quindi è giusto parlarne nel capitolo intitolato "polinomi", e secondo perché si tratta di polinomi strettamente collegati a problemi discussi in questo e nel capitolo precedente (funzione di Eulero, problemi di irriducibilità su \mathbb{Q} , ecc.).

Sappiamo che le radici n -esime dell'unità (cioè le soluzioni dell'equazione $x^n - 1 = 0$) sono gli n numeri complessi $\zeta_{n,0}, \zeta_{n,1}, \dots, \zeta_{n,n-1}$, dove

$$\zeta_{n,k} = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, \quad 0 \leq k < n.$$

3.4.1 DEFINIZIONE. Si definisce *ordine* o *perzado* di una radice n -esima dell'unità ζ il più piccolo intero positivo m a cui si deve elevare ζ per ottenere 1. Cioè $\zeta^m = 1$, ma $\zeta^h \neq 1$ per ogni $h = 1, \dots, m-1$. \square

3.4.2 LEMMA. Sia ζ una radice dell'unità tale che per qualche $t > 0$, $t \in \mathbb{N}$, $\zeta^t = 1$. Allora l'ordine m di ζ è un divisore di t .

Dimostrazione. Basta dividere t per m e ricordare la definizione di ordine. \square

3.4.3 DEFINIZIONE. Una radice n -esima ζ dell'unità si dice *primitiva* se il suo ordine è n . \square

Indichiamo con ζ_n la radice n -esima che corrisponde a $k = 1$, cioè $\zeta_n = \zeta_{n,1} = \cos(2\pi/n) + i \sin(2\pi/n)$. Si tratta di una radice primitiva, perché, per $h = 1, \dots, n-1$, per la formula di de Moivre,

$$\zeta_n^h = \cos \frac{2h\pi}{n} + i \sin \frac{2h\pi}{n} = \zeta_{n,h}$$

che è diversa da 1. Elevando ad h (per $h = 0, \dots, n-1$) la radice n -esima primitiva ζ_n si ottengono *tutte* le radici n -esime dell'unità.

3.4.4 PROPOSIZIONE. Se ζ è una radice n -esima dell'unità diversa da 1,

$$1 + \zeta + \zeta^2 + \dots + \zeta^{n-1} = 0.$$

Dimostrazione. Infatti dalla

$$(3.4.1) \quad x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \dots + x + 1)$$

posto $x = \zeta$ ($\neq 1$) in (3.4.1) si ha $\zeta^{n-1} + \zeta^{n-2} + \dots + \zeta + 1 = 0$. \square

Abbiamo trovato *una* radice n -esima primitiva dell'unità. Vogliamo ora determinarle *tutte*. Per far ciò basta calcolare l'ordine di tutte le radici n -esime e vedere quali sono quelle che hanno come ordine esattamente n . Per fare ciò partiremo da una qualunque radice n -esima primitiva dell'unità e calcoleremo l'ordine di tutte le sue potenze.

3.4.5 PROPOSIZIONE. Sia ζ una radice n -esima primitiva dell'unità. Allora ζ^k ha ordine $n/(n,k)$.

Dimostrazione. Sia $\delta = \text{MCD}(n, k)$; posto $k = k_1\delta$, $n = n_1\delta$, risulta $(n_1, k_1) = 1$. Vogliamo determinare l'ordine $m = m(k)$ di ζ^k .

Risulta

$$(\zeta^k)^{n_1} = (\zeta^{k_1\delta})^{\frac{n_1}{\delta}} = (\zeta^n)^{k_1} = 1.$$

Quindi

$$(3.4.2) \quad m \mid n_1.$$

D'altra parte,

$$\zeta^{km} = (\zeta^k)^m = 1.$$

per cui, essendo ζ una radice n -esima primitiva dell'unità, e pertanto di periodo n , segue che $n \mid km \implies n_1 \delta \mid k_1 \delta m$, da cui $n_1 \mid k_1 m$. Dato che $(n_1, k_1) = 1$, risulta

$$(3.4.3) \quad n_1 \mid m.$$

(3.4.2) e (3.4.3) comportano che $m = n_1 = n/\delta$. \square

3.4.6 COROLLARIO. *Tutte e sole le radici n -esime primitive dell'unità sono*

$$\zeta_{n,k} = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} = \zeta_n^k$$

dove $(n, k) = 1$ e $1 \leq k < n$, e quindi sono in numero di $\varphi(n)$, φ la funzione di Eulero.

Dimostrazione. Infatti dalla

$$(\zeta^k)^{n/\delta} = 1$$

segue che ζ^k è primitiva se e solo se $\delta = 1$. Inoltre, se $k \geq n$, $\zeta_{n,k}$ coincide con una delle radici con indice minore di k , data la periodicità delle funzioni sin e cos. \square

3.4.7 OSSERVAZIONE. Abbiamo visto che elevando alle varie potenze la radice primitiva $\zeta_{n,1}$ si ottengono *tutte* le radici n -esime dell'unità. Questo però vale per una qualunque radice *primitiva* n -esima, cioè ogni radice n -esima primitiva dell'unità genera tutte le radici n -esime dell'unità. \square

Consideriamo ora il polinomio

$$\Phi_n(x) = (x - \zeta_1)(x - \zeta_2) \cdots (x - \zeta_{\varphi(n)})$$

dove $\zeta_1, \zeta_2, \dots, \zeta_{\varphi(n)}$ sono le $\varphi(n)$ radici n -esime *primitive* dell'unità. Esso prende il nome di *n -esimo polinomio ciclotomico*. È ovvio che il grado di Φ_n è $\varphi(n)$. Ora, dato che ogni radice dell'unità si può ottenere elevando ad una opportuna potenza una radice primitiva, ogni ζ_i , $i = 1, \dots, \varphi(n)$, che compare nell' n -esimo polinomio ciclotomico sarà del tipo ζ^i , per i tale che $1 \leq i < n$ e $(n, i) = 1$, per una opportuna radice n -esima primitiva ζ dell'unità. Inoltre, per ogni divisore d di n esiste una radice n -esima che ha d come ordine (basta considerare $\zeta^{n/d}$: cfr. esercizio 3.4.3). Ogni radice n -esima dell'unità è quindi una radice d -esima primitiva dell'unità, dove d è il suo ordine, e tale ordine divide n (cfr. lemma 3.4.2). Radunando tutte le radici n -esime dell'unità a seconda del loro ordine d , e indicando con $\Phi_d(x)$ il polinomio ciclotomico d -esimo (le cui radici sono tutte e sole le radici d -esime primitive dell'unità), il polinomio $x^n - 1$, le cui radici sono tutte le radici n -esime dell'unità, si fattorizzerà al modo seguente:

$$(3.4.4) \quad x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Da tale relazione risulta intanto che

$$n = \sum_{d|n} \varphi(d),$$

che è una proprietà della funzione di Eulero che si può dimostrare direttamente, senza far ricorso ai polinomi ciclotomici (cfr. esercizio 2.8.1). La (3.4.4) si può anche scrivere

$$x^n - 1 = \Phi_1(x) \prod_{\substack{d|n \\ d \neq 1 \\ d \neq n}} \Phi_d(x) \Phi_n(x)$$

che ci dà un modo per calcolare il polinomio ciclotomico n -esimo in funzione dei precedenti, perché

$$\Phi_n = \frac{x^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d}.$$

Utilizzando questo metodo induttivo, calcoliamo i primi polinomi ciclotomici.

3.4.8 CALCOLO DEI PRIMI POLINOMI CICLOTOMICI.

$$\Phi_1(x) = x - 1$$

$$\Phi_2(x) = \frac{x^2 - 1}{\Phi_1(x)} = x + 1$$

$$\Phi_3(x) = \frac{x^3 - 1}{\Phi_1(x)} = x^2 + x + 1$$

$$\Phi_4(x) = \frac{x^4 - 1}{\Phi_1(x)\Phi_2(x)} = \frac{x^4 - 1}{(x - 1)(x + 1)} = x^2 + 1$$

$$\Phi_5(x) = \frac{x^5 - 1}{\Phi_1(x)} = x^4 + x^3 + x^2 + x + 1$$

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = \frac{x^6 - 1}{(x - 1)(x + 1)(x^2 + x + 1)} = x^2 - x + 1$$

$$\Phi_7(x) = \frac{x^7 - 1}{\Phi_1(x)} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\Phi_8(x) = \frac{x^8 - 1}{\Phi_1(x)\Phi_2(x)\Phi_4(x)} = \frac{x^8 - 1}{(x - 1)(x + 1)(x^2 + 1)} = x^4 - 1$$

$$\Phi_9(x) = \frac{x^9 - 1}{\Phi_1(x)\Phi_3(x)} = x^8 + x^7 + 1.$$

In generale, se p è primo,

$$\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-2} + x^{p-1}.$$

Inoltre, per $n = p^h$, p numero primo,

$$\Phi_{p^h} = 1 + x^{p^{h-1}} + \cdots + (x^{p^{h-1}})^{p-1}.$$

Infatti

$$x^{p^h} - 1 = \Phi_1 \Phi_p \Phi_{p^2} \cdots \Phi_{p^{h-1}} \Phi_{p^h}$$

da cui

$$\Phi_{p^h} = \frac{x^{p^h} - 1}{\Phi_1 \Phi_p \Phi_{p^2} \cdots \Phi_{p^{h-1}}} = \frac{x^{p^h} - 1}{x^{p^{h-1}} - 1} = 1 + x^{p^{h-1}} + \cdots + (x^{p^{h-1}})^{p-1}.$$

3.4.9 PROPOSIZIONE. I polinomi ciclotomici sono tali che

- (a) ogni $\Phi_n(x)$ è monico e a coefficienti in \mathbb{Z} ;
- (b) il grado di $\Phi_n(x)$ è $\varphi(n)$;
- (c) ogni $\Phi_n(x)$ è irriducibile su \mathbb{Q} .

Dimostrazione. (a) Si procede per induzione su n . Per $n = 1$, $\Phi_1(x) = x - 1$ che è monico e a coefficienti interi. Supponiamo vero il risultato per i $\Phi_m(x)$ con $m < n$ e dimostriamolo per $\Phi_n(x)$. Risulta

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)}.$$

Ora, facendo la divisione di $x^n - 1$ per $\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)$, si ottiene un polinomio monico e a coefficienti interi, in quanto stiamo dividendo due polinomi monici e a coefficienti interi.

(b) Deriva dalla costruzione di $\Phi_n(x)$.

(c) Dimostreremo questo punto solo nel caso in cui $n = p^h$, con p numero primo. Come abbiamo visto, risulta

$$\Phi_{p^h}(x) = 1 + x^{p^{h-1}} + \cdots + (x^{p^{h-1}})^{p-1} = \frac{x^{p^h} - 1}{x^{p^{h-1}} - 1}.$$

Per dimostrare la irriducibilità di $\Phi_{p^h}(x)$ non si può applicare direttamente il criterio di Eisenstein. Proviamo a fare la sostituzione $x = y + 1$. Si ottiene il nuovo polinomio in y

$$\begin{aligned} \Psi(y) &= \Phi_{p^h}(y + 1) = 1 + (y + 1)^{p^{h-1}} + \cdots + ((y + 1)^{p^{h-1}})^{p-1} \\ &= \frac{(y + 1)^{p^h} - 1}{(y + 1)^{p^{h-1}} - 1} = \frac{y^{p^h} + pf(y)}{y^{p^{h-1}} + pg(y)}. \end{aligned}$$

Con l'ultima uguaglianza si sono svolti i calcoli sviluppando il binomio con la formula di Newton, e in $pf(y)$ e $pg(y)$ si sono radunati tutti gli addendi che risultano multipli di p . Risulta allora

$$[1 + (y+1)^{p^{k-1}} + \cdots + ((y+1)^{p^{k-1}})^{p-1}] [y^{p^k-1} - pg(y)] = y^{p^k} + pf(y)$$

da cui, separando i termini di grado massimo in ogni polinomio, si ottiene

$$(y^{p^{k-1}})^{p-1} - \underbrace{\sum_{\text{termini di grado più basso}} \alpha_i y^i}_{\sum \alpha_i y^i} [(y^{p^{k-1}} + pg(y)) - y^{p^k} - pf(y)]$$

Sviluppando i conti e radunando gli addendi che sono multipli di p , si ottiene

$$y^{p^k-1} \sum \alpha_i y^i + \underbrace{y^{p^{k-1}(p-1)} \cdot y^{p^{k-1}}}_{y^{p^k}} = y^{p^k} + p\bar{f}(y).$$

Ne risulta

$$y^{p^{k-1}} \sum \alpha_i y^i = p\bar{f}(y)$$

che ci assicura che tutti i coefficienti α_i diversi dal coefficiente direttivo (che è 1) del polinomio $\Psi(y)$ sono multipli di p . Per potere applicare il criterio di Eisenstein resta solo da provare che p^2 non divide il termine noto. Ma questo è vero, perché il termine noto di $\Psi(y)$ si ottiene ponendo $y=0$, e quindi uguaglia la somma di p addendi uguali ad 1, cioè è p .

Abbiamo così provato che $\Psi(y)$ è irriducibile, e pertanto anche Φ_{p^n} lo è. □

Il risultato appena dimostrato, che cioè i polinomi ciclotomici sono irriducibili su \mathbb{Q} , è utile per trovare la decomposizione in fattori irriducibili su \mathbb{Q} del polinomio $x^n - 1$. Infatti tale decomposizione è

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Dai primi esempi di polinomi ciclotomici appare anche che essi hanno tutti coefficienti 0 o ± 1 . Tuttavia questo fatto non è generale, nel senso che è vero fino a circa il centesimo polinomio ciclotomico, ma poi entrano in gioco anche altri coefficienti. Anzi, è stato dimostrato che esistono polinomi ciclotomici con coefficienti arbitrariamente grandi in valore assoluto.



ESERCIZI.

- Si provi che il prodotto di due radici n -esime dell'unità è ancora una radice n -esima dell'unità, e l'inverso di una radice n -esima dell'unità è una radice n -esima dell'unità.
- Si provi che, indicato con C_n l'insieme delle radici n -esime dell'unità, si può stabilire una corrispondenza biunivoca f tra C_n e \mathbb{Z}_n tale che $f(\zeta_1 \zeta_2) = f(\zeta_1) + f(\zeta_2)$ per ogni ζ_1 e ogni ζ_2 in C_n .

3. Si provi che per ogni $d|n$ esiste una radice d -esima dell'unità che ha come ordine d . Si contino, per ogni d , quante sono le radici n -esime che hanno uno stesso ordine d .
4. Si determini la fattorizzazione (unica) in fattori irriducibili su \mathbb{Q} dei seguenti polinomi:

$$x^{18} - 1, \quad x^{20} - 1, \quad x^{21} - 1, \quad x^{30} - 1.$$



ESERCIZI DI PROGRAMMAZIONE.

1. Si scriva un programma che calcoli per ogni n l'ordine di ogni radice n -esima dell'unità.
2. Scrivere un programma che calcoli l' n -esimo polinomio ciclotomico.
3. Scrivere un programma che determini tutti i fattori irriducibili su \mathbb{Q} del polinomio $x^n - 1$.



CONTROLLO.

1. Ordine di una radice n -esima dell'unità è ...
2. Una radice n -esima primitiva è ...
3. Definire i polinomi ciclotomici.
4. Sapreste utilizzare i polinomi ciclotomici per trovare la fattorizzazione in irriducibili su \mathbb{Q} di polinomi del tipo $x^n - 1$?

3.5. L'equazione di terzo grado e la formula di Cardano

Sappiamo che esiste una formula risolutiva per la equazione di secondo grado

$$ax^2 + bx + c = 0,$$

con a, b, c in un campo contenente i razionali, una formula cioè che esprima le radici dell'equazione in funzione dei suoi coefficienti attraverso operazioni razionali ed estrazioni di radici; essa è data da

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Vogliamo ora dare la formula risolutiva per le equazioni di terzo grado con coefficienti nel campo complesso. Esamineremo poi tale formula risolutiva nel caso di equazione a coefficienti reali, per avere informazioni sulla natura delle sue radici.

Partiamo dall'equazione di terzo grado:

$$(3.5.1) \quad x^3 + ax^2 + bx + c = 0.$$

Operando la trasformazione $x = y - a/3$, la (3.5.1) diventa

$$\left(y - \frac{a}{3}\right)^3 + a\left(y - \frac{a}{3}\right)^2 + b\left(y - \frac{a}{3}\right) + c = y^3 + \left(b - \frac{a^2}{3}\right)y + c - \frac{ab}{3} + \frac{2a^3}{27} = 0.$$

Quindi risolvere la (3.5.1) equivale a risolvere una equazione del tipo

$$(3.5.2) \quad \boxed{y^3 + px + q = 0}$$

dove

$$(3.5.3) \quad p = b - \frac{a^2}{3}, \quad q = c - \frac{ab}{3} - \frac{2a^3}{27}.$$

Si tratta di una equazione *incompleta*, nel senso che manca il termine di grado due.

Partiamo dall'identità

$$(u + v)^3 - 3uv(u + v) - u^3 - v^3 = 0.$$

Se riusciamo a trovare due numeri u e v tali che

$$(3.5.4) \quad -3uv = p, \quad -u^3 - v^3 = q,$$

allora il numero $u + v$ è soluzione della (3.5.2). Ora, le due condizioni (3.5.4) sono equivalenti alle

$$u^3v^3 = -\frac{p^3}{27}, \quad u^3 + v^3 = -q.$$

Quindi u^3 e v^3 sono radici dell'equazione di secondo grado

$$x^2 + qx + \frac{p^3}{27} = 0$$

le cui radici sono

$$-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Quindi

$$(3.5.5) \quad u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

e

$$(3.5.6) \quad v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Indicate con u_1, u_2, u_3 (rispettivamente v_1, v_2, v_3) le radici cubiche soluzioni di (3.5.5) (rispettivamente (3.5.6)), risulterà

$$u_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad u_2 = \omega u_1, \quad u_3 = \omega^2 u_1$$

$$v_1 = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad v_2 = \omega v_1, \quad v_3 = \omega^2 v_1$$

con ω radice primitiva terza dell'unità, $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i$, $\omega^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{3}i$. Le radici dell'equazione $y^3 + px + q = 0$ sono quindi date dalla seguente formula, detta *formula di Cardano*, che le esprime, attraverso operazioni razionali ed estrazioni di radici quadrate e cubiche, in funzione dei coefficienti

$$(3.5.7) \quad y = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

indicando con u e v una qualunque delle radici cubiche di (3.5.5) e (3.5.6) rispettivamente. Sembra quindi che, dato che u e v possono assumere ciascuno tre valori, $u + v$ possa assumere più di tre valori, a seconda di come si combinano u_1, u_2 e u_3 con v_1, v_2 e v_3 . Tuttavia si deve osservare che *non si possono scegliere i valori degli u indipendentemente da quelli di v* : infatti, per ogni scelta di u si è obbligati a scegliere quello tra i valori di v che verifica la (3.5.4), in particolare $uv = -p/3$. Sia u_1 uno dei tre valori di u , e sia v_1 il valore corrispondente, tale cioè che $u_1 v_1 = -p/3$. Allora il valore di v corrispondente a u_2 è v_3 , perché

$$u_2 v_3 = u_1 \omega \cdot v_1 \omega^2 = u_1 v_1 \omega^3 = u_1 v_1 = -\frac{p}{3}.$$

mentre per ogni altra scelta non si ottiene il risultato voluto, ad esempio

$$u_2 v_2 = u_1 \omega v_1 \omega = u_1 v_1 \omega^2 = -\frac{p}{3} \omega^2 \neq -\frac{p}{3}.$$

Analogamente, il valore di v da associare ad u_3 è v_2 . Le tre radici dell'equazione incompleta sono pertanto

$$\boxed{y_1 = u_1 + v_1, \quad y_2 = u_1 \omega + v_1 \omega^2, \quad y_3 = u_1 \omega^2 + v_1 \omega}.$$

3.5.1 EQUAZIONI DI TERZO GRADO A COEFFICIENTI REALI. Vogliamo ora vedere se la formula di Cardano, nel caso in cui l'equazione sia a coefficienti reali, ci fornisce informazioni sulla natura delle radici. In questo caso sarà essenziale il ruolo del segno dell'espressione

$$\frac{q^2}{4} + \frac{p^3}{27}$$

che compare sotto un segno di radice quadrata (si ricordi che p e q sono reali nelle nostre ipotesi attuali). Indichiamo con Δ l'espressione

$$\boxed{\Delta = -4p^3 - 27q^2 = -108 \left(\frac{q^2}{4} + \frac{p^3}{27} \right)}.$$

Δ prende il nome di *discriminante* dell'equazione $x^3 + px + q = 0$, ed il suo segno è opposto al segno di $q^2/4 + p^3/27$.

Esaminiamo i tre casi possibili, avendo sempre sott'occhio la formula di Cardano (3.5.7).

$\Delta < 0$. In questo caso l'espressione sotto la radice quadrata è positiva, quindi dovremo estrarre la radice cubica di un numero reale, ed è noto che la radice cubica di un numero reale ha due valori che sono complessi coniugati ed uno reale. Indicata con u_1 la radice cubica reale, il valore corrispondente v_1 sarà anch'esso reale, perché deve essere $u_1 v_1 = -p/3 \in \mathbb{R}$, quindi $u_1 - v_1$ è reale e pertanto la prima soluzione dell'equazione incompleta è reale. Le altre due radici sono

$$\begin{aligned} y_2 &= u_1\omega + v_1\omega^2 = u_1\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) + v_1\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) \\ &= -\frac{u_1 + v_1}{2} + i\sqrt{3}\frac{u_1 - v_1}{2} \\ y_3 &= u_1\omega^2 + v_1\omega = \dots = -\frac{u_1 + v_1}{2} - i\sqrt{3}\frac{u_1 - v_1}{2} \end{aligned}$$

cioè sono complesse coniugate (e non reali).

Concludendo, in questo caso si hanno *una radice reale e due complesse coniugate*.

$\Delta = 0$. In questo caso

$$u = \sqrt[3]{-\frac{q}{2}}, \quad v = \sqrt[3]{-\frac{q}{2}}.$$

Se u_1 è il valore reale della radice cubica, il corrispondente v_1 è anch'esso reale (perché $u_1 v_1 = -p/3$) e risulta $u_1 = v_1$. Le radici sono

$$y_1 = u_1 + v_1 = 2u_1 \quad y_2 = u_1(\omega + \omega^2) = -u_1 \quad y_3 = u_1(\omega^2 + \omega) = -u_1.$$

Quindi *tutte e tre le radici sono reali e due sono coincidenti*.

$\Delta > 0$. In questo caso l'espressione sotto il segno di radice quadrata è negativa, quindi si tratta di estrarre radici cubiche di un numero complesso, che sono numeri complessi. Quindi *tutti* i valori di u e di v sono numeri complessi (stiamo dicendo i valori di u e v , *non* le radici $u + v$ dell'equazione). Esaminiamo l'equazione incompleta: in quanto equazione di terzo grado a coefficienti reali, *dove* avere una radice reale: supponiamo che sia $y_1 = u_1 + v_1$. Allora u_1 e v_1 sono complessi coniugati, dato che sia la loro somma, sia il loro prodotto sono

numeri reali. Analogamente saranno complessi coniugati anche $u_1\omega$ con $v_1\omega^2$, e $u_1\omega^2$ con $v_1\omega$. Quindi $y_1 = u_1 + v_1$, $y_2 = u_1\omega + v_1\omega^2$ e $y_3 = u_1\omega^2 + v_1\omega$ sono tutte reali e distinte: che siano distinte segue dal fatto che se per assurdo fosse ad esempio $y_2 = y_3$, si avrebbe $u_1(\omega - \omega^2) = v_1(\omega - \omega^2)$, che comporterebbe $u_1 = v_1$, che è palesemente assurdo perché avevamo visto che erano complessi e coniugati tra di loro. Quindi in questo caso le radici sono reali e distinte.

Vale la pena di soffermarci su quest'ultimo caso. Siamo studiando il caso di una equazione di terzo grado *a coefficienti reali e con tutte radici reali*. Tuttavia, la risoluzione di questa equazione attraverso la formula di Cardano ci porta necessariamente alla estrazione di radici cubiche di numeri complessi, che sappiamo risolvere, ma attraverso la rappresentazione del numero complesso in forma trigonometrica. Ciò significa che l'utilità pratica della formula di Cardano è scarsa. Il caso $\Delta > 0$ prende il nome di *casus irreducibilis*, perché non si riesce ad esprimere le radici in funzione dei coefficienti con estrazioni di radici reali.

3.5.2 ESEMPIO. Si consideri l'equazione di terzo grado a coefficienti reali:

$$x^3 - 7x - 6 = 0.$$

È facile vedere (utilizzando il metodo delle radici razionali) che ha come radici -1 , -2 e 3 . Supponiamo però di voler trovare queste radici utilizzando la formula di Cardano. L'equazione è già in forma ridotta, perché manca il termine di secondo grado. Si ha $p = -7$ e $q = -6$. La formula di Cardano ci dà come radici le

$$\sqrt[3]{3 + \sqrt{\frac{36}{4} - \frac{343}{27}}} + \sqrt[3]{3 - \sqrt{\frac{36}{4} - \frac{343}{27}}} = \sqrt[3]{3 + \sqrt{-\frac{100}{27}}} + \sqrt[3]{3 - \sqrt{-\frac{100}{27}}}.$$

Quindi, per risolvere questa equazione e trovare le tre radici, occorre estrarre delle radici cubiche di numeri complessi, cosa fattibile, ma certo non delle più immediate.

Riassumendo:

Studio delle radici di $y^3 + py + q = 0$, $p, q \in \mathbb{R}$:

$$\Delta = -4p^3 - 27q^2 \quad \begin{cases} \Delta < 0 \Rightarrow \text{una reale e due complesse coniugate} \\ \Delta = 0 \Rightarrow \text{tutte reali e due coincidenti} \\ \Delta > 0 \Rightarrow \text{tre reali e distinte} \end{cases}.$$

3.5.3 EQUAZIONI DI QUARTO GRADO. Esiste una formula risolutiva anche per equazioni di quarto grado. La diamo per completezza, anche se non ha una grande utilità pratica.

Partiamo da un'arbitraria equazione di quarto grado:

$$(3.5.8) \quad x^4 + ax^3 + bx^2 + cx + d = 0.$$

Con la sostituzione $x = y - a/4$ la (3.5.8) diventa

$$(3.5.9) \quad y^4 + py^2 + qy + r = 0$$

che è un'equazione di quarto grado priva di termine di terzo grado. Ora, se $q = 0$, si tratta di un'equazione biquadratica, che si sa risolvere. Supponiamo quindi $q \neq 0$. Possiamo riscrivere la (3.5.9) nella forma

$$\left(y^2 + \frac{p}{2}\right)^2 = -qy - r + \left(\frac{p}{2}\right)^2.$$

Aggiungendo un termine v all'interno del quadrato di sinistra, la precedente relazione diventa

$$(3.5.10) \quad \left(y^2 + \frac{p}{2} + v\right)^2 = -qy - r + \left(\frac{p}{2}\right)^2 + v^2 + 2vy^2 + pv.$$

Scegliendo il parametro v in modo tale che il secondo membro della (3.5.10) sia il quadrato di un polinomio lineare, ossia imponendo che risulti

$$(3.5.11) \quad q^2 - 8v \left(v^2 + pv - r + \frac{p^2}{4}\right) = 0,$$

con qualche artificio che omettiamo si ottengono le quattro soluzioni

$$y = \varepsilon \sqrt{\frac{v_0}{2}} + \sqrt{-\frac{v_0}{2} - \frac{p}{2} - \frac{\varepsilon q}{2\sqrt{2v_0}}}, \quad \varepsilon = \pm 1$$

v_0 essendo una delle soluzioni dell'equazione cubica 3.5.11.

Non si può chiudere questo paragrafo senza fare almeno un cenno ad alcuni nomi che sono legati alla risoluzione di questi problemi. Si tratta dei seguenti algebristi italiani del '500: Girolamo Cardano, Nicolò Fontana (detto Tartaglia), Antonio Maria del Fiore, Scipione dal Ferro, Rafael Bombelli, Lodovico Ferrari. Per avere un'idea delle vicissitudini di queste formule si suggerisce la lettura di [8]. Ora, nonostante infiniti tentativi fatti dalla metà del secolo sedicesimo, analoghe formule non sono state trovate per equazioni di quinto grado e oltre. Il motivo di ciò divenne chiaro solamente il secolo scorso, quando fu provata la *impossibilità* di trovare una formula generale per risolvere equazioni di grado maggiore o uguale a cinque. Tratteremo questo problema nell'ultima parte del corso.



ESERCIZI DI PROGRAMMAZIONE.

1. Scrivere un programma che determini tutti i tipi di radici di un polinomio di terzo grado a coefficienti reali (dall'esame del discriminante dell'equazione ridotta).

3.6. Polinomi simmetrici

Abbiamo introdotto l'anello dei polinomi in una indeterminata x a coefficienti in un campo \mathbb{K} , e lo abbiamo indicato con $\mathbb{K}[x]$. La definizione di anello di polinomi in una indeterminata si può estendere anche al caso in cui i coefficienti, anziché variare in un campo, varino in un anello commutativo, come ad esempio gli interi. Si parlerà in tal caso di anello dei polinomi *a coefficienti in un anello* R , e si indicherà tale anello con $R[x]$. Vedremo in seguito che le proprietà di un anello di polinomi sono diverse, a seconda che i coefficienti siano in un campo o in un anello commutativo. Per il momento ci basta avere la possibilità di definire un tale anello $R[x]$, perché questo ci permetterà di definire l'anello dei polinomi in più variabili commutative a coefficienti in un campo.

3.6.1 DEFINIZIONE. L'anello R_n dei *polinomi in n indeterminate a coefficienti nel campo \mathbb{K}* si definisce induttivamente al modo seguente:

$$R_1 \stackrel{\text{def}}{=} \mathbb{K}[x_1], \quad R_n \stackrel{\text{def}}{=} R_{n-1}[\mathbb{K}[x_n]].$$

Si scrive $R_n = \mathbb{K}[x_1, x_2, \dots, x_n]$. \square

In altre parole, un polinomio in n variabili si pensa come un polinomio in *una* variabile, con coefficienti nell'anello dei polinomi in $n - 1$ variabili. Un elemento di $\mathbb{K}[x, y] = (\mathbb{K}[x])[y]$ è quindi del tipo

$$\sum_{j=0}^n f_j y^j, \quad f_j \in \mathbb{K}[x].$$

Ad esempio, potrà essere il seguente:

$$\begin{aligned} \sum_{j=0}^2 \left(\sum_{i=0}^1 a_{ij} x^i \right) y^j &= (a_{00} + a_{10}x) + (a_{01} + a_{11}x)y + (a_{02} + a_{12}x)y^2 \\ &= a_{00} + a_{10}x + a_{01}y + a_{02}y^2 + a_{11}xy + a_{12}xy^2. \end{aligned}$$

In generale quindi gli elementi di $\mathbb{K}[x_1, x_2, \dots, x_n]$ si possono rappresentare nella forma

$$f(x_1, x_2, \dots, x_n) = \sum a_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}.$$

Due polinomi in n variabili sono *uguali* se hanno gli stessi coefficienti; inoltre si definiscono addizione e moltiplicazione di polinomi utilizzando le ordinarie leggi distributive e di elevamento a potenza. *Grado* nell'indeterminata x_i è l'esponente più alto con cui compare la x_i nel polinomio f . Dato il monomio

$$x_1^{h_1} x_2^{h_2} \cdots x_n^{h_n}$$

il *grado del monomio* è l'intero $h_1 + h_2 + \cdots + h_n$. Ebbene, si definisce *grado del polinomio* $f(x_1, x_2, \dots, x_n)$ il grado più alto dei suoi monomi. È chiaro che

un polinomio avrà in genere diversi monomi di grado massimo. È opportuno allora *ordinare* i termini (cioè i monomi) di un polinomio. L'ordinamento che si dà comunemente è l'*ordinamento lessicografico*, ossia l'ordine secondo cui sono disposte le parole nel dizionario: si definisce al modo seguente: siano

$$\alpha x_1^{h_1} x_2^{h_2} \cdots x_n^{h_n}, \quad \alpha \in \mathbb{K}, \quad h_i \geq 0$$

e

$$\beta x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}, \quad \beta \in \mathbb{K}, \quad k_i \geq 0$$

due monomi del polinomio $f(x_1, x_2, \dots, x_n)$. Ditemo che

$$\alpha x_1^{h_1} x_2^{h_2} \cdots x_n^{h_n} < \beta x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$$

se, indicato con m il minimo intero per cui $h_i \neq k_i$, risulta $h_m < k_m$. Ad esempio, si avrà, in $\mathbb{K}[x_1, x_2, x_3, x_4, x_5]$,

$$3x_1^3 x_2^6 x_3^1 x_4^1 x_5^2 < -5x_1^3 x_2^6 x_3^4 x_4^2 x_5^0.$$

Vogliamo ora studiare una classe importante di polinomi, che avrà molta importanza negli sviluppi futuri, cioè la classe dei polinomi *simmetrici*. Ricordando la definizione di permutazione (cfr. §1.6), si dà la seguente definizione.

3.6.2 DEFINIZIONE. Un polinomio $f(x_1, x_2, \dots, x_n) \in \mathbb{K}[x_1, x_2, \dots, x_n]$ si dice *simmetrico* se è *invariante*, ossia se resta lo stesso, se si opera una permutazione arbitraria delle indeterminate x_1, x_2, \dots, x_n . □

Ad esempio, i polinomi di $\mathbb{K}[x_1, x_2, x_3]$

$$\begin{aligned} 2x_1 + 2x_2 + 2x_3 - 3x_1^2 - 3x_2^2 - 3x_3^2, \\ x_1 x_2^3 + x_2 x_1^3 + x_1 x_3^3 + x_3 x_1^3 + x_2 x_3^3 + x_3 x_2^3 \end{aligned}$$

sono polinomi simmetrici, mentre non lo sono ad esempio

$$x_1^2 - x_2^2 + x_3^2, \quad x_1 + 2x_2 + 5x_3.$$

I seguenti polinomi simmetrici in n indeterminate x_1, x_2, \dots, x_n

$$\begin{aligned} \sigma_1(x_1, x_2, \dots, x_n) &= x_1 + x_2 + \cdots + x_n &= \sum_{i=1}^n x_i \\ \sigma_2(x_1, x_2, \dots, x_n) &= x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n &= \sum_{1 \leq i < j \leq n} x_i x_j \\ \sigma_3(x_1, x_2, \dots, x_n) &= x_1 x_2 x_3 + x_1 x_2 x_4 + \cdots + x_{n-2} x_{n-1} x_n &= \sum_{1 \leq i < j < k \leq n} x_i x_j x_k \\ &\vdots \\ \sigma_n(x_1, x_2, \dots, x_n) &= x_1 x_2 \cdots x_n \end{aligned}$$

prendono il nome di *polinomi simmetrici elementari o funzioni simmetriche elementari* in $\mathbb{K}[x_1, x_2, \dots, x_n]$. Tali funzioni legano i coefficienti e le radici di una equazione polinomiale in una variabile nel senso che andiamo a precisare.

Si consideri la seguente equazione polinomiale:

$$(3.6.1) \quad f(t) = t^n + a_1 t^{n-1} + a_2 t^{n-2} + \cdots + a_{n-1} t + a_n = 0.$$

Indicate con x_1, x_2, \dots, x_n le sue radici, si può scrivere

$$(3.6.2) \quad f(t) = (t - x_1)(t - x_2) \cdots (t - x_n).$$

Sviluppando i prodotti di quest'ultima equazione e confrontando i coefficienti di (3.6.1) e (3.6.2) si ottengono le seguenti relazioni:

$$a_1 = -(x_1 + x_2 + \cdots + x_n)$$

$$a_2 = x_1 x_2 + x_1 x_3 + \cdots + x_1 x_n + x_2 x_3 + \cdots + x_{n-1} x_n$$

$$a_3 = -(x_1 x_2 x_3 + x_1 x_2 x_4 + \cdots + x_{n-2} x_{n-1} x_n)$$

...

$$a_n = (-1)^n x_1 x_2 \cdots x_n.$$

Le relazioni sopra riportate prendono il nome di *formule di Viète*: esse esprimono i coefficienti di un polinomio in funzione delle sue radici. Per $n = 2$ si ritrovano le ben note relazioni che legano le radici di un'equazione di secondo grado ai coefficienti. In generale risulta $a_k = (-1)^k \sigma_k(x_1, x_2, \dots, x_n)$, cioè: i coefficienti di ogni polinomio monico in una indeterminata a coefficienti in un campo sono (a meno del segno) le funzioni simmetriche elementari delle sue radici.

Ora, l'insieme \mathbf{S} di tutti i polinomi simmetrici in n variabili a coefficienti in \mathbb{K} è un sottoanello di $\mathbb{K}[x_1, x_2, \dots, x_n]$ (cfr. esercizio 3.6.4). Ogni polinomio $f(\sigma_1, \sigma_2, \dots, \sigma_n)$ nelle funzioni simmetriche elementari è un polinomio che, rispetto alle indeterminate x_1, x_2, \dots, x_n , è simmetrico (cfr. esercizio 3.6.4), e in quanto tale è contenuto in \mathbf{S} . Si hanno pertanto le seguenti inclusioni:

$$\mathbb{K}[\sigma_1, \sigma_2, \dots, \sigma_n] \subseteq \mathbf{S} \subset \mathbb{K}[x_1, x_2, \dots, x_n].$$

Il teorema che segue mostra che la prima inclusione in realtà è una uguaglianza.

3.6.3 TEOREMA FONDAMENTALE SUI POLINOMI SIMMETRICI. *Ogni polinomio simmetrico $f(x_1, x_2, \dots, x_n)$ di $\mathbb{K}[x_1, x_2, \dots, x_n]$ si può scrivere in modo unico come polinomio a coefficienti in \mathbb{K} nei polinomi simmetrici elementari.*

Dimostrazione. Sia

$$(3.6.3) \quad \alpha x_1^{h_1} x_2^{h_2} \cdots x_n^{h_n}$$

il monomio massimo rispetto all'ordinamento lessicografico. Allora necessariamente risulta $h_1 \geq h_2 \geq \dots \geq h_n$: se infatti fosse ad esempio $h_1 < h_2$, allora, permutando x_1 con x_2 , il monomio dato si trasforma nel monomio

$$\alpha x_2^{h_1} x_1^{h_2} \cdots x_n^{h_n} = \alpha x_1^{h_2} x_2^{h_1} \cdots x_n^{h_n}$$

che è ancora un monomio di $f(x_1, x_2, \dots, x_n)$ essendo $f(x_1, x_2, \dots, x_n)$ per ipotesi simmetrico, più grande di (3.6.3) nell'ordinamento lessicografico, contro quanto supposto.

Consideriamo allora il polinomio (simmetrico in x_1, x_2, \dots, x_n)

$$\phi_1 = \alpha \sigma_1^{h_1-h_2} \sigma_2^{h_2-h_3} \cdots \sigma_{n-1}^{h_{n-1}-h_n} \sigma_n^{h_n}.$$

Il monomio massimo di ϕ_1 sarà dato dal prodotto di α per ciascuno dei monomi massimi di $\sigma_1, \sigma_2, \dots, \sigma_n$, elevati rispettivamente ad $h_1 - h_2, h_2 - h_3$, ecc., cioè

$$\alpha x_1^{h_1-h_2} (x_1 x_2)^{h_2-h_3} \cdots (x_1 x_2 \cdots x_n)^{h_n} = \alpha x_1^{h_1} x_2^{h_2} \cdots x_n^{h_n}$$

ossia esattamente il termine massimo di f . Ciò significa che il polinomio (ovviamente simmetrico) $f_1 = f - \phi_1$ avrà un monomio massimo più piccolo di quello di f , ossia di (3.6.3). A questo punto ripetiamo con il nuovo polinomio f_1 l'operazione fatta con f , ottenendo un nuovo polinomio f_2 il cui monomio massimo sarà minore del monomio massimo di f_1 , e così via. Tale procedimento termina sicuramente dopo un numero finito m di passi, quando si arriverà al polinomio nullo $f - \phi_1 - \phi_2 - \cdots - \phi_m$. Abbiamo così provato che

$$f = \phi_1 + \phi_2 + \cdots + \phi_m.$$

Dato che ogni ϕ_i è per costruzione un monomio nelle funzioni simmetriche elementari, la somma dei ϕ_i è un polinomio nelle funzioni simmetriche elementari.

Resta da provare l'unicità della scrittura. Dobbiamo provare che se un polinomio (simmetrico) ha due scritture

$$\sum \alpha_{i_1, i_2, \dots, i_n} \sigma_1^{i_1} \sigma_2^{i_2} \cdots \sigma_n^{i_n} = \sum \beta_{i_1, i_2, \dots, i_n} \sigma_1^{i_1} \sigma_2^{i_2} \cdots \sigma_n^{i_n}$$

allora $\alpha_{i_1, i_2, \dots, i_n} = \beta_{i_1, i_2, \dots, i_n}$ per tutti gli indici $i_j, j = 1, \dots, n$. Basta ovviamente provare che se $\varphi(\sigma_1, \dots, \sigma_n) = 0$, allora tutti i coefficienti di $\varphi(\sigma_1, \dots, \sigma_n)$ sono nulli, ossia il polinomio $\varphi(z_1, z_2, \dots, z_n)$ nelle indeterminate z_i è il polinomio nullo: questo equivale a dire che non esiste nessuna relazione polinomiale non nulla che lega le σ_i , ossia le σ_i sono algebricamente indipendenti. In altre parole, si tratta di provare che

$$\varphi(z_1, z_2, \dots, z_n) \neq 0 \quad \rightarrow \quad \varphi(\sigma_1, \dots, \sigma_n) \neq 0.$$

Sia $a z_1^{h_1} z_2^{h_2} \cdots z_n^{h_n}$ ($a \neq 0$) il monomio massimo (rispetto all'ordinamento lessicografico) di $\varphi(z_1, \dots, z_n)$. Ponendo $z_i = \sigma_i$ nel polinomio $\varphi(z_1, z_2, \dots, z_n)$ ed

espandendo in termini delle x_j ($j = 1, \dots, n$) (le σ_i sono funzioni delle x_j), il monomio $a\sigma_1^{h_1}\sigma_2^{h_2} \dots \sigma_n^{h_n}$ diventa il seguente polinomio (nelle x_i):

$$a\sigma_1^{h_1}\dots\sigma_n^{h_n} = a(x_1 + x_2 + \dots + x_n)^{h_1}(x_1x_2 + \dots)^{h_2} \dots (x_1 \dots x_n)^{h_n}.$$

Ora, il monomio massimo di tale polinomio è

$$ax_1^{h_1+h_2+\dots+h_n}x_2^{h_2+h_3+\dots+h_n}\dots x_n^{h_n}$$

che ha coefficiente diverso da zero e non potrà cancellarsi con nessun altro monomio. Quindi $\varphi(\sigma_1, \sigma_2, \dots, \sigma_n) \neq 0$. \square

Il teorema ora dimostrato asserisce che, indicato con S l'anello di tutti i polinomi simmetrici in n indeterminate, risulta

$$S = \mathbb{K}[\sigma_1, \sigma_2, \dots, \sigma_n].$$

3.6.4 ESEMPIO. Si scriva il polinomio simmetrico $\in \mathbb{K}[x_1, x_2, x_3]$

$$(3.6.4) \quad f = \sum_{i \neq j} x_i^2 x_j = x_1^2 x_2 + x_1^2 x_3 + x_2^2 x_1 + x_2^2 x_3 + x_3^2 x_1 + x_3^2 x_2$$

in termini dei polinomi simmetrici elementari σ_k .

Per semplificare le notazioni, indicheremo un monomio $x_1^{h_1}x_2^{h_2} \dots$ scrivendo solamente la successione $h_1 h_2 h_3 \dots$ degli esponenti corrispondenti rispettivamente a x_1, x_2, x_3, \dots . Quindi ad esempio il monomio $x_2^3 x_1^5 x_4^2 x_5 \dots$ verrà rappresentato dalla successione di interi 53021...

- (a) Monomio massimo di (3.6.4): $x_1^2 x_2$, cioè 210.
- (b) Polinomio $\phi_1: \sigma_1^{h_1-h_2} \dots = \sigma_1^{2-1} \sigma_2^{1-0} = \sigma_1 \sigma_2$.
- (c) $f_1 = f - \phi_1 = \underbrace{\sum_{i \neq j} x_i^2 x_j}_{=f} - \underbrace{(x_1 + x_2 + x_3)(x_1 x_2 + x_1 x_3 + x_2 x_3)}_{\sigma_1 \sigma_2}$

$$= \sum_{i \neq j} x_i^2 x_j - \sum_{i \neq j} x_i^2 x_j - 3(x_1 x_2 x_3).$$

- (d) Monomio massimo di $f_1 = -3x_1 x_2 x_3$ è $-3\sigma_3 = -3x_1 x_2 x_3$. Ora, $\phi_2 = -3\sigma_1^{1-1} \sigma_2^{1-1} \sigma_3^{1-0} = -3\sigma_3 = -3x_1 x_2 x_3$. $f_2 = f_1 - \phi_2 = -3x_1 x_2 x_3 + 3x_1 x_2 x_3 = 0$, quindi $f = f_1 + \phi_1 = \sigma_1 \sigma_2 + 3\sigma_3$, che è l'espressione voluta di f come *polinomio* nelle funzioni simmetriche elementari.

Si noti che già dalla fine del punto (b) avremmo potuto concludere che $f = \sigma_1 \sigma_2 + 3\sigma_3$, dato che il polinomio $f_1 = -3x_1 x_2 x_3$ si riconosceva subito essere $-3\sigma_3$. Tuttavia abbiamo preferito continuare fino in fondo come nella dimostrazione del teorema, per motivi didattici. \square

L'anello dei polinomi in n indeterminate a coefficienti in un campo \mathbb{K} è un dominio di integrità (esercizio 3.6.1). Nell'insieme delle coppie ordinate di

elementi di $\mathbb{K}[x_1, x_2, \dots, x_n] \times \mathbb{K}[x_1, x_2, \dots, x_n] \setminus \{0\}$ si definisca la seguente relazione (di equivalenza):

$$(f(x_1, x_2, \dots, x_n), g(x_1, x_2, \dots, x_n)) \varrho (f'(x_1, x_2, \dots, x_n), g'(x_1, x_2, \dots, x_n)) \iff f(x_1, x_2, \dots, x_n) \cdot g'(x_1, x_2, \dots, x_n) = f'(x_1, x_2, \dots, x_n) \cdot g(x_1, x_2, \dots, x_n).$$

Ebbene, si dà la seguente definizione.

3.6.5 DEFINIZIONE. Si definisce *funzione razionale* nelle n indeterminate x_1, x_2, \dots, x_n un elemento dell'insieme quoziente

$$\mathbb{K}(x_1, x_2, \dots, x_n) = (\mathbb{K}[x_1, x_2, \dots, x_n] \times \mathbb{K}[x_1, x_2, \dots, x_n] \setminus \{0\})/\varrho$$

e si indica al modo seguente:

$$\frac{f(x_1, x_2, \dots, x_n)}{g(x_1, x_2, \dots, x_n)}, \quad g(x_1, x_2, \dots, x_n) \neq 0. \quad \square$$

Se, come si è fatto quando si è definito il campo dei numeri razionali, si introducono in $\mathbb{K}(x_1, x_2, \dots, x_n)$ le seguenti due operazioni:

$$\begin{aligned} \frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)} + \frac{h(x_1, \dots, x_n)}{k(x_1, \dots, x_n)} &= \frac{f(x_1, \dots, x_n)k(x_1, \dots, x_n) + g(x_1, \dots, x_n)h(x_1, \dots, x_n)}{k(x_1, \dots, x_n)g(x_1, \dots, x_n)} \\ \frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)} \frac{h(x_1, \dots, x_n)}{k(x_1, \dots, x_n)} &\stackrel{\text{def}}{=} \frac{f(x_1, \dots, x_n)h(x_1, \dots, x_n)}{g(x_1, \dots, x_n)k(x_1, \dots, x_n)}. \end{aligned}$$

L'insieme $\mathbb{K}(x_1, x_2, \dots, x_n)$ diventa un campo, che è il campo dei quozienti dell'anello $\mathbb{K}[x_1, x_2, \dots, x_n]$ (cfr. §2.4) (per i dettagli si veda l'esercizio 3.6.5).

3.6.6 DEFINIZIONE. Una *funzione razionale simmetrica* è una funzione razionale che è invariante rispetto ad ogni permutazione delle indeterminate. \square

Tale definizione è ben posta, nel senso che non dipende dal particolare rappresentante della classe di equivalenza (cfr. esercizio 3.6.8).

Ebbene, il teorema fondamentale sui polinomi simmetrici si estende anche alle funzioni razionali.

3.6.7 TEOREMA FONDAMENTALE SULLE FUNZIONI RAZIONALI SIMMETRICHE. Ogni funzione razionale simmetrica nelle indeterminate x_1, x_2, \dots, x_n a coefficienti in un campo \mathbb{K} si può rappresentare sotto forma di funzione razionale nei polinomi simmetrici elementari $\sigma_1, \sigma_2, \dots, \sigma_n$ a coefficienti in \mathbb{K} .

Dimostrazione. Sia

$$\frac{f(x_1, x_2, \dots, x_n)}{g(x_1, x_2, \dots, x_n)}, \quad g(x_1, x_2, \dots, x_n) \neq 0$$

una funzione razionale simmetrica in x_1, x_2, \dots, x_n . Se dimostriamo che la simmetria della funzione razionale comporta la simmetria di \bar{f}, \bar{g} , per opportuni polinomi \bar{f}, \bar{g} , con (\bar{f}, \bar{g}) equivalente a (f, g) , avremo dimostrato il teorema, perché basta allora esprimere numeratore e denominatore come polinomi nelle funzioni simmetriche elementari, in virtù del teorema fondamentale sui *polinomi simmetrici*. Moltiplichiamo numeratore e denominatore della frazione per il prodotto degli $n! - 1$ polinomi ottenuti da g operando sulle indeterminate con tutte le permutazioni possibili ad eccezione della permutazione identica. La funzione razionale ottenuta è equivalente alla funzione razionale di partenza, e il denominatore è chiaramente un polinomio simmetrico. Ma allora, data la simmetria della funzione razionale, sarà simmetrico anche il numeratore. \square

L'insieme \tilde{S} di tutte le funzioni razionali simmetriche a coefficienti nel campo K nelle indeterminate x_1, x_2, \dots, x_n costituisce un *campo* (contenuto in $K(x_1, x_2, \dots, x_n)$). Abbiamo appena dimostrato che

$$\tilde{S} = K(\sigma_1, \sigma_2, \dots, \sigma_n).$$



ESERCIZI.

- Si provi che l'anello $K[x_1, x_2, \dots, x_n]$, con K campo, è un dominio di integrità.
- Esprimere, se possibile, i seguenti polinomi nelle tre indeterminate x_1, x_2, x_3

$$\begin{aligned} &x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 \\ &x_1^3 + x_2^3 + x_3^3 + x_2^2 + x_3^2 + x_1^2 \\ &x_1^2 + x_2^2 + x_3^2 \\ &x_1^2 x_2^2 + x_1^2 x_3^2 + x_2^2 x_3^2 \end{aligned}$$

come polinomi nelle funzioni simmetriche elementari.

- Sia $f(x)$ il polinomio $x^3 + 3x^2 - 6x + 3$. Dette $\alpha_1, \alpha_2, \alpha_3$ le tre radici di $f(x)$, si determini il polinomio monico che ha come radici $1/\alpha_1^2, 1/\alpha_2^2, 1/\alpha_3^2$ e il polinomio monico che ha come radici $\alpha_1^2, \alpha_2^2, \alpha_3^2$. Si osservi che le radici α_i non sono note.
- Si provi che l'insieme S di tutti i polinomi simmetrici a coefficienti in un campo K , nelle indeterminate x_1, x_2, \dots, x_n , costituisce un sottoanello di $K[x_1, x_2, \dots, x_n]$ e che ogni polinomio nelle funzioni simmetriche elementari è un elemento di S .
- Si provi nei dettagli che $K(x_1, x_2, \dots, x_n)$, rispetto alle operazioni definite nel testo, è un campo, che è il campo dei quozienti di $K[x_1, x_2, \dots, x_n]$.

6. Si dica se è possibile esprimere la funzione razionale

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{x}$$

come funzione razionale nelle funzioni simmetriche elementari. In caso positivo si determini una tale funzione.

7. Si provi che il sottoinsieme \tilde{S} di $\mathbb{K}(x_1, x_2, \dots, x_n)$ delle funzioni razionali simmetriche è un campo.
8. Si provi che se f/g è simmetrica, allora ogni funzione razionale ad essa equivalente è simmetrica.
9. Sia $f(x) \in \mathbb{K}[x]$ un polinomio a coefficienti in un campo \mathbb{K} , di grado n . Siano $\alpha_1, \alpha_2, \dots, \alpha_n$ le radici (non necessariamente appartenenti a \mathbb{K}) di $f(x)$. Detto Ψ un qualunque polinomio simmetrico in n variabili, a coefficienti in \mathbb{K} , si provi che l'elemento $\Psi(\alpha_1, \alpha_2, \dots, \alpha_n)$ sta in \mathbb{K} .
10. Si provi che il seguente polinomio

$$\Delta(x_1, x_2, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2$$

è un polinomio simmetrico. Esso prende il nome di *discriminante* di x_1, x_2, \dots, x_n . Si esprimano $\Delta(x_1, x_2)$ e $\Delta(x_1, x_2, x_3)$ come polinomi nelle funzioni simmetriche elementari. Si confronti l'espressione di $\Delta(x_1, x_2, x_3)$ come polinomio nelle funzioni simmetriche elementari con il discriminante dell'equazione cubica $x^3 + px + q = 0$ studiata in 3.5.1, e l'espressione di $\Delta(x_1, x_2)$ con l'ordinario discriminante di un'equazione polinomiale di secondo grado.



ESERCIZI DI PROGRAMMAZIONE.

1. Fare un programma che controlli se un polinomio in n indeterminate è simmetrico e che, in caso positivo, lo esprima come polinomio nelle funzioni simmetriche elementari.



CONTROLLO.

1. Definire il grado di un polinomio di n variabili.
2. L'ordinamento lessicografico tra monomi è ...
3. C'è un legame tra le funzioni simmetriche elementari di n variabili e le radici di un polinomio monico di grado n in una indeterminata?
4. Enunciare e spiegare il teorema fondamentale sui polinomi simmetrici.

CAPITOLO 4

Gli anelli

*Che per un uomo il meglio è certo nascere
pien di saggezza, ma tal sorte è rara,
e bello è pur dà chi ben dice apprendere.*
Sofocle, Antigone.

Nei due capitoli precedenti abbiamo studiato gli interi, i polinomi in una o più indeterminate, le classi resto modulo un intero n : tali insiemî sono tutti esempi di anelli. In questo capitolo studieremo gli anelli (commutativi) generali, nel senso che dalla loro definizione assiomatica dedurremo varie proprietà che hanno quindi validità generale. Come esempi guida è sempre bene tener presenti gli anelli studiati nei capitoli precedenti.

4.1. Prime definizioni ed esempi

Partiamo dalla definizione *assiomatica* di anello.

4.1.1 DEFINIZIONE. Un anello $(R, +, \cdot)$ è un insieme dotato di due operazioni binarie, indicate con $+$ e \cdot ,

$$\begin{array}{ccc} R \times R \longrightarrow R & & R \times R \longrightarrow R \\ (a, b) \mapsto a + b & & (a, b) \mapsto a \cdot b \end{array}$$

che prendono il nome di *addizione* e *moltiplicazione*, tali che valgano le seguenti condizioni:

- (i) (a) $+$ è *associativa*, ossia $(a + b) + c = a + (b + c) \forall a, b, c \in R$;
- (b) esiste un elemento 0 che è *neutro* rispetto a $+$, ossia $a + 0 = 0 + a = a \forall a \in R$;
- (c) $\forall a \in R$ esiste un elemento, $-a$, tale che $a + (-a) = 0$ (*esistenza dell'opposto*);
- (d) $+$ è *commutativa*, ossia $a + b = b + a \forall a, b \in R$:

- (ii) · è *associativa*, cioè $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R$;
 (iii) valgono le seguenti leggi *distributive*:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c \quad \forall a, b, c \in R.$$

D'ora in poi in genere scriveremo ab invece di $a \cdot b$.

Un insieme dotato di un'operazione che gode di (a), (b) e (c) prende il nome di *gruppo*: quindi $(R, +)$ è un gruppo. Il punto (d) dice che il gruppo è *abeliano* cioè *commutativo*. Parleremo spesso di $(R, +)$ come del *gruppo additivo* dell'anello. Nella seconda parte del corso parleremo di gruppi *generali* (ossia senza la richiesta che siano abeliani).

Un anello in cui la *moltiplicazione* sia commutativa prende il nome di *anello commutativo*. □

4.1.2 ESEMPI DI ANELLI.

- (a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ rispetto alle ordinarie operazioni di addizione e moltiplicazione.
- (b) $K[x]$ e $K[x_1, x_2, \dots, x_n]$ rispetto alle operazioni di addizione e moltiplicazione definite nel §3.1.
- (c) L'insieme \mathbb{Z}_n delle classi resto modulo n , rispetto alle operazioni definite nel §2.6.
- (d) L'insieme $M_n(K)$ delle matrici quadrate $n \times n$ sopra un campo K , o sopra un anello (ad esempio gli interi), rispetto alle ordinarie definizioni di addizione elemento per elemento e moltiplicazione righe per colonne.
- (e) Sia X un insieme e $\mathcal{P}(X)$ sia l'insieme delle parti di X . Definiamo in $\mathcal{P}(X)$ le seguenti due operazioni:

$$A + B \stackrel{\text{def}}{=} (A \cup B) \cap \bar{U}(A \cap B), \quad A \cdot B \stackrel{\text{def}}{=} A \cap B.$$

È facile vedere che si tratta di un gruppo abeliano rispetto alla prima operazione (elemento neutro è \emptyset e l'opposto di un $A \in \mathcal{P}(X)$ è l'elemento \bar{A} stesso). Anche la seconda operazione è associativa, e valgono inoltre le proprietà distributive, per cui si tratta di un anello (commutativo). In questo anello ogni elemento è *idempotente*, cioè $A^2 = A \cdot A = A$ per ogni $A \in \mathcal{P}(X)$.

- (f) Sia R un anello e X un arbitrario insieme non vuoto. Nell'insieme

$$R^X \stackrel{\text{def}}{=} \{f : X \rightarrow R\}$$

si definiscono le seguenti operazioni:

$$(f + g)(x) \stackrel{\text{def}}{=} f(x) + g(x), \quad (fg)(x) \stackrel{\text{def}}{=} f(x)g(x)$$

$\forall f, g \in R^X, \forall x \in X; (R^X, +, \cdot)$ diventa un anello: è un anello commutativo se e solo se R è commutativo, è unitario se e solo se R è unitario (la funzione unità è quella che manda ogni elemento di X nell'unità di R).

- (g) Siano R_1 e R_2 due anelli. Nel prodotto cartesiano $R_1 \times R_2$ si definiscono le seguenti operazioni:

$$(a_1, a_2) + (b_1, b_2) \stackrel{\text{def}}{=} (a_1 + b_1, a_2 + b_2)$$

$$(a_1, a_2) \cdot (b_1, b_2) \stackrel{\text{def}}{=} (a_1 b_1, a_2 b_2).$$

L'insieme $R_1 \times R_2$ con queste due operazioni diventa un anello che prende il nome di *prodotto cartesiano* di R_1 e R_2 . Spesso si indica al modo seguente:

$$R_1 \oplus R_2$$

e si chiama *somma diretta* di R_1 e R_2 . La definizione ora data può estendersi al prodotto cartesiano di n anelli. \square

Un anello finito può essere visualizzato attraverso le sue tavolette additive e moltiplicative, come si è visto in §2.6 nel caso dell'anello delle classi resto modulo 4 e modulo 5.

Dagli assiomi di anello si deducono le seguenti proprietà, che non dimostriamo, perché sono state già dimostrate quando abbiamo trattato degli interi: si controlli che nella dimostrazione di allora non è stato utilizzato il fatto che gli elementi fossero degli interi, ma si sono utilizzate solo le proprietà formali:

$$a \cdot 0 = 0 \cdot a = 0 \quad \forall a \in R$$

$$(-a)b = a(-b) = -(ab) \quad \forall a, b \in R.$$

Diamo la seguente fondamentale definizione.

4.1.3 DEFINIZIONE. Un *isomorfismo* φ tra due anelli R e R' è una corrispondenza biunivoca tra R e R' che conserva le operazioni, tale cioè che

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \forall a, b \in R$$

e

$$\varphi(ab) = \varphi(a)\varphi(b) \quad \forall a, b \in R.$$

La figura 4.1 mostra cosa significhi *conservare le operazioni*.

Due anelli R e R' tra i quali si possa determinare un isomorfismo si dicono *isomorfi*, e si scrive

$$\boxed{R \simeq R'}.$$

La relazione di *essere isomorfi* è una relazione di equivalenza. Ora, una qualunque proprietà algebrica che valga in R si trasporta in R' , e viceversa, per la

biunivocità, cioè R e R' godono delle stesse proprietà (algebriche), e quindi dal punto di vista algebrico sono indistinguibili: considereremo quindi uguali due anelli isomorfi. Quando studieremo un anello, lo penseremo assieme a tutti gli anelli ad esso isomorfi, ossia guarderemo alla sua classe di isomorfismo. Questo è un fatto generale in algebra, quando si parla di strutture algebriche.

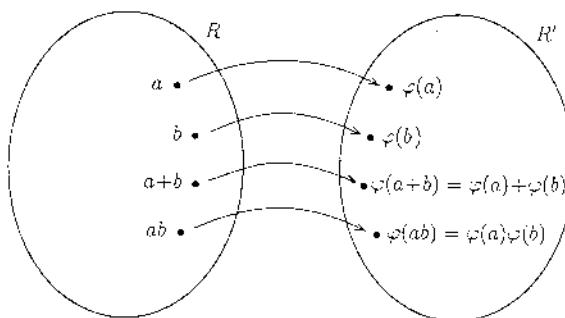


FIGURA 4.1

4.1.4 ESEMPI DI ISOMORFISMI TRA ANELLI.

- (a) L'identificazione tra polinomi a coefficienti in un campo \mathbb{K} e le successioni infinite di elementi di \mathbb{K} soddisfacenti la condizione che da un certo punto in poi i loro elementi sono tutti uguali a zero (cfr. definizione 3.1.5) stabilisce un isomorfismo tra l'anello $\mathbb{K}[x]$ e l'anello di tali successioni (con le operazioni definite allora).
- (b) L'applicazione da \mathbb{C} in \mathbb{C} che manda ogni numero complesso z nel suo coniugato \bar{z} è un isomorfismo di \mathbb{C} in sé. \square

Abbiamo già visto che esistono delle proprietà ulteriori che si possono aggiungere alla definizione di anello (senza che però siano obbligatorie). Le raccolgiamo in un elenco per comodità:

- (1) un anello si dice *commutativo* se vale la proprietà commutativa della moltiplicazione;
- (2) un anello R si dice *unitario* o *con unità* se esiste 1 in R tale che $1 \cdot a = a \cdot 1 = a$ per ogni a in R ;
- (3) un anello commutativo si dice *dominio di integrità* se non possiede divisori dello zero, cioè se $ab = 0 \implies a = 0$ o $b = 0$;
- (4) Un *campo* è un anello commutativo con unità che contiene l'inverso di ogni elemento non nullo.
- (5) Un *corpo* è un anello (non necessariamente commutativo) con unità che contiene l'inverso di ogni elemento non nullo.

È chiaro che, utilizzando queste proprietà come proprietà *base*, si può decidere se due anelli *non* sono isomorfi: ad esempio, un anello con unità non potrà mai

essere isomorfo ad un anello senza unità: quindi ad esempio \mathbb{Z} non è isomorfo come anello a $2\mathbb{Z}$.

4.1.5 DEFINIZIONE. Sia $(R, +, \cdot)$ un anello. Un sottoinsieme non vuoto S di R si dice *sottoanello* di R se S è esso stesso un anello rispetto alle stesse operazioni di R . \square

Per essere un sottoanello di un anello $(R, +, \cdot)$ un sottoinsieme S di R deve essere innanzitutto un *sottogruppo additivo* di R , ossia deve essere tale che $(S, +)$ sia un *gruppo*.

Vale il seguente criterio per stabilire se un sottoinsieme di un anello è un sottoanello.

4.1.6 PROPOSIZIONE. Sia $(R, +, \cdot)$ un anello. Un sottoinsieme non vuoto S di R è un sottoanello di R se e solo se

$$(4.1.1) \quad a - b \in S, \quad ab \in S \quad \forall a, b \in S.$$

Dimostrazione. Se S è un sottoanello, la condizione di cui sopra è banalmente verificata. Supponiamo viceversa che per ogni a e b in S si abbia $a - b$ e ab in S : da tali ipotesi, per provare che S è un sottoanello basta provare che $(S, +)$ è un gruppo additivo, ossia $a + b \in S$, $0 \in S$, e $-a \in S \quad \forall a, b \in S$ (l'associatività rispetto a $+$ è automaticamente verificata). Dato che la condizione (4.1.1) vale per ogni scelta di a e b in S , varrà anche scegliendo $a = b$, da cui $a - a = 0 \in S$. Se poi prendiamo gli elementi $0, a$, si ottiene $0 - a = -a \in S$. Infine, dati comunque a e b in S , staranno in S anche $a - b$, da cui segue $a - (-b) = a + b \in S$. \square

4.1.7 ESEMPI DI SOTTOANELLI.

- (a) Ogni anello possiede sempre due sottoanelli, detti *sottoanelli banali*: il sottoanello ridotto al solo elemento 0 e l'intero anello.
- (b) In $R = \mathbb{Z}$, $S = n\mathbb{Z}$ ($n \in \mathbb{N}$) è un sottoanello di \mathbb{Z} . La proposizione 4.1.8 mostra che ogni sottoanello di \mathbb{Z} è di questo tipo.
- (c) Sia R un anello e sia a un fissato elemento di R . Sia

$$S_a = \{x \in R \mid xa = ax\}.$$

S_a è un sottoanello di R .

- (d) Nell'anello $\mathbb{K}[x]$ il sottoinsieme dei polinomi con termine noto uguale a zero è un sottoanello.
- (e) L'intersezione di una famiglia arbitraria di sottoanelli di un anello R è un sottoanello di R . \square

4.1.8 PROPOSIZIONE. Tutti e soli i sottoanelli di \mathbb{Z} sono del tipo $n\mathbb{Z}$, al variare di n in \mathbb{N} .

Dimostrazione. Abbiamo appena osservato che ogni sottoinsieme $n\mathbb{Z}$ è un sottoanello di \mathbb{Z} . Dobbiamo provare che tutti i sottoanelli di \mathbb{Z} sono del tipo $H = n\mathbb{Z}$: basta provare che tutti i sottogruppi di \mathbb{Z} sono di questo tipo (perché questi poi contengono il prodotto di due qualunque loro elementi e quindi sono sottoanelli). Sia H un sottogruppo non nullo di \mathbb{Z} e sia a un suo elemento non nullo. Allora anche $-a \in H$, da cui H conterrà certamente elementi positivi. Sia pertanto m il minimo intero positivo appartenente ad H . Proveremo che $H = m\mathbb{Z}$. Dato che ovviamente risulta $H \supseteq m\mathbb{Z}$, basta provare l'inclusione opposta. Sia h un qualunque elemento di H . Dividendo h per m si ha $h = mq + r$ con $0 \leq r < m$. Ora, r sta in H , per cui deve necessariamente essere $r = 0$ per non contraddirre la minimalità di m . Quindi ogni elemento di H è un multiplo di m . \square

Abbiamo visto che esistono domini di integrità che non sono campi, ad esempio \mathbb{Z} è un tale esempio. Non esistono tuttavia esempi di domini di integrità finiti che non siano campi, perché sussiste il seguente risultato.

4.1.9 PROPOSIZIONE. *Un dominio di integrità finito D è un campo.*

Dimostrazione. Basta provare che esiste $1 \in D$ tale che $a1 = 1a = a$ per ogni $a \in D$ e che ogni $a \neq 0$ è invertibile in D .

Sia $D = \{a_1, a_2, \dots, a_n\}$, con gli a_i tutti diversi tra di loro. Sia $a = a_k \neq 0$. Allora gli elementi

$$aa_1, aa_2, \dots, aa_n$$

sono anch'essi tutti distinti (infatti, se $i \neq j$, $aa_i = aa_j \implies a_i = a_j$). Ma allora l'applicazione (iniettiva per quanto detto)

$$\Psi : D \longrightarrow D$$

$$a_i \longmapsto aa_i$$

è anche (essendo D finito) suriettiva e quindi biunivoca. Ciò significa che ogni elemento di D si scrive come aa_i , ossia come prodotto di a per qualche elemento $a_i \in D$. In particolare, a stesso si scriverà in questo modo, cioè

$$a = aa_{i_0} = a_{i_0}a \quad \text{per qualche } a_{i_0} \in D.$$

Ora, a_{i_0} è elemento unità per D : sia infatti $x = aa_i$ un qualunque elemento in D . Allora

$$x = aa_i = (aa_{i_0})a_i = (a_{i_0}a)a_i = a_{i_0}(aa_i) = a_{i_0}x.$$

Indicheremo tale elemento unità a_{i_0} con 1. Ora, dal fatto che $1 \in D$, 1 si scriverà come $1 = aa_j$ per qualche a_j in D . Ma allora a è invertibile. \square

 **ESERCIZI.**

1. Si provi che, se un anello R possiede unità, questa è unica.
2. Sia $(A, +)$ un gruppo abeliano. Si consideri l'insieme

$$A^A \stackrel{\text{def}}{=} \{f : A \rightarrow A\}$$

e si ponga per ogni $f, g \in A^A$

$$(4.1.2) \quad (f + g)(x) \stackrel{\text{def}}{=} f(x) + g(x), \quad (f \circ g)(x) \stackrel{\text{def}}{=} f(g(x)).$$

Si provi che $(A^A, +, \circ)$ non è un anello. Si spieghi quale proprietà degli anelli non è soddisfatta.

Considerato l'insieme

$$\text{End}(A) \stackrel{\text{def}}{=} \{f : A \rightarrow A \mid f(x+y) = f(x) + f(y)\}$$

degli *endomorfismi* del gruppo abeliano A , si provi che le (4.1.2) definiscono delle operazioni in $\text{End}(A)$ e che $(\text{End}(A), +, \circ)$ è un anello.

3. Si provi che l'anello $\text{End}(\mathbb{Z})$ con le operazioni sopra definite è isomorfo all'anello \mathbb{Z} .
4. Si provi che $\text{End}(\mathbb{Q})$ è isomorfo a \mathbb{Q} .
5. Si provi che un anello R tale che $x^2 = x$ per ogni $x \in R$ è tale che $2x = 0$ per ogni $x \in R$ ed è commutativo.
6. Dire quali dei seguenti sono anelli:

$$(\mathbb{R}, \oplus, \cdot), \quad (\mathbb{R}, \oplus', \cdot)$$

dove \mathbb{R} rappresenta i reali, la seconda operazione, \cdot , in entrambi i casi è l'ordinaria moltiplicazione tra reali, e

$$a \oplus b \stackrel{\text{def}}{=} \sqrt{a^2 + b^2}$$

$$a \oplus' b \stackrel{\text{def}}{=} \sqrt[3]{a^3 + b^3}.$$

7. Si provi che l'insieme A delle matrici della forma

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

con $a, b \in \mathbb{Z}_3$ è un sottoanello dell'anello di tutte le matrici 2×2 a elementi in \mathbb{Z}_3 . Si provi che A è un campo.

8. Sia $C[-1, 1]$ l'anello delle funzioni continue definite nell'intervallo reale $[-1, 1]$ e a valori reali, rispetto alle operazioni

$$(f - g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x).$$

Si provi che $C[-1, 1]$ non è un dominio d'integrità.

9. Si provi che l'inverso di un isomorfismo φ tra R e R' è un isomorfismo (tra R' e R).



ESERCIZI DI PROGRAMMAZIONE.

- Sia R un insieme finito con n elementi (n piccolo). Siano date due operazioni su R , attraverso due tavole, una additiva e una moltiplicativa. Si scriva un programma che sia in grado di decidere se R rispetto a queste due operazioni è un anello, c., nel caso in cui lo sia, decida se è un dominio di integrità, è commutativo, è un campo, ecc.
- Dato un anello finito R , attraverso le due tavole additiva e moltiplicativa, si scriva un programma che sia in grado di decidere se un sottoinsieme di R è un sottoanello.



CONTROLLO.

- Si diano esempi di anelli commutativi ed esempi di anelli non commutativi.
- Un sottoanello di un anello è ...
- Si caratterizzino i sottoanelli di \mathbb{Z} .

4.2. Omomorfismi tra anelli. Ideali

Abbiamo dato nel paragrafo precedente la nozione di isomorfismo tra anelli. Spesso due anelli sono tali che esiste tra di loro un'applicazione che conserva le operazioni, ma che non è biunivoca. Si dà pertanto la seguente definizione.

4.2.1 DEFINIZIONE. Dati due anelli $(R, +, \cdot)$ e $(R', +', \cdot')$, si chiama *omomorfismo* di R in R' ogni corrispondenza φ da R a R' tale che

$$\begin{aligned}\varphi(r_1 + r_2) &= \varphi(r_1) + \varphi(r_2) \\ \varphi(r_1 r_2) &= \varphi(r_1)\varphi(r_2)\end{aligned}\quad \forall r_1, r_2 \in R. \quad \square$$

Diamo alcuni esempi.

- L'applicazione tra due anelli R e R' che manda ogni elemento di R nello 0 di R' è un omomorfismo, detto *omomorfismo nullo*.
-

$$\varphi : \mathbb{Z}_6 \rightarrow \mathbb{Z}_6$$

$$\bar{a} \mapsto \bar{3}\bar{a}$$

è un omomorfismo di anelli.

- $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}$ tale che $\varphi(z) = 2z$ per ogni $z \in \mathbb{Z}$ non è un omomorfismo di anelli, perché, pur conservando la somma, non conserva il prodotto.
- $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}$ data da $\varphi(z) = |z|$ non è un omomorfismo di anelli, perché conserva il prodotto ma non la somma.

Quando un omomorfismo φ è iniettivo, si chiama *monomorfismo*. Quando φ è suriettivo, si chiama *epimorfismo*. Quando φ è biiettivo, allora φ è un *isomorfismo*.

4.2.2 PROPOSIZIONE. *Dato un omomorfismo φ tra due anelli R e R' , l'immagine dello zero di R è sempre lo zero di R' , cioè*

$$\varphi(0_R) = 0_{R'}.$$

Dimostrazione. Infatti $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$, da cui $\varphi(0_R) = 0_{R'}$. \square

4.2.3 COROLLARIO. $\varphi(-a) = -\varphi(a)$ per ogni $a \in R$.

Ora, se anche R e R' sono dotati entrambi di unità, non è detto che $\varphi(1_R) = 1_{R'}$. Ad esempio, sia

$$R = \left\{ \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix} \mid r \in \mathbb{R} \right\}$$

e R' l'anello delle matrici 2×2 a elementi in \mathbb{R} . Entrambi gli anelli possiedono unità, tuttavia l'applicazione

$$\varphi: \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}$$

è un omomorfismo tra R e R' che non manda l'unità di R , che è $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, nell'unità di R' , che è $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Tuttavia vale il seguente risultato.

4.2.4 PROPOSIZIONE. *Sia φ un omomorfismo non nullo tra due anelli unitari R e R' . Se R' è un dominio di integrità oppure φ è un epimorfismo, allora il trasformato dell'unità di R è l'unità di R' .*

Dimostrazione. Se φ è suriettivo, ogni $r' \in R'$ uguaglia $\varphi(r)$ per qualche $r \in R$, quindi

$$r' = \varphi(r) = \varphi(r \cdot 1_R) = \varphi(r)\varphi(1_R) = r'\varphi(1_R)$$

ossia $\varphi(1_R)$ funge da unità destra per R' . Analogamente si vede che funge da unità sinistra. Se R' è un dominio d'integrità la $\varphi(r) = \varphi(r)\varphi(1_R)$ (con $\varphi(r) \neq 0$) implica (per cauzione) $\varphi(1_R) = 1_{R'}$. \square

4.2.5 DEFINIZIONE. Si definisce *nucleo* di un omomorfismo φ tra R e R' il sottoinsieme di R costituito da tutti gli elementi di R che hanno come immagine lo zero di R' . Esso si indica con $\text{Ker } \varphi$. Si ha pertanto

$$\boxed{\text{Ker } \varphi \stackrel{\text{def}}{=} \{r \in R \mid \varphi(r) = 0_{R'}\}}. \quad \square$$

$\text{Ker } \varphi$ gode di una proprietà importante: non solo è un sottoanello, come si verifica facilmente, ma gode anche della seguente proprietà: moltiplicando un elemento qualunque di $\text{Ker } \varphi$ per un *elemento qualunque* di R da destra o da

sinistra, il risultato è sempre un elemento di $\text{Ker } \varphi$. Infatti, se $k \in \text{Ker } \varphi$ e r è un qualunque elemento di R , si ha

$$\varphi(k \cdot r) = \varphi(k) \cdot \varphi(r) = 0 \cdot \varphi(r) = 0,$$

da cui segue che $k \cdot r \in \text{Ker } \varphi$. Analogamente a sinistra.

I sottoanelli di R che godono di questa proprietà hanno un nome speciale.

4.2.6 DEFINIZIONE. Un *ideale destro* di un anello R è un sottogruppo additivo di R tale che per ogni $a \in I$ e ogni $r \in R$, $ar \in I$.

Un *ideale sinistro* di un anello R è un sottogruppo additivo di R tale che per ogni $a \in I$ e ogni $r \in R$, $ra \in I$.

Un *ideale bilatero* è un ideale destro e sinistro contemporaneamente. Si denota al modo seguente:

$$I \leq R . \quad \square$$

4.2.7 ESEMPI DI IDEALI.

- (a) Ogni anello R possiede sempre due ideali *banali*, $\{0\}$ e R .
- (b) Gli ideali $n\mathbb{Z}$ di \mathbb{Z} , $n \in \mathbb{N}$.
- (c) Il sottoinsieme di $\mathbb{K}[x]$ costituito dai polinomi con termine noto uguale a zero. \square

Abbiamo appena provato che il nucleo di un omomorfismo tra anelli è un ideale bilatero.

È ovvio che un ideale destro (o sinistro) di R è un sottoanello di R . Tuttavia non è vero il viceversa. Ad esempio $S_a = \{x \in R \mid ax = xa\}$ è un sottoanello, che però non è un ideale.



ESERCIZI.

1. Si consideri l'applicazione così definita:

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ z &\longmapsto kz . \end{aligned}$$

Si determinino i valori di $k \in \mathbb{Z}$ per i quali φ risulta un omomorfismo di anelli.

2. Si provi che nell'anello R di tutte le matrici $n \times n$ a elementi in un campo K il sottoinsieme costituito da tutte le matrici con l'ultima riga (colonna) nulla è un ideale destro (sinistro), che non è un ideale bilatero.
3. Sia R l'anello delle matrici $n \times n$ a elementi reali e sia S il sottoinsieme di R costituito dalle matrici *singolari* (ossia con determinante uguale a zero). Si dica se S è un ideale (sinistro, destro o bilatero) di R .
4. Sia A l'anello delle funzioni continue reali definite nell'intervallo chiuso $[-1, 1]$. Sia $S = \{f \in A \mid f(0) = 3\}$ e sia $T = \{f \in A \mid f(1/3) = 0\}$. Si dica se S e/o T sono ideali o sottoanelli o non sono né l'uno né l'altro.

5. Si provi che un campo \mathbb{K} possiede solamente gli ideali banali (ossia $\{0\}$ e $\mathbb{K}\}$).
6. Sia X un sottoinsieme di un anello R . Si definiscano i seguenti sottoinsiemi:

$$A(X) \stackrel{\text{def}}{=} \{r \in R \mid rx = 0 \ \forall x \in X\}$$

$$B(X) \stackrel{\text{def}}{=} \{r \in R \mid xr = 0 \ \forall x \in X\}.$$

Si provi che $A(X)$ è un ideale sinistro di R , $B(X)$ è un ideale destro di R . Se X è un ideale sinistro di R si provi che $A(X)$ è un ideale bilatero.

7. Sia $R = M_2(\mathbb{R})$ l'anello delle matrici 2×2 a elementi reali. Sia $X = \left\{ \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \mid x, y \in \mathbb{R} \right\}$. Facendo riferimento all'esercizio precedente, si determinino $A(X)$ e $B(X)$. Si dica se sono ideali bilateri.
8. Un elemento a di un anello R si dice *nilpotente* se $a^n = 0$ per qualche intero positivo n . Si dimostri che l'insieme N di tutti gli elementi nilpotenti di un anello commutativo R è un ideale di R . Si mostri che l'ipotesi di commutatività è essenziale.
9. Si provi che un omomorfismo φ tra gli anelli R e R' è un *monomorfismo* se e solo se $\text{Ker } \varphi = \{0\}$.
10. Sia a_0 un elemento di un campo \mathbb{K} e sia R l'anello $\mathbb{K}[x]$. Si determinino i valori di a_0 per i quali il sottoinsieme di R costituito dai polinomi che hanno termine noto uguale ad a_0 è un ideale di R .



ESERCIZI DI PROGRAMMAZIONE.

1. Siano R e R' due anelli finiti, dati attraverso le tavole additive e moltiplicative. Si scriva un programma che sia in grado di riconoscere se una data applicazione tra R e R' è o no un omomorfismo, e che, nel caso in cui l'applicazione sia un omomorfismo, ne determini nucleo e immagine.
2. Si scriva un programma che sia in grado di decidere se un dato sottoinsieme di un anello è un ideale.



CONTROLLO.

1. Si provi che un omomorfismo di anelli manda sempre lo zero del primo anello nello zero del secondo. Cosa si può dire a proposito dell'unità?
2. Se un ideale I di un anello R è contenuto in un sottoanello S , si può dire che I è anche ideale di S ? E se J è un ideale di S , si può concludere che J è ideale di tutto R ?
3. Chi sono gli ideali di \mathbb{Z} ? Sono diversi dai sottoanelli? Perché?

4.3. Relazioni compatibili e ideali. Anelli quoziente

Sia $(R, +, \cdot)$ un anello. Analogamente a quanto detto a proposito delle congruenze definite su \mathbb{Z} (cfr. proposizione 2.6.3), si dà la seguente definizione.

4.3.1 DEFINIZIONE. Una relazione di equivalenza ϱ definita su R si dice *compatibile con le operazioni di R* se per ogni $a_1, a_2, b_1, b_2 \in R$

$$a_1 \varrho a_2, \quad b_1 \varrho b_2 \quad \implies \quad \begin{cases} (a_1 + b_1) \varrho (a_2 + b_2) \\ (a_1 \cdot b_1) \varrho (a_2 \cdot b_2) \end{cases} \quad \square$$

Abbiamo visto che la *relazione di congruenza* definita su \mathbb{Z} è compatibile con entrambe le operazioni di \mathbb{Z} .

Faremo ora vedere che assegnare in un anello R una relazione di equivalenza compatibile con entrambe le operazioni di R equivale ad assegnare un ideale bilatero, nel senso precisato dalle seguenti due proposizioni.

4.3.2 PROPOSIZIONE. *Sia ϱ una relazione di equivalenza definita su un anello R , compatibile con le operazioni di R . Allora il sottoinsieme*

$$I \stackrel{\text{def}}{=} \{x \in R \mid x \varrho 0\}$$

è un ideale bilatero di R .

Dimostrazione. Si tratta di provare che per ogni x e y in I e ogni r in R , si ha $x - y \in I$ e $rx \in I$, $rx \in I$:

$$x \in I, \quad y \in I \quad \implies \quad x \varrho 0, \quad y \varrho 0 \quad \implies \quad \begin{cases} x \varrho y \\ y \varrho -y \end{cases}$$

da cui, vista la compatibilità di ϱ rispetto all'*addizione*, segue che $(x - y) \varrho 0$, ossia $x - y \in I$. Così, se $x \in I$ e $r \in R$,

$$\begin{aligned} x &\varrho 0 \\ r &\varrho r \end{aligned}$$

implicano, per la compatibilità di ϱ rispetto alla *moltiplicazione*, che $rx \varrho 0$, ossia $rx \in I$. Analogamente, si prova che $r x \in I$. \square

4.3.3 PROPOSIZIONE. *Sia I un ideale bilatero di un anello R . La relazione ϱ definita su R come segue*

$$x \varrho y \iff x - y \in I$$

è una relazione di equivalenza compatibile con le operazioni di R . Essa prende il nome di congruenza modulo I .

Dimostrazione. Che ϱ sia una relazione di equivalenza è facile vedere. Proviamo che è compatibile con le due operazioni. Siano $x_1 \varrho x_2$ e $y_1 \varrho y_2$. Allora

$$\begin{aligned} x_1 \varrho x_2 &\iff x_1 - x_2 \in I \\ y_1 \varrho y_2 &\iff y_1 - y_2 \in I \end{aligned}$$

da cui

$$(x_1 + y_1) - (x_2 + y_2) = \underbrace{(x_1 - x_2)}_{\in I} + \underbrace{(y_1 - y_2)}_{\in I} \in I$$

e quindi ϱ è compatibile con l'addizione. Inoltre,

$$x_1 y_1 - x_2 y_2 = x_1 y_1 - x_1 y_2 + x_1 y_2 - x_2 y_2 = x_1 \underbrace{(y_1 - y_2)}_{\in I} + \underbrace{(x_1 - x_2) y_2}_{\in I} \in I$$

e quindi ϱ è compatibile anche con la moltiplicazione. Si noti che abbiano sfruttato *tutte* le proprietà dell'idealele. \square

Posto

$$\begin{aligned}\mathcal{R} &\stackrel{\text{def}}{=} \{\text{relazioni di equivalenza definite su } R \text{ compatibili con le operazioni di } R\} \\ \mathcal{I} &\stackrel{\text{def}}{=} \{\text{ideali (bilateri) di } R\}.\end{aligned}$$

la corrispondenza

$$\begin{aligned}\Psi : \mathcal{R} &\longrightarrow \mathcal{I} \\ \varrho &\longmapsto I = \{x \in R \mid x \varrho 0\}\end{aligned}$$

è una corrispondenza *biunivoca* tra \mathcal{R} e \mathcal{I} , la cui inversa è la

$$\begin{aligned}\Psi^* : \mathcal{I} &\longrightarrow \mathcal{R} \\ I &\longmapsto \varrho \quad \text{dove } x \varrho y \iff x - y \in I.\end{aligned}$$

Concludendo, si ha:

4.3.4 PROPOSIZIONE. *Tutte e sole le relazioni compatibili definite su un anello R sono le congruenze modulo un ideale.*

4.3.5 ESEMPIO. Le relazioni in \mathbb{Z} compatibili con le operazioni di addizione e moltiplicazione sono esattamente le *congruenze modulo un intero n* . Infatti gli ideali sono tutti e soli i sottoinsiemi I_n del tipo $n\mathbb{Z}$, quindi

$$x \varrho y \iff x - y \in I_n = n\mathbb{Z}$$

cioè $x - y = kn$ per qualche $k \in \mathbb{Z}$. \square

Ora, se ϱ è una relazione di equivalenza definita su un anello R e compatibile con le due operazioni di R , allora si possono introdurre nell'insieme quoziante

$$R/\varrho = \{\bar{a} \mid a \in R\}, \quad \text{essendo } \bar{a} = \{x \in R \mid x \varrho a\}.$$

le seguenti due operazioni:

$$\bar{a} + \bar{b} \stackrel{\text{def}}{=} \overline{a+b}, \quad \bar{a} \cdot \bar{b} \stackrel{\text{def}}{=} \overline{a \cdot b}.$$

La compatibilità della relazione di equivalenza *garantisce* che le due operazioni sono *ben poste*: infatti, perché siano ben poste chiediamo che, dato comunque a_2 in relazione ad a_1 e dato comunque b_2 in relazione a b_1 , $a_1 + b_1$ sia in relazione ad $a_2 + b_2$ e $a_1 \cdot b_1$ sia in relazione ad $a_2 \cdot b_2$, che è esattamente il concetto di relazione di equivalenza compatibile.

Dato che assegnare una relazione compatibile ϱ su R equivale a dare un ideale I in R , in modo che la ϱ risulti definita dalla

$$x \varrho y \iff x - y \in I,$$

il quoziente R/ϱ si può indicare con R/I , dove

$$R/I \stackrel{\text{def}}{=} \{a + I \mid a \in R\},$$

con

$$a + I \stackrel{\text{def}}{=} \{a + i \mid i \in I\} = \{x \in R \mid x \varrho a\}.$$

Ora, rispetto alle due operazioni di cui è stato dotato, R/I acquista la struttura di anello, detto *anello quoziente modulo l'ideale I*. Lo zero dell'anello R/I è la classe I , l'opposto della classe $a + I$ è la classe $-a + I$, ecc.

Non solo: per come abbiamo definito le operazioni in R/I , l'applicazione π da R a R/I che associa ad ogni elemento a di R la classe $a + I$ a cui appartiene, e che prende il nome di *proiezione canonica sul quoziente*, è un *omomorfismo di anelli*, con nucleo I . Inoltre è suriettivo, ossia è un epimorfismo.

Possiamo riassumere nella proposizione che segue quanto visto in questo paragrafo.

4.3.6 PROPOSIZIONE. Sia I un ideale di un anello R .

(a) La relazione

$$x \varrho y \iff x - y \in I$$

è una relazione di equivalenza compatibile con le operazioni di R .

(b) Indicando le classi di equivalenza come

$$\bar{a} = a + I = \{a + i \mid i \in I\}$$

e ponendo

$$\bar{a} + \bar{b} \stackrel{\text{def}}{=} \overline{a+b} \quad \bar{a} \cdot \bar{b} \stackrel{\text{def}}{=} \overline{a \cdot b}$$

l'insieme quoziente $R/I = \{\bar{a} \mid a \in R\}$ diventa un anello, che si chiama *anello quoziente di R modulo l'ideale I*.

(c) *La proiezione canonica*

$$\pi : a \in R \longmapsto \bar{a} \in R/I$$

è un epimorfismo di anelli, con nucleo I .

ESERCIZI.

- Nell'anello $\mathbb{Q}[x]$ si considerino i sottoinsiemi

$$I = \{f(x)(x^2 + 5) \mid f(x) \in \mathbb{Q}[x]\}$$

$$J = \{f(x)(x^2 - x + 1) \mid f(x) \in \mathbb{Q}[x]\}.$$

Si provi che I e J sono ideali in $\mathbb{Q}[x]$, e si studino gli anelli quoziante $\mathbb{Q}[x]/I$ e $\mathbb{Q}[x]/J$.

- Sia R un anello commutativo e sia N l'insieme di tutti gli elementi nilpotenti di R . Si è già visto (cfr. esercizio 4.2.8) che tale insieme è un ideale di R . Si dimostri che il quoziante R/N è privo di elementi nilpotenti non nulli.
- Siano I e J due ideali bilateri di un anello R arbitrario. Posto

$$I + J \stackrel{\text{def}}{=} \{a + b \mid a \in I, b \in J\} \quad \text{e} \quad IJ \stackrel{\text{def}}{=} \left\{ \sum_{i=1}^n a_i b_i \mid n \in \mathbb{N}, a_i \in I, b_i \in J \right\}$$

si provi che $I + J$ e IJ sono ideali (bilateri) di R .

- Sia R un anello commutativo con unità. Siano I e J due ideali di R tali che $I + J = R$. Si provi che $IJ = I \cap J$.

ESERCIZI DI PROGRAMMAZIONE.

- Sia R un anello finito (dato attraverso le sue tavole additiva e moltiplicativa). Si scriva un programma che decida se una relazione di equivalenza definita su R è compatibile con le operazioni di R .



CONTROLLO.

- Si caratterizzino le congruenze di \mathbb{Z} compatibili con entrambe le operazioni.
- Dove interviene la compatibilità della relazione per arrivare alla nozione di anello quoziante?
- Chi sono gli elementi dell'anello quoziante modulo un ideale? Chi è la classe nulla?

4.4. I teoremi di omomorfismo e di isomorfismo tra anelli

Sappiamo che due anelli *isomorfi* sono indistinguibili da un punto di vista algebrico. Cosa si può dire riguardo a due anelli che siano *omomorfi*? Il teorema che segue dà una risposta a questa domanda.

4.4.1 TEOREMA FONDAMENTALE DI OMOMORFISMO TRA ANELLI. Siano R e R' due anelli, e sia $f : R \rightarrow R'$ un omomorfismo di anelli. Allora esiste uno e un solo isomorfismo f^* da $R/\text{Ker } f$ a $\text{Im } f$

$$R/\text{Ker } f \xrightarrow{f^*} \text{Im } f$$

tale che $f^* \circ \pi = f$, π essendo la proiezione canonica di R su $R/\text{Ker } f$.

Dimostrazione. Se vogliamo che la f^* verifichi la $f = f^* \circ \pi$, siamo costretti a definirla al modo seguente:

$$\begin{aligned} f^* : R/\text{Ker } f &\longrightarrow \text{Im } f \\ x - \text{Ker } f &\longmapsto f(x) . \end{aligned}$$

Si tratta ovviamente di vedere se questa è una buona definizione. Posto $x + \text{Ker } f = [x]$, dobbiamo provare i seguenti punti:

- (1) f^* è ben posta, ossia $[x] = [y] \implies f(x) = f(y)$;
- (2) f^* è birettiva;
- (3) f^* è un omomorfismo di anelli.

(1) $[x] = [y] \iff x - y \in \text{Ker } f \iff f(x - y) = 0 \iff f(x) = f(y)$. Le doppie implicazioni provano sia che la f^* è ben posta, sia che è intettiva.

(2) Resta da provare la sola suriettività: dato comunque un elemento di $\text{Im } f$, esso sarà del tipo $f(x)$, quindi proverrà mediante la f da un elemento $x \in R$. Ma allora $f(x)$ proverrà mediante la f^* dalla classe $[x]$, e quindi f^* è suriettiva ($\text{Im } f^* = \text{Im } f$).

(3) $f^*([x] + [y]) = f^*([x + y]) = f(x + y) = ($ essendo f un omomorfismo $) = f(x) + f(y) = f^*([x]) + f^*([y])$. Analogio discorso per il prodotto.

È ovvio che la f^* , per come è stata definita, verifica la condizione richiesta $f^* \circ \pi = f$ e che è unica.

Il teorema si può visualizzare nel diagramma di figura 4.2 dove le frecce corrispondenti agli omomorfismi f e π sono dei dati, mentre la freccia tratteggiata sta a significare che dell'isomorfismo f^* si deve provare l'esistenza.

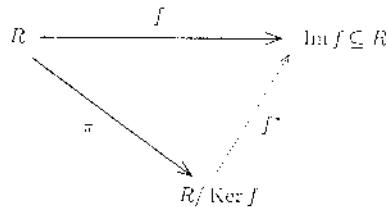


FIGURA 4.2

Il diagramma si legge al modo seguente: esiste uno ed un solo isomorfismo f^* da $R/\text{Ker } f$ a $\text{Im } f$ che rende commutativo il diagramma, ossia tale che $f^* \circ \pi = f$. \square

Il teorema ora provato dice che per determinare tutte le immagini omomorfo di un dato anello R , basta lavorare all'interno dell'anello, cercando tutti gli ideali bilateri di R : infatti ogni immagine omomorfa di un anello è, a meno di isomorfismi, un anello quoziante di R modulo un ideale di R . Inoltre, per provare che un anello quoziante R/I è isomorfo ad un anello R' basta trovare un epimorfismo tra R e R' che abbia l'ideale I come nucleo.

4.1.2 PROPOSIZIONE. *Sia f un omomorfismo tra due anelli R e R' . Allora*

- se A è un sottoanello di R , $f(A)$ è un sottoanello di R' :*
- se I è un ideale di R , $f(I)$ è un ideale di $f(R)$ ($= \text{Im } f$) (ma non necessariamente di R'):*
- se A' è un sottoanello di R' , $f^{-1}(A')$ è un sottoanello di R contenente $\text{Ker } f$:*
- se I' è un ideale di R' , $f^{-1}(I')$ è un ideale di R contenente $\text{Ker } f$.*

Dimostrazione. (a) Dati comunque due elementi $f(a)$ e $f(\bar{a})$ di $f(A)$, risulta $f(a) - f(\bar{a}) = f(a - \bar{a}) \in f(A)$ e $f(a)f(\bar{a}) = f(a\bar{a}) \in f(A)$ dato che $a - \bar{a} \in A$ e $a\bar{a} \in A$.

(b) Basta provare che $f(a)f(x) \in f(I)$ e $f(x)f(a) \in f(I)$ per ogni $a \in I$ e ogni $x \in R$. Infatti $f(a)f(x) = f(ax) \in f(I)$ perché $ax \in I$. Analogamente $f(x)f(a) \in f(I)$.

(c) Siano a e \bar{a} due elementi appartenenti a $f^{-1}(A')$, tali cioè che $f(a) \in A'$ e $f(\bar{a}) \in A'$. Allora $f(a - \bar{a}) = f(a) - f(\bar{a}) \in A'$, e $f(a\bar{a}) = f(a)f(\bar{a}) \in A'$, per cui $a - \bar{a}$ e $a\bar{a}$ stanno in $f^{-1}(A')$. Quest'ultimo contiene $\text{Ker } f$, dato che per ogni $k \in \text{Ker } f$, $f(k) = 0_{R'}$, che è contenuto in ogni anello A' .

(d) Siano $x \in R$ e $a \in f^{-1}(I')$. Dobbiamo provare che xa e ax stanno in $f^{-1}(I')$. Infatti, $f(ra) = f(x)f(a) \in I'$ (dato che $f(a) \in I'$). Analogamente $f(ax) \in I'$. Ovviamente anche in questo caso $f^{-1}(I')$ contiene $\text{Ker } f$. \square

Illustriamo il contenuto della proposizione precedente con un esempio.

4.4.3 ESEMPIO. Siano $R = \mathbb{Z}$, $R' = \mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$, e $f = \pi$ la proiezione canonica di \mathbb{Z} su $\mathbb{Z}/4\mathbb{Z}$. Sia $A = 6\mathbb{Z}$. Come mostra la figura 4.3, gli elementi di $6\mathbb{Z}$ si distribuiscono in due sole delle classi di \mathbb{Z} modulo $4\mathbb{Z}$ (un multiplo di 6, diviso per 4 può fare come resto solo 0 o 2). Passando al quoziante modulo $I = 4\mathbb{Z}$, si ha

$$\pi(A) = (A + I)/I = \{I, 2 + I\}$$

ed è facile vedere che si tratta effettivamente di un ideale di

$$R/I = \{I, 1 + I, 2 + I, 3 + I\} . \quad \square$$

$\overline{3}$	3 7 11 ...	$\longrightarrow \bullet \overline{3}$
$\overline{1}$	1 5 9 ...	$\longrightarrow \bullet \overline{1}$
$\overline{2}$	2 10 ...	$\longrightarrow \bullet \overline{2}$
$\overline{0}$	4 8 16 20 ...	$\longrightarrow \bullet \overline{0} \quad \left. \begin{array}{l} \pi(A) = (6\mathbb{Z} + I)/I \\ \end{array} \right\}$
	6 18 30 0	

$\square = 6\mathbb{Z}$

FIGURA 4.3

4.4.4 COROLLARIO. Sia R un anello, I un suo ideale bilatero e $\pi : R \rightarrow R/I$ la proiezione canonica. Allora

- (a) A sottoanello (ideale) di $R \implies \pi(A) = (A + I)/I$ è un sottoanello (ideale) di R/I ;
- (b) A' sottoanello (ideale) di $R/I \implies \pi^{-1}(A')$ è un sottoanello (ideale) di R contenente I .

Dimostrazione. Basta osservare che in questo caso l'omomorfismo π è suriettivo (quindi $\pi(R) = R/I$). \square

4.4.5 PROPOSIZIONE. Sia R un anello, I un suo ideale e $\pi : R \rightarrow R/I$ la proiezione canonica. Siano

$$\begin{aligned}\mathcal{L} &= \{\text{sottoanelli (ideali) di } R \text{ contenenti } I\} \\ \mathcal{L}' &= \{\text{sottoanelli (ideali) di } R/I\}.\end{aligned}$$

Allora la

$$\begin{aligned}\Psi : \mathcal{L} &\longrightarrow \mathcal{L}' \\ A &\longmapsto \pi(A)\end{aligned}$$

è una corrispondenza biunivoca tra \mathcal{L} e \mathcal{L}' .

Dimostrazione. Nelle ipotesi attuali ($A \supseteq I$), si ha $\pi(A) = A/I$. In virtù del corollario 4.4.4, la Ψ manda un sottoanello (ideale) di R contenente I in un sottoanello (ideale) di R/I , cioè un elemento di \mathcal{L}' . L'applicazione Ψ^* definita da $\Psi^*(A') = \pi^{-1}(A')$ è un'applicazione (in base al punto (b) del medesimo corollario) da \mathcal{L}' in \mathcal{L} . Essa è l'applicazione inversa della Ψ , in virtù delle

- (i) $\pi^{-1}(\pi(A)) = A,$
- (ii) $\pi(\pi^{-1}(A')) = A'$

(per la (i) si veda l'esercizio 4.4.2 e per la (ii) si osservi che π è suriettiva). Pertanto la Ψ è biunivoca. \square

4.4.6 ESEMPIO. Per determinare tutti gli ideali dell'anello quoziante $\mathbb{Z}/12\mathbb{Z}$ basta innanzitutto trovare tutti gli ideali di \mathbb{Z} contenenti $12\mathbb{Z}$. Questi sono i seguenti:

$$\mathbb{Z}, \quad 2\mathbb{Z}, \quad 3\mathbb{Z}, \quad 4\mathbb{Z}, \quad 6\mathbb{Z}, \quad 12\mathbb{Z}.$$

Allora gli ideali di $\mathbb{Z}/12\mathbb{Z}$ sono

$$\mathbb{Z}/12\mathbb{Z}, \quad 2\mathbb{Z}/12\mathbb{Z}, \quad 3\mathbb{Z}/12\mathbb{Z}, \quad 4\mathbb{Z}/12\mathbb{Z}, \quad 6\mathbb{Z}/12\mathbb{Z}, \quad 12\mathbb{Z}/12\mathbb{Z} = \{0\}. \quad \square$$

I seguenti due teoremi prendono il nome di teoremi di isomorfismo.

4.4.7 PRIMO TEOREMA DI ISOMORFISMO. Sia R un anello, I un suo ideale e π la proiezione canonica. Sia A un sottoanello di R non necessariamente contenente I . Allora

- (a) $\pi^{-1}(\pi(A)) = A + I = \{a + i \mid a \in A, i \in I\}$;
- (b) $A \cap I$ è un ideale di A e I è un ideale di $A + I$;
- (c) $A/(A \cap I) \cong (A + I)/I$.

Dimostrazione. Dimostriamo solo il terzo punto, perché i primi due sono dei semplici esercizi (cfr. esercizio 4.4.3).

Riferendosi alla figura 4.4, se $\pi : R \rightarrow R/I$, sia $\pi|_A$ la restrizione di π ad A , cioè

$$\pi|_A : A \longrightarrow (A + I)/I.$$

Si tratta di un omomorfismo tra anelli il cui nucleo è

$$\text{Ker } \pi|_A = \{x \in A \mid \pi|_A(x) = I\} = \{x \in A \mid x + I = I\} = A \cap I.$$

Il risultato segue in virtù del teorema fondamentale di omomorfismo tra anelli. \square

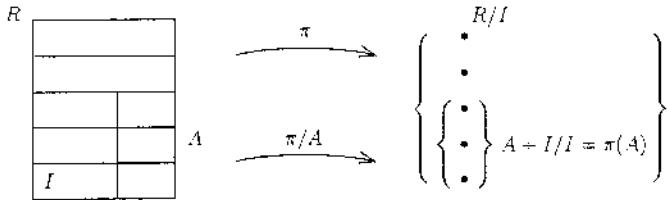


FIGURA 4.4

Illustriamo il teorema ora dimostrato con il seguente schema dove un punto collegato con un segmento ad un punto superiore rappresenta un *sottoanello*, mentre rappresenta un *ideale* se collegato con due segmenti (figura 4.5).

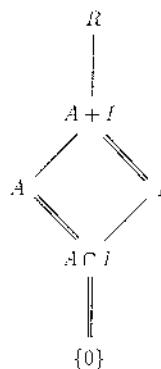


FIGURA 4.5

4.4.8 SECONDO TEOREMA DI ISOMORFISMO. *Sia R un anello, I e J siano due ideali di R tali che $I \subset J$. Allora*

$$(R/I)/(J/I) \cong R/J.$$

Dimostrazione. In base al teorema fondamentale di omomorfismo tra anelli, basta dimostrare che esiste un epimorfismo di anelli di R su $(R/I)/(J/I)$ con nucleo J . La composizione $\pi = \pi_2 \circ \pi_1$ delle proiezioni canoniche

$$R \xrightarrow{\pi_1} R/I \xrightarrow{\pi_2} (R/I)/(J/I)$$

è un epimorfismo di R su $(R/I)/(J/I)$, e risulta

$$\text{Ker } \pi = \{r \in R \mid \pi_1(r) \in \text{Ker } \pi_2\} = \{r \in R \mid r + I = j + I, \ j \in J\} = J.$$

Quintifi

$$R/J \simeq (R/I)/(J/I)$$

La situazione è illustrata nella figura 4.6 dove p è la proiezione canonica sul quoziente R/J , e la $f : R/J \rightarrow (R/I)/(J/I)$ è definita al modo seguente: $f(r+J) \stackrel{\text{def}}{=} (r+I) + J/I$. \square

$$\begin{array}{ccccc} R & \xrightarrow{\pi_1} & R/I & \xleftarrow{\pi_2} & (R/I)/(J/I) \\ p \downarrow & & f & & \nearrow \\ R/J & & & & \end{array}$$

FIGURA 4.6

4.4.9 ESEMPIO. Determiniamo esplicitamente l'isomorfismo di cui al teorema precedente nel caso in cui sia $R = \mathbb{Z}$, $I = 12\mathbb{Z}$ e $J = 3\mathbb{Z}$. Dalla figura 4.7 risulta

$$\mathbb{Z}/I = \mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}_{12}, \quad \mathbb{Z}/J = \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3, \quad J/I = (3\mathbb{Z})/(12\mathbb{Z}) \cong \bar{3}_{12}\mathbb{Z}_{12}.$$

La $f : \mathbb{Z}/J \rightarrow (J/I)/(J/I)$ è data da $f(\bar{x}_3) = \bar{x}_{12} + \bar{3}_{12}\mathbb{Z}_{12}$. Quindi

$$\begin{aligned} \bar{0}_3 &\longrightarrow \bar{0}_{12} + \bar{3}_{12}\mathbb{Z}_{12} = \{\bar{0}_{12}, \bar{3}_{12}, \bar{6}_{12}, \bar{9}_{12}\} \\ \bar{1}_3 &\longrightarrow \bar{1}_{12} + \bar{3}_{12}\mathbb{Z}_{12} = \{\bar{1}_{12}, \bar{4}_{12}, \bar{7}_{12}, \bar{10}_{12}\} \\ \bar{2}_3 &\longrightarrow \bar{2}_{12} + \bar{3}_{12}\mathbb{Z}_{12} = \{\bar{2}_{12}, \bar{5}_{12}, \bar{8}_{12}, \bar{11}_{12}\}. \end{aligned} \quad \square$$

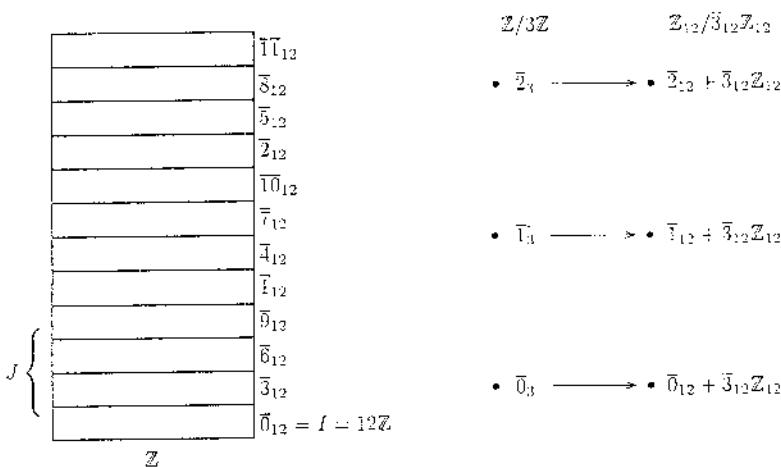


FIGURA 4.7



ESERCIZI.

- Siano r ed s due interi positivi tali che $(r, s) = 1$.
 - Considerato l'anello $\mathbb{Z}_r \times \mathbb{Z}_s$ (rispetto alle ordinarie addizione e moltiplicazione componente per componente), si provi che l'applicazione $f : \mathbb{Z} \rightarrow \mathbb{Z}_r \times \mathbb{Z}_s$ data da $a \rightarrow (\bar{a}_r, \bar{a}_s)$ è un epimorfismo di anelli.
 - Si provi (sfruttando il teorema fondamentale di omomorfismo tra anelli) che gli anelli \mathbb{Z}_{rs} e $\mathbb{Z}_r \times \mathbb{Z}_s$ sono isomorfi.
- Sia R un anello, I un suo ideale bilatero e π la proiezione canonica. Si provi che, se A è un sottoanello (o un ideale) di R contenente I , allora

$$\pi^{-1}(\pi(A)) = A.$$

3. Sia R un anello, I un suo ideale bilatero e π la proiezione canonica. Indicato con A un sottoanello di R (non contenente I), si provi che

$$\pi^{-1}(\pi(A)) = A + I,$$

che I è un ideale di $A + I$ e che $A \cap I$ è un ideale di A .

4. Siano I_1 e I_2 due ideali di un anello con unità R , tali che $I_1 + I_2 = R$. Si provi che

$$R/(I_1 \cap I_2) \cong R/I_1 \oplus R/I_2.$$

5. Si determini esplicitamente l'isomorfismo di cui al primo teorema di isomorfismo nel caso in cui siano $R = \mathbb{Z}$, $I = 4\mathbb{Z}$ e $A = 6\mathbb{Z}$.
 6. Si determini esplicitamente l'isomorfismo di cui al secondo teorema di isomorfismo, nel caso in cui siano $R = \mathbb{Z}$, $I = 10\mathbb{Z}$, $J = 2\mathbb{Z}$.
 7. Si determinino tutti gli ideali di \mathbb{Z}_{24} (si utilizzi la proposizione 4.4.5). Si determinino in generale tutti gli ideali di \mathbb{Z}_n .



CONTROLLO.

1. Enunciato del teorema fondamentale di omomorfismo tra anelli.
2. Come si determinano gli ideali di un quoziente?

4.5. Ideale generato da un sottoinsieme. Ideali primi e ideali massimali

Da questo momento in poi, salvo esplicito avviso contrario, gli anelli che studieremo saranno sempre anelli commutativi.

Sia quindi R un anello commutativo. Dato un sottoinsieme S non vuoto di R , vogliamo costruire a partire da tale insieme un ideale, nel senso precisato dalla seguente definizione.

4.5.1 DEFINIZIONE. Sia $S = \{a_1, a_2, \dots, a_m\}$ un sottoinsieme di R . Dicesi *ideale generato da S* l'intersezione di tutti gli ideali di R contenenti S . \square

Tale definizione ha senso, dato che, come è immediato verificare, l'intersezione di una famiglia arbitraria di ideali di un anello R è un ideale. Gli elementi a_1, a_2, \dots, a_m si dicono *generatori* dell'ideale, e l'ideale da essi generato si indica al modo seguente:

$$(a_1, a_2, \dots, a_m) . \quad \square$$

4.5.2 PROPOSIZIONE. L'ideale (a_1, a_2, \dots, a_m) è il più piccolo ideale contenente gli a_i ($i = 1, \dots, m$) e risulta

$$(a_1, a_2, \dots, a_m) = \left\{ \sum_{i=1}^m z_i a_i + \sum_{i=1}^m r_i a_i \mid z_i \in \mathbb{Z}, r_i \in R \right\}.$$

Dimostrazione. La prima parte è ovvia. Ora, un qualunque ideale che contenga a_1, a_2, \dots, a_m deve contenere $\sum_{i=1}^m r_i a_i$ con $r_i \in R$. Inoltre deve contenere $\sum_{i=1}^m z_i a_i$, $z_i \in \mathbb{Z}$. D'altra parte l'insieme

$$T = \left\{ \sum_{i=1}^m z_i a_i : \sum_{i=1}^m r_i a_i \cdot z_i \in \mathbb{Z}, r_i \in R \right\}$$

è un ideale contenente a_1, a_2, \dots, a_m . Quindi abbiamo provato che

$$(a_1, a_2, \dots, a_m) = T . \quad \square$$

 ATTENZIONE. Il motivo per cui nell'insieme T sono state inserite anche le somme di multipli *intesti* degli a_i è dovuto al fatto che l'insieme

$$T' = \left\{ \sum r_i a_i : r_i \in R \right\}$$

costituito solo dalle somme di multipli degli a_i mediante elementi di R e non di \mathbb{Z} è, sì, un ideale, ma non contiene necessariamente gli a_i , come invece è richiesto. Ad esempio, se $R = 2\mathbb{Z}$, $S = \{4\}$, l'insieme $T' = \{4r \mid r \in 2\mathbb{Z}\}$ è l'ideale di $2\mathbb{Z}$ costituito dai multipli di 8, e pertanto non contiene 4.

Se l'anello R è *unitario*, allora l'insieme T si riduce (cfr. esercizio 4.5.1) all'insieme T' . \square

Se l'insieme S contiene infiniti elementi e R possiede unità, allora

$$(S) = \left\{ \sum_{i=1}^t r_i s_i : r_i \in R, s_i \in S, t \in \mathbb{N} \right\}$$

ossia (S) consiste di somme *finite* (di lunghezza variabile) di elementi del tipo $r_i s_i$.

4.5.3 ESEMPI.

(a) $R = \mathbb{Z}$, $S = \{3\}$. Allora

$$(3) = \{3z \mid z \in \mathbb{Z}\} = 3\mathbb{Z} .$$

(b) R un qualunque anello con unità, $S = \{1\}$. Allora

$$(1) = R .$$

(c) $R = 2\mathbb{Z}$, $S = \{6\}$. Allora

$$(6) = \{6r + 6z \mid r \in 2\mathbb{Z}, z \in \mathbb{Z}\} = \{0, \pm 6, \pm 12, \dots\} = 6\mathbb{Z} .$$

 ATTENZIONE. L'insieme $T' = \{6r \mid r \in 2\mathbb{Z}\}$ (senza i multipli *intesti* di 6) è costituito dai multipli di 12, e quindi, pur essendo un ideale, non è il più piccolo ideale contenente 6. \square

(d) $R = \mathbb{K}[x, y]$, $S = \{x, y\}$. Allora

$$\begin{aligned}(x, y) &= \{f(x, y) \cdot x + g(x, y) \cdot y \mid f(x, y), g(x, y) \in \mathbb{K}[x, y]\} \\ &= \{\text{polinomi di } \mathbb{K}[x, y] \text{ con termine noto nullo}\}. \quad \square\end{aligned}$$

Un ideale può essere generato da vari elementi. Può succedere che possa essere generato da un solo elemento, a : in tal caso prende il nome di *ideale principale generato dall'elemento a*.

4.5.4 DEFINIZIONE. Dicesi *anello principale* ogni anello con unità tale che ogni ideale sia principale. \square

Facciamo qualche esempio.

4.5.5 ESEMPI.

(a) In \mathbb{Z} l'ideale generato da $S = \{6, 15\}$ è

$$(6, 15) = \{z_1 6 + z_2 15 \mid z_i \in \mathbb{Z}\}.$$

Ora, tra gli elementi che si possono scrivere come combinazione lineare di elementi dell'anello \mathbb{Z} c'è anche, come sappiamo, il MCD(6, 15). Quindi (si controlli bene il perché dell'uguaglianza)

$$(6, 15) = (3) = \{3z \mid z \in \mathbb{Z}\}.$$

(b) Nell'anello $R = \mathbb{Q}[x, y]$ l'insieme I di tutti i polinomi nelle due variabili x e y con termine noto uguale a zero è un ideale, cd è generato da $S = \{x, y\}$, ma non è un ideale principale (cfr. esercizio 4.5.2). Quindi $\mathbb{Q}[x, y]$ non è un anello principale. \square

4.5.6 DEFINIZIONE. Un ideale $I \neq R$ di R si dice *primo* se per ogni $a, b \in R$

$$\boxed{ab \in I \implies a \in I \text{ o } b \in I}. \quad \square$$

4.5.7 ESEMPIO. Si consideri in \mathbb{Z} l'ideale $(5) = 5\mathbb{Z}$. Se $ab \in (5)$, vuol dire che ab è un multiplo di 5, cioè 5 divide ab . Ma essendo 5 un numero primo, deve essere o a un multiplo di 5 (e quindi $a \in (5)$), oppure b un multiplo di 5 (cioè $b \in (5)$).

Invece (10) non è un ideale primo in \mathbb{Z} , perché, ad esempio, $4 \cdot 5 = 20$ sta in (10), ma né 4 né 5 stanno in (10). \square

È immediato vedere che in \mathbb{Z} , se $n \neq 0$, (n) è un ideale primo se e solo se l'intero n è primo.

4.5.8 DEFINIZIONE. Un ideale I di un anello R , $I \neq R$, si dice *massimale* se

$$\boxed{\forall U \trianglelefteq R \mid I \subseteq U \subseteq R \implies U = I \text{ o } U = R}$$

cioè non esistono in R ideali intermedi U tra I e R . \square

4.5.9 ESEMPI.

- (a) In \mathbb{Z} l'ideale (5) è massimale. Infatti, perché sia $(5) \subsetneq (m)$ in \mathbb{Z} , m deve essere un divisore di 5 distinto da 5 . Ma allora deve essere $m = 1$, per cui $(m) = (1) = \mathbb{Z}$.
- (b) In \mathbb{Z} l'ideale $\{0\}$ è primo, ma non è massimale. \square

Utilizzeremo queste due definizioni per classificare alcuni quozienti. Premettiamo il seguente lemma.

4.5.10 LEMMA. *Un anello commutativo con unità è un campo se e solo se è privo di ideali non banali.*

Dimostrazione. Sia R un campo, e sia I un ideale non nullo di R . Esisterà allora in I un $a \neq 0$. Ma allora I contiene anche $aa^{-1} = 1$, il che implica che I contiene ogni $r = 1r$. Quindi $I = R$.

Viceversa, sia R un anello commutativo con unità privo di ideali non banali. Per far vedere che R è un campo basta provare che ogni elemento non nullo è invertibile. Sia $a \neq 0$ un elemento di R . Consideriamo l'insieme $I = \{ar \mid r \in R\}$. Si tratta di un ideale, ed è diverso da zero, perché I contiene a (R possiede unità!). Ma allora $I = R$, da cui sarà $1 = a\bar{r}$ per qualche \bar{r} in R . Quindi a è invertibile. \square

4.5.11 TEOREMA. *Sia R un anello commutativo con unità. Un ideale I è massimale se e solo se R/I è un campo.*

Dimostrazione. Se R è commutativo con unità, anche R/I è commutativo con unità. Ma allora, per il lemma ora provato,

$$R/I \text{ campo} \iff R/I \text{ è privo di ideali non banali}.$$

Per la corrispondenza biunivoca che esiste tra gli ideali di R contenenti I e gli ideali di R/I , questo significa che

$$R/I \text{ campo} \iff I \text{ è massimale}.$$

Il teorema è provato. \square

4.5.12 TEOREMA. *Sia R un anello commutativo (anche senza 1) e sia I un suo ideale. Allora I è primo se e solo se R/I è un dominio di integrità.*

Dimostrazione. Dire che R/I è un dominio di integrità significa dire che

$$(a + I)(b + I) = I \implies a + I = I \text{ oppure } b + I = I.$$

Ma questa relazione si legge anche al modo seguente:

$$ab + I = I \implies a \in I \text{ oppure } b \in I$$

cioè

$$ab \in I \implies a \in I \text{ oppure } b \in I, \text{ cioè } I \text{ è primo. } \square$$

I due teoremi ora dimostrati ci dicono che *in un anello commutativo con unità* un ideale massimale è primo. Qui di seguito diamo un esempio di ideale primo non massimale.

Sia $R = \mathbb{K}[x, y]$. L'ideale (x) è un ideale primo che non è massimale. Si consideri infatti l'applicazione

$$\begin{aligned}\Psi : \mathbb{K}[x, y] &\longrightarrow \mathbb{K}[y] \\ f(x, y) &\longmapsto f(0, y).\end{aligned}$$

Si tratta di un epimorfismo, di nucleo (x) . In base al teorema fondamentale di omomorfismo tra anelli risulta

$$\mathbb{K}[y] \cong \mathbb{K}[x, y]/(x).$$

Dato che il quoziente è (isomorfo ad) un dominio di integrità, (x) è un ideale primo. Dato che il quoziente non è un campo, (x) non è un ideale massimale.

 ATTENZIONE. Si noti che il risultato secondo cui in un anello commutativo con unità un ideale massimale è primo non vale più per anelli privi di unità, come mostra il seguente esempio in un anello *senza unità*. \square

Sia $R = 2\mathbb{Z}$, e sia $I = (4) = \{0, \pm 4, \pm 8, \dots\}$. I è *massimale*: sia infatti U un ideale di R tale che $U \supset I$ e $U \neq I$. Dovrà essere per forza $U = 2\mathbb{Z}$. Infatti essendo $U \supseteq I$, U deve contenere un elemento del tipo $2k$ con k dispari. Ma allora $k+1$ è pari e $2 = \underbrace{2(k+1)}_{\in I \subset U} - 2k \in U$ e quindi $U = 2\mathbb{Z}$. Tuttavia I

non è primo. Infatti $4 = 2 \cdot 2 \in (4)$, ma $2 \notin (4)$. Oppure, si potrebbe anche verificare che I non è primo controllando che tipo di anello è il quoziente $2\mathbb{Z}/(4) = \{(4), 2 + (4)\}$. Il prodotto di due qualunque elementi di tale anello è zero, quindi non è certo un dominio di integrità, come dovrebbe essere se l'ideale fosse primo.

ESERCIZI.

1. Si provi che se R è un anello (commutativo) unitario, allora

$$(a_1, a_2, \dots, a_m) = \left\{ \sum_{i=1}^m r_i a_i \mid r_i \in R \right\}.$$

2. Si provi che l'ideale di $\mathbb{Q}[x, y]$ costituito dai polinomi con termine noto nullo non è un ideale principale.

3. Si provi che, detti a e b elementi di \mathbb{Z} , risulta

$$\begin{aligned}(a) \cap (b) &= (m), & m &= \text{mcm}(a, b) \\ (a, b) &= (d), & d &\Rightarrow \text{MCD}(a, b).\end{aligned}$$

Si generalizzi a più elementi.

- 4. Si provi che $(a) + (b) = (d)$, con $d = \text{MCD}(a, b)$ e $(a) \cdot (b) = (ab)$ (si ricordino le definizioni di somma e prodotto di ideali, date nell'esercizio 4.3.3).
- 5. Si mostri che il risultato dell'esercizio 4.4.4 è una generalizzazione del teorema cinese del resto (caso di due congruenze).
- 6. Si determini un polinomio generatore dell'ideale

$$I = (x^4 + x - 1, x^3 - 2)$$

in $\mathbb{R}[x]$. Chi sono i polinomi di I ?

- 7. Siano a_1, a_2, \dots, a_m elementi di un anello R . Quali sono gli elementi che appartengono a (a_1, a_2, \dots, a_m) nel caso in cui R non sia commutativo e non contenga unità?
- 8. Si determinino gli ideali massimali e gli ideali primi di \mathbb{Z}_{24} e di \mathbb{Z}_{30} .
- 9. Si consideri l'anello (rispetto alle ordinarie operazioni di addizione e moltiplicazione di funzioni reali)

$$R = \{f : \mathbb{R} \rightarrow \mathbb{R} \text{ continua in } [0, 4]\}.$$

Sia $M = \{f \in R \mid f(2) = 0\}$. Si provi che M è un ideale massimale di R .

- 10. Sia R un anello commutativo con unità e sia I un ideale proprio di R . Dimostrare che I è massimale se e solo se $I + aR = R$ per ogni elemento $a \in R \setminus I$.
- 11. Sia R un anello commutativo, esiano I_1 e I_2 due suoi ideali tali che

$$I_1 \not\subseteq I_2, \quad I_2 \not\subseteq I_1.$$

Si provi che $I_1 \cap I_2$ non è un ideale primo di R .

- 12. Si provi che $\mathbb{R}[x]/(x^2 - 1) \cong \mathbb{R} \oplus \mathbb{R}$ (si veda l'esempio 4.1.2(g) per la definizione di somma diretta \oplus). Si consiglia di vedere l'esercizio 4.1.4.
- 13. Si provi che l'anello \mathbb{Z}_n è principale per ogni n .



CONTROLLO.

1. Perché nella costruzione dell'ideale generato da a_1, a_2, \dots, a_m abbiamo dovuto mettere anche i multipli interi degli a_i ?
2. Legame (se esiste) tra la nozione di ideale massimale e di ideale primo.
3. È sempre vero che il quoziente di un anello rispetto ad un ideale massimale è un campo? Se sì, dimostrarlo, altrimenti dare un controesempio.

4.6. Campo dei quozienti di un dominio di integrità

In questo e nei paragrafi che seguono limiteremo il nostro studio a quei particolari anelli commutativi che sono *domini di integrità*, che cioè sono privi di divisori dello zero.

Il fatto più notevole di un dominio di integrità è che ogni dominio di integrità D si può *immergere* in un campo, che prende il nome di D, allo stesso identico modo in cui si è fatto vedere che l'anello degli interi \mathbb{Z} si può immergere nel campo \mathbb{Q} dei razionali, che è il suo campo dei quozienti, o l'anello dei polinomi a coefficienti in un campo si può immergere nel campo delle funzioni razionali. Precisiamo questi concetti, ricordando per comodità la definizione di campo dei quozienti.

4.6.1 DEFINIZIONE. Sia R un sottoanello di un campo F . Si dice che F è *campo dei quozienti* di R se ogni elemento $a \in F$ si può scrivere nella forma $a = r \cdot s^{-1}$, con r e s in R , $s \neq 0$. \square

 **ATTENZIONE.** L'anello \mathbb{Z} degli interi è un sottoanello del campo \mathbb{R} dei numeri reali, ma quest'ultimo non è il campo dei quozienti di \mathbb{Z} , dato che non è vero che ogni elemento di \mathbb{R} si può scrivere come quoziente di due interi (il secondo dei quali non nullo). Sappiamo che il campo dei quozienti di \mathbb{Z} è \mathbb{Q} . \square

È ovvio che se un anello R è contenuto in un campo, R è necessariamente un dominio di integrità. Il problema che ci poniamo è quello di vedere se per *ogni dominio di integrità D* esiste un campo F di cui D sia sottoanello e tale che F sia campo dei quozienti per D .

La risposta è positiva, e vale il seguente teorema.

4.6.2 TEOREMA. *Sia D un dominio di integrità. Allora esiste un campo $Q(D)$ contenente un sottoanello \tilde{D} isomorfo a D e tale che ogni elemento di $Q(D)$ sia della forma ab^{-1} , con $a, b \in \tilde{D}$, $b \neq 0$.*

Dimostrazione. Dato che la dimostrazione è analoga a quella sviluppata quando si è costruito il campo dei razionali a partire dagli interi, daremo solo le linee della dimostrazione, invitando lo studente a colmare i dettagli, rifacendosi alla dimostrazione fatta a suo tempo.

Si consideri l'insieme $D \times D^*$ delle coppie ordinate di elementi di D , in cui il secondo elemento della coppia è diverso da zero. Si introduca in tale insieme la seguente relazione:

$$(a, b) \varrho (a', b') \iff ab' = ba'.$$

Tale relazione è una relazione di equivalenza, e si può passare all'insieme quoziente

$$Q(D) \stackrel{\text{def}}{=} (D \times D^*) / \varrho.$$

Definiamo in $Q(D)$ le seguenti operazioni:

$$\begin{aligned}\overline{(a,b)} + \overline{(c,d)} &\stackrel{\text{def}}{=} \overline{(ad+bc, bd)} \\ \overline{(a,b)} \cdot \overline{(c,d)} &\stackrel{\text{def}}{=} \overline{(ac, bd)}.\end{aligned}$$

Le due definizioni sono *ben poste* e, rispetto a queste due operazioni, $Q(D)$ diventa un *campo*. L'applicazione

$$\begin{aligned}i : D &\rightarrow Q(D) \\ a &\mapsto \overline{(ax, x)}\end{aligned}$$

è un omomorfismo di anelli il cui nucleo è zero. Quindi, posto $\bar{D} = \text{Im } i$, \bar{D} risulta isomorfo a D . Pertanto $Q(D)$ contiene una copia esatta di D al suo interno, cioè D è immerso in $Q(D)$. Per provare che $Q(D)$ è campo dei quozienti di D , basta provare che ogni elemento $\overline{(a,b)} \in Q(D)$ si scrive come quoziente di due elementi di \bar{D} :

$$\overline{(a,b)} = \overline{(ax,x)} \overline{(x,bx)} = \overline{(ax,x)} \overline{(bx,x)}^{-1}, \quad x \neq 0. \quad \square$$



CONTROLLO.

- Si provino in tutti i dettagli tutti i punti contenuti nella dimostrazione del teorema 4.6.2.
- Si provi che due domini di integrità isomorfi hanno campi dei quozienti isomorfi e quindi in particolare il campo dei quozienti di un dominio di integrità è unico (a meno di isomorfismi).

4.7. Domini euclidei

Si è visto che sia in \mathbb{Z} , sia nell'anello dei polinomi in una indeterminata a coefficienti in un campo K , si può fare la *divisione euclidea*. Precisamente, dati due interi a e b , con $b \neq 0$, esistono due interi q ed r tali che $a = bq + r$, con $0 \leq r < |b|$, oppure, in forma leggermente modificata, che si presta meglio ad essere generalizzata.

$$a = bq + r, \quad r = 0 \text{ oppure } |r| < |b|.$$

Si noti che in questa formulazione gli interi q ed r non sono univocamente individuati: infatti, ad esempio, posto $a = 32$, $b = 9$, risulta

$$32 = 9 \cdot 3 + 5 \quad \text{e} \quad 32 = 9 \cdot 4 - 4$$

ed entrambe le relazioni verificano la condizione: $|r| < |b|$.

Analogamente, dati due polinomi $f(x)$ e $g(x)$, $g(x) \neq 0$ in $K[x]$ e indicato con $\partial g(x)$ il grado di $g(x)$, esistono due polinomi $q(x)$ e $r(x)$ in $K[x]$ tali che

$$f(x) = g(x)q(x) + r(x) \quad r(x) = 0 \text{ oppure } \partial r(x) < \partial g(x).$$

In entrambi i casi abbiamo associato ad ogni elemento di \mathbb{Z} e di $K[x]$ un *intero positivo* (il valore assoluto e il grado del polinomio rispettivamente) in modo tale che l'intero associato al resto sia più piccolo dell'intero associato al divisore. Questa possibilità ci ha permesso la determinazione (e quindi ci ha garantito l'esistenza) del MCD tra due interi o due polinomi, attraverso il cosiddetto algoritmo euclideo delle divisioni successive. La possibilità di determinare il MCD con questo metodo derivava dal fatto che gli interi positivi associati ai resti via via decrescevano e quindi ad un certo punto dovevano essere zero. L'ultimo resto non nullo era il MCD.

Traendo lo spunto da questo fatto, vogliamo definire ora una classe di anelli per i quali sia possibile associare ad ogni elemento una grandezza in modo tale da poter fare la divisione con un resto che abbia grandezza più piccola del divisore. Questo ci permetterà di ottenere in tali anelli varie proprietà interessanti a basso costo. Nella definizione che segue chiameremo "valutazione" la corrispondenza v che associa ad ogni elemento a dell'anello la sua "grandezza" $v(a)$ che sarà un intero non negativo, che via via decresce nel corso delle divisioni successive.

4.7.1 DEFINIZIONE. Sia D un dominio di integrità. Supponiamo che ad ogni elemento $a \neq 0$ si possa associare un intero non negativo $v(a)$ in modo tale che

- (a) $v(a) \leq v(ab) \quad \forall a, b \in D, a \neq 0, b \neq 0;$
- (b) dati comunque due elementi a e b in D , $b \neq 0$, esistono q ed r in D tali che

$$a = bq + r \quad r = 0 \text{ oppure } v(r) < v(b).$$

Allora D si dice *dominio euclideo* e l'applicazione

$$\begin{aligned} v : D \setminus \{0\} &\longrightarrow \mathbb{N} \\ a &\longmapsto v(a) \end{aligned}$$

prende il nome di *valutazione*. \square

4.7.2 ESEMPI L'anello \mathbb{Z} degli interi è un dominio euclideo, se come valutazione si prende il *valore assoluto*; l'anello $K[x]$ dei polinomi a coefficienti in un campo K è un dominio euclideo se si sceglie come valutazione il *grado* di ogni polinomio non nullo. Un campo K è un dominio euclideo, se ad esempio si pone $v(a) = 1 \quad \forall a \in K, a \neq 0$.

 **ATTENZIONE.** Si noti che un dominio di integrità può diventare dominio euclideo rispetto a più valutazioni. Ad esempio, un campo diventa un dominio euclideo anche rispetto alla valutazione $v(k) = 2 \quad \forall k \in K, k \neq 0$. \square

Diamo ora un esempio importante di dominio euclideo, l'*anello degli interi di Gauss*.

4.7.3 PROPOSIZIONE. Il sottoinsieme

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

del campo \mathbb{C} dei numeri complessi è un sottoanello di \mathbb{C} , che è un dominio euclideo rispetto alla seguente valutazione:

$$v(a - ib) \stackrel{\text{def}}{=} a^2 + b^2.$$

Dimostrazione. Le operazioni di addizione e moltiplicazione di \mathbb{C} sono operazioni in $\mathbb{Z}[i]$ e rispetto a queste operazioni $\mathbb{Z}[i]$ è un anello, come si verifica facilmente. Inoltre, trattandosi di un sottoanello del campo \mathbb{C} dei numeri complessi, si tratta di un dominio di integrità. Faremo ora vedere che l'applicazione v da $\mathbb{Z}[i] \setminus \{0\}$ a \mathbb{N} data da $v(a - ib) = a^2 + b^2$ verifica le proprietà di una valutazione e che quindi $\mathbb{Z}[i]$ è un dominio euclideo. Si tratta della ordinaria norma dei numeri complessi: $a^2 + b^2$ è un intero (perché tali sono a e b) ≥ 1 qualunque sia $a + bi \in \mathbb{Z}[i]$ non nullo e, dato che la norma complessa è moltiplicativa, cioè $v(xy) = v(x)v(y)$, è verificata anche la $v(x) \leq v(xy)$ per ogni $x, y \in \mathbb{Z}[i]$. Resta da provare che vale la terza proprietà della divisione.

Siano $z_1 = a + ib$ e $z_2 = c + id$ due elementi di $\mathbb{Z}[i]$, $z_2 \neq 0$. Pensiamo per un momento di lavorare, anziché in $\mathbb{Z}[i]$, in $\mathbb{Q}[i] = \{x + iy \mid x, y \in \mathbb{Q}\}$. Questo ci consente di scrivere

$$(c + id)^{-1} = \frac{c - id}{c^2 + d^2}.$$

Allora

$$(4.7.1) \quad z_1 z_2^{-1} = (a + ib) \cdot \frac{c - id}{c^2 + d^2} = \frac{ac - bd}{c^2 + d^2} + i \frac{bc - ad}{c^2 + d^2}.$$

Ora, ogni frazione di interi si può scrivere come somma di una parte intera più una parte frazionaria che sia in valore assoluto minore o uguale ad $1/2$. La (4.7.1) diventa allora

$$(4.7.2) \quad \begin{aligned} z_1 z_2^{-1} &= \alpha + \frac{r_1}{c^2 + d^2} + i(\beta + \frac{r_2}{c^2 + d^2}) \\ &= \alpha + i\beta + (\frac{r_1}{c^2 + d^2} - i\frac{r_2}{c^2 + d^2}), \end{aligned}$$

dove $\alpha + i\beta \in \mathbb{Z}[i]$, mentre $r_1/(c^2 + d^2) + ir_2/(c^2 + d^2)$ è in $\mathbb{Q}[i]$. Inoltre,

$$\left| \frac{r_1}{c^2 + d^2} \right| \leq \frac{1}{2}, \quad \left| \frac{r_2}{c^2 + d^2} \right| \leq \frac{1}{2}.$$

Moltiplichiamo ora entrambi i membri di (4.7.2) per z_2 :

$$z_1 = (\alpha + i\beta)z_2 + \left(\frac{r_1}{c^2 + d^2} + i\frac{r_2}{c^2 + d^2} \right)z_2.$$

Abbiamo così scritto una relazione del tipo

$$z_1 = z_2q + r$$

dove $q = \alpha + i\beta$ e

$$r = \left(\frac{r_1}{c^2 + d^2} + i \frac{r_2}{c^2 + d^2} \right) z_2.$$

Ora, quest'ultimo elemento sta in $\mathbb{Z}[i]$, in quanto differenza di due elementi di $\mathbb{Z}[i]$. Resta da provare che $r = 0$ oppure che $v(r) < v(z_2)$. Infatti

$$\begin{aligned} v(r) &= v\left(\frac{r_1}{c^2 + d^2} + i \frac{r_2}{c^2 + d^2}\right) v(z_2) \\ &= \left[\left(\frac{r_1}{c^2 + d^2} \right)^2 + \left(\frac{r_2}{c^2 + d^2} \right)^2 \right] v(z_2) \leq \left(\frac{1}{4} + \frac{1}{4} \right) v(z_2) \\ &= \frac{1}{2} v(z_2) < v(z_2). \quad \square \end{aligned}$$

4.7.4 DEFINIZIONE. Il sottoanello di \mathbb{C}

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

prende il nome di *anello degli interi di Gauss*. \square

Abbiamo dato così vari esempi di domini euclidei. È chiaro che ogni anello che non è un dominio di integrità, come ad esempio \mathbb{Z}_n con n non primo, non è un dominio euclideo. Tuttavia non è facile a questo punto dare esempi di *domini di integrità* che non sono domini euclidei: si tratterebbe di dimostrare che non si riesce a definire sull'anello *nessuna* funzione valutazione che goda delle proprietà richieste nella definizione. Per scoprire che un anello R non è euclideo sarà più semplice invece mostrare che in R non valgono alcune delle proprietà che devono valere in qualunque dominio euclideo, che sono cioè conseguenza della definizione di tali anelli.

Diamo pertanto qui di seguito alcune proprietà che *si deducono dalla definizione di dominio euclideo*.

Ricordando la definizione di ideale (S) generato da un sottoinsieme S , e di ideale principale (generato da un singolo elemento a), si dà la seguente definizione.

4.7.5 DEFINIZIONE. Un dominio di integrità con unità in cui ogni ideale è principale (cioè ogni dominio di integrità che sia un anello principale) prende il nome di *dominio principale*. \square

Abbiamo visto (proposizione 4.1.8) che in \mathbb{Z} tutti i sottoanelli sono del tipo $(n) = n\mathbb{Z}$ per qualche n in \mathbb{Z} , ma questi sono automaticamente degli ideali. Quindi in \mathbb{Z} ogni ideale è principale. Imitando la dimostrazione fatta per \mathbb{Z} , si prova facilmente che anche $\mathbb{K}[x]$ è un dominio principale.

Ogni campo è (ovviamente) un dominio principale.

Proviamo la seguente proposizione.

4.7.6 PROPOSIZIONE. *Ogni dominio euclideo è principale.*

Dimostrazione. Occorre provare che ogni dominio euclideo R possiede unità e che in esso ogni ideale è principale.

Sia I un ideale di R , $I \neq \{0\}$, e sia v la valutazione definita su $R \setminus \{0\}$. Sia $V = \{v(a) \mid a \in I\}$. Dato che V è non vuoto e $V \subseteq \mathbb{N}$, esisterà in V un elemento minimo, n_0 , e sia a_0 un elemento di I con tale valutazione minima, cioè $v(a_0) = n_0$. Proviamo che $I = a_0R$. Chiaramente, dato che $a_0 \in I$, sarà $a_0R \subseteq I$. Resta da provare che ogni $a \in I$ è del tipo a_0t per qualche t in R . Dividiamo a per a_0 :

$$a = a_0q + r \quad r = 0 \text{ oppure } v(r) < v(a_0).$$

Dato che $r \in I$ (in quanto differenza di due elementi di I), per non contraddirre la minimalità della valutazione di a_0 , deve essere $r = 0$, che è quanto volevamo.

Prendiamo ora come ideale I l'intero anello R . In base a quanto dimostrato al punto precedente, esisterà un elemento u in R tale che $R = uR$. Ogni elemento a in R si scriverà pertanto nella forma $a = ut$ per qualche $t \in R$. In particolare, u stesso si scriverà come $u = ue$, per qualche e in R : proveremo che e è unità per R . Infatti, per ogni a in R ,

$$a = ut = tu \implies a = t \cdot ue = tu \cdot e = ae.$$

Allora R possiede unità, e quindi $I = a_0R = (a_0)$, cioè ogni ideale è principale. \square

4.7.7 PROPOSIZIONE. *In un dominio principale R , due qualunque elementi a e b non entrambi nulli possiedono un massimo comun divisore.*

Dimostrazione. Sia $S = \{xa + yb \mid x, y \in R\}$. Risulta $S \neq \emptyset$, perché, avendo R unità, tra gli elementi di S ci sono a e b . Inoltre S è un ideale, e in quanto tale, sarà $S = (d)$ per qualche d in R . Proveremo che d è massimo comun divisore tra a e b . Infatti risulta $d|a$ e $d|b$, dato che $a \in (d)$ e $b \in (d)$. Se inoltre $d' | a$ e $d' | b$, allora $d' | d = sa + tb$. \square

4.7.8 COROLLARIO. *In ogni dominio euclideo, due qualunque elementi a e b non entrambi nulli possiedono un massimo comun divisore.*

Dato che ogni dominio euclideo, come abbiamo appena mostrato, possiede unità 1, ha senso la seguente proposizione.

4.7.9 PROPOSIZIONE. *Gli elementi invertibili di un dominio euclideo R sono tutti e soli gli elementi a valutazione minima, uguale alla valutazione dell'unità.*

Dimostrazione. Sia a un elemento invertibile di R (quindi $a \neq 0$). Allora

$$v(1) = v(a \cdot a^{-1}) \geq v(a) \implies v(a) \leq v(1).$$

D'altra parte risulta, qualunque sia $a \in R$, $a \neq 0$, $v(a) = v(a \cdot 1) \geq v(1)$, (cioè la valutazione di 1 è la valutazione minima), da cui $v(a) = v(1)$ per ogni a invertibile. Viceversa, se a è tale che $v(a) = v(1)$, allora a è invertibile. Infatti, dividendo 1 per a , si ha

$$1 = aq + r \quad r = 0 \text{ oppure } v(r) < v(a) = v(1).$$

Dato che $v(1)$ è la valutazione minima, deve necessariamente essere $r = 0$, e quindi a è invertibile.

Abbiamo così provato che l'insieme $U(R)$ degli elementi invertibili di R è dato da

$$U(R) = \{a \in R \mid v(a) = v(1)\}. \quad \square$$

Si ha così la seguente tabella:

Anello	Valutazione	Valutazione minima	Elementi invertibili
\mathbb{Z}	$v(x) = x \quad \forall x$	1	± 1
K	$v(x) = 1 \quad \forall x$	1	ogni $x \neq 0$
$K[x]$	$v(f(x)) = \partial f(x)$	0	costanti non nulle
$\mathbb{Z}[i]$	$v(a+ib) = a^2 + b^2$	1	$\pm 1, \pm i$

Ritorniamo ora al caso più generale dei domini di integrità provvisti di unità. Si può dare la nozione di divisibilità, di elementi associati, elementi primi ed elementi irriducibili, così come abbiamo fatto nel caso particolare degli interi e dei polinomi a coefficienti in un campo. Tali nozioni ci hanno permesso di stabilire la nozione di fattorizzazione di un elemento. Raduniamo qui di seguito per completezza queste definizioni, anche se sono identiche a quelle che abbiamo visto a suo tempo nei casi particolari di \mathbb{Z} e di $K[x]$.

Sia R un dominio di integrità con unità 1.

$a \mid b$ (a divide b)	\iff	$\exists c \in R \mid b = ac$
$a \sim b$ (a è associato a b)	\iff	$a \mid b \text{ e } b \mid a$
u è unità o elemento invertibile	\iff	$\exists v \in R \mid uv = vu = 1$
$a \neq 0$ e non invertibile è irriducibile	\iff	$[a = bc \implies b \text{ o } c \text{ è un'unità}]$
a è primo	\iff	$[a \mid bc \implies a \mid b \text{ o } a \mid c]$

Allo stesso modo di come si è dimostrato in \mathbb{Z} (cfr. proposizione 2.1.14), si dimostra che ogni elemento primo di un dominio di integrità con unità è irriducibile. Tuttavia il viceversa di questa proposizione non è vera. Basta dare un

esempio di anello in cui esistono elementi irriducibili e non primi. Sia $a \in \mathbb{C}$. Indichiamo con

$$\mathbb{Z}[a]$$

l'intersezione di tutti i sottoanelli di \mathbb{C} contenenti \mathbb{Z} e a . Esso coincide con il più piccolo sottoanello di \mathbb{C} contenente \mathbb{Z} e a . Se ad esempio $a = i$ (unità complessa), risulta

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}.$$

Sia ora $a = \sqrt{-3}$. Si consideri l'anello

$$\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}.$$

Determiniamo innanzitutto gli elementi invertibili di tale anello; se associamo ad ogni elemento $a + b\sqrt{-3}$ di $\mathbb{Z}[\sqrt{-3}]$ la sua norma complessa $N(a + b\sqrt{-3}) = a^2 + 3b^2$, la invertibilità di $a + b\sqrt{-3}$ implica che la sua norma valga 1: infatti, dire che $\alpha = a + b\sqrt{-3}$ è invertibile significa dire che esiste un $\beta = c + d\sqrt{-3}$ tale che $\alpha\beta = 1$. Ma allora $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$. Essendo $N(\alpha)$ un intero non negativo, deve essere $N(\alpha) = 1$. Quindi, per essere invertibile, un elemento di $\mathbb{Z}[\sqrt{-3}]$ deve avere norma uguale ad 1. Ora, la relazione $a^2 + 3b^2 = 1$ con $a, b \in \mathbb{Z}$ comporta $b = 0$ e $a = \pm 1$. Gli unici elementi invertibili in $\mathbb{Z}[\sqrt{-3}]$ sono pertanto ± 1 . Ciò premesso, vogliamo provare che in $\mathbb{Z}[\sqrt{-3}]$ esistono elementi irriducibili che non sono primi. Un tale elemento è ad esempio $1 - \sqrt{-3}$: supponiamo che sia $(1 - \sqrt{-3}) = (a + b\sqrt{-3})(c + d\sqrt{-3})$ in $\mathbb{Z}[\sqrt{-3}]$. Passando alle norme, sarà

$$4 = N(a + b\sqrt{-3})N(c + d\sqrt{-3}) = (a^2 + 3b^2)(c^2 + 3d^2).$$

L'unica possibilità è che sia $a^2 + 3b^2 = 1$ oppure $a^2 + 3b^2 = 4$, non potendo essere $a^2 + 3b^2 = 2$. La prima relazione comporta, come abbiamo visto, $a = \pm 1$, $b = 0$, cioè $a + b\sqrt{-3}$ invertibile, nel secondo caso sarà $c + d\sqrt{-3}$ ad essere invertibile. Dato che $1 + \sqrt{-3}$ è non nullo e non invertibile, abbiamo provato che $1 - \sqrt{-3}$ è irriducibile. Tuttavia non è primo: infatti dalla relazione

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 2 \cdot 2$$

che si verifica facilmente, segue che $1 + \sqrt{-3}$ divide $2 \cdot 2$, ma non divide 2: se infatti $1 + \sqrt{-3}$ dividesse 2, sarebbe $2 = (1 + \sqrt{-3})(a + b\sqrt{-3})$ per qualche $a, b \in \mathbb{Z}$, da cui, passando alle norme, si avrebbe la seguente uguaglianza in \mathbb{N} :

$$4 = 4 \cdot (a^2 + 3b^2)$$

da cui $a^2 + 3b^2 = 1$ cioè $a = \pm 1$ e $b = 0$, ossia $a + b\sqrt{-3} = \pm 1$, che darebbe la relazione assurda

$$2 = \pm(1 + \sqrt{-3}).$$

Quindi in generale irriducibile non implica primo.

Esiste una classe importante di anelli in cui la proposizione precedente si può invertire. Studieremo nel prossimo paragrafo tale classe di anelli.



ESERCIZI.

1. Sia a un elemento non nullo di un dominio di integrità con unità. Si dimostrri che a è primo se e solo se (a) è un ideale primo.
2. Si consideri la relazione (di equivalenza) di *essere associati*: si provi che la classe che contiene un elemento invertibile è costituita da tutti e soli gli elementi invertibili dell'anello.
3. Si determinino tutti gli elementi invertibili di $\mathbb{Z}[\sqrt{-7}] = \{a + b\sqrt{-7} \mid a, b \in \mathbb{Z}\}$.
4. Sia R l'anello degli interi di Gauss. Siano $I = (13)$ e $J = (3 - 2i)$. Si dica quale (quali) tra I e J sono ideali massimali. Nel caso in cui uno non sia massimale si esibisca un ideale che lo contiene.
5. Si provi che in $\mathbb{Z}[\sqrt{-5}]$ l'ideale $(3, \sqrt{-5} - 1)$ non è un ideale principale. Se ne deduca che $\mathbb{Z}[\sqrt{-5}]$ non è un dominio euclideo.
6. Si dica quali tra gli elementi di $\mathbb{Z}[\sqrt{-7}]$ che seguono sono tra loro associati:

$$3 + 4\sqrt{-7}, \quad -3 + 4\sqrt{-7}, \quad -3 - 4\sqrt{-7}.$$

7. In $\mathbb{Z}[i]$ determinare, nel caso in cui esista, il MCD tra i due seguenti interi di Gauss:

$$4 + 4i, \quad -5 + 7i.$$

8. Si dica se 3 è un elemento primo in $\mathbb{Z}[i]$.
9. Si studi il quoziente $\mathbb{Z}[i]/(2)$.
10. Si provi che un intero di Gauss $a + ib$, con $a \neq 0, b \neq 0$ è irriducibile se e solo se $a^2 + b^2$ è un numero primo di \mathbb{Z} .



ESERCIZI DI PROGRAMMAZIONE.

1. Fare un programma che operi la divisione tra interi di Gauss.
2. Fare un programma che riesca a decidere se un intero di Gauss è irriducibile (si veda l'esercizio 4.3.10).



CONTROLLO.

1. Un dominio euclideo è ...
2. In quali tipi di anelli visti finora esiste il MCD?

4.8. Domini a fattorizzazione unica

Come abbiamo detto alla fine del paragrafo precedente, tratteremo qui di una classe di anelli per la quale le nozioni di elemento primo e di elemento irriducibile coincidono. Vedremo che tale classe conterrà la classe degli anelli euclidei.

4.8.1 DEFINIZIONE. Si dice che un dominio di integrità con unità è un *dominio a fattorizzazione unica* se ogni elemento a non nullo e non invertibile si può scrivere come prodotto

$$a = \pi_1 \pi_2 \cdots \pi_n$$

dove i π_i sono irriducibili. Inoltre, se

$$a = \pi'_1 \pi'_2 \cdots \pi'_m$$

è un'altra fattorizzazione di a in fattori irriducibili, allora $m = n$ ed esiste una permutazione σ degli indici $1, 2, \dots, n$ tale che π'_i è associato a $\pi_{\sigma(i)}$ per ogni $i = 1, 2, \dots, n$. \square

La seguente proposizione caratterizza gli anelli a fattorizzazione unica, e spesso sarà preferibile utilizzare queste proprietà per provare che un dominio di integrità è a fattorizzazione unica.

4.8.2 PROPOSIZIONE. *Un dominio di integrità R con 1 è a fattorizzazione unica se e solo se valgono le seguenti proprietà:*

- (α) *ogni elemento irriducibile è primo;*
- (β) *data comunque una successione $a_1, a_2, \dots, a_i, \dots$ di elementi di R , tale che per ogni i $a_{i+1} | a_i$, allora esiste un indice j tale che, per ogni $h, k \geq j$, a_h è associato ad a_k .*

Dimostrazione. Supponiamo che R sia a fattorizzazione unica. Dimostriamo che vale la condizione (α). Sia a irriducibile, e sia $a = bc$, cioè sia $bc = aq$. Utilizzando la fattorizzazione in irriducibili di ogni elemento di R (e il fatto che a per ipotesi è irriducibile), sarà

$$b_1 b_2 \cdots b_h c_1 c_2 \cdots c_k = a q_1 q_2 \cdots q_s$$

dove i b_i, c_i, q_i sono irriducibili. Per l'unicità della fattorizzazione, a deve essere associato o ad un b_i o ad un c_i , e quindi a divide b oppure a divide c , che è la condizione richiesta per essere primo.

Dimostriamo ora che vale la condizione (β). Sia $a_1, a_2, \dots, a_i, \dots$ una successione tale che $a_{i+1} | a_i$ per ogni i . Sia n_i il numero di fattori irriducibili nella fattorizzazione (unica) di a_i , per ogni i . Allora si avrà la seguente situazione:

$$\begin{array}{ccccccccc} a_1 & a_2 & a_3 & \dots & a_j & a_{j+1} & \dots & a_i & a_{i+1} & \dots \\ n_1 & \geq n_2 & \geq n_3 & \geq \cdots & \geq n_j & = n_{j+1} & = \cdots & = n_i & = n_{i+1} & = \cdots \end{array}$$

Infatti, dato che gli n_i sono una successione non crescente di interi positivi, deve esistere un indice j tale che $n_j = n_{j+1} = n_{j+2} = \dots$, cioè da un certo indice j in poi tutti gli a_i hanno lo stesso numero di fattori irriducibili. Ma, dato che $a_{i+1} | a_i$, cioè $a_i = a_{i+1}q$, per $i \geq j$ deve essere a_{i+1} associato ad a_i .

Supponiamo ora che valgano (α) e (β).

Mostriamo l'esistenza di una fattorizzazione. Supponiamo per assurdo che esista un a in R non invertibile e non prodotto di irriducibili. In particolare non sarà irriducibile, quindi esisterà una fattorizzazione non banale

$$a = a_1 b_1$$

dove a_1 e b_1 non sono associati ad a , e uno almeno dei due non è prodotto di irriducibili; sia questo a_1 . Allora a sua volta sarà

$$a_1 = a_2 b_2$$

con a_2 e b_2 non associati ad a_1 , e almeno uno dei due non prodotto di irriducibili, sia esso a_2 . In generale

$$a_i = a_{i+1} b_{i+1}$$

con a_{i+1} , b_{i+1} non associati ad a_i e almeno uno dei due non è prodotto di irriducibili; sia ad esempio a_{i+1} . Questo procedimento non può terminare. Esiste allora una successione infinita $(a_i)_{i \in \mathbb{Z}}$ con $a_{i+1} | a_i$, tale che gli elementi non diventano mai associati tra di loro. Questo contrasta (β).

Proviamo ora l'unicità della fattorizzazione. Supponiamo di avere due fattorizzazioni di uno stesso elemento:

$$(4.8.1) \quad a_1 a_2 \cdots a_n = a'_1 a'_2 \cdots a'_m,$$

a_i, a'_i irriducibili. Procediamo per induzione sul numero dei fattori della fattorizzazione più corta. Per $n = 1$ la (4.8.1) diventa

$$(4.8.2) \quad a_1 = a'_1 a'_2 \cdots a'_t$$

a'_1 divide a_1 , ma essendo a_1 irriducibile a_1 è associato ad a'_1 . Cancellandoli da entrambi i membri si ottiene

$$1 = a'_2 a'_3 \cdots a'_t, \quad u \text{ invertibile in } R$$

che ci dice che tutti gli a'_i , per $i = 2, \dots, t$ sono invertibili. Quindi anche il lato destro della (4.8.2) è formato da un solo fattore irriducibile a'_1 . Supponiamo ora di avere provato il teorema nel caso $n - 1$ e proviamolo per n . L'elemento a'_1 , in quanto irriducibile, sarà anche primo per ipotesi; quindi deve dividere almeno uno dei fattori del primo membro; supponiamo che divida a_1 . Essendo a_1 irriducibile, a_1 e a'_1 sono associati. Possono allora essere cancellati in entrambi i membri (a meno di un fattore invertibile). Si ottiene così una relazione più corta, e si può procedere allora per induzione. \square

4.8.3 PROPOSIZIONE. *In ogni dominio a fattorizzazione unica, ogni coppia di elementi non entrambi nulli possiede un massimo comun divisore.*

Dimostrazione. Siano a e b due elementi di R . Scomponiamoli in fattori irriducibili, raccogliendo tutti gli elementi associati tra di loro, e assumendo che gli esponenti h_i e k_i possano essere nulli (quando cioè il corrispondente fattore non compare nella decomposizione). In questo modo a e b vengono ad avere formalmente lo stesso numero di fattori (anche se non tutti irriducibili, perché, ripetiamo, alcuni fattori possono in realtà non essere presenti, cioè essere uguali all'elemento invertibile 1, perché compaiono con esponente nullo). Sarà allora

$$a = up_1^{h_1} p_2^{h_2} \cdots p_n^{h_n}, \quad b = vp_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}, \quad u, v \text{ invertibili}.$$

Un massimo comun divisore, come si verifica facilmente, sarà

$$d = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$$

dove $m_j = \min(h_j, k_j)$. \square

Mostriamo ora che ogni dominio principale è a fattorizzazione unica.

4.8.4 PROPOSIZIONE. *Sia R un dominio principale. Allora esso è a fattorizzazione unica.*

Dimostrazione. Faremo vedere che in R valgono le condizioni (α) e (β) della caratterizzazione degli anelli a fattorizzazione unica.

(α) Ogni irriducibile è primo. Sia a un elemento irriducibile di R , e sia $a \mid bc$. Se I è l'ideale generato da a e b , allora esisterà un elemento d tale che $I = (a, b) = (d)$. Pertanto, sarà

$$a = dh, \quad b = dk.$$

Poiché a è irriducibile, sarà o $d \sim a$ oppure $d \sim 1$. Nel primo caso $a \mid b$, nel secondo caso, scegliendo $d = 1$, risulta $1 = ra + sb$ per opportuni r ed s in R , da cui $c = rac - sbc$ che implica $a \mid c$. Quindi a è primo.

(β) Sia $\{a_i\}$ una successione di elementi di R tali che $a_{i+1} \mid a_i$ per ogni i . Sia $I = (a_1, a_2, a_3, \dots, a_i, \dots)$ l'ideale generato da tutti gli elementi a_i . Per le ipotesi, sarà

$$I = (a_1, a_2, a_3, \dots, a_i, \dots) = (d)$$

per qualche $d \in R$. Dato che ogni elemento di I (cfr. §4.5) è una combinazione finita di a_i , sarà

$$d = r_1 a_1 + r_2 a_2 + r_3 a_3 + \cdots + r_j a_j$$

per qualche $j \in \mathbb{N}$. Ora, dato che ogni a_i è multiplo del successivo, la relazione precedente potrà essere scritta come

$$d = r_1 a_j a_1 + r_2 a_j a_2 + \cdots + r_j a_j$$

che ci assicura che per ogni $i \geq j$ $a_i \mid d$. Ma d'altra parte, $d \mid a_i$ per ogni i . Quindi

$$\begin{cases} a_i \mid d & \text{per ogni } i \geq j \\ d \mid a_i & \text{per ogni } i \end{cases}$$

implicano

$$a_i \sim d \quad \forall i \geq j$$

cioè per $i \geq j$ tutti gli a_i sono associati. \square

4.8.5 COROLLARIO. *Ogni dominio euclideo è a fattorizzazione unica.*

Ritroviamo quindi che $\mathbb{K}[x]$ è a fattorizzazione unica.

Ci poniamo ora il seguente problema. Dato un anello R , quali delle proprietà di cui gode R si trasmettono all'anello $R[x]$ dei polinomi in una indeterminata a coefficienti nell'anello R ? Sappiamo ad esempio che se R è un dominio di integrità, allora anche $R[x]$ è un dominio di integrità, ma altre proprietà non si trasmettono: ad esempio il fatto di essere a ideali principali non si trasmette: $\mathbb{Q}[x]$ è principale, ma tale non è $\mathbb{Q}[x,y] = (\mathbb{Q}[x])[y]$. Quindi non si trasmette il fatto di essere un dominio euclideo (\mathbb{Z} lo è, ma $\mathbb{Z}[x]$ non lo è) o il fatto di essere un campo (\mathbb{Q} è un campo, ma $\mathbb{Q}[x]$ non lo è). Mostreremo ora che, se R è un anello a fattorizzazione unica, tale è anche $R[x]$, cioè la proprietà della fattorizzazione unica si conserva nel passaggio da un anello R all'anello dei polinomi a coefficienti in R .

Si consiglia lo studente di riandare al §3.3, dove si è trattato di questioni di irriducibilità di polinomi a coefficienti in \mathbb{Z} e in \mathbb{Q} , perché riprenderemo molte delle definizioni date e soprattutto qui come allora entrerà in gioco in modo pesante il legame che intercorre tra un dominio di integrità ed il suo *campo dei quozienti* e quindi tra polinomi a coefficienti in un dominio di integrità e polinomi a coefficienti nel campo dei quozienti.

Sia quindi R un dominio a fattorizzazione unica, e sia

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

un polinomio in $R[x]$.

4.8.6 DEFINIZIONE. Si definisce *contenuto* o *divisore* del polinomio $f(x)$ il MCD dei suoi coefficienti, e si indica con $d(f(x))$, cioè

$$d(f(x)) \stackrel{\text{def}}{=} \text{MCD}(a_0, a_1, a_2, \dots, a_n) . \quad \square$$

Questa definizione ha senso, perché abbiamo appena dimostrato che in un dominio a fattorizzazione unica esiste il massimo comun divisore.

4.8.7 DEFINIZIONE. Un polinomio $f(x) \in R[x]$ si dice *primitivo* se il suo contenuto $d(f(x)) \sim 1$ (cioè se il contenuto è un elemento invertibile in R , ossia se i coefficienti del polinomio sono coprimi). \square

Vale la seguente proposizione.

4.8.8 PROPOSIZIONE. Sia R un dominio a fattorizzazione unica. Allora il prodotto di due polinomi primitivi in $R[x]$ è ancora un polinomio primitivo.

Dimostrazione. La dimostrazione è identica alla dimostrazione fatta nel lemma di Gauss (§3.3). L'unica avvertenza è quella di sostituire *numero primo* con *elemento irriducibile*, e ricordare che in un anello a fattorizzazione unica le due nozioni di *elemento primo* e *elemento irriducibile* coincidono. \square

4.8.9 COROLARIO. Se R è un anello a fattorizzazione unica, e se $f(x)$ e $g(x)$ appartengono a $R[x]$, allora

$$d(f(x)g(x)) = d(f(x))d(g(x)),$$

cioè il contenuto del prodotto di due polinomi uguaglia il prodotto dei contenuti.

Dimostrazione. Si può scrivere

$$f(x) = \alpha f^*(x), \quad g(x) = \beta g^*(x)$$

dove con α e β si è indicato il contenuto rispettivamente di $f(x)$ e di $g(x)$, e $f^*(x)$ e $g^*(x)$ sono polinomi primitivi. Allora

$$f(x)g(x) = \alpha \underbrace{\beta f^*(x)g^*(x)}_{\text{primitivo}} \implies d(f(x)g(x)) = \alpha \beta = d(f(x))d(g(x)). \quad \square$$

Entra ora in gioco, come si è detto, il fatto che un dominio a fattorizzazione unica, in quanto dominio di integrità, è immersibile nel suo campo dei quozienti $Q(R)$. Abbiamo visto che c'è uno stretto legame tra la riducibilità o irriducibilità di un polinomio di $\mathbb{Z}[x]$ su \mathbb{Z} e la sua riducibilità o irriducibilità dello stesso polinomio su \mathbb{Q} . Infatti

$$f(x) \in \mathbb{Z}[x] \text{ primitivo è irriducibile su } \mathbb{Z} \iff f(x) \text{ è irriducibile su } \mathbb{Q}.$$

Se poi $f(x)$ è un qualunque polinomio di $\mathbb{Z}[x]$ (anche non primitivo), la sua riducibilità su \mathbb{Q} implica la riducibilità su \mathbb{Z} . Un risultato identico vale nel caso attuale. Vale cioè un risultato analogo al teorema di Gauss (§3.3).

4.8.10 PROPOSIZIONE. Sia R un dominio a fattorizzazione unica, e sia $f(x) \in R[x]$. Allora se $f(x)$ si decomponete nel prodotto di due polinomi a coefficienti in $Q(R)$, allora si decomponete anche nel prodotto di due polinomi degli stessi gradi a coefficienti in R .

Dimostrazione. Identica alla dimostrazione del teorema di Gauss sopra menzionato. Basta ricordare che ogni elemento di $Q(R)$ si scrive come quoziente di elementi di R , così come avveniva in \mathbb{Q} . \square

 **ATTENZIONE.** Per polinomi *primativi* non occorre fare distinzione tra fattorizzazioni in $R[x]$ e fattorizzazioni in $Q(R)[x]$. Utilizzeremo questo fatto per provare il risultato annunciato all'inizio del paragrafo. \square

4.8.11 TEOREMA. *Se R è un dominio a fattorizzazione unica, allora anche $R[x]$ lo è.*

Dimostrazione. Dobbiamo provare che ogni elemento $f(x) \in R[x]$ che non sia invertibile è fattorizzabile in modo unico nel prodotto di fattori irriducibili. Scriviamo innanzitutto $f(x)$ al modo seguente:

$$(4.8.3) \quad f(x) = \underbrace{\alpha \cdot \underbrace{f^*(x)}_{\text{primitivo}}}_{\text{decomposizione unica}}.$$

Vediamo di fattorizzare separatamente i due fattori.

Cominciamo da $f^*(x)$. Pensando $f^*(x)$ come polinomio in $Q(R)[x]$, che è a fattorizzazione unica, perché $Q(R)$ è un campo, potremo fattorizzarlo in modo unico al modo seguente:

$$f^*(x) = p_1(x)p_2(x)p_3(x) \cdots p_n(x),$$

$p_i(x) \in Q(R)[x]$, $p_i(x)$ irriducibili su $Q(R)$. Ogni $p_i(x)$ a sua volta, con il solito procedimento, e usando le stesse notazioni usate nel corso della dimostrazione del teorema di Gauss, si può scrivere come

$$p_i(x) = \frac{d_i}{m_i} p_i^*(x), \quad d_i, m_i \in R$$

$p_i^*(x) \in R[x]$ e primitivi. Quindi

$$f^*(x) = \frac{d_1}{m_1} \cdot \frac{d_2}{m_2} \cdots \frac{d_n}{m_n} \cdot p_1^*(x)p_2^*(x) \cdots p_n^*(x)$$

da cui

$$m_1 m_2 \cdots m_n f^*(x) = d_1 d_2 \cdots d_n \underbrace{p_1^*(x)p_2^*(x) \cdots p_n^*(x)}_{\text{primitivo}},$$

Confrontando i contenuti, si ottiene

$$f^*(x) = p_1^*(x)p_2^*(x) \cdots p_n^*(x)$$

che rappresenta una fattorizzazione di $f^*(x)$ su R . Si tratta di una fattorizzazione in irriducibili su R . Infatti i $p_i^*(x)$, essendo associati in $Q(R)[x]$ ai $p_i(x)$ (che sono irriducibili su $Q(R)$), sono irriducibili su $Q(R)$; ma essendo primitivi, sono irriducibili anche su R .

Resta da provare che tale fattorizzazione è unica. Supponiamo

$$f^*(x) = p_1^*(x)p_2^*(x) \cdots p_n^*(x) = q_1(x)q_2(x) \cdots q_r(x)$$

con $q_i(x)$ irriducibili su R . Ora, queste sono due fattorizzazioni in fattori irriducibili anche su $Q(R)$, dove la fattorizzazione è unica; quindi deve essere $n = r$ e i $q_i(x)$ devono essere associati (in $Q(R)[x]$) ai $p_j^*(x)$. Ma, essendo i $q_i(x)$, come si verifica facilmente, primitivi anch'essi, devono essere associati ai $p_j^*(x)$ anche in R , e quindi la fattorizzazione è unica.

Passiamo ora alla fattorizzazione di α in (4.8.3). È facile vedere (si dimostrerà) che α può essere fattorizzato solamente come prodotto di elementi di R . $\alpha = \alpha_1\alpha_2 \cdots \alpha_s$ e in tale caso la fattorizzazione è unica per ipotesi. Quindi in definitiva,

$$f(x) = \underbrace{\alpha_1\alpha_2 \cdots \alpha_s}_{\text{fattorizzazione unica}} \cdot \underbrace{p_1^*(x)p_2^*(x) \cdots p_n^*(x)}_{\substack{\text{fattorizzazione unica} \\ \text{fattorizzazione unica}}} \underbrace{\alpha_1\alpha_2 \cdots \alpha_s}_{\text{fattorizzazione unica}}$$

e il teorema è completamente provato. \square

4.8.12 COROLLARIO. Se R è un dominio a fattorizzazione unica (in particolare se R è un campo), allora $R[x_1, x_2, \dots, x_n]$ è un dominio a fattorizzazione unica.

ESERCIZI.

- Si determinino le unità dell'anello $\mathbb{Z}[\sqrt{-5}]$ e si provi che l'anello non è a fattorizzazione unica.
- Si provi che le seguenti fattorizzazioni mostrano che i corrispondenti anelli non sono a fattorizzazione unica:

$$4 = 2 \cdot 2 = (3 + \sqrt{5})(3 - \sqrt{5}) \quad \text{in } \mathbb{Z}[\sqrt{5}].$$

$$6 = 2 \cdot 3 = (\sqrt{-6})(-\sqrt{-6}) \quad \text{in } \mathbb{Z}[\sqrt{-6}].$$

- Si provi che in $\mathbb{Z}[\sqrt{-5}]$ esistono coppie di elementi che non ammettono MCD.
- Si provi che in $\mathbb{K}[x, y]$, pur esistendo MCD tra due qualunque elementi non entrambi nulli, tuttavia non vale sempre l'identità di Bézout.

CONTROLLO.

- Che relazione esiste tra domini principali e domini a fattorizzazione unica?
- Elementi primi ed elementi irriducibili in domini a fattorizzazione unica. Esistono in tali anelli elementi irriducibili che non sono primi?

4.9. Confronto tra gli anelli studiati e applicazioni

Nei paragrafi precedenti abbiamo incontrato diversi tipi di anelli: i domini euclidei, principali, a fattorizzazione unica. Tutti questi anelli sono domini di integrità con unità 1, ed inoltre in ciascuno di questi anelli esiste il massimo comun divisore di due elementi non entrambi nulli.

Vogliamo in questo paragrafo raccogliere i risultati dei paragrafi precedenti, per poter vedere come tali anelli sono collegati fra loro.

Indichiamo con

$$\mathcal{C} = \{\text{campi}\},$$

$$\mathcal{E} = \{\text{domini euclidei}\},$$

$$\mathcal{P} = \{\text{domini principali}\},$$

$$\mathcal{F} = \{\text{domini a fattorizzazione unica}\},$$

$$\mathcal{D} = \{\text{domini di integrità con unità}\}.$$

Abbiamo visto che un campo è un dominio euclideo, un dominio euclideo è un dominio principale (proposizione 4.7.6), che un dominio principale è a fattorizzazione unica (proposizione 4.8.4). Quindi si hanno le seguenti inclusioni:

$$\boxed{\mathcal{C} \subset \mathcal{E} \subset \mathcal{P} \subset \mathcal{F} \subset \mathcal{D}}.$$

Le inclusioni sono proprie: basta dare esempi di domini di integrità con unità che non sono a fattorizzazione unica, di domini a fattorizzazione unica non principali, di domini principali che non sono domini euclidei, di domini euclidei che non sono campi.

4.9.1 ESEMPIO DI DOMINIO D'INTEGRITÀ CON UNITÀ CHE NON È A FATTORIZZAZIONE UNICA. Un tale esempio è $\mathbb{Z}[\sqrt{-3}]$. Infatti la uguaglianza

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 2 \cdot 2$$

che abbiamo già incontrato rappresenta due fattorizzazioni diverse in irriducibili di uno stesso elemento (completare la dimostrazione).

4.9.2 ESEMPIO DI ANELLO A FATTORIZZAZIONE UNICA CHE NON È PRINCIPALE. Un tale esempio è $\mathbb{Z}[x]$. $\mathbb{Z}[x]$ è a fattorizzazione unica (teorema 4.8.11) ma non è principale: infatti si consideri l'ideale $I = (2, x)$. Esso consiste di tutti i polinomi di $\mathbb{Z}[x]$ con termine noto pari. Non potrà mai esistere un polinomio $f(x) \in \mathbb{Z}[x]$ tale che $I = (f(x))$. Infatti dovrebbe essere contemporaneamente $2 = f(x)h(x)$ e $x = f(x)k(x)$, $h(x), k(x) \in \mathbb{Z}[x]$, il che è impossibile (si provi!).

4.9.3 ESEMPIO DI ANELLO PRINCIPALE NON EUCLIDEO. Un tale esempio è

$$\mathbb{Z}\left[\frac{1 + \sqrt{-19}}{2}\right] = \{a + b\sqrt{-19} \mid a, b \in \mathbb{Z}, a, b \text{ entrambi pari o entrambi dispari}\}.$$

Non diamo tuttavia la dimostrazione di questo fatto.

Chiudiamo il paragrafo con alcune applicazioni alla teoria dei numeri della teoria svolta. Utilizzeremo cioè un risultato degli interi di Gauss per ottenere un risultato di teoria dei numeri, che a sua volta ci sarà utile per risolvere alcuni problemi di algebra.

4.9.4 TEOREMA. *Sia p un numero dispari in \mathbb{Z} . Allora p è una somma di due quadrati se e solo se $p \equiv 4k+1$.*

Dimostrazione. Un numero dispari p è congruo ad 1 o a 3 modulo 4, cioè

$$p \equiv 1 \pmod{4}, \quad \text{o} \quad p \equiv 3 \pmod{4}.$$

Ora, se $p \equiv 3 \pmod{4}$, allora p non può essere somma di due quadrati: infatti, modulo 4, ogni intero a può essere congruo a 0, 1, 2 o 3, per cui $a^2 \equiv 0, 1$ modulo 4. Ne segue che

$$a^2 + b^2 \not\equiv 0, 1, 2 \pmod{4}.$$

Quindi, se $p \equiv 3 \pmod{4}$ l'equazione $p = a^2 + b^2$ è impossibile, cioè p non è somma di 2 quadrati. Abbiamo così provato che se p primo dispari è una somma di due quadrati, allora necessariamente $p \equiv 1 \pmod{4}$.

Proviamo ora il viceversa, cioè che se p è un numero dispari tale che $p \equiv 1 \pmod{4}$, allora risulta $p = a^2 + b^2$ per opportuni a e b in \mathbb{Z} . Osserviamo innanzitutto che se p è un numero della forma $4k+1$, allora la congruenza

$$x^2 \equiv -1 \pmod{p}$$

ammette soluzioni. Faremo vedere che una tale soluzione è $x = ((p-1)/2)!$. Infatti, dato che $p-1 = 4k$, i fattori del prodotto

$$x = \left(\frac{p-1}{2} \right)!$$

sono in numero pari, per cui x si può scrivere anche nella forma

$$x = (-1) \cdot (-2) \cdot (-3) \cdots \left(-\frac{p-1}{2} \right).$$

Ma $p-h \equiv -h \pmod{p}$, da cui

$$\begin{aligned} x^2 &= (1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2})(-1)(-2) \cdots \left(-\frac{p-1}{2} \right) \\ &\equiv (1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2})(p-1)(p-2) \cdots \frac{p+1}{2} \\ &= 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-1) = (p-1)! \equiv -1 \pmod{p}. \end{aligned}$$

L'ultima congruenza per il teorema di Wilson.

Abbiamo così trovato una soluzione di $x^2 \equiv -1 \pmod{p}$. Ciò significa che p divide $1 + x^2$, dove $x = ((p-1)/2)!$. Ora, pensando $1 + x^2$ come un elemento di $\mathbb{Z}[i]$, e scrivendolo come $1 + x^2 = (1+ix)(1-ix)$, si ha

$$p \mid (1+ix)(1-ix) \quad \text{in } \mathbb{Z}[i]$$

cioè p divide il prodotto $(1+ix)(1-ix)$, ma non divide nessuno dei due fattori; se infatti fosse

$$1 \pm i \left(\frac{p-1}{2} \right)! = p(a+ib)$$

per qualche $a, b \in \mathbb{Z}$, si avrebbe $pa = 1$ che è chiaramente assurdo. Quindi p non è primo in $\mathbb{Z}[i]$, per cui non è irriducibile. Ne segue che per qualche $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ deve essere

$$p = (\alpha + i\beta)(\gamma + i\delta),$$

da cui, passando alle norme

$$p^2 = (\alpha^2 + \beta^2)(\gamma^2 + \delta^2)$$

che è una fattorizzazione in \mathbb{N} , da cui si deduce $p = \alpha^2 + \beta^2$. \square

Diamo ora alcuni risultati utili nelle applicazioni.

4.9.5 PROPOSIZIONE. *Il prodotto di due somme di due quadrati è ancora una somma di due quadrati.*

Dimostrazione. Infatti

$$\begin{aligned} (a^2 + b^2)(c^2 + d^2) &= N(a+ib)N(c+id) = N((a+ib)(c+id)) \\ &= N(ac - bd - i(ad - bc)) = (ac - bd)^2 + (ad - bc)^2. \quad \square \end{aligned}$$

La proposizione ora provata dice che l'insieme degli interi esprimibili come somma di due quadrati è chiuso rispetto alla moltiplicazione.

Osservando che la norma di un numero complesso è uguale alla norma del suo coniugato, accanto all'espressione (4.9.1) si ha anche la seguente:

$$(a^2 - b^2)(c^2 - d^2) = (ac + bd)^2 + (ad - bc)^2.$$

Così ad esempio

$$\begin{aligned} 221 &= 13 \cdot 17 = (2^2 + 3^2)(4^2 + 1^2) = (2 \cdot 4 - 3 \cdot 1)^2 + (2 \cdot 1 + 3 \cdot 4)^2 = 5^2 + 14^2 \\ &= (2 \cdot 4 + 3 \cdot 1)^2 + (2 \cdot 1 - 3 \cdot 4)^2 = 11^2 + 10^2. \end{aligned}$$

4.9.6 TEOREMA. *Sia n un intero positivo tale che nella sua fattorizzazione in irriducibili i numeri primi della forma $4k+3$ compaiano tutti ad una potenza pari. Allora n è esprimibile come somma di due quadrati.*

Dimostrazione. Sia

$$n = 2^k \underbrace{p_1^{h_1} \cdot p_2^{h_2} \cdot p_3^{h_3} \cdots p_r^{h_r}}_{p_i \text{ primi della forma } 4k+1} \underbrace{q_1^{2t_1} \cdot q_2^{2t_2} \cdots q_s^{2t_s}}_{q_i \text{ primi della forma } 4k+3}$$

la fattorizzazione di n in fattori irriducibili. Per provare che n è somma di due quadrati basta, in base alla proposizione 4.9.5, provare che i tre fattori 2^k e i due fattori raggruppati nelle due parentesi graffe sono somme di due quadrati. Per quel che riguarda i primi due fattori (2^k o i prodotti di primi della forma $4k+1$) non c'è problema, perché 2 (e quindi anche le sue potenze, per la proposizione 4.9.5) è una somma di due quadrati, e ogni primo della forma $4k+1$ è somma di due quadrati (teorema 4.9.4) e quindi anche i loro prodotti lo sono. Per quel che riguarda i primi della forma $4k+3$, un primo di tale forma non è (cfr. teorema 4.9.4) somma di due quadrati, tuttavia essi compaiono nella fattorizzazione ad un esponente pari, e il quadrato di un numero chiaramente è un somma (banale) di due quadrati, quindi anche l'ultimo fattore è una somma di due quadrati e il teorema è provato. \square

Si noti che vale anche il viceversa di questo teorema. Qui sotto enunciamo il risultato completo ma ne omettiamo la dimostrazione, per la quale rinviamo ad esempio a [23].

4.9.7 TEOREMA. *Un intero n è una somma di due quadrati se e solo se i suoi divisori primi della forma $4k-3$ compaiono tutti con un esponente pari nella sua fattorizzazione in irriducibili.*

4.9.8 ESEMPI $5544 = 2^3 \cdot 3^2 \cdot 7 \cdot 11$ non è esprimibile come somma di due quadrati, perché non tutti i fattori primi del tipo $4k+3$, cioè 3, 7 e 11 compaiono ad esponente pari.

Invece $72 = 3^2 \cdot 2^3$ si può scrivere come $3^2 \cdot 2^2 \cdot 2 = (3^2 + 0^2) \cdot (2^2 + 2^2) = 6^2 + 6^2$.

Questi risultati sono utili ad esempio per rispondere alla domanda seguente: dato un intero positivo n , decidere se può rappresentare la norma di un intero di Gauss.

Concludiamo studiando gli elementi invertibili di $\mathbb{Z}[\sqrt{d}]$, d essendo un *non-quadrato* in \mathbb{Z} (in modo che \sqrt{d} non sia intero). Come abbiamo avuto già modo di osservare quando abbiamo studiato $\mathbb{Z}[\sqrt{-3}]$, conviene associare ad ogni elemento di $\mathbb{Z}[\sqrt{d}]$ una *norma*. Per poter includere sia il caso in cui d sia positivo, sia il caso in cui sia negativo, definiremo la seguente norma:

$$N(a + b\sqrt{d}) \stackrel{\text{def}}{=} a^2 - db^2.$$

Tale definizione deriva da questa osservazione: si definisce *coniugato* dell'elemento $x = a + b\sqrt{d}$ l'elemento $\bar{x} = a - b\sqrt{d}$. Allora la norma ora introdotta corrisponde a porre $N(x) = x\bar{x}$. È chiaro che, nel caso in cui d sia negativo, cioè

nel caso in cui il numero $a + b\sqrt{d}$ sia effettivamente complesso (cioè con parte immaginaria non nulla), tale norma coincide con l'ordinaria norma complessa. La norma ora introdotta è moltiplicativa, cioè

$$N((a + b\sqrt{d})(c + e\sqrt{d})) = N(a + b\sqrt{d})N(c + e\sqrt{d}) .$$

Infatti

$$N(x \cdot y) = (xy)(\bar{x}\bar{y}) = x\bar{x}y\bar{y} = N(x)N(y) .$$

Ora, sussiste il seguente fatto.

4.9.9 PROPOSIZIONE. *Gli elementi invertibili di $\mathbb{Z}[\sqrt{d}]$, d non quadrato in \mathbb{Z} , sono tutti e soli gli elementi $a + b\sqrt{d}$ tali che $N(a + b\sqrt{d}) = a^2 - db^2 = \pm 1$, cioè*

$$U(\mathbb{Z}[\sqrt{d}]) = \{a + b\sqrt{d} \mid N(a + b\sqrt{d}) = a^2 - db^2 = \pm 1\} .$$

Dimostrazione. Se x è invertibile, detto x^{-1} il suo inverso, sarà

$$1 = N(1) = N(xx^{-1}) = N(x)N(x^{-1})$$

da cui $N(x) = \pm 1$. Viceversa, se x è tale che $N(x) = \pm 1$, allora

$$\pm 1 = N(x) = x\bar{x}$$

da cui x è invertibile (se $N(x) = 1$, l'inverso di x è \bar{x} , se $N(x) = -1$, l'inverso di x è $-\bar{x}$). \square

Ciò premesso, passiamo allo studio degli elementi invertibili di $\mathbb{Z}[\sqrt{d}]$, $d \in \mathbb{Z}$ e non quadrato. Si tratta di risolvere le due equazioni

$$(4.9.1) \quad a^2 - db^2 = 1 \quad \text{e} \quad a^2 - db^2 = -1$$

in interi.

(1) $d = -1$ (caso degli interi di Gauss): si tratta di risolvere in interi le equazioni

$$a^2 + b^2 = 1, \quad \text{e} \quad a^2 + b^2 = -1 .$$

Ammette soluzioni solamente la prima: $a = \pm 1$, $b = 0$, o $a = 0$ e $b = \pm 1$. Quindi gli elementi invertibili di $\mathbb{Z}[i]$ sono ± 1 e $\pm i$.

(2) $d < -1$ (caso, ad esempio, di $\mathbb{Z}[\sqrt{-3}]$): si ha $a^2 - db^2 = a^2 + |d|b^2$ e quindi la $a^2 - db^2 = -1$ non ammette soluzioni. La $a^2 - db^2 = 1$ è soddisfatta solo se $b = 0$ e $a = \pm 1$. Quindi gli unici elementi invertibili sono ± 1 .

- (3) $d > 0$: questo è il caso più complesso. Osserviamo innanzitutto che se z è un'unità, anche $-z$ e $1/z$ lo sono. Inoltre, se $|z| > 1$ risulta $|1/z| < 1$. Quindi le unità diverse da ± 1 di $\mathbb{Z}[\sqrt{d}]$ sono del tipo $\pm z$, $\pm z^{-1}$. Se allora esiste una unità di $\mathbb{Z}[\sqrt{d}]$ diversa da ± 1 , possiamo supporre che sia $z > 1$. Esaminiamo l'equazione

$$a^2 - db^2 = 1, \quad d > 0$$

che viene comunemente chiamata l'*equazione di Pell*, anche se in realtà è stata studiata anche da Fermat. Si dimostra (cfr. ad esempio [10]) che tale equazione ammette sempre una soluzione non banale, ossia diversa da ± 1 . Sia allora u la più piccola unità maggiore di 1: una tale soluzione si può ottenere ad esempio ponendo nell'equazione $a^2 - db^2 = 1$ via via $b = 1, 2, \dots$ finché $1 + db^2$ non diventi un quadrato perfetto (esistono altri metodi più sofisticati, ma noi ci accontentiamo di questo).

Ovviamente tutte le potenze u^n , $n \in \mathbb{N}$ sono ancora unità maggiori di 1.

Sussiste il seguente teorema.

4.9.10 TEOREMA. *Sia u la più piccola unità maggiore di 1 dell'anello $\mathbb{Z}[\sqrt{d}]$, $d > 0$. Allora tutte le unità maggiori di 1 di $\mathbb{Z}[\sqrt{d}]$ sono del tipo u^n , $n \in \mathbb{N}$.*

Dimostrazione. Supponiamo per assurdo che esista una unità $x > 1$ che non sia una potenza di u . Allora x si troverà tra due potenze successive di u , ossia esisterà un intero positivo m tale che

$$u^m < x < u^{m+1}.$$

Moltiplicando tali diseguaglianze per u^{-m} si ottiene

$$1 < u^{-m}x < u.$$

Avremmo trovato una unità, $u^{-m}x$, strettamente contenuta tra 1 e u , il che contraddice la scelta di u . Quindi ogni unità maggiore di 1 è una potenza ad esponente intero positivo di u . \square

Concludendo, nel caso $d > 0$ l'equazione di Pell ammette infinite soluzioni. Si osservi che l'equazione $a^2 - db^2 = -1$ può invece non avere soluzioni. Non ci soffermiamo oltre a discutere su questo argomento: per uno studio approfondito si può consultare qualche testo di teoria dei numeri.

4.9.11 ESEMPIO. In $\mathbb{Z}[\sqrt{8}]$ la più piccola unità $x > 1$ è $x = 3 + \sqrt{8}$, come si verifica facilmente. Allora, per quanto visto, anche $17 + 6\sqrt{8} = (3 + \sqrt{8})^2$ è una unità. \square

 **ESERCIZI.**

1. Quali tra i seguenti elementi di $\mathbb{Z}[\sqrt{8}]$ sono associati?

$$4 + 3\sqrt{8}, \quad 2 + \sqrt{8}, \quad 36 + 13\sqrt{8}.$$

2. Si dica se i numeri 187 e 377 sono esprimibili o no come somma di due quadrati. In caso positivo, si scriva il numero come somma di due quadrati e si dica se tale scrittura è unica.


ESERCIZI DI PROGRAMMAZIONE.

1. Si faccia un programma che elenchi tutti i numeri interi minori di 3000 che sono somme di due quadrati.
2. Si scriva un programma che determini la soluzione minima maggiore di 1 dell'equazione di Pell.


CONTROLLO.

1. Qual è il criterio per riconoscere se un intero è una somma di due quadrati?
2. Elementi invertibili in $\mathbb{Z}[\sqrt{d}]$ per vari d .

4.10. La caratteristica di un dominio di integrità

Abbiamo dato diverse proprietà degli anelli, ad esempio la commutatività della moltiplicazione, l'esistenza di unità, l'esistenza di divisori dello zero, l'essere l'anello principale, ecc., proprietà che servono a distinguere tra loro due anelli, nel senso che se due anelli differiscono anche solo per una di queste proprietà, allora essi sono *diversi*, nel senso che non sono isomorfi. È opportuno a questo punto aggiungere un'altra proprietà che ci aiuterà in questo processo di confronto tra anelli.

Ricordiamo che, dato un anello R , la scrittura

$$n \cdot a, \quad n \in \mathbb{N}, a \in R$$

sta a significare la somma di n addendi uguali ad a , cioè

$$n \cdot a \stackrel{\text{def}}{=} \underbrace{a + a + \cdots + a}_{n \text{ volte}}.$$

Abbiamo visto anelli in cui addizionando un certo numero di volte ogni loro elemento si ottiene come risultato lo zero dell'anello, mentre altri in cui questo fatto non avviene mai. Ad esempio, in \mathbb{Z}_5 , addizionando *cinque* volte ogni elemento si ottiene come risultato lo zero, mentre in \mathbb{Z} non esiste nessun $n \in \mathbb{N}$, $n > 0$, tale che sia $n \cdot z = 0$ per ogni $z \in \mathbb{Z}$. Diamo allora la seguente definizione.

4.10.1 DEFINIZIONE. Sia R un anello. Se non esiste alcun intero positivo n tale che $n \cdot a = 0$ per ogni $a \in R$, allora si dice che R ha *caratteristica 0*. Se invece un tale n esiste, allora, detto m il minimo intero positivo tale che $m \cdot a = 0$ per ogni $a \in R$, si dice che R ha *caratteristica m*. \square

Gli anelli \mathbb{Z} , $\mathbb{K}[x]$, gli interi di Gauss, i campi \mathbb{Q} , \mathbb{R} , \mathbb{C} sono tutti esempi di anelli a caratteristica zero. Invece i campi \mathbb{Z}_p , con p primo, gli anelli $\mathbb{Z}_p[x]$ hanno caratteristica p , come si verifica facilmente.

Gli anelli \mathbb{Z} e $\mathbb{Z}_5[x]$ sono entrambi infiniti, sono entrambi domini di integrità, euclidei, tuttavia differiscono per la caratteristica, quindi non potrà mai esistere un isomorfismo di anelli tra di essi.

4.10.2 PROPOSIZIONE. *La caratteristica di un dominio di integrità R o è zero, oppure è un numero primo.*

Dimostrazione. Supponiamo che la caratteristica m di R non sia zero e non sia un numero primo, cioè supponiamo $m = m_1m_2$. Allora, per ogni $a \in R$, $0 = m \cdot a = (m_1m_2)a$, da cui anche $(m_1m_2)a \cdot a = 0$. Ora, dato che $(m_1m_2) \cdot ab = (m_1 \cdot a)(m_2 \cdot b)$, si avrà $0 = (m_1 \cdot a)(m_2 \cdot a)$. Si tratta del prodotto di due elementi di R che uguaglia zero; essendo R un dominio di integrità, uno almeno dei due fattori dovrà essere zero. Ma questo contrasta con la minimalità di m . Quindi m è un numero primo. Se R avesse unità, la dimostrazione sarebbe più semplice. Inoltre, se R ha unità, per vedere la caratteristica di R basta vedere qual è il più piccolo intero positivo m (se esiste) tale che $m \cdot 1 = 0$. \square

D'ora in poi indicheremo con p la caratteristica positiva di un dominio di integrità e scriveremo $\text{char } F = p$.

Le definizioni date valgono in particolare nel caso in cui il dominio di integrità sia un campo.

 ATTENZIONE. Se un campo è finito, la sua caratteristica è certamente finita (cioè positiva), ma non è vero il viceversa, cioè non è vero che se la caratteristica di un campo è finita, allora il campo è finito. Basta pensare al campo dei quozienti dell'anello $\mathbb{Z}_p[x]$, cioè il campo delle funzioni razionali a coefficienti in \mathbb{Z}_p , che è chiaramente infinito, ma ha caratteristica p . \square

Nel caso dei campi si dà la seguente ulteriore definizione.

4.10.3 DEFINIZIONE. Dicesi *sottocampo primo o fondamentale P* di un campo F la intersezione di tutti i sottocampi di F . \square

Si osservi che, essendo F un campo, esiste almeno un sottocampo di F , e l'intersezione di un numero arbitrario di sottocampi non è mai vuota, dato che ogni sottocampo deve per forza contenere 0 e 1.

4.10.4 TEOREMA. Se F ha caratteristica 0, il sottocampo fondamentale è isomorfo a \mathbb{Q} , se F ha caratteristica p , il sottocampo fondamentale è isomorfo a \mathbb{Z}_p .

Dimostrazione. Si parta dall'insieme D , contenuto in F , dei multipli interi dell'unità 1_F , cioè

$$D \stackrel{\text{def}}{=} \{m \cdot 1_F \mid m \in \mathbb{Z}\}.$$

È facile vedere che D è un anello, contenuto nel sottocampo fondamentale P di F . Esso prende il nome di *sottoanello fondamentale*. Definiamo la seguente applicazione:

$$\begin{aligned}\phi : \mathbb{Z} &\longrightarrow F \\ z &\longmapsto z \cdot 1_F.\end{aligned}$$

Si tratta di un omomorfismo di anelli: infatti

$$\begin{aligned}\phi(z+z') &= (z+z') \cdot 1_F = z \cdot 1_F + z' \cdot 1_F = \phi(z) + \phi(z') \\ \phi(zz') &= zz' \cdot 1_F = z \cdot 1_F \cdot z' \cdot 1_F = \phi(z) \cdot \phi(z').\end{aligned}$$

Per definizione, $\phi(\mathbb{Z}) = D$: inoltre $\text{Ker } \phi = \{z \in \mathbb{Z} \mid z \cdot 1_F = 0_F\}$. Quindi,

- (a) Se $\text{char } F = 0$, allora $\text{Ker } \phi = \{0\}$, cioè ϕ è iniettivo, e $D \simeq \mathbb{Z}$. Se vogliamo il sottocampo fondamentale, questo sarà il più piccolo sottocampo contenente \mathbb{Z} , ossia \mathbb{Q} .
- (b) Se $\text{char } F = p$, allora $\text{Ker } \phi = p\mathbb{Z}$, perché p rappresenta il più piccolo intero positivo appartenente a $\text{Ker } \phi$.

Quindi, per il teorema fondamentale di omomorfismo tra anelli, $D \simeq \mathbb{Z}_p$, che è un campo (= sottocampo fondamentale). \square

Quindi, ogni campo di caratteristica zero *contiene* il campo dei razionali, cioè si può pensare come ampliamento dei razionali, mentre ogni campo di caratteristica p contiene il campo \mathbb{Z}_p , cioè è estensione di \mathbb{Z}_p .

ESERCIZI.

1. Quanto vale la caratteristica dei seguenti anelli?

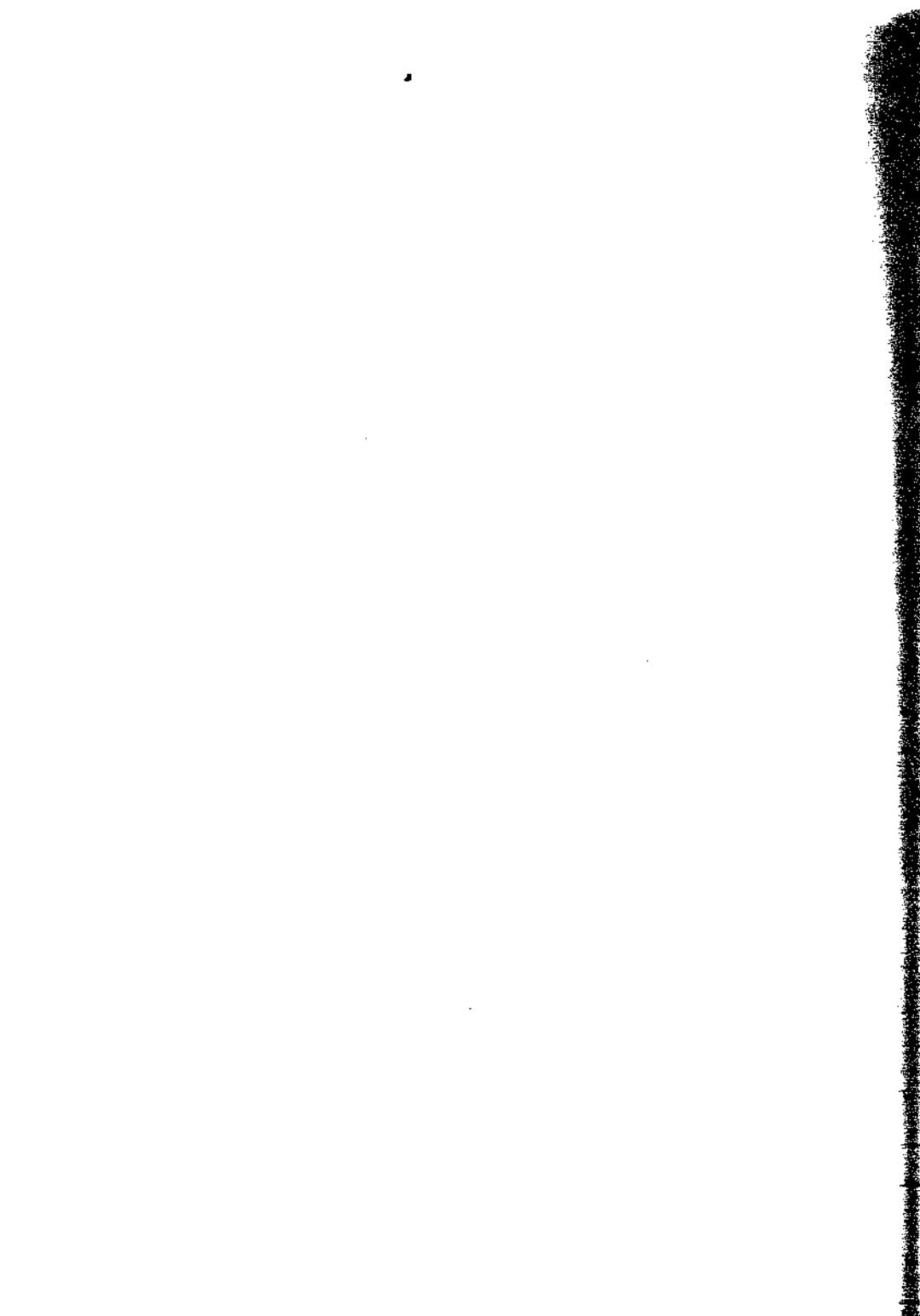
$$3\mathbb{Z}, \quad \mathbb{Z} \times 5\mathbb{Z}, \quad \mathbb{Z}_5 \times \mathbb{Z}_3.$$

2. Quanto vale la caratteristica dell'anello dell'esempio 4.1.2 (e)?

CONTROLLO.

1. La caratteristica di un dominio di integrità è sempre ...

SECONDO MODULO



CAPITOLO 5

I gruppi

*Lettor, tu vedi ben com'io innalzo,
la mia matra, e però con più arte
non ti maravigliar s'io la rincalzo.*

Dante, Purgatorio, IX, 70-73.

In questo capitolo studieremo una nuova classe di strutture algebriche, i *gruppi*: si tratta di strutture algebriche dotate di *una sola* operazione, soggetta a certe condizioni. Come si è fatto per gli anelli, allo studio sistematico dei gruppi faremo precedere l'esame di due importanti classi di gruppi, i gruppi simmetrici e i gruppi diedrali: si tratta di esempi significativi di gruppi di trasformazioni. In questi gruppi introduciamo alcune delle definizioni e delle proprietà che verranno poi date in generale. In questo modo le definizioni che verranno date e i teoremi che verranno dimostrati troveranno una giustificazione ed una esemplificazione.

5.1. Prime definizioni ed esempi

5.1.1 DEFINIZIONE. Un *gruppo* $(G, *)$ è un insieme G dotato di una operazione binaria $*$

$$\begin{aligned} G \times G &\rightarrow G \\ (a, b) &\longmapsto a * b \end{aligned}$$

che verifica le seguenti proprietà:

(a) $*$ è *associativa*, cioè

$$(a * b) * c = a * (b * c) \quad \forall a, b, c \in G;$$

(b) esiste un elemento $e \in G$ *neutro* rispetto all'operazione, tale cioè che

$$e * a = a * e = a \quad \forall a \in G;$$

(c) per ogni $a \in G$ esiste un elemento $a' \in G$, detto *inverso* di a , tale che

$$a * a' = a' * a = e \quad \forall a \in G.$$

Si noti che non si richiede la *commutatività* dell'operazione. Un gruppo $(G, *)$ in cui l'operazione è commutativa prende il nome di *gruppo abeliano*. \square

In genere, indicheremo con \cdot l'operazione del gruppo: utilizzando quindi la notazione moltiplicativa, scriveremo ab in luogo di $a \cdot b$, e denoteremo con a^{-1} l'inverso di a . Dagli assiomi di gruppo si deducono le seguenti conseguenze.

5.1.2 PROPOSIZIONE. *Sia (G, \cdot) un gruppo. Allora l'elemento neutro e è unico.*

Dimostrazione. Supponiamo per assurdo che esista un altro elemento $u \in G$, neutro rispetto all'operazione di G . Allora risulta

$$\begin{aligned} eg &= ge = g \quad \forall g \in G \\ ug &= gu = g \quad \forall g \in G. \end{aligned}$$

Le

$$\begin{aligned} eu &= ue = e \quad (u \text{ è elemento neutro}) \\ eu &= ue = u \quad (e \text{ è elemento neutro}) \end{aligned}$$

implicano $u = e$. \square

5.1.3 PROPOSIZIONE. *Sia (G, \cdot) un gruppo. Allora l'inverso di ogni elemento a di G è unico.*

Dimostrazione. Siano a' e a'' due inversi dello stesso elemento $a \in G$. Allora

$$a' = ea' = (a''a)a' = a''(aa') = a''e = a''. \quad \square$$

5.1.4 COROLLARIO. *Per ogni $a, b \in G$, l'inverso del prodotto di due elementi di G è il prodotto dei loro inversi, in ordine inverso, ossia*

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Inoltre $(a^{-1})^{-1} = a$.

Dimostrazione. Infatti $b^{-1}a^{-1}$ è un inverso di ab , quindi è l'inverso. Così, dalle $aa^{-1} = a^{-1}a = e$ segue che a è un inverso di a^{-1} , quindi è l'inverso. \square

Diamo ora alcuni esempi di gruppi. Negli esempi che seguono l'operazione $*$ sarà, a seconda dei casi, l'ordinaria addizione $+$ o la moltiplicazione \cdot .

5.1.5 ESEMPI NUMERICI.

- (a) Tutti i *gruppi (abeliani) additivi* degli anelli visti nei capitoli precedenti: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}[i], +)$, $(\mathbb{Z}[\sqrt{n}], +)$, $(\mathbb{Z}_n, +)$, $(R[x], +)$, (R anello comunitativo con unità).
- (b) Gli elementi non nulli di un *campo*, rispetto alla moltiplicazione: $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$, p primo.
- (c) $(U(\mathbb{Z}_n), \cdot) = \{\text{elementi invertibili di } \mathbb{Z}_n\}$.
- (d) L'insieme delle radici n -esime dell'unità, rispetto all'ordinaria moltiplicazione. \square

Tutti questi gruppi sono abeliani.

5.1.6 ESEMPI DI GRUPPI DI MATRICI.

$$(M_{m,n}(R), +) \stackrel{\text{def}}{=} \{\text{matrici } m \times n \text{ su un anello } R\};$$

$$(M_n(R), -) \stackrel{\text{def}}{=} \{\text{matrici quadrate } n \times n \text{ su un anello } R\};$$

$$(\mathrm{GL}_n(\mathbb{R}), \cdot) \stackrel{\text{def}}{=} \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\} = \text{gruppo lineare generale reale};$$

$$(\mathrm{SL}_n(\mathbb{R}), \cdot) \stackrel{\text{def}}{=} \{A \in M_n(\mathbb{R}) \mid \det A = 1\} = \text{gruppo lineare speciale reale};$$

$$(\mathrm{O}_n(\mathbb{R}), \cdot) \stackrel{\text{def}}{=} \{A \in M_n(\mathbb{R}) \mid A^T = A^{-1}\} = \text{gruppo ortogonale}$$

$$(\mathrm{SO}_n(\mathbb{R}), \cdot) \stackrel{\text{def}}{=} \{A \in \mathrm{O}_n(\mathbb{R}) \mid \det A = 1\}.$$

I primi due gruppi sono abeliani, tutti gli altri invece sono non abeliani per $n \geq 2$. \square

Se un gruppo $(G, *)$ è finito, con n elementi g_1, g_2, \dots, g_n , si usa rappresentarlo attraverso la sua *tavola moltiplicativa* al modo seguente:

*	g_1	g_2	g_3	\cdots	g_j	\cdots	g_n
g_1							
g_2							
g_3							
\vdots							
g_i	\cdots	\cdots	\cdots	\cdots	$g_i * g_j$	\cdots	\cdots
\vdots							
g_n							

5.1.7 DEFINIZIONE. Un *sottogruppo* S di un gruppo G è un sottoinsieme non vuoto di G tale che sia esso stesso un gruppo *rispetto alla medesima operazione di* G . \square

Quindi un sottoinsieme S di un gruppo (G, \cdot) è un sottogruppo se e solo se

- (a) l'elemento neutro e di G appartiene a S ;
- (b) S è chiuso rispetto all'operazione di G , ossia $\forall s, t \in S$ si ha $st \in S$; in altre parole, l'operazione \cdot di G è anche operazione in S , ossia

$$\cdot : S \times S \longrightarrow S:$$

- (c) per ogni s in S , $s^{-1} \in S$.

~~6.1.1~~ ATTENZIONE. $S = \{1, -1\}$ è un sottoinsieme non vuoto di \mathbb{Q} , ed è un gruppo, rispetto alla moltiplicazione, ma non è un sottogruppo di $(\mathbb{Q}, +)$, perché le operazioni di S e di \mathbb{Q} sono diverse. \square

Per indicare che un sottoinsieme H di un gruppo G è un sottogruppo di G si scrive

$$H \leq G. \quad \circ \quad H < G \quad (\text{se } H \neq G).$$

Sussiste il seguente criterio, per vedere se un sottoinsieme di un gruppo G è un sottogruppo.

5.1.8 PROPOSIZIONE. *Un sottoinsieme non vuoto S di un gruppo G è un sottogruppo di G se e solo se, dati comunque a e b in S , si ha $ab^{-1} \in S$.*

Dimostrazione. La condizione è ovviamente necessaria. Mostriamo la sufficienza. Se S è ridotto al solo elemento neutro, è automaticamente un sottogruppo. Sia allora $a \in S$, $a \neq e$: allora l'elemento $e = aa^{-1}$ sta in S . Prendendo allora i due elementi $e \in S$ e $a \in S$, si ha $a^{-1} \in S$. Infine, presi gli elementi a e b^{-1} (appartenenti ad S se a e b stanno in S per quanto mostrato ora), si ha

$$a(b^{-1})^{-1} = ab \in S.$$

La proposizione è completamente provata. \square

Diamo ora la definizione seguente.

5.1.9 DEFINIZIONE. Sia (G, \cdot) un gruppo. Dicesi centro di G il sottoinsieme di G

$$\boxed{Z(G) \stackrel{\text{def}}{=} \{g \in G : gx = xg \ \forall x \in G\}}.$$

Il centro di un gruppo è un sottogruppo di G (verificare!). \square

5.1.10 DEFINIZIONE. Sia $(G, *)$ un gruppo, sia g un elemento di G e sia i un intero. Si definisce *potenza* g^i di g con esponente i il seguente elemento di G :

$$g^i = \begin{cases} \underbrace{g * g * \cdots * g}_{i \text{ volte}} & \text{se } i > 0 \\ e & \text{se } i = 0 \\ \underbrace{g^{-1} * g^{-1} * \cdots * g^{-1}}_{-i \text{ volte}} & \text{se } i < 0. \end{cases}$$

Valgono, per ogni $i, j \in \mathbb{Z}$, le seguenti relazioni:

$$\begin{aligned} g^i * g^j &= g^{i+j} \\ (g^i)^j &= g^{ij}. \end{aligned}$$

Si lascia questa verifica per esercizio. \square

Queste definizioni si applicano qualunque sia la operazione $*$ del gruppo. Fare la *potenza* di un elemento x di un gruppo G equivale infatti ad iterare a partire da x o da x^{-1} l'operazione del gruppo.

Vale la pena di confrontare le varie definizioni viste finora a seconda che l'operazione $*$ sia la moltiplicazione \cdot o l'addizione $+$:

$$\begin{array}{lll} * = \cdot & * = + & \\ e = 1 & e = 0 & \\ a^{-1} & -a & \\ a^i = \underbrace{a \cdot a \cdots a}_{i \text{ volte}} & ia = \underbrace{a + a + \cdots + a}_{i \text{ volte}} & \text{se } i > 0 \\ a^i = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{-i \text{ volte}} & ia = \underbrace{(-a) + (-a) + \cdots + (-a)}_{-i \text{ volte}} & \text{se } i < 0. \end{array}$$

5.1.11 DEFINIZIONE. Sia G un gruppo e X un sottoinsieme di G . Si definisce *sottogruppo generato da X* il più piccolo sottogruppo di G contenente X . Esso coincide con l'intersezione di tutti i sottogruppi di G contenenti X . Si indica con $\langle X \rangle$. Quindi

$$\boxed{\langle X \rangle \stackrel{\text{def}}{=} \bigcap_{X \subseteq H \leq G} H}.$$

Nel caso in cui $X = \{g\} \subseteq G$ sia costituito da un solo elemento, allora

$$\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}.$$

Esso prende il nome di *sottogruppo ciclico* generato dall'elemento g . (Si verifichi che il sottoinsieme $\{g^i \mid i \in \mathbb{Z}\}$ è un sottogruppo contenente g e che è il più

piccolo tra tutti i sottogruppi contenenti g . Occorre mostrare che se H è un qualunque sottogruppo di G che contiene g , allora H contiene necessariamente $\langle g \rangle$). \square

La seguente proposizione ci dice chi sono nel caso generale gli elementi del sottogruppo generato da un sottoinsieme X .

5.1.12 PROPOSIZIONE. *Sia $X = \{x_1, x_2, \dots, x_n, \dots\}$ un sottoinsieme (finito o infinito) di un gruppo G . Allora*

$$\langle X \rangle = \{t_1 \cdot t_2 \cdot t_3 \cdots t_r \mid t_i \in X \text{ oppure } t_i^{-1} \in X, r \in \mathbb{N}\}.$$

Dimostrazione. Tale insieme è effettivamente un sottogruppo di G contenente X ed è contenuto in ogni sottogruppo di G che contiene X (verificare!). \square

Per capire perché si devono includere in $\langle X \rangle$ quegli elementi, facciamo un esempio, che mostri soprattutto come cambiano le cose tra il caso commutativo e quello non commutativo. Nel caso abeliano di $(\mathbb{Z}, +)$ il sottogruppo generato dai due elementi 2 e 3 è $\langle 2, 3 \rangle = \{2s + 3t \mid s, t \in \mathbb{Z}\}$ (che poi coincide con \mathbb{Z}), perché si possono *raccogliere* tutti i 2 assieme e tutti i 3 assieme. Nel caso non abeliano invece non possiamo fare questo. Ad esempio, se $X = \{a, b\}$, $\langle X \rangle$ sarà costituito da elementi del tipo

$$(5.1.1) \quad aba^{-1}baab^{-1}aaab^{-1},$$

cioè da parole di lunghezza variabile formate con un alfabeto costituito dalle lettere a , b , a^{-1} e b^{-1} . Si noti che una parola in cui le due lettere a e a^{-1} (o b e b^{-1}) sono adiacenti si può semplificare cancellando il prodotto aa^{-1} (o bb^{-1}); inoltre una parola che abbia varie lettere a adiacenti (come la (5.1.1)) si può semplificare ponendo $\underbrace{aaa \cdots a}_k = a^k$. Quindi la (5.1.1) coincide con l'elemento

$aba^{-1}ba^2b^{-1}a^3b^{-1}$. A seconda del tipo di elementi che generano G ci possono essere ulteriori semplificazioni: ad esempio, se il gruppo è abeliano, o se uno dei generatori, elevato ad una certa potenza, dà come risultato e , ecc.

Sia g un elemento di un gruppo (G, \cdot) . Può succedere che per qualche $h \in \mathbb{N}$ sia $g^h = e$ (elemento neutro di G): questo accade certamente nel caso in cui G sia finito. Infatti dovendo il sottogruppo $\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$ essere finito, esisteranno due esponenti interi distinti s e t ($s > t$) tali che $g^s = g^t$, da cui, posto $h = s - t \in \mathbb{N}$, si ha $g^h = e$. Ha senso allora la seguente definizione.

5.1.13 DEFINIZIONE. Se (G, \cdot) è un gruppo e $g \in G$, si definisce *ordine* o *periodo* di g il più piccolo intero positivo r , se esiste, tale che $g^r = e$. Se un tale intero non esiste, si dice che g ha periodo infinito. \square

Ad esempio, in $(\mathbb{Z}_4, +)$ la classe $\bar{1}$ ha periodo 4, la classe $\bar{2}$ ha periodo 2. In $(\mathbb{Z}, +)$ 1 ha periodo infinito (e così ogni elemento non nullo), in $(\mathbb{C} \setminus \{0\}, \cdot)$ l'elemento i ha periodo 4. L'elemento neutro di ogni gruppo ha periodo 1.

5.1.14 DEFINIZIONE. Sia G un gruppo finito. Dicesi *ordine* di G , e si indica con $|G|$, la sua cardinalità. \square

5.1.15 PROPOSIZIONE. *Sia G un gruppo. Se $g \in G$ ha periodo infinito e se $h \neq k$, allora $g^h \neq g^k$, e quindi $\langle g \rangle$ è un sottogruppo ciclico infinito. Se invece g ha periodo n , allora*

$$\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$$

e quindi la cardinalità di $\langle g \rangle$ è n . Inoltre $g^h = g^k$ se e solo se $h \equiv k \pmod{n}$.

Dimostrazione. Supponiamo g di periodo infinito. Allora la relazione $g^h = g^k$ (ossia $g^{h-k} = e$) implica $h = k$, per definizione di periodo infinito. Sia ora g di periodo n . Osserviamo innanzitutto che tutti gli elementi $e, g, g^2, \dots, g^{n-1}$ sono distinti (perché?). Per provare che $\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$ basta far vedere che ogni potenza g^k , $k \in \mathbb{Z}$ sta in $\{e, g, g^2, \dots, g^{n-1}\}$: infatti dividendo k per n si ha $k = nq + r$, $0 \leq r < n$, da cui $g^k = g^{nq+r} = (g^n)^q g^r = e g^r = g^r$. Quindi $g^k \in \{e, g, g^2, \dots, g^{n-1}\}$ per ogni $k \in \mathbb{Z}$.

Supponiamo ora $g^h = g^k$. Allora $g^{h-k} = e$. Dividendo $h - k$ per n si ha

$$(5.1.2) \quad h - k = nq + r, \quad 0 \leq r < n$$

da cui $g^{h-k} = (g^n)^q g^r = g^r = e$. Quest'ultima uguaglianza non contraddice il fatto che n è il periodo di g solo se $r = 0$; dalla (5.1.2) si ha $h \equiv k \pmod{n}$. Viceversa, se $h \equiv k \pmod{n}$, allora $g^{h-k} = g^{nq} = (g^n)^q = e$, ossia $g^h = g^k$. \square

Ogni elemento di un gruppo G genera, come si è visto, un sottogruppo ciclico di G . Tuttavia in genere tale sottogruppo sarà contenuto *propriamente* in G . Si dà la seguente definizione.

5.1.16 DEFINIZIONE. Un gruppo G si dice *ciclico* se esiste un elemento $g \in G$ tale che $G = \langle g \rangle$. \square

5.1.17 ESEMPI DI SOTTOGRUPPI GENERATI DA UN SOTTOINSIEME E DI GRUPPI CICLICI.

(a) Sia $G = (\mathbb{Z}, +)$.

- (i) $X = \{1\}$: $\langle 1 \rangle = \mathbb{Z}$, quindi \mathbb{Z} è un gruppo ciclico;
- (ii) $X = \{3\}$: $\langle 3 \rangle = 3\mathbb{Z} = \{\text{multipli di } 3\}$;
- (iii) $X = \{2, 3\}$: $\langle 2, 3 \rangle = \mathbb{Z}$;
- (iv) $X = \{2, 4\}$: $\langle 2, 4 \rangle = 2\mathbb{Z}$;
- (v) $X = \{m, n\}$: $\langle m, n \rangle = d\mathbb{Z}$, dove $d = \text{MCD}(m, n)$.

(b) Sia $G = \mathbb{Z}_n$. Allora $\mathbb{Z}_n = \langle 1 \rangle$, quindi \mathbb{Z}_n è ciclico.

(c) Sia $G = (\mathbb{Q} \setminus \{0\}, \cdot)$. Se $X = \{7\}$, allora

$$\langle 7 \rangle = \{7^i \mid i \in \mathbb{Z}\} = \{\dots, \frac{1}{49}, \frac{1}{7}, 1, 7, 49, \dots\}.$$

(d) Sia $G = (\text{GL}_2(\mathbb{R}), \cdot)$. Si determini $\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \rangle$. \square

5.1.18 PROPOSIZIONE. *Ogni sottogruppo di un gruppo ciclico G è un gruppo ciclico.*

Dimostrazione. Sia $H \leq G = \langle g \rangle$. Se $H = \{e\}$, allora H è certamente ciclico. Sia quindi $g^t \in H$, $g^t \neq e$. Allora anche $g^{-t} \in H$, e quindi H conterrà un elemento del tipo g^h , con $h \in \mathbb{N}$. Tra gli elementi appartenenti ad H , sia m il minimo intero positivo tale che $g^m \in H$. Proviamo che $H = \langle g^m \rangle$. Certamente $\langle g^m \rangle \subseteq H$. Viceversa, sia $g^k \in H$. Dividendo k per m si ha $k = mq + r$, $0 \leq r < m$, da cui

$$g^k = g^{mq}g^r, \quad \text{cioè} \quad g^r = g^{-mq}g^k \in H.$$

Deve allora essere $r = 0$, ossia $k = mq$, cioè $g^k = (g^m)^q \in \langle g^m \rangle$. \square

5.1.19 PROPOSIZIONE. *Sia $G = \langle g \mid g^n = 1 \rangle$ un gruppo ciclico di ordine n . Allora*

- (a) *l'ordine di ogni suo sottogruppo è un divisore di n :*
- (b) *per ogni divisore k di n esiste uno e un solo sottogruppo di G di ordine k .*

Dimostrazione. Sia $H = \langle g^m \rangle$ un sottogruppo di G . Risulta

$$(g^m)^n = (g^n)^m = e^m = e.$$

Quindi (cfr. esercizio 5.1.16), il periodo di g^m divide n . Dato che l'ordine di H coincide con il periodo di g^m , si ha la tesi.

Sia ora k un divisore di n . Il sottogruppo $\langle g^{n/k} \rangle$ ha ordine k . Faremo vedere che è l'unico sottogruppo di G di quest'ordine. Sia H un sottogruppo di G di ordine k . Esso sarà del tipo $H = \langle g^m \rangle$, con m il minimo intero positivo tale che $g^m \in H$. Inoltre, $m \mid n$, come si vede facendo la divisione di n per m . Allora $|H| = k = |\langle g^m \rangle| = n/m$. Ne segue che $m = n/k$, e quindi $H = \langle g^{n/k} \rangle$. \square

5.1.20 ESEMPIO. In $G = \langle g \mid g^{20} = e \rangle$, gruppo ciclico di ordine 20, il sottogruppo di ordine 5 è quello generato da $g^{20/5} = g^4$ ed è

$$\{g^4, (g^4)^2 = g^8, (g^4)^3 = g^{12}, (g^4)^4 = g^{16}, (g^4)^5 = g^{20} = e\}. \quad \square$$

Chiudiamo il paragrafo dando altri esempi di gruppi, di natura geometrica, i cosiddetti *gruppi di trasformazioni*. Tali gruppi hanno un'importanza notevole, dato che i gruppi (astratti) sono nati come *gruppi di trasformazioni*. Vediamo di capire di che cosa si tratta.

Sta X un insieme arbitrario. Si consideri l'insieme $\mathcal{S}(X)$ di tutte le *trasformazioni o corrispondenze biunivoche* di X in sé. Se indichiamo con \circ il prodotto operatorio, ossia se $f \circ g$ è definito da $(f \circ g)(x) = f(g(x))$, è facile vedere che $(\mathcal{S}(X), \circ)$ è un gruppo, non abeliano.

5.1.21 DEFINIZIONE. Un gruppo G si dice *gruppo di trasformazioni* di un insieme X se G è un sottogruppo del gruppo $(\mathcal{S}(X), \circ)$ di tutte le corrispondenze biunivoche di X in sé. \square

5.1.22 ESEMPI DI GRUPPI DI TRASFORMAZIONI.

(a) Il *gruppo delle isometrie* del piano.

5.1.23 DEFINIZIONE. Dicesi *isometria* o *movimento rigido* del piano una trasformazione del piano in sé che conserva le distanze. \square

L'insieme di tutte le isometrie del piano costituisce un esempio di gruppo di trasformazioni, come è facile verificare.

Qui di seguito descriviamo alcune di tali trasformazioni.

Sia $X = \mathbb{R}^2$ il piano ordinario dove si sia fissato un riferimento cartesiano. Sono isometriche:

(i) Le traslazioni T del piano in sé, cioè le corrispondenze biunivoche sui punti (x, y) del piano definite dalle

$$\begin{cases} x' = x + a, \\ y' = y + b, \end{cases} \quad a, b \in \mathbb{R}.$$

(ii) Le *riflessioni* di \mathbb{R}^2 in sé, cioè le trasformazioni del tipo

$$\begin{cases} x' = x \cos \vartheta + y \sin \vartheta \\ y' = x \sin \vartheta - y \cos \vartheta \end{cases}.$$

È facile vedere che applicando due volte una tale trasformazione si ottiene l'identità.

(iii) Le *rotazioni*, cioè le corrispondenze

$$\begin{cases} x' = -x \cos \vartheta + y \sin \vartheta \\ y' = -x \sin \vartheta - y \cos \vartheta \end{cases}.$$

Tutte queste trasformazioni complessivamente si possono rappresentare con le seguenti equazioni:

$$\begin{cases} x' = x \cos \vartheta + y \sin \vartheta + \alpha \\ y' = \varepsilon x \sin \vartheta - \varepsilon y \cos \vartheta + \beta \end{cases}$$

dove $\varepsilon = \pm 1$.

La matrice $A = \begin{pmatrix} \cos \vartheta & \sin \vartheta \\ \varepsilon \sin \vartheta & -\varepsilon \cos \vartheta \end{pmatrix}$ è una matrice *ortogonale*. Il suo determinante vale ± 1 .

Si può far vedere che il gruppo delle isometrie del piano è generato (secondo la definizione 5.1.11) dalle traslazioni, rotazioni e riflessioni. In realtà sono sufficienti le sole riflessioni per generare l'intero gruppo delle isometrie del piano (ogni isometria del piano è esprimibile come prodotto di al più tre riflessioni).

- (b) Il gruppo delle *affinità* o *trasformazioni affini* del piano. Si tratta delle corrispondenze biunivoche del piano in sé che mutano rette in rette e conservano il parallelismo. Esse si possono rappresentare mediante le seguenti equazioni:

$$\begin{cases} x' = ax + by + \alpha \\ y' = cx + dy + \beta \end{cases} \quad \det A \neq 0, \quad \text{se } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

con $\alpha, \beta \in \mathbb{R}$, $a, b, c, d \in \mathbb{R}$.

- (c) *Il gruppo di un grafo.*

5.1.24 DEFINIZIONE. Un *grafo* $\Gamma = (V, L)$ consiste di un insieme non vuoto V di *vertici* e di un insieme L di coppie non ordinate di elementi distinti di V chiamate *lati*. \square

Ad esempio, in figura 5.1 è mostrato il disegno di un grafo, con cinque vertici e sei lati. Consideriamo tutte le possibili corrispondenze biunivoche di un grafo in sé, cioè di V in sé, che mandano lati in lati. L'insieme di tali corrispondenze, rispetto al prodotto operatorio, costituisce un gruppo, detto *gruppo del grafo*. Si tratta di un gruppo di trasformazioni sull'insieme V dei vertici del grafo. Nel caso del grafo disegnato in figura, il suo gruppo è costituito da due elementi: l'applicazione identica e l'applicazione che scambia 1 con 4 e 2 con 3, e lascia fisso 5.

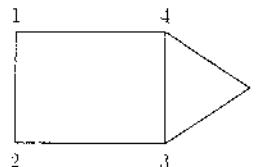


FIGURA 5.1

L'importanza dei gruppi di trasformazioni risiede nel fatto che attraverso questi gruppi si possono definire vari tipi di geometrie, nel senso che è stato suggerito da F. Klein, matematico del secolo scorso, nel suo *programma di Erlangen*. Precisamente, una geometria, secondo Klein, è lo studio delle proprietà invarianti rispetto ad un dato gruppo di trasformazioni. Quindi, ad esempio, la ordinaria *geometria euclidea* è lo studio delle proprietà invarianti rispetto al gruppo delle isometrie, la *geometria affine* è lo studio delle proprietà invarianti rispetto al gruppo affine, la *geometria proiettiva* è lo studio delle proprietà invarianti rispetto al gruppo proiettivo, la *topologia* è lo studio delle proprietà delle

figure invarianti rispetto al gruppo degli omomorfismi (ossia le applicazioni biunivoche e bicontinue), ecc.

Da queste semplici osservazioni appare chiara l'importanza dello studio dei gruppi, ed in particolare dei gruppi di trasformazioni. Come abbiamo detto, i gruppi sono nati come gruppi di trasformazioni, e solo più tardi si è sviluppata la teoria generale dei gruppi, con la loro definizione assiomatica, passando dal concreto all'astratto. Quindi, apparentemente i gruppi di trasformazioni rappresentano solamente un esempio di gruppo. Tuttavia, verrà tra breve provato l'importante teorema che afferma che *ogni gruppo si può identificare con un gruppo di trasformazioni*, dimostrando cioè che ogni gruppo *astratto* ha una sua realizzazione *concreta* come gruppo di trasformazioni.

Nei prossimi paragrafi studieremo altri importanti gruppi di trasformazioni: il gruppo simmetrico e i gruppi diedrali.

ESERCIZI.

- Si provi che tutti i sottogruppi di $(\mathbb{Z}, +)$ sono i sottoinsiemi del tipo $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$. Se ne deduca che tutti i sottogruppi di \mathbb{Z} sono ciclici.
- Si provi che l'intersezione arbitraria di sottogruppi di un gruppo G è un sottogruppo di G .
- Si provi che l'unione insiemistica di due sottogruppi di un gruppo G è un sottogruppo di G se e solo se uno dei due sottogruppi è contenuto nell'altro. Si verifichi questo fatto nel caso di due sottogruppi di $(\mathbb{Z}, +)$.
- Siano S e T due sottogruppi di un gruppo G . Indicato con ST l'insieme

$$ST \stackrel{\text{def}}{=} \{st \mid s \in S, t \in T\}$$

si provi che ST è un sottogruppo se e solo se $ST = TS$ (uguaglianza di sottoinsiemi).

- Si provi che l'insieme S delle matrici $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ dove $a, b \in \mathbb{R}$ e non sono contemporaneamente nulli è un sottogruppo di $(\mathrm{GL}_2(\mathbb{R}), \cdot)$.
- Si dimostri che, se a e b sono elementi di un gruppo G tali che $ab = ba$, allora il sottogruppo generato da $X = \{a, b\}$ è abeliano.
- Sia G un gruppo abeliano e n un intero positivo. Sia S il sottoinsieme di G formato da tutte le potenze n -esime degli elementi di G , ossia

$$S \stackrel{\text{def}}{=} \{g^n \mid g \in G\}.$$

Si provi che S è un sottogruppo di G .

- Si provi che l'insieme $U(\mathbb{Z}_n)$ degli elementi invertibili di \mathbb{Z}_n è un gruppo rispetto alla moltiplicazione.
- Si provi che in un gruppo (G, \cdot) , dati comunque due elementi a e b di G , ciascuna delle equazioni

$$ax = b, \quad ya = b$$

ammette un'unica soluzione.

10. Si provi che in un gruppo (G, \cdot) vagono le seguenti *leggi di cancellazione*:

$$\begin{aligned} ax = ay &\implies x = y \\ xa = ya &\implies x = y. \end{aligned}$$

11. Sia (G, \cdot) un gruppo. Sia s un fissato elemento di G . Si definisca in G una nuova operazione $*$ al modo seguente:

$$a * b \stackrel{\text{def}}{=} a \cdot s \cdot b \quad \forall a, b \in G.$$

Si dica se $(G, *)$ è un gruppo.

12. Si consideri l'insieme $S = \mathbb{R} \setminus \{-1\}$ costituito da tutti i numeri reali diversi da -1 .

- (a) Si dica, motivando la risposta, se S è un gruppo rispetto all'ordinaria moltiplicazione tra numeri reali.
(b) Si dica se è un gruppo rispetto alla seguente moltiplicazione:

$$x * y \stackrel{\text{def}}{=} x - y - xy, \quad \forall x, y \in S.$$

13. Determinare tutti i sottogruppi di \mathbb{Z} che contengono il numero 6.

14. Sia $*$ l'operazione su \mathbb{N} così definita: $a * b$ si ottiene a partire da a e b rappresentando a e b in base 10 e sommando modulo 10 le *cifre* corrispondenti. In pratica, $a * b$ si ottiene facendo l'addizione di a e b secondo le regole usuali, ma scordandosi il riporto. Ad esempio,

$$1097 * 9023 = 10, \quad 342 * 1773 = 1015.$$

Dire se $(\mathbb{N}, *)$ è un gruppo. Si ripeta lo stesso esercizio, sostituendo la base 10 con una base arbitraria n .

15. Si provi che un gruppo non abeliano non è mai ciclico.
16. Si provi che se g è un elemento di un gruppo G tale che $g^n = e$ per qualche $n \in \mathbb{N}$, allora il periodo di g è un divisore di n .
17. Provare che un elemento $\bar{a} \in \mathbb{Z}_n$ ha ordine n/d , dove $d = \text{MCD}(a, n)$.
18. Si determinino in \mathbb{Z}_{10000} tutti gli elementi di ordine 4 e 8.
19. Sia $G = \langle g \mid g^n = e \rangle$ un gruppo ciclico con n elementi. Si provi che $\langle g^k \rangle$ ha n/d elementi, dove $d = \text{MCD}(n, k)$. Se ne deduca che tutti e soli i generatori di G sono i g^k con $(n, k) = 1$.
20. Sia $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R}, a, b \neq 0 \right\}$. Quali sono i periodi degli elementi di G ? Quali sono i periodi degli elementi di $G' = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{C}, a, b \neq 0 \right\}$?



ESERCIZI DI PROGRAMMAZIONE.

Sia X un insieme finito dotato di un'operazione $*$ data attraverso una tavola moltiplicativa.

1. Si scriva un programma che sia capace di riconoscere se l'operazione è associativa.

2. Si scriva un programma che sia in grado di vedere se l'insieme X rispetto all'operazione $*$ è un gruppo.
3. Sia $(G, *)$ un gruppo finito, dato attraverso la sua tavola moltiplicativa.
 - (a) Si scriva un programma capace di riconoscere se un sottoinsieme S di G è un sottogruppo;
 - (b) si scriva un programma che calcoli il periodo di ogni elemento;
 - (c) si scriva un programma capace di decidere se il gruppo è ciclico.



CONTROLLO.

1. Quali sono le condizioni perché un sottoinsieme di un gruppo sia un sottogruppo?
2. L'ordine di un elemento di un gruppo è ...
3. Gruppi ciclici e loro proprietà. Quali sono gli ordini ammissibili dei sottogruppi di un gruppo ciclico finito? Quanti sottogruppi di un dato ordine ci sono?

5.2. Il gruppo simmetrico S_n

Abbiamo introdotto nel paragrafo precedente il gruppo $(\mathcal{S}(X), \circ)$ di tutte le corrispondenze biunivoche dell'insieme X in sé. Nel caso in cui l'insieme X sia finito, il gruppo $\mathcal{S}(X)$ si indica con S_n , se n rappresenta la cardinalità di $X = \{x_1, x_2, \dots, x_n\}$, e prende il nome di *gruppo simmetrico di grado n*. Data la grande importanza di tale gruppo, e dato che è uno dei primi esempi di gruppo non abeliano che incontriamo, vale la pena di dedicare due interi paragrafi allo studio delle principali proprietà di tale gruppo.

Sia $X = \{1, 2, \dots, n\}$. Ogni elemento σ di S_n , in quanto corrispondenza biunivoca di X in sé, rappresenta una *permutazione* di $\{1, 2, \dots, n\}$. Quindi la cardinalità $|S_n|$ di S_n è

$$|S_n| = n!$$

Sia $n = 6$, $X = \{1, 2, 3, 4, 5, 6\}$ e sia σ la corrispondenza (biunivoca) che agisce al modo seguente:

$$\begin{aligned} \sigma : X &\longrightarrow X \\ 1 &\longmapsto 5 \\ 2 &\longmapsto 1 \\ 3 &\longmapsto 4 \\ 4 &\longmapsto 6 \\ 5 &\longmapsto 2 \\ 6 &\longmapsto 3. \end{aligned}$$

Scriviamo σ come matrice 2×6 al modo seguente:

$$(5.2.1) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 4 & 6 & 2 & 3 \end{pmatrix}.$$

Si noti che, in virtù della biunivocità della σ , nella seconda riga, che contiene le immagini degli elementi di X , figurano tutti gli elementi della prima riga, in ordine diverso. In generale, un elemento di S_n verrà indicato con la seguente matrice $2 \times n$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ i_1 & i_2 & i_3 & i_4 & \dots & i_n \end{pmatrix}.$$

Il composto delle due permutazioni σ e τ , dove ad esempio, σ è la permutazione di prima e τ è la permutazione

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

è la permutazione che si ottiene operando dapprima su X con la τ e poi con la σ , cioè il prodotto

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 4 & 6 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 3 & 4 & 6 \end{pmatrix}$$

si deve fare da *destra a sinistra* (trattandosi di un ordinario prodotto operatorio); il risultato è la permutazione

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 6 & 3 \end{pmatrix}$$

Se facciamo il prodotto nell'ordine inverso, cioè $\tau \circ \sigma$, il risultato è:

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

Il gruppo (S_n, \circ) è pertanto un gruppo non abeliano. D'ora in poi scrivremo $\sigma \circ \tau = \sigma\tau$.

Indicheremo con id l'elemento neutro di S_n , ossia la permutazione identica

$$\text{id} = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}.$$

È facile calcolare l'inversa di una permutazione: è la permutazione ottenuta semplicemente scambiando le due righe e poi riordinando le colonne in modo che gli elementi della prima riga siano nell'ordinamento naturale. Ad esempio, l'inversa della permutazione

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

è la permutazione

$$\sigma^{-1} = \begin{pmatrix} 3 & 1 & 4 & 6 & 2 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 1 & 3 & 6 & 4 \end{pmatrix}.$$

A partire da una permutazione σ si possono costruire tutte le sue potenze σ^k ad esponenti interi. Sia r il minimo intero positivo tale che $\sigma^r = \text{id}$. Tale intero esiste sicuramente, come si è visto nel paragrafo precedente, ed è l'ordine o periodo della permutazione σ (cfr. definizione 5.1.13).

5.2.1 ESEMPIO. Calcoliamo il periodo della permutazione

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

Le varie potenze di σ sono

$$\begin{aligned} \sigma^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 1 & 5 & 2 \end{pmatrix} \neq \text{id}, & \sigma^3 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 2 & 5 & 3 \end{pmatrix} \neq \text{id}, \\ \sigma^4 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 5 & 4 \end{pmatrix} \neq \text{id}, & \sigma^5 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \text{id}. \end{aligned}$$

Quindi il periodo di σ è 5. \square

Daremo ora la importante nozione di *orbita* di un elemento di $X = \{1, 2, \dots, n\}$ mediante una permutazione σ di S_n .

Si fissi una permutazione σ . Definiamo in X la seguente relazione:

$$x \equiv_{\sigma} y \iff y = \sigma^i(x) \text{ per qualche } i \in \mathbb{Z}.$$

Non è difficile provare che si tratta di una relazione di equivalenza definita su X . Ne segue che X viene ripartito in classi di equivalenza.

5.2.2 DEFINIZIONE. Si definisce *orbita* $\mathcal{O}_{\sigma}(x)$ dell'elemento $x \in X$ sotto l'azione di σ la classe di equivalenza di x , ossia

$$\boxed{\mathcal{O}_{\sigma}(x) \stackrel{\text{def}}{=} \{y \in X \mid y = \sigma^i(x) \text{ per qualche } i \in \mathbb{Z}\}}. \quad \square$$

Ora, essendo X finito, dato comunque un $x \in X$, esisterà un intero positivo minimo $m = m(x)$ tale che $\sigma^m(x) = x$; infatti, dovranno esistere due interi distinti h e k ($h > k$) tali che $\sigma^h(x) = \sigma^k(x)$, da cui, applicando σ^{-k} ad entrambi i membri, si ottiene

$$\sigma^{h-k}(x) = x.$$

5.2.3 PROPOSIZIONE. Sia $\sigma \in \mathcal{S}_n$. Detto $m = m(x)$ l'intero positivo minimo tale che $\sigma^m(x) = x$, l'orbita dell'elemento x sotto l'azione di σ è il sottoinsieme di X

$$\mathcal{O}_\sigma(x) = \{x = \sigma^0(x), \sigma(x), \sigma^2(x), \dots, \sigma^{m-1}(x)\}.$$

Dimostrazione. Si tratta di mostrare che ogni $\sigma^i(x)$, con $i \in \mathbb{Z}$, coincide con uno degli m elementi $x = \sigma^0(x), \sigma(x), \sigma^2(x), \dots, \sigma^{m-1}(x)$ di X . Infatti, dalla $i = mq + r$, $0 \leq r < m$ si ottiene

$$\sigma^i(x) = \sigma^{mq+r}(x) = \sigma^r(\sigma^m)^q(x) = \sigma^r(\sigma^{\pm m}(\sigma^{\pm m} \cdots (\sigma^{\pm m}(x)))) = \sigma^r(x). \quad \square$$

5.2.4 DEFINIZIONE. Un *ciclo* di σ è l'insieme ordinato

$$(x, \sigma(x), \sigma^2(x), \dots, \sigma^{m-1}(x)).$$

L'intero m dicesi *lunghezza* del ciclo. \square

5.2.5 ESEMPIO. Sia $\sigma \in \mathcal{S}_6$ la permutazione

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

Partendo da $1 \in X$, l'orbita di 1 mediante σ è il sottoinsieme di X

$$\mathcal{O}_\sigma(1) = \{1, 3, 2\}.$$

Si noti che l'orbita di 1 mediante σ può essere rappresentata anche come il sottoinsieme $\{1, 2, 3\}$, ossia è semplicemente il sottoinsieme di X costituito dagli elementi 1, 2, 3, e quindi l'ordine con cui si scrivono i suoi elementi all'interno della parentesi graffa non ha importanza. Se ora *ordiniamo* gli elementi di $\mathcal{O}_\sigma(1)$ in modo che ogni elemento sia il trasformato mediante la σ del precedente e il primo sia il trasformato dell'ultimo, allora otteniamo un *ciclo* della permutazione σ . In questo caso il ciclo che si ottiene partendo dall'elemento 1 è

$$(1, 3, 2).$$

Per distinguere le due nozioni, gli elementi di un ciclo si dispongono tra parentesi tonde. È chiaro che anche $(3, 2, 1)$ coincide con il ciclo $(1, 3, 2)$, e così anche $(2, 1, 3)$, ma non così il ciclo $(1, 2, 3)$, perché l'elemento 2 non è il trasformato mediante la σ di 1.

Partiamo ora da un elemento che non stia nell'orbita $\mathcal{O}_\sigma(1)$, ad esempio 5, e calcoliamo la sua orbita mediante la σ . Sarà

$$\mathcal{O}_\sigma(5) = \{4, 5, 6\}.$$

Il ciclo corrispondente è il seguente

$$(5, 6, 4) = (6, 4, 5) = (4, 5, 6).$$

Non ci sono altri elementi in X che non siano già contenuti nei cicli considerati, quindi i cicli della permutazione σ sono $(1, 3, 2)$ e $(5, 6, 4)$. \square

Si noti che ciascuno dei cicli $(1, 3, 2)$ e $(5, 6, 4)$ rappresenta una permutazione, precisamente quella che manda ogni elemento del ciclo nel successivo e l'ultimo nel primo, e lascia fissi tutti gli altri elementi. Quindi $\gamma_1 = (1, 3, 2)$ è un altro modo di scrivere la permutazione

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

e $\gamma_2 = (5, 6, 4)$ corrisponde alla permutazione

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

Ma il fatto notevole è che la permutazione originaria σ risulta uguale al prodotto dei suoi due cicli γ_1 e γ_2 (ed è indipendente dall'ordine con cui li prendo, dato che i due cicli γ_1 e γ_2 sono disgiunti):

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

Potremo quindi scrivere direttamente

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 6 & 4 \end{pmatrix} = \gamma_1 \gamma_2 = (1, 3, 2)(5, 6, 4) = \gamma_2 \gamma_1 = (5, 6, 4)(1, 3, 2).$$

Proviamo in generale quanto verificato in questo caso particolare.

5.2.6 PROPOSIZIONE. *Ogni permutazione $\sigma \in S_n$ è prodotto dei suoi cicli (che sono ovviamente disgiunti).*

Dimostrazione. Indicati con $\gamma_1, \gamma_2, \dots, \gamma_k$ i cicli disgiunti della σ , per provare che $\sigma = \gamma_1 \gamma_2 \cdots \gamma_k$ occorre provare che per ogni $x \in X = \{1, 2, \dots, n\}$ si ha

$$\sigma(x) = (\gamma_1 \gamma_2 \cdots \gamma_k)(x).$$

Ora, ogni $x \in X$ compare nella scrittura di uno solo dei cicli $\gamma_1, \gamma_2, \dots, \gamma_k$; sia questo il ciclo $\gamma_i = (x, \sigma(x), \dots, \sigma^{m-1}(x))$. Inoltre, per ogni $j \neq i$, e ogni $y = \sigma^j(x)$ (cioè per ogni y che compare nella scrittura di γ_i) risulta

$$\gamma_j(y) = y.$$

Allora, per ogni $x \in X$

$$(\gamma_1 \gamma_2 \cdots \gamma_k)(x) = (\gamma_1 \gamma_2 \cdots \gamma_i)(x) = \gamma_1 \gamma_2 \cdots \gamma_{i-1}(\sigma(x)) = \sigma(x).$$

Quindi $\sigma = \gamma_1 \gamma_2 \cdots \gamma_k$. \square

Ora, una volta che si scriva una permutazione come prodotto dei suoi cicli, è più facile determinarne il periodo. Si osservi innanzitutto che un ciclo di lunghezza m ha periodo m . Ciò premesso, si dimostra la seguente proposizione.

5.2.7 PROPOSIZIONE. *Il periodo di una permutazione $\sigma \in S_n$ è il minimo comune multiplo delle lunghezze dei suoi cicli.*

Dimostrazione. Se $\sigma = \gamma_1 \gamma_2 \cdots \gamma_k$, indicato con m_i l'ordine del ciclo i -esimo, e con $M = \text{lcm}(m_1, m_2, \dots, m_k)$, si tratta di provare che M uguaglia il periodo N di σ . Infatti

$$\sigma^M = (\gamma_1 \gamma_2 \cdots \gamma_k)^M \stackrel{\text{cicli disgiunti}}{=} \gamma_1^M \gamma_2^M \cdots \gamma_k^M = \text{id}$$

quindi $N \mid M$. Inoltre,

$$\text{id} = \sigma^N = \gamma_1^N \gamma_2^N \cdots \gamma_k^N = \text{id} \cdot \text{id} \cdot \text{id} \cdots \text{id} .$$

Ma allora $m_i \mid N$ per ogni $i = 1, \dots, k$, da cui $M \mid N$. Quindi $N = M$. \square

5.2.8 COROLLARIO. *Ogni permutazione è prodotto di 2-cicli (o trasposizioni).*

Dimostrazione. Ogni ciclo si può scrivere come prodotto di trasposizioni; ad esempio

$$(1, 2, 3, \dots, m) = (1, m)(1, m-1)(1, m-2) \cdots (1, 3)(1, 2) .$$

Dato che ogni permutazione è prodotto dei suoi cicli, il corollario è provato. \square

Si noti che la scrittura di una permutazione come prodotto di trasposizioni non è unica. Ad esempio

$$\begin{aligned} \sigma &= (2, 3, 4)(1, 6, 5) = (2, 4)(2, 3)(1, 5)(1, 6) \\ &= (3, 4, 2)(6, 5, 1) = (3, 2)(3, 4)(5, 6)(5, 1) . \end{aligned}$$

5.2.9 DEFINIZIONE. Una permutazione si dice *pari* se è prodotto di un numero pari di trasposizioni, si dice *dispari* se è prodotto di un numero dispari di trasposizioni. \square

 **ATTENZIONE.** Questa definizione potrebbe essere priva di significato se una permutazione si potesse scrivere al tempo stesso come prodotto di un numero pari e di un numero dispari di trasposizioni. Tuttavia questa eventualità non si può presentare, come ora mostreremo. \square

5.2.10 PROPOSIZIONE. *Se una permutazione si scrive come prodotto di un numero pari (dispari) di trasposizioni, ogni altra sua scrittura come prodotto di trasposizioni è ancora costituita da un numero pari (dispari) di trasposizioni.*

Dimostrazione. Dimostreremo il teorema osservando il comportamento di una permutazione nei confronti del seguente polinomio:

$$p(x_1, x_2, \dots, x_n) \stackrel{\text{def}}{=} \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Se σ è un elemento di S_n , allora poniamo

$$\sigma(p(x_1, x_2, \dots, x_n)) \stackrel{\text{def}}{=} p(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

Ad esempio, se $n = 4$ e $\sigma = (2, 3, 4)$, allora

$$p(x_1, x_2, x_3, x_4) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$$

e

$$\sigma(p(x_1, \dots, x_4)) = (x_1 - x_3)(x_1 - x_4)(x_1 - x_2)(x_3 - x_4)(x_3 - x_2)(x_4 - x_2).$$

Proveremo che se si parte da una *trasposizione* τ , allora

$$\tau(p(x_1, x_2, \dots, x_n)) = -p(x_1, x_2, \dots, x_n)$$

cioè il suo effetto è quello di *cambiare segno al polinomio*.

Sia dunque $\tau = (i, j)$, con $i < j$. I fattori del polinomio che sentiranno l'effetto della τ sono solamente i fattori che contengono *almeno* uno tra x_i e x_j . Se con a indichiamo un numero diverso da i e da j , la situazione che si presenterà è pertanto la seguente:

Fattori di $p(x_1, \dots, x_n)$ coinvolti

$$\begin{array}{ll} x_a - x_i & (a < i) \\ x_a - x_j & (a < j) \\ x_i - x_a & (i < a) \\ x_j - x_a & (j < a) \\ x_i - x_j & \end{array}$$

Fattori trasformati

$$\begin{array}{ll} \tau(x_a - x_i) = x_a - x_j \\ \tau(x_a - x_j) = x_a - x_i \\ \tau(x_i - x_a) = x_j - x_a \\ \tau(x_j - x_a) = x_i - x_a \\ \tau(x_i - x_j) = x_j - x_i. \end{array}$$

Ora, nel primo e nel quarto caso non avviene nessun cambiamento di segno. Nel secondo caso, se $a < i$, $x_a - x_i$ *uguaglia* un fattore del polinomio originario, se invece risulta $i < a$, allora ha segno *opposto*: quindi il cambiamento di segno si ha per tutti gli a tali che $i < a < j$. Nel terzo caso, se $j < a$, $x_j - x_a$ *uguaglia* uno dei fattori del polinomio originario, altrimenti (cioè per $a < j$) *uguaglia l'opposto* di un fattore di $p(x_1, x_2, \dots, x_n)$: quindi il cambiamento di segno si ha per tutti gli a tali che $i < a < j$. Nell'ultimo caso naturalmente $x_j - x_i = -(x_i - x_j)$. In definitiva, i casi in cui si avrà un cambiamento di segno sono in numero di $2(j - i - 1) + 1$. Infatti gli a tali che $i < a < j$ sono in numero di $j - i - 1$, e tale numero va contato due volte (caso secondo e caso terzo). Il numero totale essendo dispari, segue che $\tau(p(x_1, \dots, x_n)) = -p(x_1, \dots, x_n)$.

Una volta che abbiamo provato questo fatto, è chiaro che, data comunque una permutazione $\sigma \in S_n$, si avrà

$$\sigma(p(x_1, x_2, \dots, x_n)) = \pm p(x_1, x_2, \dots, x_n)$$

a seconda che σ si scriva come prodotto di un numero pari o dispari di trasposizioni. Quindi una stessa σ non si può scrivere al tempo stesso come prodotto di un numero pari e di un numero dispari di trasposizioni. La proposizione è dimostrata. \square

Sia ora

$$A_n \stackrel{\text{def}}{=} \{\text{permutazioni pari di } S_n\}.$$

Si tratta di un *sottogruppo* di S_n (cfr. esercizio 5.2.4), che prende il nome di *sottogruppo alterno*.

Quanti sono gli elementi di A_n ?

Siano

$$\pi_1, \pi_2, \dots, \pi_k$$

le k permutazioni pari (tutte diverse) che dobbiamo contare. Sia τ una qualunque trasposizione. Allora le permutazioni seguenti

$$(5.2.2) \quad \pi_1\tau, \pi_2\tau, \dots, \pi_k\tau$$

sono permutazioni *dispari* e *tutte distinte*. Che siano dispari è ovvio. Quanto al fatto che siano tutte distinte, supponiamo che sia

$$\pi_i\tau = \pi_j\tau.$$

Allora

$$\pi_i\tau\tau^{-1} = \pi_j\tau\tau^{-1} \implies \pi_i = \pi_j.$$

Questa è la cosiddetta *legge di cancellazione* nei gruppi (cfr. esercizio 5.1.10). Si osservi che è importante che l'elemento da cancellare sia sempre dalla stessa parte, perché il gruppo non è abeliano.

Abbiamo quindi trovato *almeno* k permutazioni dispari, cioè

numero h delle permutazioni dispari \geq numero k delle permutazioni pari.

Ma ora ripetiamo lo stesso discorso partendo dalle permutazioni dispari. Siano

$$\delta_1, \delta_2, \dots, \delta_h$$

le h permutazioni dispari. Allora le

$$\delta_1\tau, \delta_2\tau, \dots, \delta_h\tau$$

sono h permutazioni pari, da cui segue che $k \geq h$. Confrontando con la relazione precedente, possiamo concludere che $k = h$, cioè:

5.2.11 PROPOSIZIONE. *L'ordine del sottogruppo alterno A_n di S_n è*

$$\frac{n!}{2}.$$

Concludiamo questo paragrafo esaminando in dettaglio il caso $n = 3$. Il gruppo S_3 ha 6 elementi, che scriviamo nella scrittura ciclica

$$S_3 = \{\text{id}, (1, 2, 3), (1, 3, 2), (1, 2), (1, 3), (2, 3)\}.$$

La tavola di moltiplicazione di questo gruppo è la seguente:

\circ	id	$(1, 2, 3)$	$(1, 3, 2)$	$(1, 2)$	$(1, 3)$	$(2, 3)$
id	id	$(1, 2, 3)$	$(1, 3, 2)$	$(1, 2)$	$(1, 3)$	$(2, 3)$
$(1, 2, 3)$	$(1, 2, 3)$	$(1, 3, 2)$	id	$(1, 3)$	$(2, 3)$	$(1, 2)$
$(1, 3, 2)$	$(1, 3, 2)$	id	$(1, 2, 3)$	$(2, 3)$	$(1, 2)$	$(1, 3)$
$(1, 2)$	$(1, 2)$	$(2, 3)$	$(1, 3)$	id	$(1, 3, 2)$	$(1, 2, 3)$
$(1, 3)$	$(1, 3)$	$(1, 2)$	$(2, 3)$	$(1, 2, 3)$	id	$(1, 3, 2)$
$(2, 3)$	$(2, 3)$	$(1, 3)$	$(1, 2)$	$(1, 3, 2)$	$(1, 2, 3)$	id

Il sottogruppo alterno A_3 è

$$A_3 = \{\text{id}, (1, 2, 3), (1, 3, 2)\}.$$

Esistono in S_3 altri sottogruppi. Diamo qui di seguito l'elenco completo dei sottogruppi di S_3 , invitando lo studente inanzitutto a verificare che si tratta effettivamente di sottogruppi, e poi che non ce ne sono altri.

$$H_1 = \{\text{id}\}.$$

$$H_2 = \{\text{id}, (1, 2)\} = \langle (1, 2) \rangle.$$

$$H_3 = \{\text{id}, (1, 3)\} = \langle (1, 3) \rangle.$$

$$H_4 = \{\text{id}, (2, 3)\} = \langle (2, 3) \rangle.$$

$$A_3 = \{\text{id}, (1, 2, 3), (1, 3, 2)\} = \langle (1, 2, 3) \rangle.$$

$$S_3.$$

Il primo e l'ultimo nella lista (cioè il sottogruppo ridotto al solo elemento neutro, e l'intero gruppo) prendono il nome di sottogruppi *boranti*.



ESERCIZI.

1. Si determinino le inverse delle seguenti permutazioni di S_8 :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 5 & 6 & 3 & 2 & 7 & 1 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 6 & 2 & 8 & 7 & 1 & 5 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 2 & 4 & 7 & 6 & 5 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 8 & 7 & 4 \end{pmatrix}.$$

Si determini il loro periodo e si scrivano come prodotti di cicli disgiunti.

2. Si dica se il seguente sottoinsieme S di S_4 è un sottogruppo:

$$S = \{\text{id}, (1, 3, 2), (1, 2, 3), (1, 2), (3, 4), (2, 3), (1, 3)(2, 4), (1, 2)(3, 4), \\ (1, 2, 3, 4), (1, 3, 2, 4), (2, 1, 3, 4), (2, 1, 4, 3)\}.$$

3. In S_4 si determini il sottogruppo generato dal sottoinsieme

$$X = \{(1, 2, 3), (1, 4)\}.$$

4. Si provi che il sottoinsieme di S_n costituito dalle permutazioni pari è un sottogruppo. È il sottoinsieme costituito dalle permutazioni dispari?
5. Quali sono le strutture cicliche delle permutazioni di S_{14} con periodo 20? Quali tra queste sono permutazioni pari e quali dispari? Il sottoinsieme S delle permutazioni di S_{14} con periodo 20 costituiscono un sottogruppo di S_{14} ?
6. Si provi che S_{30} possiede un sottogruppo di ordine 209.
7. Si dica se si può, con le ordinarie regole del "gioco del quindici", passare dalla configurazione di sinistra a quella di destra.

2	1	10	9
11	8	7	5
4	12	6	3
13	15	14	

1	5	4	8
10	3	13	6
11	15	14	12
7	9	2	

8. Si provi che A_n è generato dai 3-cicli.



ESERCIZI DI PROGRAMMAZIONE.

1. Si scriva un programma che elenchi, per ogni n , le permutazioni di n elementi.
2. Si scriva un programma che scriva ogni permutazione come prodotto di cicli disgiunti.
3. Si scriva un programma che calcoli la parità di ogni permutazione.



CONTROLLO.

1. L'orbita di un elemento $x \in \{1, 2, \dots, n\}$ mediante una permutazione $\sigma \in S_n$ è ...
2. Cicli di una permutazione.
3. Parità di una permutazione. Perché ha senso la definizione che è stata data?
4. Permutazioni pari e dispari e loro numero. Quali tra queste costituiscono un sottogruppo?
5. Sapreste dare un esempio di gruppo non ciclico in cui tutti i sottogruppi propri sono ciclici? (Un esempio lo avete incontrato in questo stesso paragrafo.)

5.3. Classi coniugate in S_n

Un concetto importante nei gruppi è quello di elementi coniugati e classi coniugate. Definiremo questo concetto in S_n , dove scopriremo che sarà molto facile trovare i coniugati di un data permutazione.

5.3.1 DEFINIZIONE. Siano σ e σ' due permutazioni di S_n . Si dice che la permutazione σ è *coniugata* alla permutazione σ' se esiste una permutazione τ in S_n tale che

$$\sigma' = \tau \sigma \tau^{-1}. \quad \square$$

Ad esempio, le due permutazioni di S_5

$$\sigma = (1, 3, 4) \quad \text{e} \quad \sigma' = (3, 2, 5)$$

sono coniugate, perché $\sigma' = \tau \sigma \tau^{-1}$, con $\tau = (1, 3, 2)(4, 5)$; infatti

$$(3, 2, 5) = \underbrace{(1, 3, 2)}_{\tau}(4, 5) \underbrace{(1, 3, 4)}_{\sigma} \underbrace{((1, 2, 3)(4, 5))}_{\tau^{-1}}.$$

Probabilmente non è affatto chiaro come è saltata fuori questa permutazione τ che ci ha permesso di dire che σ e σ' erano coniugate. La proposizione che segue ci illuminerà.

5.3.2 PROPOSIZIONE. *Sia σ una permutazione, scritta come prodotto di cicli disgiunti. Allora:*

- (a) *Ogni permutazione coniugata $\sigma' = \tau \sigma \tau^{-1}$ di σ ha la stessa struttura ciclica di σ . Inoltre, gli interi che compaiono nei cicli di σ' si ottengono applicando la permutazione τ agli interi che compaiono nei cicli di σ .*
- (b) *Se σ e σ' sono due permutazioni di S_n che hanno la stessa struttura ciclica, allora sono coniugate.*

Dimostrazione. Siano a e b due interi *consecutivi* nella scrittura di uno qualunque dei cicli di σ (considerando consecutivi anche l'ultimo e il primo del ciclo), cioè sia

$$b = \sigma(a).$$

Esaminiamo come agisce $\tau\sigma\tau^{-1}$ sui vari elementi. Se poniamo $\tau(a) = s$ e $\tau(b) = t$, allora

$$\tau\sigma\tau^{-1}(s) = \tau\sigma(a) = \tau(b) = t$$

cioè, se b è il successivo di a nella scrittura ciclica di σ , allora $\tau(b)$ è il successivo di $\tau(a)$ nella scrittura ciclica di $\tau\sigma\tau^{-1}$. Ciò significa che se ad esempio

$$\sigma = (a, b, c, d)(e, f, g)(h, i)$$

allora

$$\tau\sigma\tau^{-1} = (\tau(a), \tau(b), \tau(c), \tau(d))(\tau(e), \tau(f), \tau(g))(\tau(h), \tau(i)).$$

Questo risolve completamente il punto (α), perché ci dice al tempo stesso che σ e $\tau\sigma\tau^{-1}$ hanno la stessa struttura ciclica e anche quali sono i nuovi elementi da inserire nei cicli della permutazione coniugata.

Siano ora

$$\sigma = (a, b, c, d)(e, f, g)(h, i)$$

$$\sigma' = (a', b', c', d')(e', f', g')(h', i')$$

due permutazioni che hanno la stessa struttura ciclica. Proveremo che sono coniugate. Infatti (controllare!)

$$\sigma' = \tau\sigma\tau^{-1}$$

dove τ è una permutazione tale che

$$\begin{aligned}\tau : a &\longmapsto a' \\ b &\longmapsto b' \\ c &\longmapsto c' \\ d &\longmapsto d' \\ e &\longmapsto e' \\ f &\longmapsto f' \\ g &\longmapsto g' \\ h &\longmapsto h' \\ i &\longmapsto i'\end{aligned}$$

ossia τ è una permutazione del tipo

$$\tau = \begin{pmatrix} a & \cdots & b & \cdots & c & \cdots & d & \cdots & e & \cdots & f & \cdots & g & \cdots & h & \cdots & i & \cdots \\ \downarrow & & \downarrow & \\ a' & \cdots & b' & \cdots & c' & \cdots & d' & \cdots & e' & \cdots & f' & \cdots & g' & \cdots & h' & \cdots & i' & \cdots \end{pmatrix},$$

che cioè sugli elementi a, b, c, \dots, i si comporta come detto, e sugli eventuali altri elementi si comporta come vuole (compatibilmente al fatto che deve trattarsi di una permutazione). \square

Questa proposizione ci offre pertanto un metodo rapido per calcolare la coniugata di una permutazione, senza svolgere tutti i prodotti.

5.3.3 ESEMPIO.

In S_7 siano

$$\sigma = (1, 5)(2, 3, 4), \quad \tau = (1, 4, 3)(2, 6, 7, 5).$$

Calcoliamo, senza svolgere tutti i prodotti, $\tau\sigma\tau^{-1}$. Risulta

$$\tau\sigma\tau^{-1} = (4, 2)(6, 1, 3).$$

Viceversa, siano date le due permutazioni

$$\sigma = (1, 3, 5)(2, 7), \quad \sigma' = (3, 1, 7)(5, 2)$$

che hanno la stessa struttura ciclica. Si chiede di trovare una τ tale che sia $\sigma' = \tau\sigma\tau^{-1}$. La τ in questione deve essere tale che

$$3 = \tau(1), \quad 1 = \tau(3), \quad 7 = \tau(5), \quad 5 = \tau(2), \quad 2 = \tau(7).$$

Una possibile τ è

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 4 & 7 & 6 & 2 \end{pmatrix}$$

ma un'altra possibilità è ad esempio

$$\tilde{\tau} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 6 & 7 & 4 & 2 \end{pmatrix}.$$

Risulta $\sigma' = \tau\sigma\tau^{-1} = \tilde{\tau}\sigma\tilde{\tau}^{-1}$. \square

Ora, la relazione di *essere coniugato* è una relazione di equivalenza, come si verifica facilmente. La proposizione precedente ci permette di trovare subito le classi coniugate.

5.3.4 PROPOSIZIONE.

Le classi coniugate in S_n sono tante quante le diverse strutture cicliche.

In S_3 , S_4 e S_5 le diverse strutture cicliche sono

$$\begin{aligned} S_3 & \quad (-), (-,-), (-,-,-) \\ S_4 & \quad (-), (-,-), (-,-,-), (-,-,-,-), (-,-)(-,-) \\ S_5 & \quad (-), (-,-), (-,-,-), (-,-,-,-), (-,-,-,-,-), \\ & \quad (-,-)(-,-), (-,-,-)(-,-). \end{aligned}$$

Con $(-)$ si intende la permutazione identica. Quindi in S_3 , S_4 e S_5 ci sono rispettivamente 3, 5 e 7 classi coniugate. Precisamente:

$$\begin{aligned} S_3 & \quad (-) = \{\text{id}\} \\ & \quad (-,-) = \{(1,2), (1,3), (2,3)\} \\ & \quad (-,-,-) = \{(1,2,3), (1,3,2)\}; \\ S_4 & \quad (-) = \{\text{id}\} \\ & \quad (-,-) = \{(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\} \\ & \quad (-,-,-) = \{(1,2,3), (1,2,4), (1,3,4), (1,3,2), \\ & \quad \quad (1,4,2), (1,4,3), (2,3,4), (2,4,3)\} \\ & \quad (-,-,-,-) = \{(1,2,3,4), (1,2,4,3), (1,3,2,4), \\ & \quad \quad (1,3,4,2), (1,4,2,3), (1,4,3,2)\} \\ & \quad (-,-,-)(-,-) = \{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}. \end{aligned}$$

Quindi la determinazione delle classi coniugate in S_n è molto semplice.

Vediamo ora di *contare* quante permutazioni ci sono in ogni classe coniugata. Per fare questo basta saper contare quanti sono gli r -cicli, $r = 1, \dots, n$ e i prodotti di cicli.

5.3.5 PROPOSIZIONE. In S_n gli r -cicli sono in numero di

$$\frac{1}{r} \frac{n!}{(n-r)!}.$$

Dimostrazione. Fissati r numeri, gli r -cicli formati con questi r numeri sono $(r-1)!$: infatti, supposto (cosa che si può sempre fare) che i cicli comincino tutti con lo stesso elemento, questi sono tanti quante le permutazioni di $r-1$ elementi, cioè $(r-1)!$. Dato che si possono scegliere r numeri tra n in $\binom{n}{r}$ modi, in totale gli r -cicli distinti in S_n sono

$$\binom{n}{r} \cdot (r-1)! = \frac{1}{r} \frac{n!}{(n-r)!}. \quad \square$$

Con simili ragionamenti si possono contare quanti sono le permutazioni che sono prodotto di cicli di varia lunghezza. Calcoliamo il numero di permutazioni dentro ogni classe coniugata di S_4 :

Struttura ciclica Numero di coniugati distinti

(-)	1
(-, -)	$\binom{4}{2} = 6$
(-, -, -)	$\binom{4}{3} \cdot 2! = 8$
(-, -, -, -)	$\binom{4}{4} \cdot 3! = 6$
(-, -)(-, -)	$\binom{4}{2} \cdot \binom{2}{2} \cdot \frac{1}{2} = 3$.

5.3.6 DEFINIZIONE. Fissato l'intero n , si dice che la successione di interi positivi n_1, n_2, \dots, n_t con $n_1 \geq n_2 \geq n_3 \dots \geq n_t$ costituisce una *partizione* dell'intero n se

$$n = n_1 + n_2 + \dots + n_t . \quad \square$$

Ad esempio, le partizioni dell'intero 4 sono

$$\begin{aligned} 4 &= 4 \\ 4 &= 3 + 1 \\ 4 &= 2 + 2 \\ 4 &= 2 + 1 + 1 \\ 4 &= 1 + 1 + 1 + 1 . \end{aligned}$$

Ora, si riconoscerà che ogni partizione dell'intero 4 corrisponde ad una delle cinque strutture cicliche di una permutazione di S_4 (l'ultima corrisponde all'identità, la prima ad un 4-ciclo).

Vale quindi la seguente proposizione.

5.3.7 PROPOSIZIONE. *Le classi coniugate di S_n sono tante quante le partizioni dell'intero n .*

Abbiamo dato pertanto un metodo che ci permette sia di calcolare il numero di classi coniugate, sia la "consistenza" di ogni classe coniugata in S_n . Se invece vogliamo risolvere questo stesso problema ad esempio nel sottogruppo alterno A_n , dobbiamo stare attenti, e ricordare bene la definizione di elementi coniugati: due permutazioni σ e σ' di A_n sono coniugate in A_n se esiste una permutazione τ in A_n tale che

$$\sigma' = \tau \sigma \tau^{-1} .$$

Quindi può succedere che due permutazioni di A_n , coniugate in S_n , non lo siano in A_n perché non esiste una τ in A_n tale che $\tau \sigma \tau^{-1} = \sigma'$, ossia tutte le τ

che funzionano stanno in S_n e non in A_n . Ad esempio, si verifichi che le classi coniugate in A_4 sono le seguenti:

$$\begin{aligned} & \{\text{id}\} \\ & \{(1, 2, 3), (1, 3, 4), (1, 4, 2), (2, 4, 3)\} \\ & \{(1, 3, 2), (1, 4, 3), (1, 2, 4), (2, 3, 4)\} \\ & \{(1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}. \end{aligned}$$



ESERCIZI.

1. Si determini la cardinalità di ogni classe coniugata di S_5 .
2. Si provi che il gruppo S_n è generato dalle $n - 1$ trasposizioni

$$(1, 2), (2, 3), (3, 4), \dots, (n - 1, n).$$

3. Si provi che S_n è generato dalle sole due permutazioni

$$(1, 2), (1, 2, 3, \dots, n).$$

4. Si provi che, per ogni n , il centro di S_n (cfr. definizione 5.1.9) è costituito dal solo elemento neutro.



ESERCIZI DI PROGRAMMAZIONE.

1. Si scriva un programma che calcoli per ogni n il numero di classi coniugate in S_n (cioè il numero di partizioni dell'intero n). Si suggerisce di scrivere una partizione di un intero n come una coppia di vettori (m_1, m_2, \dots, m_k) e (p_1, p_2, \dots, p_k) dove gli m_i e p_i sono interi non nulli tali che m_i rappresenti la molteplicità delle parti p_i della partizione. Ad esempio, la partizione di 22

$$22 = 7 + 4 + 4 + 2 + 2 + 2 + 1$$

ha come parti gli interi $p_1 = 7$, $p_2 = 4$, $p_3 = 2$ e $p_4 = 1$, rispettivamente con molteplicità $m_1 = 1$, $m_2 = 2$, $m_3 = 3$ e $m_4 = 1$. Essa verrà quindi rappresentata con la coppia di vettori:

$$(m_1, m_2, m_3, m_4) = (1, 2, 3, 1), \quad (p_1, p_2, p_3, p_4) = (7, 4, 2, 1).$$

2. Si scriva un programma che conti il numero di elementi di ogni classe coniugata di S_n .
3. Si scriva un programma che calcoli la coniugata di una data permutazione σ mediante una permutazione τ .



CONTROLLO.

1. Due permutazioni di S_n sono coniugate quando ...
2. Che legame c'è tra le partizioni di un intero n e le classi coniugate in S_n ?
3. Cosa significa che due permutazioni di A_n sono coniugate in A_n ?

5.4. I gruppi diedrali

Sia data una figura nel piano. I movimenti rigidi (isometrie) che la mutano in sé corrispondono alle *simmetrie* della figura stessa.

Si pensi ad esempio alla figura 5.2.

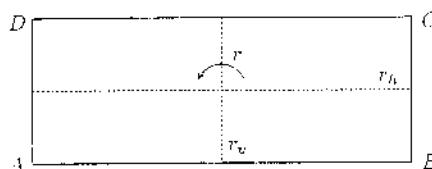


FIGURA 5.2

Ribaltando il rettangolo rispetto a ciascuna delle rette tratteggiate, il rettangolo viene mutato in sé. È facile vedere che l'insieme dei movimenti che muta in sé il rettangolo è costituito da quattro elementi: l'identità e (ossia il "movimento" che non muove nulla), il ribaltamento r_h rispetto all'asse tratteggiato orizzontale, il ribaltamento r_v rispetto all'asse tratteggiato verticale, e infine la rotazione r in senso antiorario di π attorno al centro del rettangolo. L'insieme di questi movimenti forma un gruppo (di trasformazioni), come si verifica immediatamente. Tale gruppo prende il nome di *gruppo di Klein* e si indica anche con la lettera V , (da vier = quattro). La sua tavola di moltiplicazione è la seguente:

c	e	r	r_h	r_v
e	e	r	r_h	r_v
r	r	e	r_v	r_h
r_h	r_h	r_v	e	r
r_v	r_v	r_h	r	e

Se, anziché partire da un rettangolo, si parte da un quadrato, saranno di più i movimenti rigidi che si possono fare senza mutare la figura, cioè sono maggiori le simmetrie della figura. In questo caso (figura 5.3) il gruppo dei movimenti rigidi che mutano in sé il quadrato è costituito dall'identità, dalle tre rotazioni in senso antiorario (di $\pi/2$, di π , di $3\pi/2$ rispettivamente), e dai quattro ribaltamenti (rispetto alle due rette orizzontale e verticale e alle due diagonali).

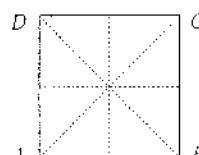


FIGURA 5.3

Si consideri ora il gruppo, che indicheremo con D_3 , dei movimenti rigidi (isometrie) che mutano in sé un triangolo equilatero. I possibili movimenti sono (si veda la figura 5.4):

$$r_1 = \text{rotazione di } \frac{2\pi}{3},$$

$$r_2 = \text{rotazione di } \frac{4\pi}{3},$$

$$r_0 = \text{rotazione identica};$$

inoltre i tre ribaltamenti s_1, s_2, s_3 rispetto ai tre assi di simmetria del triangolo.

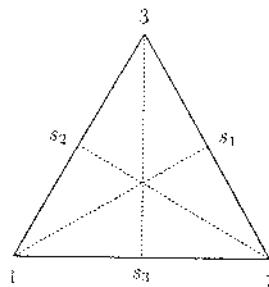


FIGURA 5.4

La tavola di moltiplicazione di questo gruppo è la seguente:

\circ	id	r_1	r_2	s_1	s_2	s_3
id	id	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	id	s_3	s_1	s_2
r_2	r_2	id	r_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	id	r_1	r_2
s_2	s_2	s_3	s_1	r_2	id	r_1
s_3	s_3	s_1	s_2	r_1	r_2	id

Si vede immediatamente che questa tavola coincide con la tavola di moltiplicazione di S_3 , non appena si ponga

$$r_1 = (1, 2, 3)$$

$$r_2 = (1, 3, 2)$$

$$s_1 = (2, 3)$$

$$s_2 = (1, 3)$$

$$s_3 = (1, 2)$$

cioè non appena si faccia corrispondere ad ogni movimento rigido la corrispondente permutazione dei vertici del triangolo. Quindi il gruppo dei movimenti

che mutano in sé un triangolo equilatero si può identificare con il gruppo S_3 , la corrispondenza essendo data associando ad ogni movimento rigido che muta in sé il triangolo la corrispondente permutazione dei vertici. Tale gruppo rientra in una classe importante di gruppi, la classe dei *gruppi diedrali*.

5.4.1 DEFINIZIONE. Dicesi *gruppo diedrale* D_n il gruppo dei movimenti rigidi che mutano in sé un poligono regolare di n lati. \square

Vediamo in generale di studiare D_n . Esso possiede n rotazioni $r_k(2\pi/n)$, $k = 1, \dots, n$, attorno al centro del poligono, corrispondenti agli angoli

$$\frac{2\pi}{n}, \quad 2 \cdot \frac{2\pi}{n}, \quad 3 \cdot \frac{2\pi}{n}, \dots, \quad k \cdot \frac{2\pi}{n}, \dots, \quad n \cdot \frac{2\pi}{n} = \text{id}.$$

Inoltre D_n possiede n ribaltamenti s_i ($i = 1, \dots, n$) rispetto agli n assi di simmetria del poligono: se n è dispari, questi assi di simmetria sono le bisettrici degli angoli del poligono, se $n = 2k$ è pari sono le k bisettrici e i k assi, come si vede dalla figura 5.5.

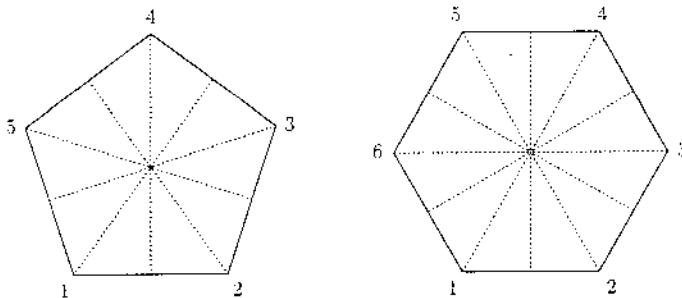


FIGURA 5.5

In definitiva

$$|D_n| = 2n.$$

Dato che i movimenti rigidi di un poligono regolare si possono pensare come permutazioni dei vertici, risulta

$$D_n \subseteq S_n.$$

Per $n = 3$ abbiamo visto che $D_3 = S_3$; per $n > 3$ risulta

$$D_n \subsetneq S_n$$

dato che $|D_n| = 2n$, $|S_n| = n!$, e $2n \leq n!$, e sono uguali solo per $n = 3$.

Indichiamo con r la rotazione di $2\pi/n$; essa ha ordine n , e genera il sottogruppo di tutte le rotazioni, nel senso che ogni rotazione è una opportuna potenza di r (cfr. definizione 5.1.10). Infatti

$$r^k = r_{k \cdot 2\pi/n} \quad k = 1, \dots, n.$$

Inoltre, l'ordine della rotazione r^k è n/d , con $d = \text{MCD}(n, k)$. (Si ricordi quanto detto a proposito delle radici n -esime dell'unità, proposizione 3.4.5.)

L'ordine di ogni ribaltamento s_i è ovviamente 2.

Il gruppo D_n per $n > 2$ è non abeliano (cfr. esercizio 5.4.1).

5.4.2 PROPOSIZIONE. *Sia r la rotazione di $2\pi/n$ attorno al centro di un poligono regolare e s un qualunque ribaltamento. Allora il gruppo diedrale D_n è generato da r ed s e risulta*

$$D_n = \langle r, s \rangle = \{\text{id}, r, r^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s\}.$$

Dimostrazione. Dimostreremo che ogni simmetria del poligono si può scrivere nella forma

$$r^i s^k, \quad i = 0, \dots, n-1, \quad k = 0, 1,$$

avendo indicato con s (senza perdita di generalità) il ribaltamento attorno al vertice 1 del poligono. Dalla figura 5.5 si vede che si può identificare r con la permutazione $(1, 2, \dots, n)$ e s ($= s^{-1}$) con la permutazione

$$s = s^{-1} = (2, n)(3, n-1) \cdots (k, n-k+2)(k+1, n-k+1)$$

$$\begin{cases} n = 2k+2 & n \text{ pari} \\ n = 2k+1 & n \text{ dispari.} \end{cases}$$

Dalla

$$srs^{-1} = (1, n, n-1, \dots, 3, 2) = r^{-1}$$

che si ricava con la regola del calcolo della coniugata di una permutazione, si ha quindi

$$sr = r^{n-1}s$$

da cui si ricavano facilmente le seguenti relazioni che garantiscono il risultato cercato:

$$\begin{aligned} r^\alpha r^\beta &= r^\gamma, & \gamma &\equiv \alpha + \beta \pmod{n} \\ r^\alpha (r^\beta s) &= r^\gamma s, & \gamma &\equiv \alpha + \beta \pmod{n} \\ (r^\alpha s) r^\beta &= r^\delta s, & \delta &\equiv \alpha + (n - \beta) \pmod{n} \\ (r^\alpha s) (r^\beta s) &= r^\delta, & \delta &\equiv \alpha + (n - \beta) \pmod{n}. \quad \square \end{aligned}$$

Si noti che ogni elemento di D_n , in quanto movimento rigido, è rappresentato da una matrice ortogonale. In particolare

$$r \longleftrightarrow R = \begin{pmatrix} \cos(2\pi/n) & \sin(2\pi/n) \\ -\sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}$$

$$s \longleftrightarrow S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Risulta, come si verifica facilmente, $R^n = I = S^2$ e $SR = R^{n-1}S$. Identificando pertanto r con R e s con S , il sottogruppo generato dalle matrici R, S coincide con il gruppo diedrale D_n . Abbiamo così provato che ogni gruppo D_n si può pensare come sottogruppo del gruppo ortogonale $(O_2(\mathbb{R}), \cdot)$.

ESERCIZI.

1. Si provi che D_n , per $n > 2$ è un gruppo non abeliano.
2. Si studi in dettaglio il gruppo D_4 delle simmetrie di un quadrato, determinando il periodo di ciascuno dei suoi elementi.
3. Si determini il centro di D_n per ogni n (cfr. definizione 5.1.9).
4. Si determinino le classi coniugate in D_4 .

ESERCIZI DI PROGRAMMAZIONE.

1. Si faccia un programma che studi tutte le proprietà del gruppo D_4 delle simmetrie di un quadrato (periodo degli elementi, classi coniugate, centro, sottogruppi, ecc.).

CONTROLLO.

1. È vero che D_n è un sottogruppo di S_n ? In quali casi coincidono?
2. Per ogni n il gruppo diedrale D_n si può generare con due elementi: è possibile che esista un sistema di generatori costituito da un solo elemento? Giustificare la risposta.
3. Il prodotto di due rotazioni è ...
Il prodotto di due ribaltamenti è ...
Il prodotto di una rotazione per un ribaltamento è ...
Il prodotto di un ribaltamento per una rotazione è ...

5.5. Classi laterali modulo un sottogruppo e teorema di Lagrange

Dopo avere esaminato in dettaglio alcuni importanti esempi di gruppi, torniamo a studiare le proprietà generali di un gruppo.

Sia (G, \cdot) un gruppo e sia H un suo sottogruppo. Definiamo in G la seguente relazione:

$$(5.5.1) \quad a \varrho_d b \iff ab^{-1} \in H.$$

N.B. Se l'operazione di G fosse l'addizione, la relazione sarebbe

$$a \varrho_d b \iff a - b \in H$$

che è una nostra vecchia conoscenza nel caso $G = \mathbb{Z}$ e $H = n\mathbb{Z}$.

Per questo motivo la (5.5.1) prende il nome di *congruenza destra* mod H . La (5.5.1) è una relazione di equivalenza (verificare!). Il gruppo G viene pertanto ripartito in classi di equivalenza, che prendono il nome di *classi laterali destre modulo il sottogruppo H* o *lateralì destri modulo H* . Il *destro* deriva dal fatto che si può definire quest'altra relazione (anch'essa di equivalenza), la congruenza sinistra modulo H :

$$a \varrho_s b \iff b^{-1}a \in H$$

e in tal caso si otterrebbero i lateralì sinistri. Nel caso in cui sia $G = \mathbb{Z}$ e $H = n\mathbb{Z}$ le due relazioni di equivalenza coincidono e quindi coincidono anche i lateralì destri e sinistri.

Vogliamo renderci conto di come sono fatte in generale queste classi. Sia a un elemento di G e sia $\varrho_d(a)$ la sua classe di equivalenza modulo la relazione (5.5.1). Allora

$$\begin{aligned}\varrho_d(a) &\stackrel{\text{def}}{=} \{b \in G \mid b \varrho a\} = \{b \in G \mid ba^{-1} \in H\} \\ &= \{b \in G \mid ba^{-1} = h, h \in H\} \\ &= \{b \in G \mid b = ha \text{ per qualche } h \in H\} \subseteq Ha.\end{aligned}$$

Il viceversa è facile da provare. Quindi la classe $\varrho_d(a)$ coincide con il sottoinsieme Ha di G , dove

$$Ha \stackrel{\text{def}}{=} \{ha \mid h \in H\}.$$

Ora, a differenza di quello che accade ad esempio nel caso della relazione di coniugio, qui accade il seguente fatto notevole.

5.5.1 PROPOSIZIONE. *Tutte le classi laterali (destre o sinistre) hanno la stessa cardinalità, che è la cardinalità del sottogruppo H .*

Dimostrazione. Basta dimostrare che esiste una corrispondenza biunivoca tra due classi laterali destre (sinistre) qualsiasi, perché questo significa che tutte le classi laterali destre (sinistre) hanno la stessa cardinalità di H (che è una classe laterale destra e sinistra al tempo stesso). Siano quindi Ha e Hb due qualunque classi laterali destre. La corrispondenza

$$\psi : Ha \longrightarrow Hb$$

definita ponendo

$$\psi(ha) = hb$$

- (a) è iniettiva: se $\psi(h_1a) = \psi(h_2a)$, allora vuol dire che $h_1b = h_2b$, da cui, per la legge di cancellazione, $h_1 = h_2$ e quindi $h_1a = h_2a$;
 (b) è suriettiva: dato comunque un elemento di Hb , questo sarà del tipo hb per qualche $h \in H$. Esso proviene allora da ha . \square

5.5.2 ESEMPIO. Sia $G = S_3$ e sia H il sottogruppo generato dalla permutazione (2, 3). Calcoliamo sia i laterali destri sia i laterali sinistri.

LATERALI DESTRI:

$$H = H(2, 3) = \{\text{id}, (2, 3)\},$$

$$H(1, 2) = \{(1, 2), (2, 3)(1, 2)\} = \{(1, 2), (1, 3, 2)\} = H(1, 3, 2),$$

$$H(1, 3) = \{(1, 3), (2, 3)(1, 3)\} = \{(1, 3), (1, 2, 3)\} = H(1, 2, 3),$$

LATERALI SINISTRI:

$$H = (2, 3)H = \{\text{id}, (2, 3)\},$$

$$(1, 2)H = \{(1, 2), (1, 2)(2, 3)\} = \{(1, 2), (1, 2, 3)\} = (1, 2, 3)H,$$

$$(1, 3)H = \{(1, 3), (1, 3)(2, 3)\} = \{(1, 3), (1, 3, 2)\} = (1, 3, 2)H.$$

Tutte le classi laterali (sia destre sia sinistre) hanno lo stesso numero di elementi (uguale alla cardinalità di H , cioè 2). Si vede tuttavia un fatto importante: le classi laterali destre non coincidono con le classi laterali sinistre. Infatti la situazione che si presenta è rappresentata in figura 5.6.

S_3		S_3	
(1, 3)	(1, 2, 3)	$H(1, 3) \neq (1, 3)H$	(1, 3) (1, 3, 2)
(1, 2)	(1, 3, 2)	$H(1, 2) \neq (1, 2)H$	(1, 2) (1, 2, 3)
e	(2, 3)	H	H

FIGURA 5.6

Se prendiamo invece come sottogruppo il sottogruppo

$$K = \{\text{id}, (1, 2, 3), (1, 3, 2)\}$$

le classi laterali destre e sinistre rispetto a questo sottogruppo sono le seguenti.

LATERALI DESTRI:

$$K = K(1, 2, 3) = K(1, 3, 2) = \{\text{id}, (1, 2, 3), (1, 3, 2)\},$$

$$\begin{aligned} K(1, 2) &= \{(1, 2), (1, 2, 3)(1, 2), (1, 3, 2)(1, 2)\} = \{(1, 2), (1, 3), (2, 3)\} \\ &= K(1, 3) = K(2, 3), \end{aligned}$$

LATERALI SINISTRI:

$$\begin{aligned} K &= (1, 2, 3)K = (1, 3, 2)K = \{\text{id}, (1, 2, 3), (1, 3, 2)\}, \\ (1, 2)^* K &= \{(1, 2), (1, 2)(1, 2, 3), (1, 2)(1, 3, 2)\} = \{(1, 2), (2, 3), (1, 3)\} \\ &= (2, 3)K = (1, 3)K. \end{aligned}$$

In questo caso le classi laterali destre coincidono con le classi laterali sinistre. Vedremo fra breve il motivo che sta sotto questa diversità di comportamento. \square

La proposizione ora dimostrata, che ci dice che tutte le classi laterali (destre o sinistre) hanno la stessa cardinalità, ha particolare interesse nel caso in cui il gruppo G sia *finito*.

5.5.3 TEOREMA DI LAGRANGE. *Sia G un gruppo finito e sia H un suo sottogruppo. Allora l'ordine di H divide l'ordine di G .*

Dimostrazione. Sia $|G| = n$ e $|H| = m$, e sia i il numero delle classi laterali destre modulo H . Per quanto visto nella proposizione precedente, gli n elementi di G si ripartiscono nelle i classi laterali destre, ciascuna delle quali ha m elementi. Quindi

$$(5.5.2) \quad n = i \cdot m. \quad \square$$

5.5.4 DEFINIZIONE. Sia G un gruppo e sia H un sottogruppo di G . Si dice *indice di H in G* la cardinalità dei laterali (destri o sinistri) modulo H . Si indica con $[G : H]$. \square

5.5.5 COROLLARIO. *Sia G un gruppo finito e sia H un suo sottogruppo. L'indice di H in G divide l'ordine del gruppo.*

Dimostrazione. Basta leggere la (5.5.2). \square

 **ATTENZIONE.** Il teorema di Lagrange ci dice quali sono gli ordini *ammissibili* per i sottogruppi di un gruppo finito. Ad esempio, ci dice che un gruppo di ordine 10 non può avere un sottogruppo di ordine 4 o 6 o 8. Si badi bene che non dice nulla riguardo all'*esistenza* di un sottogruppo che abbia un ordine ammissibile. Esso quindi dà una condizione necessaria, ma non sufficiente, per l'esistenza di un sottogruppo di dato ordine. \square

Il teorema di Lagrange ha molte importanti conseguenze:

5.5.6 COROLLARIO. *Un gruppo G che abbia come ordine un numero primo è necessariamente un gruppo ciclico.*

Dimostrazione. Un gruppo di ordine un numero primo può avere, in base al teorema di Lagrange, come sottogruppi solamente i sottogruppi banali. Sia a un elemento diverso dall'elemento neutro e . Si consideri il sottogruppo generato da a . Esso possiede almeno due elementi (a ed e), quindi $\langle a \rangle = G$, e G è ciclico. \square

Abbiamo già visto (cfr. §5.1) che in un gruppo finito ogni elemento g ha necessariamente ordine (o periodo) finito: lo indicheremo con $o(g)$. Come ulteriore conseguenza del teorema di Lagrange si ha:

5.5.7 COROLLARIO. *Se G è finito, allora l'ordine $o(g)$ di ogni $g \in G$ divide l'ordine di G .*

Dimostrazione. Basta osservare che $o(g) = |\langle g \rangle|$. \square

5.5.8 COROLLARIO. *Se G è finito e $|G| = n$, allora*

$$g^n = e \quad \forall g \in G .$$

Dimostrazione. $g^{|G|} = g^{k \cdot o(g)} = (g^{o(g)})^k = e^k = e$. \square

Come conseguenza di questo corollario ritroviamo il teorema di Eulero (cfr. §2.8):

5.5.9 TEOREMA. *Indicata con φ la funzione di Eulero, se $(a, n) = 1$, risulta*

$$a^{\varphi(n)} \equiv 1 \pmod{n} .$$

Dimostrazione. Indicato con U_n l'insieme degli elementi invertibili di \mathbb{Z}_n , cioè quelle classi \bar{a} tali che $(a, n) = 1$, esso è un gruppo ed è tale che $|U_n| = \varphi(n)$. Quindi

$$\overline{a^{\varphi(n)}} = \bar{a}^{\varphi(n)} = \bar{1}$$

cioè $a^{\varphi(n)} \equiv 1 \pmod{n}$. \square

ESERCIZI.

1. Siano σ e τ le seguenti due permutazioni di S_4 :

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

Si determini il sottogruppo H generato da σ e τ e si studino le classi laterali destre e sinistre.

2. Sia G il gruppo delle rotazioni del piano che lasciano fisso un punto 0. Detta Φ la rotazione di π , si consideri il sottogruppo H generato da Φ . Si studino i laterali destri e sinistri modulo H .
3. Nel gruppo D_4 delle simmetrie di un quadrato si determinino tutti i sottogruppi e si studino rispetto ad essi i laterali (destri e/o sinistri).



ESERCIZI DI PROGRAMMAZIONE.

1. Si utilizzi il programma fatto negli esercizi di programmazione del §5.1 per verificare il teorema di Lagrange e per verificare che ogni gruppo che ha come ordine un numero primo è ciclico.



CONTROLLO.

1. Laterali destri e sinistri modulo un sottogruppo. Dare degli esempi (diversi da quelli presentati nel testo) da cui risulti che i laterali destri e sinistri non sempre coincidono.
2. Come si utilizzano i laterali destri (o sinistri) nella dimostrazione del teorema di Lagrange?
3. Il teorema di Lagrange offre una condizione necessaria o sufficiente (o entrambe) per l'esistenza di un sottogruppo che abbia come ordine un divisore dell'ordine del gruppo?

5.6. Isomorfismo tra gruppi e il teorema di Cayley

Come abbiamo già visto nel caso degli anelli, non siamo interessati a distinguere due gruppi quando godono delle identiche proprietà algebriche, quando cioè sono *algebricamente indistinguibili*. Nella classe di tutti i gruppi introduciamo pertanto una relazione che ha esattamente questo compito, di identificare gruppi che sono algebricamente indistinguibili. Introduciamo quindi anche per i gruppi la nozione di isomorfismo.

5.6.1 DEFINIZIONE. Siano $(G, *)$ e (G', \cdot) due gruppi. Diremo che G è *isomorfo* a G' e si scrive $G \cong G'$ se esiste un'applicazione biunivoca φ tra G e G' che conserva l'operazione, tale cioè che

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b) \quad \forall a, b \in G.$$

Una tale applicazione prende il nome di *isomorfismo*. \square

Abbiamo già visto gruppi tra di loro isomorfi, ad esempio il gruppo D_3 delle simmetrie di un triangolo equilatero ed il gruppo S_3 . In questo caso un isomorfismo è dato associando ad ogni movimento rigido la corrispondente permutazione sui vertici del triangolo.

Un altro gruppo che è isomorfo ai precedenti è il gruppo $GL_2(\mathbb{Z}_2)$. Esso consiste delle seguenti matrici:

$$GL_2(\mathbb{Z}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}.$$

Si invita lo studente a determinare esplicitamente un isomorfismo di tale gruppo con i precedenti.

Il gruppo di Klein è isomorfo al gruppo degli elementi invertibili di \mathbb{Z}_8 (si verifichi).

Il gruppo $(\mathbb{R}, +)$ è isomorfo al gruppo moltiplicativo dei numeri reali positivi, attraverso la funzione e^x (si veda la figura 5.7).

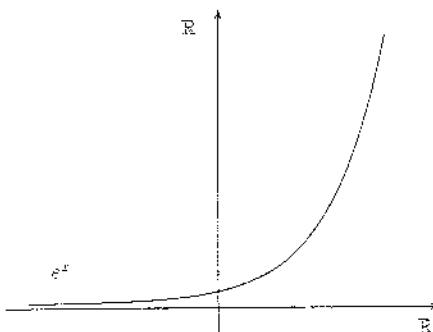


FIGURA 5.7

Quando due gruppi sono isomorfi, *tutte* le proprietà algebriche soddisfatte dal primo sono soddisfatte anche dal secondo e viceversa. Esempi di proprietà che si conservano sono ad esempio l'abelianità, la cardinalità, l'ordine dei vari elementi, il fatto di essere ciclico, di avere sottogruppi di un dato ordine, ecc. Se quindi due gruppi differiscono anche solo in una di queste (o altre) proprietà, allora si può concludere che i due gruppi *non sono isomorfi*.

- (1) $(\mathbb{Z}, +)$ non è isomorfo a $(\mathbb{Q} \setminus \{0\}, \cdot)$. Infatti in \mathbb{Z} ogni elemento diverso dallo zero ha periodo infinito, mentre in $\mathbb{Q} \setminus \{0\}$ esistono *due* elementi, 1 e -1 , di periodo finito.
- (2) $(U(\mathbb{Z}_8), \cdot)$ e $(\mathbb{Z}_4, +)$ sono entrambi gruppi di ordine quattro, ma non sono isomorfi perché in \mathbb{Z}_4 esiste un elemento di periodo 4, mentre in $U(\mathbb{Z}_8)$ non esiste un tale elemento.
- (3) $(\mathbb{C} \setminus \{0\}, \cdot)$ e $(\mathbb{R} \setminus \{0\}, \cdot)$ non sono isomorfi, perché in $(\mathbb{R} \setminus \{0\}, \cdot)$ gli ordini dei suoi elementi sono ∞ , 1 e 2, mentre in $(\mathbb{C} \setminus \{0\}, \cdot)$ esistono elementi di ogni ordine (si pensi alle radici n -esime dell'unità).
- (4) Dato un intero n pari, $n > 4$, esistono *almeno due* gruppi non isomorfi di ordine n . Basta prendere \mathbb{Z}_n e il gruppo diedrale $D_{n/2}$: non sono isomorfi, dato che il primo è abeliano, mentre il secondo non lo è.

Nella definizione 5.1.21, abbiamo definito i gruppi di trasformazioni e abbiamo visto vari esempi di tali gruppi. Faremo ora vedere che ogni gruppo si può sempre pensare come un opportuno gruppo di trasformazioni.

5.6.2 TEOREMA DI CAYLEY. *Ogni gruppo è isomorfo ad un gruppo di trasformazioni.*

Dimostrazione. Si tratta di dimostrare che ogni gruppo G è isomorfo ad un sottogruppo di $S(X)$ per un opportuno insieme X . Ebbene, prendiamo come

insieme X il gruppo G stesso, e definiamo la seguente applicazione:

$$\begin{aligned} T_a : G &\longrightarrow G \\ x &\longmapsto ax \quad \forall x \in G . \end{aligned}$$

T_a è la moltiplicazione sinistra per a . Si tratta di una *corrispondenza biunivoca* di G in sé. Infatti

- (1) $ax = ay \implies x = y$, cioè T_a è iniettiva.
- (2) Per ogni $y \in G$ esiste $x \in G$ tale che $y = ax$: basta prendere $x = a^{-1}y$.
Quindi T_a è suriettiva.

Abbiamo così provato che

$$T_a \in \mathcal{S}(G) .$$

Definiamo allora la seguente applicazione:

$$\begin{aligned} \Psi : (G, \cdot) &\longrightarrow (\mathcal{S}(G), \circ) \\ a &\longmapsto T_a . \end{aligned}$$

- (1) Ψ conserva l'operazione: si tratta di far vedere che

$$\Psi(ab) = \Psi(a) \circ \Psi(b)$$

cioè

$$T_{ab} = T_a \circ T_b .$$

Infatti

$$T_{ab}(x) = ab \cdot x = a(bx) = T_a(T_b(x)) \quad \forall x \in G$$

che ci dice appunto che $T_{ab} = T_a \circ T_b$.

- (2) Ψ è iniettiva. Infatti, se $\Psi(a) = \Psi(b)$, cioè $T_a = T_b$, allora in particolare

$$a \cdot T_a(e) = T_b(e) = b \implies a = b .$$

Chiaramente tale applicazione non è suriettiva: si confrontino le cardinalità di G e di $\mathcal{S}(G)$. Tuttavia, l'immagine di Ψ , cioè

$$\Psi(G) \stackrel{\text{def}}{=} \{T_a \mid a \in G\}$$

è un sottogruppo di $\mathcal{S}(G)$ (si verifichil) che risulta quindi *isomorfo* a G (si veda la figura 5.8). \square

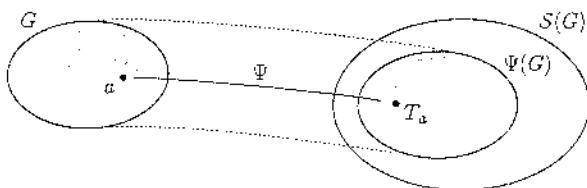


FIGURA 5.8

Se G è finito e $G = n$, allora il teorema ci dice che G è isomorfo ad un sottogruppo di S_n . Quindi di ogni gruppo di un dato ordine n esiste una coppia dentro S_n . Ma allora basta studiare un solo tipo di gruppo, cioè S_n , per conoscere *tutti* i gruppi! La cosa però non è praticabile, perché supponiamo di voler studiare un gruppo G di ordine 10. Basta (...) quindi studiare S_{10} , che però ha il piccolo difetto di avere più di tre milioni e mezzo di elementi. Forse è meglio studiare direttamente il gruppo G . Questa osservazione è stata fatta per mostrare che l'importanza del teorema di Cayley è solamente di natura teorica, e non pratica, come uno invece sarebbe tentato di pensare. È chiaro d'altra parte che si potrebbe cercare di scegliere un X più "economico". È quanto cercheremo di fare nei prossimi paragrafi; dovremo però premettere alcune nozioni importanti.

ESERCIZI.

- Si determinino quattro sottogruppi diversi di S_4 isomorfi a S_3 e nove isomorfi a S_2 .
- Indicato con \mathbb{Q} l'insieme dei razionali, si dica se il gruppo additivo $(\mathbb{Q}, +)$ è o no isomorfo al gruppo moltiplicativo $(\mathbb{Q} \setminus \{0\}, \cdot)$.
- Si verifichi il teorema di Cayley nel caso in cui sia $G = \langle g \mid g^4 = 1 \rangle$, e nel caso in cui G sia il gruppo di Klein.
- Sia G il gruppo moltiplicativo degli elementi invertibili di \mathbb{Z}_8 e sia G' il gruppo moltiplicativo degli elementi invertibili di \mathbb{Z}_{12} . Si provi che sono isomorfi tra di loro. A quale altro gruppo noto sono isomorfi?
- Dimostrare che l'insieme

$$S = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid x, y \in \mathbb{R}, x, y \text{ non entrambi nulli} \right\}$$

- è un sottogruppo di $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ isomorfo a (\mathbb{C}^*, \cdot) , dove $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
- Si provi che (\mathbb{Z}_4, \div) è isomorfo a $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$.

ESERCIZI DI PROGRAMMAZIONE.

- Dato un gruppo G di ordine n , fare un programma che determini per ogni n l'ordine del gruppo in cui si trova immerso G in base al teorema di Cayley (tale programma dovrà averlo già fatto!). Dai risultati del programma ci si rende conto della non utilità pratica del teorema di Cayley.



CONTROLLO.

1. Enunciato e significato del teorema di Cayley. Perché la sua importanza è soprattutto teorica, più che pratica? Spiegare.

5.7. Omomorfismi

Come nel caso degli anelli, si dà la definizione di omomorfismo tra gruppi.

5.7.1 DEFINIZIONE. Siano $(G, *)$ e (G', \cdot) due gruppi. Una applicazione φ tra G e G' si dice *omomorfismo* se

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b) \quad \forall a, b \in G. \quad \square$$

Un omomorfismo quindi è un'applicazione tra due gruppi che conserva l'operazione. Ad ogni omomorfismo tra due gruppi restano associati due importanti sottoinsiemi di G e G' rispettivamente, il nucleo e l'immagine:

$$\text{Ker } \varphi \stackrel{\text{def}}{=} \{g \in G \mid \varphi(g) = e_{G'}\}$$

$$\text{Im } \varphi \stackrel{\text{def}}{=} \{g' \in G' \mid g' = \varphi(g) \text{ per qualche } g \in G\}$$

È facile dimostrare che $\text{Ker } \varphi$ è un sottogruppo di G , mentre $\text{Im } \varphi$ è un sottogruppo di G' .

Indicando per semplicità con \cdot sia l'operazione di G sia l'operazione di G' , valgono le seguenti proprietà:

5.7.2 PROPOSIZIONE. Siano G e G' due gruppi e sia φ un omomorfismo tra G e G' . Indicati con e e con e' gli elementi neutri rispettivamente di G e di G' rispettivamente. allora

- (a) $\varphi(e) = e'$:
- (b) $\varphi(g^{-1}) = \varphi(g)^{-1}$ per ogni $g \in G$.

Dimostrazione. (a) $e' \varphi(g) = \varphi(g) = \varphi(eg) = \varphi(e)\varphi(g)$, quindi per la legge di cancellazione in G'

$$e' = \varphi(e).$$

(b) $\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e) = e'$, da cui $\varphi(g^{-1}) = \varphi(g)^{-1}$. \square

Un omomorfismo che sia iniettivo si dice *monomorfismo*, un omomorfismo che sia suriettivo si dice *epimorfismo*. Un omomorfismo che sia contemporaneamente iniettivo e suriettivo è un *isomorfismo*. Lasciamo come esercizio la seguente proposizione.

5.7.3 PROPOSIZIONE. Sia φ un omomorfismo tra due gruppi G e G' . Allora φ è un monomorfismo se e solo se $\text{Ker } \varphi = \{e\}$.

Sia φ un omomorfismo tra due gruppi G e G' , con nucleo $K = \text{Ker } \varphi$. Dato che K è un sottogruppo di G , possiamo costruire le classi laterali destre di G modulo K . Risulta

$$\begin{aligned} a \varrho_d b &\iff ab^{-1} \in K \iff \varphi(ab^{-1}) = e' \\ &\iff \varphi(a)\varphi(b)^{-1} = e' \iff \varphi(a) = \varphi(b). \end{aligned}$$

Quindi due elementi a e b in G sono in relazione ϱ_d modulo $\text{Ker } \varphi$ se e solo se hanno la stessa immagine mediante φ (si veda la figura 5.9). La cardinalità di $\text{Im } \varphi$ uguaglia quindi l'indice di K in G .

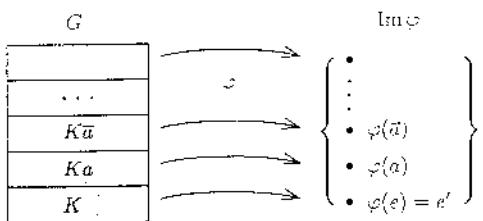


FIGURA 5.9

5.7.4 ESEMPI.

(a) Si consideri l'applicazione:

$$\begin{aligned} \varphi : (\text{GL}_n(\mathbb{R}), \cdot) &\longrightarrow (\mathbb{R} \setminus \{0\}, \cdot) \\ A &\longmapsto \det A. \end{aligned}$$

Si tratta di un omomorfismo il cui nucleo è dato da $\text{SL}_n(\mathbb{R}) = \{A \in \text{GL}_n(\mathbb{R}) \mid \det A = 1\}$. L'immagine di φ è costituita da tutti i numeri reali diversi da zero. Si verifichi che due matrici stanno nella stessa classe laterale destro modulo il nucleo se e solo se hanno la stessa immagine mediante φ , cioè se e solo se hanno lo stesso determinante.

(b) L'applicazione φ di $(\mathbb{R} \setminus \{0\}, \cdot)$ in sé data da

$$\varphi(x) = \frac{1}{|x|}$$

è un omomorfismo, il cui nucleo è $K = \{\pm 1\}$, e la cui immagine è costituita dai reali positivi. \square

5.7.5 PROPOSIZIONE. *Sia φ un omomorfismo tra due gruppi G e G' . Allora:*

- (a) *Se G è finito, l'ordine di $\text{Im } \varphi$ divide l'ordine di G (e l'ordine di G' , se anche G' è finito).*
- (b) *Se G è ciclico, allora $\text{Im } \varphi$ è ciclico.*
- (c) *Se g ha periodo finito, allora il periodo di $\varphi(g)$ divide il periodo di g .*

Dimostrazione. (a) Ricordiamo che $|\text{Im } \varphi|$ uguaglia l'indice di K in G , che è un divisore di $|G|$ (corollario 5.5.5).

(b) Se $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$, allora $\text{Im } \varphi = \{\varphi(g^k) \mid k \in \mathbb{Z}\} = \{\varphi(g)^k \mid k \in \mathbb{Z}\} = \langle \varphi(g) \rangle$.

(c) Sia g un elemento di periodo n . Allora

$$\varphi(g)^n = \varphi(g^n) = \varphi(e) = e'.$$

Ma allora, detto h il periodo di $\varphi(g)$, dalla $n = hq + r$ con $0 \leq r < h$ si ha

$$\underbrace{\varphi(g)^n}_{=e'} = \underbrace{(\varphi(g)^h)^q}_{=e'} \cdot \varphi(g)^r$$

da cui $\varphi(g)^r = e'$, ossia $r = 0$ e quindi h divide n . \square

5.7.6 APPLICAZIONI.

(a) Omomorfismi che hanno come dominio un gruppo ciclico.

Si osservi innanzitutto che ogni omomorfismo che ha come dominio un gruppo ciclico $G = \langle g \rangle$ è definito non appena si conosca l'immagine del solo generatore g . Ciò premesso, distinguiamo i due casi, in cui il gruppo ciclico sia infinito, e quello in cui il gruppo sia finito di ordine n .

(α) Se $G = \langle g \rangle$ è infinito, l'immagine del generatore g può essere un qualunque elemento di G' , quindi gli omomorfismi di un gruppo ciclico infinito in un gruppo G' sono tanti quanti gli elementi di G' .

(β) Sia $G = \langle g \mid g^n = 1 \rangle$ ciclico di ordine n . In questo caso le immagini di g mediante un omomorfismo φ sono da ricercarsi tra quegli elementi di G' il cui ordine è un divisore di n , e viceversa, dato comunque un elemento di G' che ha ordine un divisore di n , esiste uno e un solo omomorfismo che manda g in tale elemento.

Quindi gli omomorfismi di un gruppo ciclico finito di ordine n sono tanti quanti gli elementi di G' che hanno come periodo un divisore di n .

(b) Come conseguenza di quanto detto al punto (a), si ha che l'unico omomorfismo da \mathbb{Z}_8 a \mathbb{Z}_5 è l'omomorfismo nullo. Tale fatto si può vedere anche al modo seguente: se φ è un omomorfismo di \mathbb{Z}_8 in \mathbb{Z}_5 , allora $|\text{Im } \varphi|$ deve dividere sia 8 sia 5, quindi $|\text{Im } \varphi| = 1$. \square



ESERCIZI.

- Si provi che se φ è un isomorfismo tra due gruppi G e G' , allora per ogni $g \in G$ il periodo di g uguaglia il periodo di $\varphi(g)$.
- Si contino tutti gli isomorfismi tra due gruppi ciclici G e G' dello stesso ordine.
- Si determinino tutti gli omomorfismi del gruppo additivo $(\mathbb{Q}, +)$ dei razionali in $(\mathbb{Z}, +)$.

4. Sia φ un omomorfismo tra due gruppi G e G' . Si provi che se G è abeliano, allora $\text{Im } \varphi$ è abeliano.

 **ESERCIZI DI PROGRAMMAZIONE.**

- Si scriva un programma che verifichi se una data applicazione tra due gruppi finiti è un omomorfismo.
- Si scriva un programma che verifichi (attraverso l'esame del nucleo) se un omomorfismo tra due gruppi è un monomorfismo.
- Si scriva un programma che verifichi la proposizione 5.7.5.

 **CONTROLLO.**

- Determinare alcune proprietà degli omomorfismi tra due gruppi.
- Per verificare se un omomorfismo è iniettivo basta ...

5.8. Relazioni compatibili e sottogruppi normali. Gruppi quoziante

Sia G un gruppo e sia ϱ una relazione di equivalenza definita su G , *compatibile con l'operazione del gruppo*, tale cioè, ricordiamo, che

$$g_1 \varrho g'_1, \quad g_2 \varrho g'_2 \implies g_1 g_2 \varrho g'_1 g'_2$$

La situazione è illustrata nella figura 5.10.

g_2	g'_2
$g_1 g_2$	$g'_1 g'_2$
g_1	g'_1

FIGURA 5.10

Tenendo presenti le definizioni date nel §5.5 di congruenza destra ϱ_d e sinistra ϱ_s modulo un sottogruppo, dimostreremo la seguente proposizione.

5.8.1 PROPOSIZIONE. *Sia G un gruppo e sia ϱ una relazione di equivalenza compatibile definita su G . Posto*

$$H = \{x \in G \mid x \varrho e\}$$

- H è un sottogruppo di G .
- Indicate con ϱ_d e ϱ_s le relazioni di congruenza destra e sinistra modulo H , risulta

$$\varrho = \varrho_d = \varrho_s .$$

In altre parole,

$$x \varrho y \iff xy^{-1} \in H \iff y^{-1}x \in H.$$

Dimostrazione. (a) Infatti:

$$e \varrho e \implies e \in H.$$

Inoltre, per ogni $x, y \in H$

$$\begin{array}{c} x \varrho e \\ y \varrho e \end{array} \implies xy \varrho ee = e \implies xy \in H.$$

Infine

$$\begin{array}{c} x \varrho e \\ x^{-1} \varrho x^{-1} \end{array} \implies e \varrho x^{-1} \implies x^{-1} \in H.$$

(b) $x \varrho y$ e $y^{-1} \varrho y^{-1}$ implicano (per la compatibilità di ϱ) $xy^{-1} \varrho e$, ossia $x \varrho_d y$. Viceversa, se $x \varrho_d y$ allora $xy^{-1} \in H$, cioè $xy^{-1} \varrho e$, da cui (sempre per la compatibilità di ϱ) $x \varrho y$. Quindi $x \varrho y \iff x \varrho_d y$. Analogamente con ϱ_s . \square

La proposizione appena provata ci dice questo: data in G una *qualsiasi* relazione di equivalenza ϱ *compatibile con l'operazione del gruppo*, la partizione in classi da essa determinata altro non è che la partizione in laterali (destri o sinistri) modulo il *sottogruppo* H coincidente con la classe dell'elemento neutro. Inoltre i laterali destri coincidono con i laterali sinistri, ossia $Hx = xH$ per ogni $x \in G$. Si noti che nel giungere a questo risultato si è utilizzata in modo sostanziale la compatibilità della relazione ϱ .

Ci poniamo ora il problema inverso. Possiamo dire che, *dato comunque* un sottogruppo H di G , le relazioni di congruenza ϱ_d e ϱ_s modulo H sono compatibili? La risposta è in genere negativa, come mostra il seguente esempio.

Sia $G = S_3$ e H il sottogruppo $H = \{(2, 3)\}$. La figura 5.11 illustra la ripartizione di S_3 in classi modulo ϱ_d e ϱ_s , rispettivamente, cioè la ripartizione in laterali destri e sinistri rispettivamente modulo H .

S_3	ϱ_d	S_3	ϱ_s
$\{(1, 3)\}$	$(1, 2, 3)$	$\{(1, 3)\}$	$(1, 3, 2)$
$\{(1, 2)\}$	$(1, 3, 2)$	$(1, 2)$	$(1, 2, 3)$
e	$(2, 3)$	e	$(2, 3)$

FIGURA 5.11

Nessuna delle due relazioni è compatibile, perché ad esempio

$$(1, 2, 3)(1, 3, 2) = \text{id} \in H, \quad \text{ma} \quad (1, 3)(1, 2) = (1, 2, 3) \notin H.$$

Si osservi anche che $\varrho_d \neq \varrho_s$. Infatti esistono elementi x e y tali che $xy^{-1} \in H$ ma $y^{-1}x \notin H$. Basta prendere ad esempio $x = (1, 3, 2)$ e $y = (1, 2)$. Risulta $xy^{-1} = (2, 3) \in H$, ma $y^{-1}x = (1, 3) \notin H$.

Quale ipotesi aggiuntiva occorre perché le relazioni ϱ_d e ϱ_s siano compatibili? La risposta ci viene data dalla proposizione che segue.

5.8.2 PROPOSIZIONE. *Sia H un sottogruppo di G , e siano ϱ_d e ϱ_s le relazioni di congruenza destra e sinistra modulo H . Condizione necessaria e sufficiente perché ϱ_d (o ϱ_s) sia compatibile è che sia*

$$\varrho_d = \varrho_s, \quad \text{ossia} \quad Hx = xH \quad \forall x \in G.$$

Dimostrazione. Osserviamo innanzitutto che moltiplicando a destra per uno stesso elemento di G due elementi equivalenti modulo ϱ_d si ottengono ancora elementi equivalenti modulo ϱ_d , e così moltiplicando a sinistra per uno stesso elemento di G due elementi equivalenti modulo ϱ_s si ottengono due elementi ancora equivalenti mediante la ϱ_s . Sia ora $\varrho_d = \varrho_s = \varrho$, e siano $x \varrho x'$ e $y \varrho y'$. Allora sarà $xy \varrho x'y$ e $x'y \varrho x'y'$, da cui

$$xy \varrho x'y'$$

ossia ϱ_d ($= \varrho_s$) è compatibile.

Viceversa, supponiamo che ϱ_d sia compatibile. Allora $x \varrho_d y \iff xy^{-1} \varrho_d e$. Ma allora, per la compatibilità di ϱ_d , $y^{-1} \varrho_d x^{-1}$, cioè $y^{-1}(x^{-1})^{-1} = y^{-1}x \in H$ e quindi $x \varrho_d y \iff x \varrho_s y$ e $\varrho_d = \varrho_s$. \square

Riassumendo:

5.8.3 COROLLARIO. *Sia ϱ una relazione di equivalenza compatibile definita in un gruppo G . Allora il sottoinsieme $H = \{x \in G \mid x \varrho e\}$ è un sottogruppo di G e risulta $\varrho = \varrho_d = \varrho_s$ modulo H . Viceversa, se H è un sottogruppo di G tale che $\varrho_d = \varrho_s$, allora la $\varrho = \varrho_s = \varrho_d$ è una relazione compatibile.*

I sottogruppi H di un gruppo G per i quali la relazione ϱ_d (e quindi anche la ϱ_s) è compatibile, e per i quali quindi le classi di equivalenza rispetto alla ϱ_d (ossia i laterali destri modulo H) coincidono con le classi di equivalenza modulo la ϱ_s (ossia i laterali sinistri modulo H) hanno un nome particolare.

5.8.4 DEFINIZIONE. Un sottogruppo H di un gruppo G si dice *normale in G* se per ogni $x \in G$

$$Hx = xH.$$

Si scrive $H \leq G$. \square

Ad esempio, in S_3 il sottogruppo alterno è un sottogruppo normale, mentre il sottogruppo $\{\text{id}, (1, 2)\}$ non lo è.

In un gruppo abeliano ogni sottogruppo è normale in G , quindi tutte le relazioni di congruenza modulo un qualunque sottogruppo sono compatibili. Inoltre, ogni gruppo possiede sempre due sottogruppi normali (banali). L'intero gruppo e il sottogruppo ridotto al solo elemento neutro.

ATTENZIONE. Nella definizione di sottogruppo normale abbiamo specificato *normale in G* . Infatti un sottogruppo N può essere normale in un sottogruppo H ma non nell'intero gruppo G (si veda esercizio 5.8.8). Una volta data la nozione di sottogruppo normale in un gruppo G , il corollario 5.8.3 dice che tutte e sole le relazioni compatibili definite su di un gruppo G sono le relazioni di congruenza modulo un sottogruppo normale. Posto

$$\begin{aligned}\mathcal{R} &\stackrel{\text{def}}{=} \{\text{relazioni d'equivalenza definite su } G, \text{ compatibili con l'operazione di } G\} \\ \mathcal{N} &\stackrel{\text{def}}{=} \{\text{sottogruppi normali in } G\}\end{aligned}$$

la corrispondenza

$$\begin{aligned}\Psi : \mathcal{R} &\longrightarrow \mathcal{N} \\ \varrho &\longmapsto N = \{x \in G \mid x \varrho e\}\end{aligned}$$

è una corrispondenza *biunivoca* tra \mathcal{R} e \mathcal{N} , la cui inversa è la

$$\begin{aligned}\Psi^* : \mathcal{N} &\longrightarrow \mathcal{R} \\ N &\longmapsto \varrho = \varrho_d = \varrho_s\end{aligned}$$

dove $x \varrho y \iff xy^{-1} \in N \circ y^{-1}x \in N$.

La funzione svolta negli anelli dagli ideali è svolta nei gruppi dai sottogruppi normali. \square

Proseguiamo il paragrafo dando delle definizioni equivalenti di sottogruppo normale. Conviene ricordare un concetto che era stato introdotto nel caso di S_n , il concetto di elementi coniugati.

5.8.5 DEFINIZIONE. Sia G un gruppo. Due elementi x e y di G si dicono se esiste un elemento $g \in G$ tale che

$$y = gxg^{-1}. \quad \square$$

È facile vedere che tale relazione è una relazione di equivalenza. Se il gruppo G è abeliano ogni classe di elementi coniugati è costituita da un solo elemento. In un qualunque gruppo, la classe coniugata che contiene l'elemento neutro è costituita dall'elemento neutro solamente. Torneremo tra qualche paragrafo allo studio delle classi coniugate.

Dato un sottogruppo H di G indicheremo con xHx^{-1} l'insieme

$$xHx^{-1} \stackrel{\text{def}}{=} \{xhx^{-1} \mid h \in H\}.$$

È facile vedere che si tratta ancora di un sottogruppo di G , che prende il nome di *sottogruppo coniugato* di H , che in genere non coincide con H . Si indica anche con H^x . Esso coincide con H se e solo se H è un sottogruppo normale di G . Nella proposizione che segue raccogliamo una serie di definizioni equivalenti di sottogruppo normale, lasciando per esercizio la dimostrazione (cfr. esercizio 5.8.4).

5.8.6 PROPOSIZIONE. *Sia N un sottogruppo di un gruppo G . Allora le seguenti affermazioni sono equivalenti:*

- (a) N è normale in G ;
- (b) $N^x = N$ per ogni $x \in G$;
- (c) $xnx^{-1} \in N$ per ogni $x \in G$ e ogni $n \in N$;
- (d) N è unione di classi coniugate di G .

In virtù di queste affermazioni è quindi molto facile ad esempio trovare in S_4 tutti i sottogruppi normali: devono innanzitutto essere sottogruppi, e pertanto il loro ordine deve essere un divisore di 24, per il teorema di Lagrange, ma devono essere anche unioni di classi coniugate, di ciascuna delle quali conosciamo la cardinalità. Si invita lo studente a determinare esplicitamente tutti i sottogruppi normali di S_4 . (cfr. esercizio 5.8.5).

L'importanza delle relazioni compatibili è facilmente osservabile dalla seguente considerazione. Sia ϱ una relazione compatibile definita in G e sia N il corrispondente sottogruppo normale, ossia $N = \{x \in G \mid x \varrho e\}$. Nell'insieme quoziante G/ϱ , i cui elementi sono i laterali (destri e sinistri, dato che coincidono) modulo N , si può definire la seguente operazione:

$$Nx * Ny \stackrel{\text{def}}{=} Nxy.$$

Tale operazione, per il fatto che la relazione ϱ è compatibile, è ben posta, ossia non dipende dai particolari rappresentanti che si scelgono. Rispetto a tale operazione l'insieme quoziante G/ϱ diventa, come è facile provare, un gruppo, che prende il nome di *gruppo quoziante* modulo N . Esso si indica anche con G/N .

Quindi, dato un sottogruppo $N \trianglelefteq G$,

$$G/N \stackrel{\text{def}}{=} \{xN = Nx \mid x \in G\}$$

con

$$Nx = \{nx \mid n \in N\}.$$

Inoltre la proiezione canonica

$$\pi : G \longrightarrow G/N$$

$$g \longmapsto Ng$$

è un epimorfismo di gruppi, con nucleo N .

Visualizziamo quanto detto al modo seguente in un esempio concreto. Sia $G = S_3$ e sia $H = A_3$ il sottogruppo alterno. Le due relazioni ϱ_d e ϱ_s , individuate da H coincidono. Se riordiniamo gli elementi di S_3 in modo che i primi tre elementi siano $\text{id}, (1, 2, 3), (1, 3, 2)$ e gli ultimi tre siano $(1, 2), (1, 3), (2, 3)$, se cioè disponiamo gli elementi di S_3 a seconda della loro appartenenza ad una stessa classe laterale, la tavola moltiplicativa di S_3 diventa la seguente:

	id	$(1, 2, 3)$	$(1, 3, 2)$	$(1, 2)$	$(1, 3)$	$(2, 3)$
id	id	$(1, 2, 3)$	$(1, 3, 2)$	$(1, 2)$	$(1, 3)$	$(2, 3)$
$(1, 2, 3)$	$(1, 2, 3)$	$(1, 3, 2)$	id	$(1, 3)$	$(2, 3)$	$(1, 2)$
$(1, 3, 2)$	$(1, 3, 2)$	id	$(1, 2, 3)$	$(2, 3)$	$(1, 2)$	$(1, 3)$
$(1, 2)$	$(1, 2)$	$(2, 3)$	$(1, 3)$	id	$(1, 3, 2)$	$(1, 2, 3)$
$(1, 3)$	$(1, 3)$	$(1, 2)$	$(2, 3)$	$(1, 2, 3)$	id	$(1, 3, 2)$
$(2, 3)$	$(2, 3)$	$(1, 3)$	$(1, 2)$	$(1, 3, 2)$	$(1, 2, 3)$	id

Coloriamo ora con uno stesso colore gli elementi che appartengono ad uno stesso laterale. Allora la tavola precedente diventa

	id	$(1, 2, 3)$	$(1, 3, 2)$	$(1, 2)$	$(1, 3)$	$(2, 3)$
id	id	$(1, 2, 3)$	$(1, 3, 2)$	$(1, 2)$	$(1, 3)$	$(2, 3)$
$(1, 2, 3)$	$(1, 2, 3)$	$(1, 3, 2)$	id	$(1, 3)$	$(2, 3)$	$(1, 2)$
$(1, 3, 2)$	$(1, 3, 2)$	id	$(1, 2, 3)$	$(2, 3)$	$(1, 2)$	$(1, 3)$
$(1, 2)$	$(1, 2)$	$(2, 3)$	$(1, 3)$	id	$(1, 3, 2)$	$(1, 2, 3)$
$(1, 3)$	$(1, 3)$	$(1, 2)$	$(2, 3)$	$(1, 2, 3)$	id	$(1, 3, 2)$
$(2, 3)$	$(2, 3)$	$(1, 3)$	$(1, 2)$	$(1, 3, 2)$	$(1, 2, 3)$	id

Vediamo che i colori si dispongono in forma di quadrato, ciascuno in corrispondenza ai colori che si trovano sulla riga superiore e sulla colonna di sinistra. Dimenticando gli elementi che si trovano sotto il colore, e chiamando B (bianco) e N (nero) i due laterali, la tavola precedente diventa

	B	N
B	B	N
N	N	B

che corrisponde alla tavola moltiplicativa di un gruppo (di ordine due).

Vediamo se si può fare la stessa cosa partendo dal gruppo $H = \{\text{id}, (1, 2)\}$ di S_3 . Disponendo gli elementi di S_3 a seconda della loro appartenenza alle tre classi laterali *destre* (ora dobbiamo specificare se destro o sinistro, perché non coincidono) si ottiene la seguente tavola di moltiplicazione

.	id	(1, 2)	(1, 3)	(1, 3, 2)	(2, 3)	(1, 2, 3)
id	id	(1, 2)	(1, 3)	(1, 3, 2)	(2, 3)	(1, 2, 3)
(1, 2)	(1, 2)	id	(1, 3, 2)	(1, 3)	(1, 2, 3)	(2, 3)
(1, 3)	(1, 3)	(1, 2, 3)	id	(2, 3)	(1, 3, 2)	(1, 2)
(1, 3, 2)	(1, 3, 2)	(2, 3)	(1, 2)	(1, 2, 3)	(1, 3)	id
(2, 3)	(2, 3)	(1, 3, 2)	(1, 2, 3)	(1, 2)	id	(1, 3)
(1, 2, 3)	(1, 2, 3)	(1, 3)	(2, 3)	id	(1, 2)	(1, 3, 2)

Se coloriamo con uno stesso colore gli elementi appartenenti ad una stessa classe, si vede che questi colori non si dispongono secondo quadrati, ma secondo rettangoli (ossia quelli che dovrebbero essere dei quadrati si "spezzano" in due parti rettangolari):

.	id	(1, 2)	(1, 3)	(1, 3, 2)	(2, 3)	(1, 2, 3)
id	id	(1, 2)	(1, 3)	(1, 3, 2)	(2, 3)	(1, 2, 3)
(1, 2)	(1, 2)	id	(1, 3, 2)	(1, 3)	(1, 2, 3)	(2, 3)
(1, 3)	(1, 3)	(1, 2, 3)	id	(2, 3)	(1, 3, 2)	(1, 2)
(1, 3, 2)	(1, 3, 2)	(2, 3)	(1, 2)	(1, 2, 3)	(1, 3)	id
(2, 3)	(2, 3)	(1, 3, 2)	(1, 2, 3)	(1, 2)	id	(1, 3)
(1, 2, 3)	(1, 2, 3)	(1, 3)	(2, 3)	id	(1, 2)	(1, 3, 2)

Indicati i colori con le lettere B, N ed R, la situazione che si presenta è la seguente:

	B	B	N	N	R	R
B	B	B	N	N	R	R
B	B	B	N	N	R	R
N	N	R	B	R	N	B
N	N	R	B	R	N	B
R	R	N	R	B	B	N
R	R	N	R	B	B	N

Non si riesce pertanto a definire un'operazione nel quoziente (ossia tra i *colori* B, N ed R). Il motivo è che la relazione ϱ_d in questo caso non coincide con la ϱ_s e quindi non è compatibile.



ESERCIZI.

1. Determinare il gruppo quoziente di S_3 rispetto al suo unico sottogruppo normale non banale.
2. Verificare che in $(GL_n(\mathbb{R}), \cdot)$ il sottogruppo $(SL_n(\mathbb{R}), \cdot)$ è un sottogruppo normale. Si studi il quoziente. A quale gruppo noto è isomorfo?
3. Verificare che il sottogruppo $(SO_2(\mathbb{R}), \cdot)$ costituito dalle matrici ortogonali con determinante uguale a 1 è un sottogruppo normale nel gruppo $(O_2(\mathbb{R}), \cdot)$ delle matrici ortogonali. Si studi il quoziente. Quanti elementi ha?
4. Si dimostrino tutti i punti della proposizione 5.8.6.
5. Tenendo conto della caratterizzazione dei sottogruppi normali N di un gruppo G, e della struttura delle classi coniugate nei gruppi simmetrici, si trovino tutti i sottogruppi normali di S_4 .
6. Sfruttando la definizione di sottogruppo normale, si dimostri che l'operazione

$$Nx * Ny = Nx y$$

è ben posta.

7. Si provi che il sottogruppo alterno A_n è normale in S_n e si studi il quoziente S_n/A_n .
8. Siano H e K due sottogruppi di un gruppo G, e sia $H \trianglelefteq K$. Si provi con un esempio che ciò non comporta che sia $H \trianglelefteq G$.
9. Sia $H \leq G$. Si dice *normalizzante* di H in G l'insieme $N_G(H)$ dove

$$N_G(H) \stackrel{\text{def}}{=} \{x \in G \mid H^x = H\}.$$

Si provi che $N_G(H)$ è un sottogruppo di G e che $H \trianglelefteq N_G(H)$. Inoltre si provi che $H \leq G$ se e solo se $N_G(H)$ coincide con tutto G.



ESERCIZI DI PROGRAMMAZIONE.

1. Si scriva un programma che decida se un sottogruppo di un gruppo finito G è un sottogruppo normale in G.



CONTROLLO.

1. Che legame c'è tra le nozioni di relazione compatibile in un gruppo e di sottogruppo normale?
2. Il gruppo quoziente modulo un sottogruppo normale è ...

5.9. Il teorema fondamentale di omomorfismo tra gruppi e applicazioni

Nel paragrafo precedente abbiamo introdotto il concetto di sottogruppo normale in un gruppo G e di gruppo quoziante (modulo un sottogruppo normale). Dato un omomorfismo φ tra due gruppi G e G' , è facile vedere che il nucleo $\text{Ker } \varphi$ è un sottogruppo normale di G . Ha senso allora considerare il gruppo quoziante $G/\text{Ker } \varphi$. Sussiste il seguente importante teorema.

5.9.1 TEOREMA FONDAMENTALE DI OMOMORFISMO TRA GRUPPI. *Siano G e G' due gruppi e sia φ un omomorfismo tra di essi. Allora esiste ed è unico un isomorfismo*

$$\varphi^* : G/\text{Ker } \varphi \simeq \text{Im } \varphi$$

tale che

$$\varphi = \varphi^* \circ \pi$$

π essendo la proiezione canonica di G sul quoziante $G/\text{Ker } \varphi$.

La situazione è illustrata dalla figura 5.12.

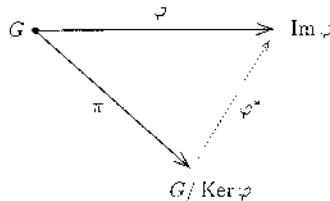


FIGURA 5.12

Dimostrazione. Definiamo un'applicazione φ^* da $G/\text{Ker } \varphi$ a $\text{Im } \varphi$ al modo seguente:

$$\varphi^*(\text{Ker } \varphi g) \stackrel{\text{def}}{=} \varphi(g) \quad \forall g \in G.$$

Vale ovviamente la $\varphi = \varphi^* \circ \pi$. Occorre allora provare i seguenti punti:

- (1) φ^* è ben posta, ossia $\text{Ker } \varphi g_1 = \text{Ker } \varphi g_2 \implies \varphi(g_1) = \varphi(g_2)$.
- (2) φ^* è biiettiva.
- (3) φ^* è un omomorfismo di gruppi.

(1) $\text{Ker } \varphi g_1 = \text{Ker } \varphi g_2 \iff g_1 g_2^{-1} \in \text{Ker } \varphi \iff \varphi(g_1 g_2^{-1}) = e_{G'} \iff \varphi(g_1) = \varphi(g_2)$. Le doppie implicazioni provano sia che la φ^* è ben posta, sia che è iniettiva.

(2) Resta da provare solamente la suriettività. Dato comunque un elemento di $\text{Im } \varphi$, esso sarà del tipo $\varphi(g)$ per qualche $g \in G$. Ma allora $\varphi(g)$ proverà mediante la φ^* dalla classe $\text{Ker } \varphi g$, e quindi la φ^* è suriettiva.

$$\begin{aligned} (3) \quad \varphi^*(\text{Ker } \varphi g_1 * \text{Ker } \varphi g_2) &= \varphi^*(\text{Ker } \varphi g_1 g_2) = \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) \\ &= \varphi^*(\text{Ker } \varphi g_1) \varphi^*(\text{Ker } \varphi g_2). \quad \square \end{aligned}$$

L'identificazione di $\text{Im } \varphi$ con il quoziente $G/\text{Ker } \varphi$ sostanzialmente ci dice che tutti gli epimorfismi da un gruppo G si possono identificare con gli omomorfismi canonici sul quoziente.

Questo teorema ha diverse applicazioni. La prima applicazione è la classificazione dei gruppi ciclici.

5.9.2 COROLARIO. *Sia (G, \cdot) un gruppo ciclico. Allora, se G è infinito, G è isomorfo a $(\mathbb{Z}, +)$; se G è finito e ha ordine n , allora $G \cong (\mathbb{Z}_n, +)$.*

Dimostrazione. Sia $G = \langle g \rangle$. Si consideri l'applicazione

$$\begin{aligned} \varphi : (\mathbb{Z}, +) &\longrightarrow G = \langle g \rangle \\ k &\longmapsto g^k. \end{aligned}$$

Si tratta di un omomorfismo (suriettivo). Se $G = \langle g \rangle$ è infinito, allora se $h \neq k$ segue che $g^h \neq g^k$. Questo ci dice che la φ è iniettiva, per cui $\text{Ker } \varphi = \{0\}$. Per il teorema fondamentale di omomorfismo tra gruppi risulta

$$G \cong \mathbb{Z}.$$

Se invece $G = \langle g \rangle$ è ciclico di ordine n , allora $\text{Ker } \varphi = n\mathbb{Z}$, da cui

$$G \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n. \quad \square$$

5.9.3 DEFINIZIONE. Sia G un gruppo. Un *automorfismo* di G è un isomorfismo di G in sé. \square

Ad esempio, se G è abeliano, l'applicazione φ

$$\begin{aligned} \varphi : G &\longrightarrow G \\ x &\longmapsto x^{-1} \end{aligned}$$

è un automorfismo, che è diverso dall'automorfismo identico se esiste in G un elemento x che non coincide con il suo inverso.

Indicato con $\text{Aut}(G)$ l'insieme di tutti gli automorfismi del gruppo G , è facile vedere che $(\text{Aut}(G), \circ)$ è un gruppo, che è quindi un sottogruppo del gruppo $(S(G), \circ)$ di tutte le corrispondenze biunivoche di G in sé.

Tra gli automorfismi di un gruppo G c'è una classe importante di automorfismi, detti automorfismi interni.

5.9.4 DEFINIZIONE. Sia G un gruppo. Dicesi *automorfismo interno* di G ogni automorfismo T_g definito al modo seguente:

$$\begin{aligned} T_g : G &\longrightarrow G \\ x &\longmapsto gxg^{-1}. \end{aligned}$$

Si provi che un automorfismo interno è effettivamente un automorfismo. \square

L'insieme $\mathcal{I}(G)$ di tutti gli automorfismi interni di un gruppo G costituisce un *sottogruppo normale* di $\text{Aut}(G)$ (cfr. esercizio 5.9.2).

Abbiamo già visto (cfr. definizione 5.1.9) che il *centro* di G , che si indica con $Z(G)$, è definito dalla

$$Z(G) \stackrel{\text{def}}{=} \{g \in G \mid gx = xy \ \forall x \in G\}.$$

Il centro è un sottogruppo normale in G (cfr. esercizio 5.9.3).

È chiaro che, se il gruppo G è abeliano, il centro coincide con l'intero gruppo e $\mathcal{I}(G)$ si riduce al solo automorfismo identico. In generale, $\mathcal{I}(G)$ è tanto più piccolo, quanto più grande è il centro di G , nel senso precisato dal corollario che segue.

5.9.5 COROLLARIO. *Sia G un gruppo. Se $\mathcal{I}(G)$ è il gruppo degli automorfismi interni di G e $Z(G)$ è il centro di G , allora si ha*

$$\mathcal{I}(G) \cong G/Z(G).$$

Dimostrazione. Definiamo la seguente applicazione:

$$\begin{aligned} \psi : G &\longrightarrow \text{Aut}(G) \\ g &\longmapsto T_g. \end{aligned}$$

Si tratta di un omomorfismo, il cui nucleo è il centro di G (si dimostri) e la cui immagine è $\mathcal{I}(G)$. Quindi il risultato segue dal teorema fondamentale di omomorfismo. \square

Diamo un'ultima applicazione del teorema fondamentale di omomorfismo tra gruppi. Supponiamo di voler studiare un gruppo quoziante G/N . Un modo per affrontare il problema è quello di costruire un omomorfismo φ di G in un gruppo noto, il cui nucleo sia proprio N . In questo modo, potremo dire che G/N è isomorfo all'immagine di φ , che sta dentro il gruppo noto.

Ad esempio, supponiamo di volere studiare il quoziante $\text{GL}_n(\mathbb{R})/\text{SL}_n(\mathbb{R})$. Definiamo la seguente applicazione:

$$\begin{aligned} \psi : \text{GL}_n(\mathbb{R}) &\longrightarrow (\mathbb{R} \setminus \{0\}, \cdot) \\ A &\longmapsto \det A; \end{aligned}$$

ψ è un omomorfismo suriettivo, il cui nucleo è proprio $SL_n(\mathbb{R})$. Quindi

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R} \setminus \{0\}.$$

ESERCIZI.

1. Si provi che se G è ciclico infinito, allora $\text{Aut}(G)$ è isomorfo a \mathbb{Z}_2 , se G è ciclico di ordine n , allora $\text{Aut}(G)$ è isomorfo a $(U(\mathbb{Z}_n), \cdot)$, il gruppo degli elementi invertibili di \mathbb{Z}_n .
2. Si provi che $I(G) \trianglelefteq \text{Aut}(G)$.
3. Si provi che il centro di un gruppo è un sottogruppo normale in G .
4. Si provi che un gruppo privo di sottogruppi propri è necessariamente ciclico di ordine un numero primo.
5. Si determini il gruppo degli automorfismi di \mathbb{Z}_9 e si dica se tale gruppo di automorfismi è ciclico o no.
6. Sia G il gruppo abeliano additivo costituito da tutte le funzioni continue definite in $[0, 1]$ e a valori in \mathbb{R} . Si consideri il sottoinsieme

$$N = \{f \in G \mid f(1/3) = 0\}.$$

Si provi che $N \trianglelefteq G$ e si studi il quoziente, dicendo a quale gruppo noto è isomorfo.

7. In $GL_2(\mathbb{C})$ si consideri il sottogruppo H generato dalle due matrici $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ e $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Si determini l'ordine di tale sottogruppo, scrivendo esplicitamente tutti i suoi elementi e i rispettivi periodi. Si dica se tale sottogruppo è ciclico e/o abeliano. Indicato con g l'unico elemento di periodo 2, si dica se il sottogruppo da esso generato è normale in H e se è normale in $GL_2(\mathbb{C})$.
8. Si determinino tutti gli omomorfismi del gruppo simmetrico S_3 nel gruppo $(\mathbb{Z}_{15}, +)$.
9. Si provi che la corrispondenza in un gruppo che associa ad ogni elemento di un gruppo G il suo inverso è un automorfismo se e solo se G è abeliano.
10. Sia H il sottoinsieme di S_4

$$H = \{\text{id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}.$$

Si mostri che H è un sottogruppo normale di S_4 . Si studi il quoziente S_4/H .

11. Si determini il gruppo degli automorfismi interni del gruppo A_4 (sottogruppo altenro di S_4).
12. Si determini il gruppo degli automorfismi del gruppo \mathbb{Z}_{15} . Si dica se si tratta di un gruppo ciclico. Quale degli automorfismi è interno?
13. Sia D_4 il gruppo delle simmetrie di un quadrato, e sia N l'unico sottogruppo normale di ordine 2 di D_4 . Si studi il quoziente D_4/N .
14. Sia G un gruppo. Si definisce *sottogruppo derivato* di G , e si indica con G' , il sottogruppo di G generato dagli elementi $xyx^{-1}y^{-1}$, al variare di x e y in G .

(a) Si provi che $G' \trianglelefteq G$.

(b) Si provi che $G' = \{e\} \iff G$ è abeliano.

15. Nel gruppo $(\mathbb{R}^2, +) = \{(a, b) \mid a, b \in \mathbb{R}\}$ si consideri il sottogruppo $S = \{(a, 3a) \mid a \in \mathbb{R}\}$. Si studi il quoziente \mathbb{R}^2/S .



CONTROLLO.

- Il teorema fondamentale di omomorfismo tra gruppi: enunciato e applicazioni.
- Automorfismi di un gruppo e automorfismi interni.
- È vero che tutti i gruppi ciclici sono abeliani? E che tutti i gruppi abeliani sono ciclici? Quanti gruppi ciclici (non isomorfi) di fissato ordine n ci sono? E gruppi ciclici infiniti?

5.10. I teoremi di isomorfismo

Siano H e K due sottogruppi di un gruppo G . Poniamo

$$\overline{HK} \stackrel{\text{def}}{=} \{hk \mid h \in H, k \in K\}.$$

Ad esempio, se $G = S_3$, $H = \{\text{id}, (1, 2)\}$, $K = \{\text{id}, (1, 3)\}$, allora $HK = \{\text{id}, (1, 3), (1, 2), (1, 3, 2)\}$. Tale sottoinsieme chiaramente non è un sottogruppo di S_3 . Si noti anche che $KH \neq HK$ (si verifichi). Sussiste la seguente proposizione.

5.10.1 PROPOSIZIONE. *Sia G un gruppo e siano N ed H due sottogruppi di G tali che $N \trianglelefteq G$. Allora $NH = HN$ è un sottogruppo di G .*

Dimostrazione. Essendo N normale in G , risulta $NH = HN$. Siano ora $x = nh$ e $y = n'h'$ due elementi in NH : proveremo che xy^{-1} appartiene a NH . Risulta

$$xy^{-1} = nhn'^{-1}n'^{-1} \in nHN = nNH \subseteq NH$$

che è quanto volevamo provare. \square

Si osservi che in realtà nella dimostrazione della proposizione non abbiamo utilizzato completamente il fatto che N fosse normale. Basta l'ipotesi che i due sottogruppi N e H siano tali che $NH = HN$ (cfr. esercizio 5.1.4).

Se il gruppo G è abeliano, il prodotto HK di due suoi sottogruppi qualsiasi è un sottogruppo.

Se H e K sono due sottogruppi di un gruppo G , tali che $HK = KH$, abbiamo appena visto che HK è un sottogruppo. Ma allora esso coincide con il sottogruppo generato da H e K , ossia

$$\langle H, K \rangle = HK.$$

Ciò premesso, lasciamo come esercizio la dimostrazione della seguente proposizione.

5.10.2 PROPOSIZIONE. *Sia φ un omomorfismo tra due gruppi G e G' . Allora*

$H \leq G \implies \varphi(H)$ è un sottogruppo di G' contenuto in $\text{Im } \varphi$;

$K' \leq G' \implies \varphi^{-1}(K')$ è un sottogruppo di G contenente $\text{Ker } \varphi$.

5.10.3 COROLLARIO. *Sia G un gruppo, N un sottogruppo normale in G e $\pi : G \rightarrow G/N$ la proiezione canonica. Allora*

- (a) *se H è un sottogruppo di G , $\pi(H) = HN/N$ è un sottogruppo di G/N ;*
- (b) *se H' è un sottogruppo di G/N , $\pi^{-1}(H')$ è un sottogruppo di G contenente N .*

Dimostrazione. Basta osservare che in questo caso l'omomorfismo π è suriettivo, quindi $\pi(G) = \text{Im } \pi = G/N$. \square

5.10.4 PROPOSIZIONE. *Sia G un gruppo e sia $N \trianglelefteq G$. Sia π la proiezione canonica sul quoziente:*

$$\pi : G \longrightarrow G/N .$$

Allora esiste una corrispondenza biunivoca ψ tra i sottogruppi H di G contenenti $N = \text{Ker } \pi$ e i sottogruppi del quoziente G/N .

Dimostrazione. Definiamo ψ al modo seguente:

$$\psi : H \longrightarrow \pi(H) .$$

Proveremo che ψ è invertibile mostrando che

- (i) $\pi^{-1}(\pi(H)) = H \quad \forall H \leq G, H \supseteq N$
- (ii) $\pi(\pi^{-1}(K)) = K \quad \forall K \leq G/N .$

Risulta sempre $H \subseteq \pi^{-1}(\pi(H))$. Sia allora $x \in \pi^{-1}(\pi(H))$; ciò significa che $\pi(x) \in \pi(H)$, ossia $\pi(x) = \pi(h)$ per qualche $h \in H$. Ma allora x e h sono in relazione modulo N , cioè $x \in hN$. Ma $N \subseteq H$, da cui $x \in H$. La (ii) vale essendo π suriettiva. \square

Sussistono i seguenti due teoremi di isomorfismo.

5.10.5 PRIMO TEOREMA DI ISOMORFISMO. *Sia G un gruppo, N un sottogruppo normale in G e π la proiezione canonica. Sia H un qualunque sottogruppo di G . Allora*

- (a) $\pi^{-1}(\pi(H)) = HN$;
- (b) $N \cap H$ è normale in H ;
- (c) $H/(N \cap H) \cong HN/N$.

Dimostrazione. Sia $H \leq G$. Allora, essendo

$$\pi(nh) = \pi(n)\pi(h) = \pi(h) \in \pi(H),$$

si ha

$$HN \subseteq \pi^{-1}(\pi(H)).$$

Vale anche l'altra inclusione $\pi^{-1}(\pi(H)) \subseteq HN$, dato che, se $x \in \pi^{-1}(\pi(H))$, allora $\pi(x) \in \pi(H)$, da cui $\pi(x) = \pi(h)$, ossia $x \in hN$.

Infine, $N \cap H \trianglelefteq H$: infatti (cfr. figura 5.13), indicata con $\pi|_H$ la restrizione ad H della proiezione canonica $\pi : G \rightarrow G/N$ risulta

$$\text{Im } \pi|_H = HN/N, \quad \text{Ker } \pi|_H = H \cap N.$$

Queste relazioni ci dicono al tempo stesso che $H \cap N$ è normale in H , essendo nucleo di un omomorfismo e

$$HN/N \cong H/H \cap N. \quad \square$$

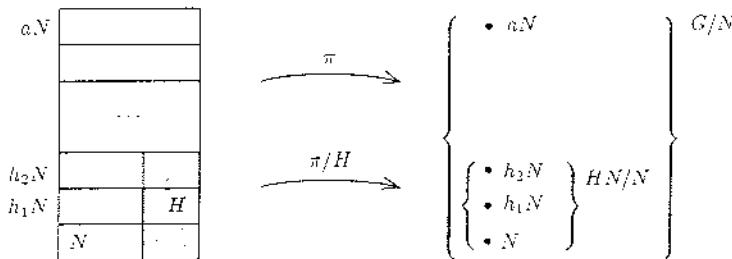


FIGURA 5.13

5.10.6 SECONDO TEOREMA DI ISOMORFISMO. Sia G un gruppo e sia $N \trianglelefteq G$. Se H è un sottogruppo di G contenente N , allora

$$H \trianglelefteq G \iff H/N \trianglelefteq G/N.$$

Inoltre risulta

$$G/H \cong (G/N)/(H/N).$$

Dimostrazione. Sia $H \trianglelefteq G$, $H \supseteq N$. Per far vedere che H/N è normale in G/N mostriremo che è chiuso rispetto alla coniugazione: infatti per ogni $gN \in G/N$ e ogni $hN \in H/N$

$$gN \cdot hN \cdot (gN)^{-1} = ghg^{-1}N \in H/N.$$

Viceversa, sia ora $H/N \leq G/N$. Consideriamo le seguenti composizioni di epimorfismi:

$$G \xrightarrow{\pi_1} G/N \xrightarrow{\pi_2} (G/N)/(H/N)$$

dove π_1 e π_2 sono le proiezioni canoniche. La composizione $\varrho = \pi_2 \circ \pi_1$ è un epimorfismo di nucleo H , quindi $H \trianglelefteq G$. Per il teorema fondamentale di omomorfismo

$$(G/N)/(H/N) \cong G/H . \quad \square$$

5.10.7 ESEMPIO. Sia $G = \mathbb{Z}_{24}$, $H = \langle \bar{2} \rangle$ e $N = \langle \bar{6} \rangle$. Risulta

$$G/N = \{N, \bar{1} + N, \bar{2} + N, \bar{3} + N, \bar{4} + N, \bar{5} + N\} .$$

Dato che

$$H = \{0, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}, \bar{12}, \bar{14}, \bar{16}, \bar{18}, \bar{20}, \bar{22}\}$$

si ha

$$H/N = \{N, \bar{2} + N, \bar{4} + N\} .$$

$(G/N)/(H/N)$ è isomorfo a \mathbb{Z}_2 , e così pure $G/H = \mathbb{Z}_{24}/2\mathbb{Z}_{24}$. \square

ESERCIZI.

1. Sia $G = \mathrm{GL}_2(\mathbb{R})$ e siano $H = \langle \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rangle$ e $K = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$. Si studino H e K e si verifichi che HK non è un sottogruppo di $\mathrm{GL}_2(\mathbb{R})$.
2. Sia \mathbb{Q}^* il gruppo moltiplicativo dei razionali, sia $N = \{1, -1\}$ e sia H il sottogruppo di \mathbb{Q}^* generato da $1/3$. Si studi HN/N e si verifichi il primo teorema di isomorfismo.



CONTROLLO.

1. Come sono legati i sottogruppi di un quoziente G/N ai sottogruppi di G ?
2. Se H è un sottogruppo di G , $N \trianglelefteq G$ e π è la proiezione canonica di G su G/N , la controimmagine di $\pi(H)$ è data da ...

5.11. L'azione di un gruppo su un insieme: orbite e stabilizzatori

In questo paragrafo vedremo i gruppi "entrare in azione", nel senso che andiamo a spiegare. Sia G un gruppo e sia X un insieme.

5.11.1 DEFINIZIONE. Un'azione del gruppo G sull'insieme X è un'applicazione

$$\ast : G \times X \longrightarrow X$$

$$(g, x) \longmapsto g \ast x$$

tale che

- (i) $e \ast x = x$ (e elemento neutro di G) per ogni $x \in X$;

(ii) $(g_1 g_2) * x = g_1 * (g_2 * x)$ per ogni $x \in X$ e ogni $g_1, g_2 \in G$.

Si noti che ogni $g \in G$ determina in questo modo una corrispondenza bitunivoca ψ_g di X in sé data da $\psi_g(x) = g * x$, la cui inversa è la $\psi_{g^{-1}}$. Le condizioni (i) e (ii) dicono che la corrispondenza ψ da G al gruppo $S(X)$ di tutte le corrispondenze biunivoche di X in sé data da

$$(5.11.1) \quad \begin{aligned} \psi : G &\longrightarrow S(X) \\ g &\longmapsto \psi_g \end{aligned}$$

è un *omomorfismo di gruppi*. Si dice anche che il gruppo G *agisce* sull'insieme X (come gruppo di trasformazioni), e l'insieme X prende il nome di G -insieme. \square

Per ogni $g \in G$ e ogni $x \in X$, indicheremo $g * x$ semplicemente con gx : si noti tuttavia che questa notazione *non* ha il significato di una *moltiplicazione* tra elementi! In questa nuova forma "compatta" le (i) e (ii) si riscrivono al modo seguente:

$$\begin{aligned} e_G x &= x & \forall x \in X \\ (g_1 g_2)x &= g_1(g_2x) & \forall x \in X, \forall g_1, g_2 \in G. \end{aligned}$$

Può essere utile leggere l'equazione $y = gx$ dicendo che l'elemento $g \in G$ *muove* l'elemento $x \in X$ all'elemento $y \in X$, o, equivalentemente, che x è *messo in y* da g .

Dalla (5.11.1) risulta che gli elementi di G si possono pensare come *permutazioni* o *trasformazioni* dell'insieme X .

Dato un G -insieme X , resta definita su X la seguente relazione:

$$x \sim y \iff \exists g \in G \mid y = gx.$$

Si tratta di una relazione di equivalenza. Le classi di equivalenza prendono il nome di *orbita*. L'orbita di un elemento $x \in X$ si indica con $\mathcal{O}(x)$:

$$\boxed{\mathcal{O}(x) \stackrel{\text{def}}{=} \{y \in X \mid y = gx \text{ per qualche } g \in G\}}.$$

In termini di movimenti, l'orbita di un elemento $x \in X$ è costituita da tutti gli $y \in X$ a cui l'elemento x può essere mosso mediante elementi di G . Si può anche dire che nell'orbita di x ci sono tutti gli elementi che non si possono distinguere da x sotto l'azione di G .

5.11.2 ESEMPI.

- (a) Ogni gruppo G *agisce su se stesso*, cioè su $X = G$ per *coniugazione*. In questo caso

$$g * x \stackrel{\text{def}}{=} gxg^{-1}.$$

L'orbita di un elemento $x \in X (= G)$ è costituita da tutti gli $y \in G (= X)$ tali che $y = gxg^{-1}$ per qualche $g \in G$. Le orbite sono quindi le *classi di coniugio*.

Da questo esempio appare chiaro come la scrittura "compatta" gx in luogo di $g * x$ stia in questo caso a rappresentare non il "prodotto" gx in G , (che pure questa volta avrebbe senso), bensì l'elemento $g x g^{-1}$.

- (b) Il gruppo simmetrico S_n agisce in modo naturale (per definizione stessa di S_n) sull'insieme $X = \{1, 2, \dots, n\}$:

$$\sigma * x = \sigma(x) = \text{il trasformato di } x \text{ mediante la } \sigma.$$

L'orbita di un elemento x di X è costituita da tutti gli $y \in X$ per i quali esista una $\sigma \in S_n$ tale che $y = \sigma(x)$. È chiaro quindi che esiste un'unica orbita rispetto a questa relazione di equivalenza, ossia, come anche si dice, S_n opera transitivamente su X . Infatti, dato un elemento $x \in X$, un qualunque $y \in X$ è in relazione ad x , perché esiste certamente una permutazione che manda x in y .

- (c) Sia $\sigma = (4, 5)(1, 3, 6)(2, 7, 8) \in S_8$ e sia $G = \langle \sigma \rangle$. Allora le orbite in cui viene ripartito $X = \{1, 2, \dots, 8\}$ secondo l'azione naturale di G su X sono tre: $\{4, 5\}$, $\{1, 3, 6\}$ e $\{2, 7, 8\}$. In generale, se σ è una permutazione di S_n , posto $G = \langle \sigma \rangle$, e $X = \{1, 2, \dots, n\}$, il G -insieme X secondo l'azione naturale di S_n viene ripartito in orbite che corrispondono ai cicli della permutazione σ .
- (d) Sia $G = \mathrm{GL}_n(\mathbb{R})$ il gruppo di tutte le matrici invertibili ad elementi reali. Esso agisce su $X = \mathbb{R}^n$ mediante la seguente azione naturale:

$$A * \mathbf{x} \stackrel{\text{def}}{=} A\mathbf{x}$$

dove $\mathbf{x} = (x_1, x_2, \dots, x_n)^T$ e $A\mathbf{x}$ è l'ordinario prodotto tra matrici. Quante sono le orbite?

- (e) Sia H un sottogruppo di un gruppo G . Definiamo la seguente azione del gruppo H su G :

$$h * g \stackrel{\text{def}}{=} hg \quad (\text{moltiplicazione in } G) \quad \forall h \in H, \forall g \in G.$$

Questa volta l'azione è l'ordinaria moltiplicazione in G . Le orbite sono i laterali destri modulo il sottogruppo H .

Si tratta effettivamente di un'azione:

$$(h_1 h_2)g = h_1(h_2 g) \quad \forall g \in G, \forall h_1, h_2 \in H.$$

- (f) La seguente:

$$h * g \stackrel{\text{def}}{=} gh$$

*non è un'azione, perché $(h_1 h_2) * g = gh_1 h_2 \neq h_1 * (h_2 * g) = gh_2 h_1$. Occorre modificarla al modo seguente:*

$$h * g \stackrel{\text{def}}{=} gh^{-1}.$$

Le orbite sono i *lateralini sinistri*.

- (g) Il gruppo additivo \mathbb{Z} agisce sulla retta reale $X = \mathbb{R}$ per traslazione:

$$n * r \stackrel{\text{def}}{=} n + r \quad \forall n \in \mathbb{Z}, \forall r \in \mathbb{R}.$$

L'orbita di un elemento r in \mathbb{R} è costituita da tutti i *traslati* di r mediante interi, cioè $\mathcal{O}(r) = \{r + n \mid n \in \mathbb{Z}\}$.

- (h) Il gruppo ortogonale $O_n(\mathbb{R})$ agisce su \mathbb{R}^n in modo naturale, e le orbite sono circonference. \square

Se G è un gruppo che agisce su un insieme X , un problema importante che si presenta è di calcolare la cardinalità di ogni orbita, e, se il gruppo è finito e agisce su di un insieme finito, determinare il numero di orbite. È quanto faremo in questo paragrafo. Per fare ciò occorrono alcune definizioni e risultati validi in generale.

5.11.3 DEFINIZIONE. Sia G un gruppo che agisce su di un insieme X . Si definisce *stabilizzatore* St_x di un elemento $x \in X$ l'insieme degli elementi $y \in G$ che fissano x , ossia

$$St_x \stackrel{\text{def}}{=} \{y \in G \mid yx = x\}. \quad \square$$

5.11.4 PROPOSIZIONE. Il sottoinsieme St_x di G è un sottogruppo di G . Inoltre risulta $St_{gx} = g St_x g^{-1}$, ossia gli stabilizzatori di elementi che si trovano nella stessa orbita sono coniugati.

Dimostrazione. Dimostriamo solo la seconda parte, lasciando per esercizio la verifica che St_x è un sottogruppo:

$$y \in St_{gx} \iff y(gx) = gx \iff g^{-1}yg \in St_x \iff y \in g St_x g^{-1}.$$

Quindi

$$St_{gx} = g St_x g^{-1}. \quad \square$$

Lo stabilizzatore di un elemento x prende anche il nome di *sottogruppo di isotropia* di x .

Lo stabilizzatore di un elemento $x \in \mathbb{R}$ dell'esempio 5.11.2 (g) è il sottogruppo di \mathbb{Z} ridotto al solo zero.

Lo stabilizzatore St_x di un elemento $x \in X$ nel caso dell'esempio 5.11.2 (a) (azione di coniugio) è dato da

$$St_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}.$$

Esso coincide con l'insieme degli elementi $g \in G$ che *commutano con x* e prende il nome di *centralizzante dell'elemento x* . Si indica con $C(x)$.

Osserviamo che, se lo stabilizzatore di un elemento $x \in X$ è molto grande, significa che l'elemento x è fissato da molti elementi di G , quindi ha poche possibilità di "essere mosso", ossia la sua orbita è piccola. La proposizione che segue precisa la relazione che c'è tra la cardinalità dell'orbita e l'indice dello stabilizzatore.

5.11.5 PROPOSIZIONE. *Sia X un G -insieme. La cardinalità dell'orbita $\mathcal{O}(x)$ dell'elemento $x \in X$ uguaglia l'indice di St_x in G .*

Dimostrazione. Occorre stabilire una corrispondenza biunivoca tra $\mathcal{O}(x)$ e

$$\mathcal{S} \stackrel{\text{def}}{=} \{\text{laterali destri di } \text{St}_x\} = \{\text{St}_x g \mid g \in G\}.$$

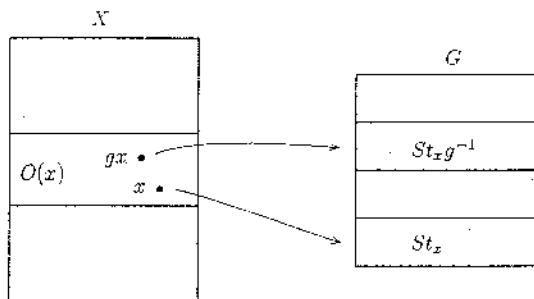


FIGURA 5.14

Basta porre

$$\begin{aligned} \mathcal{O}(x) &\longrightarrow \mathcal{S} \\ gx &\longmapsto \text{St}_x g^{-1}. \end{aligned}$$

Si tratta di un'applicazione *ben posta* e *iniettiva*. Infatti

$$\begin{aligned} g_1 x = g_2 x &\iff g_2^{-1} g_1 x = x \iff g_2^{-1} g_1 \in \text{St}_x \\ &\iff \text{St}_x g_1^{-1} = \text{St}_x g_2^{-1}. \end{aligned}$$

Inoltre è *suriettiva*, perché dato comunque un laterale destro $\text{St}_x g$, esso proviene dall'elemento $g^{-1}x \in \mathcal{O}(x)$. \square

5.11.6 COROLLARIO. *La cardinalità della classe di coniugio di un elemento x di un gruppo G uguaglia l'indice del centralizzante $C(x)$.*

5.11.7 COROLLARIO. *Se G è un gruppo finito che opera su di un insieme X , per ogni $x \in X$ risulta*

$$|\mathcal{O}(x)| \cdot |\text{St}_x| = |G|.$$

5.11.8 ESEMPIO. Riprendiamo l'esempio 5.11.2(e), dove X è un gruppo G e il gruppo che agisce è un sottogruppo H di G , e l'azione è la moltiplicazione destra. Sia $g \in G$. Allora $\mathcal{O}(g) = Hg$, $\text{St}_g = \{e\}$, per cui l'indice di St_g in H uguaglia la cardinalità di H e la proposizione 5.11.5 (stante la proposizione 5.5.1) è verificata. \square

5.11.9 ESEMPIO. Consideriamo l'azione naturale di S_4 su $X = \{1, 2, 3, 4\}$. Prendiamo $x = 1 \in X$. Allora

$$\mathcal{O}(1) = \{1, 2, 3, 4\}, \quad \text{St}_1 \cong S_3,$$

quindi $|\mathcal{O}(1)| = 4$, $|\text{St}_1| = 6$, da cui $4 \cdot 6 = 24 = |\mathcal{S}_4|$. \square

5.11.10 ESEMPIO. Sia X l'insieme costituito da tutte le parole con 7 lettere. Vogliamo contare quante sono le parole distinte che si possono costruire che abbiano due A , tre B e due C .

Il gruppo S_7 agisce su X permutando le lettere: ad esempio,

$$(135)(27)ABCAGFE = GEAACFB.$$

Le parole che cerchiamo sono quelle che stanno nell'orbita $\mathcal{O}(x)$, dove

$$x = AABBBCC.$$

Calcoliamo a questo scopo lo stabilizzatore di x : St_x risulta costituito da tutte le permutazioni $\sigma \in S_7$ tali che

$$\sigma(AABBBCC) = AABBBCC.$$

Esso coincide quindi con l'insieme di tutte le permutazioni che scambiano tra loro solo le prime due posizioni, solo la terza, quarta e quinta posizione e solamente le ultime due. In tutto tale stabilizzatore ha $2 \cdot 3! \cdot 2! = 24$ elementi. Allora

$$|\mathcal{O}(x)| = \frac{|S_7|}{|\text{St}_x|} = \frac{7!}{24} = 210. \quad \square$$

Nel caso in cui l'azione del gruppo sia l'azione di coniugio, il corollario 5.11.7 permette di ottenere il risultato seguente:

5.11.11 COROLLARIO. *Sia G un gruppo finito. Detto $\mathcal{C}(x)$ il centralizzante dell'elemento $x \in G$, sussiste la seguente relazione:*

$$(5.11.2) \quad |G| = \sum \frac{|G|}{|\mathcal{C}(x)|}$$

dove la somma è estesa agli $x \in G$, uno per ogni classe di coniugio.

Dimostrazione. Basta osservare che, detto c_x il numero dei coniugati dell'elemento $x \in G$, risulta

$$|G| = \sum c_x$$

dove si prende un x per ogni classe coniugata. Dato che $c_x = |\mathcal{O}(x)|$, e $C(x) = St_x$, la relazione dell'enunciato segue dal corollario precedente. \square

L'equazione (5.11.2) del corollario precedente prende il nome di *equazione delle classi*.

Ricordando la definizione di centro $Z(G)$ di un gruppo e osservando che un elemento x appartiene al centro se e solo se la sua classe coniugata è costituita dal solo elemento x , la (5.11.2) può scriversi al modo seguente:

$$(5.11.3) \quad |G| = |Z(G)| + \sum \frac{|G|}{|C(x)|}$$

dove ora la somma è estesa agli $x \notin Z(G)$, uno per ogni classe di coniugio.

5.11.12 ESEMPIO. Sia $G = S_3$. Le classi coniugate sono

$$C_1 = \{\text{id}\}$$

$$C_2 = \{(1, 2), (1, 3), (2, 3)\}$$

$$C_3 = \{(1, 2, 3), (1, 3, 2)\}.$$

Indicato con $C(x)$ il centralizzante dell'elemento x , prendiamo un x in ogni classe coniugata. Allora si ha

$$C(\text{id}) = S_3$$

$$C((1, 2)) = \{\text{id}, (1, 2)\}$$

$$C((1, 2, 3)) = \{\text{id}, (1, 2, 3), (1, 3, 2)\}.$$

Verifichiamo l'equazione delle classi:

$$|S_3| = 6 = \frac{6}{|C(\text{id})|} + \frac{6}{|C((1, 2))|} + \frac{6}{|C((1, 2, 3))|} = \frac{6}{6} + \frac{6}{2} + \frac{6}{3} = 1 + 3 + 2.$$

Si noti come i laterali destri modulo lo stabilizzatore $St_{(1, 2)} = C((1, 2))$ sono tre, tanti quanti i coniugati di $(1, 2)$, in conformità con la proposizione 5.11.5 e il corollario 5.11.6. \square

Chiudiamo il paragrafo con il seguente teorema dovuto a Burnside, che offre un modo per calcolare il numero di orbite di un G -insieme finito.

5.11.13 TEOREMA DI BURNSIDE. *Sia G un gruppo finito e sia X un G -insieme finito. Allora il numero s di orbite in X rispetto all'azione di G è dato dalla seguente espressione:*

$$s = \frac{1}{|G|} \sum_{g \in G} |X_g|$$

dove con X_g si è indicato l'insieme

$$X_g = \{x \in X \mid gx = x\}.$$

Dimostrazione. Sia N la cardinalità dell'insieme costituito da tutte le coppie (g, x) tali che $gx = x$. Fissato $g \in G$, esistono $|X_g|$ coppie che hanno g come primo elemento. Fissato invece x , ci sono $|\text{St}_x|$ coppie che hanno x come secondo elemento. Quindi si ha la seguente uguaglianza:

$$(5.11.4) \quad N = \sum_{g \in G} |X_g| = \sum_{x \in X} |\text{St}_x|.$$

In base al corollario 5.11.7, l'ultimo membro della precedente uguaglianza uguaglia

$$|G| \sum_{x \in X} \frac{1}{|\mathcal{O}(x)|}.$$

Ora, tenendo conto del fatto che tutti gli x che appartengono ad una stessa orbita $\mathcal{O}(x)$ contribuiscono per

$$|\mathcal{O}(x)| \frac{1}{|\mathcal{O}(x)|} = 1$$

in $\sum_{x \in X} 1/|\mathcal{O}(x)|$, si vede che $\sum_{x \in X} 1/|\mathcal{O}(x)|$ rappresenta precisamente il numero s di orbite che stiamo cercando. La (5.11.4) quindi diventa

$$\sum_{g \in G} |X_g| = |G| s$$

e il teorema è completamente dimostrato. \square

Il teorema di Burnside sostanzialmente dice che il numero di orbite è la media sul gruppo dei punti fissati dai singoli elementi del gruppo.

5.11.14 ESEMPIO. Contare in quanti modi diversi, ossia distinguibili, si possono disporre attorno ad una tavola circolare (nella quale quindi non ci sono posti privilegiati) sei persone.

Sia X l'insieme di tutte le possibili disposizioni delle sei persone. Risulta $|X| = 6!$. Operando una rotazione delle persone, si ottiene una disposizione delle persone che non è distinguibile dalla precedente. Facciamo quindi agire su X il gruppo G (ciclico di ordine 6) delle possibili rotazioni. Allora il numero

delle disposizioni delle persone che ci interessano (ossia le disposizioni distinguibili) non è dato dalla cardinalità di X , ossia $6! = 720$, ma dal numero di orbite distinte: infatti non siamo in grado di distinguere due disposizioni di persone che appartengono alla stessa orbita (perché si tratta semplicemente di due disposizioni *ruotate* attorno alla tavola). Utilizziamo allora la formula del teorema di Burnside. Si ha $|X_g| = 0$ per ogni rotazione g diversa dalla rotazione identica, e $|X_{id}| = 6!$ (la rotazione identica fissa tutte le $6!$ disposizioni). Quindi

$$s = \frac{1}{|G|} \sum_{g \in G} |X_g| = \frac{1}{6} 6! + 5! = 120 . \quad \square$$

5.11.15 ESEMPIO. Contare i braccialetti distinti che si possono produrre con cinque perle e tre coralli.

Possiamo pensare le perle e i coralli equidistanti sul braccialetto, quindi vertici di un ottagono regolare. Ogni configurazione è individuata non appena si sistemano i tre coralli. Quindi in tutto le configurazioni sono $\binom{8}{3} = 56$. Ma non sono tutte distinte: per vedere quali sono distinte, occorre vedere quale gruppo agisce sull'insieme di tutte le configurazioni e poi contare solo le configurazioni che stanno in orbite diverse rispetto a questa azione. Questa volta il gruppo che agisce non è il gruppo ciclico delle rotazioni, ma il gruppo diedrale delle simmetrie di un ottagono: infatti il braccialetto può non solo essere ruotato, ma anche ribaltato (cosa che non poteva accadere nel caso della tavola). Si osservi però che il gruppo agisce non sui vertici dell'ottagono, ma sulle *configurazioni*. Per contare il numero di orbite, utilizzando il teorema di Burnside, occorre contare per ogni elemento g di D_8 il numero X_g di configurazioni fissate. L'identità fissa tutte le 56 configurazioni, le rotazioni non fissano nessuna configurazione. Quanto ai ribaltamenti, i quattro ribaltamenti rispetto agli assi del poligono non fissano nessuna configurazione, mentre ciascuno dei ribaltamenti che ha come asse la bisettrice del poligono fissa 6 configurazioni (quelle che hanno una perla e un corallo sui vertici del poligono che si trovano sulla bisettrice: si verifichi che sono 6). In definitiva il numero s cercato è

$$\begin{aligned} s &= \frac{1}{16} \underbrace{(56 + 0 + 0 + 0 + 0 + 0 - 0 - 0 + 0 + 0 - 0 + 0 + 6 + 6 + 6 + 6)}_{\text{fissate dalle rotazioni}} \\ &= \frac{80}{16} = 5 . \quad \square \end{aligned}$$

ESERCIZI.

- Indicate rispettivamente con $\sigma^{\mathcal{S}_n}$ e con σ^{A_n} la classe di coniugio della permutazione σ di A_n rispettivamente in \mathcal{S}_n e in A_n ; si provi che $\sigma^{\mathcal{S}_n}$ coincide con σ^{A_n} se esiste una permutazione *dispari* di \mathcal{S}_n che commuta con σ .

altrimenti

$$\sigma^{\mathcal{S}_n} = \sigma^{A_n} \cup \{(1, 2)\sigma(1, 2)^{-1}\}^{A_n}$$

ossia la classe di coniugio di σ in \mathcal{S}_n si spezza nella unione di due classi coniugate in A_n con rappresentanti σ e $(1, 2)\sigma(1, 2)^{-1}$.

2. Si determini il numero di classi coniugate di A_5 e la cardinalità di ogni classe.
3. Per ogni permutazione $\sigma \in S_3$ si determini lo stabilizzatore rispetto all'azione di S_3 su se stesso per coniugio. Si verifichi che l'ordine di S_3 uguaglia il prodotto di $|St_\sigma| \cdot |\mathcal{O}(\sigma)|$. Si ripeta questo esercizio con \mathcal{S}_n .
4. Si determini il centro del gruppo D_4 delle simmetrie di un quadrato e si scriva l'equazione delle classi per tale gruppo.
5. Quante parole (anche senza significato) distinte di 6 lettere si possono formare permutando le lettere della parola GRUPPO? Fare un ragionamento utilizzando le nozioni di azione, orbita, stabilizzatore.
6. Si determini il numero di posizioni diverse in cui si possono disporre 4 chiavi di colori diversi in un portachiavi circolare. (Quale gruppo G si fa agire sull'insieme X di tutte le possibili disposizioni? Non è solo possibile ruotare il portachiavi, ma anche ribaltarlo.)
7. E se le 4 chiavi dell'esercizio precedente fossero due verdi e due gialle?
8. Si studi l'equazione delle classi per il gruppo alterno A_4 .
9. (a) Una fabbrica di bicchieri produce bicchieri con p strisce verticali, con p numero primo, ogni striscia potendo essere di r colori. Determinare quanti modelli distinti deve costruire la fabbrica.
 (b) Si provi che in tal modo si riesce a ridimostrare il piccolo teorema di Fermat (teorema 2.6.9).
10. Determinare i centralizzanti di $(1, 2)$ e di $(1, 2, 3, 4)$ in S_4 . Determinare i centralizzanti di $(1, 2)$ e $(1, 2, 3, 4, 5)$ in S_5 . Si suggerisce di utilizzare alcune proprietà studiate in questo paragrafo.
11. Generalizzare il punto precedente determinando i centralizzanti degli r -cicli di \mathcal{S}_n .



CONTROLLO.

1. Cosa si intende per azione di un gruppo su di un insieme?
2. La cardinalità dell'orbita di un elemento uguaglia ...
3. Sia X un G -insieme, con G gruppo finito. La cardinalità delle orbite è sempre un divisore dell'ordine del gruppo?
4. Se X è un G -insieme finito, con G gruppo finito, come si contano le orbite?

5.12. Il teorema di Cauchy e i teoremi di Sylow

Il teorema del paragrafo precedente, secondo cui, dato un gruppo finito G e un G -insieme X ,

$$|\mathcal{O}(x)| \cdot |\text{St}_x| = |G|$$

ha varie applicazioni. Prima fra tutti il seguente teorema dovuto a Cauchy.

5.12.1 TEOREMA DI CAUCHY. *Sia G un gruppo di ordine n e sia p un numero primo che divide n . Allora G contiene un elemento di periodo p .*

Dimostrazione. Si tratta di trovare un elemento $x \neq e$ tale che $x^p = e$. Sia X l'insieme di tutte le stringhe ordinate $\mathbf{x} = (x_1, x_2, \dots, x_p)$ di elementi di G tali che $x_1 x_2 \cdots x_p = e$.

(1) X ha una cardinalità che è un multiplo di p : infatti, x_1, x_2, \dots, x_{p-1} possono essere scelti ciascuno in modo arbitrario in G , cioè ciascuno in $n = |G|$ modi; dopo di che x_p è determinato dalla relazione $x_1 x_2 \cdots x_p = e$. Quindi il numero di tali stringhe è n^{p-1} , che è un multiplo di p , dato che tale è n .

(2) Si può definire la seguente azione naturale di \mathbb{Z}_p su X : per ogni $t \in \mathbb{Z}_p$ si pone

$$t(x_1, x_2, \dots, x_p) \stackrel{\text{def}}{=} (x_{t+1}, x_{t+2}, \dots, x_t)$$

che corrisponde ad una traslazione di t degli indici e loro riduzione modulo p : si tratta effettivamente di un'azione.

(3) Per il corollario 5.11.7 applicato al gruppo \mathbb{Z}_p , la cardinalità di ogni orbita divide p , quindi ogni orbita è costituita o da una sola stringa, oppure da p stringhe. Se tutte le orbite diverse dall'orbita costituita dalla sola stringa (e, e, \dots, e) fossero costituite da p stringhe, l'ordine di X non potrebbe essere un multiplo di p , contraddicendo il punto (1). Ciò significa che deve esistere un'orbita (non ridotta alla sola stringa (e, e, \dots, e)) che contiene un solo elemento, il che significa che contiene una stringa $(x_1, x_2, \dots, x_p) \neq (e, e, \dots, e)$ che è lasciata fissa da ogni elemento di \mathbb{Z}_p . Questo comporta (dato il tipo di azione di \mathbb{Z}_p su X) che $x_1 = x_2 = \cdots = x_p$, ossia x_1 è un elemento di periodo p , come cercavamo. \square

Abbiamo già visto che, dato un gruppo di ordine n , non è vero che per ogni divisore di n esiste un sottogruppo che abbia quello come ordine. Il teorema ora dimostrato ci garantisce che per ogni *divisore primo* dell'ordine di un gruppo, esiste un sottogruppo che ha quello come ordine: l'esistenza infatti di un elemento di periodo p ci garantisce che il sottogruppo da esso generato ha ordine p .

Possiamo dare le seguenti altre due applicazioni riguardanti i cosiddetti *p-gruppi*.

5.12.2 DEFINIZIONE. Sia p un numero primo. Dicesi p -gruppo un gruppo che ha come ordine una potenza di p . \square

5.12.3 TEOREMA. *Sia G un p -gruppo. Allora il centro $Z(G)$ è non banale.*

Dimostrazione. Consideriamo la partizione di G in classi coniugate. La cardinalità di ogni classe sarà pertanto 0 o 1 o una potenza di p . Il centro di G è costituito da tutti gli elementi che commutano con ogni elemento di G , e quindi è costituito da tutte le classi che possiedono un solo elemento. Se quindi il centro fosse banale, l'ordine di G sarebbe congruo ad 1 modulo p , che contraddice l'ipotesi che sia $|G| = p^k$. \square

5.12.4 TEOREMA. *Un gruppo G di ordine p^2 è abeliano.*

Dimostrazione. Per quanto detto nel teorema precedente, il centro $Z(G)$ di G è non banale; esso avrà quindi 0 o p o p^2 elementi. Supponiamo che abbia p elementi, e sia a un elemento non appartenente a $Z(G)$. Allora il centralizzante di a , $C(a) = \{g \in G \mid ga = ag\}$ è un sottogruppo di G contenente propriamente $Z(G)$. Ma allora, per il teorema di Lagrange, non può che coincidere con tutto G , il che è assurdo, perché a dovrebbe allora stare nel centro. Resta dunque la possibilità che $Z(G)$ abbia p^2 elementi, cioè coincida con tutto G . G è in tal caso abeliano. \square

Terminiamo enunciando e dimostrando i teoremi di Sylow, che sono molto utili per risolvere vari tipi di problemi di natura combinatorica sui gruppi finiti. Si tratta di tre teoremi, noti comunemente come primo, secondo e terzo teorema di Sylow. Per semplicità li raduniamo in un unico enunciato.

Premettiamo una definizione.

5.12.5 DEFINIZIONE. Un p -sottogruppo P di un gruppo finito G con la proprietà che la sua cardinalità è la potenza massima di p che divide $|G|$, prende il nome di p -sottogruppo di Sylow. \square

5.12.6 TEOREMI DI SYLOW. *Sia G un gruppo finito il cui ordine sia $p^\alpha \cdot m$, dove p è un numero primo e m non è divisibile per p . Allora:*

- G contiene un sottogruppo di ordine p^α , cioè un p -sottogruppo di Sylow;*
- se H è un p -gruppo (con p^h elementi, $h \leq \alpha$), allora è contenuto in un p -sottogruppo di Sylow;*
- due qualunque p -sottogruppi di Sylow di G sono coniugati;*
- il numero di p -sottogruppi di Sylow di G distinti è un divisore di m ed è congruo ad 1 modulo p .*

Dimostrazione. Sia X l'insieme di tutti i sottoinsiemi di G che hanno p^α elementi. Facciamo agire G su X per traslazione sinistra: dato comunque un

$U \in X$ e dato comunque un $g \in G$, poniamo $g * U \stackrel{\text{def}}{=} gU$. Dato che la cardinalità di X è

$$|X| = \binom{p^\alpha \cdot m}{p^\alpha}$$

che non è divisibile per p (si veda esercizio 5.12.9), deve esistere un elemento $A \in X$ tale che $\mathcal{O}(A)$ abbia un numero di elementi che *non è un multiplo di p*. Ma allora, per la relazione

$$|\mathcal{O}(A)| \cdot |\text{St}_A| = |G|$$

segue che $|\text{St}_A|$ deve essere un multiplo di p^α . Per definizione di stabilizzatore, e ricordando il tipo di azione che abbiamo definito, dato comunque un elemento $a \in A$ e dato comunque un $g \in \text{St}_A$, risulta $ga \in A$, il che significa che il laterale destro $\text{St}_A a$ è contenuto in A per ogni $a \in A$. Questo implica che la cardinalità di $\text{St}_A a$ è minore o al più uguale alla cardinalità di A , ossia p^α . Dato poi che $\text{St}_A a$ ha la stessa cardinalità di St_A , ne segue che St_A è un *sottogruppo di G di esattamente p^α elementi*. Abbiamo provato il punto (a).

Sia ora \mathcal{P} l'insieme di tutti i p -sottogruppi di Sylow di G . Tale insieme è non vuoto, per il punto (a). Notiamo che se $S \in \mathcal{P}$, allora staranno in \mathcal{P} tutti i coniugati di S mediante elementi di G , dato che si tratta di sottogruppi dello stesso ordine massimo p^α . Indicata quindi con $\mathcal{O}(S)$ l'orbita di S rispetto all'azione di G su \mathcal{P} per coniugazione, si ha $\mathcal{O}(S) \subseteq \mathcal{P}$. Inoltre la cardinalità di $\mathcal{O}(S)$ divide m . Infatti, essendo (cfr. esercizio 5.8.9)

$$\text{St}_S = \{g \in G \mid gSg^{-1} = S\} = N_G(S) \text{ (normalizzante di } S \text{ in } G)$$

è chiaro che $\text{St}_S \supseteq S$, quindi $|\text{St}_S| = p^\alpha r$. La cardinalità di $\mathcal{O}(S)$ non può quindi che dividere m (in base alla solita relazione $|\mathcal{O}(S)| \cdot |\text{St}_S| = |G|$) ed essere coprima con p .

Passiamo alla dimostrazione del punto (b). Sia H un qualunque p -sottogruppo di G , e sia $|H| = p^h$, con $h \leq \alpha$. Facciamo agire H su $\mathcal{O}(S)$ per coniugazione, ossia poniamo $hT = hTh^{-1}$ per ogni $T \in \mathcal{O}(S)$: si tratta di un'azione su $\mathcal{O}(S)$, perché il coniugato di un elemento di $\mathcal{O}(S)$ sta ancora in $\mathcal{O}(S)$. $\mathcal{O}(S)$ viene così ripartita in sottoorbite, ciascuna delle quali ha una cardinalità che divide p^h (cfr. corollario 5.11.7, applicato al gruppo $G = H$). La cardinalità di $\mathcal{O}(S)$ sarà la somma delle cardinalità di tutte queste sottoorbite (si veda figura 5.15).

I p -sottogruppi di Sylow che sono stati rappresentati in figura 5.15 con lo stesso simbolo stanno nella stessa sottoorbita mediante l'azione di H . Ciò significa ad esempio che tutti quelli contrassegnati, come A , con il simbolo \bullet sono del tipo hAh^{-1} , per qualche $h \in H$. Dato che la cardinalità di $\mathcal{O}(S)$ divide m ed è coprima con p , una almeno di queste sottoorbite deve avere un solo elemento. Questo significa che esiste un $T \in \mathcal{O}(S)$ tale che $hTh^{-1} = T$ per ogni $h \in H$ (si veda figura 5.16).

Ma allora $H \subseteq \text{St}_T = \{g \in G \mid gTg^{-1} = T\} = N_G(T)$ (normalizzante di T in G). Chiaramente $T \trianglelefteq N_G(T)$. Si può allora costruire il quoziente $N_G(T)/T$ e considerare il sottogruppo $HT/T \leq N_G(T)/T$. In base al primo teorema di isomorfismo, si ha $HT/T \cong H/H \cap T'$. Ora, $|HT/T|$ è un divisore di m , ed è quindi primo con p , mentre $|H/H \cap T'| = p^r$ per qualche $r \geq 0$ e $\leq h$. Deve quindi necessariamente essere $|H/H \cap T'| = 1$, ossia $H \subseteq T$.

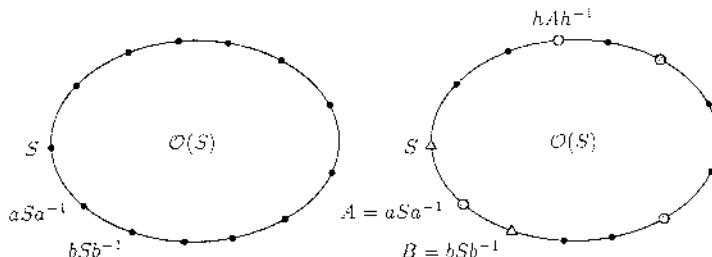


FIGURA 5.15

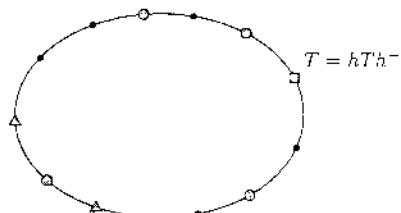


FIGURA 5.16

Abbiamo così provato che ogni p -sottogruppo H è contenuto in un p -sottogruppo di Sylow T , e con ciò il punto (b) è provato.

Proviamo il punto (c). Nelle stesse notazioni del punto precedente, si tratta di provare che $O(S) = P$, ossia che l'orbita $O(S)$ esaurisce tutti i p -sottogruppi di Sylow. Nel punto precedente abbiamo provato che ogni p -sottogruppo H è contenuto in un coniugato di S . Questo vale in particolare nel caso in cui H sia un p -sottogruppo di Sylow. In questo caso necessariamente H coincide con un coniugato di S , dato che ogni p -sottogruppo di Sylow ha p^{α} elementi.

Dimostriamo (d). Riprendendo l'azione per coniugazione del p -sottogruppo di Sylow H su $O(S)$, la sottoorbita di $O(S)$ costituita da un solo elemento è unica, altrimenti H coinciderebbe con un altro p -sottogruppo di Sylow. Essendo la cardinalità di tutte le altre sottoorbite una potenza di p (con esponente maggiore di zero), la cardinalità di $O(S)$ pertanto è congrua a 1 modulo p . \square

5.12.7 APPLICAZIONI. Ogni sottogruppo di ordine 20 contiene un sottogruppo normale.

Il numero di 5-sottogruppi di Sylow deve essere un divisore di 4, ossia può essere 1, 2, o 4. Deve però anche essere congruo ad 1 modulo 5, quindi non può essere che 1. Ora, se un p -sottogruppo di Sylow è unico, questo è necessariamente normale (cfr. esercizio 5.12.1). \square

Un gruppo privo di sottogruppi normali non banali si dice *semplice*. Abbiamo così provato che un gruppo di ordine 20 non è semplice.

Un'altra conseguenza dei teoremi di Sylow è il seguente teorema, che avremo modo di utilizzare varie volte nell'ultima parte del corso.

5.12.8 TEOREMA. *Sia G un gruppo di ordine $p^\alpha m$, con m non divisibile per p . Allora G possiede una catena di sottogruppi*

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_i \subset H_{i+1} \subset \cdots \subset H_\alpha$$

tale che per $0 \leq i \leq \alpha$, H_i è un sottogruppo normale di H_{i+1} , e $|H_{i+1}/H_i| = p$.

Dimostrazione. Procederemo per induzione su $|G|$. Per $|G| = 1$ non c'è nulla da dimostrare. Supporremo allora il teorema vero per ogni gruppo di ordine minore dell'ordine di G e lo dimostreremo per G . G contiene un sottogruppo H di ordine p^α . Ora, sappiamo che un tale gruppo ha centro $Z(H)$ non banale. Ma allora, per il teorema di Cauchy, esiste un sottogruppo H_1 di ordine p contenuto in $Z(H)$. H_1 è un sottogruppo normale di H (essendo contenuto nel centro), quindi il quoziente H/H_1 è un gruppo di ordine minore dell'ordine di G . Per l'ipotesi induttiva, esiste una catena di sottogruppi in H/H_1

$$H_1/H_1 \subseteq \cdots \subseteq H_i/H_1 \subseteq H_{i+1}/H_1 \cdots \subseteq H_\alpha/H_1 = H/H_1$$

tale che

$$(5.12.1) \quad H_i/H_1 \trianglelefteq H_{i+1}/H_1$$

e

$$(5.12.2) \quad \left| \frac{H_{i+1}/H_1}{H_i/H_1} \right| = p .$$

In virtù dei teoremi di isomorfismo, dalla (5.12.1) si ricava che $H_i \trianglelefteq H_{i+1}$ e dalla (5.12.2) che

$$\left| \frac{H_{i+1}/H_1}{H_i/H_1} \right| = |H_{i+1}/H_i| = p . \quad \square$$

5.12.9 COROLLARIO. *Ogni gruppo G di ordine $p^\alpha m$, (m, p) = 1, possiede un sottogruppo H_i di ordine p^i , per ogni $i = 0, 1, \dots, \alpha$.*

Dimostrazione. Il risultato è implicito nel teorema. \square

5.12.10 COROLLARIO. *Ogni p -gruppo G contiene un sottogruppo di indice p in G .*

Dimostrazione. Nelle ipotesi attuali H_σ del teorema 5.12.8 coincide con G . \square

ESERCIZI.

1. Provare che se un gruppo G ha un solo p -sottogruppo di Sylow H , allora $H \trianglelefteq G$.
2. Si provi che il gruppo alterno A_4 non possiede sottogruppi di ordine 6.
3. Si provi che un gruppo finito G è un p -gruppo se e solo se ogni elemento di G ha come ordine una potenza di p .
4. Si provi che un gruppo non abeliano di ordine p^3 ha un centro di ordine p .
5. Si determinino tutti i 2-sottogruppi di Sylow e 3-sottogruppi di Sylow di S_3 e di S_4 .
6. Si provi che un gruppo di ordine 65 possiede un sottogruppo normale non banale.
7. Sia G un gruppo con pq elementi, p e q primi, $p < q$. Si provi che G possiede uno e un solo sottogruppo di ordine q . Si provi inoltre che se p non divide $q - 1$, allora G è ciclico.
8. Sia G un gruppo di ordine $|G| = 2m$, con m dispari maggiore di 1. Si provi che G possiede un sottogruppo normale non banale, e che quindi G non è semplice.
9. Provare che se p è primo e m non è divisibile per p , allora $\binom{p^a m}{p^a}$ non è divisibile per p .
10. Si determinino tutti i gruppi di ordine 33.

ESERCIZI DI PROGRAMMAZIONE.

1. Si scriva un programma che calcoli, dato un gruppo finito, i possibili ordini dei p -sottogruppi di Sylow, per i vari p divisori primi dell'ordine di G .
2. Ricordiamo che se $n = p^a m$ e $(m, p) = 1$ e 1 è l'unico divisore di n (e quindi di m) congruente ad 1 modulo p allora un gruppo di ordine n possiede un sottogruppo normale, quindi non è semplice. Si applichi questo criterio di "non semplicità" a tutti gli interi non primi compresi tra 1 e 100, e si listino tutti gli interi che soddisfano questo criterio. Si verifichi che gli unici interi $n \leq 100$ non primi per i quali non è escluso (usando solo questo criterio di non semplicità) che esista un gruppo semplice di ordine n sono i seguenti:

12, 24, 30, 48, 56, 60, 72, 80, 90, 96 .

Utilizzando poi l'esercizio 5.12.8 si riducano ulteriormente le possibilità.

Si ripeta il programma per gli interi $n \leq 250$.

CONTROLLO.

1. Nel teorema di Cauchy è essenziale il fatto che il numero p sia primo? Può valere anche se p non è primo? Discutere questa eventualità.
2. Determinare i p -sottogruppi di Sylow di alcuni gruppi a vostra scelta e verificare su questi esempi la validità dei teoremi di Sylow.

5.13. Il teorema di Cayley generalizzato

Sappiamo dal teorema di Cayley (cfr. §5.6) che ogni gruppo è isomorfo ad un gruppo di trasformazioni, ossia è (isomorfo ad) un sottogruppo di $\mathcal{S}(X)$ per un opportuno insieme X . Per dimostrare il teorema abbiamo preso come X l'insieme G stesso. Abbiamo tuttavia fatto notare che $\mathcal{S}(G)$ è molto grande rispetto a G . Cerchiamo quindi, se possibile, di trovare un X più piccolo rispetto a G , in modo che $\mathcal{S}(X)$ diventi più piccolo. Vedremo cosa si potrà fare.

5.13.1 TEOREMA DI CAYLEY GENERALIZZATO. *Sia G un gruppo e sia H un suo sottogruppo. Posto $X = \{xH\}_{x \in G}$, allora esiste un omomorfismo $\Psi : G \rightarrow \mathcal{S}(X)$ il cui nucleo è il più grande sottogruppo normale di G contenuto in H .*

Dimostrazione. L'applicazione

$$\begin{aligned} T_g : X &\longrightarrow X \\ xH &\longmapsto gxH \end{aligned}$$

è una corrispondenza biunivoca di X in sé, e in quanto tale è un elemento di $\mathcal{S}(X)$. Possiamo pertanto definire la seguente applicazione

$$\begin{aligned} \Psi : G &\longrightarrow \mathcal{S}(X) \\ g &\longmapsto T_g. \end{aligned}$$

Risulta, per ogni xH in X

$$T_{gg'}(xH) = gg'(xH) = g(g'xH) = T_g(T_{g'}xH)$$

ossia $T_{gg'} = T_g \circ T_{g'}$, e quindi Ψ è un omomorfismo tra G e $\mathcal{S}(X)$. Cerchiamone il nucleo.

$$\begin{aligned} \text{Ker } \Psi &= \{g \in G \mid T_g = \text{id}\} = \{g \in G \mid T_g(xH) = xH \forall x \in G\} \\ &= \{g \in G \mid gxH = xH \forall x \in G\}. \end{aligned}$$

Posto $K = \text{Ker } \Psi$, facciamo vedere che K è il più grande sottogruppo normale di G contenuto in H .

- (1) $K \trianglelefteq G$, essendo il nucleo di un omomorfismo.
- (2) $K \subseteq H$: infatti

$$k \in K \implies kxH = xH \quad \forall x \in G.$$

In particolare per $x = e$ si ottiene

$$kH = H \implies k \in H.$$

- (3) Se $N \trianglelefteq G$, $N \subseteq H$, allora $N \subseteq K$. Infatti, essendo $N \trianglelefteq G$ e $N \subseteq H$ si ha per ogni $n \in N$ e ogni $x \in G$ (e quindi per ogni $x^{-1} \in G$) la seguente serie di implicazioni:

$$\begin{aligned} xnx^{-1} \in N \subseteq H &\implies xnx^{-1}H = H \\ &\implies nx^{-1}H = x^{-1}H \\ &\implies N \subseteq K. \quad \square \end{aligned}$$

Con la scelta di X di questo teorema siamo riusciti a ridurre la grandezza di $S(X)$, tuttavia abbiamo perso (in genere) l'iniettività della applicazione Ψ . Tuttavia la caratterizzazione del nucleo della Ψ come il più grande sottogruppo normale di G contenuto in H ci dà informazioni sul gruppo G , che passiamo ad elencare.

5.13.2 CONSEGUENZE DEL TEOREMA.

- (a) Sia G un gruppo *semplice*, ossia privo di sottogruppi normali non banali. Allora la Ψ è iniettiva. In questo caso quindi siamo riusciti ad ottenere G come gruppo di trasformazioni come nel teorema di Cayley, con un X più piccolo.
- (b) Sia G un gruppo finito, sia H un suo sottogruppo, e $i(H)$ il numero dei laterali sinistri di H in G , di modo che $|S(X)| = i(H)!$. Se G ed H sono tali che $|G| \nmid i(H)!$, allora certamente Ψ non è iniettiva: se infatti lo fosse, sarebbe

$$|G| = |\text{Im } \Psi| \quad \text{divisore di } i(H)!.$$

Quindi esiste in G un sottogruppo normale. \square

5.13.3 ESEMPIO. Sia G un gruppo finito di ordine 35, e sia H un suo sottogruppo di ordine 7 (sicuramente esistente, per il teorema di Cauchy). Allora risulta

$$i(H) = 5, \quad i(H)! = 120, \quad |G| = 35 \nmid 120.$$

Esiste quindi in G un sottogruppo normale non banale contenuto in H . Essendo l'ordine di H un numero primo, questo sottogruppo normale deve necessariamente coincidere con H , cioè H è normale. \square

ESERCIZI.

1. Sia G un gruppo di ordine 42. Si provi che G contiene un sottogruppo normale non banale in G .
2. Si provi che un gruppo di ordine 77 possiede un sottogruppo normale non banale.
3. Si provi che nella lista dei "possibili" ordini (inferiori a 100) di gruppi semplici dell'esercizio di programmazione 5.12.2, utilizzando il teorema di Cayley generalizzato, si salvano i soli due interi 56 e 60.



ESERCIZI DI PROGRAMMAZIONE.

1. Sia G un gruppo di ordine $n < 100$. Per ogni divisore primo p di n , si elenchino gli ordini dei p -sottogruppi di Sylow H di G tali che $n \nmid i(H)!$. Si listino gli n per i quali esiste un sottogruppo H con questa proprietà: tali interi non possono essere ordini di un gruppo semplice.



CONTROLLO.

1. Quali vantaggi offre, rispetto al teorema di Cayley, il teorema generalizzato?
2. Presentare alcune applicazioni del teorema.

5.14. Prodotti diretti e semidiretti

Spesso in matematica si costruiscono nuove strutture a partire da strutture date: è un po' come quando, dati due numeri, se ne costruisce il prodotto. In questo paragrafo faremo vedere come, dati due gruppi, si riesce a costruire un nuovo gruppo, detto loro *prodotto diretto*. In un secondo tempo, daremo delle condizioni che ci permettano, dato un gruppo, di vedere se è (isomorfo ad) un prodotto diretto di due gruppi. Quest'ultimo problema corrisponde in un certo senso a "fattorizzare" un numero grande in fattori più piccoli.

5.14.1 DEFINIZIONE. Siano G_1 e G_2 due gruppi, ciascuno con la propria operazione, che per semplicità indicheremo con il simbolo ordinario di moltiplicazione. Si definisce *prodotto diretto esterno* di G_1 e G_2 il prodotto cartesiano $G_1 \times G_2$ di G_1 e G_2 , dotato della seguente operazione:

$$(g_1, g_2) * (g'_1, g'_2) \stackrel{\text{def}}{=} (g_1 g'_1, g_2 g'_2) . \quad \square$$

È facile dimostrare che il prodotto diretto esterno di due gruppi risulta un gruppo. (cfr. esercizio 5.14.1).

Diamo qui di seguito alcuni esempi.

5.14.2 ESEMPI.

- (a) Siano $G_1 = \mathbb{Z}_2$ e $G_2 = \mathbb{Z}_3$. Allora

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{2})\} .$$

Gli ordini degli elementi di $\mathbb{Z}_2 \times \mathbb{Z}_3$ sono rispettivamente 1, 3, 3, 2, 6, 6. Si tratta di un gruppo ciclico di ordine 6, quindi

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6 .$$

- (b) Siano $G_1 = \mathbb{Z}_2$ e $G_2 = \mathbb{Z}_4$. Il prodotto diretto esterno $\mathbb{Z}_2 \times \mathbb{Z}_4$ è costituito da 8 elementi, ma questa volta non esiste nessun elemento di periodo 8, quindi non si tratta del gruppo ciclico di ordine 8, cioè $\mathbb{Z}_2 \times \mathbb{Z}_4 \not\cong \mathbb{Z}_8$. \square

5.14.3 TEOREMA. Siano G_1 e G_2 due gruppi, e sia $G = G_1 \times G_2$ il loro prodotto diretto esterno. Allora esistono in $G_1 \times G_2$ due sottogruppi \tilde{G}_1 e \tilde{G}_2 tali che

- (a) $\tilde{G}_1 \cong G_1$, $\tilde{G}_2 \cong G_2$;
- (b) $\tilde{G}_1 \trianglelefteq G$, $\tilde{G}_2 \trianglelefteq G$;
- (c) $G = \tilde{G}_1 \tilde{G}_2$;
- (d) $\tilde{G}_1 \cap \tilde{G}_2 = \{e_{G_1}, e_{G_2}\} =$ sottogruppo banale di $G_1 \times G_2$.

Dimostrazione. Basta prendere

$$\tilde{G}_1 \stackrel{\text{def}}{=} \{(g_1, e_{G_2}) \mid g_1 \in G_1\}$$

$$\tilde{G}_2 \stackrel{\text{def}}{=} \{(e_{G_1}, g_2) \mid g_2 \in G_2\}$$

dove con e_{G_1} e e_{G_2} si sono indicati gli elementi neutri rispettivamente di G_1 e G_2 . Si lascia come esercizio la verifica di tutte le asserzioni. \square

Se un gruppo possiede due sottogruppi \tilde{G}_1 e \tilde{G}_2 che verificano le condizioni (b), (c) e (d) del teorema precedente, si dice che G è un *prodotto diretto interno* dei suoi sottogruppi \tilde{G}_1 e \tilde{G}_2 . Abbiamo quindi appena dimostrato che un gruppo che sia un prodotto diretto esterno di due gruppi è isomorfo al loro prodotto diretto interno.

Il fatto interessante è che vale il viceversa, ossia le asserzioni elencate nel teorema caratterizzano i gruppi che sono prodotto diretto esterno di due gruppi. Precisamente, vale il seguente teorema.

5.14.4 TEOREMA. Sia G un gruppo, e siano G_1 e G_2 due suoi sottogruppi tali che

- (a) $G_1 \trianglelefteq G$, $G_2 \trianglelefteq G$;
- (b) $G = G_1 G_2$;
- (c) $G_1 \cap G_2 = \{e\}$.

Allora G è isomorfo al prodotto diretto esterno $G_1 \times G_2$.

Prima di passare alla dimostrazione di questo teorema, premettiamo due lemmi.

5.14.5 LEMMA. Sia G un gruppo e siano H e K due sottogruppi di G tali che

$$H \trianglelefteq G, \quad K \trianglelefteq G, \quad H \cap K = \{e\}.$$

Allora, per ogni $h \in H$ e ogni $k \in K$ risulta $hk = kh$.

Dimostrazione. Sia $x = hkh^{-1}k^{-1}$. Dalla $x = (hkh^{-1})k^{-1}$, si vede che x appartiene a K , essendo $hkh^{-1} \in K$ per la normalità di K in G . Dalla $x = h(kh^{-1}k^{-1})$, per la normalità di H in G , x risulta invece appartenere ad H . Essendo $H \cap K = \{e\}$, ne segue che $x = hkh^{-1}k^{-1} = e$, da cui $hk = kh$. \square

5.14.6 LEMMA. Sia G un gruppo e siano H e K due suoi sottogruppi tali che

- (a) $G = HK$;
- (b) $H \cap K = \{e\}$.

Allora ogni $g \in G$ si scrive in modo unico come prodotto di un elemento di H per un elemento di K .

Dimostrazione. Per (a), ogni $g \in G$ si scrive come hk per qualche $h \in H$, $k \in K$. Per provare l'unicità della scrittura, supponiamo che sia

$$g = hk = h'k'$$

Allora $h^{-1}hkk'^{-1} = h^{-1}h'k'k'^{-1}$, da cui $kk'^{-1} = h^{-1}h' \in H \cap K = \{e\}$. Quindi $h = h'$, $k = k'$ e la scrittura è unica. \square

Passiamo ora alla dimostrazione del teorema.

Dimostrazione del teorema 5.14.4. Definiamo la seguente applicazione:

$$\begin{aligned}\Psi : G_1 \times G_2 &\longrightarrow G \\ (g_1, g_2) &\longmapsto g_1g_2.\end{aligned}$$

L'applicazione è suriettiva per la (b) dell'enunciato. È iniettiva per il lemma 5.14.6. Si tratta inoltre di un omomorfismo, per il lemma 5.14.5. Abbiamo quindi provato che il gruppo G è isomorfo al prodotto diretto di G_1 per G_2 . \square

I teoremi provati ci dicono che potremo parlare indifferentemente di prodotto diretto esterno o interno di due gruppi, dato che si tratta di concetti equivalenti. L'ultimo teorema ci dice che per decidere se un gruppo è o non è (isomorfo ad) un prodotto diretto, basta lavorare dall'interno del gruppo stesso, cercando se esistono due sottogruppi normali in G che verifichino le condizioni del teorema.

Diamo qui di seguito alcuni esempi in tale senso.

5.14.7 ESEMPIO. Il gruppo $(\mathbb{Z}, +)$ non è mai prodotto diretto di due gruppi non banali, dato che due suoi sottogruppi non nulli arbitrari si intersecano sempre in modo non banale. \square

5.14.8 ESEMPIO. Il gruppo simmetrico S_3 non è prodotto diretto, dato che possiede un solo sottogruppo normale non banale. \square

5.14.9 ESEMPIO. Il gruppo diedrale D_4 non è prodotto diretto, perché due qualunque sottogruppi normali non banali di D_4 si intersecano in modo non banale, dato che contengono tutti l'elemento r^2 . \square

5.14.10 ESEMPIO. Il gruppo ortogonale $O_3(\mathbb{R})$ è isomorfo al prodotto diretto di SO_3 (gruppo delle matrici 3×3 ortogonalni a determinante 1) per \mathbb{Z}_2 . Più in generale,

$$O_n \simeq SO_n \times \mathbb{Z}_2, \quad n \text{ dispari}. \quad \square$$

5.14.11 ESEMPIO. \mathbb{Z}_{12} è isomorfo al prodotto diretto di $\mathbb{Z}_3 \times \mathbb{Z}_4$. Infatti i due sottogruppi

$$H = \{\bar{0}, \bar{4}, \bar{8}\}, \quad K = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$$

sono (ovviamente) normali, a intersezione ridotta alla sola classe $\bar{0}$, e sono tali che $\mathbb{Z}_{12} = H + K$. Inoltre, $H \cong \mathbb{Z}_3$ e $K \cong \mathbb{Z}_4$. \square

5.14.12 ESEMPIO. $(\mathbb{C}, +)$ è isomorfo a $(\mathbb{R}, +) \times (\mathbb{R}, +)$. \square

La definizione di prodotto diretto esterno di due gruppi si estende in modo naturale al caso di più di due fattori.

5.14.13 DEFINIZIONE. Siano dati i gruppi G_1, G_2, \dots, G_k . Si definisce *prodotto diretto esterno* di G_1, G_2, \dots, G_k l'insieme

$$G_1 \times G_2 \times \cdots \times G_k = \{(g_1, g_2, \dots, g_k) \mid g_i \in G_i\}$$

dotato dell'operazione seguente:

$$(g_1, g_2, \dots, g_k)(g'_1, g'_2, \dots, g'_k) \stackrel{\text{def}}{=} (g_1 g'_1, g_2 g'_2, \dots, g_k g'_k). \quad \square$$

È facile vedere che $G_1 \times G_2 \times \cdots \times G_k$ dotato di questa operazione diventa un gruppo.

Valgono le seguenti proprietà:

5.14.14 PROPOSIZIONE. Sia $G = G_1 \times G_2 \times \cdots \times G_k$. Allora

(a) se ogni fattore ha ordine finito,

$$|G_1 \times G_2 \times \cdots \times G_k| = |G_1| |G_2| \cdots |G_k|;$$

(b) $G_1 \times G_2 \times \cdots \times G_k$ è abeliano se e solo se ogni G_i è abeliano;

(c) $|(g_1, g_2, \dots, g_k)| = \text{lcm}(|g_1|, |g_2|, \dots, |g_k|)$: l'ordine è infinito se uno dei g_i ha ordine infinito;

(d) se ogni G_i ha ordine finito, $G_1 \times G_2 \times \cdots \times G_k$ è ciclico se e solo se ogni G_i è ciclico e $(|G_i|, |G_j|) = 1$ per ogni $i \neq j$.

Dimostrazione. I punti (a), (b) sono ovvi.

(c) Sia $m = \text{lcm}(|g_1|, |g_2|, \dots, |g_k|)$ e sia t l'ordine di (g_1, g_2, \dots, g_k) . Dalla

$$(e, e, \dots, e) = (g_1, g_2, \dots, g_k)^t = (g_1^t, g_2^t, \dots, g_k^t)$$

risulta che t è un multiplo di ogni $|g_i|$ e quindi $m \mid t$. D'altra parte dalla

$$(e, e, \dots, e) = (g_1^m, g_2^m, \dots, g_k^m) = (g_1, g_2, \dots, g_k)^m$$

si ha $t \mid m$. Quindi $t = m$.

(d) (\Rightarrow) Che i G_i siano ciclici è ovvio, in quanto isomorfi a sottogruppi di un gruppo ciclico. Indicato con g_i un generatore di G_i , l'elemento $g = (g_1, g_2, \dots, g_k)$ ha ordine massimo tra tutti gli elementi di $G_1 \times G_2 \times \dots \times G_k$ e in virtù del punto precedente il suo ordine è il $\text{mcm}(g_1, g_2, \dots, g_k)$. Se fosse $(|G_i|, |G_j|) = d \neq 1$ per qualche i, j , $i \neq j$, allora l'ordine di (g_1, g_2, \dots, g_k) sarebbe

$$\frac{|g_1| \cdot |g_2| \cdots |g_k|}{d} < |g_1| \cdot |g_2| \cdots |g_k|$$

e non potrebbe quindi essere generatore di $G_1 \times G_2 \times \dots \times G_k$.

(\Leftarrow) Se ogni G_i è ciclico e $(|G_i|, |G_j|) = 1$ per ogni i, j , $i \neq j$, allora, indicato con g_i un generatore di G_i per ogni $i = 1, \dots, k$, l'elemento (g_1, g_2, \dots, g_k) ha ordine $|g_1| \cdot |g_2| \cdots |g_k|$ e quindi $G_1 \times G_2 \times \dots \times G_k$ è ciclico. \square

5.14.15 COROLLARIO. $\mathbb{Z}_r \times \mathbb{Z}_s$ è isomorfo a \mathbb{Z}_{rs} (cioè è ciclico) se e solo se $(r, s) = 1$.

L'analogo del teorema 5.14.4 nel caso di prodotto di più di due gruppi è il seguente.

5.14.16 TEOREMA. Sia G un gruppo e siano N_1, N_2, \dots, N_k sottogruppi di G tali che

- (a) $N_i \leq G$;
- (b) $G = N_1 N_2 \cdots N_k$;
- (c) $N_i \cap (N_1 N_2 \cdots N_{i-1} \widehat{N_i} N_{i+1} \cdots N_k) = \{e\}$ per ogni $i = 1, \dots, k$.

Allora G è isomorfo al prodotto diretto $N_1 \times N_2 \times \cdots \times N_k$.

Dimostrazione. Si invita lo studente a fare da sé la dimostrazione. \square

Con questa caratterizzazione a disposizione, si invita lo studente a provare che un gruppo abeliano finito è prodotto diretto dei suoi sottogruppi di Sylow.

Ritorniamo ora al caso di prodotto diretto di due gruppi. Abbiamo visto che l'essere un gruppo G prodotto diretto equivale all'esistenza in G di due sottogruppi \bar{G}_1 e \bar{G}_2 normali in G , tali che $G = \bar{G}_1 \bar{G}_2$ e $\bar{G}_1 \cap \bar{G}_2 = \{e\}$. Nel dimostrare questa equivalenza si era rivelato essenziale (si veda il lemma 5.14.5) il fatto che

$$(5.14.1) \quad g_1 g_2 \cdot g'_1 g'_2 = g_1 g'_1 \cdot g_2 g'_2 \quad \forall g_1, g'_1 \in \bar{G}_1, \forall g_2, g'_2 \in \bar{G}_2.$$

Supponiamo ora che il gruppo G possieda un sottogruppo normale N e un altro sottogruppo (non necessariamente normale) H tali che

$$G = NH, \quad N \cap H = \{e\}.$$

In questo caso la (5.14.1) non vale più: cioè in genere $nh \cdot n'h' \neq nn' \cdot hh'$. Si può tuttavia dire che risulta

$$(5.14.2) \quad nh \cdot n'h' = nhn'h^{-1} \cdot hh'$$

dove $hn'h^{-1}$, essendo coniugato di un elemento di N , che è normale, è un elemento di N . Cioè il prodotto di due elementi nh e $n'h'$ di NH non uguaglia (come nel caso in cui i due sottogruppi erano entrambi normali) il prodotto di an' per hh' , ma il prodotto di $n(hn'h^{-1})$ per hh' ; la differenza quindi è che al posto di n' si deve mettere il coniugato di n' mediante l'elemento h . Resta quindi individuato per ogni $h \in H$ la seguente applicazione

$$\begin{aligned}\gamma_h : N &\longrightarrow N \\ n' &\longmapsto hn'h^{-1}\end{aligned}$$

che risulta un *automorfismo* di N . Si noti che nel caso in cui anche H sia normale, tale automorfismo risulta l'automorfismo identico: infatti risulta $hn' = n'h$, da cui $hn'h^{-1} = n'$.

Si può pertanto definire la seguente applicazione:

$$\begin{aligned}\Phi : H &\longrightarrow \text{Aut}(N) \\ h &\longmapsto \gamma_h.\end{aligned}$$

Si tratta di un *omomorfismo*. La relazione (5.14.2) si può scrivere in termini di questo omomorfismo al modo seguente:

$$nh \cdot n'h' = n\Phi(h)(n') \cdot hh'.$$

Si noti che, nel caso in cui anche il sottogruppo H sia normale in G , $\Phi(h)(n') = n'$, da cui si ritrova la (5.14.1).

Siano ora G_1 e G_2 due *gruppi arbitrari*, e sia Φ un omomorfismo da G_2 ad $\text{Aut}(G_1)$. Nel prodotto cartesiano $G_1 \times G_2$ possiamo definire la seguente operazione:

$$(5.14.3) \quad \boxed{(g_1, g_2)(g'_1, g'_2) \stackrel{\text{def}}{=} (g_1 \Phi(g_2)(g'_1), g_2 g'_2)} :$$

$G_1 \times G_2$ dotato di questa operazione diventa un gruppo, e i sottoinsiemi

$$\begin{aligned}\tilde{G}_1 &= \{(g_1, e_{G_2}) \mid g_1 \in G_1\} \\ \tilde{G}_2 &= \{(e_{G_1}, g_2) \mid g_2 \in G_2\}\end{aligned}$$

sono due sottogruppi, di cui il primo è un sottogruppo *normale* in $G_1 \times G_2$, isomorfo a G_1 , e il secondo isomorfo a G_2 (si verifichi).

5.14.17 DEFINIZIONE. Siano dati due gruppi G_1 e G_2 e un omomorfismo Φ da G_2 ad $\text{Aut}(G_1)$. Allora il prodotto cartesiano $G_1 \times G_2$ dotato dell'operazione (5.14.3) prende il nome di *prodotto semidiretto* di G_1 e G_2 tramite l'omomorfismo Φ . Esso si indica con

$$G_1 \coprod_{\Phi} G_2 .$$

Vale il seguente teorema, che generalizza l'analogo nel caso dei prodotti diretti. \square

5.14.18 TEOREMA. *Siano N ed H due sottogruppi di un gruppo G . Se N è normale in G , inoltre $G = NH$ e $N \cap H = \{e\}$, allora G è isomorfo al prodotto semidiretto $N \coprod_{\Phi} H$, dove $\Phi : H \rightarrow \text{Aut}(N)$ è l'omomorfismo definito dalla*

$$\Phi(h)(n) = hn h^{-1} .$$

Dimostrazione. L'applicazione

$$\begin{aligned} \Psi : N \coprod_{\Phi} H &\longrightarrow G \\ (n, h) &\longmapsto nh \end{aligned}$$

è un omomorfismo suriettivo, il cui nucleo è il solo elemento neutro, quindi si tratta di un isomorfismo. Si lasciano i dettagli per esercizio (cfr. esercizio 5.14.13). \square

5.14.19 ESEMPIO. Siano $G = S_3$, $N = \langle (1, 2, 3) \rangle$ e $H = \langle (1, 2) \rangle$. Allora risulta

$$S_3 \cong N \coprod_{\Phi} H$$

dove $\Phi((1, 2))((1, 2, 3)) = (1, 2)(1, 2, 3)(1, 2)^{-1} = (1, 3, 2)$.

La corrispondenza tra $N \coprod_{\Phi} H$ e S_3 è la seguente:

$$\begin{aligned} (\text{id}, \text{id}) &\longrightarrow \text{id} \\ ((1, 2, 3), \text{id}) &\longrightarrow (1, 2, 3) \\ ((1, 3, 2), \text{id}) &\longrightarrow (1, 3, 2) \\ (\text{id}, (1, 2)) &\longrightarrow (1, 2) \\ ((1, 2, 3), (1, 2)) &\longrightarrow (1, 3) \\ ((1, 3, 2), (1, 2)) &\longrightarrow (2, 3) . \quad \square \end{aligned}$$

 **ESERCIZI.**

1. Si provi che il prodotto diretto di due gruppi (definizione 5.14.1) è un gruppo.
2. Si provino tutti i dettagli del teorema 5.14.3.
3. A quale gruppo è isomorfo $\mathbb{Z}_3 \times \mathbb{Z}_8$?
4. Si dica se il gruppo ciclico \mathbb{Z}_{16} è o no isomorfo al prodotto diretto $\mathbb{Z}_4 \times \mathbb{Z}_4$.
5. Si dica se $(\mathbb{Q}, +)$ è o no prodotto diretto di due suoi sottogruppi propri.
6. Si provi che un gruppo di ordine 15 è necessariamente ciclico.
7. Si provi che $U(\mathbb{Z}_7)$ è un prodotto diretto. Si dica poi se è un gruppo ciclico.
8. Si determinino i possibili ordini degli elementi del prodotto diretto $\mathbb{Z} \times \mathbb{Z}_6$. Si dica se si tratta di un gruppo ciclico. Cosa si può dire di $\mathbb{Z} \times \mathbb{Z}$? È ciclico?
9. Quali tra i seguenti gruppi dello stesso ordine,

$$\mathbb{Z}_{16}, \quad \mathbb{Z}_8 \times \mathbb{Z}_2, \quad \mathbb{Z}_4 \times \mathbb{Z}_4, \quad \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

sono isomorfi?

10. Si determinino i periodi degli elementi di $\mathbb{Z}_2 \times D_5$.
11. Si dica se S_4 è prodotto diretto di due suoi sottogruppi non banali.
12. Sia $G = H \times K$ prodotto diretto dei due gruppi H e K . Indicati con $Z(H)$ e $Z(K)$ i centri di H e K rispettivamente, si dica se è vera o no la seguente uguaglianza:

$$Z(H \times K) = Z(H) \times Z(K),$$

avendo indicato con $Z(H \times K)$ il centro di $H \times K$. Nel caso in cui l'uguaglianza sia vera, la si provi.

13. Si provino tutti i dettagli della dimostrazione del teorema 5.14.18.
14. Si provi che il gruppo E_2 di tutti i movimenti rigidi del piano è prodotto semidiretto del gruppo ortogonale $O_2(\mathbb{R})$ e del gruppo T delle traslazioni.

 **CONTROLO.**

1. Si elenchi le condizioni perché un gruppo sia prodotto diretto di due gruppi.
2. Come è legato il periodo di un elemento (g_1, g_2, \dots, g_k) di un prodotto diretto al periodo dei singoli g_i ?
3. Che cosa è il prodotto semidiretto di due gruppi? In quali casi coincide con il prodotto diretto?

5.15. Gruppi risolubili

In questo paragrafo daremo dei risultati su una classe di gruppi, chiamati gruppi risolubili. Tali gruppi hanno questo nome perché, come vedremo, sono collegati al problema della "risoluzione" di equazioni algebriche. Cominciamo con una definizione.

5.15.1 DEFINIZIONE. Sia G un gruppo. Dicesi *commutatore* di due elementi x e y di G , e si indica con $[x, y]$, l'elemento

$$[x, y] \stackrel{\text{def}}{=} xyx^{-1}y^{-1}.$$

Si definisce *sottogruppo commutatore* o *sottogruppo derivato* di G il sottogruppo, che si denota con G' , generato da tutti i commutatori. Quindi

$$G' \stackrel{\text{def}}{=} \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle. \quad \square$$

Il commutatore $[x, y]$ coincide con l'elemento neutro di G se e solo se $xy = yx$. Quindi G è abeliano se e solo se $G' = \{e\}$.

Ogni elemento di G' è della forma $a_1^{h_1}a_2^{h_2}\cdots a_t^{h_t}$, dove a_j è del tipo $xyx^{-1}y^{-1}$, $h_j = \pm 1$ e t è un intero positivo. Se si osserva poi che l'inverso di un commutatore è ancora un commutatore, allora si vede che G' è costituito da *prodotti* di commutatori.

Calcoliamo il derivato S'_3 di S_3 . Risulta

$$\text{id} = (1, 2)\text{id}(1, 2)^{-1}\text{id}^{-1} \in S'_3$$

$$(1, 2, 3) = (1, 2)(1, 2, 3)(1, 2)^{-1}(1, 2, 3)^{-1} \in S'_3$$

$$(1, 3, 2) = (1, 2)(1, 3, 2)(1, 2)^{-1}(1, 3, 2)^{-1} \in S'_3.$$

Quindi $A_3 \subseteq S'_3$. D'altra parte ogni commutatore è una permutazione pari, quindi $S'_3 \subseteq A_3$. Quindi il commutatore di S_3 è il sottogruppo alterno A_3 .

5.15.2 PROPOSIZIONE. *Sia G un gruppo. Allora*

- (a) *il derivato G' è un sottogruppo normale, e il quoziente G/G' è abeliano;*
- (b) *se $N \trianglelefteq G$, allora G/N è abeliano se e solo se $G' \leq N$, ossia G' è il più piccolo sottogruppo normale di G tale che il quoziente sia abeliano.*
- (c) *se N è un sottogruppo normale di G , allora anche N' è un sottogruppo normale di G .*

Dimostrazione. (a) Si tratta di provare che per ogni $x \in G'$ e per ogni $g \in G$ risulta $gxg^{-1} \in G'$. Basta provare (perché?) che il coniugato di un commutatore è ancora un commutatore. Sia $x = aba^{-1}b^{-1}$. Allora

$$\begin{aligned} gxg^{-1} &= g(aba^{-1}b^{-1})g^{-1} = \underbrace{gag^{-1}}_e \underbrace{gbg^{-1}}_e \underbrace{ga^{-1}}_e \underbrace{g^{-1}gb^{-1}g^{-1}}_e \\ &= (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \\ &= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} \in G'. \end{aligned}$$

Proviamo ora che G/G' è abeliano: siano $G'x$ e $G'y$ due elementi di G/G' . Allora $G'x \cdot G'y = G'xy = G'yx = G'y \cdot G'x$.

(b) Basta osservare che

$$Nxy = Nyx \iff Nxyx^{-1}y^{-1} = N \iff xyx^{-1}y^{-1} \in N.$$

(c) Basta provare che $gnmn^{-1}m^{-1}g^{-1}$ sta in N' per ogni $g \in G$ e ogni $n, m \in N$. Infatti

$$\begin{aligned} gnmn^{-1}m^{-1}g^{-1} &= gng^{-1}gm\cancel{g^{-1}}gn^{-1}\cancel{g^{-1}}gm^{-1}\cancel{g^{-1}} \\ &= \underbrace{gng^{-1}}_{\in N} \underbrace{gm}_{\in N} \underbrace{\cancel{g^{-1}}}_{\in N} \underbrace{gn^{-1}\cancel{g^{-1}}}_{\in N} \underbrace{gm^{-1}\cancel{g^{-1}}}_{\in N} \\ &= gng^{-1}gm(gng^{-1})^{-1}(gmg^{-1})^{-1} \in N'. \quad \square \end{aligned}$$

Partendo ora da G' si può definire il sottogruppo commutatore di G' , ossia $(G')'$: lo indicheremo con $G^{(2)}$. Si tratta di un sottogruppo di G normale in G (e quindi anche in G'). In generale si definisce il sottogruppo commutatore $G^{(n)}$ di ordine n come il gruppo $(G^{(n-1)})'$. Ogni $G^{(k)}$ è un sottogruppo normale in G ed è tale che $G^{(k-1)}/G^{(k)}$ è abeliano.

Fatte queste premesse, passiamo a definire il concetto di gruppo risolubile.

5.15.3 DEFINIZIONE. Un gruppo G si dice *risolubile* se è possibile trovare una catena finita di sottogruppi M_i

$$G = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_s = \{e\}$$

tale che ciascuno degli M_i sia normale nel precedente M_{i-1} e ogni quoziente M_{i-1}/M_i sia abeliano. \square

5.15.4 ESEMPI DI GRUPPI RISOLUBILI.

- (a) Ogni gruppo abeliano G è risolubile: basta prendere come catena la catena costituita dai due soli sottogruppi G e $\{e\}$.
- (b) Il gruppo simmetrico S_3 è risolubile: basta prendere la catena

$$S_3 \supset A_3 \supset \{e\}.$$

- (c) Il gruppo simmetrico S_4 è risolubile: basta prendere la catena

$$S_4 \supset A_4 \supset V \supset \{e\}$$

dove $V = \{\text{id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$.

- (d) Ogni gruppo di ordine pq (p e q primi) è risolubile. Se $p = q$, G è un gruppo abeliano (cfr. teorema 5.12.4). Possiamo quindi supporre $p < q$. In base ai teoremi di Sylow, esiste un q -sottogruppo di Sylow N normale. Allora basta prendere la catena

$$G \supset N \supset \{e\}.$$

Si completino i dettagli. \square

Un gruppo *semplice non abeliano* è ovviamente *non risolubile*.

Diamo qui di seguito una caratterizzazione dei gruppi risolubili che coinvolga i sottogruppi derivati, che abbiamo definito sopra.

5.15.5 PROPOSIZIONE. *Un gruppo G è risolubile se e solo se esiste un $m \in \mathbb{N}$ tale che $G^{(m)} = \{e\}$.*

Dimostrazione. Supponiamo che sia $G^{(m)} = \{e\}$ per qualche m . Posto $M_i = G^{(i)}$, consideriamo la catena

$$M_0 = G \supset M_1 \supset M_2 \supset \cdots \supset M_m = \{e\}.$$

Dato che ogni M_i è normale in G , lo sarà a maggior ragione in ogni M_{i-1} . Inoltre

$$M_{i-1}/M_i = G^{(i-1)}/G^{(i)} = G^{(i-1)}/(G^{(i)})'$$

e quindi ogni quoziente è abeliano; G è dunque risolubile.

Viceversa, supponiamo G risolubile. Esiste allora una catena finita di sottogruppi

$$G = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_s = \{e\}$$

tale che, per ogni i , $M_i \triangleleft M_{i-1}$ e M_{i-1}/M_i è abeliano. Ma allora in base alla proposizione 5.15.2 risulta $M'_{i-1} \subseteq M_i$. Si ha quindi la seguente situazione:

$$M_1 \supset M'_0 = G'$$

$$M_2 \supset M'_1 \supset G^{(2)} \quad (\text{dall'inclusione precedente, passando ai derivati})$$

...

$$M_i \supset M'_{i-1} \supset G^{(i)}$$

...

$$M_s = \{e\} \supset M'_{s-1} \supset G^{(s)}.$$

L'ultima relazione dice che $G^{(s)} = \{e\}$. \square

5.15.6 COROLLARIO. *Se un gruppo è risolubile, tale è anche ogni suo sottogruppo e ogni sua immagine omomorfa.*

Abbiamo visto che ogni gruppo semplice non abeliano non è risolubile. Il prossimo teorema offrirà una classe di gruppi (non semplici e non abeliani) non risolubili: tali gruppi saranno fondamentali nello studio della risolubilità di equazioni algebriche.

5.15.7 TEOREMA. *Per ogni $n \geq 5$ il gruppo simmetrico S_n non è risolubile.*

Dimostrazione. Sia $n \geq 5$. Proveremo il teorema facendo vedere che, per ogni k , $\mathcal{S}_n^{(k)}$ contiene tutti i 3-cicli. Il risultato seguirà dalla proposizione 5.15.5.

Proviamo che, se N è un sottogruppo normale di \mathcal{S}_n con $n \geq 5$ che contiene tutti i 3-cicli, allora anche N' contiene tutti i 3-cicli. Se N contiene tutti i 3-cicli, conterrà in particolare $(1, 2, 3)$ e $(1, 4, 5)$: si osservi che stiamo sfruttando il fatto che $n \geq 5$, e quindi si possono usare cinque simboli distinti. Allora N' conterrà il commutatore $(1, 2, 3)(1, 4, 5)(1, 2, 3)^{-1}(1, 4, 5)^{-1} = (1, 2, 3)(1, 4, 5)(1, 3, 2)(1, 5, 4) = (1, 2, 4)$. Ora, essendo, in base al punto (c) della proposizione 5.15.2, $N' \trianglelefteq \mathcal{S}_n$, se contiene un 3-ciclo conterrà l'intera classe coniugata, ossia tutti i 3-cicli.

Partiamo quindi da $N = \mathcal{S}_n$ (che è certamente normale in \mathcal{S}_n). Allora \mathcal{S}'_n contiene tutti i 3-cicli. Essendo $\mathcal{S}'_n \leq \mathcal{S}_n$, il suo derivato $\mathcal{S}^{(2)}_n$ ($\trianglelefteq \mathcal{S}_n$) conterrà tutti i 3-cicli, e così via, ogni $\mathcal{S}_n^{(k)}$ conterrà tutti i 3-cicli. \square

 ATTENZIONE. L'ipotesi $n \geq 5$ è essenziale, dato che abbiamo visto che per $n < 5$ \mathcal{S}_n è risolubile. \square

ESERCIZI.

- Si provi che un gruppo risolubile è semplice se e solo se è ciclico di ordine un numero primo.
- Si provi che per $n \geq 5$ il gruppo alterno A_n è semplice.
- Si provi che per $n \geq 5$ il gruppo simmetrico \mathcal{S}_n non è risolubile sfruttando il risultato dell'esercizio precedente.
- Sia G un gruppo che possiede un sottogruppo normale N risolubile tale che anche G/N sia risolubile. Provare che G è risolubile.
- Si decida se un gruppo di ordine 91 è risolubile o no.



CONTROLLO.

- Il sottogruppo derivato di un gruppo G è
- Definire e caratterizzare i gruppi risolubili.
- Per quali valori di n i gruppi \mathcal{S}_n sono risolubili?

5.16. I gruppi di simmetria delle decorazioni

Abbiamo già studiato i gruppi delle simmetrie di un poligono regolare. Studieremo ora i gruppi di simmetria di figure arbitrarie, per poi studiare i gruppi di simmetria delle "decorazioni".

Oltre ai *gruppi diedrali* (che, come abbiamo visto, compaiono come gruppi di simmetria di poligoni regolari) non è difficile vedere che anche i *gruppi ciclici* compaiono come gruppi di simmetria di particolari figure, ad esempio la figura 5.17(a). Le simmetrie che mutano in sé questa figura sono le quattro rotazioni di $0, \pi/2, \pi$, e $3\pi/2$ radianti.

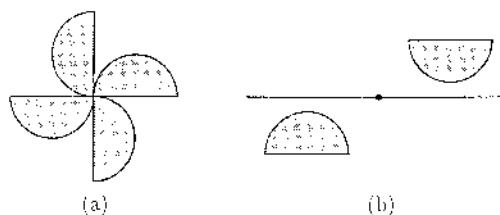


FIGURA 5.17

Non ogni gruppo finito può essere pensato come gruppo di simmetria di una figura piana. Faremo vedere che lo possono essere solamente i gruppi già nominati, cioè i gruppi diedrali e i gruppi ciclici.

Ricordiamo che l'insieme delle isometrie (o movimenti rigidi) del piano forma un gruppo, il gruppo euclideo E_2 . Le *traslazioni* ne sono un sottogruppo, T , e il sottoinsieme costituito dalle *rotazioni* attorno all'origine e dalle *riflessioni* rispetto a rette passanti per l'origine forma un sottogruppo, detto *gruppo ortogonale*, O_2 : come abbiamo visto nel §5.1, esso è rappresentato da matrici ortogonali. Il sottogruppo O_2 non è altro che lo stabilizzatore dell'origine rispetto all'azione naturale di E_2 sul piano. Il sottoinsieme delle sole rotazioni costituisce a sua volta un sottogruppo di O_2 , che si indica come abbiamo già visto con SO_2 (gruppo ortogonale speciale), rappresentato dalle matrici ortogonali con determinante uguale ad 1. Ogni isometria del piano è o una rotazione seguita da una traslazione, oppure una riflessione seguita da una traslazione. Quest'ultimo movimento ad esempio è illustrato in figura 5.17 (b).

Nostro scopo ora è quello di classificare i sottogruppi finiti di isometrie del piano, o, equivalentemente, i sottogruppi finiti di O_2 .

Sussiste il seguente teorema.

5.16.1 TEOREMA. *I sottogruppi finiti di O_2 sono i gruppi ciclici e i gruppi diedrali, cioè i gruppi \mathbb{Z}_n e D_n , al variare di $n \in \mathbb{N}$.*

Dimostrazione. Sia G un sottogruppo non banale di O_2 . Supponiamo innanzitutto che G sia completamente contenuto in SO_2 , sia cioè costituito interamente da rotazioni. Indichiamo con R_ϕ la matrice che rappresenta la rotazione in senso antiorario dell'angolo ϕ , con $0 \leq \phi < 2\pi$. Sia $R_\mu \in G$ tale che μ sia positivo e il più piccolo possibile (tale angolo esiste, perché G è finito). Presa allora una qualunque R_ϕ in G , esisterà un intero k tale che $k\mu \leq \phi < (k+1)\mu$. Ma allora $R_{\phi-k\mu} = R_\phi \circ (R_\mu)^{-k}$ sta in G , e risulta $0 \leq \phi - k\mu < \mu$. Per non contraddirre la minimialità di μ , deve essere $\phi - k\mu = 0$, cioè $R_\phi = (R_\mu)^k$. G è generato da R_μ , ed è quindi ciclico. Supponiamo ora che G non sia contenuto tutto in SO_2 , e sia $N = G \cap SO_2$: si veda figura 5.18.

Dato che N è costituito dalle matrici di G con determinante uguale ad 1, esso ha indice 2 in G e, per quanto dimostrato nella prima parte del teorema,

è ciclico. Scegliamo un generatore R di N , e un elemento $S \in G \setminus N$; S rappresenta una riflessione, e pertanto ha periodo 2. Se $R = I$, allora G consiste dei soli elementi I e S , ed è quindi ciclico di ordine 2. Altrimenti, indicato con $n \geq 2$ il periodo di R , G è costituito dai seguenti elementi:

$$\{I, R, R^2, \dots, R^{n-1}, S, RS, R^2S, \dots, R^{n-1}S\}$$

con $R^n = 1$, $S^2 = 1$ e $SR = R^{-1}S$. G è pertanto il gruppo diedrale D_n . \square

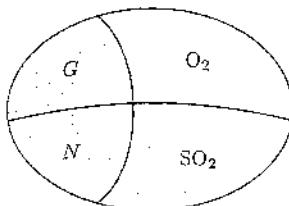


FIGURA 5.18

Per completezza, enunciamo anche il seguente risultato, anche se non avremo occasione di utilizzarlo.

5.16.2 PROPOSIZIONE. *Un sottogruppo finito di SO_3 è isomorfo o ad un gruppo ciclico, o ad un gruppo diedrale, oppure al gruppo delle simmetrie di rotazione di uno dei solidi regolari (o solidi platonici): tetraedro, cubo, ottaedro, dodecaedro, icosaedro.*

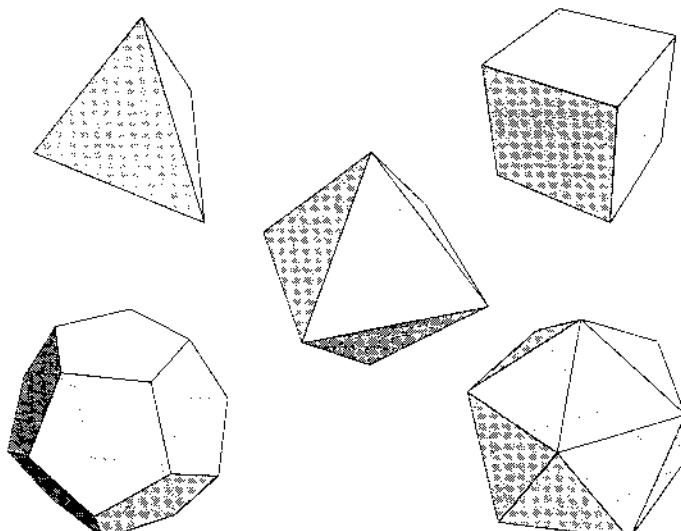


FIGURA 5.19. I solidi platonici.

Classificheremo ora i gruppi che sono gruppi di simmetria di figure del piano che si ripetono indefinitamente nel piano, cioè i gruppi di simmetria delle *decorazioni* (o anche, come si chiamano espressivamente, delle *carte da parati*). Li chiameremo semplicemente *gruppi delle decorazioni*. Un esempio di decorazione è mostrato in figura 5.20.

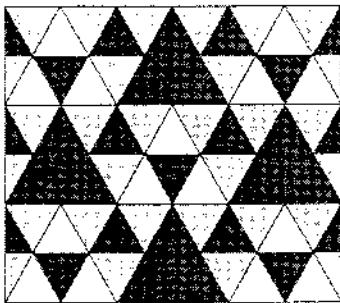


FIGURA 5.20

Ricordando che ogni isometria del piano è individuata da una coppia (\mathbf{v}, A) , dove \mathbf{v} rappresenta il vettore traslazione e A è la matrice ortogonale corrispondente alla rotazione o alla riflessione, consideriamo l'applicazione π da E_2 in O_2 così definita:

$$\pi((\mathbf{v}, A)) \stackrel{\text{def}}{=} A .$$

Tale applicazione è un omomorfismo di gruppi, come si verifica immediatamente. Il nucleo di π consiste di tutte le isometrie del tipo (\mathbf{v}, I) , cioè le traslazioni. Se G è un sottogruppo di E_2 , poniamo

$$H \stackrel{\text{def}}{=} G \cap T, \quad J \stackrel{\text{def}}{=} \pi(G) .$$

H verrà chiamato il *sottogruppo delle traslazioni di G* , e J il *gruppo puntuale o cristalografico di G* . I gruppi G che vogliamo studiare, cioè i gruppi (di simmetria) delle decorazioni, sono quindi gruppi tali che il loro sottogruppo H delle traslazioni è generato da due traslazioni indipendenti, mentre il loro gruppo puntuale J è finito.

5.16.3 DEFINIZIONE. Si dice *reticollo generato da due vettori \mathbf{v} e \mathbf{w}* l'insieme L di tutte le combinazioni lineari

$$m\mathbf{v} + n\mathbf{w} \quad \text{con } m, n \text{ in } \mathbb{Z}. \quad \square$$

Sia $\mathcal{O}(0)$ l'orbita dell'origine del piano \mathbb{R}^2 sotto l'azione di H ; $\mathcal{O}(0)$ conterrà sicuramente due vettori indipendenti. Sceglieremo un vettore non nullo \mathbf{a} di lunghezza minima in $\mathcal{O}(0)$ e successivamente un vettore \mathbf{b} in $\mathcal{O}(0)$ di lunghezza minima tra tutti quelli non paralleli ad \mathbf{a} .

5.16.4 PROPOSIZIONE. *L'orbita $\mathcal{O}(0)$ coincide con il reticolo L generato da a e b .*

Dimostrazione. Chiaramente L è contenuto in $\mathcal{O}(0)$ perché $\mathcal{O}(0)$ è un sottogruppo di \mathbb{R}^2 e contiene a e b . Faremo vedere che non può esistere un elemento x in $\mathcal{O}(0)$ ma non in L . Il reticolo L è mostrato in figura 5.21.

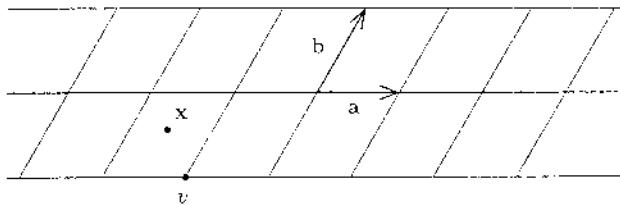


FIGURA 5.21

Il vettore x apparterrà ad un parallelogramma del reticolo L . Sia v il vertice del parallelogramma più vicino a x . Allora il vettore $x - v$ non è il vettore nullo, è diverso dai vettori a e b , e la sua lunghezza è minore di $|b|$. Dato che x e v stanno in $\mathcal{O}(0)$, anche $x - v$ sta in $\mathcal{O}(0)$ e pertanto, per la scelta di a , sarà $|a| \leq |x - v| < |b|$. Ma allora $x - v$ non è parallelo ad a , e perciò viene contraddetta la scelta di b . Quindi un tale punto x non può esistere e pertanto $\mathcal{O}(0) \equiv L$. \square

A seconda della forma dei parallelogrammi del reticolo, i possibili reticolati di una decorazione del piano sono dei seguenti *cinque* tipi:

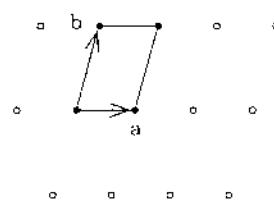


FIGURA 5.22

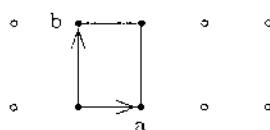


FIGURA 5.23

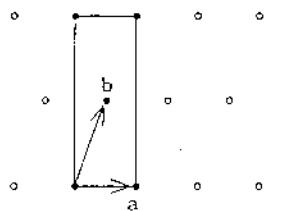


FIGURA 5.24

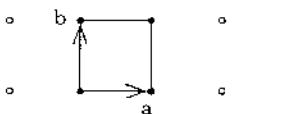


FIGURA 5.25

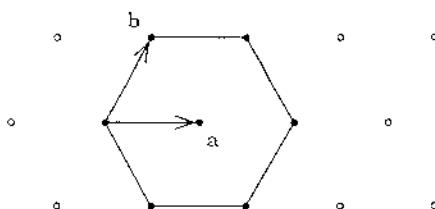


FIGURA 5.26

Infatti, sostituendo, se necessario, \mathbf{b} con $-\mathbf{b}$, si ha innanzitutto

$$|\mathbf{a} - \mathbf{b}| \leq |\mathbf{a} + \mathbf{b}|.$$

Si hanno quindi le seguenti possibilità:

- $|\mathbf{a}| < |\mathbf{b}| < |\mathbf{a} - \mathbf{b}| < |\mathbf{a} + \mathbf{b}|$
- $|\mathbf{a}| < |\mathbf{b}| < |\mathbf{a} - \mathbf{b}| = |\mathbf{a} + \mathbf{b}|$
- $|\mathbf{a}| < |\mathbf{b}| = |\mathbf{a} - \mathbf{b}| < |\mathbf{a} + \mathbf{b}|$
- $|\mathbf{a}| = |\mathbf{b}| < |\mathbf{a} - \mathbf{b}| = |\mathbf{a} + \mathbf{b}|$
- $|\mathbf{a}| = |\mathbf{b}| = |\mathbf{a} - \mathbf{b}| < |\mathbf{a} + \mathbf{b}|$
- $|\mathbf{a}| = |\mathbf{b}| < |\mathbf{a} - \mathbf{b}| < |\mathbf{a} + \mathbf{b}|$

Queste possibilità corrispondono alle situazioni precedenti. Infatti l'ultima disegualanza rientra nel caso del rettangolo centrato, con lati $a - b$ e $a + b$ (si veda infatti la figura 5.27).

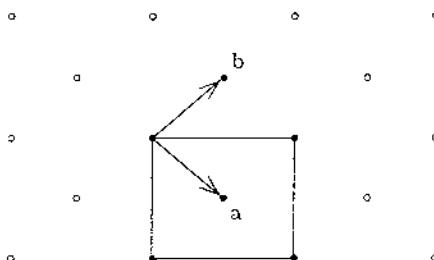


FIGURA 5.27

Sussiste inoltre il seguente importante risultato.

5.16.5 PROPOSIZIONE. *Il periodo di una rotazione in un gruppo delle decorazioni può essere solamente 2, 3, 4 o 6.*

Dimostrazione. Dato che il gruppo puntuale delle decorazioni è finito, ogni rotazione R avrà periodo finito. Sia n il suo ordine. Possiamo allora supporre che la matrice di rotazione sia

$$R = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}.$$

Sia al solito a un vettore non nullo di lunghezza minima in L . Allora anche il vettore $R(a)$, cioè il vettore ruotato mediante R , sta in L . Se fosse $n > 6$, allora sarebbe $2\pi/n < \pi/3$, per cui $R(a) - a$ avrebbe lunghezza minore di a e sta in L , e questo contraddice la scelta di a (si veda la figura 5.28).

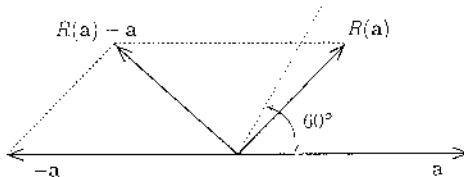


FIGURA 5.28

Anche il caso $n = 5$ deve essere escluso, perché in questo caso l'angolo tra $R^2(a)$ (cioè a ruotato due volte mediante la rotazione R) e $-a$ vale 36° , e allora è il vettore ($\in L$) $R^2(a) + a$ ad avere lunghezza minore di a .

Abbiamo così provato che il gruppo puntuale di una decorazione è generato da una rotazione di uno dei seguenti angoli: $0, \pi, 2\pi/3, \pi/2, \pi/3$ e da una (eventuale) riflessione. \square

Ebbene, con queste informazioni a disposizione, si può dimostrare il seguente teorema.

5.16.6 TEOREMA. *Esistono in tutto 17 gruppi di decorazioni non isomorfi.*

Chi volesse approfondire lo studio dei gruppi delle decorazioni del piano è invitato a studiare i disegni dell'artista olandese M.C. Escher (1898-1972) che uniscono in modo affascinante arte e rigore matematico. Una fonte preziosa di decorazioni che si prestano ad essere studiate dal punto di vista della teoria dei gruppi è l'Alhambra (Granada, sec. XIII e XIV). Un approfondito studio dei gruppi di simmetria delle decorazioni si trova in [40]. Gran parte del contenuto di questo paragrafo è tratto da [3].



ESERCIZI.

1. Osservate delle carte da parati o delle stoffe con disegni ripetitivi e cercate di scoprire tutte le simmetrie, e quindi i gruppi associati.
2. Esaminate i disegni di Escher e studiatene le simmetrie.

5.17. Classificazione dei gruppi abeliani finiti

Con le nozioni acquisite nei paragrafi precedenti siamo in grado di enunciare e provare in parte il *teorema fondamentale sui gruppi abeliani finiti*, in base al quale, dato comunque un intero positivo n , saremo in grado di stabilire chi sono e quanti sono i gruppi abeliani di ordine n , e stabilire se due gruppi abeliani di uno stesso ordine sono isomorfi o no.

Ricordiamo (cfr. definizione 5.12.2) che un p -gruppo è un gruppo che ha come ordine una potenza di p . Ogni elemento di un p -gruppo ha ovviamente come periodo una potenza di p . Ad esempio, ogni gruppo ciclico di ordine un numero primo p è un p -gruppo.

N.B. Si può anche definire p -gruppo un gruppo tale che ogni suo elemento abbia come ordine una potenza di p . In tal caso si includono anche gruppi infiniti. Nel caso finito le due definizioni sono equivalenti (cfr. esercizio 5.12.3).

5.17.1 TEOREMA. *Sia G un gruppo abeliano finito. Per ogni primo p tale che $p \mid |G|$ poniamo*

$$\Sigma_p \stackrel{\text{def}}{=} \{x \in G \text{ che hanno come ordine una potenza di } p\}.$$

Allora

- (a) ogni Σ_p è un sottogruppo di G (che è un p -sottogruppo di G);

(b) G è prodotto diretto di tutti i Σ_p , al variare di p tra tutti i divisori primi di $|G|$.

Dimostrazione. Risulta

$$\Sigma_p = \{x \in G \mid x^{p^s} = e \text{ per qualche } s\}.$$

Il primo punto è facile da provare (si ricordi che G è abeliano!). Passiamo quindi a provare il secondo punto. Sia x un qualunque elemento di G . Allora x avrà un certo periodo n , con $n \mid |G|$. Sia $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, p_i primi distinti e $\alpha_i \geq 1$, per ogni $i = 1, \dots, r$. Posto $q_i = n/(p_i^{\alpha_i})$, chiaramente risulta $(q_1, q_2, \dots, q_r) = 1$; esistono quindi degli interi k_i tali che

$$1 = k_1 q_1 + k_2 q_2 + \cdots + k_r q_r.$$

Allora

$$x = x^1 = x^{k_1 q_1 + k_2 q_2 + \cdots + k_r q_r} = x^{k_1 q_1} x^{k_2 q_2} \cdots x^{k_r q_r}.$$

Ora,

$$(x^{q_i})^{p_i^{\alpha_i}} = x^n = 1 \quad \forall i = 1, \dots, r.$$

Quindi $x^{q_i} \in \Sigma_{p_i}$. Ma allora anche $x^{k_i q_i} \in \Sigma_{p_i}$. Abbiamo quindi dimostrato che ogni x in G si scrive come prodotto di elementi di Σ_{p_i} , cioè

$$G = \Sigma_{p_1} \Sigma_{p_2} \cdots \Sigma_{p_k}.$$

Per provare che $G \cong \Sigma_{p_1} \times \Sigma_{p_2} \times \cdots \times \Sigma_{p_k}$, basta ora provare (cfr. teorema 5.14.16) che

$$\Sigma_{p_i} \cap \Sigma_{p_1} \Sigma_{p_2} \cdots \widehat{\Sigma}_{p_i} \cdots \Sigma_{p_k} = \{e\}.$$

Ma questo è ovvio, perché non può esistere un elemento che sta contemporaneamente in Σ_{p_i} e in $\Sigma_{p_1} \Sigma_{p_2} \cdots \widehat{\Sigma}_{p_i} \cdots \Sigma_{p_k}$, perché dovrebbe avere periodo al tempo stesso una potenza di p_i e un numero coprimo con p_i . \square

Abbiamo così provato che ogni gruppo abeliano finito G è isomorfo a $\Sigma_{p_1} \times \Sigma_{p_2} \times \cdots \times \Sigma_{p_k}$, dove

$$\Sigma_{p_i} = \{x \in G \mid x^{p_i^{s_i}} = e \text{ per qualche } s_i\}.$$

Ciascuno dei Σ_{p_i} prende il nome di *componente primaria* di G .

Dovremo ora studiare i singoli fattori Σ_{p_i} della decomposizione.

Sussiste il seguente teorema.

5.17.2 TEOREMA. *Sia Σ_p un p -gruppo abeliano finito. Allora Σ_p è un prodotto diretto di gruppi ciclici (di ordine una potenza di p).*

Dimostrazione. Daremo solo un cenno della dimostrazione, senza entrare nei dettagli. Sia s uno qualunque degli elementi di Σ_p di ordine massimo p^α , e sia T un sottogruppo massimale rispetto alla condizione di avere intersezione banale con il sottogruppo $\langle s \rangle$ generato da s , cioè

$$\langle s \rangle \cap T = \{e\}.$$

Si dimostra (tralasciamo la dimostrazione) che

$$\langle s \rangle T = \Sigma_p.$$

Questo ci assicura che

$$\Sigma_p \cong \langle s \rangle \times T.$$

La dimostrazione del teorema procede ora per induzione. Partiamo da T , e scegliamo in T un elemento s' di ordine massimo. Sia T' un sottogruppo di T massimale rispetto alla condizione

$$T' \cap \langle s' \rangle = \{e\}.$$

Così proseguendo si arriva per forza alla conclusione che

$$\Sigma_p \cong \langle s_1 \rangle \times \langle s_2 \rangle \times \cdots \times \langle s_l \rangle,$$

cioè Σ_p è prodotto diretto di gruppi ciclici. \square

Abbiamo così dimostrato il seguente teorema.

5.17.3 TEOREMA. *Ogni gruppo abeliano finito G è prodotto diretto di gruppi ciclici i cui ordini sono potenze dei primi che compaiono nella fattorizzazione di $n = |G|$. Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, allora*

$$G = \underbrace{\mathbb{Z}_{p_1^{a_{1,1}}} \times \mathbb{Z}_{p_1^{a_{1,2}}} \times \cdots \times \mathbb{Z}_{p_1^{a_{1,s}}}}_{\Sigma_{p_1}} \times \underbrace{\mathbb{Z}_{p_2^{a_{2,1}}} \times \mathbb{Z}_{p_2^{a_{2,2}}} \times \cdots \times \mathbb{Z}_{p_2^{a_{2,t}}}}_{\Sigma_{p_2}} \times \cdots \times \underbrace{\mathbb{Z}_{p_k^{a_{k,1}}} \times \mathbb{Z}_{p_k^{a_{k,2}}} \times \cdots \times \mathbb{Z}_{p_k^{a_{k,r}}}}_{\Sigma_{p_k}}$$

dove per ogni $i = 1, \dots, k$ gli interi $a_{i,j}$ sono tali che $\sum_j a_{i,j} = \alpha_i$ e sono ordinati in modo tale che $a_{i,j(i)} \geq \cdots \geq a_{i,2} \geq a_{i,1} > 0$.

Abbiamo così provato un teorema di esistenza di una tale decomposizione.

5.17.4 DEFINIZIONE. Gli interi $p_i^{\alpha_{i,j}}$ che compaiono nella decomposizione si chiamano i *divisori elementari* di G . Per ogni fissata componente primaria Σ_{p_i} , $i = 1, \dots, k$, gli esponenti $a_{i,j(i)}$ si chiamano gli *invarianti* di Σ_{p_i} . \square

Tali interi sono determinati univocamente dal gruppo G e lo determinano univocamente, nel senso che due gruppi abeliani dello stesso ordine sono isomorfi se e solo se hanno gli stessi divisori elementari e gli stessi invarianti. Ci limitiamo ad enunciare questo risultato.

5.17.5 TEOREMA FONDAMENTALE SUI GRUPPI ABELIANI FINITI. *Sia G un gruppo abeliano finito di ordine $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Allora*

- (a) *G è isomorfo ad un prodotto diretto di gruppi ciclici di ordini potenze dei primi che compaiono nella fattorizzazione di G :*

$$G = \underbrace{\mathbb{Z}_{p_1^{a_{1,1}}} \times \mathbb{Z}_{p_1^{a_{1,2}}} \times \cdots \times \mathbb{Z}_{p_1^{a_{1,t}}}}_{\Sigma_{p_1}} \times \underbrace{\mathbb{Z}_{p_2^{a_{2,1}}} \times \mathbb{Z}_{p_2^{a_{2,2}}} \times \cdots \times \mathbb{Z}_{p_2^{a_{2,t}}}}_{\Sigma_{p_2}} \times \cdots$$

dove per ogni $i = 1, \dots, k$ gli interi $a_{i,j}$ sono tali che $\sum_j a_{i,j} = \alpha_i$ e sono ordinati in modo tale che $a_{i,j(i)} \geq \cdots \geq a_{i,2} \geq a_{i,1} > 0$.

- (b) *Tale fattorizzazione è unica, nel senso che se due gruppi abeliani finiti sono isomorfi, allora hanno gli stessi divisori elementari.*

Il teorema fondamentale sui gruppi abeliani finiti ci offre quindi la struttura di tutti i gruppi abeliani finiti.

Il seguente corollario ci garantisce che per i gruppi abeliani finiti il teorema di Lagrange si inverte.

5.17.6 COROLLARIO. *Se m divide l'ordine di un gruppo abeliano finito G , allora G contiene un sottogruppo di ordine m .*

Dato un intero N , per contare quanti sono i gruppi abeliani che hanno quello come ordine, si deve vedere in quanti modi si riesce a fattorizzare ogni Σ_p della sua decomposizione come prodotto di gruppi ciclici (di ordine potenze di p). Cioè si deve contare in quanti modi si può scrivere

$$\Sigma_p = \mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \cdots \times \mathbb{Z}_{p^{n_s}}.$$

Si deve avere

$$|\Sigma_p| = p^n = p^{n_1} p^{n_2} p^{n_s} = p^{n_1+n_2+\cdots+n_s}.$$

Si tratta di contare in quanti modi si può scrivere n come somma di $n_1 + n_2 + \cdots + n_s$, con $n_1 \geq n_2 \geq \cdots \geq n_s$. Ma questo numero coincide con il numero $p(n)$ di partizioni di n . Quindi ogni Σ_p con $|\Sigma_p| = p^n$ si può scrivere in $p(n)$ modi come prodotto di gruppi ciclici di ordini le varie potenze di p . Ne segue che per determinare il numero di gruppi non isomorfi di un dato ordine N , basta procedere al modo seguente:

- (1) Si fattorizza N nel prodotto di potenze di primi distinti:

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

- (2) Risulta

$$p_1^{\alpha_1} = |\Sigma_{p_1}|, \quad p_2^{\alpha_2} = |\Sigma_{p_2}|, \quad \dots, \quad p_k^{\alpha_k} = |\Sigma_{p_k}|.$$

- (3) Si contano i diversi invarianti di ogni Σ_{p_i} , il che equivale a contare il numero $p(\alpha_i)$ di partizioni di ogni α_i .

- (4) Il numero totale di gruppi abeliani non isomorfi di ordine $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ è dato quindi da

$$p(\alpha_1)p(\alpha_2) \cdots p(\alpha_k).$$

Diamo qui di seguito alcuni esempi.

5.17.7 ESEMPIO. Determinare quanti sono i gruppi abeliani di ordine $N = 1620$ ed elencarli tutti.

Si ha $N = 2^2 \cdot 3^4 \cdot 5$.

Ogni G con $N = 1620$ elementi risulta decomposto nel prodotto diretto

$$G = \Sigma_2 \times \Sigma_3 \times \Sigma_5$$

dove

$$|\Sigma_2| = 2^2, \quad |\Sigma_3| = 3^4, \quad |\Sigma_5| = 5$$

e

$$p(\alpha_1) = p(2) = 2, \quad p(\alpha_2) = p(4) = 5, \quad p(\alpha_3) = p(1) = 1.$$

Quindi il numero totale di gruppi abeliani di ordine $N = 1620$ è dato da $p(2)p(4)p(1) = 10$.

Le diverse fattorizzazioni di Σ_2 sono

$$\mathbb{Z}_{2^2}, \quad \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Quelle di Σ_3 sono

$$\mathbb{Z}_{3^4}, \quad \mathbb{Z}_{3^3} \times \mathbb{Z}_3, \quad \mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2}, \quad \mathbb{Z}_{3^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3, \quad \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3.$$

E infine, Σ_5 si scrive solamente come \mathbb{Z}_5 . Ogni gruppo abeliano di ordine 1620 deve quindi esser isomorfo ad uno dei seguenti (tutti non isomorfi tra di loro):

Σ_2	\times	Σ_3	\times	Σ_5
\mathbb{Z}_1	\times	\mathbb{Z}_{81}	\times	\mathbb{Z}_5
\mathbb{Z}_1	\times	$\mathbb{Z}_{27} \times \mathbb{Z}_3$	\times	\mathbb{Z}_5
\mathbb{Z}_1	\times	$\mathbb{Z}_9 \times \mathbb{Z}_9$	\times	\mathbb{Z}_5
\mathbb{Z}_1	\times	$\mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	\times	\mathbb{Z}_5
\mathbb{Z}_4	\times	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	\times	\mathbb{Z}_5
$\mathbb{Z}_2 \times \mathbb{Z}_2$	\times	\mathbb{Z}_{81}	\times	\mathbb{Z}_5
$\mathbb{Z}_2 \times \mathbb{Z}_2$	\times	$\mathbb{Z}_{27} \times \mathbb{Z}_3$	\times	\mathbb{Z}_5
$\mathbb{Z}_2 \times \mathbb{Z}_2$	\times	$\mathbb{Z}_9 \times \mathbb{Z}_9$	\times	\mathbb{Z}_5
$\mathbb{Z}_2 \times \mathbb{Z}_2$	\times	$\mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	\times	\mathbb{Z}_5
$\mathbb{Z}_2 \times \mathbb{Z}_2$	\times	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	\times	\mathbb{Z}_5

5.17.8 ESEMPIO. Si dica quanti sono e chi sono tutti i gruppi abeliani di ordine $N = 1155$.

Risulta $N = 3 \cdot 5 \cdot 7 \cdot 11$. Ogni gruppo abeliano G di ordine $N = 1155$ si fattorizza nelle seguenti componenti primarie:

$$G = \Sigma_3 \times \Sigma_5 \times \Sigma_7 \times \Sigma_{11}$$

con

$$|\Sigma_3| = 3, \quad |\Sigma_5| = 5, \quad |\Sigma_7| = 7, \quad |\Sigma_{11}| = 11.$$

G risulta pertanto necessariamente il seguente gruppo:

$$G = \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}$$

ossia si tratta del gruppo ciclico di ordine 1155. Quindi esiste un solo gruppo abeliano di ordine 1155.

Questo è un fatto generale. Se $N = p_1 p_2 \cdots p_k$, con i p_i primi distinti, allora esiste un solo gruppo abeliano di ordine N , che è ovviamente il gruppo ciclico di quell'ordine. \square

5.17.9 OSSERVAZIONE. Si noti che, per quanto detto, il numero di gruppi abeliani non isomorfi di ordine, ad esempio, 3^4 uguaglia il numero di gruppi abeliani non isomorfi di ordine 5^4 , perché nel contare intervengono solamente gli esponenti: si hanno quindi in tutto cinque gruppi non isomorfi in entrambi i casi. Tuttavia, quando si devono poi elencare esplicitamente, allora ovviamente si dovrà tener conto del numero primo base della potenza (cioè $p_1 = 3$ nel primo caso e $p_2 = 5$ nel secondo).

Nel primo caso i gruppi saranno

$$\mathbb{Z}_{3^4}, \quad \mathbb{Z}_{3^3} \times \mathbb{Z}_3, \dots$$

e nel secondo caso

$$\mathbb{Z}_{5^4}, \quad \mathbb{Z}_{5^3} \times \mathbb{Z}_5, \dots \quad \square$$

ESERCIZI.

1. Si determinino tutti i gruppi abeliani dei seguenti ordini:

$$56, \quad 2100, \quad 800, \quad 45, \quad 27.$$

Per ciascuno dei gruppi trovati si determini l'ordine massimo dei suoi elementi.

2. Sia $U(\mathbb{Z}_{30})$ il gruppo degli elementi invertibili di \mathbb{Z}_{30} . Si determini la sua decomposizione in gruppi ciclici. In particolare si riconosca se è un gruppo ciclico.
3. Di un gruppo abeliano G si sa che ha ordine 72, che possiede un elemento di periodo 36, e che nessun suo sottogruppo è isomorfo a \mathbb{Z}_8 . Si può dire a chi è isomorfo G ?



ESERCIZI DI PROGRAMMAZIONE.

1. Si scriva un programma che determini, per ogni intero positivo n , il numero di gruppi abeliani non isomorfi di ordine n .



CONTROLLO.

1. Il prodotto diretto di gruppi ciclici finiti è un gruppo ciclico finito? È un gruppo abeliano? È vero che ogni gruppo abeliano finito è prodotto diretto di gruppi ciclici? Come sono legati gli ordini di tali gruppi ciclici all'ordine del gruppo?
2. Dato comunque un divisore m dell'ordine di un gruppo abeliano finito G esiste un sottogruppo di G che ha ordine m ?
3. Dire come si determina il numero di gruppi abeliani non isomorfi di un dato ordine n .

CAPITOLO 6

Campi e loro estensioni

...
*ora i miei fertili campi sono d'altri,
né per me trascinano i muli il dente dell'aratro
del tempo del mio viaggio funesto sopra il mare.*
Teognide, Lirici greci, trad. di S. Quasimodo.

In questo capitolo parleremo di vari tipi di ampliamenti o estensioni di campi: estensioni semplici, estensioni finite, algebriche, normali, ecc. Studieremo poi i campi finiti e dimostreremo il teorema di Wedderburn, secondo cui ogni corpo finito è un campo. Le nozioni sulle estensioni affrontate in questo capitolo verranno poi utilizzate nel prossimo.

6.1. Estensioni di campi

Il campo \mathbb{Q} dei razionali è un sottocampo del campo \mathbb{R} dei reali, e questo a sua volta è un sottocampo del campo \mathbb{C} dei complessi. Si dice anche che \mathbb{C} è un *ampliamento* o un'estensione di \mathbb{R} e di \mathbb{Q} , e così \mathbb{R} è un ampliamento o una estensione di \mathbb{Q} . In definitiva, appare naturale la seguente definizione.

6.1.1 DEFINIZIONE. Un *ampliamento* (o un'estensione) di un campo F è un qualunque campo K che contenga F . \square

Ad essere precisi, un'estensione (o ampliamento) di un campo F è una *coppia* (K, ι) costituita da un campo K e un monomorfismo (di campi) ι da F in K . Generalmente identificheremo un elemento a di F con la sua immagine $\iota(a)$ in K , e considereremo F come sottocampo di K .

Abbiamo già dato a suo tempo (cfr. §4.10) la definizione di *caratteristica* di un campo e di *sottocampo primo* o *fondamentale*. Abbiamo visto che il sottocampo fondamentale di ogni campo di caratteristica zero è il campo razionale

\mathbb{Q} , mentre il sottocampo fondamentale di ogni campo di caratteristica p è il campo \mathbb{Z}_p delle classi modulo p . Quindi ogni campo di caratteristica zero è estensione del campo dei razionali (ossia "contiene" il campo dei razionali), mentre ogni campo di caratteristica p è estensione di \mathbb{Z}_p . Da un certo punto in poi dovremo limitarci ai campi di caratteristica zero, tuttavia per il momento le definizioni si possono dare per tutti i casi.

Sarà essenziale a questo punto che lo studente rinfreschi le sue nozioni sugli spazi vettoriali: in particolare riveda le nozioni di dipendenza e indipendenza lineare, base e dimensione. Infatti (cfr. esercizio 6.1.1) ogni campo K si può pensare (rispetto alle sue due operazioni) come *spazio vettoriale sopra un suo qualunque sottocampo F* . Si potrà allora parlare di dipendenza e indipendenza su F di elementi del campo, dimensione su F , ecc.

6.1.2 DEFINIZIONE. Sia F un campo e sia K una sua estensione. Si definisce *grado* dell'estensione K sul campo F , e si indica con $[K : F]$, la dimensione di K come spazio vettoriale su F . \square

6.1.3 ESEMPIO. Il campo \mathbb{C} dei complessi è un'estensione di grado due sul campo \mathbb{R} dei reali, dato che una base di \mathbb{C} su \mathbb{R} è data da 1 e i , mentre è un'estensione di grado 1 su se stesso. \square

6.1.4 ESEMPIO. Il campo $\mathbb{R}(x)$ delle funzioni razionali a coefficienti in \mathbb{R} ha dimensione infinita su \mathbb{R} , dato che contiene le funzioni razionali $1, x, x^2, \dots, x^i, \dots$ che sono linearmente indipendenti su \mathbb{R} . \square

6.1.5 DEFINIZIONE. Un ampliamento K di un campo F si dice *finito* se il suo grado $[K : F]$ è finito. Si dice *infinito* in caso contrario. \square

Il seguente teorema riguarda gli ampliamenti finiti (cfr. figura 6.1).

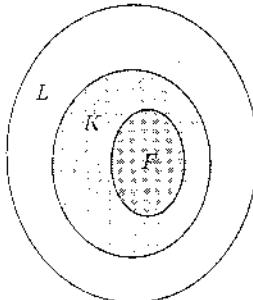


FIGURA 6.1

6.1.6 TEOREMA. Sia L un ampliamento finito di K e sia K a sua volta un ampliamento finito di F . Allora

- (a) L è ampliamento finito di F ;
 (b) $[L : F] = [L : K][K : F]$.

Schematicamente, la situazione è illustrata in figura 6.2. Si tratta di una situazione a torre (cioè una estensione su una estensione).



FIGURA 6.2

Dimostrazione. Sia $[L : K] = m$, $[K : F] = n$, e siano $X = \{x_1, x_2, \dots, x_m\}$ una base di L su K e $Y = \{y_1, y_2, \dots, y_n\}$ una base di K su F . Proveremo che gli elementi $\{x_i y_j\}_{i=1, \dots, m, j=1, \dots, n}$ sono una base di L su F , e quindi questo dimostra entrambi i punti (a) e (b).

(a) Gli $x_i y_j$ sono generatori. Sia l un qualunque elemento di L . Allora

$$l = \sum_{i=1}^m k_i x_i, \quad k_i \in K$$

dato che x_1, x_2, \dots, x_m sono una base di L su K . D'altra parte, essendo y_1, y_2, \dots, y_n una base di K su F , ogni k_i si scriverà come combinazione lineare degli y_j , a coefficienti in F . Ne segue

$$l = \sum_{i=1}^m \left(\sum_{j=1}^n a_{ij} y_j \right) x_i = \sum_{i,j} a_{ij} y_j x_i .$$

(b) Gli $x_i y_j$ sono linearmente indipendenti su F . Supponiamo

$$\sum_{i,j} a_{ij} (y_j x_i) = 0, \quad a_{ij} \in F .$$

Allora si ha

$$0 = \sum_{i=1}^m \left(\underbrace{\sum_{j=1}^n a_{ij} y_j}_{c_i K} \right) x_i$$

da cui, per la indipendenza degli x_i su K ,

$$\sum_{j=1}^n a_{ij} y_j = 0.$$

Essendo gli y_j indipendenti su F , segue che $a_{ij} = 0$ per ogni i, j . \square

6.1.7 COROLLARIO. *Sia L un ampliamento finito di F e K un sottocampo di L contenente F . Allora*

$$[K : F] \mid [L : F].$$

Dimostrazione. Se L è un'estensione finita di F , anche ogni sottocampo di L sarà un'estensione finita di F (ovvio, si pensino come spazi vettoriali!). Non solo, se L ha grado finito su F , cioè se L ha dimensione finita come spazio vettoriale su F , a maggior ragione avrà dimensione finita su K (ampliando il campo degli scalari si "riducono" gli elementi indipendenti, cioè si abbassa la dimensione), cioè $[L : K] < \infty$. Per il teorema ora provato

$$[L : F] = [L : K][K : F] \implies [K : F] \mid [L : F]. \quad \square$$

Si noti che questo corollario si può pensare come l'analogo per le estensioni finite del teorema di Lagrange per i gruppi finiti.

6.1.8 COROLLARIO. *Se K è un ampliamento di F che ha come grado un numero primo p , allora non ci sono campi intermedi tra K e F .*

I teoremi precedenti sostanzialmente ci permettono di calcolare il grado di estensioni complicate attraverso i gradi di estensioni più semplici.

È importante a questo punto vedere come si possono, dato un campo F e un suo ampliamento K , costruire degli ampliamenti intermedi tra K e F .

Sia K un'estensione di F e sia S un sottoinsieme di K . Indicheremo con

$$F[S] \text{ e } F(S)$$

rispettivamente l'intersezione di tutti i *sottoanelli* di K contenuti F e S , e l'intersezione di tutti i *sottocampi* di K contenenti F e S . Risulta ovviamente

$$F[S] \subseteq F(S) \subseteq K.$$

Inoltre $F(S)$ è il campo dei quozienti di $F[S]$. Si dice che il campo $F(S)$ è stato ottenuto *aggiungendo* il sottoinsieme S . Abbiamo dato una descrizione di $F(S)$ dall'esterno, cioè come l'intersezione di tutti i sottocampi contenenti F e S , ovvero come il più piccolo sottocampo contenente F e S . Tuttavia, vorremmo sapere esattamente chi sono i suoi elementi (come quando si è data la nozione di sottogruppo generato da un sottoinsieme S). Cominciamo dal caso

più semplice, che consiste nell' *aggiungere ad F un solo elemento $a \in K$* . Studieremo cioè il caso in cui $S = \{a\}$. Si dice in tal caso che $F(a)$ è un'estensione semplice del campo F . Vediamo chi sono i suoi elementi.

6.1.9 PROPOSIZIONE. *Sia K un'estensione di F e sia $a \in K$. Allora*

$$F(a) = \left\{ \frac{\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_s a^s}{\beta_0 + \beta_1 a + \beta_2 a^2 + \cdots + \beta_t a^t} \mid \alpha_i, \beta_j \in F, \right. \\ \left. s, t \in \mathbb{N}, \beta_0 + \beta_1 a + \cdots + \beta_t a^t \neq 0 \right\}.$$

Dimostrazione. Poniamo

$$T = \left\{ \frac{\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_s a^s}{\beta_0 + \beta_1 a + \beta_2 a^2 + \cdots + \beta_t a^t} \mid \alpha_i, \beta_j \in F, \right. \\ \left. s, t \in \mathbb{N}, \beta_0 + \beta_1 a + \cdots + \beta_t a^t \neq 0 \right\}.$$

Chiaramente

$$T \supseteq F(a)$$

dato che T è un campo che contiene F ed a . D'altra parte vale anche la inclusione inversa, $T \subseteq F(a)$, perché gli elementi di T devono stare in *qualunque* campo contenente F ed a . \square

Diamo qui di seguito due esempi di estensioni semplici, dai quali risultano due comportamenti sostanzialmente diversi.

6.1.10 ESEMPIO. Sia $F = \mathbb{Q}$, $K = \mathbb{R}$ e $a = \pi$. Come si è visto,

$$\mathbb{Q}(\pi) = \left\{ \frac{\alpha_0 + \alpha_1 \pi + \alpha_2 \pi^2 + \cdots + \alpha_s \pi^s}{\beta_0 + \beta_1 \pi + \beta_2 \pi^2 + \cdots + \beta_t \pi^t} \mid \alpha_i, \beta_j \in \mathbb{Q}, s, t \in \mathbb{N} \right\}. \quad \square$$

6.1.11 ESEMPIO. Sia $F = \mathbb{Q}$ e $K = \mathbb{R}$ e sia $a = \sqrt{3}$. In base a quanto detto, risulta

$$\mathbb{Q}(\sqrt{3}) = \left\{ \frac{\alpha_0 + \alpha_1 \sqrt{3} + \alpha_2 \sqrt{3}^2 + \cdots + \alpha_s \sqrt{3}^s}{\beta_0 + \beta_1 \sqrt{3} + \beta_2 \sqrt{3}^2 + \cdots + \beta_t \sqrt{3}^t} \mid \alpha_i, \beta_j \in \mathbb{Q}, \right. \\ \left. s, t \in \mathbb{N}, \beta_0 + \beta_1 \sqrt{3} + \cdots + \beta_t \sqrt{3}^t \neq 0 \right\}.$$

Tuttavia, dato che $\sqrt{3}^2 = 3$, le espressioni dentro $\mathbb{Q}(\sqrt{3})$ si possono ridurre al modo seguente:

$$\mathbb{Q}(\sqrt{3}) = \left\{ \frac{\alpha_0 + \alpha_1 \sqrt{3}}{\beta_0 + \beta_1 \sqrt{3}} \mid \alpha_i, \beta_j \in \mathbb{Q}, \beta_0 + \beta_1 \sqrt{3} \neq 0 \right\}.$$

Ma

$$\frac{1}{\beta_0 + \beta_1 \sqrt{3}} = \frac{\beta_0 - \beta_1 \sqrt{3}}{\beta_0^2 - 3\beta_1^2} = \frac{\beta_0}{\beta_0^2 - 3\beta_1^2} - \left(\frac{\beta_1}{\beta_0^2 - 3\beta_1^2} \right) \sqrt{3},$$

e

$$\frac{\beta_0}{\beta_0^2 - 3\beta_1^2}, \quad \frac{\beta_1}{\beta_0^2 - 3\beta_1^2}$$

sono entrambi elementi di \mathbb{Q} . Quindi gli elementi di $\mathbb{Q}(\sqrt{3})$ possono scriversi tutti nella forma $q_0 + q_1 \sqrt{3}$, con $q_0, q_1 \in \mathbb{Q}$. In definitiva

$$\mathbb{Q}(\sqrt{3}) = \{q_0 + q_1 \sqrt{3} \mid q_0, q_1 \in \mathbb{Q}\}. \quad \square$$

A cosa è dovuto il diverso comportamento delle due estensioni? Nel secondo caso le espressioni dentro l'estensione *possono essere semplificate*, mentre nel primo caso questa semplificazione non si è potuta fare. Il motivo della diversità di comportamento delle due estensioni va da ricercarsi nella *natura* dell'elemento a che si sta "aggiungendo". È opportuno a questo punto dare alcune definizioni.

6.1.12 DEFINIZIONE. Sia F un campo e K una estensione di F . Un elemento $a \in K$ si dice *algebrico su F* se $f(a) = 0$ per qualche polinomio non nullo $f(x) \in F[x]$. Un elemento a si dice *trascendente su F* se non soddisfa nessun polinomio non nullo a coefficienti in F . \square

Se $K = \mathbb{C}$ e $F = \mathbb{Q}$, gli elementi di \mathbb{C} algebrici o trascendenti su \mathbb{Q} si chiamano semplicemente *numeri algebrici* o *numeri trascendenti*. Il numero π è trascendente (la dimostrazione di questo fatto è dovuta a Lindemann), come anche il numero e , base dei logaritmi naturali (dimostrazione di Hermite). Nell'Appendice dimostreremo l'*irrazionalità* dei due numeri (non la loro trascendenza). Apparentemente scenderanno di più i numeri algebrici, perché sono quelli con i quali abbiamo più comunemente a che fare, tuttavia non è difficile provare che i numeri algebrici *hanno la potenza del numerabile*, mentre i numeri trascendenti hanno *la potenza del continuo*, che è la potenza dei numeri reali. Quindi "quasi tutti i numeri" sono trascendenti. Si possono costruire numeri trascendenti, a partire da numeri algebrici, elevando ad un esponente b algebrico e irrazionale, una base a algebrica, diversa da 0 e 1. Quindi ad esempio $3^{\sqrt{3}}$ è trascendente. È noto che e^π è trascendente, mentre non si sa se sia trascendente ad esempio π^e .

Ora, la diversa natura dell'elemento a si riflette sulla struttura di $F(a)$. I teoremi che seguono chiariranno questo legame.

6.1.13 TEOREMA. *Sia F un campo e K una sua estensione. Detto a un elemento di K , l'applicazione*

$$\begin{aligned}\Psi_a : F[x] &\longrightarrow K \\ f(x) &\longmapsto f(a)\end{aligned}$$

risulta un omomorfismo di anelli e la sua immagine coincide con $F[a]$. Tale omomorfismo prende il nome di omomorfismo valutazione.

Dimostrazione. Per ogni $f, g \in F[x]$ risulta

$$\begin{aligned}\Psi_a(f+g) &= (f+g)(a) = f(a) + g(a) = \Psi_a(f) + \Psi_a(g) \\ \Psi_a(fg) &= (fg)(a) = f(a)g(a) = \Psi_a(f)\Psi_a(g).\end{aligned}$$

Quindi si tratta di un omomorfismo di anelli.

L'immagine $\text{Im } \Psi_a$ è un sottoanello di K che contiene F ed a , e pertanto contiene $F[a]$. D'altra parte, se t è un elemento in $\text{Im } \Psi_a$, sarà $t = \Psi_a(f)$ per qualche $f \in F[x]$. Se

$$f(x) = \sum_{i=0}^n \alpha_i x^i, \quad \alpha_i \in F$$

allora

$$t = \Psi_a(f) = \sum_{i=0}^n \alpha_i a^i \in F[a].$$

Quindi $\text{Im } \Psi_a = F[a]$. \square

6.1.14 COROLLARIO. *Sia F un campo e sia K una sua estensione. Detto a un elemento di K e Ψ_a l'omomorfismo valutazione, a risulta algebrico se e solo se $\text{Ker } \Psi_a \neq 0$, (e quindi a trascendente se e solo se $\text{Ker } \Psi_a = 0$).*

Dimostrazione. Un elemento a è algebrico su F se e solo se esiste un polinomio non nullo $f \in F[x]$ tale che $f(a) = 0$. Quindi a è algebrico su F se e solo se $\text{Ker } \Psi \neq 0$. \square

6.1.15 TEOREMA. *Se F è un campo, K è un'estensione di F e a è un elemento trascendente su F , allora esiste un isomorfismo tra $F(a)$ e il campo $F(x)$ delle funzioni razionali a coefficienti in F . In particolare, $[F(a) : F]$ è infinito.*

Dimostrazione. Dal teorema 6.1.13, dal corollario 6.1.14 e dal teorema fondamentale di omomorfismo tra anelli segue che

$$F[a] \cong F[x].$$

Allora anche i loro campi dei quozienti sono isomorfi, ossia

$$F(a) \cong F(x).$$

$[F(a) : F]$ è infinito perché $1, a, a^2, \dots, a^i, \dots$ sono linearmente indipendenti su F . \square

Se quindi K è un'estensione di F , tutte le estensioni $F(a)$ con a trascendente su F sono isomorfe tra di loro: si può riguardare l'elemento a come una *indeterminata* x , e $F(a)$ si identifica con le funzioni razionali nella indeterminata x . Il prossimo teorema mostrerà come il fatto che $F(a)$ sia finito o infinito su F caratterizza l'essere a algebrico o trascendente su F .

6.1.16 TEOREMA. *Sia K una estensione di F e sia a un elemento algebrico su F . Allora, se Ψ_a è l'omomorfismo di valutazione da $F[x]$ in K ,*

- (a) $\text{Ker}(\Psi_a) = (p(x))$ dove $p(x)$ è un polinomio irriducibile monico in $F[x]$ che prende il nome di polinomio minimo di a su F ;
- (b) un polinomio $f(x) \in F[x]$ è annullato da a se e solo se $p(x)$ divide $f(x)$;
- (c) $F(a) = F[a]$ e $F(a) \cong F[x]/(p(x))$;
- (d) se il grado di $p(x)$ è n , allora $[F(a) : F] = n$ e $F(a)$ ha come base $1, a, a^2, \dots, a^{n-1}$.

Dimostrazione. (a) In virtù del teorema fondamentale di omomorfismo di anelli risulta

$$F[a] \cong F[x]/\text{Ker } \Psi_a.$$

Ora, $F[a]$, in quanto sottoanello di un campo, è un dominio di integrità, per cui (per la caratterizzazione al quoziente dei domini di integrità), $\text{Ker } \Psi_a$ è un ideale primo, e pertanto generato da un polinomio irriducibile. Se lo si divide per il suo coefficiente direttivo, si ottiene il polinomio monico e irriducibile cercato. Esso è il polinomio di grado minimo annullato da a .

(b) Un polinomio $f(x)$ in $F[x]$ è tale che $f(a) = 0$ se e solo se $f(x) \in \text{Ker } \Psi_a$ e quindi se e solo se $p(x) \mid f(x)$.

(c) Risulta $F[a] = F(a)$, perché nelle ipotesi attuali ($\text{Ker } \Psi_a$ generato da un elemento irriducibile) il quoziente $F[x]/\text{Ker } \Psi_a$, e quindi $F[a]$, risulta un campo. Dato che $F[a]$ contiene F ed a , ne segue che $F[a] = F(a)$ e $F(a) \cong F[x]/(p(x))$.

(d) Sia $n = \deg(p(x))$. Dimostreremo che gli elementi $1, a, a^2, \dots, a^{n-1}$ sono una base per $F[a]$ ($= F(a)$). Dimostriamo innanzitutto l'*indipendenza*: sia

$$\sum_{i=0}^{n-1} \alpha_i a^i = 0, \quad \alpha_i \in F$$

e si consideri il polinomio $f(x) = \sum_{i=0}^{n-1} \alpha_i x^i \in F[x]$. Dato che si tratta di un polinomio annullato da a , appartiene a $\text{Ker } \Psi_a$, e quindi è multiplo di $p(x)$.

Essendo il grado di $p(x)$ n mentre il grado di $f(x)$ è $n - 1$, $f(x)$ deve necessariamente essere il polinomio nullo e quindi tutti gli α_i devono essere nulli. L'indipendenza di $1, a, \dots, a^{n-1}$ è così provata.

Proviamo ora che $1, a, \dots, a^{n-1}$ sono generatori di $F[a]$. Se t è un elemento di $F[a]$, esisterà un polinomio $f(x) \in F[x]$ tale che $t = \Psi_a(f(x)) = f(a)$. Dividendo $f(x)$ per $p(x)$ si ottiene

$$f(x) = q(x)p(x) + r(x) \quad r = 0 \text{ o } \partial r(x) < \partial p(x).$$

Valutando tale relazione su a si ottiene

$$f(a) = q(a) \underbrace{p(a)}_{=0} + r(a) = r(a).$$

Abbiamo pertanto espresso $t = f(a)$ come combinazione lineare a coefficienti in F degli elementi $1, a, \dots, a^{n-1}$, che sono quindi generatori. \square

Si noti che la scrittura di ogni elemento di $F[a]$ nella forma $f(a) = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \dots + \alpha_{n-1} a^{n-1}$ è unica, dato che $1, a, a^2, \dots, a^{n-1}$ costituiscono una base.

6.1.17 COROLLARIO. *Sia K un'estensione di un campo F e sia $a \in K$. Allora a è algebrico se e solo se $F(a)$ è un'estensione finita, mentre è trascendente se e solo se $F(a)$ è un'estensione infinita.*

Dimostrazione. Conseguenza dei teoremi 6.1.15 e 6.1.16. \square

Abbiamo caratterizzato completamente le estensioni semplici. Supponiamo ora di voler costruire l'estensione $\mathbb{Q}(S)$, dove $S = \{\sqrt{3}, \sqrt{5}\}$ e calcolarne il grado su \mathbb{Q} . Il modo con cui procederemo è quello di aggiungere prima $\sqrt{3}$, ottenendo l'estensione $\mathbb{Q}(\sqrt{3})$, e poi aggiungere l'elemento $\sqrt{5}$ a $\mathbb{Q}(\sqrt{3})$ (cfr. figura 6.3).

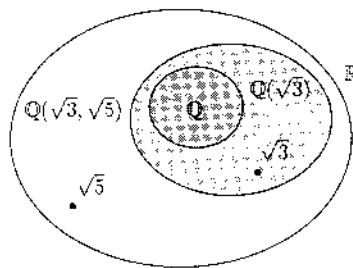


FIGURA 6.3

Utilizzando il risultato contenuto nel teorema 6.1.6 si può facilmente calcolare il grado dell'estensione. $\sqrt{3}$ è algebrico su \mathbb{Q} , di grado 2, dato che il suo polinomio minimo è $x^2 - 3$; in base al teorema 6.1.16, $\mathbb{Q}(\sqrt{3}) \cong \mathbb{Q}[x]/(x^2 - 3)$.

Aggiungiamo ora $\sqrt{5}$ a $\mathbb{Q}(\sqrt{3})$. Il polinomio $x^2 - 5$ è irriducibile (non solo su \mathbb{Q} , ma anche) su $\mathbb{Q}(\sqrt{3})$ (perché?). Quindi l'estensione $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = (\mathbb{Q}(\sqrt{3}))(\sqrt{5})$ ha grado due su $\mathbb{Q}(\sqrt{3})$. In definitiva,

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Dato che una base di $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ su $\mathbb{Q}(\sqrt{3})$ è $\{1, \sqrt{5}\}$ e una base di $\mathbb{Q}(\sqrt{3})$ su \mathbb{Q} è $\{1, \sqrt{3}\}$, una base di $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ su \mathbb{Q} è data da

$$1, \quad \sqrt{3}, \quad \sqrt{5}, \quad \sqrt{3}\sqrt{5} = \sqrt{15}$$

e

$$\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \{a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} \mid a, b, c, d \in \mathbb{Q}\}.$$

Con i risultati dimostrati finora, siamo in grado di provare il seguente teorema.

6.1.18 TEOREMA. *Sia K un'estensione di F . Allora gli elementi di K algebrici su F formano un sottocampo di K .*

Dimostrazione. Basta provare che, se a e b sono algebrici su F , lo sono anche $a \pm b$, ab e a/b .

Sia a di grado n , e b di grado m . Allora

$$[F(a) : F] = n.$$

Consideriamo $F(a, b) = (F(a))(b)$. Essendo b algebrico di grado m su F , esso sarà algebrico di grado $\leq m$ su $F(a)$. Ne segue che

$$[F(a, b) : F] = [F(a, b) : F(a)][F(a) : F] \leq nm.$$

Ora, $a \pm b$, ab , a/b appartengono tutti a $F(a, b)$, cioè $F(a \pm b)$, $F(ab)$, $F(a/b)$ stanno tutti dentro $F(a, b)$, che è un'estensione finita di F . Per il corollario 6.1.17, $a \pm b$, ab e a/b sono tutti algebrici su F . \square

6.1.19 OSSERVAZIONE. Nel corso del teorema precedente abbiamo provato che se a e b sono algebrici rispettivamente di grado n e m , allora $a \pm b$, ab e a/b sono algebrici di grado $\leq nm$. \square

6.1.20 OSSERVAZIONE. L'insieme \mathbb{A} di tutti i numeri algebrici su \mathbb{Q} costituisce il campo dei numeri algebrici. Tale campo è chiaramente un'estensione di \mathbb{Q} , in cui ogni elemento $a \in \mathbb{A}$ è algebrico, e quindi $[\mathbb{Q}(a) : \mathbb{Q}] < \infty$, tuttavia risulta

$$[\mathbb{A} : \mathbb{Q}] = \infty.$$

Supponiamo per assurdo che sia $[\mathbb{A} : \mathbb{Q}] = n$. Faremo vedere che esiste un elemento α algebrico su \mathbb{Q} e di grado maggiore di n . Basta prendere ad esempio

$$\alpha = \sqrt[n]{2}.$$

α è radice del polinomio (irriducibile su \mathbb{Q}) $x^{n+1} - 2$. Quindi tale polinomio è il polinomio minimo per α , che ha quindi grado $n + 1$. Risulta allora

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = n + 1 > [\mathbb{A} : \mathbb{Q}] = n.$$

Questo contraddice il fatto che $\alpha \in \mathbb{A}$ (vedi figura 6.4). \square

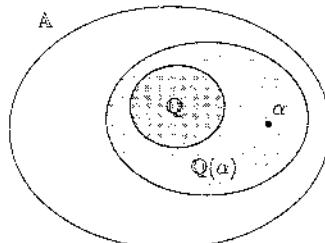


FIGURA 6.4

Cerchiamo ora di risolvere alcuni problemi relativi alle estensioni.

6.1.21 PROBLEMA. Sia K un'estensione di F e sia $a \in K$ un elemento algebrico su F . Sia $p(x)$ il suo polinomio minimo su F (cioè il polinomio monico $\in F[x]$ di grado minimo annullato da a). Si provi che $p(x)$ è irriducibile su F . Viceversa, se $p(x)$ è un polinomio monico e irriducibile in $F[x]$, si provi che è il polinomio minimo per ciascuna delle sue radici.

Dimostrazione. Sia $p(x) = f(x)g(x)$, con $f(x), g(x) \in F[x]$, una fattorizzazione propria di $p(x)$, ossia con i gradi dei fattori strettamente minori del grado di $p(x)$. Allora $0 = p(a) = f(a)g(a)$, comporta, trattandosi di una relazione in un campo, che è privo di divisori dello zero, o $f(a) = 0$, oppure $g(a) = 0$, ma questo contrasta con la ipotesi che $p(x)$ sia il polinomio minimo annullato da a .

Viceversa, sia $f(x)$ un polinomio monico e irriducibile in $F[x]$. Indicata con a una delle radici di $f(x)$, dobbiamo provare che $f(x)$ è il polinomio minimo di a . A tal fine, basta provare che, detto I l'ideale di tutti i polinomi in $F[x]$ annullati da a , risulta $I = (f(x))$. Sia dunque $I = (g(x))$. Dovrà allora essere $f(x)$ un multiplo di $g(x)$. Data la irriducibilità di $f(x)$, sarà $f(x) = \alpha g(x)$, con $\alpha \in F$. Ma allora $(f(x)) = (g(x))$. \square

6.1.22 PROBLEMA. Sia K un'estensione di F e sia $a \in K$. Abbiamo visto che, se a è algebrico su F ,

$$F(a) = F[a].$$

Si determini l'inverso di un elemento $g(a) \in F(a)$, $g(a) \neq 0$, esprimendolo nella forma $\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_{n-1} a^{n-1}$, essendo n il grado del polinomio minimo $p(x)$ di a su F .

Dimostrazione. Sia $g(a) = a_0 + a_1a + \cdots + a_{n-1}a^{n-1}$. Consideriamo il polinomio $g(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. Dato che $g(a) \neq 0$, $g(x)$ non è multiplo di $p(x)$. Allora

$$(g(x), p(x)) = 1$$

e quindi esistono $s(x), t(x)$ in $F[x]$ tali che

$$1 = s(x)g(x) + t(x)p(x).$$

Ponendo $x = a$ si ottiene

$$1 = s(a)g(a) + t(a)\underbrace{p(a)}_{=0} = s(a)g(a).$$

L'elemento $s(a)$ (nel quale siano state ridotte le potenze superiori ad n con la relazione $p(a) = 0$) è l'inverso cercato di $g(a)$. \square

Le estensioni K di un campo F in cui ogni elemento (come nel caso di \mathbb{A}) è algebrico su F meritano una definizione a parte.

6.1.23 DEFINIZIONE. Un ampliamento K di un campo F si dice *algebrico* se ogni elemento di K è algebrico su F . \square

Ad esempio, il campo \mathbb{C} dei numeri complessi è un'estensione algebrica di \mathbb{R} . Infatti ogni elemento $a + ib$ appartenente a \mathbb{C} soddisfa il polinomio (a coefficienti in \mathbb{R}),

$$x^2 - 2ax + (a^2 + b^2).$$

Ovviamente ogni estensione *finita* di un campo F è un'estensione algebrica, ma non è vero il viceversa: infatti ad esempio \mathbb{A} è un'estensione algebrica, ma infinita. Sussiste il seguente importante teorema.

6.1.24 TEOREMA. *Sia L un ampliamento algebrico di K e sia K un ampliamento algebrico di F . Allora L è un ampliamento algebrico su F .*

Dimostrazione. Per provare il teorema, basta far vedere che *ogni elemento di L appartiene ad una estensione finita di F .*

Sia $l \in L$. Dato che l è algebrico su K , l annulla un polinomio

$$k_0 + k_1x + k_2x^2 + \cdots + k_nx^n, \quad k_i \in K.$$

Ora, ogni k_i , in quanto elemento di K , che è algebrico su F , è algebrico su F , e quindi

$$[F(k_0) : F] < \infty, \quad [F(k_0, k_1) : F] < \infty, \quad \dots, \quad [F(k_0, k_1, \dots, k_n) : F] < \infty.$$

Aggiungiamo ora l a $F(k_0, k_1, \dots, k_n)$. Risulta

$$\begin{aligned} & [(F(k_0, k_1, \dots, k_n))(l) : F] \\ & = [(F(k_0, k_1, \dots, k_n))(l) : F(k_0, k_1, \dots, k_n)] [F(k_0, k_1, \dots, k_n) : F]. \end{aligned}$$

Il primo fattore del secondo membro è $< \infty$, dato che l è algebrico su $F(k_0, k_1, \dots, k_n)$ perché soddisfa un polinomio a coefficienti in $F(k_0, k_1, \dots, k_n)$, il secondo fattore è $< \infty$ per quanto visto prima. Quindi, appartenendo ad una estensione finita di F , l è algebrico su F . Può essere utile visualizzare il contenuto del teorema con la figura 6.5. \square

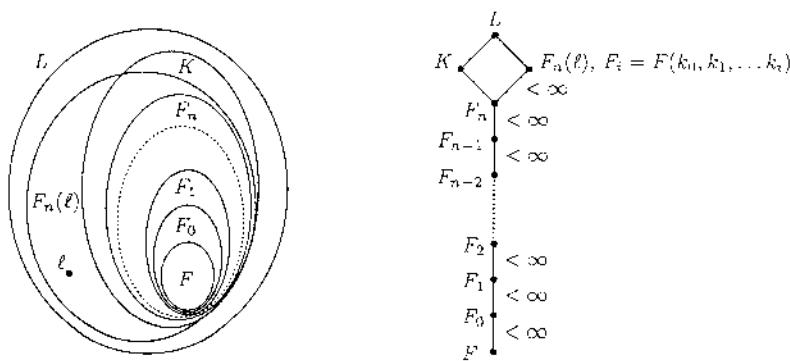


FIGURA 6.5

6.1.25 DEFINIZIONE. Un campo K si dice *algebricamente chiuso* se non ha estensioni algebriche proprie. \square

6.1.26 TEOREMA. Il campo \mathbb{A} di tutti i numeri algebrici è algebricamente chiuso.

Dimostrazione. Basta provare che le radici di ogni polinomio a coefficienti numeri algebrici sono numeri algebrici.

Sia $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ un polinomio a coefficienti in \mathbb{A} . Consideriamo l'estensione

$$K = \mathbb{Q}(a_0, a_1, \dots, a_{n-1}).$$

Si tratta di una estensione finita di \mathbb{Q} . Sia s una qualunque radice di $f(x)$. $K(s)$ è un'estensione finita di K , perché s è algebrico su K . Ma allora $K(s)$ è un'estensione finita anche di \mathbb{Q} , e s è algebrico. \square

Il campo \mathbb{C} dei numeri complessi è algebricamente chiuso, in virtù del teorema fondamentale dell'algebra, che proveremo nell'ultimo capitolo.

Si può dimostrare, ma questo va oltre gli scopi del testo, che, dato comunque un campo K , esiste un'estensione algebrica di K che è algebricamente chiusa. Una tale estensione prende il nome di *chiusura algebrica* di K . Due chiusure algebriche di uno stesso campo sono isomorfe in un isomorfismo che ristretto a K è l'identità.

ESERCIZI.

- Provare che ogni campo K , rispetto alle sue due operazioni, è uno spazio vettoriale sopra un suo qualunque sottocampo.
- Sia K il sottocampo di \mathbb{C} $\mathbb{Q}(\sqrt[3]{2})$, e sia $\alpha = 1/(1 + 2\sqrt[3]{2})$. Si provi che $\alpha \in K$, $\alpha \notin \mathbb{Q}$. Si studi $\mathbb{Q}(\alpha)$.
- Si dica quali delle seguenti affermazioni sono esatte e si giustifichi in ogni caso la risposta:
 - $\sqrt{2} + \sqrt{3}$ è algebrico su \mathbb{Q} ;
 - $\sqrt{2} + \sqrt{3}$ è algebrico su $\mathbb{Q}(\sqrt{2})$;
 - $\sqrt{2} + \sqrt{3}$ è trascendente su \mathbb{Q} ;
 - $\sqrt{2} + \sqrt{3}$ è algebrico di grado 6 su \mathbb{Q} .
- Si dica se gli elementi

$$\frac{\pi + 2}{\pi + \sqrt{2}}, \quad \sqrt[3]{2} + \sqrt{5}, \quad \sqrt[3]{4 + \sqrt{5}}, \quad \sqrt{2 + \sqrt{2}}$$

- sono trascendenti o algebrici. Se algebrici, si calcoli il polinomio minimo.
- Si determini una base per le seguenti estensioni:

$$\begin{aligned} \mathbb{Q}(\sqrt{2}\sqrt{3}), \quad \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) &\quad \text{su } \mathbb{Q}, \\ \mathbb{Q}(\sqrt[3]{3} + \sqrt{5}) &\quad \text{su } \mathbb{Q}(\sqrt{5}). \end{aligned}$$

- Sia p un numero primo e sia ξ una radice p -esima primitiva dell'unità. Si studi l'estensione

$$\mathbb{Q}(\xi).$$

- Si provi che

$$\mathbb{Q}(\sqrt{i}) = \mathbb{Q}(\sqrt{2}, i).$$

- Si dica se l'elemento $\sqrt{3} + \sqrt{7}$ è algebrico sui \mathbb{Q} . In caso positivo si determini il polinomio minimo.
- Si provi che $\sqrt{2} + i$ è algebrico di grado 4 su \mathbb{Q} e di grado 2 su \mathbb{R} .
- Si provi che l'ordine di un campo finito è una potenza di un numero primo.
- Si provi che $\{1, \sqrt{5}\}$ è una base di $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ su $\mathbb{Q}(\sqrt{3})$.

**CONTROLLO.**

1. Che cos'è il grado di una estensione?
2. Che cosa si intende con il simbolo $F(a)$?
3. Se a è algebrico, $F(a) \dots$
Se a è trascendente, $F(a) \dots$
4. Legame tra estensioni algebriche ed estensioni finite.

6.2. Campo di spezzamento di un polinomio

Scopo di questo paragrafo è di provare l'esistenza di un "campo di spezzamento" per ogni polinomio $f(x) \in F[x]$. Diamo qui di seguito la definizione.

6.2.1 DEFINIZIONE. Sia $f(x) \in F[x]$. Un'estensione finita E di F si dice *campo di spezzamento su F* di $f(x)$ se $f(x)$ si spezza su E in fattori lineari, e ciò non avviene su un sottocampo proprio di E . \square

6.2.2 ESEMPIO. Si consideri il polinomio $f(x) = x^2 - 3 \in \mathbb{Q}[x]$. Il campo $\mathbb{Q}(\sqrt{3})$ è una estensione di \mathbb{Q} , contiene le radici $\pm\sqrt{3}$ di $f(x)$, e quindi il polinomio $f(x)$ si spezza su $\mathbb{Q}(\sqrt{3})$ in fattori lineari:

$$x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$$

e inoltre $\mathbb{Q}(\sqrt{3})$ è il più piccolo campo per cui ciò avviene. Quindi $\mathbb{Q}(\sqrt{3})$ è campo di spezzamento per il polinomio $x^2 - 3$. \square

6.2.3 ESEMPIO. Sia $f(x) = x^2 + 1$. Se lo si pensa come polinomo a coefficienti in \mathbb{Q} , il suo campo di spezzamento è $\mathbb{Q}(i)$, se invece lo si pensa come polinomo a coefficienti in \mathbb{R} , il suo campo di spezzamento è $\mathbb{R}(i) = \mathbb{C}$. \square

Da quest'ultimo esempio si vede intanto che nella determinazione di un campo di spezzamento per un polinomio è essenziale *specificare il campo su cui si sta considerando il polinomio*. Inoltre appare chiaro che, se di un polinomio $f(x)$ si conoscono le radici, come è avvenuto negli esempi dati, la determinazione di un campo di spezzamento per $f(x)$ è semplice, perché basta "aggiungere" al campo F le radici del polinomio $f(x)$. Supponiamo tuttavia di volere trovare un campo di spezzamento per il polinomio $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Tale polinomio non ha radici nel campo \mathbb{Z}_2 : dove andiamo a cercarle? E se $f(x)$ è un polinomio di grado elevato su \mathbb{Q} privo di radici razionali? Come facciamo a trovare un campo che contenga tutte le radici di $f(x)$, se non le conosciamo, e che sia il più piccolo tra tutti quelli che contengono le radici? Il problema che vogliamo risolvere è quindi il seguente: dato un polinomio $f(x) \in F(x)$, *del quale non si conoscano esplicitamente le radici*, determinare un campo E che contenga F , sul quale $f(x)$ si spezzi in fattori lineari (il che equivale a dire che E contiene tutte le radici di $f(x)$) e che goda della proprietà di minimalità tra tutti i campi che godono di questa proprietà. Cominciamo a porci un obiettivo

più semplice. Dato un polinomio, cercare un campo che contenga il campo dei coefficienti del polinomio e contenga *una* radice del polinomio. Ritorniamo al caso del polinomio $f(x) = x^2 - 3 \in \mathbb{Q}[x]$. Consideriamo l'anello

$$K = \mathbb{Q}[x]/(x^2 - 3).$$

Esso gode delle seguenti proprietà:

- (1) È un *campo*: infatti il polinomio $f(x) = x^2 - 3$ è irriducibile su \mathbb{Q} .
- (2) È un'estensione di \mathbb{Q} : si consideri infatti la proiezione canonica

$$\begin{aligned}\Psi : \mathbb{Q}[x] &\longrightarrow \mathbb{Q}[x]/(x^2 - 3) \\ f(x) &\longmapsto f(x) + (x^2 - 3).\end{aligned}$$

L'insieme $\bar{\mathbb{Q}} = \{a + (x^2 - 3) \mid a \in \mathbb{Q}\}$ è un campo che è isomorfo a \mathbb{Q} : infatti, se $a, b \in \mathbb{Q}$, $a + (x^2 - 3) = b + (x^2 - 3)$ se e solo se $a = b$ (si veda la figura 6.6). Quindi $K = \mathbb{Q}[x]/(x^2 - 3) \supset \bar{\mathbb{Q}} \cong \mathbb{Q}$.

- (3) K contiene una radice α di $x^2 - 3$: poniamo α uguale alla classe $x + (x^2 - 3)$. Allora

$$\begin{aligned}\alpha^2 - 3 &= (x + (x^2 - 3))^2 - 3 = x^2 + (x^2 - 3) - 3 \\ &= x^2 - 3 + (x^2 - 3) = (x^2 - 3)\end{aligned}$$

che è la classe nulla di $\mathbb{Q}[x]/(x^2 - 3)$.

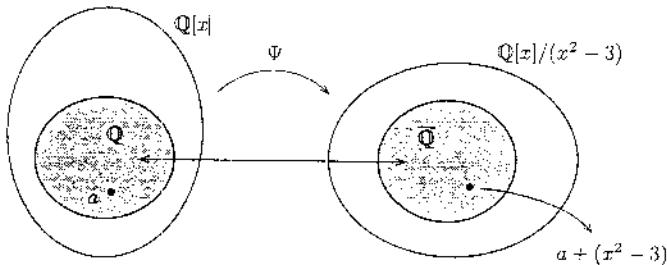


FIGURA 6.6

Ora, da questo esempio, si vede come (e d'altra parte lo sapevamo già) il campo $K = \mathbb{Q}[x]/(x^2 - 3)$ sia una realizzazione di $\mathbb{Q}(\sqrt{3})$ che *non fa intervenire elementi estranei ai dati del problema*, che consistono nel campo \mathbb{Q} e nel polinomio $f(x) \in \mathbb{Q}[x]$. Ma allora appare chiaro come ci dovremo comportare per trovare un campo che contenga una radice del polinomio $x^2 + x + 1 \in \mathbb{Z}_2[x]$. Essendo $f(x)$ irriducibile su \mathbb{Z}_2 , $\mathbb{Z}_2[x]/(x^2 + x + 1)$ è un campo, con 4 elementi, che è un'estensione di \mathbb{Z}_2 . Risulta

$$\mathbb{Z}_2[x]/(x^2 + x + 1) = \mathbb{Z}_2(\xi) = \{a + b\xi \mid a, b \in \mathbb{Z}_2, \xi^2 + \xi + 1 = 0\},$$

quindi consiste dei quattro elementi $0, 1, \xi, 1 + \xi$, con ξ tale che $\xi^2 + \xi + 1 = 0$; ξ è pertanto una radice di $f(x)$.

Ebbene, dopo avere visto come possono andare le cose in alcuni casi particolari, passiamo senz'altro alla teoria generale. Dimostreremo che per ogni polinomio $f(x) \in F[x]$, F campo arbitrario, si riesce a costruire un campo che contiene una radice di $f(x)$. Dopo di che, con un procedimento induttivo, dimostreremo che esiste un campo che contiene tutte le radici di $f(x)$.

6.2.4 LEMMA. *Sia $p(x)$ un polinomio irriducibile di grado $n \geq 1$ appartenente a $F[x]$. Allora esiste un ampliamento E di F , con $[E : F] = n$, nel quale $p(x)$ ha una radice.*

Dimostrazione. Si tratta in sostanza di ripetere quanto abbiamo visto negli esempi. Il campo che cerchiamo è

$$F[x]/(p(x)) .$$

Infatti è un campo, perché $(p(x))$ è massimale essendo $p(x)$ irriducibile; è un ampliamento di F dato che dall'omomorfismo Ψ

$$\begin{aligned} \Psi : F[x] &\longrightarrow F[x]/(p(x)) \\ f(x) &\longmapsto f(x) + (p(x)) \end{aligned}$$

risulta che $F[x]/(p(x))$ contiene $\bar{F} = \{a + (p(x)) \mid a \in F\}$ che è isomorfo a F . Si tratta inoltre di un ampliamento finito di grado n di F , dato che una sua base è

$$1 + (p(x)), \quad x + (p(x)), \dots, \quad x^{n-1} + (p(x)) .$$

Infine, la classe $\alpha = x + (p(x))$ è una radice di $p(x)$, perché se $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$, allora

$$\begin{aligned} p(\alpha) &= \alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 \\ &= (x + (p(x)))^n + a_{n-1}(x + (p(x)))^{n-1} + \dots + a_1(x + (p(x))) + a_0 \\ &= x^n + (p(x)) + a_{n-1}(x^{n-1} + (p(x))) + \dots + a_1(x + (p(x))) + a_0 \\ &= x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 + (p(x)) = (p(x)) = 0_{F[x]/(p(x))} . \quad \square \end{aligned}$$

6.2.5 LEMMA. *Sia $f(x)$ un polinomio arbitrario di grado $n \geq 1$ appartenente a $F[x]$. Allora esiste un ampliamento finito E di F in cui $f(x)$ ha una radice. Risulta inoltre*

$$[E : F] \leq n .$$

Dimostrazione. Sia $p(x)$ un fattore irriducibile di $f(x)$. Per il lemma precedente, esiste un ampliamento E di F dove $p(x)$ ha una radice (e quindi anche $f(x)$ ha una radice), e $[E : F] = \partial p(x) \leq n$. \square

6.2.6 ESEMPIO. Sia $f(x) = x^4 - 2x^2 - 3 \in \mathbb{Q}[x]$. Risulta $f(x) = (x^2 - 3)(x^2 + 1)$. Entrambi i polinomi fattori sono irriducibili su \mathbb{Q} . Prendiamo $p(x) = x^2 - 3$. Abbiamo appena visto che il campo $E = \mathbb{Q}[x]/(x^2 - 3)$ possiede una radice di $x^2 - 3$: quindi possiede anche una radice di $f(x)$. Risulta $[E : \mathbb{Q}] = 2 < 4 = \partial f(x)$. \square

Ricordando la definizione 6.1.25 di campo algebricamente chiuso, si hanno le seguenti caratterizzazioni.

6.2.7 TEOREMA. *Sia K un campo. Allora le seguenti affermazioni sono equivalenti:*

- (a) *K è algebricamente chiuso;*
- (b) *ogni polinomio non costante $f(x) \in K[x]$ si fattorizza in fattori lineari in $K[x]$;*
- (c) *ogni polinomio non costante $f(x) \in K[x]$ ammette una radice in K .*

Dimostrazione. (a) \Rightarrow (b) Per induzione sul grado n di f . Se $n = 1$, f è lineare, e non c'è nulla da provare. Sia allora $n > 1$ e supponiamo vero il teorema per tutti i polinomi di grado $< n$. Aggiungendo a K una radice α di f , si ottiene una estensione $K(\alpha)$ che è finita (cfr. teorema 6.1.16) e quindi algebrica. Ne segue che $K(\alpha) = K$, ossia $\alpha \in K$. Allora esiste un $g(x) \in K[x]$ tale che $f(x) = (x - \alpha)g(x)$. Il risultato segue per l'induzione ammessa.

(b) \Rightarrow (c) Ovvio.

(c) \Rightarrow (a) Supponiamo per assurdo che esista un'estensione algebrica propria E di K : sia α un elemento (ovviamente algebrico su K) $\in E \setminus K$. Allora α soddisfa un polinomio irriducibile di grado > 1 in $K[x]$: ma questo contraddice il fatto che per ipotesi tale polinomio deve avere una radice in K (e quindi non può essere irriducibile). \square

Siamo ora in grado di dimostrare il teorema di esistenza di un campo di spezzamento per ogni polinomio.

6.2.8 TEOREMA. *Sia $f(x) \in F[x]$ un polinomio di grado $n \geq 1$. Allora esiste un ampliamento E di F di grado $\leq n!$ dove $f(x)$ ha tutte le radici.*

Dimostrazione. Procediamo per induzione sul grado n del polinomio. Per $n = 1$ il polinomio ammette tutte le radici (cioè una) in F , e quindi $E = F$. Supponiamo di avere dimostrato il teorema per tutti i polinomi di grado $n - 1$, e dimostriamolo per i polinomi di grado n . Per il lemma precedente, esiste un ampliamento E_0 di F , con $[E_0 : F] \leq n$, dove $f(x)$ ha una radice α . Allora in $E_0[x]$ si ha la seguente fattorizzazione:

$$f(x) = (x - \alpha)g(x), \quad g(x) \in E_0[x], \quad \partial g(x) = n - 1.$$

Per l'induzione ammessa, esiste un ampliamento finito E di E_0 con $[E : E_0] \leq (n - 1)!$, in cui $g(x)$ ha $n - 1$ radici (si veda la figura 6.7).

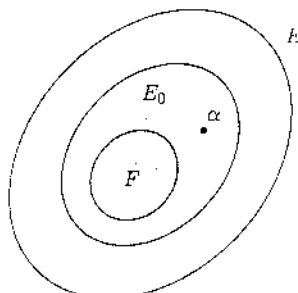


FIGURA 6.7

Dato che le radici di $f(x)$ sono o la radice α , oppure le radici di $g(x)$, ne segue che E è un'estensione di F che contiene tutte le radici di $f(x)$. \square

Una volta dimostrato che esiste un ampliamento *finito* di F che contiene tutte le radici di $f(x)$, esisterà ovviamente anche un ampliamento *finito minimo* con questa proprietà. Quindi il teorema ora dimostrato ci garantisce l'esistenza di un per ogni polinomio $f(x) \in F[x]$. Questo teorema ci garantisce anche che il grado $[E : F]$ è limitato superiormente da $n!$, dove n è il grado del polinomio.

È chiaro dalla dimostrazione dei teoremi che si può arrivare al campo di spezzamento di un polinomio per vie diverse, quindi, una volta dimostrata l'esistenza di un campo di spezzamento per un polinomio, resta il problema di confrontare tra di loro i campi di spezzamento di uno stesso polinomio. Il problema che affronteremo ora riguarda quindi la *unicità* o meno di un campo di spezzamento di un dato polinomio.

Il seguente teorema dimostra l'unicità del campo di spezzamento di un polinomio.

6.2.9 TEOREMA. *Tutti i campi di spezzamento di un polinomio $f(x) \in F[x]$ sono tra di loro isomorfi.*

Abbiamo bisogno di alcune definizioni, prima di procedere nella dimostrazione del teorema.

6.2.10 DEFINIZIONE. Sia φ un isomorfismo tra due campi F e F' . Se R e R' sono due anelli (o due campi) tali che $R \supseteq F$ e $R' \supseteq F'$, allora si dice che un isomorfismo ψ tra R e R' è una *estensione* dell'isomorfismo φ se $\psi|_F$ coincide con φ . \square

Siano ora F e F' due campi isomorfi tra di loro mediante un isomorfismo τ . Allora si può estendere tale isomorfismo τ ad un isomorfismo $\tilde{\tau}$ tra $F[x]$ e

$F'[x]$ ponendo

$$\begin{aligned}\bar{\tau} : F[x] &\longrightarrow F'[x] \\ x &\longmapsto x \\ a &\longmapsto \tau(a) \quad \forall a \in F.\end{aligned}$$

Se $f(x) = \sum_{i=1}^n a_i x^i$, allora $\bar{\tau}(f(x)) = \sum_{i=1}^n \tau(a_i) x^i$.

6.2.11 TEOREMA. *Sia τ un isomorfismo tra i due campi F e F' e siano $f(x)$ e $f'(x)$ due polinomi tali che $f'(x) = \bar{\tau}(f(x))$, essendo $\bar{\tau}$ l'isomorfismo definito sopra. Sia E un campo di spezzamento di $f(x)$ e E' un campo di spezzamento di $f'(x)$. Allora l'isomorfismo τ tra F e F' si può estendere ad un isomorfismo $\bar{\Psi}$ tra E ed E' .*

Dimostrazione. La dimostrazione procede per induzione sul numero k , dove k è il numero di radici di $f(x)$ che non appartengono ad F . Se $k = 0$, allora tutte le radici di $f(x)$ stanno in F , per cui $f(x)$ si spezza in F in fattori lineari, da cui $E = F$. Per l'isomorfismo $\bar{\tau}$, anche $f'(x) = \bar{\tau}f(x)$ si spezza in F' , per cui $E' = F'$. L'isomorfismo originario τ tra F e F' è pertanto un isomorfismo tra E ed E' e $\bar{\Psi} = \tau$.

Supponiamo ora di aver provato il teorema per ogni polinomio che abbia al più $k - 1$ radici fuori di F . Dimostriamolo nel caso in cui $f(x)$ abbia k radici fuori di F . Fattorizziamo $f(x)$ in fattori irriducibili su F :

$$f(x) = p_1(x)p_2(x) \cdots p_r(x), \quad p_i(x) \in F[x]$$

e sia

$$f'(x) = p'_1(x)p'_2(x) \cdots p'_r(x), \quad p'_i(x) \in F'[x]$$

la corrispondente (mediante $\bar{\tau}$) fattorizzazione di $f'(x)$. Almeno uno dei fattori $p_i(x)$ (possiamo supporre che sia $p_1(x)$), deve avere grado strettamente maggiore di 1, altrimenti tutte le radici sarebbero in F e sarebbe $k = 0$, caso che abbiamo già provato. Sia α una radice di $p_1(x)$. Allora anche $f'(x) = \bar{\tau}(f(x))$ ha un fattore irriducibile, $p'_1(x)$, di grado strettamente maggiore di 1, e sia α' una radice di $p'_1(x)$. Se $n = \partial p_1(x)$, l'applicazione

$$\begin{aligned}F[x]/(p_1(x)) &\longrightarrow F'[x]/(p'_1(x)) \\ \sum_{i=0}^{n-1} a_i x^i + (p_1(x)) &\longmapsto \sum_{i=0}^{n-1} a'_i x^i + (p'_1(x)), \quad a'_i = \tau(a_i)\end{aligned}$$

è un isomorfismo (verificare). D'altra parte valgono i seguenti isomorfismi:

$$F(\alpha) \xrightarrow{\cong} F[x]/(p_1(x))$$

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mapsto a_0 + a_1x + \cdots + a_{n-1}x^{n-1} = (p_1(x)).$$

$$F'(\alpha') \xrightarrow{\cong} F'[x]/(p'_1(x))$$

$$a'_0 + a'_1\alpha' + \cdots + a'_{n-1}\alpha'^{n-1} \mapsto a'_0 + a'_1x + \cdots + a'_{n-1}x^{n-1} = (p'_1(x)).$$

Per la transitività della relazione di isomorfismo, segue che

$$F(\alpha) \xrightarrow{\cong} F'(\alpha')$$

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mapsto a'_0 + a'_1\alpha' + \cdots + a'_{n-1}\alpha'^{n-1}.$$

Quest'ultimo isomorfismo, che chiameremo Ψ , è una estensione di τ . Partiamo ora dai campi $F(\alpha)$ e $F'(\alpha') = \Psi(F(\alpha))$ come campi base (si veda la figura 6.8).

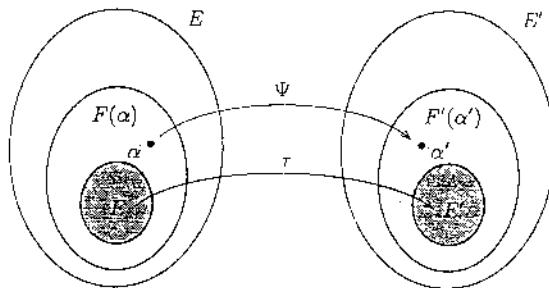


FIGURA 6.8

Allora $f(x)$ ha al più $k - 1$ radici fuori di $F(\alpha)$ e $f'(x)$ ha al più $k - 1$ radici fuori di $F'(\alpha')$. Quindi Ψ , per l'ipotesi induttiva, si può estendere ad un isomorfismo $\bar{\Psi}$ tra E ed E' . Tale isomorfismo $\bar{\Psi}$ è ovviamente anche una estensione dell'isomorfismo τ , con il che abbiamo concluso il teorema. \square

6.2.12 COROLLARIO. *Tutti i campi di spezzamento di un polinomio $f(x) \in F[x]$ sono isomorfi in un isomorfismo che fissa F .*

Dimostrazione. Basta porre nel teorema precedente $F' = F$, e τ l'applicazione identica. Se E ed E' sono due campi di spezzamento di $f(x)$, allora $E \simeq E'$ (in un isomorfismo che subordina l'automorfismo identico su F), in virtù del teorema precedente. \square

6.2.13 COROLLARIO. *Sia $p(x) \in F[x]$ un polinomio irriducibile e siano α e β due radici di $p(x)$. Allora*

$$F(\alpha) \simeq F(\beta)$$

secondo un isomorfismo che porta α in β e lascia fissi gli elementi di F .

Dimostrazione. Gli isomorfismi del teorema 6.2.11 diventano

$$\begin{aligned} F(\alpha) &\simeq F[x]/(p(x)) \simeq F(\beta) \\ a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} &\longrightarrow a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + (p(x)) \\ &\longmapsto a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1}. \quad \square \end{aligned}$$

Ad esempio, le tre radici del polinomio irriducibile su \mathbb{Q} $x^3 - 2$ sono $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$, ω radice terza primitiva dell'unità. Risulta

$$\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}(\sqrt[3]{2}\omega) \simeq \mathbb{Q}(\sqrt[3]{2}\omega^2).$$

Ogni isomorfismo è tale che fissa \mathbb{Q} e manda una radice in un'altra. Si osservi che è essenziale l'ipotesi che il polinomio sia irriducibile.

 **ATTENZIONE.** Si stia attenti però: si tratta di tre estensioni tutte isomorfe tra di loro, ma nessuna delle tre è il campo di spezzamento di $x^3 - 2$: il campo di spezzamento di $x^3 - 2$ ha grado 6 ed è $\mathbb{Q}(\sqrt[3]{2}, \omega)$. \square

Chindiamo con la seguente proposizione.

6.2.14 PROPOSIZIONE. *Per ogni fissato intero positivo $n \in \mathbb{N}$ il campo di spezzamento di $x^n - 1$ su \mathbb{Q} è $\mathbb{Q}(\zeta)$, dove ζ è una qualunque radice n -esima primitiva dell'unità. Risulta $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$, $\varphi(n)$ essendo la funzione di Eulero di n .*

Dimostrazione. Tutte le radici n -esime dell'unità sono potenze di una radice n -esima primitiva, quindi per ottenere il campo di spezzamento basta aggiungere a \mathbb{Q} una qualunque radice n -esima primitiva dell'unità. Inoltre risulta $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ perché il polinomio minimo di ζ è l' n -esimo polinomio, $\Phi_n(x)$, che è irriducibile su \mathbb{Q} e ha grado $\varphi(n)$. \square

ESERCIZI.

- Si determinino tutti i polinomi irriducibili $p(x)$ di secondo grado a coefficienti in \mathbb{Z}_2 . Per ciascuno di questi si determini il campo $\mathbb{Z}_2[x]/(p(x))$.
- Si provi che il polinomio $f(x) = x^3 + x^2 + 1$ è irriducibile su \mathbb{Z}_2 . Indicata con α una sua radice (che quindi non appartiene a \mathbb{Z}_2 , ma a $\mathbb{Z}_2(\alpha)$), si provi che $\mathbb{Z}_2(\alpha)$ è il campo di spezzamento di $f(x)$.
- Sia α una radice del polinomio $x^2 + x + 1 \in \mathbb{Z}_5[x]$, irriducibile su \mathbb{Z}_5 . Si studi l'estensione $\mathbb{Z}_5(\alpha)$.
- Si dica se il polinomio $x^2 + 1$ è riducibile o irriducibile su \mathbb{Z}_3 . Si elenchino gli elementi di $\mathbb{Z}_3(\alpha)$, dove α è una radice di $x^2 + 1$. Si diano le tavole di addizione e moltiplicazione di $\mathbb{Z}_3(\alpha)$.
- Determinare l'inverso dell'elemento $3 + a$ in $\mathbb{Z}_5(a)$, dove a è radice del polinomio $x^2 + x + 1$.

6. Si determini il campo di spezzamento su \mathbb{Q} di ciascuno dei seguenti polinomi appartenenti a $\mathbb{Q}[x]$:

$$\begin{aligned} &x^3 + 2x^2 + 5x + 10 \\ &x^4 - 7x^2 + 10 \\ &x^5 + 2x^4 - 5x^3 - 10x^2 + 6x + 12 \\ &x^3 - 1 \\ &x^6 - x^4 - 4x^2 - 4 \\ &x^4 - 4x^2 - 2. \end{aligned}$$

7. Si determini il campo di spezzamento su $\mathbb{Q}(\sqrt{3})$ del polinomio di $\mathbb{Q}(\sqrt{3})[x]$

$$x^3 - \sqrt{3}x^2 - 2x - 2\sqrt{3}.$$



CONTROLLO.

1. Campo di spezzamento su F di un polinomio $f(x) \in F[x]$ è ...
2. Il grado su F del campo di spezzamento di un polinomio $f(x) \in F[x]$ è legato in qualche modo al grado di $f(x)$?

6.3. Campi finiti

In questo paragrafo studieremo i campi con un numero finito di elementi. Tali campi hanno, come si è già visto, caratteristica p , cioè sono estensioni di \mathbb{Z}_p . Prima di procedere in questo studio però ci serviranno ulteriori risultati sui polinomi, e in particolare sulle radici multiple di un polinomio.

Diamo innanzitutto la definizione *formale* (che non fa intervenire la nozione di limite) di derivata di un polinomio.

6.3.1 DEFINIZIONE. Sia F un campo e sia $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ un polinomio in $F[x]$. Si definisce *derivata* di $f(x)$, e si indica con $f'(x)$, il polinomio appartenente a $F[x]$

$$f'(x) \stackrel{\text{def}}{=} na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2x + a_1. \quad \square$$

È facile controllare che valgono le stesse proprietà della derivazione ordinaria, ossia

$$(f(x) + g(x))' = f'(x) + g'(x), \quad (f(x)g(x))' = f'(x)g(x) + f(x)g'(x).$$

6.3.2 PROPOSIZIONE. Un polinomio $f(x) \in F[x]$ ha una radice multiplo (in una opportuna estensione) se e solo se $f(x)$ e $f'(x)$ hanno in comune un fattore non banale (ossia di grado maggiore di zero).

Dimostrazione. Si noti che non occorre dire dove $f(x)$ e $f'(x)$ hanno in comune un fattore non banale, perché se $f(x)$ e $f'(x)$ hanno in comune un fattore non banale in un campo $K \supseteq F$, allora essi hanno un fattore comune non banale anche in F , perché altrimenti la relazione

$$s(x)f(x) + t(x)f'(x) = 1, \quad s(x), t(x) \in F[x]$$

che dice che $f(x)$ e $f'(x)$ sono coprimi in F sarebbe una relazione anche in K , per cui i due polinomi sarebbero coprimi anche in K . Sia dunque α una radice multipla di $f(x)$, cioè

$$f(x) = (x - \alpha)^m g(x), \quad m > 1.$$

Allora

$$f'(x) = m(x - \alpha)^{m-1}g(x) + (x - \alpha)^m g'(x)$$

da cui risulta che α è radice anche di $f'(x)$.

Viceversa, supponiamo che $f(x)$ e $f'(x)$ abbiano un fattore comune non banale. Supponiamo per assurdo che $f(x)$ non abbia radici multiple, cioè sia

$$f(x) = \prod_{i=1}^n (x - \alpha_i),$$

con α_i tutte distinte tra di loro. Allora

$$f'(x) = \sum_{i=1}^n (x - \alpha_1)(x - \alpha_2) \cdots (\widehat{x - \alpha_i}) \cdots (x - \alpha_n)$$

da cui, come si vede facilmente, risulta $f'(\alpha_i) \neq 0$ per ogni $i = 1, \dots, n$, e questo contraddice l'ipotesi che $f(x)$ e $f'(x)$ abbiano un fattore comune. \square

6.3.3 DEFINIZIONE. Un polinomio irriducibile $f(x) \in F[x]$ si dice *separabile* se è privo di radici multiple. Se non è separabile, si dice *inseparabile*.

Ciò significa che nel suo campo di spezzamento un polinomio separabile $f(x)$ si fattorizza al modo seguente

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

con le α_i tutte distinte. \square

6.3.4 ESEMPIO DI POLINOMIO SEPARABILE. Il polinomio $f(x) = x^2 - 3 \in \mathbb{Q}[x]$ è irriducibile su \mathbb{Q} , e ha tutte radici distinte.

6.3.5 ESEMPIO DI POLINOMIO INSEPARABILE. Sia $K = \mathbb{Z}_3(t)$ il campo delle funzioni razionali nell'indeterminata t , a coefficienti in \mathbb{Z}_3 . Il polinomio

$$f(x) = x^3 - t \in \mathbb{Z}_3(t)[x]$$

è inseparabile. Sia infatti α uno zero di $f(x)$ (nel suo campo di spezzamento). Allora deve risultare $\alpha^3 - t = 0$, da cui

$$(x - \alpha)^3 = x^3 - \alpha^3 = x^3 - t = f(x).$$

Quindi, se β è un'altra radice di $f(x)$ allora

$$0 = f(\beta) = (\beta - \alpha)^3 \implies \beta = \alpha$$

ossia tutte le radici sono uguali.

Resta da provare che $f(x) = x^3 - t$ è irriducibile su $K = \mathbb{Z}_3(t)$. Se fosse riducibile, dato che si tratta di un polinomio di terzo grado, avrebbe una radice in K , cioè esisterebbe una funzione razionale

$$\alpha(t) = \frac{a_0 + a_1 t + \cdots + a_r t^r}{b_0 + b_1 t + \cdots + b_s t^s}, \quad a_i, b_i \in \mathbb{Z}_3$$

talé che $\alpha^3 = t$. Ma questo non può accadere, come è facile controllare.

La proposizione che segue ci dice in quali casi un polinomio irriducibile possiede radici multiple.

6.3.6 PROPOSIZIONE. *Sia $f(x)$ un polinomio irriducibile appartenente a $F[x]$. Allora, se F ha caratteristica zero, $f(x)$ non è mai inseparabile. Se F ha caratteristica p , $f(x)$ è inseparabile se e solo se $f(x) = g(x^p)$, ossia è un polinomio nella variabile x^p :*

$$f(x) = a_0 + a_1 x^p + \cdots + a_n x^{np}.$$

Dimostrazione. Sappiamo che un polinomio $f(x)$ è inseparabile se e solo se $f(x)$ e $f'(x)$ hanno un fattore comune di grado ≥ 1 . Ma, dato che in questo caso $f(x)$ è irriducibile, e dato che $f'(x)$ ha grado inferiore al grado di $f(x)$, ne segue che un polinomio irriducibile è inseparabile se e solo se $f'(x) = 0$, ossia

$$(6.3.1) \quad i a_i = 0 \quad \forall i = 1, \dots, n.$$

Ora, in caratteristica zero queste relazioni implicano $a_i = 0$ per ogni $i = 1, \dots, n$, ossia $f(x)$ si riduce ad una costante a_0 , che è priva di radici. In caratteristica p le (6.3.1) implicano che si devono annullare quegli a_i tali che non sia $i \equiv 0 \pmod{p}$. Quindi $f(x)$ è un polinomio in cui restano solo i monomi corrispondenti alle potenze di x^p . Viceversa, ogni tale polinomio è effettivamente inseparabile, perché la sua derivata è zero. Abbiamo concluso la dimostrazione. \square

Passiamo ad esaminare la struttura dei campi finiti. Proveremo i seguenti fatti.

- (1) Ogni campo finito ha p^n elementi, p numero primo.
- (2) Due campi finiti con lo stesso numero p^n di elementi sono isomorfi.

- (3) Dato comunque un numero primo p ed un intero positivo n esiste un campo con p^n elementi.

6.3.7 TEOREMA. *Ogni campo finito K possiede p^n elementi, p essendo un numero primo.*

Dimostrazione. Questo risultato era già stato dimostrato nell'esercizio 6.1.10, ad ogni modo lo ripetiamo per completezza. Ogni campo finito K ha caratteristica finita p , ed è pertanto estensione del campo \mathbb{Z}_p . Risulta pertanto uno spazio vettoriale di dimensione n su \mathbb{Z}_p , e in quanto tale possiede p^n elementi. \square

6.3.8 LEMMA. *Ogni elemento a di un campo finito con p^n elementi soddisfa la relazione*

$$a^{p^n} = a .$$

Dimostrazione. Se $a = 0$ la relazione è vera. Prendiamo allora gli elementi $a \neq 0$ in K . Essi formano un gruppo moltiplicativo con $p^n - 1$ elementi, e quindi ogni $a \neq 0$ soddisfa (per i ben noti risultati di teoria dei gruppi)

$$a^{p^n-1} = 1 .$$

Moltiplicando per a , si ottiene la relazione richiesta. \square

6.3.9 LEMMA. *Un campo K con p^n elementi è il campo di spezzamento del polinomio*

$$x^{p^n} - x \in \mathbb{Z}_p[x] .$$

Dimostrazione. Per il lemma precedente, i p^n elementi del campo K soddisfano il polinomio $x^{p^n} - x$. Tale polinomio non può avere altre radici, dato che il suo grado è p^n . Quindi il polinomio $x^{p^n} - x$ si spezza in K . Non può spezzarsi in un campo più piccolo, perché perderemmo altrimenti qualche radice. Quindi K è il campo di spezzamento di $x^{p^n} - x$. \square

6.3.10 TEOREMA. *Due campi con p^n elementi sono isomorfi.*

Dimostrazione. Sono entrambi campi di spezzamento dello stesso polinomio $x^{p^n} - x$ e pertanto sono isomorfi, per l'unicità dei campi di spezzamento di uno stesso polinomio. \square

Passiamo ora a provare l'esistenza di un campo con p^n elementi per ogni valore di p primo ed n .

6.3.11 TEOREMA. *Dati comunque un numero primo p e un intero positivo n , esiste un campo con p^n elementi.*

Dimostrazione. Costruiamo, a partire dai due interi n e p , il seguente polinomio, a coefficienti in \mathbb{Z}_p ,

$$x^{p^n} - x.$$

Nel campo di spezzamento L (sicuramente esistente) di tale polinomio, si consideri il sottoinsieme

$$K \stackrel{\text{def}}{=} \{a \in L \mid a^{p^n} = a\}.$$

La cardinalità di K uguaglia il numero di radici distinte di $x^{p^n} - x$: ma queste radici sono tutte distinte (si calcoli la derivata del polinomio!). Quindi $|K| = p^n$. Se facciamo vedere che tale sottoinsieme è un campo, avremo trovato il campo desiderato, che coinciderà con L . Basta provare che per ogni $a, b \in K$, $a \pm b$, ab e ab^{-1} stanno ancora in K . Infatti sono verificate le seguenti uguaglianze modulo p

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n} = a \pm b$$

$$(ab)^{p^n} = a^{p^n}b^{p^n} = ab$$

$$(ab^{-1})^{p^n} = a^{p^n}(b^{p^n})^{-1} = ab^{-1}. \quad \square$$

Concludiamo con qualche risultato che ci dà una idea più precisa della struttura di un campo finito.

6.3.12 TEOREMA. Il gruppo moltiplicativo di un campo finito è ciclico.

Dimostrazione. Si osservi che l'ipotesi di finitezza è essenziale: il teorema cioè è falso nel caso di campi infiniti; ad esempio, $(\mathbb{R} \setminus \{0\}, \cdot)$ non è ciclico, dato che contiene un elemento, -1 che ha periodo 2, mentre un tale elemento non esiste in $(\mathbb{Z}, +)$. Sia dunque K un campo finito. Consideriamo il suo gruppo moltiplicativo $K^* = K \setminus \{0\}$. In quanto gruppo abeliano finito, sarà (utilizzando le stesse notazioni del teorema di struttura dei gruppi abeliani finiti)

$$K^* = \Sigma_{q_1} \Sigma_{q_2} \cdots \Sigma_{q_r}$$

dove i q_i sono i primi che compaiono nella fattorizzazione dell'ordine $p^n - 1$ di K^* , le Σ_{q_i} sono le componenti primarie, ciascuna delle quali è prodotto di gruppi ciclici. Per provare che K^* è ciclico basta provare che ogni Σ_{q_i} è ciclico, cioè che possiede un elemento di periodo uguale al suo ordine. Per non appesantire la notazione, poniamo $\Sigma_{q_i} = \Sigma_q$:

$$\Sigma_q = \mathbb{Z}_{q^{\alpha_1}} \times \mathbb{Z}_{q^{\alpha_2}} \times \cdots \times \mathbb{Z}_{q^{\alpha_r}}$$

con $\alpha_1 + \alpha_2 + \cdots + \alpha_r = \alpha$, dove $|\Sigma_q| = q^\alpha$. Supponiamo per assurdo che l'ordine massimo degli elementi di Σ_q sia $q^{\alpha_1} < q^\alpha$. Allora ogni elemento s di Σ_q è tale che $s^{q^{\alpha_1}} = 1$. Ma allora avremmo l'assurdo che il polinomio $x^{q^{\alpha_1}} - 1$ possiede più radici del suo grado. \square

6.3.13 PROPOSIZIONE. *Ogni campo finito F di caratteristica p possiede un automorfismo σ tale che $\sigma(a) = a^p$ per ogni $a \in F$.*

Dimostrazione. σ è bivoca e conserva le operazioni (controllare). \square

L'automorfismo σ della proposizione prende il nome di *automorfismo di Frobenius*.



ESERCIZI.

- Si dica se esistono campi dei seguenti ordini:

16. 36. 401. 3763.

Per i casi in cui esistano, si costruiscano.

- Sia K un campo, con $|K| = p^n$. Si provi che esiste un polinomio $p(x) \in \mathbb{Z}_p[x]$ di grado n , tale che $K \cong \mathbb{Z}_p[x]/(p(x))$.
- Costruire un campo con 25 elementi.
- Sia K un campo con $|K| = p^n$. Se F è un sottocampo di K , si provi che $|F| = p^m$, dove m divide n . Viceversa, si provi che per ogni divisore m di n esiste un unico sottocampo F di K con $|F| = p^m$.
- Sulla base dell'esercizio precedente, si determinino tutti i sottocampi di un campo con 32 elementi, tutti i sottocampi di un campo con 125 elementi e tutti i sottocampi di un campo con 15625 elementi.



CONTROLLO.

- Un polinomio è separabile quando ...
- Esistono polinomi irriducibili con radici multiple? In quali casi?
- Quali sono le possibili cardinalità per un campo finito? In corrispondenza a ciascuna delle possibili cardinalità esiste sempre un campo con quella cardinalità? Quanti ne esistono?

6.4. Il teorema di Wedderburn sui corpi finiti

In questo paragrafo dimostreremo un bellissimo teorema, dovuto a Wedderburn, che prova che ogni corpo finito è un campo.

Ricordiamo che un corpo è un anello con unità in cui ogni elemento non nullo è invertibile: non si richiede che la moltiplicazione sia commutativa. Un esempio di corpo (effettivamente non commutativo) è il seguente, detto corpo dei quaternioni reali, introdotto da Hamilton:

$$\mathbb{H} = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \mid \alpha_0, \dots, \alpha_3 \in \mathbb{R}\}.$$

$$i^2 = j^2 = k^2 = ijk = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j\}.$$

Si invita lo studente a fare tutte le verifiche. Si tratta ovviamente di un corpo infinito (dato che contiene i numeri reali e i numeri complessi).

Il teorema che dimostreremo ci dice che non troveremo mai corpi (non commutativi) finiti.

6.4.1 TEOREMA DI WEDDERBURN. *Ogni corpo finito K è un campo.*

Dimostrazione. Seguiremo la dimostrazione data in [24]. Si tratta di una dimostrazione interessante, perché fa intervenire tanti risultati di varia natura studiati nel corso.

Dimostreremo il teorema provando che il centro $Z(K) = \{k \in K : kx = xk \forall x \in K\}$ coincide con K .

Sia $|Z(K)| = q$. Essendo $Z(K)$ un sottocampo di K , K è uno spazio vettoriale su $Z(K)$, e in quanto tale ha q^n elementi. Dovremo quindi provare che $n = 1$. Sia $a \in K$, e sia $C(a)$ il suo centralizzante: si tratta di un sottocorpo di K contenente il centro, quindi avrà $q^{n(a)}$ elementi. Asseriamo che $n(a)$ divide n . $C(a)^* = C(a) \setminus \{0\}$ è un sottogruppo del gruppo moltiplicativo K^* di K , quindi, per il teorema di Lagrange, $q^{n(a)} - 1$ è un divisore di $q^n - 1$ e quindi $n(a) \mid n$ (esercizio 6.4.1). Nel gruppo K^* l'equazione delle classi (cfr. (5.11.4)) si scrive al modo seguente:

$$(6.4.1) \quad q^n - 1 = q - 1 + \sum_{n(a) \mid n, n(a) \neq n} \frac{q^n - 1}{q^{n(a)} - 1}.$$

La condizione $n(a) \neq n$ equivale alla condizione $a \notin Z(K^*)$. La relazione (6.4.1) è una relazione tra interi. Faremo vedere che se $n > 1$ tale relazione non può essere verificata.

Basterà provare che esiste un intero che divide $(q^n - 1)/(q^{n(a)} - 1)$ per tutti i divisori $n(a)$ di n diversi da n , ma che non divide $q - 1$: in tal caso la (6.4.1) sarà impossibile, a meno che non sia $n = 1$. Per la determinazione di questo intero (che dipende da n e da q) ci verrà in aiuto l' n -esimo polinomio ciclotomico $\Phi_n(x)$ che, come sappiamo, è un polinomio a coefficienti interi. La relazione

$$x^n - 1 = \Phi_n(x)(x^d - 1) \prod_{k|n, k \neq d} \Phi_k(x)$$

è una relazione del tipo

$$x^n - 1 = \Phi_n(x)(x^d - 1)f(x), \quad f(x) \in \mathbb{Z}[x]$$

che vale qualunque sia x . In particolare quindi per ogni intero t

$$\Phi_n(t) \mid \frac{t^n - 1}{t^d - 1}, \quad d \mid n, \quad d \neq n.$$

Per $t = q$ si avrà pertanto

$$\Phi_n(q) \mid \frac{q^n - 1}{q^{n(a)} - 1} \quad \forall n(a) \mid n, \quad n(a) \neq n.$$

D'altra parte $\Phi_n(q)$ divide anche $q^n - 1$, per cui, in base alla (6.4.1), dovrebbe dividere $q - 1$. In particolare dovrebbe essere $|\Phi_n(q)| \leq q - 1$. Ma se $n > 1$ questo è impossibile: infatti $\Phi_n(q) = \prod(q - \vartheta^i)$, con ϑ variabile tra tutte le radici n -esime primitive dell'unità, e $|q - \vartheta| > |q^i - \vartheta| = q - 1$, cioè $|\Phi_n(q)| = \prod(q - \vartheta) > q - 1$ (si veda la figura 6.9).

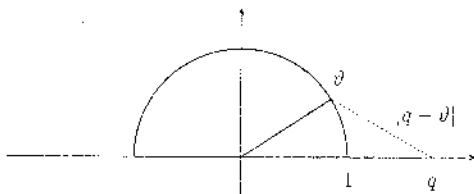


FIGURA 6.9

Deve quindi necessariamente essere $n = 1$ e il teorema è provato. \square

ESERCIZI.

- Si provi che se t è un intero maggiore di 1, e $t^m - 1$ divide $t^n - 1$, allora $m \mid n$.

6.5. Estensioni normali

Abbiamo già visto che, dato un polinomio irriducibile in $F[x]$ e una sua radice α , non è detto che il campo di spezzamento di $f(x)$ sia $F(\alpha)$, cioè non è detto che il campo che contiene una radice di un polinomio irriducibile contenga tutte le radici. Si è visto infatti che $\sqrt[3]{2}$ è radice del polinomio irriducibile su \mathbb{Q} $x^3 - 2$, ma $\mathbb{Q}(\sqrt[3]{2})$ non è il campo di spezzamento di $x^3 - 2$.

6.5.1 DEFINIZIONE. Sia K un'estensione di un campo F . Due elementi α e β di K , algebrici sopra F , si dicono *coniugati su F* se hanno lo stesso polinomio minimo su F . \square

Ad esempio, $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ e $\omega^2\sqrt[3]{2}$, dove ω è una radice terza primitiva dell'unità, sono elementi coniugati, perché radici di uno stesso polinomio irriducibile, che è anche il loro polinomio minimo (si ricordi che ogni polinomio irriducibile è polinomio minimo per ciascuna delle sue radici).

Sussiste la seguente proposizione.

6.5.2 PROPOSIZIONE. *Sia K un'estensione del campo F . Allora le seguenti asserzioni sono equivalenti:*

- l'estensione K su F è chiusa rispetto ai coniugati, ossia se $F \subseteq L \subseteq K$, $a \in K$ e $b \in L$ è coniugato di a su F , allora b sta in K (in altre parole, se K contiene un elemento, contiene tutti i suoi coniugati);*

- (b) se $f(x)$ è un polinomio irriducibile in $F[x]$, e se α è una radice di $f(x)$ che sta in K , allora $f(x)$ si spezza in K , cioè K contiene tutte le radici di $f(x)$.

Dimostrazione. (a) \Rightarrow (b) Sia α una radice del polinomio irriducibile $f(x) \in F[x]$. Sia L il campo di spezzamento di $f(x)$ su K , e β una radice di $f(x)$ in L . Allora risulta $F \subseteq K \subseteq L$ e quindi, essendo K chiusa rispetto ai coniugati, β appartiene a K . Pertanto $f(x)$ si spezza su K .

(b) \Rightarrow (a) Sia $F \subseteq K \subseteq L$, sia $a \in K$ e $b \in L$, b coniugato ad a su F . Allora a e b hanno lo stesso polinomio minimo $f(x)$ su F , e quindi anche b sta in K . \square

Ricordando che un sottogruppo N di un gruppo G si dice *normale* in G se contenendo un elemento contiene tutti i suoi coniugati, appare naturale dare la seguente definizione.

6.5.3 DEFINIZIONE. Un'estensione K di F si dice estensione *normale* di F se K è chiusa rispetto ai coniugati. \square

Il prossimo teorema mostra il legame tra estensioni normali e campi di spezzamento.

6.5.4 TEOREMA. Un'estensione K di un campo F è finita e normale se e solo se K è il campo di spezzamento di qualche polinomio di $F[x]$.

Dimostrazione. Sia K un'estensione finita e normale di F . Allora risulta (per il solo fatto di essere un'estensione finita)

$$K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$$

per certi α_i algebrici su F . Sia $p_i(x) \in F[x]$ il polinomio minimo di α_i . Poniamo

$$f(x) \stackrel{\text{def}}{=} p_1(x)p_2(x) \cdots p_n(x).$$

Ogni $p_i(x)$ è irriducibile su F , possiede uno zero α_i in K e quindi, per la normalità di K su F si spezza su K . Quindi anche $f(x)$ si spezza su K . Dato che K è generato da F e dagli α_i (che sono gli zeri di $f(x)$), segue che K è campo di spezzamento di $f(x)$.

Sia ora K campo di spezzamento su F di qualche polinomio $f(x) \in F[x]$. Per definizione di campo di spezzamento, l'estensione K su F è finita. Dobbiamo provare che si tratta di un'estensione normale, ossia che ogni polinomio $g(x)$ irriducibile in $F[x]$, che abbia una radice α in K , si spezza in K . Sia $L \supseteq K$ il campo di spezzamento del polinomio $f(x)g(x)$, che contiene il campo di spezzamento K di $f(x)$. Sia β un'altra radice di $g(x)$, che apparirà ad L . Si tratta di far vedere che β sta in K . Dato che α sta in K , risulta

$$[K(\alpha) : K] = 1.$$

Basta quindi provare che anche $[K(\beta) : K] = [K(\alpha) : K]$ ($\doteq 1$). Consideriamo allora le estensioni mostrate in figura 6.10.

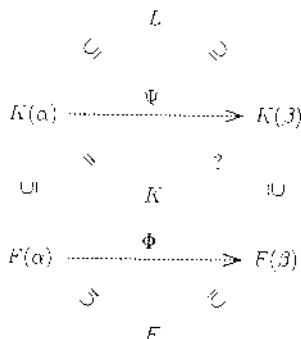


FIGURA 6.10

Dato che α e β hanno lo stesso polinomio minimo $g(x)$, risulta

$$[F(\alpha) : F] = [F(\beta) : F]$$

e inoltre esiste un isomorfismo

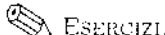
$$\begin{aligned}
 \phi : F(\alpha) &\longrightarrow F(\beta) \\
 \alpha &\longmapsto \beta \\
 a &\longmapsto a \quad \forall a \in F .
 \end{aligned}$$

Dato che K era il campo di spezzamento di $f(x)$ su F , $K(\alpha)$ risulta il campo di spezzamento di $f(x)$ sopra $F(\alpha)$. Analogamente, $K(\beta)$ è il campo di spezzamento di $f(x)$ sopra $F(\beta)$. Esiste allora un'estensione dell'isomorfismo ϕ ad un isomorfismo $\psi : K(\alpha) \rightarrow K(\beta)$ tale che $\psi|_{F(\alpha)} \equiv \phi$. Inoltre $[K(\alpha) : F(\alpha)] = [K(\beta) : F(\beta)]$. Usando ora ripetutamente il teorema dei gradi delle estensioni composte,

$$\begin{aligned}
 [K(\alpha) : K][K : F] &= [K(\alpha) : F] = [K(\alpha) : F(\alpha)][F(\alpha) : F] \\
 &= [K(\beta) : F(\beta)][F(\beta) : F] = [K(\beta) : F] \\
 &= [K(\beta) : K][K : F]
 \end{aligned}$$

da cui, dividendo per $[K : F]$, si ottiene il risultato desiderato

$$1 = [K(\alpha) : K] = [K(\beta) : K]. \quad \square$$



Esercizi.

- Quali delle seguenti estensioni sono normali?

$$\mathbb{Q}(\sqrt{11}i) \text{ su } \mathbb{Q}; \quad \mathbb{Q}(\sqrt{5}, \sqrt[3]{3}) \text{ su } \mathbb{Q}(\sqrt[3]{3}); \quad \mathbb{Q}(\sqrt[3]{3}) \text{ su } \mathbb{Q}.$$

2. Determinare i coniugati su \mathbb{Q} di
 - (a) $(-1 + \sqrt{3}i)/2$;
 - (b) ζ , radice ottava primitiva dell'unità.



CONTROLLO.

1. Definizioni equivalenti di estensione normale.
2. Darc esempi di estensioni normali e di estensioni non normali.

6.6. Estensioni finite in caratteristica zero

Da questo momento in poi supporremo i campi di caratteristica zero, cioè estensioni dei razionali. Il motivo di ciò è dovuto al fatto che il cosiddetto teorema fondamentale della teoria di Galois (che vedremo nel prossimo capitolo), richiede due condizioni ulteriori, ossia che le estensioni siano *normali* e *separabili*. Quest'ultima proprietà in caratteristica zero è sempre verificata (per estensioni algebriche). Ricordiamo (cfr. definizione 6.3.3) che un polinomio irriducibile si dice separabile se è privo di radici multiple.

6.6.1 DEFINIZIONE. Un'estensione algebrica K di un campo F si dice *separabile* se ogni $a \in K$ è separabile, ossia se è separabile il suo polinomio minimo. \square

Ora, in caratteristica zero, ogni estensione algebrica è separabile, perché, come abbiamo visto, ogni polinomio irriducibile possiede tutte radici distinte, mentre in caratteristica p esistono polinomi irriducibili che ammettono radici multiple. Mettendoci quindi in caratteristica zero, non abbiamo problemi di questo tipo.

Vediamo subito come, utilizzando proprio questa proprietà delle estensioni in caratteristica zero (che cioè un polinomio irriducibile ha radici distinte) si riesce a dimostrare che ogni estensione finita in caratteristica zero è semplice.

Basterà provare la seguente proposizione.

6.6.2 PROPOSIZIONE. Siano a e b due elementi algebrici sopra un campo F di caratteristica zero. Allora esiste un elemento $\alpha \in F(a, b)$ tale che $F(a, b) = F(\alpha)$.

Dimostrazione. Siano $f(x)$ e $g(x)$ in $F[x]$ i polinomi minimi di a e b rispettivamente. Indicata con K un'estensione in cui entrambi i polinomi si spezzano, siano

$$a = a_1, a_2, \dots, a_n, \quad b = b_1, b_2, \dots, b_m$$

le radici in K di $f(x)$ e di $g(x)$ rispettivamente. In virtù della irriducibilità di $f(x)$ e $g(x)$, tutti gli a_i (e tutti i b_i) sono diversi tra di loro. Per ogni $i = 1, \dots, n$ e ogni $j = 2, \dots, m$ l'equazione in λ

$$a_i + \lambda b_j = a + \lambda b$$

ammette una ed una sola soluzione in K , data da

$$\lambda = \frac{a_i - a}{b - b_j}.$$

Ora, F ha caratteristica zero, e in quanto tale possiede infiniti elementi. Sceglieremo quindi un elemento $\gamma \in F$ che non soddisfi nessuna delle $n(m-1)$ equazioni precedenti. Indichiamo con α l'elemento $\alpha = a + \gamma b$. Proveremo che

$$F(a, b) = F(\alpha).$$

Chiaramente basta provare che $F(\alpha) \supseteq F(a, b)$, e per far questo è sufficiente provare che $b \in F(\alpha)$ (perché?). Si consideri il polinomio

$$h(x) \stackrel{\text{def}}{=} f(\alpha - \gamma x) \in F(\alpha)[x].$$

L'elemento b è radice comune di $g(x)$ e di $h(x)$, e quindi $x - b$ è un fattore in una opportuna estensione di $F(\alpha)$ sia di $g(x)$ sia di $h(x)$. Anzi, si tratta del loro massimo comun divisore: infatti $h(x)$ non può avere come radici (in una opportuna estensione) qualche altra radice di $g(x)$, perché, per la nostra scelta di γ , $\alpha - \gamma b_i \neq a_i$ per ogni i . Non può nemmeno $(g(x), h(x))$ essere $(x - b)^t$ con $t > 1$, perché $g(x)$ ha tutte radici semplici. Quindi $(x - b)$ è il massimo comun divisore tra $g(x)$ e $h(x)$, e, in quanto tale, appartiene a $F(\alpha)[x]$, perché $F(\alpha)$ è il comune campo dei coefficienti di $g(x)$ e $h(x)$. Questo ci garantisce che $b \in F(\alpha)$. \square

Abbiamo così provato che ogni estensione finita K di F in caratteristica zero è semplice, cioè $K = F(\alpha)$ per un opportuno $\alpha \in K$. Un tale elemento prende il nome di *elemento primitivo* e il corrispondente teorema si usa chiamare "teorema dell'elemento primitivo". Quindi:

6.6.3 TEOREMA DELL'ELEMENTO PRIMITIVO. *Ogni estensione finita K di un campo F in caratteristica zero è semplice.*

Dato che (cfr. esercizio 6.6.2) un'estensione finita di un campo finito è certamente semplice, il solo caso in cui un'estensione finita può non essere semplice è il caso di un'estensione finita di un campo infinito di caratteristica p .



ESERCIZI.

- Si provi che $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
- Sia K un'estensione finita di un campo finito F . Si provi che K è un'estensione semplice.
- Sia F un campo finito. Si dimostri che l'anello dei polinomi $F[x]$ contiene polinomi irriducibili su F di qualunque grado.

CAPITOLO 7

La teoria di Galois

*Qual è 'l geométra che tutto s'affige
per misurar lo cerchio, e non ritrova,
pensando, quel principio ond'elli indige,
tal era lo a quella vista nova:*

Dante, Paradiso, XXXIII, 133–136.

Questo capitolo è dedicato alla cosiddetta *teoria di Galois*, che culmina nell'elegantissimo teorema di corrispondenza di Galois. Questa teoria permette di trasportare risultati relativi ai gruppi a risultati relativi ai campi e viceversa. Le tecniche utilizzate da Galois permettono inoltre di risolvere importanti questioni di geometria e della teoria delle equazioni.

7.1. Costruzioni con riga e compasso

Continueremo a lavorare, come abbiamo detto alla fine del capitolo precedente, con campi di caratteristica zero, estensioni quindi di \mathbb{Q} . Con i metodi studiati nel capitolo precedente saremo in grado di provare la *impossibilità di certi tipi di costruzioni classiche, con il solo aiuto di una riga non graduata e di un compasso*.

Sia dato nel piano reale $\mathbb{R} \times \mathbb{R}$ un insieme \mathcal{P} (finito o infinito) di punti. Si considerino le seguenti *operazioni fondamentali*:

- (1) Tracciare la retta per due punti arbitrari di \mathcal{P} ;
- (2) disegnare il segmento che unisce due punti di \mathcal{P} ;
- (3) disegnare una circonferenza, avente centro in un punto di \mathcal{P} e raggio uguale alla distanza di due punti di \mathcal{P} .

7.1.1 DEFINIZIONE. Un punto si dice *costruibile in un passo a partire da \mathcal{P}* se risulta punto di intersezione di due qualunque rette o di una retta e una circonferenza o di due circonferenze tracciate utilizzando le operazioni (1)–(3). □

7.1.2 DEFINIZIONE. Un punto $P \in \mathbb{R}^2$ si dice *costruibile a partire da \mathcal{P}* se esiste una successione finita di punti $P_1, P_2, \dots, P_n = P$ tali che per ogni $j = 1, \dots, n$ il punto P_j sia costruibile in un passo a partire dall'insieme di punti

$$\mathcal{P} \cup \{P_1, P_2, \dots, P_{j-1}\}. \quad \square$$

7.1.3 DEFINIZIONE. Una *costruzione con riga e compasso* o *costruzione euclidea* è una successione finita di operazioni fondamentali. \square

Diamo qui di seguito alcuni esempi di costruzioni euclidee: da ora in poi quando parleremo di *costruzioni* (anche senza dire euclidee), intenderemo sempre *costruzioni con riga e compasso*.

7.1.4 COSTRUIRE IL PUNTO MEDIO DI UN SEGMENTO. Sia AB il segmento dato. Siano C_1 e C_2 le circonference con centri rispettivamente in A e in B e raggi uguali alla lunghezza del segmento AB . Indicati con P_1 e P_2 i punti di intersezione di C_1 e C_2 , il punto medio cercato è dato dall'intersezione della retta per P_1 e P_2 con la retta r (vedi figura 7.1).

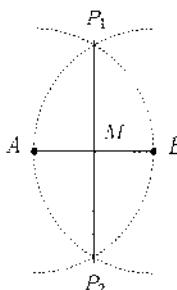


FIGURA 7.1

7.1.5 COSTRUIRE LA RETTA PERPENDICOLARE AD UNA DATA RETTA r E PASSANTE PER UN PUNTO P . Supponiamo dappriama $P \notin r$. La retta r sarà individuata da due punti P_1 e P_2 . Si traccia allora la circonferenza C di centro il punto P e raggio uguale alla distanza tra P e uno dei due punti, sia esso P_1 . Se la circonferenza C risulta tangente alla retta data, la retta per P e P_1 è la perpendicolare cercata, altrimenti, indicato con P'_1 l'ulteriore punto di intersezione di C con la retta r , la perpendicolare cercata è la retta passante per P e per il punto medio del segmento $P_1P'_1$ (figura 7.2). E se $P \in r$?

7.1.6 DATO UN PUNTO ED UNA RETTA NON PASSANTE PER ESSO, COSTRUIRE LA RETTA PER IL PUNTO PARALLELA ALLA RETTA DATA. Basta ripetere due volte la costruzione della perpendicolare.

Vediamo ora come possiamo utilizzare i risultati *algebrici* dei paragrafi precedenti per interpretare questi problemi.

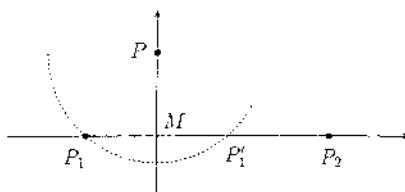


FIGURA 7.2

7.1.7 DEFINIZIONE. Un numero reale α si dice *costruibile* se con riga, compasso e l'unità di misura fissata, si riesce a costruire un segmento di lunghezza $|\alpha|$. \square

Si noti che con riga e compasso e l'unità di misura si riesce a costruire in $\mathbb{R} \times \mathbb{R}$ un sistema di assi cartesiani ortogonali (cfr. esercizio 7.1.1).

Da quanto detto in precedenza, è chiaro che un punto P è *costruibile* se e solo se lo sono le sue coordinate rispetto ad un fissato sistema di assi cartesiani. Parleremo pertanto in modo equivalente di *punti costruibili* e *numeri reali costruibili*.

Un numero complesso $a + ib$ è costruibile se è costruibile il punto $P \equiv (a, b)$ nel sistema di assi fissato. Parleremo quindi sempre di numeri reali costruibili, dato che a questi ci si può sempre ricondurre.

Indicato con \mathcal{C} l'insieme di tutti i punti costruibili a partire da due soli punti (gli estremi dell'unità di misura), vale la seguente proposizione.

7.1.8 PROPOSIZIONE.

- (a) $\mathcal{C} \supset \mathbb{Z}$;
- (b) $\mathcal{C} \supset \mathbb{Q}$;
- (c) \mathcal{C} è un campo.

Dimostrazione. (a) Si traccia la retta per $O = 0$ e $U = 1$, e, con apertura uguale ad 1 e centro in 1 si costruisce il punto 2, ecc.

(b) Basta provare che ogni numero della forma $1/n$ è costruibile. (Si veda la figura 7.3 e si ricordi il teorema di Talete). Ogni numero razionale sarà poi somma di frazioni del tipo $1/n$, che si possono costruire.

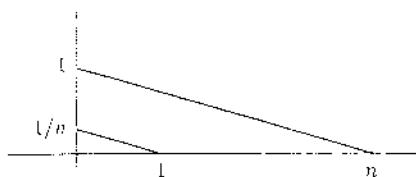


FIGURA 7.3

(c) Per provare che \mathbb{C} è un campo basta provare che, dati α e $\beta \in \mathbb{C}$, allora $\alpha \pm \beta$, $\alpha \cdot \beta$ e α/β , con $\beta \neq 0$, sono costruibili. Per quel che riguarda $\alpha \pm \beta$, la costruzione è ovvia. La figura 7.4 mostra le costruzioni per $\alpha\beta$ e per α/β .

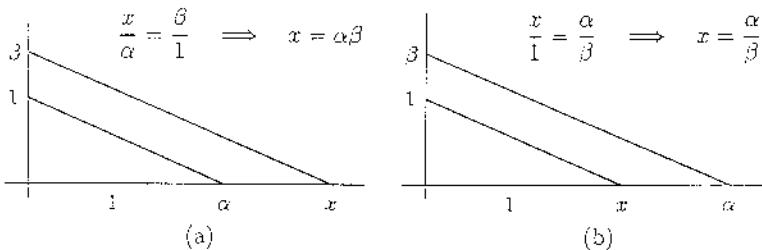


FIGURA 7.4

In definitiva, abbiamo provato che l'insieme dei numeri reali costruibili è un sottocampo di \mathbb{R} che contiene i razionali. \square

Nostro scopo ora è quello di dare una caratterizzazione *algebrica* degli elementi del campo \mathbb{C} .

Sia F un qualunque sottocampo dei numeri reali.

7.1.9 DEFINIZIONE. Si definisce *piano* di F il sottoinsieme $F \times F$ di $\mathbb{R} \times \mathbb{R}$. Si definisce *retta* di F una qualunque retta che congiunga due punti del piano di F . Si definisce *circonferenza* di F una qualunque circonferenza che abbia centro in un punto del piano di F e raggio di lunghezza un numero di F . \square

Se si fissa un riferimento in $F \times F$, una retta di F ha equazione

$$ax + by + c = 0, \quad a, b, c \in F.$$

Una circonferenza di F ha equazione

$$x^2 + y^2 + ax + by + c = 0, \quad a, b, c \in F.$$

Ora, partendo dai punti P del piano di F (F sottocampo dei reali), quali nuovi punti del piano reale si possono ottenere con costruzioni euclidee? Ci sono ovviamente tre modi per ottenere dei punti:

- (1) *Intersecando due rette di F :* in questo caso però non si ottengono *nuovi* punti, perché due rette del piano di F si intersecano in un punto a coordinate in F (si tratta di risolvere un sistema lineare).
- (2) *Intersecando una retta e una circonferenza di F .*
- (3) *Intersecando due circonferenze di F .* Questo caso è riconducibile al secondo.

Nel secondo caso, il punto di intersezione avrà coordinate che sono soluzioni di un'equazione quadratica, e pertanto staranno in F oppure in un'estensione quadratica di F , $F(\sqrt{a})$, $a \in F$. I soli punti del piano reale che si possono

costruire a partire dal piano di F sono quindi punti le cui coordinate stanno in campi della forma $F(\alpha)$, con $\alpha \in \mathbb{R}$, $\alpha^2 \in F$. D'altra parte, ogni punto a coordinate in $F(\alpha)$, $\alpha \in \mathbb{R}$, $\alpha^2 \in F$ è effettivamente costruibile: la seguente costruzione (cfr. figura 7.5) offre infatti il modo di costruire la radice quadrata di un numero a costruibile. Si traccia la circonferenza di diametro $1+a$. Tracciata poi la perpendicolare per il punto 1 , e detto P il punto di intersezione di tale perpendicolare con la circonferenza, la lunghezza x del segmento $\{1, P\}$ è la radice quadrata cercata: infatti per il teorema di Euclide, $1 : x = x : a$.

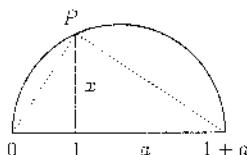


FIGURA 7.5

Quindi, *tutti e soli i punti del piano reale costruibili in un passo a partire dal piano di F sono i punti a coordinate nei campi della forma $F(\alpha)$, con $\alpha \in \mathbb{R}$, $\alpha^2 \in F$.*

Consideriamo ora il campo $F_1 = F(\alpha)$, con $\alpha \in \mathbb{R}$, $\alpha^2 \in F$. I punti del piano reale costruibili in un passo a partire dal piano di F_1 sono tutti e soli quelli a coordinate appartenenti a $F_1(\beta)$, con $\beta \in \mathbb{R}$, $\beta^2 \in F_1$. Continuando in questo modo, si vede che un punto c del piano reale è costruibile *a partire dal piano di un campo F* se e solo se esiste una successione finita di sottocampi

$$F_0 = F \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$$

tali che $\forall i = 1, \dots, n$

$$F_i = F_{i-1}(\alpha_i), \quad \alpha_i \in \mathbb{R}, \quad \alpha_i^2 \in F_{i-1}$$

e c ha coordinate in F_n . Dato che sappiamo che tutti i numeri costruibili contengono il campo \mathbb{Q} dei numeri razionali, abbiamo in definitiva dimostrato quanto segue, che è proprio la caratterizzazione algebrica cercata dei punti (o dei numeri reali) costruibili.

7.1.10 PROPOSIZIONE. *Un numero reale c è costruibile se e solo se esiste un numero finito di numeri reali $\alpha_1, \alpha_2, \dots, \alpha_n$ tali che*

$$\alpha_1^2 \in \mathbb{Q}, \quad \alpha_i^2 \in \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_{i-1}), \quad i = 2, \dots, n$$

in modo tale che

$$c \in \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n).$$

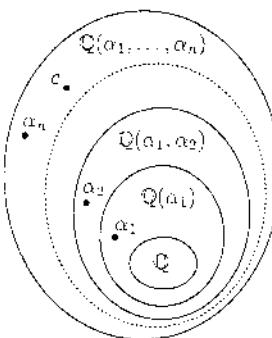


FIGURA 7.6 .

Calcoliamo ora il grado dell'estensione $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$ in cui si trova l'elemento c . Per come è stata costruita, si ha

$$\begin{aligned} [\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n) : \mathbb{Q}] &= [\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n) : \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_{n-1})] \\ &\cdot [\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_{n-1}) : \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_{n-2})] \cdots \\ &\cdot [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)] \cdot [\mathbb{Q}(\alpha_1) : \mathbb{Q}]. \end{aligned}$$

Ogni fattore del prodotto a secondo membro ha grado 1 o 2, quindi in definitiva

$$[\mathbb{Q}(\alpha_1, \dots, \alpha_n) : \mathbb{Q}] = 2^h$$

per un opportuno $h \in \mathbb{N}$.

Si hanno pertanto le seguenti conseguenze.

7.1.11 PROPOSIZIONE. *Se c è un numero reale costruibile, allora esso appartiene ad un ampliamento K di grado una potenza di 2.*

Questa proposizione ci dice intanto che *nessun numero trascendente è costruibile*. Inoltre ci dà un importante criterio di *non costruibilità* per i numeri algebrici.

7.1.12 PROPOSIZIONE. *Se un numero reale soddisfa un polinomio irriducibile di grado n che non è una potenza di 2, allora il numero non è costruibile.*

Dimostrazione. Se α soddisfa un polinomio *irriducibile* di grado n , sappiamo che questo è il suo polinomio minimo; quindi vuol dire che l'estensione $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n \neq 2^h$. Quindi α non può appartenere ad un ampliamento algebrico di grado una potenza di 2, come dovrebbe avvenire se α fosse costruibile. \square

Siamo ora in grado di mostrare che molte costruzioni classiche sono impossibili.

7.1.13 DUPLICAZIONE DEL CUBO. Il problema è il seguente: dato un cubo di volume V unitario, costruire un cubo di volume doppio. Il problema si riduce alla costruzione di un segmento di lunghezza $\sqrt[3]{2}$. Ora, posto $\alpha = \sqrt[3]{2}$, α soddisfa il polinomio *irriducibile su \mathbb{Q}* $x^3 - 2$. Dato che il grado di questo polinomio non è una potenza di 2, per la proposizione 7.1.12, α non può essere costruibile.

7.1.14 QUADRATURA DEL CERCHIO. Il problema consiste nel costruire un quadrato di area uguale a quella di un cerchio assegnato di raggio 1.

Si tratta quindi di disegnare un quadrato di lato $\sqrt{\pi}$. Ma questo è impossibile, dato che $\sqrt{\pi}$ è trascendente (se fosse algebrico, sarebbe algebrico anche π).

7.1.15 RETTIFICAZIONE DELLA CIRCONFERENZA. Costruire un segmento di lunghezza pari alla lunghezza di una circonferenza di raggio unitario.

Si tratta di costruire un segmento di lunghezza 2π . Se una tale costruzione fosse possibile, l'elemento 2π dovrebbe essere algebrico, mentre è trascendente.

7.1.16 TRISEZIONE DELL'ANGOLO. Dato un angolo, costruirne la sua terza parte.

Faremo vedere che *non ogni angolo può essere trisecato*. Basta prendere $3\vartheta = \pi/3$, e pretendere di costruire $\vartheta = \pi/9$. Costruire un angolo ϑ equivale a costruire $\cos \vartheta$. Ora, dalle ben note relazioni trigonometriche,

$$(7.1.1) \quad \cos 3\vartheta = 4\cos^3 \vartheta - 3\cos \vartheta$$

da cui, per $3\vartheta = \pi/3$,

$$\frac{1}{2} = 4\cos^3 \frac{\pi}{9} - 3\cos \frac{\pi}{9}.$$

Quindi $\cos(\pi/9)$ soddisfa il polinomio (irriducibile su \mathbb{Q} , si provi!)

$$8x^3 - 6x - 1 = 0$$

che ha grado che non è una potenza di due. Quindi $\cos(\pi/9)$ non è costruibile e $\pi/3$ non è trisecabile.

Facciamo vedere invece che certi angoli sono trisecabili. Ad esempio un tale angolo è $\pi/2$. Risulta infatti dalla (7.1.1)

$$0 = 4\cos^3 \frac{\pi}{6} - 3\cos \frac{\pi}{6}$$

da cui si ricava che $\cos(\pi/6)$ soddisfa il polinomio $4x^3 - 3x$. Tale polinomio non è irriducibile, e il polinomio minimo di $\cos(\pi/6)$ è il polinomio di secondo grado $f(x) = 4x^2 - 3$. $\cos(\pi/6)$ sta quindi in un'estensione *quadratica* di \mathbb{Q} e pertanto è costruibile: risulta infatti $\cos(\pi/6) = \sqrt{3}/2$, che sappiamo bene essere costruibile.

 ATTENZIONE. Vale la pena a questo punto di mettere in luce un fatto importante: se un elemento soddisfa un polinomio irriducibile di grado una potenza di 2, *non* possiamo concludere che l'elemento è costruibile. Nel caso visto ora abbiamo potuto concludere la costruibilità di $\cos(\pi/6)$ perché il suo polinomio minimo aveva grado *esattamente* due. \square

 ESERCIZI.

1. Si provi che con riga e compasso si riesce a disegnare un sistema di assi cartesiani.
2. Si provi che se α e β sono due numeri trascendenti, allora $\alpha + \beta$ o $\alpha\beta$ è trascendente.



CONTROLLO.

1. Cosa si intende per punto costruibile?
2. Che struttura algebrica ha l'insieme di tutti i punti costruibili?
3. π è costruibile? Giustificare la risposta.

7.2. *F*-automorfismi di un'estensione, gruppi di Galois e campi fissati

Continuiamo a lavorare in caratteristica zero. Nelle definizioni che seguono penseremo, per maggiore concretezza, le estensioni contenute in \mathbb{C} . Si noti tuttavia che tutti i risultati continuano a valere sostituendo a \mathbb{C} la chiusura algebrica, sempre esistente, dei campi in questione.

7.2.1 DEFINIZIONE. Sia K un'estensione di un campo F . Un monomorfismo di K in \mathbb{C} che fissa gli elementi di F si chiama *F-monomorfismo* di K su F . \square

Ad esempio, se $F = \mathbb{Q}$, $K = \mathbb{Q}(\alpha)$, dove α è la radice quinta reale di $x^5 - 3$, resta definito un *F-monomorfismo* φ da K a \mathbb{C} mandando α in $\omega\alpha$ (ω radice quinta primitiva dell'unità) e ogni $a \in F$ in se stesso.

Indicheremo con $\mathcal{I}(K, F)$ l'insieme di tutti gli *F-monomorfismi* di K .

In molti testi si parla di *F-isomorfismi*, anziché di *F-monomorfismi*. Abbiamo preferito chiamarli *F-monomorfismi*, per evitare possibili ambiguità.

7.2.2 PROPOSIZIONE. Se $F = \mathbb{Q}$, ogni monomorfismo di K è un \mathbb{Q} -monomorfismo.

Dimostrazione. Sia φ un monomorfismo di K . Allora risulta

$$\varphi(0) = 0, \quad \varphi(1) = 1,$$

$$\varphi(n) = \varphi(\underbrace{1 + 1 + \cdots + 1}_n) = \underbrace{\varphi(1) + \varphi(1) + \cdots + \varphi(1)}_n = \underbrace{1 + 1 + \cdots + 1}_n = n,$$

$$\varphi\left(\frac{m}{n}\right) = \varphi(m)\varphi(n^{-1}) = \varphi(m)\varphi(n)^{-1} = mn^{-1} = \frac{m}{n}. \quad \square$$

Sia K un'estensione finita di F . Ci proponiamo di determinare tutti gli F -monomorfismi di K . Essendo K estensione finita di F , sarà (cfr. Proposizione 6.6.2) $K = F(\alpha)$ per qualche $\alpha \in K$. Se $[K : F] = n$, ogni elemento $k \in K$ si scrive nella forma

$$k = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}, \quad c_i \in F.$$

Sia φ un F -monomorfismo di K . Allora

$$\varphi(k) = \varphi(c_0) + \cdots + \varphi(c_{n-1})\varphi(\alpha)^{n-1} = c_0 + c_1\varphi(\alpha) + \cdots + c_{n-1}\varphi(\alpha)^{n-1},$$

cioè φ è completamente determinato una volta che si conosca $\varphi(\alpha)$. Possiamo dire di più: $\varphi(\alpha)$ è coniugato ad α su F (cfr. definizione 6.5.1). Infatti vale la seguente proposizione.

7.2.3 PROPOSIZIONE. *Sia $K = F(\alpha)$ un'estensione finita di F e sia φ un F -monomorfismo di K . Allora $\varphi(\alpha)$ è coniugato ad α su F , ossia $\varphi(\alpha)$ e α hanno lo stesso polinomio minimo su F .*

Dimostrazione. Sia $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, ($a_i \in F$) il polinomio minimo di α . Dovremo provare che $\varphi(\alpha)$ è ancora radice di $p(x)$. Si hanno infatti le seguenti uguaglianze:

$$\begin{aligned} p(\varphi(\alpha)) &= a_0 + a_1\varphi(\alpha) + \cdots + a_n\varphi(\alpha)^n \\ &= \varphi(a_0) + \varphi(a_1)\varphi(\alpha) + \cdots + \varphi(a_n)\varphi(\alpha^n) \\ &= \varphi(a_0 + a_1\alpha + \cdots + a_n\alpha^n) = \varphi(0) = 0. \quad \square \end{aligned}$$

Quindi i possibili trasformati di una radice α di un polinomio irriducibile a coefficienti in F sono da ricercarsi tra le radici del polinomio stesso. Ad esempio, si consideri l'estensione $K = \mathbb{Q}(\sqrt{5})$ di \mathbb{Q} . Se $f(x) = x^2 - 5$, allora il trasformato di $\sqrt{5}$ mediante un \mathbb{Q} -monomorfismo di K non può che essere $\sqrt{5}$ o $-\sqrt{5}$.

Come conseguenza di questi risultati possiamo intanto concludere con il seguente teorema.

7.2.4 TEOREMA. *Sia K un'estensione finita di F , di grado n . Allora esistono al più n F -monomorfismi di K . In altre parole,*

$$|\mathcal{I}(K, F)| \leq [K : F].$$

Dimostreremo che ne esistono esattamente n . Premettiamo il seguente lemma.

7.2.5 LEMMA. *Sia F un campo e sia $F(\alpha)$ un'estensione di grado n . Sia ϑ un monomorfismo da F a \mathbb{C} , e sia $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + x^n$, ($a_i \in F$) il polinomio minimo di α . Indicato con p_ϑ il polinomio a coefficienti in \mathbb{C} $p_\vartheta = \vartheta(a_0) + \vartheta(a_1)x + \cdots + x^n$ e con β una radice di p_ϑ , esiste un monomorfismo estensione di ϑ ad $F(\alpha)$ che manda α in β .*

Dimostrazione. La dimostrazione di questo lemma è analoga a quella svolta nel corso della dimostrazione del teorema 6.2.11: la ripetiamo per completezza. Ogni elemento $s \in F(\alpha)$ si scrive in modo unico al modo seguente:

$$s = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}, \quad a_i \in F.$$

Definiamo $\varphi : F(\alpha) \rightarrow \mathbb{C}$ così:

$$(7.2.1) \quad \varphi(s) \stackrel{\text{def}}{=} \vartheta(a_0) + \vartheta(a_1)\beta + \cdots + \vartheta(a_{n-1})\beta^{n-1}.$$

È ovvio che φ è un'estensione di ϑ e che manda α in β . È anche chiaro che φ conserva la somma. Dimostriamo che conserva il prodotto. Sia $t = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$ un altro elemento di $F(\alpha)$. Consideriamo allora i seguenti polinomi, associati rispettivamente a s e a t :

$$f(x) \stackrel{\text{def}}{=} a_0 + a_1x + \cdots + a_{n-1}x^{n-1}, \quad g(x) \stackrel{\text{def}}{=} b_0 + b_1x + \cdots + b_{n-1}x^{n-1}.$$

Dividendo $f \cdot g$ per p

$$f(x)g(x) = p(x) \cdot q(x) + r(x) \quad r(x) = r_0 + r_1x + \cdots + r_{n-1}x^{n-1}$$

e valutando in α questa relazione, si ottiene, tenendo presente che $p(\alpha) = 0$,

$$st = f(\alpha)g(\alpha) = r(\alpha).$$

Se ora, per ogni polinomio $v(x) = \sum_{i=0}^m c_i x^i$, indichiamo con $v_\vartheta(x)$ il polinomio $\sum_{i=0}^m \vartheta(c_i)x^i$, si avrà la seguente serie di uguaglianze:

$$\begin{aligned} \varphi(s \cdot t) &= r_\vartheta(\beta) = \underbrace{p_\vartheta(\beta)}_{=0} q_\vartheta(\beta) + r_\vartheta(\beta) \\ &= (p \cdot q + r)_\vartheta(\beta) = (f \cdot g)_\vartheta(\beta) = f_\vartheta(\beta) \cdot g_\vartheta(\beta) = \varphi(s) \cdot \varphi(t). \end{aligned}$$

Quindi φ conserva anche il prodotto: è un omomorfismo. Inoltre, essendo $\varphi(1) = 1$, φ non è l'omomorfismo nullo, e quindi, in quanto omomorfismo non nullo tra campi, è un monomorfismo. \square

Siamo ora in grado di provare che esistono in tutto esattamente n F -monomorfismi.

7.2.6 **TEOREMA.** *Sia K un'estensione di F , di grado n , e sia $\alpha \in K$ tale che $K = F(\alpha)$. Siano $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ i coniugati ad α su F . Allora*

- (a) $\alpha_1, \alpha_2, \dots, \alpha_n$ sono tutti distinti;
- (b) per ogni $j = 1, \dots, n$, esiste uno ed un solo F -monomorfismo φ_j di K in \mathbb{C} tale che $\varphi_j(\alpha) = \alpha_j$;
- (c) i φ_j del punto precedente esauriscono gli F -monomorfismi di K in \mathbb{C} .

Dimostrazione. (a) $\alpha_1, \alpha_2, \dots, \alpha_n$ sono distinti perché zeri di un polinomio irriducibile in caratteristica zero (cfr. proposizione 6.3.6).

(b) Se nel lemma 7.2.5 si prende come ϑ l'applicazione che fissa tutti gli elementi di F , allora $p_\vartheta = p$, il lemma ci dice che esiste un F -monomorfismo φ , che manda α in α_j , e questo è dato da

$$\varphi_j(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = a_0 + a_1\alpha_j + \cdots + a_{n-1}\alpha_j^{n-1}.$$

(c) Abbiamo trovato n F -monomorfismi distinti φ_j perché gli α_i sono distinti, e quindi non ce ne possono essere altri, in base al teorema 7.2.4. \square

Hanno molta importanza alcuni F -monomorfismi particolari, che passiamo a definire.

7.2.7 DEFINIZIONE. Sia F un campo e K una sua estensione. Un F -automorfismo σ di K è un F -monomorfismo di K su K stesso. Indicheremo con $G(K, F)$ l'insieme di tutti gli F -automorfismi di K . \square

Non ogni F -monomorfismo è un F -automorfismo: basta riprendere l'esempio dato all'inizio del paragrafo. Il trasformato mediante φ di α non appartiene a $\mathbb{Q}(\alpha)$ (α è reale, mentre $\varphi(\alpha) = \omega\alpha$ è complesso e non reale).

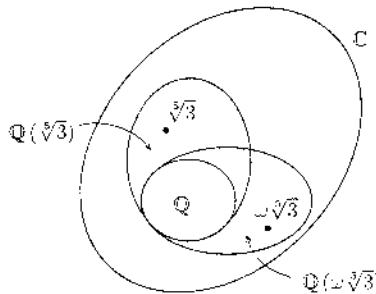


FIGURA 7.7

Il fatto importante degli F -automorfismi è che rispetto al prodotto operatorio l'insieme $G(K, F)$ di tutti gli F -automorfismi di un'estensione K di F è un sottogruppo del gruppo di tutti gli automorfismi di K .

7.2.8 PROPOSIZIONE. L'insieme $G(K, F)$ di tutti gli F -automorfismi di un'estensione K di F è un sottogruppo del gruppo di tutti gli automorfismi di K .

Dimostrazione. Si ha, per definizione di F -automorfismo,

$$G(K, F) \stackrel{\text{def}}{=} \{\sigma : K \rightarrow K \mid \sigma(a) = a \ \forall a \in F\}.$$

Siano σ, τ elementi di $G(K, F)$. Allora il loro prodotto $\sigma \circ \tau$ è un automorfismo che fissa F , perché

$$(\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma(a) = a \quad \forall a \in F.$$

Inoltre σ^{-1} è un automorfismo e

$$a = \sigma^{-1}(\sigma(a)) = \sigma^{-1}(a).$$

Quindi $G(K, F)$ è un sottogruppo del gruppo di tutti gli automorfismi di K . \square

7.2.9 DEFINIZIONE. Il gruppo $G(K, F)$ di tutti gli automorfismi di K che fissano F prende il nome di *gruppo di Galois dell'estensione K di F* . \square

Abbiamo visto che ogni geometria è lo studio delle proprietà delle figure che sono invarianti rispetto a particolari gruppi di trasformazioni. Ebbene, ora noi abbiamo a disposizione un gruppo di trasformazioni, e in questo spirito, i gruppi degli F -automorfismi stanno ai campi come i gruppi di movimenti stanno alle figure geometriche. Sia gli automorfismi, sia i movimenti offrono dei mezzi per studiare la *simmetria*, o la connessione interna tra le parti dell'estensione (rispettivamente della figura).

Vale il seguente risultato.

7.2.10 TEOREMA. *Sia K un'estensione finita di un campo F e sia n il suo grado. Allora*

$$|G(K, F)| \leq [K : F].$$

Dimostrazione. È una conseguenza immediata del teorema 7.2.6, non appena si osservi che $G(K, F) \subseteq \mathcal{I}(K, F)$. \square

7.2.11 DEFINIZIONE. Sia K un campo e G un gruppo di automorfismi di K . Si definisce

$$\boxed{K_G \stackrel{\text{def}}{=} \{k \in K \mid \sigma(k) = k \ \forall \sigma \in G\}}$$

e prende il nome di *campo fissato da G* . \square

Perché abbia senso chiamare *campo* l'insieme K_G , dobbiamo provare la seguente proposizione.

7.2.12 PROPOSIZIONE. *Sia K un campo e sia G un gruppo di automorfismi di K . L'insieme $K_G = \{k \in K \mid \sigma(k) = k \ \forall \sigma \in G\}$ è un sottocampo di K .*

Dimostrazione. Siano $k_1, k_2 \in K_G$. Allora, per ogni $\sigma \in G$

$$\begin{aligned} \sigma(k_1 \pm k_2) = \sigma(k_1) \pm \sigma(k_2) &= k_1 \pm k_2 \implies k_1 \pm k_2 \in K_G \\ \sigma(k_1 k_2^{-1}) = \sigma(k_1)\sigma(k_2)^{-1} &= k_1 k_2^{-1} \implies k_1 k_2^{-1} \in K_G. \quad \square \end{aligned}$$

Sia ora K un'estensione di un campo F . Se $G(K, F)$ è il gruppo di Galois dell'estensione K su F , risulta, come è immediato verificare dalla definizione di $G(K, F)$,

$$\boxed{K_{G(K,F)} \supseteq F}.$$

Diamo alcuni esempi di gruppi di Galois di particolari estensioni e dei campi fissati da tali gruppi.

7.2.13 ESEMPIO. Sia $K = \mathbb{C}$, campo dei complessi e $F = \mathbb{R}$.

Se $\sigma \in G(\mathbb{C}, \mathbb{R})$, dato che $\mathbb{C} = \mathbb{R}(i)$, basta calcolare $\sigma(i)$. Ora, il polinomio minimo di i su \mathbb{R} è $x^2 + 1$, e pertanto $\sigma(i)$ deve per forza essere ancora una radice dello stesso polinomio, cioè $\pm i$. Le due applicazioni

$$\begin{aligned}\sigma_1 : \mathbb{C} &\longrightarrow \mathbb{C} \\ a + ib &\longmapsto a - ib\end{aligned}$$

e

$$\begin{aligned}\sigma_2 : \mathbb{C} &\longrightarrow \mathbb{C} \\ a + ib &\longmapsto a + ib\end{aligned}$$

sono rispettivamente l'automorfismo identico e l'automorfismo di coniugio. Quindi

$$G(\mathbb{C}, \mathbb{R}) = \{\sigma_1, \sigma_2\} \cong \mathbb{Z}_2.$$

Calcoliamo ora il campo fissato da $G(\mathbb{C}, \mathbb{R})$, ossia

$$\mathbb{C}_{G(\mathbb{C}, \mathbb{R})} = \{k \in \mathbb{C} \mid \sigma(k) = k \ \forall \sigma \in G(\mathbb{C}, \mathbb{R})\}.$$

Dato che l'identità fissa tutti gli elementi, basta cercare gli elementi $k \in \mathbb{C}$ che vengono fissati da σ_2 . Quindi

$$\begin{aligned}\mathbb{C}_{G(\mathbb{C}, \mathbb{R})} &= \{k \in \mathbb{C} \mid \sigma_2(k) = k\} = \{a + ib \mid \sigma_2(a + ib) = a + ib\} \\ &= \{a + ib \mid a - ib = a + ib\} = \mathbb{R}.\end{aligned}$$

In questo caso $K_{G(K, F)}$ che, come sappiamo, deve contenere F , coincide con F . \square

7.2.14 ESEMPIO. Sia $K = \mathbb{Q}(\sqrt[3]{5})$ e $F = \mathbb{Q}$. Per trovare tutti i possibili automorfismi di $\mathbb{Q}(\sqrt[3]{5})$ (che fissano \mathbb{Q}), basta vedere quali possono essere le immagini di $\alpha = \sqrt[3]{5}$. Dato che il polinomio minimo di α su \mathbb{Q} è $x^3 - 5$, $\sigma(\alpha)$ deve essere un'altra radice dello stesso polinomio. Ora, oltre ad α , le altre due radici di $x^3 - 5$ sono complesse, e quindi non appartengono a $\mathbb{Q}(\sqrt[3]{5}) \subset \mathbb{R}$. Ne segue

che l'unica possibilità è $\sigma(\alpha) = \alpha$, ossia l'unico automorfismo di $G(\mathbb{Q}(\sqrt[3]{5}), \mathbb{Q})$ è l'automorfismo identico:

$$G(\mathbb{Q}(\sqrt[3]{5}), \mathbb{Q}) = \{\text{id}\}.$$

È ovvio allora che il campo fissato da $G(\mathbb{Q}(\sqrt[3]{5}), \mathbb{Q})$ è tutto $\mathbb{Q}(\sqrt[3]{5})$, e quindi in questo caso

$$K_{G(K, F)} = \mathbb{Q}(\sqrt[3]{5})_{G(\mathbb{Q}(\sqrt[3]{5}), \mathbb{Q})} = \mathbb{Q}(\sqrt[3]{5}) \supset \mathbb{Q}.$$

Si noti che in questo caso, a differenza del precedente,

$$1 = |G(\mathbb{Q}(\sqrt[3]{5}), \mathbb{Q})| < |\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}| = 3. \quad \square$$

7.2.15 ESEMPIO. Sia ora $K = \mathbb{Q}(\sqrt[3]{5}, \omega)$, dove ω è una radice primitiva terza dell'unità. Tenendo conto del fatto che $\sqrt[3]{5}$ è radice del polinomio irriducibile $x^3 - 5$ e ω è radice del polinomio irriducibile $x^2 + x + 1$, si provi che $G(\mathbb{Q}(\sqrt[3]{5}, \omega), \mathbb{Q})$ è costituito da 6 automorfismi ed è isomorfo a S_3 . Si osservi che in questo caso

$$6 = |G(\mathbb{Q}(\sqrt[3]{5}, \omega), \mathbb{Q})| = |\mathbb{Q}(\sqrt[3]{5}, \omega) : \mathbb{Q}| = 6.$$

Si calcoli infine il campo fissato da $G(\mathbb{Q}(\sqrt[3]{5}, \omega), \mathbb{Q})$. \square

7.2.16 ESEMPIO. Sia ζ una radice n -esima primitiva dell'unità. Calcoliamo $\mathbb{Q}(\zeta)$. Sappiamo che ζ soddisfa l' n -esimo polinomio ciclotomico $\Phi_n(x)$ che, come sappiamo, anche se lo abbiamo provato solo in parte, è irriducibile su \mathbb{Q} . Quindi si tratta del polinomio minimo di ζ su \mathbb{Q} . Quindi

$$|\mathbb{Q}(\zeta) : \mathbb{Q}| = \varphi(n).$$

Ora, ogni elemento di $G(\mathbb{Q}(\zeta), \mathbb{Q})$ manda ζ in un'altra radice di $\Phi_n(x)$, ossia in un elemento del tipo ζ^r , con $1 \leq r \leq n$ e $(n, r) = 1$. Viceversa, se r è un intero tale che $1 \leq r \leq n$ e $(n, r) = 1$, l'applicazione σ_r che manda ζ in ζ^r dà luogo ad un automorfismo di $\mathbb{Q}(\zeta)$. Questa osservazione ci suggerisce di definire la seguente applicazione tra il gruppo $U(\mathbb{Z}_n)$ degli elementi invertibili di \mathbb{Z}_n e $G(\mathbb{Q}(\zeta), \mathbb{Q})$:

$$\begin{aligned} \Psi : U(\mathbb{Z}_n) &\longrightarrow G(\mathbb{Q}(\zeta), \mathbb{Q}) \\ \bar{k} &\longmapsto \sigma_k. \end{aligned}$$

Tale corrispondenza è bimivoca. Dimostriamo che si tratta di un omomorfismo di gruppi. Se $i, j \in U(\mathbb{Z}_n)$ sono tali che $ij \equiv k \pmod{n}$, facciamo vedere che $\sigma_i \sigma_j = \sigma_k$: infatti

$$\sigma_i \sigma_j(\zeta) = \sigma_i(\zeta^j) = \zeta^{ij} = \zeta^k = \sigma_k(\zeta).$$

Abbiamo così provato che

$$G(\mathbb{Q}(\zeta), \mathbb{Q}) \cong U(\mathbb{Z}_n). \quad \square$$

Notiamo che in tutti gli esempi visti, risulta come deve essere.

$$(7.2.2) \quad |G(K, F)| \leq [K : F] \quad \text{e} \quad K_{G(K, F)} \supseteq F.$$

In alcuni casi, ma non in tutti, vale il segno di uguaglianza.

ATTENZIONE. Osserviamo che gli esempi in cui valgono i segni di uguaglianza (sia per quel che riguarda l'uguaglianza dell'ordine di $G(K, F)$ con il grado $[K : F]$, sia per quel che riguarda l'uguaglianza di $K_{G(K, F)}$ con F), corrispondono a casi in cui K è un'estensione *normale* di F . Si tratterà di vedere se questo è vero in generale. La risposta è positiva, e lo dimostreremo fra breve. \square

Abbiamo visto (definizione 7.2.9) che ad ogni estensione K di un campo F possiamo associare un *gruppo*, il suo gruppo di Galois $G(K, F)$. Vogliamo ora stabilire una relazione tra l'*insieme dei campi intermedi di un'estensione* K di F e l'*insieme dei sottogruppi* di $G(K, F)$.

Sia K un'estensione di F e sia $G(K, F)$ il suo gruppo di Galois. Per ogni campo intermedio T di K contenente F si definisce

$$G(K, T) \stackrel{\text{def}}{=} \{\sigma \in G(K, F) \mid \sigma(t) = t \ \forall t \in T\}.$$

Per ogni H sottogruppo di $G(K, F)$ si definisce

$$K_H \stackrel{\text{def}}{=} \{k \in K \mid \sigma(k) = k \ \forall \sigma \in H\}.$$

Ebbene, valgono le seguenti proprietà.

7.2.17 PROPOSIZIONE. *Sia K un'estensione di F e sia $G(K, F)$ il suo gruppo di Galois. Per ogni sottogruppo H di $G(K, F)$ e ogni sottocampo intermedio T tale che $F \subseteq T \subseteq K$, si ha*

- (a) $G(K, K) = \text{id}$;
- (b) se T_1, T_2 sono campi tali che $F \subseteq T_1 \subseteq T_2 \subseteq K$, allora

$$G(K, T_2) \subseteq G(K, T_1);$$

- (c) $G(K, T)$ è un sottogruppo di $G(K, F)$;
- (d) $K_{\text{id}} = K$;
- (e) se H_1, H_2 sono sottogruppi di $G(K, F)$ tali che $H_1 \subseteq H_2 \subseteq G(K, F)$, allora

$$K_{H_2} \subseteq K_{H_1};$$

- (f) K_H è un sottocampo intermedio tra F e K :

- (g) $H \subseteq G(K, K_H)$;
 (h) $T \subseteq K_{G(K, T)}$.

Dimostrazione. Viene lasciata per esercizio. \square



ESERCIZI.

1. Si dimostrino tutti i punti della proposizione 7.2.17.
2. Provare che l'unico autonormorfismo di \mathbb{R} è l'autonomorfismo identico.
3. Si determini il gruppo di Galois $G(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q})$ e il suo campo fissato.



CONTROLLO.

1. Se F è un campo e K una sua estensione, cosa si intende per F -monomorfismo? e per F -automorfismo?
2. Date un esempio di F -monomorfismo di un'estensione che non è un F -automorfismo.
3. In che modo si può associare un gruppo ad ogni estensione? Chi sono i suoi elementi?
4. Che relazione c'è tra il grado di un'estensione e l'ordine del gruppo di Galois dell'estensione?

7.3. Estensioni galoisiane e il teorema di corrispondenza di Galois

Abbiamo già visto nel paragrafo precedente una relazione tra i sottogruppi del gruppo di Galois di un'estensione e i sottocampi intermedi dell'estensione. Raccogliamo qui di seguito quanto visto finora.

Sia K un'estensione di un campo F di caratteristica zero, e sia $G(K, F)$ il suo gruppo di Galois. Per ogni estensione intermedia T di F contenuta in K abbiamo definito il seguente sottoinsieme di $G(K, F)$ (che si dimostra essere un sottogruppo):

$$G(K, T) \stackrel{\text{def}}{=} \{\sigma \in G(K, F) \mid \sigma(t) = t \ \forall t \in T\}.$$

Per ogni sottogruppo H di $G(K, F)$, abbiamo definito

$$K_H \stackrel{\text{def}}{=} \{k \in K \mid \sigma(k) = k \ \forall \sigma \in H\}.$$

Tale sottoinsieme è un sottocampo di K che prende il nome di campo fissato da H .

Siano

$$\mathcal{F} \stackrel{\text{def}}{=} \{\text{tutti i campi intermedi tra } K \text{ e } F\}$$

e

$$\mathcal{G} \stackrel{\text{def}}{=} \{\text{tutti i sottogruppi di } G(K, F)\}.$$

Definiamo le seguenti due applicazioni

$$\begin{aligned}\Psi : \mathcal{F} &\longrightarrow \mathcal{G} \\ T &\longmapsto G(K, T)\end{aligned}$$

e

$$\begin{aligned}\Phi : \mathcal{G} &\longrightarrow \mathcal{F} \\ H &\longmapsto K_H.\end{aligned}$$

L'ultima proposizione del paragrafo precedente ci dice che la situazione è la seguente:

$$\begin{array}{ccc}\Psi : \mathcal{F} & \longrightarrow & \mathcal{G} \\ K & \longmapsto & G(K, K) = \{\text{id}\} \\ \sqcup & & \cap \\ T_1 & \longmapsto & G(K, T_1) \\ \sqcup & & \cap \\ T_2 & \longmapsto & G(K, T_2) \\ \sqcup & & \cap \\ F & \longmapsto & G(K, F)\end{array}$$

e

$$\begin{array}{ccc}\Phi : \mathcal{G} & \longrightarrow & \mathcal{F} \\ \{\text{id}\} & \longmapsto & K_{\{\text{id}\}} = K \\ \cap & & \cup \\ H_1 & \longrightarrow & K_{H_1} \\ \cap & & \cup \\ H_2 & \longrightarrow & K_{H_2} \\ \cap & & \cup \\ G(K, F) & \longrightarrow & K_{G(K, F)} \supseteq F.\end{array}$$

Quindi tali applicazioni *invertono le relazioni di inclusione*. Inoltre

$$(7.3.1) \quad \Phi(\Psi(T)) = \Phi(G(K, T)) = K_{G(K, T)} \supseteq T$$

$$(7.3.2) \quad \Psi(\Phi(H)) = \Psi(K_H) = G(K, K_H) \supseteq H.$$

Abbiamo visto anche casi in cui (7.3.1) è propria; ad esempio se $K = \mathbb{Q}(\sqrt[3]{5})$, $F = \mathbb{Q}$, $T = \mathbb{Q}$,

$$\Phi(\Psi(\mathbb{Q})) = \Phi(G(\mathbb{Q}(\sqrt[3]{5}), \mathbb{Q})) = \Phi(\{\text{id}\}) = \mathbb{Q}(\sqrt[3]{5}) \supsetneq \mathbb{Q}.$$

Quanto alla seconda inclusione, il prossimo teorema mostrerà come per estensioni finite vale sempre il segno di uguaglianza.

7.3.1 TEOREMA. *Sia K un'estensione finita di F e sia H un sottogruppo di $G(K, F)$. Indicato con K_H il campo fissato da H , allora*

$$(a) \quad [K : K_H] = |H|, \quad (b) \quad H = G(K, K_H).$$

Dimostrazione. Abbiamo già visto (proposizione 7.2.17) che

$$H \subseteq G(K, K_H) \implies |H| \leq |G(K, K_H)|$$

ed essendo K un'estensione finita di K_H , il teorema 7.2.10 dice che

$$|G(K, K_H)| \leq [K : K_H].$$

Quindi

$$|H| \leq |G(K, K_H)| \leq [K : K_H].$$

Queste due disuguaglianze ci dicono che basta provare il punto (a) del teorema, perché se $|H| = [K : K_H]$, allora H , sottogruppo di $G(K, K_H)$, con lo stesso ordine di $G(K, K_H)$, deve coincidere con $G(K, K_H)$. Proviamo quindi che

$$[K : K_H] = |H|.$$

Essendo K estensione finita di F , e quindi anche di K_H , esisterà un elemento $a \in K$ tale che $K = K_H(a)$. Se $[K : K_H] = m$, il polinomio minimo $p(x) \in K_H[x]$ di a avrà grado m . Indichiamo con $\sigma_1 = \text{id}, \sigma_2, \dots, \sigma_h$ gli h elementi di H . Formiamo le h funzioni simmetriche elementari negli h elementi $a = \sigma_1(a), \sigma_2(a), \dots, \sigma_h(a)$

$$\alpha_1 = \sigma_1(a) + \sigma_2(a) + \cdots + \sigma_h(a)$$

$$\alpha_2 = \sum_{i < j} \sigma_i(a)\sigma_j(a)$$

...

$$\alpha_h = \sigma_1(a)\sigma_2(a) \cdots \sigma_h(a).$$

Un qualunque elemento $\sigma_i \in H$ lascia fisse tali funzioni, come è ovvio verificare. Quindi gli elementi α_i stanno in K_H . Il polinomio

$$f(x) = (x - a)(x - \sigma_2(a)) \cdots (x - \sigma_h(a))$$

ha ovviamente come radice a , ed è a coefficienti in K_H , dato che sviluppando i prodotti si ottiene

$$f(x) = x^h - \alpha_1 x^{h-1} + \cdots + (-1)^h \alpha_h$$

che abbiamo visto essere a coefficienti in K_H . Ma allora, dato che il grado del polinomio *minimo* annullato da a è m , deve essere $h \geq m$, cioè $|H| \geq [K : K_H]$. Quindi $|H| = [K : K_H]$. \square

Le corrispondenze Ψ e Φ prendono il nome di *corrispondenze di Galois*. Ha senso chiedersi sotto quali ipotesi ulteriori le due applicazioni Ψ e Φ sono l'una l'inversa dell'altra, ossia quando avviene che in (g) e (h) della proposizione 7.2.17 vale il segno di uguaglianza. A questo scopo diamo un'altra caratterizzazione di un'estensione normale.

7.3.2 TEOREMA. *Sia K un'estensione finita di F . Le seguenti affermazioni sono equivalenti:*

- (i) K è un'estensione normale di F ;
- (ii) $K_{G(K,F)} \equiv F$.

Dimostrazione. (i) \Rightarrow (ii) Sia K normale su F . Dobbiamo provare che

$$(7.3.3) \quad K_{G(K,F)} = F.$$

Procederemo per induzione su $[K : F]$. Per $[K : F] = 1$ si ha $K = F$ e $K_{G(K,F)} = K_{\text{id}} = K = F$, quindi il risultato (7.3.3) è vero. Supponiamo vero il risultato (7.3.3) per ogni estensione normale K_1 di F_1 , con $[K_1 : F_1] < [K : F]$ e dimostriamolo per l'estensione K su F .

Essendo K estensione normale su F , K sarà campo di spezzamento di un polinomio $f(x) \in F[x]$. Possiamo supporre che $f(x)$ abbia un fattore irriducibile $p(x) \in F[x]$ di grado maggiore di 1, altrimenti vorrebbe dire che $K = F$, e quindi (7.3.3) sarebbe automaticamente vera. Siano $\alpha_1, \alpha_2, \dots, \alpha_s$ le s radici distinte di $p(x)$, appartenenti a K . K oltre ad essere campo di spezzamento di $f(x)$ considerato come polinomio a coefficienti in F , è anche campo di spezzamento di $f(x)$ pensato come polinomio a coefficienti in $F(\alpha_1)$. Ora,

$$[K : F(\alpha_1)] = \frac{n}{s} < n$$

quindi scatta l'ipotesi induttiva, e si può concludere che

$$(7.3.4) \quad K_{G(K,F(\alpha_1))} = F(\alpha_1).$$

Per provare (7.3.3) dobbiamo ora far vedere che, se $k \in K$ è lasciato fisso da ogni automorfismo di $G(K, F)$, allora k appartiene ad F , cioè non esiste fuori di F un elemento che sia lasciato fisso da *ogni* elemento di $G(K, F)$. Un tale elemento k (fissato da ogni elemento di $G(K, F)$) è certamente lasciato fisso da ogni elemento di $G(K, F(\alpha_1))$. In virtù di (7.3.4), k deve stare in $F(\alpha_1)$; esso si scriverà allora nella forma

$$(7.3.5) \quad k = a_0 + a_1\alpha_1 + \cdots + a_{s-1}\alpha_1^{s-1}, \quad a_i \in F.$$

In virtù dei teoremi sui campi di spezzamento, per ogni $i = 1, \dots, s$ esiste un automorfismo σ_i di K tale che

$$\begin{aligned}\sigma_i(\alpha_1) &= \alpha_i \\ \sigma_i(a) &= a \quad \forall a \in F\end{aligned}$$

essendo α_i , $i = 1, \dots, s$, tutte le radici (distinte) di $p(x)$. Ora, ogni σ_i lascia fisso k , dato che $k \in K_{G(K,F)}$, e anche ogni a_i . Quindi applicando σ_i alla relazione (7.3.5) si ottiene

$$(7.3.6) \quad k = a_0 + a_1\alpha_i + \dots + a_{s-1}\alpha_i^{s-1} \quad \forall i = 1, \dots, s.$$

Ma allora il polinomio

$$a_{s-1}x^{s-1} + \dots + a_1x + (a_0 - k)$$

è un polinomio di grado $s-1$ che, in virtù della (7.3.6), ammette s radici. Questo implica che deve trattarsi del polinomio nullo, e quindi in particolare $k - a_0 = 0$, cioè $k = a_0 \in F$.

Proviamo ora l'altra direzione, (ii) \Rightarrow (i). Per ipotesi vale la $K_{G(K,F)} = F$. Dobbiamo provare che K è campo di spezzamento di un polinomio a coefficienti in F . Sia $a \in K$ tale che $K = F(a)$ e sia

$$G(K,F) = \{\sigma_1 = \text{id}, \sigma_2, \dots, \sigma_n\}.$$

Si consideri il polinomio

$$f(x) = (x - \sigma_1(a))(x - \sigma_2(a)) \cdots (x - \sigma_n(a)).$$

Come sappiamo, i coefficienti di questo polinomio sono le funzioni simmetriche elementari α_i nelle radici $\sigma_1(a), \sigma_2(a), \dots, \sigma_n(a)$, e in quanto tali ogni α_i sta in $K_{G(K,F)} = F$. Quindi $f(x)$ è un polinomio appartenente a $F[x]$, K contiene tutte le radici di $f(x)$, e non può esistere un altro campo più piccolo contenente tutte le radici del polinomio e F , perché un tale campo dovrebbe contenere la radice a ed F , e quindi deve coincidere con $K = F(a)$. Quindi K è campo di spezzamento di un polinomio a coefficienti in F , ed è quindi un'estensione normale di F . \square

7.3.3 DEFINIZIONE. Una estensione galoisiana K di F è un'estensione finita e normale di F . \square

Si può anche dire che un'estensione galoisiana è un'estensione finita K di F tale che, se $\varphi \in I(K,F)$, allora $\varphi(K) \subseteq K$.

Siamo ora in grado di provare il seguente teorema che sarà la chiave di volta per la dimostrazione del teorema di corrispondenza di Galois. Ricordiamo che, mentre l'insieme $I(K,F)$ degli F -monomorfismi di un'estensione di grado n su F possiede sempre n F -monomorfismi, la stessa cosa non avviene per $G(K,F)$: nell'esempio 7.2.14 succedeva che $|G(K,F)| = 1$, mentre

$[K : F] = 3 = |\mathcal{I}(K, F)|$. È chiaro che se pretendiamo, come è ragionevole aspettarsi, che la struttura di $G(K, F)$ ci dia informazioni sui sottocampi dell'estensione K su F , un gruppo con un solo elemento non ci sarà di grande aiuto! Ebbene, se K è un'estensione galoisiana, il gruppo di Galois $G(K, F)$ viene a coincidere con $\mathcal{I}(K, F)$, e quindi ha ordine uguale al grado dell'estensione.

7.3.4 TEOREMA. *Sia K un'estensione galoisiana di F . Allora*

$$|G(K, F)| = [K : F].$$

Dimostrazione. Dal teorema 7.3.1 sappiamo che, qualunque sia il sottogruppo H di $G(K, F)$, si ha

$$|H| = [K : K_H].$$

Ma allora, per $H = G(K, F)$, tenuto conto che $K_{G(K, F)} = F$ essendo l'estensione galoisiana, sarà

$$|G(K, F)| = [K : K_{G(K, F)}] = [K : F]. \quad \square$$

Vale inoltre il seguente risultato, che si rivelerà fondamentale nel teorema di corrispondenza di Galois.

7.3.5 PROPOSIZIONE. *Sia K un'estensione galoisiana di F e sia T un campo intermedio, $F \subseteq T \subseteq K$. Le seguenti affermazioni sono equivalenti:*

- (i) T è un'estensione normale di F ;
- (ii) $\sigma(T) \subseteq T$ per ogni $\sigma \in G(K, F)$.

Dimostrazione. (i) \Rightarrow (ii) Sia $\sigma \in G(K, F)$, $t \in T$ e $s = \sigma(t)$. t è algebrico su F (perché appartiene ad un'estensione finita); detto $p(x) \in F[x]$ il suo polinomio minimo, $\sigma(t)$ è radice dello stesso polinomio. Ma allora t ed s sono coniugati su F . Essendo T normale su F , s deve appartenere a T .

(ii) \Rightarrow (i) Siano $\alpha \in T$ e $\beta \in K$ coniugati su F . Dobbiamo provare che β appartiene a T . α e β , in quanto coniugati su F , sono radici di uno stesso polinomio irriducibile a coefficienti in F , e pertanto esiste un F -isomorfismo τ

$$\begin{aligned} \tau : F(\alpha) &\longrightarrow F(\beta) \\ \alpha &\longmapsto \beta \\ a &\longmapsto a \quad \forall a \in F. \end{aligned}$$

Ma allora τ si estende ad un automorfismo $\sigma : K \rightarrow K$ per cui σ appartiene a $G(K, F)$. Allora, per l'ipotesi (ii), $\sigma(T) \subseteq T$ da cui $\beta = \sigma(\alpha)$ sta in T . \square

Abbiamo parlato di gruppo di Galois associato ad un'estensione K di F . Con la seguente definizione vediamo che ad ogni polinomio in $F[x]$ possiamo associare un gruppo.

7.3.6 DEFINIZIONE. Sia $f(x)$ un polinomio a coefficienti in un campo F . Si definisce *gruppo di Galois del polinomio $f(x)$* il gruppo di Galois della estensione K su F , dove K è il campo di spezzamento di $f(x)$. \square

Per quanto visto nel §7.2 a proposito degli F -monomorfismi (e degli F -automorfismi), il gruppo di Galois $G(K, F)$ di un polinomio $f(x) \in F[x]$ di grado n agisce sull'insieme $R = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ delle radici del polinomio (si ricordi §5.11). Quindi R viene ripartito in orbite. Se in particolare $f(x)$ è irriducibile, $G(K, F)$ agisce transitivamente sull'insieme delle sue n radici, ossia date comunque due radici α_i e α_j di $f(x)$, esiste un elemento σ di $G(K, F)$ tale che $\sigma(\alpha_i) = \alpha_j$. Ciò significa che esiste un'unica orbita, e quindi le radici di un polinomio irriducibile sono indistinguibili tra di loro rispetto all'azione di $G(K, F)$; non esiste pertanto una radice privilegiata rispetto ad un'altra.

Torniamo ora al gruppo di Galois di un polinomio, secondo la definizione 7.3.6. Trattandosi del gruppo di Galois associato ad un'estensione *galoisiana*, le due corrispondenze Ψ e Φ sono l'una l'inversa dell'altra. Non solo, nella corrispondenza tra l'insieme dei campi intermedi tra K e F e l'insieme dei sottogruppi di $G(K, F)$ avviene ora il notevole fatto che si conserva la normalità, nel senso che ad estensioni normali corrispondono sottogruppi normali e viceversa. Il seguente fondamentale teorema di corrispondenza di Galois precisa come si comportano le due corrispondenze.

7.3.7 TEOREMA DI CORRISPONDENZA DI GALOIS. *Sia $f(x)$ un polinomio a coefficienti in un campo F . Detto K il suo campo di spezzamento, sia $G(K, F)$ il suo gruppo di Galois. Indicato con \mathcal{F} l'insieme di tutti i sottocampi T di K che contengono F e con \mathcal{G} l'insieme di tutti i sottogruppi di $G(K, F)$, la*

$$\begin{aligned}\Psi : \mathcal{F} &\longrightarrow \mathcal{G} \\ T &\longmapsto G(K, T)\end{aligned}$$

è una corrispondenza biunivoca tra \mathcal{F} e \mathcal{G} , la cui inversa è la

$$\begin{aligned}\Phi : \mathcal{G} &\longrightarrow \mathcal{F} \\ H &\longmapsto K_H\end{aligned}$$

ossia

$$K_{G(K, T)} = T, \quad G(K, K_H) = H.$$

Inoltre valgono le seguenti proprietà:

(a) $[K : T] = |G(K, T)|$, $[T : F] = \frac{|G(K, F)|}{|G(K, T)|}$;

(b) T è un ampliamento normale di F se e solamente se $G(K, T)$ è un sottogruppo normale di $G(K, F)$;

(c) se T è un ampliamento normale di F , allora il gruppo $G(T, F)$ è tale che

$$G(T, F) \cong G(K, F)/G(K, T).$$

Dimostrazione. Che sia $H = G(K, K_H)$ si è già visto. Per quel che riguarda $T = K_{G(K, T)}$, questa relazione deriva dal teorema 7.3.2, una volta che si sia osservato che, essendo K estensione normale di F , è anche estensione normale di T . Le due relazioni dicono che le due applicazioni Ψ e Φ sono l'una l'inversa dell'altra.

Dimostrazione di (a): K è estensione normale di T , quindi $[K : T] = |G(K, T)|$ in base al teorema 7.3.4. Inoltre,

$$[K : F] = [K : T][T : F], \quad [K : F] = |G(K, F)|, \quad [K : T] = |G(K, T)|$$

da cui

$$[T : F] = \frac{|G(K, F)|}{|G(K, T)|}.$$

Dimostrazione di (b). Nella proposizione 7.3.5 si è visto che T è un'estensione normale di F se e solo se, per ogni $\sigma \in G(K, F)$, $\sigma(T) \subseteq T$. Ma allora, preso comunque un $\tau \in G(K, T)$, risulterà

$$\tau(\sigma(t)) = \sigma(t) \quad \forall t \in T, \quad \forall \sigma \in G(K, F).$$

Questa relazione equivale alla

$$\sigma^{-1}\tau\sigma(t) = t$$

ossia alla

$$\sigma^{-1}G(K, T)\sigma \subseteq G(K, T) \quad \forall \sigma \in G(K, F)$$

che è la condizione perché $G(K, T)$ sia normale in $G(K, F)$.

Viceversa, se $G(K, T) \trianglelefteq G(K, F)$, allora T è un'estensione normale di F ; infatti dalla

$$\sigma^{-1}\tau\sigma(t) = t \quad \forall t \in T, \quad \forall \tau \in G(K, T), \quad \forall \sigma \in G(K, F)$$

segue

$$\tau(\sigma(t)) = \sigma(t) \quad \forall t \in T, \quad \forall \sigma \in G(K, F), \quad \forall \tau \in G(K, T).$$

Quindi, dato che $\sigma(t)$ è fissato da τ e dato che $K_{G(K, T)} = T$ essendo K estensione normale, segue che $\sigma(t) \in T$.

Dimostrazione di (c). Dato che $\sigma(T) \subseteq T$ per ogni $\sigma \in G(K, F)$, allora ogni $\sigma \in G(K, F)$ induce un automorfismo $\sigma' \in G(T, F)$ definito da

$$\sigma'(t) = \sigma(t) \quad \forall t \in T.$$

Chiaramente $\sigma'(a) = a \forall a \in F$, quindi σ' appartiene a $G(T, F)$. L'applicazione

$$\begin{aligned}\varphi : G(K, F) &\longrightarrow G(T, F) \\ \sigma &\longmapsto \sigma'\end{aligned}$$

è un *omomorfismo* del gruppo $G(K, F)$ nel gruppo $G(T, F)$, il cui nucleo è

$$\begin{aligned}\text{Ker } \varphi &\stackrel{\text{def}}{=} \{\sigma \in G(K, F) \mid \sigma' = e_{G(T, F)}\} \\ &= \{\sigma \in G(K, F) \mid \sigma'(t) = t \forall t \in T\} = G(K, T).\end{aligned}$$

Quindi, per il teorema fondamentale di omomorfismo,

$$\text{Im } \varphi \simeq G(K, F)/G(K, T)$$

da cui

$$|\text{Im } \varphi| = \frac{|G(K, F)|}{|G(K, T)|} = [T : F] \stackrel{\text{per (7.3.1)}}{=} |G(T, F)|.$$

Quindi $\text{Im } \varphi = G(T, F)$, e la (7.3.3) è dimostrata. \square

Illustriamo il teorema di corrispondenza di Galois nel caso in cui il polinomio $f(x)$ sia $x^3 - 2 \in \mathbb{Q}[x]$. Risulta $x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2})$, ω radice terza primitiva dell'unità. Il campo di spezzettamento K di $x^3 - 2$ è $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Un elemento $\sigma \in G(K, \mathbb{Q})$ è individuato non appena si conoscano $\sigma(\sqrt[3]{2})$ e $\sigma(\omega)$. Il polinomio minimo su \mathbb{Q} di $\sqrt[3]{2}$ è $x^3 - 2$, il polinomio minimo di ω su \mathbb{Q} è $x^2 + x + 1$. Esistono in tutto sei automorfismi:

$$\sigma_1 = \text{id}$$

$$\sigma_2 : \quad \sigma_2(\omega) = \omega^2, \quad \sigma_2(\sqrt[3]{2}) = \sqrt[3]{2}$$

$$\sigma_3 : \quad \sigma_3(\omega) = \omega, \quad \sigma_3(\sqrt[3]{2}) = \omega\sqrt[3]{2}$$

$$\sigma_4 = \sigma_3^2 : \quad \sigma_4(\omega) = \omega, \quad \sigma_4(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$$

$$\sigma_5 = \sigma_2 \circ \sigma_3 : \quad \sigma_5(\omega) = \omega^2, \quad \sigma_5(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$$

$$\sigma_6 = \sigma_2 \circ \sigma_3^2 : \quad \sigma_6(\omega) = \omega^2, \quad \sigma_6(\sqrt[3]{2}) = \omega\sqrt[3]{2}.$$

Risulta, come è facile controllare, $G(K, \mathbb{Q}) \simeq S_3$. I sottogruppi non banali di $G(K, \mathbb{Q})$ sono $H_1 = \langle \sigma_2 \rangle$, $H_2 = \langle \sigma_3 \rangle$, $H_3 = \langle \sigma_6 \rangle$, $H_4 = \langle \sigma_3 \rangle$, $|H_1| = |H_2| = |H_3| = 2$, $|H_4| = 3$.

I campi fissati sono i seguenti:

$$K_{H_1} = \mathbb{Q}(\sqrt[3]{2}), \quad [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

$$K_{H_2} = \mathbb{Q}(\omega\sqrt[3]{2}), \quad [\mathbb{Q}(\omega\sqrt[3]{2}) : \mathbb{Q}] = 3$$

$$K_{H_3} = \mathbb{Q}(\omega^2\sqrt[3]{2}), \quad [\mathbb{Q}(\omega^2\sqrt[3]{2}) : \mathbb{Q}] = 3$$

$$K_{H_4} = \mathbb{Q}(\omega), \quad [\mathbb{Q}(\omega) : \mathbb{Q}] = 2.$$

In definitiva si ha la corrispondenza illustrata in figura 7.8.

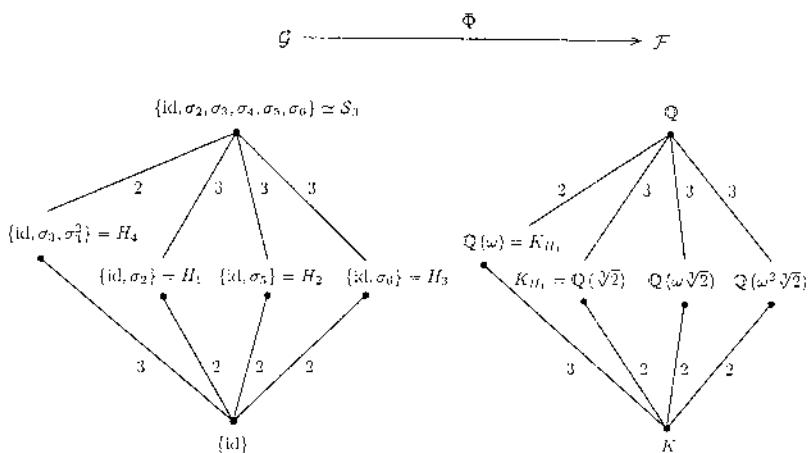


FIGURA 7.8

Chiudiamo il paragrafo calcolando esplicitamente il gruppo di Galois associato al polinomio $x^n - 1 \in \mathbb{Q}[x]$.

7.3.8 PROPOSIZIONE. *Sia n un fissato elemento di \mathbb{N} . Il gruppo di Galois del polinomio $x^n - 1$ è isomorfo al gruppo moltiplicativo $U(\mathbb{Z}_n)$ degli elementi invertibili di \mathbb{Z}_n .*

Dimostrazione. Il campo di spezzamento di $x^n - 1$ su \mathbb{Q} è (cfr. proposizione 6.2.14) $\mathbb{Q}(\zeta)$, dove ζ è una qualunque radice n -esima primitiva dell'unità, e sappiamo che il grado di $\mathbb{Q}(\zeta)$ su \mathbb{Q} è $\varphi(n)$. In base all'esempio 7.2.16, $U(\mathbb{Z}_n) \cong G(\mathbb{Q}(\zeta), \mathbb{Q})$. \square



ESERCIZI.

- Si determini il gruppo di Galois di ciascuno dei seguenti polinomi a coefficienti in \mathbb{Q} :

$$x^3 + 2x^2 + 5x + 10$$

$$x^4 - 7x^2 + 10$$

$$x^5 + 2x^4 - 5x^3 - 10x^2 + 6x + 12$$

$$x^3 - 1$$

$$x^3 - 7$$

$$x^4 - 5$$

$$x^4 - 4x^2 + 2 .$$

2. Determinare campo di spezzamento K e gruppo di Galois del polinomio $x^6 + x^4 - 4x^2 - 4 \in \mathbb{Q}[x]$. Si determinino tutti i sottocampi di K .
3. Si completi, con tutti i dettagli, l'esempio del gruppo di Galois di $x^3 - 2$, controllando quali sono le estensioni normali, ecc.
4. Sia K il campo di spezzamento del polinomio di $\mathbb{Q}(\sqrt{3})[x]$

$$x^3 + \sqrt{3}x^2 - 2x - 2\sqrt{3}.$$

Si determini $G(K, \mathbb{Q}(\sqrt{3}))$.

5. Sia K il campo $\mathbb{Q}(i, \sqrt[3]{5})$. Determinare il gruppo degli automorfismi di K . Si dica poi se K è un'estensione galoisiana di \mathbb{Q} .
6. Si dica se il campo $\mathbb{Q}(i\sqrt[3]{2})$ è un'estensione galoisiana di \mathbb{Q} e si determini il sottocampo di $\mathbb{Q}(i\sqrt[3]{2})$ lasciato fisso da $G(\mathbb{Q}(i\sqrt[3]{2}), \mathbb{Q})$.
7. Si determini il gruppo di Galois del polinomio $x^5 - 3 \in \mathbb{Q}(\zeta)[x]$ su $\mathbb{Q}(\zeta)$, dove ζ è una radice quinta primitiva dell'unità.
8. Confrontare i gruppi di Galois dei polinomi in $\mathbb{Q}[x]$ $x^8 - 1$ e $x^4 + 1$.
9. Si verifichi il teorema di corrispondenza di Galois nel caso del polinomio $x^5 - 1$ a coefficienti in \mathbb{Q} . Determinare una espressione esplicita, in termini di radici quadrate, della radice quinta primitiva dell'unità, ζ_5 .
10. Siano K un'estensione galoisiana di F , H_1 e H_2 sottogruppi di $G(K, F)$ e T_1, T_2 sottocampi di K contenenti F tali che $G(K, T_1) = H_1$ e $G(K, T_2) = H_2$. Si provi che

$$G(K, T_1(T_2)) = H_1 \cap H_2, \quad G(K, T_1(T_2)) = \langle H_1, H_2 \rangle;$$

con $\langle H_1, H_2 \rangle$ si denota il sottogruppo generato da H_1 e H_2 , ossia il sottogruppo costituito da tutti i prodotti finiti di elementi di H_1 e H_2 , e con $T_1(T_2)$ si denota il sottocampo composto di T_1 e T_2 , ossia il sottocampo generato su T_1 da T_2 (che coincide con il sottocampo generato su T_2 da T_1).

11. Si provi che se $\varphi \in I(K, F)$ è tale che $\varphi(K) \subseteq K$, allora $\varphi(K) = K$, ossia φ è un automorfismo. Quindi un'estensione galoisiana è tale che $I(K, F) = G(K, F)$.



CONTROLLO.

1. Enumerare e spiegare bene il teorema di corrispondenza di Galois.

7.4. Applicazioni del teorema di corrispondenza di Galois

Come prima applicazione del teorema di corrispondenza di Galois, diamo una dimostrazione (basata su semplici nozioni algebriche sviluppate nel corso) del teorema fondamentale dell'algebra. Ricordiamo (cfr. definizione 6.1.25) che un campo K si dice *algebricamente chiuso* se ogni polinomio si spezza in fattori lineari su K .

Premettiamo il seguente lemma.

7.4.1 LEMMA. *Sia F una campo di caratteristica zero tale che ogni estensione finita K di F , $K \neq F$, sia tale che $[K : F]$ sia divisibile per un numero primo p . Allora ogni estensione finita di F ha come grado una potenza di p .*

Dimostrazione. Sia K un'estensione finita di F . Non è restrittivo supporre che K sia un'estensione normale di F . Sia $G(K, F)$ il gruppo di Galois di tale estensione. Dato che $[K : F]$ per ipotesi è divisibile per p , e dato che $[K : F] = |G(K, F)|$, se $|G(K, F)|$ è divisibile per p^α , ma non per $p^{\alpha-1}$, allora, per i teoremi di Sylow, $G(K, F)$ conterrà un sottogruppo H di ordine p^α . Il campo fissato K_H è tale che

$$[K_H : F] = \frac{|G(K, F)|}{|G(K, K_H)|} = \frac{|G(K, F)|}{|H|}$$

e quest'ultimo *non* è divisibile per p . Quindi deve essere $[K_H : F] = 1$, cioè $K_H = F$, da cui $G(K, F) = H$, per cui $[K : F] = |G(K, F)| = p^n$ per qualche n . \square

7.4.2 TEOREMA FONDAMENTALE DELL'ALGEBRA. *Il campo \mathbb{C} dei numeri complessi è algebricamente chiuso.*

Dimostrazione. Il campo \mathbb{R} non può avere nessuna estensione finita di grado dispari maggiore di 1: se così fosse, essendo l'estensione semplice, del tipo $\mathbb{R}(a)$, il polinomio minimo di a sarebbe un polinomio *irriducibile* su \mathbb{R} di grado dispari maggiore di 1, il che è assurdo. Quindi ogni estensione finita di \mathbb{R} ha un grado divisibile per 2; in virtù del lemma 7.4.1, con $p = 2$, ogni estensione K di \mathbb{R} ha come grado una potenza di 2. Sia $f(x)$ un polinomio in $\mathbb{C}[x]$, e sia K il suo campo di spezzamento su \mathbb{C} . Faremo vedere che $K = \mathbb{C}$, cioè ogni polinomio a coefficienti in \mathbb{C} si spezza in \mathbb{C} .

In quanto campo di spezzamento, K è un'estensione finita e normale di \mathbb{C} . Risulta

$$2^n = [K : \mathbb{R}] = [K : \mathbb{C}][\mathbb{C} : \mathbb{R}] = [K : \mathbb{C}] \cdot 2 \implies [K : \mathbb{C}] = 2^{n-1}.$$

Allora

$$|G(K, \mathbb{C})| = [K : \mathbb{C}] = 2^{n-1}.$$

Se fosse $K \neq \mathbb{C}$, sarebbe $n > 1$, per cui, in base al corollario 5.12.10, $G(K, \mathbb{C})$ possiederebbe un sottogruppo H di indice 2; ma allora

$$[K_H : \mathbb{C}] = 2.$$

relazione impossibile, dato che ogni polinomio a coefficienti in \mathbb{C} di grado 2 si spezza sicuramente. Ne segue che deve essere $K = \mathbb{C}$. \square

Diamo ora un'altra importante applicazione del teorema di corrispondenza di Galois, che in realtà non si dovrebbe chiamare *applicazione*, dal momento che è stata la *motivazione* da cui è nata l'intera teoria di Galois. Essa riguarda la possibilità di trovare le soluzioni di una equazione polinomiale in funzione dei coefficienti dell'equazione, usando solo le operazioni fondamentali ed estrazioni di radici, o, come si usa dire, di *risolvere per radicali una data equazione polinomiale*. Formule risolutive di questo tipo sono state viste nel §3.5, in relazione alle equazioni di secondo, terzo e quarto grado. Galois ha dato una condizione necessaria e sufficiente per la risolubilità per radicali di una data equazione polinomiale, condizione legata alla natura del gruppo di Galois del polinomio in questione, ossia alla *risolubilità del gruppo*: nel §5.15 si è data la definizione e si sono viste le prime proprietà dei gruppi *risolubili*. Cominciamo con la seguente definizione.

7.4.3 DEFINIZIONE. Un'estensione L di un campo F si dice *radicale* se

$$L = F(\alpha_1, \alpha_2, \dots, \alpha_m)$$

con $\alpha_i^{n_i} \in F$, $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$ ($i = 1, \dots, m$) per interi positivi n_1, n_2, \dots, n_m . \square

Gli elementi α_i si dicono formare una successione radicale per L su F . Ad esempio, se $F = \mathbb{Q}$ le seguenti sono estensioni radicali:

$$\mathbb{Q}(\sqrt[3]{4}), \quad \mathbb{Q}\left(\sqrt{5}, \sqrt[3]{2\sqrt{5}+4}, \sqrt{6+\sqrt[3]{2\sqrt{5}+4}}\right).$$

In pratica, un'estensione radicale di un campo F si ottiene aggiungendo via via radici n -esime, per vari n (figura 7.9).

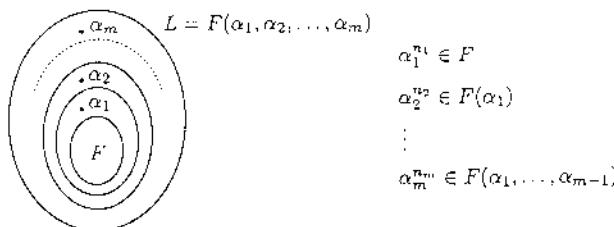


FIGURA 7.9

7.4.4 DEFINIZIONE. Sia $f(x) \in F[x]$. Si dice che $f(x)$ è *risolubile per radicali* su F se il suo campo di spezzamento K su F è contenuto in un'estensione radicale L su F . \square

Stiamo quindi chiedendo che ogni elemento del campo di spezzamento (e quindi ogni radice del polinomio) sia esprimibile per radicali. In altre parole, dati un campo F e un polinomio $f(x) \in F[x]$, si dice che $f(x)$ è risolubile per radicali se è possibile trovare una successione di campi

$$F_1 = F(\alpha_1), \quad F_2 = F_1(\alpha_2), \dots, \quad F_m = F_{m-1}(\alpha_m)$$

tale che $\alpha_1^{n_1} \in F$, $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$ e tale che tutte le radici di $f(x)$ stiano in F_m .

Ad esempio, il polinomio $x^n - 1$ è risolubile per radicali, perché il suo campo di spezzamento $\mathbb{Q}(\zeta)$, ζ radice n -esima primitiva dell'unità, è lui stesso un'estensione radicale.

Il lemma che segue ci sarà utile tra poco.

7.4.5 LEMMA. *Sia F un campo che contiene tutte le radici n -esime dell'unità. Se a è un elemento non nullo di F , allora il gruppo di Galois di $x^n - a$ è abeliano.*

Dimostrazione. Se α è una radice di $x^n - a$, tutte le radici di $x^n - a$ sono $\alpha, \omega\alpha, \omega^2\alpha, \omega^{n-1}\alpha$, con ω radice n -esima primitiva dell'unità. Quindi (si ricordi che F contiene tutte le radici n -esime dell'unità) il campo $K = F(\alpha)$ è il campo di spezzamento di $x^n - a$ (si verifichino i dettagli). Detti σ e τ due elementi di $G(K, F)$, per provare che $\sigma\tau = \tau\sigma$ basta provare che $\sigma(\tau(\alpha)) = \tau(\sigma(\alpha))$. Ora, dato che un elemento di $G(K, F)$ manda una radice di $x^n - a$ in un'altra radice dello stesso polinomio, si avrà

$$\sigma(\alpha) = \omega^h \alpha, \quad \tau(\alpha) = \omega^k \alpha.$$

Quindi

$$\sigma(\tau(\alpha)) = \sigma(\omega^k \alpha) = \omega^k \omega^h \alpha = \omega^{h+k} \alpha = \tau(\sigma(\alpha))$$

dato che $\sigma(\omega^i) = \omega^i$ perché $\omega \in F$. \square

Non è restrittivo supporre che un'estensione radicale sia *galoisiana*. Infatti il seguente lemma mostra che ogni estensione radicale è contenuta in un'estensione radicale galoisiana.

7.4.6 LEMMA. *Sia L un'estensione radicale su F . Allora L è contenuta in un'estensione radicale M di F tale che M sia un'estensione galoisiana su F .*

Dimostrazione. Sia $L = F(\alpha_1, \alpha_2, \dots, \alpha_m)$ con $\alpha_1^{n_1} \in F$ e $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$. Se $p_i(x)$ è il polinomio minimo di α_i , sia M il campo di spezzamento del polinomio $f(x) = p_1(x)p_2(x) \cdots p_m(x)$. M è un'estensione galoisiana di F contenente L e radicale: infatti $F(\alpha_i)$ è isomorfo a $F(\beta_{ij})$, dove β_{ij} è una qualunque radice di $p_i(x)$, e tale isomorfismo si può estendere ad un F -automorfismo di M . Dato che α_i appartiene ad un'estensione radicale di F , anche ogni β_{ij} appartiene ad un'estensione radicale di F . \square

Il lemma provato è importante, perché ci permette di utilizzare il teorema di corrispondenza di Galois per dimostrare il prossimo teorema.

7.4.7 TEOREMA. *Sia L un'estensione galoisiana radicale di un campo F . Allora il suo gruppo di Galois $G(L, F)$ è risolubile.*

Dimostrazione. Sia $L = F(\alpha_1, \alpha_2, \dots, \alpha_m)$ con $\alpha_i^{n_i} \in F$ e $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$. Se indichiamo con n il $\text{mcm}(n_1, n_2, \dots, n_m)$, ogni α_i è tale che $\alpha_i^n \in F$ e $\alpha_i^n \in F(\alpha_1, \alpha_2, \dots, \alpha_{i-1})$, quindi nella definizione di estensione radicale si può, senza perdita di generalità, supporre che tutti gli n_i siano uguali ad un intero n . Sia ζ una radice n -esima primitiva dell'unità, e sia $L' = L(\zeta)$. L' è anch'essa un'estensione galoisiana di F . Sia $H = G(L', F)$ il gruppo di Galois di L' su F . Poniamo

$$(7.4.1) \quad L_0 \stackrel{\text{def}}{=} F, \quad L_1 \stackrel{\text{def}}{=} F(\zeta), \quad L_i \stackrel{\text{def}}{=} F(\zeta, \alpha_1, \alpha_2, \dots, \alpha_{i-1})$$

per $i = 2, \dots, m+1$. Ovviamente $L_{m+1} = L'$ e

$$(7.4.2) \quad F = L_0 \subseteq L_1 \subseteq \dots \subseteq L_{m+1} = L'.$$

In base al teorema di corrispondenza di Galois, a tale catena di estensioni corrisponde la seguente catena di sottogruppi di $G(L', F)$

$$G(L', F) \supseteq G(L', L_1) \supseteq G(L', L_2) \supseteq \dots \supseteq G(L', L') = \{e\}.$$

Asseriamo che ciascuno dei sottogruppi della catena è normale nel precedente e che i quozienti sono abeliani. L_1 è campo di spezzamento del polinomio $x^n - 1$ e in quanto tale è un'estensione galoisiana, quindi, per il teorema di corrispondenza di Galois, $G(L', L_1) \trianglelefteq G(L', F)$; inoltre il suo gruppo di Galois $G(L_1, F)$ è abeliano (cfr. proposizione 7.3.8); ma $G(L_1, F) \cong G(L', F)/G(L', L_1)$, quindi il primo quoziente della catena è abeliano. Esaminiamo ora le altre estensioni, L_{i+1} su L_i , della catena (7.4.2): ciascuna di queste estensioni contiene le radici n -esime dell'unità, ed è tale che $L_{i+1} = L_i(\alpha_i)$, α_i essendo una radice di $x^n - a_i$, $a_i = \alpha_i^n \in L_i$. Ma allora ogni L_{i+1} è un'estensione galoisiana di L_i , e quindi (per il teorema di corrispondenza di Galois) si ha $G(L', L_{i+1}) \trianglelefteq G(L', L_i)$; inoltre (lemma 7.4.5) ha gruppo di Galois $G(L_{i+1}, L_i) \cong G(L', L_i)/G(L', L_{i+1})$ abeliano.

Abbiamo così provato che il gruppo $G(L', F)$ è risolubile. Resta da provare che $G(L, F)$ è risolubile. La situazione è la seguente:

$$F \subseteq L \subseteq L'.$$

Posto $H_1 = G(L', F)$, $H_2 = G(L', L)$, è $H_2 \trianglelefteq H_1$ (essendo l'estensione L su F galoisiana) e $G(L, F) \cong H_1/H_2$. Essendo $G(L, F)$ quoziente di un gruppo risolubile, è risolubile (cfr. corollario 5.15.6). Il teorema è concluso. \square

Abbiamo così provato che il gruppo di Galois di ogni estensione galoisiana radicale è risolubile. È immediato allora provare che un polinomio risolubile per radicali ha gruppo di Galois risolubile.

7.4.8 PROPOSIZIONE. *Sia $f \in F[x]$ un polinomio risolubile per radicali su F . Allora il suo gruppo di Galois è risolubile.*

Dimostrazione. Per definizione di polinomio risolubile, esisterà un'estensione radicale (che possiamo senza perdita di generalità supporre galoisiana) L tale che sia $F \subseteq K \subseteq L$. Dobbiamo provare che $G(K, F)$ è risolubile. Essendo K estensione galoisiana di F , $G(L, K) \trianglelefteq G(L, F)$, e $G(K, F) \cong G(L, F)/G(L, K)$. Ma $G(L, F)$, per il teorema 7.4.7, è risolubile, quindi tale è anche $G(K, F)$, in quanto immagine omomorfa di un gruppo risolubile. \square

Vale anche il viceversa di questo teorema, ma ci limitiamo ad enunciarlo.

7.4.9 TEOREMA. *Un polinomio $f(x) \in F[x]$ è risolubile per radicali su F se e solo se il suo gruppo di Galois è risolubile.*

7.4.10 DEFINIZIONE. Sia $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ un polinomio a coefficienti in un campo F . Diremo che si tratta del *polinomio generale di grado n su F* se lo pensiamo come polinomio su $F(a_1, a_2, \dots, a_n)$. \square

In altre parole, non stiamo considerando i coefficienti a_1, a_2, \dots, a_n come fissati elementi del campo F ma come elementi di $F(a_1, a_2, \dots, a_n)$. Dire pertanto che il polinomio "generale" di grado n su F è risolubile per radicali equivale a trovare una formula per le radici di $f(x)$ nella quale intervengono radici m -esime per vari m di funzioni razionali in a_1, \dots, a_n .

Con il prossimo teorema proveremo il famoso risultato di Abel-Ruffini, secondo cui il polinomio generale di grado n con $n \geq 5$, non è risolubile per radicali, cioè non esiste una formula che generalizza la ben nota formula risolutiva per le equazioni polinomiali di secondo grado e le formule risolutive per le equazioni di terzo e quarto grado, che esprimono le radici del polinomio in funzione dei coefficienti con operazioni razionali e con estrazioni di radici.

7.4.11 TEOREMA DI ABEL-RUFFINI. *Il polinomio generale di grado $n \geq 5$ non è risolubile per radicali.*

Dimostrazione. Basta provare che il suo gruppo di Galois non è risolubile. Proveremo che il suo gruppo di Galois è l'intero gruppo simmetrico S_n , che sappiamo non essere risolubile per $n \geq 5$.

Innanzitutto, il campo di spezzamento di $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ su $F(a_1, a_2, \dots, a_n)$ è il campo delle funzioni razionali in x_1, x_2, \dots, x_n . Infatti i coefficienti a_i del polinomio $f(x)$ sono le funzioni simmetriche elementari delle

radici x_1, x_2, \dots, x_n . Quindi $F(x_1, x_2, \dots, x_n)$ contiene $F(a_1, a_2, \dots, a_n)$ e il polinomio $f(x)$ si spezza in $F(x_1, x_2, \dots, x_n)$ in fattori lineari

$$f(x) = (x - x_1)(x - x_2) \cdots (x - x_n)$$

e non si può spezzare in un campo più piccolo.

Ora $F(a_1, a_2, \dots, a_n)$ risulta essere il campo dei quozienti nelle funzioni simmetriche elementari, e in quanto tale è contenuto nel campo fissato da S_n . In realtà coincide esattamente con tale campo, perché abbiamo visto a suo tempo che *ogni funzione razionale simmetrica, cioè fissata da S_n , è esprimibile come funzione razionale nelle funzioni simmetriche elementari* (teorema 3.6.7).

Quindi, dalla relazione $G(K, K_H) = H$ per ogni sottogruppo H dell'intero gruppo di Galois, segue, per $H = S_n$ e $K = F(x_1, x_2, \dots, x_n)$ e tenuto conto che $K_{S_n} = F(a_1, a_2, \dots, a_n)$,

$$G(K, F(a_1, a_2, \dots, a_n)) = G(K, K_{S_n}) = S_n$$

cioè il gruppo di Galois del polinomio generale di grado n è il gruppo simmetrico su n elementi. \square

Esistono altri casi in cui il gruppo di Galois di un polinomio coincide con tutto S_n , e quindi, se $n \geq 5$, il polinomio non è risolubile per radicali. Il prossimo teorema ne offre un esempio.

7.4.12 TEOREMA. *Sia $p(x)$ un polinomio a coefficienti in \mathbb{Q} , irriducibile su \mathbb{Q} e di grado p primo. Se $p(x)$ ha esattamente due radici non reali nel campo \mathbb{C} dei numeri complessi, allora il suo gruppo di Galois su \mathbb{Q} è il gruppo simmetrico S_p .*

Dimostrazione. Sia K il campo di spezzamento di $p(x)$ su \mathbb{Q} . Detta α una radice di $p(x)$, essendo $p(x)$ irriducibile, risulta $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$, da cui $[K : \mathbb{Q}]$ è divisibile per p . Ora, se $G(K, \mathbb{Q})$ è il gruppo di Galois di $p(x)$, risulta $|G(K, \mathbb{Q})| = [K : \mathbb{Q}]$, e quindi l'ordine di $G(K, \mathbb{Q})$ è divisibile per p . Per il teorema di Cauchy, in $G(K, \mathbb{Q})$ esiste un elemento, σ , di periodo p , ossia un p -ciclo.

Ora, sappiamo che $p(x)$ possiede solamente due radici non reali, siano esse α_1, α_2 . Deve essere $\alpha_2 = \overline{\alpha_1}$; siano $\alpha_3, \dots, \alpha_p$ le altre radici (reali). Allora il campo di spezzamento di $p(x)$ è $K = \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_p)$. L'applicazione τ che manda un elemento nel suo complesso coniugato è un automorfismo che muta K in sé, lascia fisse tutte le radici α_i con $i \neq 1, 2$ e manda α_1 in α_2 . Si tratta quindi di un automorfismo di periodo 2, appartenente a $G(K, \mathbb{Q})$. Pensato il gruppo di Galois come immerso in S_p , (pensando cioè ogni elemento del gruppo di Galois come una permutazione delle p radici del polinomio), τ corrisponde alla trasposizione $(1, 2)$. Quindi $G(K, \mathbb{Q})$ contiene una trasposizione τ ed un p -ciclo σ . Prendendo, se necessario, una potenza del p -ciclo, che, essendo p primo, è ancora un p -ciclo, possiamo supporre che il p -ciclo sia $(1, 2, \dots, p)$.

Dato che ogni gruppo simmetrico S_n è generato da $(1, 2)$ e $(1, 2, \dots, n)$, si ha che il gruppo di Galois di $p(x)$ coincide con tutto S_p . \square

7.4.13 COROLLARIO. *Nelle ipotesi del teorema precedente, il campo di spezzamento di $p(x)$ su \mathbb{Q} ha grado $p!$.*

Dimostrazione. Conseguenza dell'uguaglianza

$$|G(K, F)| = [K : F]. \quad \square$$

Chiudiamo il paragrafo con un problema. Dato un gruppo finito G , esiste una estensione K di \mathbb{Q} tale che $G \cong G(K, \mathbb{Q})$? Stiamo chiedendo se ogni gruppo finito è isomorfo al gruppo di Galois di qualche estensione dei razionali. Se togliamo la richiesta che l'estensione sia un'estensione dei razionali, la risposta è positiva, e semplice da dimostrare (cfr. esercizio 7.4.3). Il problema posto invece è un problema molto difficile. Si sa che i gruppi simmetrici e i gruppi alterni sono realizzabili come gruppi di Galois su \mathbb{Q} . È stato dimostrato da Shafarevich nel 1954 che ogni gruppo risolubile di ordine dispari è gruppo di Galois di qualche estensione dei razionali. A tutt'oggi il problema è aperto.



ESERCIZI.

1. Si costruiscano dei polinomi a coefficienti in \mathbb{Q} e di grado n il cui gruppo di Galois sia il gruppo S_n .
2. Si provi che ogni polinomio a coefficienti in \mathbb{R} è risolubile per radicali su \mathbb{R} .
3. Sia G un gruppo finito. Si provi che esiste un'estensione galoisiana E su F tale che $G(E, F) \cong G$. Questo significa che ogni gruppo finito si può pensare come gruppo di Galois di qualche estensione E di un opportuno campo F .



CONTROLLO.

1. Una estensione radicale è ...
2. Un polinomio è risolubile per radicali quando ...

7.5. Costruzione di poligoni regolari

In questo paragrafo affronteremo il problema della costruitibilità di poligoni regolari con n lati. Osserviamo innanzitutto che saper costruire un poligono regolare di n lati equivale a saper costruire l'angolo $2\pi/n$, o, equivalentemente, $\cos(2\pi/n)$.

Dimostreremo la seguente importante caratterizzazione.

7.5.1 TEOREMA. *Condizione necessaria e sufficiente perché un poligono regolare con n lati sia costruibile è che, indicata con ζ una radice n -esima primitiva dell'unità, esista un $h \in \mathbb{N}$ tale che sia*

$$[\mathbb{Q}(\zeta), \mathbb{Q}] = 2^h.$$

Dimostrazione. Come è immediato verificare, risulta

$$\zeta + \frac{1}{\zeta} = 2 \cos \frac{2\pi}{n} \in \mathbb{R}$$

e quindi un n -gono regolare è costruibile se e solo se $\zeta + 1/\zeta$ è costruibile. Si avrà quindi

$$\mathbb{Q}(\cos \frac{2\pi}{n}) = \mathbb{Q}(\zeta + \frac{1}{\zeta}) \subset \mathbb{Q}(\zeta).$$

Studiamo questo campo intermedio $\mathbb{Q}(\zeta + 1/\zeta)$.

Detto $K = \mathbb{Q}(\zeta)$ il campo di spezzamento di $x^n - 1$, sappiamo (cfr. proposizione 6.2.14) che

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n).$$

Sia $\sigma \in G(K, \mathbb{Q})$, e sia $\sigma(\zeta) = \zeta^r$ per qualche r tale che $1 < r < n$. Quindi

$$\sigma(\zeta + \frac{1}{\zeta}) = \zeta^r + \frac{1}{\zeta^r} = 2 \cos \frac{2\pi r}{n}.$$

Esaminiamo $G(K, \mathbb{Q}(\zeta + 1/\zeta))$. Se $\sigma \in G(K, \mathbb{Q}(\zeta + 1/\zeta))$, deve essere $\sigma(\zeta + 1/\zeta) = \zeta + 1/\zeta$, ossia $2 \cos(2\pi/n) = 2 \cos(2\pi r/n)$, relazione che nell'intervallo $(1, n)$ è verificata solo da $r = n - 1$. Gli unici elementi di $G(K, \mathbb{Q}(\zeta + 1/\zeta))$ sono quindi l'automorfismo identico e l'automorfismo che manda ζ in $1/\zeta$. Ma per il teorema di corrispondenza di Galois,

$$|G(K, \mathbb{Q}(\zeta + 1/\zeta))| = [K : \mathbb{Q}(\zeta + 1/\zeta)],$$

quindi

$$[K : \mathbb{Q}(\zeta + 1/\zeta)] = 2,$$

da cui

$$(7.5.1) \quad [\mathbb{Q}(\zeta + 1/\zeta) : \mathbb{Q}] = \frac{\varphi(n)}{2}.$$

Proviamo che la condizione del teorema è necessaria. Se $\zeta + 1/\zeta$ è costruibile, sappiamo (cfr. proposizione 7.1.11) che $\mathbb{Q}(\zeta + 1/\zeta)$ è un'estensione di grado 2^t per qualche $t \in \mathbb{N}$. Ma allora, per la (7.5.1), anche $\varphi(n)$ è una potenza di 2, e quindi $[\mathbb{Q}(\zeta), \mathbb{Q}]$ è una potenza di 2.

Dimostriamo la sufficienza. Supponiamo che $[\mathbb{Q}(\zeta) : \mathbb{Q}] (= \varphi(n))$ sia una potenza 2^t , $t \in \mathbb{N}$. Abbiamo visto sopra che $\mathbb{Q}(\zeta + 1/\zeta)$ è un sottocampo di $\mathbb{Q}(\zeta)$, ha grado $\varphi(n)/2$ su \mathbb{Q} ed è il campo fissato da $H_1 = \{\text{id}, \sigma\}$, dove σ è l'automorfismo che manda ζ in $1/\zeta$. Allora $|G(\mathbb{Q}(\zeta), \mathbb{Q})| = 2^t$ e, in virtù del

teorema 5.12.8, applicato al caso $m = 1$, esiste una catena di sottogruppi H_j di ordini 2^j , $j = 0, 1, \dots, t$

$$\text{id} = H_0 < H_1 < \dots < H_t = G(\mathbb{Q}(\zeta), \mathbb{Q}) .$$

In virtù del teorema di corrispondenza di Galois, si avranno le seguenti relazioni tra i campi fissati da tali sottogruppi:

$$\mathbb{Q} = K_{H_t} \subset K_{H_{t-1}} \subset \dots \subset K_{H_1} = \mathbb{Q}(\zeta + \frac{1}{\zeta})$$

con $[K_{H_{j-1}} : K_{H_j}] = 2$ per ogni $j = 0, \dots, t$. Essendo ciascuna di queste estensioni di grado due sulla precedente, riusciamo via via a costruire con radici quadrate successive gli elementi di $\mathbb{Q}(\zeta + 1/\zeta)$, e in particolare $\zeta + 1/\zeta$ è costruibile. Il teorema è completamente provato. \square

7.5.2 COROLLARIO. *Un n -gono regolare è costruibile se e solo se $\varphi(n) = 2^k$ per qualche $k \in \mathbb{N}$.*

Dimostrazione. Basta ricordare che $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$. \square

Vediamo quali conseguenze porta questo fatto. Ricordiamo che se $n = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r}$, con i p_i primi distinti, allora

$$\varphi(n) = \varphi(p_1^{t_1}) \cdots \varphi(p_r^{t_r}) = (p_1^{t_1} - p_1^{t_1-1}) \cdots (p_r^{t_r} - p_r^{t_r-1}) .$$

Chiediamoci allora per quali valori di p e di k $p^k - p^{k-1}$ è una potenza di 2. Se $p = 2$, $p^k - p^{k-1}$ è una potenza di 2 per ogni k . Se $p \neq 2$, allora $p^k - p^{k-1}$ è una potenza di 2 se e solo se $k = 1$ e $p - 1 = 2^t$ per qualche $t \in \mathbb{N}$. Quindi (cfr. §2.9) il numero primo p deve essere un *primo di Fermat* cioè della forma $p = 2^{2^h} + 1$. Possiamo concludere con il seguente teorema.

7.5.3 TEOREMA. *Sia $n \in \mathbb{N}$, $n > 2$. Un n -gono regolare è costruibile se e solo se i primi dispari che compaiono nella sua fattorizzazione sono primi di Fermat distinti, ossia la fattorizzazione di n è del tipo*

$$n = 2^k p_1 p_2 \cdots p_s$$

dove i p_1, p_2, \dots, p_s sono primi di Fermat distinti.

A tutt'oggi si conoscono solo cinque primi di Fermat (quelli corrispondenti ai valori $h = 0, 1, 2, 3, 4$). La situazione per la costruibilità degli n -goni regolari

per i primi valori di n è quindi la seguente:

NUMERO DI LATI	COSTRUIBILE
$\boxed{3} = 2 + 1$	sì
$4 = 2^2$	sì
$\boxed{5} = 2^2 + 1$	sì
$6 = 2 \cdot 3$	sì
7	no
$8 = 2^3$	sì
$9 = 3 \cdot 3$	no
$10 = 2 \cdot 5$	sì
11	no
$12 = 2^2 \cdot 3$	sì
13	no
$14 = 2 \cdot 7$	no
$15 = 3 \cdot 5$	sì
$16 = 2^4$	sì
$\boxed{17}$	sì
$18 = 2 \cdot 3^2$	no
19	no
$20 = 2^2 \cdot 5$	sì
$21 = 3 \cdot 7$	no
$22 = 2 \cdot 11$	no
23	no
$24 = 2^3 \cdot 3$	sì
$25 = 5^2$	no.

I numeri inquadrati sono primi di Fermat.

ESERCIZI.

1. Si disegni effettivamente con riga e compasso un pentagono regolare. (Si consiglia di utilizzare l'esercizio 7.3.9. per avere un'espressione esplicita di ζ_5 , radice quinta primitiva dell'unità.)

ESERCIZI DI PROGRAMMAZIONE.

1. Si scriva un programma che listi gli n per i quali l' n -gono regolare è costruibile.



CONTROLLO.

1. Se ζ è una radice n -esima dell'unità tale che $[\mathbb{Q}(\zeta), \mathbb{Q}] = 5$ si può costruire l' n -gono regolare? E se $[\mathbb{Q}(\zeta), \mathbb{Q}] = 8$? Ripercorrere la dimostrazione del teorema 7.5.1 in questo caso.

7.6. Calcolo esplicito di alcuni gruppi di Galois

In questo paragrafo finale accenneremo al problema del calcolo esplicito del gruppo di Galois di un polinomio. Sembra che una domanda a cui abbiamo già dato una risposta, dato che negli esercizi dei paragrafi passati abbiamo spesso chiesto di calcolare il gruppo di Galois di un dato polinomio. Ma c'era un inganno: di tutti i polinomi dei quali si chiedeva di trovare il gruppo, si conoscevano le radici. Il problema che ci poniamo è il seguente: trovare un algoritmo per il calcolo in linea di principio del gruppo di Galois di un qualunque polinomio (del quale non si conoscano le radici). Un tale algoritmo esiste, ma è difficilmente utilizzabile, perché i calcoli che intervengono sono mostruosi, anche per polinomi di grado basso. Tuttavia ha il vantaggio, rispetto ad altri algoritmi più efficienti, di potere essere presentato con il bagaglio algebrico svolto finora. Noi non lo presenteremo qui, ma suggeriamo di vederlo ad esempio in [36] o [46].

Noi ci accontenteremo intanto di studiare il gruppo di Galois di un'equazione cubica generale di terzo grado a coefficienti razionali. Sia

$$f(x) = x^3 - s_1x^2 + s_2x - s_3$$

un polinomio di terzo grado a coefficienti in \mathbb{Q} . Sappiamo che i coefficienti s_i sono le funzioni simmetriche elementari nelle radici (incognite) $\alpha_1, \alpha_2, \alpha_3$ di $f(x)$. Se $f(x)$ è riducibile, allora il suo gruppo di Galois è il gruppo identico o \mathbb{Z}_2 a seconda che abbia tutte le radici razionali o una sola. Supponiamo quindi che $f(x)$ sia irriducibile su \mathbb{Q} . Sia $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ il suo campo di spezzamento. Il gruppo di Galois $G(K, \mathbb{Q})$ opera transitivamente sulle radici di un polinomio irriducibile, quindi è un sottogruppo transitivo di S_3 : non può che essere A_3 o tutto S_3 . La seguente proposizione caratterizza i polinomi di terzo grado irriducibili su \mathbb{Q} il cui gruppo di Galois è A_3 .

7.6.1 PROPOSIZIONE. *Sia $f(x)$ un polinomio irriducibile di terzo grado a coefficienti razionali. Allora il suo gruppo di Galois è il sottogruppo alterno A_3 se $\Delta = s_1^2s_2^2 + 18s_1s_2s_3 - 27s_3^2 - 4s_1^3s_3 - 4s_2^3$ è un quadrato perfetto in \mathbb{Q} , è tutto S_3 altrimenti.*

Dimostrazione. Per il teorema di corrispondenza di Galois il campo fissato dal sottogruppo alterno A_3 , K_{A_3} , coincide con \mathbb{Q} se e solo se $G(K, \mathbb{Q}) = A_3$. Dato che A_3 contiene i due 3-cicli $(1, 2, 3)$ e $(1, 3, 2)$, tutte le espressioni in $\alpha_1, \alpha_2, \alpha_3$ che vengono lasciate fisse dai due 3-cicli devono stare in \mathbb{Q} . Due

tali espressioni sono ad esempio le seguenti: $h = \alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1$ e $k = \alpha_1^2\alpha_3 + \alpha_2^2\alpha_1 + \alpha_3^2\alpha_2$. Non è difficile provare che $K_{A_3} = \mathbb{Q}(h, k)$. Quindi $G(K, \mathbb{Q}) = A_3$ se e solo se h e k sono razionali. Tenendo conto delle relazioni tra i coefficienti s_i e le radici α_j , si trova (si facciano i conti) che $h + k = s_1s_2 - 3s_3$, mentre $hk = s_1^3s_3 - 9s_3^2 - 6s_1s_2s_3 + s_2^3$. Quindi h e k sono radici dell'equazione di secondo grado $x^2 + ax + b$ dove $a = -s_1s_2 + 3s_3$ e $b = s_1^3s_3 + 9s_3^2 - 6s_1s_2s_3 + s_2^3$; h e k saranno razionali se e solo se $\sqrt{a^2 - 4ac} \in \mathbb{Q}$, ossia se e solo se $a^2 - 4b$ è un quadrato perfetto in \mathbb{Q} . La proposizione è conclusa. \square

Vale la pena di dimostrare anche la seguente proposizione più generale.

7.6.2 PROPOSIZIONE. *Sia F un campo di caratteristica zero, sia $f(x) \in F[x]$ e siano $\alpha_1, \alpha_2, \dots, \alpha_n$ i suoi zeri nel campo di spezzamento K . Posto $\delta = \prod_{i < j} (\alpha_i - \alpha_j)$ e $\Delta(f) = \delta^2$, allora*

- (i) $\Delta(f)$ appartiene a F ;
- (ii) $\Delta(f)$ è un quadrato perfetto in F se e solo se il gruppo di Galois $G(K, F)$ di $f(x)$ è contenuto in A_n .

Dimostrazione. (i) Se $\sigma \in S_n$, $\sigma(\delta) = \pm \delta$ a seconda che σ sia una permutazione pari o una permutazione dispari (si veda la proposizione 5.2.10). Quindi δ sta in K_{A_n} e Δ è lasciato fisso da ogni permutazione di S_n e quindi sta in F .

(ii) Se $\Delta(f)$ è un quadrato perfetto, allora $\delta \in F$, ossia δ è lasciato fisso da $G(K, F)$: ma dato che le permutazioni dispari cambiano δ in $-\delta$, vuol dire che in $G(K, F)$ ci possono stare solo permutazioni pari, cioè $G(K, F) \leq A_n$. Viceversa, sia $G(K, F) \leq A_n$. Allora $\delta \in K_{G(K, F)} = F$, e quindi $\Delta(f)$ è un quadrato perfetto. \square

$\Delta(f)$ prende il nome di *discriminante* del polinomio $f(x)$. Per riconoscere se $G(K, F) \leq A_n$ si deve calcolare $\Delta(f)$: trattandosi di un polinomio simmetrico negli zeri di $f(x)$, in virtù del teorema fondamentale sui polinomi simmetrici è un polinomio nelle funzioni simmetriche elementari delle radici (cioè nei coefficienti del polinomio). Quindi in linea di principio si sa calcolare.

ESERCIZI.

1. Si provi che $\Delta(f) = 0$ se e solo se $f(x)$ ha una radice multipla.

Appendice

In questa appendice forniamo la dimostrazione della *irrazionalità* di e e di π . La dimostrazione della irrazionalità di π è tratta da [Niven]. Per la dimostrazione della *trascendenza* di π (Lindemann, 1882) e di e (Hermite, 1873), si rinvia ad esempio a [24] (per la trascendenza di e) o a [46] (per entrambi).

Cominciamo con la irrazionalità di e , che è semplice.

A.1 IRRAZIONALITÀ DI e . È noto che dalla

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

servendosi delle stime dell'errore nella formula di Taylor, si ricava la seguente relazione

$$(A.1) \quad e = \sum_{k=0}^n \frac{1}{k!} + E_n, \quad \text{dove} \quad \frac{1}{(n+1)!} \leq E_n < \frac{3}{(n+1)!}$$

che ci permette di calcolare e con qualsiasi grado di approssimazione. Riscriviamo la (A.1) nella seguente forma:

$$(A.2) \quad \frac{1}{(n+1)!} \leq e - \sum_{k=0}^n \frac{1}{k!} < \frac{3}{(n+1)!}$$

da cui, moltiplicando tutti i membri di (A.2) per $n!$, si ottiene

$$\frac{1}{n+1} \leq n! e - \underbrace{\sum_{k=0}^n \frac{n!}{k!}}_{\in \mathbb{Z}} < \frac{3}{n+1}.$$

Ora, se $n > 2$, $3/(n+1)$ è $\leq 3/4$. Supponiamo per assurdo che e sia razionale: allora potremmo scegliere un n tale che $n!e$ sia intero. Ma allora $n!e - \sum_{k=0}^n n!/k!$ sarebbe un intero (differenza di due interi) positivo e minore di $3/4$, cosa che è palesemente assurda.

A.2 IRRAZIONALITÀ DI π . Supponiamo per assurdo che π sia razionale, cioè che esistano due interi positivi a e b tali che sia $\pi = a/b$. Consideriamo il seguente polinomio:

$$f(x) = \frac{x^n(a-bx)^n}{n!}.$$

L'intero n è per il momento arbitrario, e solo alla fine verrà scelto in modo opportuno. Il polinomio $n!f(x)$ ha grado $2n$, è a coefficienti interi. Espandendo $f(x)$ si ottiene

$$(A.3) \quad f(x) = \frac{a_0x^n + a_1x^{n+1} + \dots + a_nx^{2n}}{n!}$$

con gli a_i (intesti) dati dalle espressioni

$$a_0 = a^n, a_1 = -na^{n-1}b, \dots, a_i = (-1)^i \binom{n}{i} a^{n-i}b^i, \dots, a_n = (-1)^n b^n.$$

Dalla (A.3) risulta che $f^{(i)}(0)$ uguaglia $i!$ moltiplicato per il coefficiente di x^i in (A.3).

Ora, dato che la potenza più bassa di x che compare in $f(x)$ è n , ne segue che per $i < n$ risulta $f^{(i)}(0) = 0$. Per $i \geq n$

$$f^{(i)}(0) = \frac{i!}{n!} a_{i-n}.$$

Dato che $i \geq n$, $i!/n!$ è un intero, ed essendo a_{i-n} intero, si ha che

$f^{(i)}(0)$ è un intero per ogni i .

Inoltre risulta

$$f(x) = f(\pi - x), \quad \text{e} \quad f^{(i)}(x) = (-1)^i f^{(i)}(\pi - x) \quad \forall i.$$

Infatti $f(x) = (b^n/n!)x^n(\pi - x)^n = f(\pi - x)$, e la seconda relazione è conseguenza delle regole di derivazione delle funzioni composte. In particolare,

$$f(0) = f(\pi), \quad f^{(i)}(0) = (-1)^i f^{(i)}(\pi).$$

Quindi anche

$f^{(i)}(\pi)$ è un intero per ogni $i \geq 0$.

Proviamo la seguente proposizione.

A.3 PROPOSIZIONE. *Sia $f(x)$ la funzione sopra definita*

$$f(x) = \frac{x^n(a - bx)^n}{n!}, \quad a, b \in \mathbb{N}.$$

Allora, qualunque sia l'intero positivo n , l'integrale

$$\int_0^\pi f(x) \sin x \, dx$$

è un intero.

Dimostrazione. Definiamo la seguente funzione:

$$F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \cdots + (-1)^n f^{(2n)}(x).$$

Risulta

$$F''(x) = f^{(2)}(x) - f^{(4)}(x) + \cdots + (-1)^n f^{(2n)}(x) = f(x) - F(x).$$

Quindi

$$\begin{aligned} \frac{d}{dx}(F'(x) \sin x - F(x) \cos x) \\ &= F''(x) \sin x + F'(x) \cos x - F'(x) \cos x - F(x) \sin x \\ &= (F''(x) + F(x)) \sin x = f(x) \sin x. \end{aligned}$$

Ne segue che

$$\int_0^\pi f(x) \sin x \, dx = [F'(x) \sin x - F(x) \cos x]_0^\pi = F(\pi) + F(0).$$

Ora, dato che $F(0)$ e $F(\pi)$ sono interi, risulta intero anche $F(0) + F(\pi)$. Ne segue che l'integrale è un intero. \square

Sceglieremo ora un n in modo tale che questa asserzione risulti assurda. Per $0 < x < \pi$ risulta

$$f(x) = \frac{x^n(a - bx)^n}{n!} \leq \frac{\pi^n a^n}{n!}$$

e

$$0 < \sin x \leq 1.$$

Quindi

$$0 < \int_0^\pi f(x) \sin x \, dx < \int_0^\pi \frac{\pi^n a^n}{n!} \, dx = \frac{\pi^{n+1} a^n}{n!}.$$

Ora, $\lim_{n \rightarrow \infty} (\pi^{(n+1)} a^n) / n! = 0$, quindi, scegliendo un n sufficientemente grande, si può fare in modo che sia

$$\frac{\pi^{(n+1)} a^n}{n!} < 1.$$

Ma allora $\int_0^\pi f(x) \sin x dx$ deve essere un intero > 0 e < 1 , che è chiaramente un assurdo. Quindi τ non può essere razionale, ed è pertanto irrazionale.

Tavola dei gruppi dei primi ordini

Ordine	#	Abeliani	#	Non abeliani
1	1	$\{e\}$	0	—
2	1	\mathbb{Z}_2	0	—
3	1	\mathbb{Z}_3	0	—
4	2	\mathbb{Z}_4, V	0	—
5	1	\mathbb{Z}_5	0	—
6	1	$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$	1	$S_3 \cong D_3$
7	1	\mathbb{Z}_7	0	—
8	3	$\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	2	D_4, Q
9	2	$\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$	0	—
10	1	$\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$	1	D_5
11	1	\mathbb{Z}_{11}	0	—
12	2	$\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$	3	$A_4, M, D_6 \cong \mathbb{Z}_2 \times D_3$
13	1	\mathbb{Z}_{13}	0	—
14	1	$\mathbb{Z}_{14} \cong \mathbb{Z}_2 \times \mathbb{Z}_7$	1	D_7
15	1	$\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$	0	—

V = gruppo di Klein

D_n = gruppo diedrale delle simmetrie di un n -gono regolare

$Q = \langle \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \mid i^2 = -1 \rangle$ = gruppo dei quaternioni

$M = \langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} \mid i^2 = -1, \omega \text{ radice terza primitiva dell'unità} \rangle$

A_4 = gruppo alterno

Alfabeto greco

α, A	alfa	η, H	eta	ν, N	nu	τ, T	tau
β, B	beta	$\theta, \vartheta, \Theta$	theta ^(t)	ξ, Ξ	xi	ν, Y	epsilon
γ, Γ	gamma	ι, I	iota	\circ, O	omicron	σ, φ, Φ	phi
δ, Δ	delta	κ, K	cappa	π, Π	pi	χ, X	chi ^(t)
ε, E	epsilon	λ, Λ	lambda	ρ, P	ro	ψ, Ψ	psi
ζ, Z	zeta	μ, M	mi	$\sigma, \varsigma, \Sigma$	sigma	ω, Ω	oméga

^(t) "th" aspirato come in inglese;

⁽ⁱ⁾ "ch" aspirato come in tedesco.

Esercizi riassuntivi

- Provare che un gruppo di ordine 12 non è mai semplice.
- Dire se $\pi^2 - 1$ è algebrico (su \mathbb{Q}). E su $\mathbb{Q}(\pi^3)$? Giustificare le risposte.
- Sia G un gruppo finito. Si determinino tutti gli omomorfismi di G in $(\mathbb{Z}, +)$.
- Sia r un fissato elemento non nullo di \mathbb{R} . Si definisca la seguente relazione in \mathbb{R} :

$$x \varrho y \pmod{r}, \iff x - y = hr, \quad h \in \mathbb{Z}.$$

Si provi che si tratta di una relazione di equivalenza. Si decida (giustificando le risposte), se si tratta di una relazione compatibile rispetto alle operazioni di \mathbb{R} .

- Provare che ogni elemento di un campo finito è somma di due quadrati.
- Sia G un gruppo di ordine 100 e si supponga che esistano in G 50 elementi g_i ($i = 1, \dots, 50$) tutti distinti che non sono generatori, tali cioè che $\langle g_i \rangle \neq G$ per ogni $i = 1, \dots, 50$. Si può concludere che G non è ciclico?
- Sia G un gruppo non abeliano di ordine 24 e sia $g \in G$ tale che $g^{12} \neq e$. Queste condizioni determinano univocamente il periodo di g ?
- Sia G un gruppo e sia g un fissato elemento di G . Quale (o quali) tra le condizioni (a) e (b) implicano che necessariamente G è ciclico?
 - $|G| = 125$ e $o(g) > 40$.
 - $|G| = 120$ e $o(g) > 40$.
- Si provi che ogni p -gruppo finito è risolubile.
- Dare un esempio di gruppo infinito in cui ogni elemento ha periodo finito.
- Si dimostri che esistono al più n^{n^2} gruppi non isomorfi di ordine n .
- Determinare tutti gli omomorfismi di anello di \mathbb{Z} in sé.
- Si determini il campo fissato dall'automorfismo di $\mathbb{Q}(\pi)$ in sé che manda π in $-\pi$.

14. Si provi che il gruppo di Galois di $x^{10} - 1 \in \mathbb{Q}[x]$, su \mathbb{Q} è isomorfo al prodotto diretto dei gruppi di Galois su \mathbb{Q} dei polinomi $x^2 - 1$ e $x^5 - 1$. Si generalizzi al modo seguente: se r ed s sono due interi coprimi, si provi che il gruppo di Galois su \mathbb{Q} di $x^{rs} - 1$ è isomorfo al prodotto diretto del gruppo di Galois di $x^r - 1$ per il gruppo di Galois di $x^s - 1$.
15. Determinare il più piccolo intero n tale che S_n contenga un elemento di ordine 91. E il più piccolo intero n tale che S_n contenga un elemento di ordine 391. Generalizzare.
16. Siano K ed F due campi tali che $F \subseteq K$, e sia $a \in K$. Se $b \in K$ è tale che $b^n = a$, per qualche $n \in \mathbb{N}$, dimostrare che b è algebrico su F se e solo se a è algebrico su F .
17. Un anello si dice booleano se ogni $x \in R$ è tale che $x^2 = x$. Sia R un anello booleano.
- Si provi che è un anello commutativo.
 - Si provi che se R è un dominio d'integrità, allora può contenere al più due elementi.
 - Si provi che ogni ideale primo di R è massimale.
18. Sia K un campo finito di caratteristica p . Si provi che l'applicazione $\sigma_p : K \rightarrow K$ data da $\sigma_p(a) = a^p$ per ogni $a \in K$ è un automorfismo (detto *automorfismo di Frobenius*). Si determini il campo fissato da σ_p .
19. Sia K un'estensione galoisiana di grado 6 di un campo F . Si dimostri che esiste una ed una sola estensione galoisiana L di F di grado 2 su F .
20. Sia $p(x) \in \mathbb{Q}[x]$ e sia K il suo campo di spezzamento. Dimostrare che, se $p(x)$ ha grado 4 e $[K : \mathbb{Q}] > 6$, allora $p(x)$ è irriducibile su \mathbb{Q} .
21. Si determini un campo con 125 elementi.

Soluzioni degli esercizi

Capitolo 1

- 1.1.1 $x \in (A \cup B) \cup C \iff x \in A \cup B \circ x \in C \iff x \in A \circ x \in B \circ x \in C \iff x \in A \circ x \in B \cup C \iff x \in A \cup (B \cup C)$.
- 1.1.2 Dimostrazione analoga al precedente.
- 1.1.3 Se $B \subseteq A$, ovviamente è $A \cup B = A$. Viceversa, supponiamo per assurdo che sia $B \not\subseteq A$. Allora $\exists x \in B, x \notin A$. Allora $A \cup B \supset A$.
- 1.1.4 $x \in (A \cup B) \cap C \iff x \in A \cup B \circ x \in C \iff (x \in A \circ x \in B) \circ x \in C \iff (x \in A \circ x \in C) \circ (x \in B \circ x \in C) \iff x \in (A \cap C) \cup (B \cap C)$.
- 1.1.5 $x \in \complement(A \cap B) \iff x \notin A \cap B \iff x \notin A \circ x \notin B \iff x \in \complement A \circ x \in \complement B \iff x \in \complement(A \cup B)$.
- 1.2.1 (a) $a \equiv b \forall a$ perché $a - a = 0$ è un multiplo di n qualunque sia n .
 (b) $a \equiv b \pmod{n} \iff a - b = hn, h \in \mathbb{Z}, \iff b - a = -(a - b) = -(hn) = (-h)n \iff b \equiv a \pmod{n}$.
 (c) $a \equiv b \pmod{n} \iff a - b = hn, h \in \mathbb{Z}, b \equiv c \pmod{n} \iff b - c = kn, k \in \mathbb{Z}$, quindi $a - c = (a - b) + (b - c) = hn + kn = (h + k)n$, da cui $a \equiv c \pmod{n}$.

Le classi di equivalenza sono

$$\bar{0} = \{\text{intesi che divisi per } n \text{ danno per resto } 0\} = \{kn \mid k \in \mathbb{Z}\}$$

$$\bar{1} = \{\text{intesi che divisi per } n \text{ danno per resto } 1\} = \{kn + 1 \mid k \in \mathbb{Z}\}$$

...

$$\overline{n-1} = \{\text{intesi che divisi per } n \text{ danno per resto } n-1\} = \{kn + n - 1 \mid k \in \mathbb{Z}\}.$$

Nel caso $n = 5$ sono in numero di 5, e sono $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ e $\bar{4}$.

- 1.2.2 (a) R ed S ma non T: $A = \{a, b, c\}, \varrho = \{(a, a), (b, b), (c, c), (a, b), (b, a), (b, c), (c, b)\}$.
 (b) R e T ma non S: $A = \{a, b, c\}, \varrho = \{(a, a), (b, b), (c, c), (a, b)\}$, oppure una relazione d'ordine.

- (c) S e T ma non R: Sia A l'insieme degli studenti che si sono prenotati per la sessione estiva dell'esame di algebra. Definiamo su A la seguente relazione di equivalenza R : $a R b \iff$ sono soddisfatte le seguenti due condizioni: a e b si sono presentati all'esame e hanno preso lo stesso voto. La R è chiaramente simmetrica e transitiva, ma non è necessariamente riflessiva (può esserci uno studente $a \in A$ che non si è presentato all'esame, quindi a non è in relazione con se stesso).
- 1.2.3 Si tratta della relazione di *essere divisore*. È riflessiva, perché $a | a \forall a \in \mathbb{N}$. È transitiva (ovvio), e antisimmetrica, perché le $a | b$ e $b | a$ implicano rispettivamente $b = ah$ e $a = bk$, $h, k \in \mathbb{N}$. Quindi $a = ahk$ e, per la cancellazione, $hk = 1$ che in \mathbb{N} implica $h = k = 1$ e quindi $a = b$. In \mathbb{Z} invece $hk = 1$ implica che $h = \pm 1$ quindi $a = \pm b$. In \mathbb{Z} la relazione pur essendo riflessiva e transitiva, non è antisimmetrica, e quindi non è una relazione d'ordine.
- 1.3.1 Da A a B sono 8: nessuna iniettiva, 6 suriettive. Da B ad A sono 9: 6 iniettivo, nessuna suriettiva.
- 1.3.2 Dobbiamo provare che $(g \circ f)(a) = (g \circ f)(a')$ implica $a = a'$. $(g \circ f)(a) = g(f(a)) = g(f(a'))$. Essendo g iniettiva risulta $f(a) = f(a')$; essendo f iniettiva segue $a = a'$.
- 1.3.3 Si tratta di provare che $\forall x \in A$ $(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$. Infatti, $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$ e $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$.
- 1.3.4 (a), (b), (d), (e), (f).
- 1.3.5 (a) $\text{Im} = \mathbb{Z}$, iniettiva, suriettiva.
 (b) $\text{Im} = 3$, né iniettiva, né suriettiva.
 (d) $\text{Im} = \mathbb{N}$, né iniettiva, né suriettiva.
 (e) $\text{Im} = \mathbb{Z}$, iniettiva e suriettiva.
 (f) $\text{Im} = \mathbb{N}$, né iniettiva, né suriettiva.
- 1.3.6 Se $f : A \rightarrow B$ ammette inverso sinistro $g : B \rightarrow A$, ossia $g \circ f = \text{id}_A$, allora $f(a_1) = f(a_2)$ implica $gf(a_1) = gf(a_2)$ da cui $a = b \implies f$ è iniettiva. Viceversa, se f è iniettiva, si può definire una $g : B \rightarrow A$ al modo seguente: $g(b) = a$ (dove a è quell'unico elemento (per l'iniettività) di A tale che $f(a) = b$) se b appartiene all'immagine di f , altrimenti $g(b) = a_0$, dove a_0 è un *qualunque* fissato elemento di A . Si tratta effettivamente di un'applicazione, tale che $g \circ f = \text{id}_A$.
 Se f ammette un inverso destro g , allora la $f \circ g = \text{id}_B$ implica che, per ogni $b \in B$, $b = f(g(b))$, ossia ogni $b \in B$ è l'immagine di qualcosa mediante la f , cioè f è suriettiva. Viceversa, se f è suriettiva, dato comunque $b \in B$, esiste almeno un a tale che $f(a) = b$. Definiamo una g ponendo $g(b) = a$, dove a è un elemento tale che $f(a) = b$. Risulta $(f \circ g)(b) = f(g(b)) = f(a) = b$ per ogni $b \in B$, quindi $f \circ g = \text{id}_B$.
- 1.3.7 Si tratta di un'applicazione suriettiva, ma non iniettiva. In base all'esercizio precedente esisterà solo un inverso destro. Per determinare una $g : \mathbb{R}^+ \rightarrow \mathbb{C}$ tale che $f \circ g = \text{id}_{\mathbb{R}^+}$, basta porre per ogni $r > 0$ $g(r) = \sqrt{r}$. Si ha $f(g(r)) = f(\sqrt{r}) = r$ per ogni $r \in \mathbb{R}^+$.

- 1.3.8 (a) $a \in f(X \cup Y) \iff a \in f(X) \circ a \in f(Y) \iff [x = f(x) \text{ per qualche } x \in X \circ a = f(y) \text{ per qualche } y \in Y] \iff a = f(t) \text{ per qualche } t \in X \cup Y \iff a \in f(X \cup Y)$.
- (b) $a \in f(X \cap Y) \implies a = f(c) \text{ per qualche } c \in X \cap Y$. Quindi $a \in f(X)$ e $a \in f(Y)$, cioè $a \in f(X) \cap f(Y)$. L'altra inclusione non vale sempre. Ad esempio, sia $f(x) = \sin x : \mathbb{R} \rightarrow \mathbb{R}$. Sia $X = [0, \pi/2]$, $Y = [\pi/2, \pi]$. Risulta $f(X \cap Y) = f(\pi/2) = 1$. Dato che $f(X) = f(Y) = [0, 1]$ si ha $f(X) \cap f(Y) = [0, 1] \supset f(X \cap Y)$. L'uguaglianza $f(X \cap Y) = f(X) \cap f(Y)$ vale se e solo se f è iniettiva.
- (c) $a \in f^{-1}(X' \cup Y') \iff f(a) \in X' \cup Y' \iff [f(a) \in X' \circ f(a) \in Y'] \iff [a \in f^{-1}(X') \circ a \in f^{-1}(Y')] \iff a \in f^{-1}(X') \cup f^{-1}(Y')$.
- (d) Analoga.
- 1.4.2 Per induzione su n . Per $n = 0$ si ha $1 = 1$, quindi la base dell'induzione è vera. Supponendo vera la $\sum_{k=0}^{n-1} (4k+1) = (2(n-1)+1)n$, dimostriamola per n . $\sum_{k=0}^n (4k+1) = \sum_{k=0}^{n-1} (4k+1) + 4n+1 = 2n^2 + 3n + 1 = (2n+1)(n+1)$.
- 1.4.3 Per $n = 1$ è vera. Supponiamo vera la $1^2 + 2^2 + 3^2 + \dots + (n-1)^2 = ((n-1)n(2(n-1)+1))/6$ e dimostriamola per n . $1^2 + 2^2 + 3^2 + \dots + n^2 = ((n-1)n(2(n-1)+1))/6 + n^2 = (n(n+1)(2n+1))/6$.
- 1.4.4 Per induzione su $n = |X|$. Se $n = 1$, il numero di sottoinsiemi di X è 2, quindi la formula vale. Supponiamo vero che ogni insieme X con $n-1$ elementi abbia 2^{n-1} sottoinsiemi e dimostriamolo se $|X| = n$. Fissiamo un elemento $x \in X$. L'insieme $X \setminus \{x\}$ possiede $n-1$ elementi, e quindi possiede 2^{n-1} sottoinsiemi. Per ottenere i sottoinsiemi di X si devono aggiungere a questi 2^{n-1} sottoinsiemi quegli altri 2^{n-1} che si ottengono da quelli aggiungendo l'elemento x . In tutto si hanno allora $2^{n-1} + 2^{n-1} = 2^n$ sottoinsiemi.
- 1.4.5 È falsa per $n = 2$. In questo caso infatti l'intersezione dei due insiemi con $n-1$ elementi è vuota.
- 1.4.7 Per induzione sul numero n di tutte le rette. Se $n = 1$ è ovvio che bastano due colori. Supponiamo quindi di avere provato che è possibile colorare con solo due colori le regioni formate da meno di n rette, e dimostriamolo nel caso in cui si aggiunga la n -esima retta, r . Dividiamo le regioni in due gruppi, a seconda del lato in cui si trovano rispetto alla r . Basta allora lasciare invariata la colorazione di tutte le regioni che si trovano da una delle due parti e scambiare invece il colore di quelle che si trovano dall'altra parte. Dobbiamo verificare che si tratta di una "buona" colorazione: infatti, se due regioni confinanti si trovano dalla stessa parte della r , avranno colorazioni diverse (avevamo colorazioni diverse prima dell'aggiunzione della r , e ora o manterranno i loro colori, o questi saranno invertiti, ma comunque saranno diversi). Se le due regioni si trovano da lati opposti rispetto alla r i loro colori saranno diversi, perché il colore di una delle due è stato invertito.
- 1.4.9 Osserviamo che il numero m_n di mosse necessarie per trasferire n dischi uguaglia il doppio del numero m_{n-1} di mosse necessarie per trasferire $n-1$ dischi più una mossa. Infatti con m_{n-1} mosse si trasferiscono sull'asticella di mezzo gli $n-1$ dischi che si trovano sopra l' n -esimo (il più largo). Poi si muove il disco più largo sulla terza asticella, e infine si fanno altre m_{n-1} mosse per

trasferire sulla terza asticella gli $n - 1$ dischi. Quindi la relazione ricorsiva è $m_0 = 0$, $m_n = 2m_{n-1} + 1$.

Per esprimere m_n in funzione di n , dai primi casi sembra di poter dire che $m_n = 2^n - 1$: questa non è una dimostrazione. È un modo per cercare di indovinare la formula, da dimostrare poi per induzione. Procediamo allora per induzione su n . Per $n = 0$ $m_0 = 2^0 - 1 = 0$, che è la base dell'induzione. Supponiamo vera la $m_{n-1} = 2^{n-1} - 1$ e dimostriamola per n : $m_n = 2m_{n-1} + 1 = 2 \cdot (2^{n-1} - 1) + 1 = 2^n - 1$.

- 1.4.10 Si consideri per ogni x, y il sottoinsieme $\{x, y\}$. In quanto sottoinsieme non vuoto, esso avrà un elemento minimo. Si concluda.

- 1.5.1 Sia $A = \{a_1, a_2, \dots, a_i, \dots\}$ un insieme numerabile e sia X un suo sottoinsieme. Se $X = \emptyset$, X è finito, e il risultato è vero. Sia $X \neq \emptyset$ e sia i_1 il più piccolo intero positivo tale che $a_{i_1} \in X$. Sia poi i_2 il più piccolo intero positivo, con $i_2 > i_1$ tale che $a_{i_2} \in X$, e così via. Allora $X = \{a_{i_1}, a_{i_2}, \dots\}$. Se il sottoinsieme $\{i_1, i_2, \dots\}$ di \mathbb{N} è limitato, allora X è finito, altrimenti esso è numerabile.

- 1.5.2 Basta osservare che \mathbb{N} contiene gli interi pari, che sono in corrispondenza biunivoca con \mathbb{N} (tramite la $f(n) = 2n$).

- 1.5.3 Sia X l'insieme finito e sia X' un insieme che lo contenga propriamente. Procederemo per induzione sulla cardinalità n di X . Se $n = 1$, X contiene un solo elemento x_1 . Sia f una qualunque applicazione iniettiva di X in X' . Se $f(x_1) = x_1$, allora ogni elemento $x' \in X'$ diverso da x_1 (e un tale elemento esiste perché X' contiene propriamente X) non è immagine di nessun elemento di X e quindi la f non può essere biunivoca. Se $f(x_1) = x' \neq x_1$, allora è x_1 a non essere immagine di nessun elemento di X . Ancora, la f non può essere biunivoca. La base dell'induzione è provata. Supponiamo ora di avere dimostrato il teorema per ogni insieme con $n - 1$ elementi e dimostriamolo nel caso di insiemi con n elementi. Sia $X = \{x_1, x_2, \dots, x_n\}$ e supponiamo che esista una corrispondenza biunivoca f tra X e X' (che contiene X). Sia x_{n+1} un elemento (sicuramente esistente) in $X' \setminus X$. Sia $f(x_n) = x'$. Essendo f biunivoca, esisterà un $x_i \in X$ tale che $f(x_i) = x_{n+1}$. Se $x' \neq x_{n+1}$ possiamo sempre definire una nuova corrispondenza f' (ancora biunivoca) da X a X' così definita: $f'(x_j) = f(x_j)$ per ogni $j \neq i, n$, $f'(x_i) = x'$, $f'(x_n) = x_{n+1}$. Non è quindi restrittivo supporre che la corrispondenza f che stiamo supponendo biunivoca mandi x_n in x_{n+1} . Ma allora avremmo trovato una corrispondenza biunivoca tra $X \setminus \{x_n\}$ e $X' \setminus \{x_{n+1}\}$, il che è assurdo, perché $X \setminus \{x_n\}$ è finito e contenuto propriamente in $X' \setminus \{x_{n+1}\}$.

- 1.5.4 Se X è finito non può, per quanto visto al punto precedente, avere la stessa potenza di una sua parte propria. Ciò significa che se X ha la stessa potenza di una sua parte propria, allora X è necessariamente infinito. Resta da provare che ogni insieme infinito possiede un sottoinsieme proprio che ha la sua stessa potenza. Infatti ogni insieme infinito X possiede certamente un sottoinsieme numerabile, sia esso S . Si noti che in questa asserzione si fa uso dell'assioma della scelta. L'insieme $X' = X \setminus S$ è tale che $X = S \cup X'$ e $X' \cap S = \emptyset$. Ora, S contiene, per quanto visto nell'esercizio 1.5.1, un sottoinsieme proprio numerabile S' . L'insieme $X' \cup S'$ è una parte propria di X ed è equipotente a

X . Detta infatti φ una corrispondenza biunivoca (sicuramente esistente) tra i due insiemi numerabili S e S' , definiamo una f tra $X = S \cup X'$ e $S' \cup X'$ al modo seguente:

$$f(x) = \begin{cases} x & \text{se } x \in X' \\ \varphi(x) & \text{se } x \in S. \end{cases}$$

Tale corrispondenza è ovviamente biunivoca.

- 1.5.5 Dimostriamo solo (b). Dato $r \in \mathbb{R}$, la sua classe di equivalenza è data da $[r] = \{x \in \mathbb{R} : x = r + q, q \in \mathbb{Q}\} = r + \mathbb{Q}$. In particolare, se $r \in \mathbb{Q}$ la sua classe di equivalenza è \mathbb{Q} . Tutte le classi di equivalenza hanno la stessa cardinalità, che è la cardinalità del numerabile, perché sono tutte equipotenti alla classe \mathbb{Q} . Se l'insieme \mathbb{R}/ϱ fosse numerabile, \mathbb{R} sarebbe numerabile anch'esso, come unione di una infinità numerabile di insiemi numerabili (le sue classi).
- 1.6.1 Sono in numero di m^n (per ogni elemento a di A ci sono m scelte per la sua immagine, quindi ...).
- 1.6.2 $n!$. Le iniettive sono anche suriettive in questo caso.
- 1.6.3 $m(m-1)(m-2)\cdots(m-n+1)$.
- 1.6.4 Si parta dall'identità $(n+1)/(k(n-k+1)) = 1/k + 1/(n-k+1)$. Moltiplicando ambo i membri per $n!/(k-1)!(n-k)!$ si ottiene

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

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

Capitolo 2

- 2.1.1 (a) $(n, m) \varrho (n, m)$ perché $n+m = m+n$ ($+$ è commutativa).
 (b) $(n, m) \varrho (n', m') \Rightarrow (n', m') \varrho (n, m)$. Infatti $(n, m) \varrho (n', m') \Leftrightarrow n+m = m+n' \Leftrightarrow n'+m = m'+n \Leftrightarrow (n', m') \varrho (n, m)$.
 (c) $(n, m) \varrho (p, q) \Leftrightarrow n+q = m+p$, $(p, q) \varrho (r, s) \Leftrightarrow p+s = q+r$. Sommando membro a membro si ottiene $n+q+p+s = m+p+q+r$ da cui per semplificazione (e sfruttando la commutatività dell'addizione) $n+s = m+r$ ossia $(n, m) \varrho (r, s)$.
- 2.1.3 $ac = bc$, $c \neq 0 \Rightarrow (a-b)c = 0$. Essendo \mathbb{Z} privo di divisori dello zero, si ha $a-b=0$, ossia $a=b$.
- 2.1.4 Per induzione su n . Per $n=2$ si tratta della definizione di elemento primo. Supponiamo vero che se p divide un prodotto di $n-1$ fattori, allora divide almeno uno dei fattori. Sia $p \mid a_1 a_2 \cdots a_n$: allora $p \mid a_1 (a_2 \cdots a_n)$. Ma allora $p \mid a_1$ o $p \mid a_2 \cdots a_n$. Per l'ipotesi induttiva p dividerà almeno uno dei fattori.
- 2.2.1 Sia (\bar{x}, \bar{y}) una soluzione intera della (1) $ax + by = c$, $a, b, c \in \mathbb{Z}$. Sia (x_0, y_0) una soluzione di $ax + by = 0$, tale cioè che $ax_0 + by_0 = 0$. Allora $(\bar{x} + x_0, \bar{y} + y_0)$ è soluzione della (1). Infatti

$$a(\bar{x} + x_0) + b(\bar{y} + y_0) = \underbrace{a\bar{x} + b\bar{y}}_{=c} + \underbrace{ax_0 + by_0}_{=0} = c.$$

Viceversa, siano (\bar{x}, \bar{y}) e (x', y') due soluzioni della (1). Allora

$$a(\bar{x} - x') + b(\bar{y} - y') = a\bar{x} + b\bar{y} - ax' - by' = c - c = 0,$$

cioè (x', y') differisce da (\bar{x}, \bar{y}) per una soluzione dell'equazione omogenea. Indicato con d il MCD(a, b), siano a', b', c' tali che $a = da'$, $b = db'$, $c = dc'$. Allora la (1) si può semplificare nella $a'x + b'y = c'$. Ora, le soluzioni (x_0, y_0) della $a'x + b'y = 0$ sono $x_0 = -b't$, $y_0 = a't$, $t \in \mathbb{Z}$. Quindi in definitiva tutte e sole le soluzioni della (1) sono del tipo (x', y') , dove $x' = \bar{x} - \frac{b}{d}t$, $y' = \bar{y} + \frac{a}{d}t$ al variare di $t \in \mathbb{Z}$.

- 2.3.1 Se fosse $\sqrt{p} = a/b$, $a, b \in \mathbb{Z}$ e primi fra loro, sarebbe $b^2p = a^2$. Ora, il fattore irriducibile p a sinistra compare un numero dispari di volte, mentre a destra un numero pari di volte. Questo contraddice il teorema fondamentale dell'aritmetica.
- 2.5.1 Supponiamo per assurdo che esista un $d > 1$ che divide F_n e F_{n+1} . Allora dividerà anche $F_{n-1} = F_{n+1} - F_n$. Continuando all'indietro, d dovrà dividere $F_2 = 1$, il che è assurdo.
- 2.5.2 Per quanto dimostrato nell'esercizio precedente, gli unici valori sono $n = 1, 2$.
- 2.5.3 Pensato fissato k , procediamo per induzione su n . Per $n = 1$ la relazione diventa $F_{k+1} = F_kF_2 + F_{k-1}F_1 = F_k + F_{k-1}$, che è vera. Supponiamo quindi vera la formula vera per ogni $0 \leq m < n$ e dimostriamola per n . Per l'induzione ammessa, saranno vere le seguenti due relazioni:

$$F_{n-1+k} = F_kF_n + F_{k-1}F_{n-1} \quad \text{e} \quad F_{n-2+k} = F_kF_{n-1} + F_{k-1}F_{n-2}.$$

Sommendo membro a membro, si ottiene

$$\begin{aligned} \underbrace{F_{n-1+k} + F_{n-2+k}}_{=F_{n+k}} &= F_k(F_n + F_{n-1}) + F_{k-1}(F_{n-1} + F_{n-2}) \\ &= F_kF_{n+1} + F_{k-1}F_n. \end{aligned}$$

Per provare che F_{kn} è multiplo di F_n , procederemo per induzione su k . Per $k = 1$ è ovvia. Supponiamo vero che F_{hm} sia multiplo di F_n per ogni $m \leq k$ e dimostriamolo per $k + 1$. La relazione precedente ci garantisce allora il risultato, perché

$$F_{(k+1)n} = F_{kn+n} = F_nF_{kn+1} + F_{n-1}F_{kn}.$$

Ora, per l'induzione ammessa, sia F_n , sia F_{kn} sono multipli di F_n , quindi lo sarà anche $F_{(k+1)n}$.

- 2.5.4 Dimostriamo innanzitutto che, se $m = nq + r$, allora $\text{MCD}(F_m, F_n) = \text{MCD}(F_n, F_r)$. Si ha la seguente serie di uguaglianze: $\text{MCD}(F_m, F_n) = \text{MCD}(F_{nq+r}, F_n) =$ (per la relazione dimostrata nell'esercizio 2.5.3) $= \text{MCD}(F_rF_{nq-1} + F_{r+1}F_{nq}, F_n)$. Ora, F_{nq} è un multiplo di F_n , quindi $\text{MCD}(F_rF_{nq-1} + F_{r+1}F_{nq}, F_n) = \text{MCD}(F_rF_{nq-1}, F_n)$. Se dimostriamo che $(F_{nq-1}, F_n) = 1$, allora si può concludere che $\text{MCD}(F_rF_{nq-1}, F_n) = \text{MCD}(F_r, F_n)$ che è quanto volevamo provare. Sta $\text{MCD}(F_{nq-1}, F_n) = d$: allora $d \mid F_n$ (e quindi anche F_{nq}) e F_{nq-1} . In quanto divisore di due numeri di Fibonacci successivi, deve essere $d = 1$.

Con questo risultato a disposizione, il fatto che $\text{MCD}(F_n, F_m) = F_d$, con $d = \text{MCD}(n, m)$, è immediato. Infatti, operando l'algoritmo euclideo partendo da m e n , e indicando con r_t l'ultimo resto non nullo (che è quindi il $\text{MCD}(m, n)$), si avrà

$$\text{MCD}(F_m, F_n) = \text{MCD}(F_{r_1}, F_n) = \cdots = \text{MCD}(F_{r_{t-1}}, F_{r_t}) = F_{r_t}.$$

L'ultima uguaglianza valendo perché dato che r_t divide r_{t-1} , allora (per quanto visto) F_{r_t} divide $F_{r_{t-1}}$.

- 2.5.5 Si è già provato che, se $n \mid m$, allora $F_n \mid F_m$. Dobbiamo dimostrare il viceversa, ossia $F_n \mid F_m \implies n \mid m$. $F_n \mid F_m \implies \text{MCD}(F_n, F_m) = F_n$. Ma per quanto ora dimostrato, $\text{MCD}(F_n, F_m) = F_d$, con $d = \text{MCD}(n, m)$. Allora $d = n$, e se $\text{MCD}(n, m) = n$, significa che $n \mid m$.

- 2.5.6 Per induzione su n . Per $n = 1$ il risultato è ovvio. Supponiamo vero il risultato per ogni intero $< n$ e dimostriamolo per n . Se n è un numero di Fibonacci, il risultato è vero. Sia quindi $F_k < n < F_{k+1}$. Allora $0 < n - F_k < F_{k+1} - F_k = F_{k-1}$. Per l'ipotesi induttiva $n - F_k$ è una somma di numeri di Fibonacci distinti, $n - F_k = F_{k_1} + F_{k_2} + \cdots + F_{k_r}$, $k_1 > k_2 > \cdots > k_r$. Le $0 < n - F_k < F_{k-1}$ comportano $k_1 < k$, da cui $n = F_k + F_{k_1} + F_{k_2} + \cdots + F_{k_r}$ è una somma di numeri di Fibonacci distinti.

- 2.5.7 Per $n = 1$ $F_1 \geq ((1 + \sqrt{5})/2)^{-1}$ è vera. Posto $\alpha = (1 + \sqrt{5})/2$, supponiamo vera la $F_m \geq \alpha^{n-2}$ per ogni $m < n$ e dimostriamola per n . Si ha $F_n = F_{n-1} + F_{n-2} \geq \alpha^{n-3} + \alpha^{n-4} = \alpha^{n-4}(\alpha + 1) = \alpha^{n-4}\alpha^2 = \alpha^{n-2}$.

- 2.5.8 Si è visto che per n grandi $F_n \approx (1/\sqrt{5})\alpha^n$, quindi da un certo punto in poi $F_{n+1}/F_n \approx (1 + \sqrt{5})/2$.

- 2.5.9 Basta sommare le seguenti relazioni:

$$F_1 = F_2$$

$$F_3 = F_4 - F_2$$

$$F_5 = F_6 - F_4$$

...

$$F_{2n-1} = F_{2n} - F_{2(n-1)}.$$

- 2.5.10 Per induzione su n . Per $n = 1$ il risultato è vero. Per l'ipotesi induttiva, supponiamo vere le seguenti relazioni:

$$F_n = \sum_{\substack{h+k=n-1 \\ k \leq h}} \binom{h}{k}$$

$$F_{n+1} = \sum_{\substack{h+k=n \\ k \leq h}} \binom{h}{k}.$$

Sommmando, e tenendo conto della relazione $\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$ segue il risultato.

- 2.5.11 Per $k = 0$, $r_0 = 0 = F_0 = 0$, quindi la base dell'induzione è verificata. Supponiamo che la diseguaglianza sia verificata per ogni m tale che sia $0 \leq m < k$ e dimostriamola per k . Dalla

$$r_{n-k} = r_{n-k+1}q_{n-k+2} + r_{n-k+2},$$

essendo per l'ipotesi induttiva $r_{n-k+1} \geq F_{k-1}$, e $r_{n-k+2} \geq F_{k-2}$, ed inoltre essendo $q_{n-k+2} \geq 1$ si ha

$$r_{n-k} \geq F_{k-1} + F_{k-2} = F_k.$$

- 2.5.12 Se a e b ($a \geq b$) sono due interi tali che $D(a, b) \geq n$, significa che l'ultimo resto non nullo è $\geq r_{n-1}$, quindi, in base al risultato dell'esercizio precedente, risulta $r_{n-k} \geq F_k$. In particolare, $b = r_0 \geq F_n$. Dunque, se $b < F_n$, allora certamente deve essere $D(a, b) < n$.

- 2.5.13 Se $n > m$, allora $e_n = e_m(e_1e_2 \cdots \hat{e}_m \cdots e_{n-1}) + 1$ cioè $e_n \equiv 1 \pmod{m}$. Quindi $\text{MCD}(e_n, e_m) = 1$ se $n \neq m$. $D(e_n, e_m) = 2$.

2.6.1 Per n primo.

2.6.2 $57432 \equiv 3 \pmod{9}$. Quindi

$$57432^{1142} = ((57432)^2)^{571} \equiv (3^2)^{571} \equiv 0 \pmod{9}.$$

$89741 \equiv 2 \pmod{3}$. Quindi

$$(89741)^{527} \equiv 2^{527} = ((2^2)^{263} \cdot 2 \equiv 1 \cdot 2 \equiv 2 \pmod{3}).$$

- 2.6.3 $302^{46} \equiv 2^{16} \equiv (2^5)^3 \cdot 2^4 \pmod{100} \equiv 28^3 \cdot 16 \equiv 4 \cdot 16 = 64 \pmod{100}$.

- 2.6.4 Se n è un multiplo di 5 il risultato è vero. Si può allora supporre $(n, 5) = 1$ e servirsi del piccolo teorema di Fermat:

$$n^{17} = (n^4)^4 \cdot n \equiv n \pmod{5}, \quad n^{15} = (n^4)^3 \cdot n^3 \equiv n^3 \pmod{5}.$$

Quindi

$$2n^{17} + 2n^{15} + 3n^3 + 3n \equiv 2n + 2n^3 + 3n^3 + 3n = 5n + 5n^3 \equiv 0 \pmod{5}.$$

- 2.6.5 $4096 = 2^{12}$, quindi $\text{MCD}(4096, \dots, 1) = 1$.

$1296 = 2^4 \cdot 3^4$. Il secondo numero è divisibile per 2 ma non per 4, per 3 ma non per 9. Quindi il MCD è 6.

- 2.6.6 Un qualunque intero, modulo 4, è congruo a 0, 1, 2 o 3. Il suo quadrato è congruo a 0 o 1. La somma di due quadrati sarà quindi congrua modulo 4 a 0, 1 o 2, mai a 3.

- 2.7.1 Vengono date solo le soluzioni fondamentali, cioè comprese tra 0 e il modulo n :

(a) $x = 3$.

(b) La congruenza è equivalente alla $x \equiv 3 \pmod{2}$, che ammette una sola soluzione modulo 2: $x = 1$.

(c) $x = 4$.

(d) Non risolvibile.

- 2.7.2 Una tale congruenza è, ad esempio, $11x \equiv 0 \pmod{319}$, $d = \text{MCD}(11, 319) = 11$. Tutte le soluzioni sono del tipo $x_0 + h(n/d)$, $h \in \mathbb{Z}$. Nel nostro caso $x_0 = 0$, quindi tutte le soluzioni sono $h \cdot 29$, $h \in \mathbb{Z}$. Quelle non congrue modulo 319 sono le 11 soluzioni

$$k \cdot 29, \quad k = 0, \dots, 10.$$

- 2.7.3 $x = 43 + 45k$, $k \in \mathbb{Z}$.

- 2.7.4 $x = 97 + 120h$, $h \in \mathbb{Z}$.

- 2.7.5 Il sistema ammette soluzioni se e solo se il $\text{MCD}(n, m)$ divide $a - b$. Se una soluzione esiste, essa è unica modulo $\text{mcm}(n, m)$.

- 2.7.6 Il problema equivale a risolvere il seguente sistema di congruenze:

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{4} \\ x \equiv 1 \pmod{5} \\ x \equiv 1 \pmod{6} \\ x \equiv 0 \pmod{7}. \end{cases}$$

Soluzione: $x = 301$.

- 2.7.8 $385 = 5 \cdot 7 \cdot 11$. La data congruenza lineare è equivalente (perché?) al seguente sistema:

$$\begin{cases} 4x \equiv 3 \pmod{5} \\ 4x \equiv 3 \pmod{7} \\ 4x \equiv 3 \pmod{11}. \end{cases}$$

- 2.8.1 Fissato un divisore positivo d di n , definiamo il sottoinsieme M_d di \mathbb{N} al modo seguente: $M_d \stackrel{\text{def}}{=} \{m : (m, n) = d\}$. Allora l'insieme degli interi compresi tra 1 ed n viene ripartito in classi, a seconda di quanto vale il loro massimo comune divisore con n . Ora, $(m, n) = d \iff (m/d, n/d) = 1$. Quindi il numero di interi che si trovano nella classe M_d uguaglia il numero di interi $\leq n/d$ e relativamente primi con n/d , cioè $|M_d| = \varphi(n/d)$, cioè $n = \sum_{d|n} \varphi(n/d)$. Quest'ultima somma si può ovviamente scrivere $\sum_{d|n} \varphi(d)$.

- 2.8.2 $9^{\varphi(100)} = 9^{40} \equiv 1 \pmod{100}$. Quindi $9^{201} = (9^{40})^5 \cdot 9 \equiv 9 \pmod{100}$. Per il teorema di Eulero, $3^{40} \equiv 1 \pmod{100}$, quindi $3^{950} = 3^{40 \cdot 23} \cdot 3^{30} = (3^{40})^{23} \cdot (3^5)^6 \equiv 1 \cdot 43^6 \equiv 49^3 \equiv 49 \pmod{100}$.

- 2.8.3 $U(\mathbb{Z}_n) = \{\bar{a} \in \mathbb{Z}_n : (a, n) = 1\}$. Si conclude.

- 2.8.4 Se n non è primo, \mathbb{Z}_n possiede divisori dello zero, e quindi non può essere un campo. D'altra parte, se $n = p$ è primo, ogni elemento di $\mathbb{Z}_p \setminus \{0\}$ è invertibile.

- 2.8.5 $\bar{2}$.

- 2.9.2 (a) $4084223 = 11 \cdot 13^5$.

- (b) $2773 = 59 \cdot 47$ (con la fattorizzazione di Fermat).

(c) 3041 è primo.

(d) $1025^2 - 1044541 = 78^2$, quindi $1044541 = (1025 + 78) \cdot (1025 - 78) = 1103 \cdot 947$. Quest'ultima è la fattorizzazione cercata, essendo i due fattori primi (si verifichi).

(e) In questo caso $k = 41$.

$$k^2 - 1643 = 41^2 - 1643 = 1681 - 1643 = 38 \quad (\text{non quadrato})$$

$$(k+1)^2 - 1643 = 42^2 - 1643 = 1764 - 1643 = 121 = 11^2$$

quindi

$$1643 = 42^2 - 11^2 = (42 - 11)(42 + 11) = 31 \cdot 53.$$

2.9.3 $2^{10} = 1024 \equiv 383 \pmod{641}$, $2^{18} = 2^{10} \cdot 2^6 \equiv 154 \pmod{641}$. Quindi $2^{32} \equiv 640 \equiv -1 \pmod{641}$.

2.9.4 Se di un intero n si conosce la fattorizzazione in irriducibili, sappiamo calcolare φ (cfr. proposizione 2.8.2). Se si sa che n è prodotto di due primi p e q la conoscenza di φ permette di trovare p e q . Basta risolvere le: $p \cdot q = n$ e $(p-1)(q-1) = \varphi(n)$.

2.9.5 $2279 = 43 \cdot 53$.

2.10.3 (i) $n^2 + 2 = (1 \ 1)_b$; $n^2 + 2n = (1 \ (2n-1))_b$;

$$(n^2 + 2)^2 = \begin{cases} (1 \ 2 \ 1)_b & \text{se } b \neq 2 \\ (1 \ 0 \ 0 \ 1)_2 & \text{se } b = 2. \end{cases}$$

(ii) $\alpha^2 = (1 \ 0 \ (n^2 - 1) \ n^2)_b$.

2.11.1 (a) $\sqrt{2}$. (b) 2. (c) 2.

2.11.2 (a) $\cos(\pi/8 + k\pi/2) + i\sin(\pi/8 + k\pi/2)$, $k = 0, 1, 2, 3$.

(b) 1, $(-1 + \sqrt{3}i)/2$, $(-1 - \sqrt{3}i)/2$.

(c) $\frac{1}{2} \pm ((\sqrt{3})/2)i$.

Capitolo 3

3.1.1 $(-1, 1, 0, -2, 0, 0, 1, 0, \dots, 0, \dots)$, $(0, 1, 1, 0, 0, -3, 0, \dots, 0, \dots)$.

3.2.1 Sia \mathbb{K} un campo e siano a e b in \mathbb{K} . Proveremo che se $ab = 0$ e $a \neq 0$, allora necessariamente $b = 0$. Se $a \neq 0$, a ammette inverso, a^{-1} . Moltiplicando ambo i membri della $ab = 0$ per a^{-1} si ha $a^{-1}(ab) = a^{-1} \cdot 0$, da cui $(a^{-1}a)b = 0$, cioè $b = 0$.

3.2.2 $\text{MCD}(x^4 + x - 1, x^4 - 2) = 1$.

$$\text{MCD}(x^5 - x^3 + x^2 - 2x + 1, x^4 + x^3 + 2x^2 + x + 1) = x^2 + 1$$

$$\text{In } \mathbb{Z}_7[x] \text{ MCD}(x^3 + x^2 - 6x + 1, x^4 - 2x^3 - 2x - 1) = x^2 + 1.$$

3.2.3 Una possibile soluzione è $h(x) = 2(-x^2 + 3x + 1)$, $k(x) = 2(x - 3)$.

- 3.2.4 Dire che α è radice di f_i con molteplicità k_i ($i = 1, 2$) significa che $f_i = (x - \alpha)^{k_i} q_i(x)$, con $q_i(\alpha) \neq 0$.

$$\begin{aligned} f_1 f_2 &= (x - \alpha)^{k_1} q_1(x) \cdot (x - \alpha)^{k_2} q_2(x) = (x - \alpha)^{k_1 + k_2} q_1(x) q_2(x) \\ &= (x - \alpha)^{k_1 + k_2} g(x), \quad g(\alpha) \neq 0. \end{aligned}$$

Posto $m = \min(k_1, k_2)$,

$$f_1 + f_2 = (x - \alpha)^m [(x - \alpha)^{k_1 - m} q_1(x) + (x - \alpha)^{k_2 - m} q_2(x)].$$

Ora, il polinomio all'interno della parentesi quadra potrebbe avere radice α se $k_1 = k_2$ (in tal caso $q_1(x) + q_2(x)$ potrebbe avere una radice α). Se però è $k_1 \neq k_2$, allora sicuramente il polinomio dentro la parentesi quadra non ha radice α .

- 3.3.1 Si ha

$$x^5 + 2x^4 - 5x^3 - 10x^2 + 6x + 12 = (x^2 - 3)(x^2 - 2)(x + 2)$$

(fattorizzazione su \mathbb{Q})

$$= (x - \sqrt{3})(x + \sqrt{3})(x - \sqrt{2})(x + \sqrt{2})(x + 2)$$

(fattorizzazione su \mathbb{R} e su \mathbb{C})

$$= x^3(x + 1)^2$$

(fattorizzazione su \mathbb{Z}_2).

- 3.3.2 Trattandosi di un polinomio di grado 3, per ogni a è riducibile sia su \mathbb{C} sia su \mathbb{R} . Qualunque sia a il polinomio è irriducibile su \mathbb{Q} (con il criterio d'Eisenstein, per $p = 5$, qualunque sia $a \in \mathbb{Z}$).

- 3.3.4 È irriducibile su \mathbb{Q} , perché è irriducibile su \mathbb{Z}_3 : è privo di radici su \mathbb{Z}_3 , quindi se si spezza su \mathbb{Z}_3 si spezza in un fattore di secondo grado e un fattore di terzo grado: facendo i conti si vede che ciò non è possibile.

- 3.3.5 Sono tutti irriducibili su \mathbb{Q} perché irriducibili su \mathbb{Z}_3 .

- 3.3.6 Si ha

$$\begin{aligned} x^5 + x^4 + x^3 + x + 1 &= (x^3 + 3x + 2)(x + 4)(x - 2) \\ x^4 + 2x + 3 &= (x^2 + x + 2)(x + 2)^2 \\ x^6 + 4x + 1 &= (x^3 - 3x^2 + 4x + 1)(x^3 + 2x^2 + 1) \\ x^4 - 1 &= (x + 2)(x + 3)(x + 1)(x + 4) \\ x^4 + 1 &= (x^2 + 3)(x^2 + 2). \end{aligned}$$

- 3.4.1 $(\zeta_1 \cdot \zeta_2)^n = \zeta_1^n \zeta_2^n = 1 \cdot 1 = 1$; $1 = (\zeta \zeta^{-1})^n = \zeta^n (\zeta^{-1})^n = 1 \cdot (\zeta^{-1})^n$.

- 3.4.2 Basta definire $f : C_n \rightarrow \mathbb{Z}_n$ al modo seguente: $f(\zeta^k) = [k]$. Controllare i dettagli.

- 3.4.3 Basta prendere $\zeta^{n/d}$. Per ogni d le radici n -esime di ordine d sono $\varphi(d)$.

3.4.4 Si ha

$$\begin{aligned}x^{18}-1 &= \Phi_1\Phi_2\Phi_3\Phi_6\Phi_9\Phi_{18} \\&= (x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^6+x^3+1)(x^5-x^3+1); \\x^{20}-1 &= \Phi_1 \cdot \Phi_2 \cdot \Phi_4 \cdot \Phi_5 \cdot \Phi_{10} \cdot \Phi_{20} \\&= (x-1)(x+1)(x^2+1)(x^4+x^3+x^2+x+1)(x^4-x^3+x^2-x+1) \\&\quad \cdot (x^8-x^6+x^4-x^2+1); \\x^{21}-1 &= \Phi_1 \cdot \Phi_3 \cdot \Phi_7 \cdot \Phi_{21} \\&= (x-1)(x^2+x+1)(x^6+x^5-x^4+x^3+x^2+x+1) \\&\quad \cdot (x^{12}+x^{11}+x^9-x^8+x^6-x^4+x^3-x+1).\end{aligned}$$

- 3.6.2 $x_1^2x_2+x_2^2x_3+x_3^2x_1$ non è simmetrico, perché non è invariante ad esempio rispetto alla permutazione $(1,3)$. Quindi non è esprimibile come polinomio nelle funzioni simmetriche elementari.

$$\begin{aligned}x_1^3+x_2^3+x_3^3+x_2^3+x_3^3+x_1^3 &= \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 + \sigma_1^2 - 2\sigma_2, \\x_1^2+x_2^2+x_3^2 &= \sigma_1^2 - 2\sigma_2, \\x_1^2x_2^2+x_1^2x_3^2+x_2^2x_3^2 &= \sigma_2^2 - 2\sigma_1\sigma_3.\end{aligned}$$

- 3.6.3 Indicate con $\sigma_1, \sigma_2, \sigma_3$ le funzioni simmetriche elementari di $\alpha_1, \alpha_2, \alpha_3$, risulta:

$$\sigma_1 = -3, \quad \sigma_2 = -6, \quad \sigma_3 = -3.$$

Indicate con $\Sigma_1, \Sigma_2, \Sigma_3$ le funzioni simmetriche elementari di $1/\alpha_1^2, 1/\alpha_2^2, 1/\alpha_3^2$, risulta (facendo i conti) $\Sigma_1 = 2, \Sigma_2 = 7/3, \Sigma_3 = 1/9$. Quindi il polinomio monico richiesto è $g(x) = x^3 - 2x^2 + \frac{7}{3}x - \frac{1}{9}$.

- 3.6.6 No, non è simmetrica.

- 3.6.8 Indicando con f^σ un polinomio f con le variabili permutate mediante la permutazione σ , essendo la $\frac{f}{g}$ simmetrica si ha $f/g = f^\sigma/g^\sigma$, cioè $fg^\sigma = gf^\sigma$. Sia ora \bar{f}/\bar{g} una funzione razionale equivalente alla f/g , cioè $f\bar{g} = g\bar{f}$. Dobbiamo provare che $f^\sigma\bar{g}^\sigma = \bar{f}^\sigma$. Dalla $f\bar{g} = g\bar{f}$ segue (permutando le variabili), $f^\sigma\bar{g}^\sigma = g^\sigma\bar{f}^\sigma$. Moltiplicando entrambi i membri per f , si ha

$$ff^\sigma\bar{g}^\sigma = fg^\sigma\bar{f}^\sigma = gf^\sigma\bar{f}^\sigma$$

da cui $fg^\sigma = g\bar{f}^\sigma$.

- 3.6.9 In base al teorema fondamentale sulle funzioni simmetriche, Ψ è un polinomio nelle funzioni simmetriche elementari $\sigma_1, \sigma_2, \dots, \sigma_n$. Se $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$, allora $\sigma_i(\alpha_1, \dots, \alpha_n) = \pm a_i/a_n \in \mathbb{K}$. Quindi $\Psi(\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{K}$.

- 3.6.10 $\Delta(x_1, x_2) = \sigma_1^2 - 4\sigma_2$.
 $\Delta(x_1, x_2, x_3) = \sigma_1^2\sigma_2^2 - 4\sigma_2^3 - 4\sigma_1^3\sigma_3 + 27\sigma_3^2 + 18\sigma_1\sigma_2\sigma_3$.

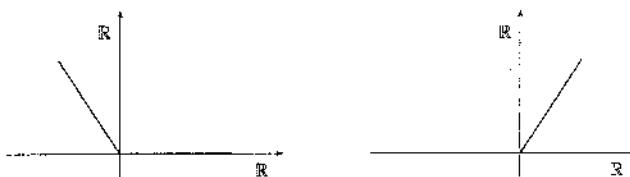
Capitolo 4

- 4.1.1 Siano e ed e' le due unità. Allora $ee' = e'e = e$ (per il fatto che e' è unità). Ma $ee' = e'e = e'$ perché e è unità. Quindi $e = e'$.
- 4.1.2 Si controllino entrambe le proprietà distributive. $\text{End}(A)$ è invece un anello.
- 4.1.3 Basta considerare l'applicazione da $\text{End}(\mathbb{Z})$ in \mathbb{Z} che associa ad ogni $f \in \text{End}(\mathbb{Z})$ l'elemento $f(1) \in \mathbb{Z}$. Si tratta di un isomorfismo.
- 4.1.4 Stessa applicazione del numero precedente.
- 4.1.5 Per ogni $a \in R$ $(a + a)^2 = a - a$, quindi, sviluppando il quadrato, $a^2 + a^2 = a^2 + a^2 = a + a$. Essendo $a^2 = a$ si ha $a + a = 0$, cioè $2a = 0$ per ogni $a \in R$; quindi ogni elemento uguaglia il suo opposto. Dalla $(a + b)^2 = a + b$ segue $a^2 + ab + ba + b^2 = a + b$ e ancora, dalle $a^2 = a$ e $b^2 = b$ si ha $ab + ba = 0$. Ma dal fatto che $ba + ba = 0$, cioè $ba = -ba$ segue che $ab = ba$ per ogni $a, b \in R$. Se $a \oplus b = \sqrt{a^2 + b^2}$, (R, \oplus) non è un sottoanello: infatti non possiede elemento neutro rispetto a \oplus : 0 funge da elemento neutro solamente per i reali positivi.
 (R, \oplus') è invece un anello (commutativo).
- 4.1.7 La verifica che A è un sottoanello è banale. Si tratta di un anello commutativo, perché

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac - bd & -(bc + ad) \\ bc + ad & ac - bd \end{pmatrix} = \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Possiede unità $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Ogni elemento non nullo è invertibile: risulta $\det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2 + b^2$, $a, b \in \mathbb{Z}_3$. Ora, in \mathbb{Z}_3 gli unici elementi che sono quadrati sono 0 e 1. Quindi $a^2 + b^2 = 0$ se e solo se $a = b = 0$. Quindi l'intera matrice è nulla e ogni matrice non nulla ha determinante diverso da zero ed è quindi invertibile.

- 4.1.8 Basta prendere le due funzioni non nulle f e g da \mathbb{R} ad \mathbb{R}



il cui prodotto è la funzione nulla.

- 4.1.9 L'inverso φ^{-1} di φ è certamente biunivoco. Resta da provare che conserva le operazioni, ossia che, dati comunque $x', y' \in R'$,

$$\varphi^{-1}(x' + y') = \varphi^{-1}(x') + \varphi^{-1}(y'), \quad \varphi^{-1}(x' \cdot y') = \varphi^{-1}(x') \cdot \varphi^{-1}(y').$$

Ora, $x' = \varphi(x)$ per uno e un solo $x \in R$, e così $y' = \varphi(y)$ per uno e un solo $y \in R$. Allora

$$\varphi^{-1}(x' + y') = \varphi^{-1}(\varphi(x) + \varphi(y)) = \varphi^{-1}(\varphi(x+y)) = x+y = \varphi^{-1}(x') + \varphi^{-1}(y').$$

Stesso discorso per il prodotto.

- 4.2.1 $k = 0$ e $k = 1$.
- 4.2.2 È un sottogruppo additivo. Inoltre il prodotto di una matrice quadrata con l'ultima riga uguale a zero per una qualunque matrice quadrata è una matrice che ha ancora l'ultima riga uguale a zero.
- 4.2.3 Non è un sottogruppo, perché la somma di due matrici con determinante uguale a zero può avere determinante diverso a zero: per esempio $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- 4.2.4 S non è un sottoanello, T è un ideale.
- 4.2.5 Sia I un ideale non nullo di K , e sia $a \in I$, $a \neq 0$. Allora $aa^{-1} = 1 \in I$. Contenendo l'unità, I coincide con K .
- 4.2.6 $A(X)$ è un sottogruppo additivo perché $r_1, r_2 \in A(X) \implies r_1x = 0$ e $r_2x = 0 \implies (r_1 - r_2)x = 0 \implies r_1 - r_2 \in A(X)$. Anche $B(X)$ è un sottogruppo additivo. Ora, $\forall a \in A(X), \forall r \in R, (ra)x = r(ax) = 0$, cioè $ra \in A(X)$. Quindi $A(X)$ è un ideale sinistro. Stesso discorso per mostrare che $B(X)$ è un ideale destro. Se X è un ideale sinistro, allora $\forall a \in A, r \in R, (ar)x = a(\underbrace{rx}) = 0$, quindi $A(X)$ è ideale bilatero.
- 4.2.7 In questo caso X è un ideale sinistro, e
- $$A(X) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \forall x, y \in \mathbb{R} \right\}$$
- da cui $A(X) = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$ (ideale bilatero). $B(X) = \left\{ \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \mid c, d \in \mathbb{R} \right\}$ (ideale destro, non sinistro).
- 4.2.8 Dobbiamo provare che la somma o la differenza di due elementi nilpotenti è ancora nilpotente, e il prodotto di un elemento nilpotente per un qualunque elemento è un elemento nilpotente. Siano a, b nilpotenti e siano $n, m \in \mathbb{N}$ tali che $a^n = 0, b^m = 0$. Allora $(a \pm b)^{n+m} = 0$. Infatti $(a \pm b)^{n+m} = \sum_{r=0}^{n+m} \binom{n+m}{r} a^r (\pm b)^{n+m-r}$, e quindi se $r \geq n \implies a^r = 0 \implies \binom{n+m}{r} a^r (\pm b)^{n+m-r} = 0$, se $r < n$ risulta $(\pm b)^{n+m-r} = 0$ e quindi ancora la tesi. Se a è nilpotente con indice di nilpotenza n e x è un elemento arbitrario, si ha $(ax)^n = a^n x^n = 0$. In entrambi i casi abbiamo utilizzato la commutatività. Controesempio: $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ e $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ sono nilpotenti con indice di nilpotenza 2, ma la loro somma $A + B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ non è nilpotente.
- 4.2.9 Se φ è iniettivo, ovviamente $\text{Ker } \varphi = \{0\}$. Supponiamo allora $\text{Ker } \varphi = \{0\}$ e proviamo che φ è iniettivo. $\varphi(x) = \varphi(y) \implies \varphi(x - y) = 0 \implies x - y \in \text{Ker } \varphi$; essendo $\text{Ker } \varphi = \{0\}$, $x = y$.
- 4.2.10 Solo per $a_0 = 0$.
- 4.3.1 $\mathbb{Q}[x]/I = \{a - bx + I \mid a, b \in \mathbb{Q}\}$, $\mathbb{Q}[x]/J = \{a + bx + J \mid a, b \in \mathbb{Q}\}$.
- 4.3.2 $(a + N)^n = a^n + N = N \iff a^n \in N \iff a^n$ è nilpotente $\iff a$ è nilpotente (perché?).
- 4.3.4 $IJ \subseteq I \cap J$. Se $1 \in R$, $R(I \cap J) = I \cap J$. Quindi $I \cap J = R(I \cap J) = (I + J)(I \cap J) \subseteq IJ$.

- 4.4.4 Basta trovare un omomorfismo suriettivo di R in $R/I_1 \oplus R/I_2$ con nucleo $I_1 \cap I_2$. Definiamo $\varphi : R \rightarrow R/I_1 \oplus R/I_2$ ponendo $\varphi(x) = (x + I_1, x + I_2)$. Che si tratti di un omomorfismo con nucleo $I_1 \cap I_2$ è ovvio. Proviamo la suriettività: occorre provare che dato comunque $(r + I_1, s + I_2) \in R/I_1 \oplus R/I_2$, esiste $x \in R$ tale che $\varphi(x) = (r + I_1, s + I_2)$. Dato che $R = I_1 + I_2$, $r = a_1 + a_2$, $s = b_1 + b_2$ per opportuni $a_i, b_i \in I_i$ ($i = 1, 2$). L'elemento $x = a_2 + b_1$ è tale che

$$x \equiv a_2 \equiv r \pmod{I_1}, \quad x \equiv b_1 \equiv s \pmod{I_2},$$

per cui $\varphi(x) = (r + I_1, s + I_2)$.

- 4.4.7 Gli ideali di \mathbb{Z} contenenti $24\mathbb{Z}$ sono: $\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}, 8\mathbb{Z}, 12\mathbb{Z}, 24\mathbb{Z}$, quindi gli ideali di \mathbb{Z}_{24} sono $\mathbb{Z}/24\mathbb{Z} = \mathbb{Z}_{24}, 2\mathbb{Z}/24\mathbb{Z}$, ecc.

- 4.5.1 Se $1 \in R$, tra gli elementi r, a_i ci sono gli a_i .

- 4.5.2 Si provi con (x, y) .

- 4.5.4 Dati comunque $a_1, a_2 \in \mathbb{Z}$, dobbiamo provare che esiste un $x \in \mathbb{Z}$ tale che

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}.$$

Poniamo nell'esercizio 4.4.4 $R = \mathbb{Z}$, $I_1 = m_1\mathbb{Z}$, $I_2 = m_2\mathbb{Z}$, $(m_1, m_2) = 1$ e osserviamo che $I_1 \cap I_2 = m\mathbb{Z}$, $m\mathbb{Z} \cap m_2\mathbb{Z} = (m_1 m_2)\mathbb{Z}$.

- 4.5.5 $\text{MCD}(x^4 + x - 1, x^3 - 2) = -53/27 \sim 1$, quindi $I = (1) \simeq \mathbb{R}[x]$.

- 4.5.8 M è un ideale. Supponiamo che esista un ideale I contenente M e diverso da M . Allora esiste una funzione $g(x) \in I$, $g(x) \notin M$. Ma se $g(x) \notin M$, $g(2) = \alpha \neq 0$. Allora la funzione differenza $d(x) = g(x) - \alpha \in M \subset I$. Concludere.

- 4.5.9 $I + aR$ è un ideale di R e contiene propriamente I , quindi se I è massimale, necessariamente $I + aR = R$. Viceversa, supponiamo $I + aR = R$ per ogni $a \in R \setminus I$. Sia U un qualunque ideale tale che $I \subseteq U \subseteq R$, $U \neq I$. Allora esiste un $a \in U \setminus I \iff U \supseteq I + aR = R \iff U = R$.

- 4.5.10 Siano $a \in I_1$, $a \notin I_2$, $b \in I_2$, $b \notin I_1$. $ab \in I_1 \cap I_2$, ma $a \notin I_1 \cap I_2$, $b \notin I_1 \cap I_2$. Quindi $I_1 \cap I_2$ non è un ideale primo.

- 4.7.1 a primo $\iff [(a | bc \implies a | b \text{ o } a | c)]$. (a) primo $\iff |bc| \in (a) \implies b \in (a) \text{ o } c \in (a)$, quindi ...

- 4.7.2 Sia a un elemento invertibile. Gli associati di a sono gli elementi b tali che $b = au$, con u elemento invertibile. Quindi sono invertibili.

- 4.7.3 ± 1 .

- 4.7.4 $13 = (3 - 2i)(3 + 2i)$, quindi 13 è riducibile e $I = (13)$ non è massimale. $3 - 2i$ invece è irriducibile, quindi $(3 - 2i)$ è massimale. Risulta $(13) \subset (3 - 2i)$.

- 4.7.6 Gli unici elementi invertibili di $\mathbb{Z}[\sqrt{-7}]$ sono ± 1 , quindi sono associati solo $3 + 4\sqrt{-7}$ e $-3 - 4\sqrt{-7}$.

- 4.7.8 Sì.

- 4.7.9 È costituito da quattro classi: $\bar{0}, \bar{1}, \bar{i}, \bar{1+i}$. Non è un campo, perché (2) non è massimale ($2 = (1+i)(1-i)$). Possiede divisori dello zero: $\bar{1+i} \cdot \bar{1+i} = \bar{0}$.

- 4.8.1 Le unità sono ± 1 . $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, e $3, 2 + \sqrt{-5}, 2 - \sqrt{-5}$ sono irriducibili in $\mathbb{Z}[\sqrt{-5}]$. 3 e $2 \pm \sqrt{-5}$ non sono associati, quindi le due fattorizzazioni sono diverse.
- 4.8.3 $9 \in 6 + i3\sqrt{5}$.
- 4.8.4 In $\mathbb{K}[x, y]$ esiste MCD perché è un dominio a fattorizzazione unica. Tuttavia ad esempio x e y sono due polinomi per i quali il MCD non è esprimibile con l'identità di Bézout: infatti $\text{MCD}(x, y) = 1$ ma nella relazione $1 = xs(x, y) + yt(x, y)$ il lato destro è somma di due polinomi con termine noto nullo, quindi si tratta di un polinomio con termine noto nullo, a differenza del lato sinistro.
- 4.9.1 $4 + 3\sqrt{8} \in 36 + 13\sqrt{8}$.
- 4.9.2 $187 = 11 \cdot 17$: quindi non è somma di due quadrati. $377 = 13 \cdot 29$, quindi $377 = 4^2 + 19^2 = 16^2 + 11^2$.
- 4.10.1 0; 0; 15.
- 4.10.2 2.

Capitolo 5

- 5.1.1 Sia $H \subseteq \mathbb{Z}$, $H \neq 0$. Allora H conterrà sicuramente un elemento positivo (perché?) h . Tra tutti gli elementi positivi appartenenti ad H sia n il più piccolo. Chiaramente $\langle n \rangle = n\mathbb{Z} \subseteq H$. Per provare l'altra inclusione basta dividere ogni $a \in H$ per n : dalla $a = nq + r$, $0 \leq r < n$ e dal fatto che a e nq stanno in H si ha $r \in H$ da cui $r = 0$ per non contraddirre la minimialità della scelta di n .
- 5.1.2 $x \in \bigcap_i H_i \Leftrightarrow x \in H_i \forall i$. Quindi $\forall x, y \in \bigcap_i H_i$ si ha $xy^{-1} \in H_i$ per ogni i e quindi $xy^{-1} \in \bigcap_i H_i$ (condizione di sottogruppo).
- 5.1.3 Siano H e K due sottogruppi di G . Se $H \subseteq K$ o $K \subseteq H$ chiaramente $H \cup K$ coincide con K o H rispettivamente, quindi è un gruppo. Viceversa, se $H \not\subseteq K$ e $K \not\subseteq H$, esiste $h \in H, h \notin K$ e un $k \in K, k \notin H$. Allora hk non può appartenere né ad H né a K (perché?) e allora $hk \notin H \cup K$ e quindi $H \cup K$ non è un sottogruppo. Nel caso di $(\mathbb{Z}, +)$ se $H = 3\mathbb{Z}$ e $K = 2\mathbb{Z}$, $3 \in H$, $3 \notin K$, $2 \in K$, $2 \notin H$, 5 dovrebbe stare nell'unione, ma $5 \notin H$ e $5 \notin K$.
- 5.1.4 Sia $ST = TS$. Allora $\forall st, s't' \in ST$ si ha $st(s't')^{-1} = stt'^{-1}s'^{-1} = st\bar{s} = ss_1t_1 \in ST$, avendo posto $t t'^{-1} = \bar{t} \in T$, $s = s'^{-1} \in S$. Viceversa, sia ST sottogruppo. Dobbiamo provare che $st \in ST$ implica $st \in TS$ e viceversa. Se $st \in ST$, allora anche $(st)^{-1} \in ST$, ossia $(st)^{-1} = s_1t_1$ per qualche $s_1 \in S$ e $t_1 \in T$. Allora $st = (s_1t_1)^{-1} = t_1^{-1}s_1^{-1} \in TS$, quindi $ST \subseteq TS$. Il viceversa è analogo.
- 5.1.5 Il prodotto di elementi di S è ancora un elemento di S (si verifichi). Per $a = 1, b = 0$ si ha la matrice identica, che quindi appartiene ad S . L'inversa della $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ è la matrice (ancora in S):

$$\begin{pmatrix} a & -b \\ \frac{a^2 + b^2}{a^2 + b^2} & \frac{a^2 + b^2}{a^2 + b^2} \\ b & a \\ \frac{a^2 + b^2}{a^2 + b^2} & \frac{a^2 + b^2}{a^2 + b^2} \end{pmatrix}.$$

- 5.1.6 Dato che $ab = ba$, risulta $\langle a, b \rangle = \{a^i b^j \mid i, j \in \mathbb{Z}\}$. Dalla $ab = ba$ si vede facilmente che $a^h b^k = b^k a^h$. Quindi

$$(a^i b^j)(a^h b^k) = a^{i+h} b^{j+k} = a^{h+i} b^{k+j} = (a^h b^k)(a^i b^j)$$

cioè due qualunque elementi di $\langle a, b \rangle$ commutano e quindi $\langle a, b \rangle$ è abeliano.

- 5.1.7 Siano $a^n, b^n, a, b \in G$ due elementi arbitrari di S . Allora

$$a^n(b^n)^{-1} = (\text{dato che il gruppo è abeliano}) = (ab^{-1})^n$$

quindi è ancora un elemento di S .

- 5.1.8 Dati comunque \bar{a} e $\bar{b} \in \mathbb{Z}_n$, \bar{a} e \bar{b} sono invertibili in \mathbb{Z}_n , allora anche il loro prodotto lo è, perché $\bar{a}\bar{b}^{-1} = \bar{a}^{-1} \cdot \bar{b}^{-1}$. La classe $\bar{1}$ è l'elemento neutro. Se $\bar{a} \in U(\mathbb{Z}_n)$, significa che \bar{a} è invertibile. Allora il suo inverso \bar{a}^{-1} sta in $U(\mathbb{Z}_n)$ perché $(\bar{a}^{-1})^{-1} = \bar{a}$.

In generale, con un ragionamento identico, si prova che, dato un anello con unità R , il sottoinsieme $U(R)$ di tutti gli elementi invertibili di R costituisce un gruppo.

- 5.1.9 La (unica) soluzione di $ax = b$ è $x = a^{-1}b$. La (unica) soluzione di $ya = b$ è $y = ba^{-1}$.

- 5.1.10 Basta moltiplicare entrambi i membri della prima relazione a sinistra per a^{-1} e entrambi i membri della seconda a destra per a^{-1} .

- 5.1.11 $a * b \in G$, quindi $*$ è un'operazione. L'operazione $*$ è associativa:

$$\begin{aligned} (a * b) * c &= (a * s * b) * c = (a * s * b) \cdot s * c = (\text{il prodotto } \cdot \text{ è associativo}) \\ &= a * s * (b * s * c) = a * (b * c). \end{aligned}$$

Elemento neutro: si deve cercare un $e \in G$ tale che per ogni $a \in G$

$$a * e = e * a = a, \quad \text{cioè} \quad a * s * e = e * s * a = a$$

ossia $e = s^{-1}$. Inverso di a : è un x tale che $a * s * x = s^{-1}$. Quindi $x = s^{-1}a^{-1}s^{-1}$.

- 5.1.12 (a) No, perché non è chiuso rispetto alla moltiplicazione ordinaria: ad es. $2 \cdot (-1/2) = -1 \notin \mathbb{R} \setminus \{-1\}$.

(b) $(S, *)$ è un gruppo:

Chiusura: $x + y + xy = -1 \iff x + y + xy + 1 = 0 \iff x(1+y) + (1+y) = 0 \iff (x+1)(y+1) = 0 \iff x+1 = 0 \circ y+1 = 0$, che non può succedere perché $x, y \in S$.

Associatività: $(x * y) * z = (x + y + xy) * z = x + y + xy + z + xz + yz + xyz$. (N.B. Nel prodotto xyz non occorre mettere le parentesi, perché si tratta della moltiplicazione ordinaria in \mathbb{R}). $x * (y * z) = \dots = x + y + z + yz + xy + xz + xyz = (x * y) * z$.

Elemento neutro: Si deve cercare un $e \in S$ tale che

$$e * x = x = x * e \quad \forall x \in S.$$

N.B. Basta solo $e * x = x$ perché $*$ è comunitativa:

$$e * x = e + x + ex = x \quad \forall x \in S \implies e + ex = 0 \quad \forall x \in S.$$

Quindi $e(1+x) = 0$ per ogni $x \in S$. Ora, $1+x \neq 0$ se e solo se $x \in S$, quindi l'ultima relazione implica $e = 0$, che è quindi l'elemento neutro.

Inverso: $x * x' = 0$ implica $x + x' + xx' = 0$, da cui $x + x'(1+x) = 0$ ossia $x' = -x/(1+x)$. Si noti che $1+x \neq 0$ perché $x \in S$. Quindi ogni elemento di S è invertibile, e $(S, *)$ è un gruppo.

5.1.13 Tutti i sottogruppi di \mathbb{Z} sono del tipo $n\mathbb{Z}$. Ora, $n\mathbb{Z} \ni 6$ se e solo se esiste un $k \in \mathbb{Z}$ tale che $nk = 6$. I sottogruppi $n\mathbb{Z}$ che contengono 6 sono quindi \mathbb{Z} , $2\mathbb{Z}$, $3\mathbb{Z}$ e $6\mathbb{Z}$.

5.1.14 Il risultato dell'operazione \oplus è ancora un numero naturale, quindi \oplus è chiusa, \oplus è associativa perché tale è l'addizione modulo 10. L'elemento neutro è lo zero. L'opposto del numero $n_1 n_2 \dots n_k$ è il numero $n'_1 n'_2 \dots n'_k$, dove n'_i è l'opposto modulo 10 di n_i . Quindi (\mathbb{N}, \oplus) è un gruppo. Dato che il periodo di ogni cifra n_i può essere 1, 2, 5 o 10, il periodo di ogni elemento $n_1 n_2 \dots n_k$ è il mcm tra i periodi delle sue cifre, quindi potrà essere 1, 2, 5 o 10.

Si può generalizzare a basi arbitrarie n : (\mathbb{N}, \oplus_n) è un gruppo, i cui elementi possono avere come periodi tutti i divisori di n .

5.1.15 Un gruppo ciclico è sempre abeliano.

5.1.16 Detto m il periodo di g , basta dividere n per m per scoprire che il resto della divisione deve per forza essere nullo.

5.1.17 Sia $\bar{a} \neq 0$ e sia k il suo ordine. Per definizione di ordine, k è il più piccolo intero positivo tale che $k\bar{a} = 0$. Allora deve essere ka un multiplo di n (e ovviamente ka è un multiplo di a). Allora ka è multiplo comune di a e di n ; dovendo essere il minimo, esso è il $\text{mcm}(a, n)$. Quindi $ka = an / (\text{mcm}(a, n))$, ossia $k = n / (\text{mcm}(a, n))$.

5.1.18 In base all'esercizio precedente, si tratta di determinare le classi \bar{a} tali che $\frac{2^4 5^4}{(a, 2^4 5^4)} = 4$. Deve essere $(a, 2^4 5^4) = 2^2 5^4$. Le classi di periodo 4 sono quindi: 2500 e $\overline{7500}$. Con un ragionamento analogo, quelle di periodo 8 sono $\overline{1250}$, 3750 , 6250 e $\overline{8750}$.

5.1.19 Si veda proposizione 3.4.5. Le radici n -esime sono un gruppo ciclico di ordine n . Dire che $\langle g^k \rangle$ ha $\frac{n}{d}$ elementi significa dire che il periodo di g^k è n/d .

5.1.20 In G gli unici elementi di periodo finito sono $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (periodo 1), $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ (periodo 2 $\forall c \in \mathbb{R}$), $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ (periodo 2 $\forall c \in \mathbb{R}$) e $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ (periodo 2). Si osservi infatti che si ha

$$\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}^n = \begin{pmatrix} a^n & c(a^{n-1} + a^{n-2}b + \dots + b^{n-1}) \\ 0 & b^n \end{pmatrix},$$

quindi tutti gli elementi di G con $a \neq \pm 1$, $b \neq \pm 1$ hanno periodo infinito. Inoltre, per $a = b = 1$, l'elemento $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ verifica la

$$\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & nc \\ 0 & 1 \end{pmatrix}$$

quindi, se $c \neq 0$, ha periodo infinito, se $c = 0$, è l'identità.

Nel caso G' , gli elementi di periodo finito sono gli elementi: $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, con a, b radici n -esime dell'unità.

5.2.1 $(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 5 & 6 & 3 & 2 & 7 & 1 & 4 \end{smallmatrix}) = (1, 8, 4, 3, 6, 7)(2, 5)$ ha periodo 6, la sua inversa è

$$(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 8 & 6 & 3 & 2 & 1 & 4 \end{smallmatrix}) = (1, 7, 6, 3, 4, 8)(2, 5).$$

$(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 6 & 2 & 8 & 7 & 1 & 5 \end{smallmatrix}) = (1, 4, 2, 3, 6, 7)(5, 8)$ ha periodo 6, la sua inversa è

$$(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 4 & 2 & 1 & 8 & 3 & 6 & 5 \end{smallmatrix}) = (1, 7, 6, 3, 2, 4)(5, 8).$$

$(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 2 & 4 & 7 & 6 & 5 & 1 \end{smallmatrix}) = (1, 8)(2, 3)(5, 7)$ ha periodo 2 e quindi coincide con la sua inversa.

$(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 6 & 8 & 7 & 4 & 1 \end{smallmatrix}) = (1, 2, 3)(4, 5, 6, 8)$ ha periodo 12, e la sua inversa è

$$(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 2 & 8 & 4 & 5 & 7 & 6 \end{smallmatrix}) = (1, 3, 2)(4, 8, 6, 5).$$

5.2.2 Non è un sottogruppo: ad esempio, $(1, 2)(1, 2, 3, 4) = (2, 3, 4) \notin S$.

5.2.4 Il prodotto di due permutazioni pari è ancora pari, e così l'inversa di una permutazione pari è pari. Il prodotto di due permutazioni dispari è invece una permutazione pari, quindi le permutazioni dispari non sono chiuse rispetto al prodotto.

5.2.5 Le possibili strutture cicliche sono (10-ciclo) · (4-ciclo), pari; (5-ciclo) · (5-ciclo) · (4-ciclo), dispari; (5-ciclo) · (4-ciclo) · (4-ciclo), pari; (5-ciclo) · (4-ciclo) · (2-ciclo) · (2-ciclo), dispari; (5-ciclo) · (4-ciclo) · (2-ciclo), pari; (5-ciclo) · (4-ciclo), dispari.

Gli elementi di periodo 20 non costituiscono un sottogruppo, perché ad esempio, (oltre al fatto che l'identità non ha periodo 20), il prodotto dei seguenti due elementi di periodo 20

$$(12345)(6789)(12345)(6789) = (13524)(68)(79)$$

è un elemento di periodo 10.

5.2.6 Basta provare che esiste in S_{30} una permutazione di periodo 209. Dato che $209 = 11 \cdot 19$, una tale permutazione è ad esempio il prodotto di un 11-ciclo per un 19-ciclo disgiunti (esistono in S_{30}).

5.2.7 Indichiamo con A e con B le configurazioni iniziali e finali. Supponiamo, come avviene nel nostro caso, che il quadratino vuoto \square si trovi in basso a destra in entrambe le configurazioni. Una mossa è una trasposizione di tipo (i, \square) ($i = 1, \dots, 15$). Ora, se \square , nel passaggio da A a B viene mosso verso l'alto un certo numero di volte, un analogo numero di volte deve venire mosso verso il basso, e analogamente, se viene spostato a sinistra di un certo numero di caselle, deve essere spostato verso destra lo stesso numero di caselle. Quindi il numero totale di mosse nel passaggio da A a B è un numero pari di trasposizioni. Questo significa che la permutazione che fa passare da A a B deve necessariamente essere una permutazione pari. Nel nostro caso la permutazione è

$$\begin{pmatrix} 2 & 1 & 10 & 9 & 11 & 8 & 7 & 5 & 4 & 12 & 6 & 3 & 13 & 15 & 14 & \square \\ 1 & 5 & 4 & 8 & 10 & 3 & 13 & 6 & 11 & 15 & 14 & 12 & 7 & 9 & 2 & \square \end{pmatrix} = (1, 5, 6, 14, 2)(3, 12, 15, 9, 8)(4, 11, 10)(7, 13)$$

che è dispari. Quindi non si può passare dalla configurazione di sinistra a quella di destra.

- 5.2.8 Basta provare che ogni elemento di A_n è prodotto di 3-cicli. Ogni $\sigma \in A_n$ è, per definizione di permutazione pari, prodotto di un numero pari di trasposizioni. Il risultato sarà provato se mostreremo che il prodotto di due trasposizioni è sempre o un 3-ciclo o un prodotto di due 3-cicli. Se le due trasposizioni coincidono, si ottiene la permutazione identica, che è certamente prodotto di un 3-ciclo per il suo inverso. Supponiamo che le due trasposizioni siano disgiunte, ad esempio siano $\sigma = (1, 2)$, $\tau = (3, 4)$: allora si può scrivere $\sigma\tau = (1, 2, 3)(2, 3, 4)$. Se le due trasposizioni hanno un simbolo comune, sia ad esempio $\sigma = (1, 2)$, $\tau = (2, 3)$: allora $(1, 2)(2, 3) = (1, 2, 3)$.

- 5.3.1 Si ha

$$\begin{aligned} |(-)| &= 1, & |(-, -)| &= 10, & |(-, -, -)| &= 20, \\ |(-, -)(-, -)| &= 15, & |(-, -, -, -)| &= 30, & |(-, -, -)(-, -)| &= 20, \\ |(-, -, -, -, -)| &= 24. \end{aligned}$$

- 5.3.2 Sia $G = \langle(m, m+1), m = 1, \dots, n-1\rangle$. G contiene allora $(1, 2)(2, 3)(1, 2) = (1, 3)$, $(1, 3)(3, 4)(1, 3) = (1, 4)$, etc. Quindi G contiene tutte le trasposizioni $(1, r)$, $(r = 2, \dots, n)$. Ma allora contiene ogni trasposizione (r, s) , $(r \neq s)$, perché $(1, s)(1, r)(1, s) = (r, s)$. Risulta $G = S_n$.

- 5.3.3 Sia $G = \langle(1, 2), (1, 2, \dots, n)\rangle$. Allora G contiene

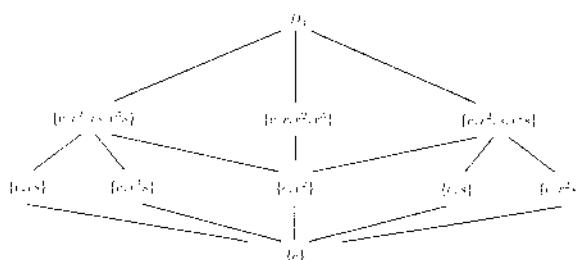
$$\begin{aligned} (1, 2, \dots, n)(1, 2)(1, n, n-1, \dots, 3, 2, 1) &= (2, 3), \\ (1, 2, \dots, n)(2, 3)(1, n, n-1, \dots, 3, 2, 1) &= (3, 4), \quad \text{etc.} \end{aligned}$$

G contiene allora tutte le trasposizioni del tipo $(m, m+1)$ e, per l'esercizio 5.3.2 $G = S_n$.

- 5.3.4 Un elemento g appartiene al centro di un gruppo se e solamente se la sua classe coniugata è ridotta a $\{g\}$. Ora, in S_n l'unico elemento la cui classe coniugata è costituita da un solo elemento è l'elemento neutro. Quindi $Z(S_n) = \{\text{id}\}$.

- 5.4.1 $sr = r^{n-1}s \neq rs$ per $n > 2$.

- 5.4.2 Ci sono 5 elementi di periodo 2, s , r^2 , sr , sr^3 , sr^2 , e quindi cinque sottogruppi di ordine 2. Ci sono poi due elementi di periodo 4, r e r^3 . Il reticolo dei sottogruppi di D_4 è il seguente:



5.4.3 Il centro di D_n è $\{\text{id}\}$ o $\{\text{id}, r^{n/2}\}$ a seconda che n sia dispari o pari: infatti $sr^i = r^{n-i}s$ e $n - i = i$ se e solo se $i = 0$ o $n = 2i$.

5.4.4 Le classi coniugate sono cinque: $\{e\}$, $\{r^2\}$, $\{r, r^3\}$, $\{s, sr^2\}$, $\{sr, sr^3\}$.

5.5.1 $H = \{\text{id}, (1, 3, 4), (1, 4, 3), (1, 3), (3, 4), (1, 4)\}$. I laterali destri sono quattro, e così i laterali sinistri, ma non coincidono.

5.5.2 G è un gruppo abeliano. Il sottogruppo H contiene due elementi, id e Φ .

5.5.3 Ci sono tre sottogruppi di ordine 4: $\{e, r^2, rs, r^3s\}$, $\{e, r, r^2, r^3\}$, $\{e, r^2, s, r^2s\}$; e cinque sottogruppi di ordine 2, $\{e, rs\}$, $\{e, r^3s\}$, $\{e, r^2\}$, $\{e, s\}$, $\{e, r^2s\}$. Sceglieremo il sottogruppo $H = \{e, r^3s\}$ e calcoliamo i laterali destri: $H(r^3s) = H = \{e, r^3s\}$, $Ir = H(r^2s) = \{r, r^2s\}$, $Ir^2 = H(rs) = \{r^2, rs\}$, $Rs = H(r^3) = \{s, r^3\}$. H non è normale in D_4 , perché ad esempio $Ir \neq rH$.

5.6.1 Basta prendere

$$\text{St}_1 = \{\text{id}, (2, 3), (2, 4), (3, 4), (2, 3, 4), (2, 4, 3)\}.$$

$$\text{St}_2 = \{\text{id}, (1, 3), (1, 4), (3, 4), (1, 3, 4), (1, 4, 3)\},$$

$$\text{St}_3 = \{(1, 4), (2, 4), (1, 2), (1, 2, 4), (1, 4, 2)\}.$$

$$\text{St}_4 = \{\text{id}, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\},$$

dove St_i è il sottogruppo di tutte le permutazioni di S_4 che fissano l'elemento i . I nove sottogruppi isomorfi a S_2 sono i nove sottogruppi generati dai nove elementi di periodo due di S_4 , cioè le sei trasposizioni e i tre elementi $(1, 2)(3, 4)$, $(1, 3)(2, 4)$ e $(1, 4)(2, 3)$.

5.6.2 $(\mathbb{Q}, +)$ non è isomorfo a $\mathbb{Q} \setminus \{0\}$, perché in $(\mathbb{Q}, +)$ ogni elemento diverso dall'elemento neutro ha periodo infinito, mentre in $\mathbb{Q} \setminus \{0\}$ l'elemento -1 ha periodo 2.

5.6.3 Il gruppo ciclico di ordine 4 si può identificare con il sottogruppo di S_4 $\{\text{id}, (1, 2, 3, 4), (1, 2)(3, 4), (1, 4, 3, 2)\}$. Il gruppo di Klein si può identificare con il sottogruppo di S_4 $\{\text{id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$.

5.6.4 $G = U(\mathbb{Z}_8) = \{\bar{1}_8, \bar{3}_8, \bar{5}_8, \bar{7}_8\} \cong V$ (gruppo di Klein).

$$G' = U(\mathbb{Z}_{12}) = \{\bar{1}_{12}, \bar{5}_{12}, \bar{7}_{12}, \bar{11}_{12}\} \cong V.$$

Un isomorfismo tra G e G' si ottiene ad esempio mandando $\bar{3}_8$ in $\bar{5}_{12}$, $\bar{5}_8$ in $\bar{7}_{12}$, $\bar{7}_8$ in $\bar{11}_{12}$.

5.6.5 Il prodotto di elementi di S è ancora un elemento di S , $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S$, l'inverso di $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ è

$$\frac{1}{x^2 + y^2} \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \in S.$$

Un isomorfismo con (\mathbb{C}^*, \cdot) si ottiene associando alla matrice $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ il numero complesso $x + iy$: occorre verificare che si tratta di un isomorfismo.

5.6.6 Entrambi sono ciclici di ordine quattro. Un isomorfismo si trova mandando un generatore in un generatore. Un tale isomorfismo è ad esempio

$$\phi : (\mathbb{Z}_4, +) = \langle \bar{1} \rangle \longrightarrow (\mathbb{Z}_5, \cdot) = \langle 2 \rangle$$

$$\bar{0} \mapsto 1$$

$$\bar{1} \mapsto 2$$

$$\bar{2} = 2 \cdot \bar{1} \longrightarrow \bar{2}^2 = \bar{4}$$

$$\bar{3} = 3 \cdot \bar{1} \longrightarrow \bar{3}^3 = \bar{3}.$$

- 5.7.1 Sia n l'ordine di g . Sappiamo (proposizione 5.7.5) che l'ordine di $\varphi(g)$ divide n . Supponiamo per assurdo che l'ordine di $\varphi(g)$ sia m , $0 < m < n$. Allora $e = \varphi(g)^m = \varphi(g^n)$: per l'iniettività, deve essere $g^n = e$, che è un assurdo.
- 5.7.2 Per individuare un omomorfismo che ha per dominio un gruppo ciclico G basta dare l'immagine di un generatore di G . Se vogliamo che si tratti di un isomorfismo, un generatore di G deve andare in un generatore di G' . Quindi il numero di isomorfismi tra G e G' , se $|G| = |G'| = n$ è $\varphi(n)$.
- 5.7.4 Siano $a', b' \in \text{Im } \varphi$. Allora $a' = \varphi(a)$, $b' = \varphi(b)$ per qualche $a, b \in G$. $a'b' = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = b'a'$.
- 5.8.1 È il gruppo ciclico di ordine 2.
- 5.8.5 $A_4 \times K = \{\text{id}, (1, 2)(3, 4), (1, 4)(2, 3), (1, 3)(2, 4)\}$.
- 5.8.6 Siano $Nx = Nx'$ (ossia $x' = nx$), $Ny = Ny'$ (ossia $y' = ny$): dobbiamo provare che $Nxy = Nx'y'$. Infatti $x'y' = nxny = nxy$ (dato che $N \trianglelefteq G$).
- 5.8.7 Il coniugato di una permutazione pari è una permutazione pari, quindi A_n assieme ad ogni elemento contiene tutti i coniugati, e quindi $A_n \triangleleft S_n$. Il quoziente è costituito da due classi, quella contenente le permutazioni pari e quella contenente le permutazioni dispari. In generale, ogni sottogruppo di indice 2 in un gruppo è normale nel gruppo.
- 5.8.8 Siano $H = \{e, rs\}$, $K = \{e, r^2, rs, r^3s\}$ in D_4 . Risulta $H < K$, ma $H \not\trianglelefteq G$.
- 5.9.1 Sia $G = \langle g \rangle$ ciclico infinito e sia φ un automorfismo di G : esso è individuato dal valore che assume su g . Quindi dovrà essere $\varphi(g) = g^i$ per qualche $i \in \mathbb{Z}$. D'altra parte, essendo φ suriettivo, dovrà essere $g = \varphi(g^r) = g^{ir}$ per qualche $r \in \mathbb{Z}$. Allora $g = \varphi(g^r) = \varphi(g)^r = g^{ir} \Rightarrow ir = 1$: trattandosi di interi, tale relazione comporta $i = \pm 1$. Ciascuno di questi valori dà luogo ad un automorfismo. Quindi $\text{Aut}(G) \cong \mathbb{Z}_2$.
- Sia ora $G = \langle g \rangle$ il gruppo ciclico di ordine n . Un automorfismo φ di G deve mandare g in un altro generatore di G , ossia in un g^i , con i tale che $(i, n) = 1$, $0 < i < n$: indicato con φ_i l'applicazione di G in sé che manda g in g^i (i soggetto alle restrizioni di cui sopra), φ è un automorfismo di G . L'applicazione Ψ da $U(\mathbb{Z}_n)$ a $\text{Aut}(G)$ data da $\Psi(i) = \varphi_i$ è biumivoca e conserva l'operazione. Quindi $\text{Aut}(G) \cong U(\mathbb{Z}_n)$.
- 5.9.3 Se $x, y \in Z(G)$, allora $(xy)g = x(yg) = x(gy) = (xg)y = g(xy)$ per ogni $g \in G$, quindi $xy \in Z(G)$. Se $x \in Z(G)$, $x^{-1}(xy)x^{-1} = x^{-1}(gx)x^{-1}$, da cui $gx^{-1} = x^{-1}g$ per ogni $g \in G$, cioè $g^{-1} \in Z(G)$. Quindi $Z(G)$ è un sottogruppo. È normale, perché $Z(G) = \{x \in G : gx = xg \forall g \in G\} = \{x \in G \mid gxg^{-1} = x \forall g \in G\}$, ossia $Z(G)$ è l'insieme di tutti gli elementi che coincidono con i loro coniugati: è ovvio allora che si tratta di un sottogruppo normale in G .
- 5.9.4 Sia G privo di sottogruppi propri. Se $G = \{e\}$, non c'è nulla da provare. Sia $g \in G$, $g \neq e$ e sia $H = \langle g \rangle$: deve necessariamente essere $H = G$, quindi G è ciclico. Non può essere G infinito, perché un gruppo ciclico infinito contiene

infiniti sottogruppi. Quindi è ciclico finito, e il suo ordine è un numero primo, altrimenti conterrebbe per ogni divisore del suo ordine un sottogruppo.

- 5.9.5 $\text{Aut}(\mathbb{Z}_9) \cong U(\mathbb{Z}_9) = \{\bar{1}_9, \bar{2}_9, \bar{4}_9, \bar{5}_9, \bar{7}_9, \bar{8}_9\}$. Si tratta di un gruppo ciclico (di ordine 6).
- 5.9.6 Tutte le funzioni che appartengono alla stessa classe godono della proprietà che assumono lo stesso valore in $1/3$. $G/N \cong (\mathbb{R}, +)$.
- 5.9.7 Il sottogruppo generato dalle due matrici è un gruppo di ordine 8: $\begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix}$ e $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ hanno periodo 4. L'elemento di periodo 2 è $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ che genera un sottogruppo normale in H e anche in $\text{GL}_2(\mathbb{C})$. Il gruppo H non è abeliano.
- 5.9.8 I tre elementi di periodo 2 di S_3 , ossia $(1, 2), (1, 3), (2, 3)$ devono per forza andare nella classe nulla di \mathbb{Z}_{15} , perché non ci sono in \mathbb{Z}_{15} elementi di periodo 2. Ma questi tre elementi generano tutto S_3 , quindi l'unico omonomorfismo è l'omomorfismo banale.
- 5.9.9 Se G è abeliano, è ovvio che l'applicazione che associa ad ogni elemento il suo inverso è un automorfismo. Viceversa, supponiamo che l'applicazione φ tale che $\varphi(x) = x^{-1}$ sia un automorfismo. Allora $\varphi(xy) = (xy)^{-1} = \varphi(x)\varphi(y) = x^{-1}y^{-1}$, per cui $y^{-1}x^{-1} = x^{-1}y^{-1}$ per ogni $x, y \in G$, quindi G è abeliano.
- 5.9.11 $\mathcal{I}(A_4) \cong A_4$, dato che il centro di A_4 è ridotto al solo elemento neutro.
- 5.9.12 $\text{Aut}(\mathbb{Z}_{15}) \cong U(\mathbb{Z}_{15}) = \{\bar{1}_{15}, \bar{2}_{15}, \bar{4}_{15}, \bar{7}_{15}, \bar{8}_{15}, \bar{11}_{15}, \bar{13}_{15}, \bar{14}_{15}\}$. Non è ciclico, perché non contiene elementi di periodo 8. Essendo \mathbb{Z}_{15} abeliano, l'unico automorfismo interno è l'automorfismo identico.
- 5.9.13 $N = \{e, r^2\}$. Il quoziente è isomorfo al gruppo di Klein.
- 5.9.14 (a) Si tratta di provare che $\forall x \in G'$ e $\forall g \in G$ risulta $gxg^{-1} \in G'$. Basta provare (perché?) che il coniugato di un commutatore è ancora un commutatore. Sia $x = aba^{-1}b^{-1}$. Allora
- $$\begin{aligned} gxg^{-1} &= g(aba^{-1}b^{-1})g^{-1} = ga\underbrace{g^{-1}gb}_{e}g^{-1}\underbrace{ga^{-1}}_{e}\underbrace{g^{-1}b^{-1}}_{e}g^{-1} \\ &= (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \\ &= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} \in G' \end{aligned}$$
- (b) $G' = \{e\} \iff xyx^{-1}y^{-1} = e \quad \forall x, y \in G \iff xy = yx \quad \forall x, y \in G$, cioè se e solo se G è abeliano.
- 5.9.15 Geometricamente le classi laterali sono rette parallele alla retta $y = 3x$. $\mathbb{R}^2/S \cong (\mathbb{R}, +)$.
- 5.10.2 $H = \{(4/3)^i \mid i \in \mathbb{Z}\}$, $HN = \{hn \mid h \in H, n \in N\} = \{\pm(1/3)^i \mid i \in \mathbb{Z}\}$. $H \cap N = \{1\}$. Una classe laterale in HN/N ha la forma $\{x, -x\}$, con $x \in HN$, cioè $x = \pm 1/3^i$. Ma allora ogni classe di HN/N è una potenza di $(1/3)N$, e quindi HN/N è il gruppo ciclico infinito generato dalla classe $1/3N$. Dato che $H \cap N = \{1\}$, allora $H/(H \cap N) \cong H$, che è ciclico infinito. Abbiamo così verificato che $H/(H \cap N) \cong HN/N$.
- 5.11.1 Sia $\sigma \in A_n$. Supponiamo che σ commuti con qualche permutazione dispari $\delta \in S_n$. Sia $\tau \in \sigma^{S_n}$, $\tau = \alpha\sigma\alpha^{-1}$ per qualche $\alpha \in S_n$. Se $\alpha \in A_n$, allora $\tau \in \sigma^{A_n}$; se α è dispari, allora $\delta\alpha \in A_n$, e $\tau = \alpha\sigma\alpha^{-1} = \alpha\delta\sigma\delta^{-1}\alpha^{-1} = (\alpha\delta)\sigma(\alpha\delta)^{-1}$, da cui ancora $\tau \in \sigma^{A_n}$. Quindi $\sigma^{S_n} \subseteq \sigma^{A_n}$ da cui $\sigma^{S_n} = \sigma^{A_n}$.

Supponiamo ora che σ non commuti con nessuna permutazione dispari. Allora il centralizzante $C_{S_n}(\sigma)$ di σ in S_n coincide con il centralizzante $C_{A_n}(\sigma)$ di σ in A_n . Per il corollario 5.11.6,

$$|\sigma^{A_n}| = \frac{|A_n|}{|C_{A_n}(\sigma)|} = \frac{1}{2} \frac{|S_n|}{|C_{A_n}(\sigma)|} = \frac{1}{2} \frac{|S_n|}{|C_{S_n}(\sigma)|} = \frac{1}{2} |\sigma^{S_n}|.$$

Osserviamo ora che ogni permutazione dispari ha la forma $(1, 2)\tau$ per qualche permutazione pari τ . Quindi la classe di coniugio $((1, 2)\sigma(1, 2)^{-1})^{A_n}$ di $(1, 2)\sigma(1, 2)^{-1}$ in A_n coincide con $\{\delta\sigma\delta^{-1} \mid \delta \text{ dispari}\}$. In definitiva,

$$\sigma^{S_n} = \{\tau\sigma\tau^{-1} \mid \tau \text{ pari}\} \cup \{\tau\sigma\tau^{-1} \mid \tau \text{ dispari}\} = \sigma^{A_n} \cup ((1, 2)\sigma(1, 2)^{-1})^{A_n}.$$

5.11.2 Le classi coniugate di A_5 sono cinque, e sono quelle che hanno come rappresentanti: l'identità, $(1, 2, 3)$, $(1, 2)(3, 4)$, $(1, 2, 3, 4, 5)$ e $(1, 3, 4, 5, 2)$. Nell'ordine, la cardinalità di ciascuna classe è: 1, 20, 15, 12, 12.

5.11.4 $D_4 = \langle r, s \mid r^4 = s^2 = 1, sr = r^3s \rangle$, $Z(D_4) = \{e, r^2\}$. L'equazione delle classi è

$$|D_4| = |Z(D_4)| + \frac{|D_4|}{|C(r)|} + \frac{|D_4|}{|C(s)|} + \frac{|D_4|}{|C(sr)|}$$

dove $C(r) = \{1, r, r^2, r^3\}$, $C(s) = \{1, s, r^2, r^2s\}$, $C(sr) = \{1, r^3s, r^2, rs\}$.

5.11.6 3.

5.11.7 2.

5.11.9 (a) Il numero totale delle configurazioni è r^p . Il gruppo che agisce è \mathbb{Z}_p . Il numero delle orbite (cioè il numero di bicchieri distinti) è $(1/p)(r^p + (p-1)r)$.
(b) p divide $r^p + (p-1)r$ per cui $p \mid r^p - r$, cioè $r^p \equiv r \pmod{p}$.

5.11.10 In S_4 $C((1, 2)) = \{\text{id}, (1, 2), (3, 4), (1, 2)(3, 4)\}$,

$C((1, 2, 3, 4)) = \{\text{id}, (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2)\}$.

5.11.11 In S_n $C((1, 2)) = \{\tau, (1, 2)\tau \mid \tau \text{ permutazioni che lasciano fissi } 1 \text{ e } 2\}$.
 $C((1, 2, \dots, n)) = \{(1, 2, \dots, n)^i \mid i = 0, \dots, n-1\}$. Spiegare perché.

5.12.1 gHg^{-1} è ancora un p -sottogruppo di Sylow (infatti la cardinalità di H coincide con la cardinalità di gHg^{-1} e inoltre gHg^{-1} è un sottogruppo). Dovendo essere H unica, deve essere necessariamente $gHg^{-1} = H$, ossia $H \trianglelefteq G$.

5.12.2 Un sottogruppo di A_4 di ordine 6, supposto esistente, è certamente normale in A_4 , avendo indice 2; indichiamolo con N . Sia k il numero di 3-sottogruppi di Sylow di N . Allora (per i teoremi di Sylow) $k \mid 6$ e $k \equiv 1 \pmod{3}$; quindi $k = 1$. Indichiamo con S tale 3-sottogruppo di Sylow di N . S è un 3-sottogruppo di Sylow anche di A_4 ($12 = 2^2 \cdot 3$). Sia T un 3-sottogruppo di Sylow di A_4 . Allora S e T sono coniugati, ossia $T = \sigma S \sigma^{-1}$ per qualche $\sigma \in A_4$, e allora

$$T = \sigma S \sigma^{-1} \subseteq \sigma N \sigma^{-1} = N$$

Quindi T è un 3-sottogruppo di Sylow di N e deve quindi coincidere con S . S è quindi l'unico 3-sottogruppo di Sylow di A_4 . Ma allora S deve contenere tutti gli elementi di A_4 di ordine 3 (perché altrimenti questi genererebbero

altri 3-sottogruppi di Sylow). Tali elementi sono in numero di 8, e questo è assurdo, perché S ha 3 elementi. Quindi A_4 non può contenere un sottogruppo di ordine 6.

- 5.12.4 $Z \neq \{e\}$ (perché il centro di un p -gruppo è non banale), e $Z \neq G$, dato che G non è abeliano. Se fosse $|Z| = p^2$, sarebbe $|G/Z| = p$ e quindi G/Z sarebbe ciclico. Ma allora (perché?) G sarebbe abeliano. Quindi Z ha ordine p .

- 5.12.5 I 2-Sylow di S_4 sono i tre sottogruppi di ordine 2. C'è un solo 3-Sylow, normale, $\langle (1, 2, 3) \rangle$.

$|S_4| = 2^3 \cdot 3$, quindi i 2-Sylow di S_4 hanno ordine 8, mentre i 3-Sylow hanno ordine 3 e sono i 4 sottogruppi $\langle (1, 2, 3) \rangle, \langle (1, 2, 4) \rangle, \langle (1, 3, 4) \rangle$ e $\langle (2, 3, 4) \rangle$. Si noti che sono tutti coniugati tra di loro (come deve essere).

Un 2-Sylow di S_4 è

$$\{\text{id}, (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2), (1, 2)(3, 4), (1, 4)(2, 3), (2, 4), (1, 3)\}.$$

isomorfo a D_4 . Per trovare gli altri, dato che sono tutti coniugati tra di loro, basta coniugare il gruppo trovato. Se ne trovano esattamente tre distinti.

- 5.12.7 G contiene un sottogruppo normale H di ordine p , un sottogruppo normale K di ordine q . $G \cong H \times K$ (perché?).

- 5.12.9 In $\mathbb{Z}_p[x]$ $(1+x)^{p^n} = 1 + x^{p^n} \implies (1+x)^{p^nm} = (1 + x^{p^n})^m$. Confrontare il coefficiente di x^{p^n} di sinistra con quello di destra dell'ultima uguaglianza per ottenere $\binom{p^nm}{p^n} = m \in \mathbb{Z}_p$.

- 5.13.1 Sia H un sottogruppo di G di ordine 7 (esiste per il teorema di Cauchy). Risulta $|G| \nmid |\langle i(H) \rangle|$. Quindi, per il teorema di Cayley generalizzato, indicato con X l'insieme delle classi laterali sinistre modulo H , l'applicazione $\psi : G \rightarrow \mathcal{S}(X)$ data da $\psi(g) = T_g$, dove $T_g(xH) = gxH$ è un omomorfismo che non è un isomorfismo, e quindi il nucleo è non banale, ed è il più grande sottogruppo normale di G contenuto in H . Ne consegue che H stesso è normale in G .

- 5.13.2 Come prima, prendendo un sottogruppo (che esiste) di ordine 11.

- 5.13.3 Con ciascuno dei gruppi rimasti cercare un sottogruppo con cui ripetere il solito ragionamento.

- 5.14.3 A \mathbb{Z}_{40} .

- 5.14.4 No, perché $\mathbb{Z}_4 \times \mathbb{Z}_5$ non è ciclico (non possiede nessun elemento di ordine 10).

- 5.14.5 $(\mathbb{Q}, +)$ non può essere prodotto diretto di due suoi sottogruppi propri, perché due sottogruppi non banali di \mathbb{Q} hanno sempre intersezione non banale. Siano infatti H_1 e H_2 due sottogruppi non banali di $(\mathbb{Q}, -)$, e sia $a_1/b_1 \in H_1, a_2/b_2 \in H_2$. Supposti b_1 e b_2 positivi, si ha $a_1 = b_1(a_1/b_1) \in H_1$, $a_2 = b_2(a_2/b_2) \in H_2$, per cui $a_1 \cdot a_2 \in H_1 \cap H_2$.

- 5.14.6 Ogni gruppo G di ordine $15 = 3 \cdot 5$ contiene (cfr. il teorema di Sylow) un unico sottogruppo H di ordine 3 ed un unico sottogruppo K di ordine 5. Tali gruppi hanno intersezione ovviamente ridotta al solo elemento neutro, e sono ciclici. Detto a un generatore di H e b un generatore di K , l'elemento ab ha periodo 15 (si escludano le altre possibilità 1, 3 e 5). Quindi G è ciclico.

- 5.14.7 $U(\mathbb{Z}_7) = \{1_7, 2_7, 3_7, 4_7, 5_7, 6_7\}$. Sì, è ciclico.

- 5.14.8 1, 2, 3, 6, ∞ . Non è ciclico infinito, perché possiede elementi di periodo 2 e 3, mentre un gruppo ciclico infinito possiede solamente elementi di periodo infinito e 1. Anche $\mathbb{Z} \times \mathbb{Z}$ non è ciclico: non può esistere un elemento $(n, m) \in \mathbb{Z} \times \mathbb{Z}$ che genera tutto $\mathbb{Z} \times \mathbb{Z}$ (perché?).
- 5.14.9 Nessuno.
- 5.14.10 1, 2, 5, 10.
- 5.14.11 No, gli unici sottogruppi normali di S_4 sono A_4 (sottogruppo alterno) e $K = \{\text{id}, (1, 2)(3, 4), (1, 3)(2, 4), (2, 3)(1, 4)\}$.
- 5.14.12 È vera. $(x, y) \in Z(H \times K) \iff (x, y)(h, k) = (h, k)(x, y)$ per ogni $(h, k) \in H \times K$, $\iff (xh, yk) = (hx, ky)$ per ogni $h \in H, k \in K$, $\iff xh = hx, yk = ky$ per ogni $h \in H, k \in K \iff x \in Z(H), y \in Z(K) \iff (x, y) \in Z(H) \times Z(K)$.
- 5.15.1 Se G è semplice e risolubile, deve necessariamente essere abeliano (la catena deve essere costituita da due soli gruppi, l'intero gruppo e il sottogruppo ridotto al solo elemento neutro). Allora G è un gruppo privo di sottogruppi (normali), e quindi ciclico di ordine un numero primo. Il viceversa è ovvio.
- 5.15.2 Sia N un sottogruppo normale di A_n diverso da $\{e\}$. La linea della dimostrazione è la seguente: (a) si prova che N contiene un 3-ciclo; (b) si prova che allora N contiene tutti i 3-cicli. Allora si può concludere che N coincide con tutto A_n , dato che i 3-cicli generano A_n .
 - (a) Si esaminano via via i vari elementi di N , e sfruttando la normalità di N in A_n e il fatto che si può giocare con almeno 5 simboli, si prova che in ogni caso contiene un 3-ciclo.
 - (b) Supponiamo che N contenga il ciclo $(1, 2, 3)$ (non è restrittiva questa ipotesi). Allora per ogni $i \geq 4$ N conterrà (essendo $N \trianglelefteq A_n$ ed essendo ogni 3-ciclo una permutazione pari) il 3-ciclo $(3, 2, i)(1, 2, 3)(3, 2, i)^{-1} = (1, i, 2)$. Ma allora N conterrà $(1, i, 2)^{-1} = (1, 2, i)$ per ogni $i \geq 4$. Non è difficile vedere che questi 3-cicli generano tutto A_n , quindi $N = A_n$.
- 5.15.3 Se S_n fosse risolubile (per $n \geq 5$), allora anche A_n sarebbe risolubile e semplice, e quindi A_n sarebbe ciclico di ordine un numero primo, cosa che è falsa per $n \geq 5$.
- 5.15.4 Siano

$$\begin{aligned} N &= N_r \supseteq N_{r-1} \supseteq \cdots \supseteq N_1 = \{e\} \\ G/N &= M_1 \supseteq M_2 \supseteq \cdots \supseteq M_k = N/N \end{aligned}$$

le successioni che realizzano la risolubilità di N e G/N . Ogni M_i , in quanto sottogruppo del quoziente G/N è del tipo M'_i/N , M'_i sottogruppo di G contenente N . La successione

$$G = M'_1 \supseteq \cdots \supseteq M'_k = N = N_1 \supseteq N_2 \supseteq \cdots \supseteq N_h = \{e\}$$

realizza la risolubilità di G (si verifichi).

- 5.17.1 $56 = 2^3 \cdot 7$, quindi i gruppi abeliani che hanno ordine 56 sono $\mathbb{Z}_8 \times \mathbb{Z}_7$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_7$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_7$. L'unico ciclico è il primo.

- 5.17.2 $U(\mathbb{Z}_{30}) = \{\bar{1}_{30}, \bar{7}_{30}, \bar{11}_{30}, \bar{13}_{30}, \bar{17}_{30}, \bar{19}_{30}, \bar{23}_{30}, \bar{29}_{30}\}$. $\bar{7}_{30}, \bar{13}_{30}, \bar{17}_{30}$, e $\bar{23}_{30}$ hanno periodo 4, tutti gli altri (tranne 1) hanno periodo 2. Quindi $U(\mathbb{Z}_{30})$ non è ciclico. Risulta $U(\mathbb{Z}_{30}) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.
- 5.17.3 $72 = 3^2 \cdot 2^3$, G abeliano, quindi $G \cong \Sigma_3 \times \Sigma_2$, con $|\Sigma_3| = 9$ e $|\Sigma_2| = 8$. Potrebbe essere $\Sigma_3 = \mathbb{Z}_9$ o $= \mathbb{Z}_3 \times \mathbb{Z}_3$, $\Sigma_2 = \mathbb{Z}_8$ o $= \mathbb{Z}_4 \times \mathbb{Z}_2$ o $= \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Se G deve contenere un elemento di periodo 36 dovrà essere necessariamente $\Sigma_3 = \mathbb{Z}_9$ e $\Sigma_2 = \mathbb{Z}_8$ o $= \mathbb{Z}_4$. Ma G non contiene nessun sottogruppo isomorfo a \mathbb{Z}_8 , quindi necessariamente $G \cong \mathbb{Z}_9 \times \mathbb{Z}_4 \times \mathbb{Z}_2$.

Capitolo 6

- 6.1.1 Sia K il campo e F un suo sottocampo: $(K, +)$ è un gruppo abeliano. Inoltre per ogni $k \in K$ e ogni $\alpha \in F$, l'elemento $\alpha \cdot k \in K$ (prodotto in K). Sono verificate tutte le proprietà di spazio vettoriale (si controlli).
- 6.1.2 $1 + 2\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2}) \implies 1/(1 + 2\sqrt[3]{2}) \in \mathbb{Q}(\sqrt[3]{2})$, dato che si tratta di un campo. $1 + 2\sqrt[3]{2} \notin \mathbb{Q}$, altrimenti $\sqrt[3]{2}$ apparterebbe a \mathbb{Q} (assurdo perché $x^3 - 2$ è irriducibile su \mathbb{Q}). Anche senza calcolare chi è $\frac{1}{1+2\sqrt[3]{2}}$, si può concludere che $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2})$, perché $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ (primo), per cui non ci sono campi intermedi.
- 6.1.3 (a), (b); sì. (c), (d); no.
- 6.1.4 Sia $\alpha = (\pi + 2)/(\pi + \sqrt{2})$. Si ha $\pi(1 - \alpha) = \alpha\sqrt{2} - 2$. Essendo $\alpha \neq 1$, se α fosse algebrico, anche π sarebbe algebrico. Quindi α è trascendente. Tutti gli altri sono algebrici.
Il polinomio minimo di $\sqrt[3]{2} + \sqrt[3]{5}$ è $x^6 - 15x^4 - 4x^3 + 75x^2 - 60x - 121$. Si tratta effettivamente del polinomio minimo, perché $\sqrt[3]{2} + \sqrt[3]{5} \notin \mathbb{Q}(\sqrt[3]{2})$ e quindi $\mathbb{Q}(\sqrt[3]{2} + \sqrt[3]{5}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{5})$ e $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{5}) : \mathbb{Q}] = 6$.
Polinomio minimo di $\sqrt[3]{4} + \sqrt[3]{5}$ è $x^6 - 8x^3 + 11$.
Polinomio annullato da $\sqrt[3]{2} + \sqrt[3]{2}$ è $x^4 - 4x^2 + 2$, che è irriducibile per Eisenstein, quindi si tratta del polinomio minimo.
- 6.1.5 $[\mathbb{Q}(\sqrt[3]{2}\sqrt[3]{3}) : \mathbb{Q}] = 2$: il polinomio minimo è $x^2 - 6$, e una base è $\{1, \sqrt[3]{2}\sqrt[3]{3}\}$.
 $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$. Una base è $\{1, \sqrt[3]{2}, \sqrt[3]{2}, \sqrt[3]{2}^2, \sqrt[3]{2}\sqrt[3]{2}, \sqrt[3]{2}\sqrt[3]{2}^2\}$.
 $[\mathbb{Q}(\sqrt[3]{3} + \sqrt[3]{5}) : \mathbb{Q}(\sqrt[3]{5})] = 2$ e una base è $\{1, \sqrt[3]{3}\}$.
- 6.1.6 ξ soddisfa il polinomio $x^p - 1$, tuttavia tale polinomio non è il polinomio minimo per ξ , dato che non è irriducibile. Risulta infatti $x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \dots + x + 1)$. Ora, ξ non soddisfa $x - 1$, ma soddisfa $x^{p-1} + x^{p-2} + \dots + x + 1$, e quest'ultimo è irriducibile su \mathbb{Q} , (si ricordi quanto detto a proposito dei polinomi ciclotomici) e pertanto è il polinomio minimo di ξ . Si ha pertanto $[\mathbb{Q}(\xi) : \mathbb{Q}] = p - 1$, e una base di $\mathbb{Q}(\xi)$ è data da $\{1, \xi, \xi^2, \dots, \xi^{p-2}\}$.
- 6.1.7 Risulta

$$(*) \quad \sqrt{i} = (\cos \pi/2 + i \sin \pi/2)^{1/2} = \cos \pi/4 + i \sin \pi/4 = 1/\sqrt{2} + i1/\sqrt{2}.$$

Inoltre, $i\sqrt{i} = -1/\sqrt{2} + i1/\sqrt{2}$, da cui $\sqrt{i} - i\sqrt{i} = \sqrt{2}$. Dato inoltre che $i = (\sqrt{i})^2$, ne segue che $\mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\sqrt{i})$. D'altra parte, per la (*), $\mathbb{Q}(\sqrt{i}) \subseteq \mathbb{Q}(\sqrt{2}, i)$, da cui l'uguaglianza delle due estensioni.

- 6.1.8 Posto $\alpha = \sqrt{3} + \sqrt{7}$, si ha $\alpha - \sqrt{3} = \sqrt{7}$. Elevando al quadrato, $(\alpha - \sqrt{3})^2 = 7 \Rightarrow \alpha^2 + 3 - 2\alpha\sqrt{3} = 7$ e quindi $(\alpha^2 - 4)^2 = 12\alpha^2 \Rightarrow \alpha^4 - 20\alpha^2 + 16 = 0$. Il polinomio minimo è pertanto $x^4 - 20x^2 + 16$. Infatti α non può soddisfare un polinomio di grado inferiore; un tale polinomio dovrebbe avere grado 2, ma in tal caso $\sqrt{3} + \sqrt{7}$ dovrebbe appartenere a $\mathbb{Q}(\sqrt{3})$, e quindi dovrebbe appartenere a $\mathbb{Q}(\sqrt{3})$ anche $\sqrt{7}$, che è impossibile.
- 6.1.9 Sia $\alpha = \sqrt{2} + i$, $i \notin \mathbb{R}$ e $\alpha - \sqrt{2} = i$. Elevando al quadrato ambo i membri, $\alpha^2 + 2 - 2\sqrt{2}\alpha = -1$. Quindi $x^2 - 2\sqrt{2}x + 3$ è il polinomio minimo di α su \mathbb{R} . Il polinomio minimo su \mathbb{Q} è ...
- 6.1.10 Un campo finito ha caratteristica p per qualche p primo, quindi è estensione di \mathbb{Z}_p . Ma allora si tratta di uno spazio vettoriale di dimensione n su \mathbb{Z}_p , per cui ha p^n elementi.
- 6.1.11 Basta far vedere che $\sqrt{3}$ e $\sqrt{5}$ si possono scrivere come combinazione di 1 e $\sqrt{5}$ a coefficienti in $\mathbb{Q}(\sqrt{3})$. Infatti $\sqrt{3} = \alpha \cdot 1 + \beta \cdot \sqrt{5}$, con $\alpha = \sqrt{3}$, $\beta = 0$, $\sqrt{5} = \gamma \cdot 1 + \delta \cdot \sqrt{5}$, con $\gamma = 0$, $\delta = 1$.
- 6.2.1 L'unico polinomio irriducibile di secondo grado a coefficienti in \mathbb{Z}_2 è $x^2 + x + 1$. $\mathbb{Z}_2[x]/(x^2 + x + 1) = \{a + b\xi \mid \xi^2 = \xi + 1\}$.
- 6.2.2 Si tratta di un polinomio di terzo grado privo di radici in \mathbb{Z}_2 , quindi è irriducibile. $\mathbb{Z}_2(\alpha) = \{0, 1, 1 + \alpha, \alpha^2, 1 + \alpha^2, \alpha + \alpha^2, 1 + \alpha + \alpha^2, \alpha \mid \alpha^3 + \alpha^2 + 1 = 0\}$. Risulta $x^3 + x^2 + 1 = (x - \alpha)(x - \alpha^2)(x - (1 + \alpha + \alpha^2))$, quindi $\mathbb{Z}_2(\alpha)$ è il campo di spezzamento di $x^3 + x^2 + 1$ su \mathbb{Z}_2 , che ha perciò grado 3 su \mathbb{Z}_2 , strettamente minore del massimo possibile, 3! = 6.
- 6.2.3 $\mathbb{Z}_5(\alpha) \cong \mathbb{Z}_5[x]/(x^2 + x + 1)$. Si tratta di un campo con 25 elementi.
- 6.2.4 È irriducibile su \mathbb{Z}_3 perché di grado 2 e privo di radici in \mathbb{Z}_3 . Risulta

$$\mathbb{Z}_3(\alpha) = \{0, 1, 2, \alpha, 2\alpha, 1 + \alpha, 1 + 2\alpha, 2 + \alpha, 2 + 2\alpha\}.$$

La tavola di moltiplicazione viene costruita tenendo conto che $\alpha^2 = -1$.

- 6.2.5 L'inverso è $2a + 1$.
- 6.2.6 (a) $\mathbb{Q}(\sqrt{5}i)$; (b) $\mathbb{Q}(\sqrt{2}, \sqrt{5})$; (c) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$; (d) $\mathbb{Q}(\xi)$, $\xi = (-1 - \sqrt{3}i)/2$ radice terza primitiva dell'unità; (e) $\mathbb{Q}(\sqrt{2}, i)$; (f) $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$. Le radici di $x^4 - 4x^2 + 2$ sono $\pm\sqrt{2 \pm \sqrt{2}}$. Dato che $\mathbb{Q}(\sqrt{2 + \sqrt{2}}) = \{q_0 + q_1\sqrt{2 + \sqrt{2}} + q_2(2 + \sqrt{2}) + q_3\sqrt{2 + \sqrt{2}}^3\}$, si ha che $2 + \sqrt{2}$ (e quindi $\sqrt{2}$) sta in $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$. Ma allora anche $\sqrt{2 - \sqrt{2}} = \sqrt{2}/(\sqrt{2 + \sqrt{2}}) \in \mathbb{Q}(\sqrt{2 + \sqrt{2}})$.
- 6.2.7 $x^3 + \sqrt{3}x^2 - 2x - 2\sqrt{3} = (x + \sqrt{3})(x^2 - 2)$ quindi il campo di spezzamento su $\mathbb{Q}(\sqrt{3})$ è $\mathbb{Q}(\sqrt{3}, \sqrt{2})$.
- 6.3.1 $16 = 2^4$, quindi esiste un campo con 16 elementi: lo si può costruire come $\mathbb{Z}_2[x]/(p(x))$, dove $p(x)$ è un polinomio irriducibile di grado 4 su \mathbb{Z}_2 (ad esempio $p(x) = x^4 + x + 1$).
- $36 = 2^2 \cdot 3^2$ non è potenza di un primo, quindi non esistono campi con 36 elementi.

401 è un numero primo (basta controllare che non è divisibile per 2, 3, 5, 7, 13, 17, e 19), quindi esiste un campo con 401 elementi, ed è \mathbb{Z}_{401} .

$3763 = 53 \cdot 71$ (si utilizzi il metodo di Fermat) e quindi non esistono campi con 3763 elementi.

6.3.2 Sia a un generatore del gruppo degli elementi non nulli di K (si sa che il gruppo moltiplicativo di un campo finito è ciclico). Proviamo che a è algebrico di grado n . Si consideri il polinomio $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$; in quanto polinomio a coefficienti in un campo, $f(x)$ sarà prodotto di irriducibili e, dato che a è radice di $f(x)$, a sarà radice di qualche polinomio irriducibile su \mathbb{Z}_p , sia esso $p(x)$. Allora $\mathbb{Z}_p(a) \cong \mathbb{Z}_p[x]/(p(x))$, e dato che $\mathbb{Z}_p(a) = K$ possiede p^n elementi, vuol dire che il polinomio $p(x)$ ha grado n .

6.3.3 Un tale campo K esiste perché $25 = 5^2$. Si può pensare come campo di spezzamento su \mathbb{Z}_5 del polinomio $x^{25} - x$ (cfr. teorema 6.3.11) oppure (cfr. esercizio 6.3.2) si può pensare come $\mathbb{Z}_5[x]/(p(x))$, $p(x)$ polinomio irriducibile di grado 2 su \mathbb{Z}_5 . Un tale polinomio è ad esempio $p(x) = x^2 + 3$. Allora $K = \{a + b\alpha \mid a, b \in \mathbb{Z}_5, \alpha^2 = -3 = 2\}$. Gli elementi di K sono quindi $0, 1, 2, 3, 4, \alpha, 2\alpha, 3\alpha, 4\alpha, 1 + \alpha, 1 + 2\alpha, 1 + 3\alpha, 1 + 4\alpha, 2 + \alpha, 2 + 2\alpha, 2 + 3\alpha, 2 + 4\alpha, 3 + \alpha, 3 + 2\alpha, 3 + 3\alpha, 3 + 4\alpha, 4 + \alpha, 4 + 2\alpha, 4 + 3\alpha, 4 + 4\alpha$.

Non è difficile vedere (con un po' di tentativi) che $2 + \alpha$ è generatore di K^* . Quindi $K = \mathbb{Z}_5(2 + \alpha)$.

6.3.4 Risulta $K \supset F \supset \mathbb{Z}_p$. Ora, $n = [K : \mathbb{Z}_p] = [K : F][F : \mathbb{Z}_p]$, quindi $[F : \mathbb{Z}_p] = k \mid n$, da cui $|F| = p^k$ con $k \mid n$. Viceversa, proviamo che per ogni divisore k di n esiste ed è unico un sottocampo F di K con p^k elementi. Se esiste un tale campo F , ogni elemento di F soddisfa il polinomio $f(x) = x^{p^k} - x$, e $f(x)$ possiede al più p^k radici in K : quindi, se un tale F esiste, è necessariamente unico. D'altra parte l'insieme F di tutte le radici di $f(x)$ è un sottocampo con p^k elementi ed è contenuto in K : infatti ogni radice di $f(x)$ dentro il suo campo di spezzamento L è anche radice di $x^{p^n} - x$ (perché?); ora, K è campo di spezzamento per $x^{p^n} - x$, quindi tutte le radici di $f(x)$ stanno in K , da cui $F \subseteq K$.

6.3.5 Un campo di ordine $32 = 2^5$ contiene un sottocampo di ordine 2 (ossia \mathbb{Z}_2) e uno di ordine 32 (ossia l'intero campo). Un campo di ordine $125 = 5^3$ contiene un sottocampo di ordine 5 (cioè \mathbb{Z}_5), e l'intero campo. Un campo di ordine $15625 = 5^6$ contiene un sottocampo di ordine 5 (cioè \mathbb{Z}_5), uno di ordine 5^2 , uno di ordine $125 = 5^3$ e l'intero campo.

6.4.1 Dividendo $x^n - 1$ per $x^m - 1$ si ottiene: $x^n - 1 = (x^m - 1)(x^{n-m} + x^{n-2m} + \dots + x^{n-km}) + x^{n-km} - 1$, dove k è il più grande intero positivo tale che $n - km \geq 0$. Se $t > 1$ è un intero tale che t^{m-1} divide t^{n-1} , deve essere $n = km$ per qualche $k \in \mathbb{N}$.

6.5.1 Sì; sì; no.

6.5.2 (a) Il polinomio minimo è $x^2 + x + 1$. I coniugati sono le due radici del polinomio, cioè $(-1 \pm \sqrt{3}i)/2$.

(b) In generale, se ζ è una radice n -esima primitiva dell'unità, il suo polinomio minimo è l' n -esimo polinomio ciclotomico, quindi i coniugati di ζ sono

tutte le radici n -esime primitive dell'unità, ossia le ζ^k , con $1 \leq k \leq n-1$, $(n, k) = 1$. Quindi, nel caso $n = 8$, ...

- 6.6.1 Basta provare che $\sqrt{2}$ e $\sqrt{3}$ si possono scrivere come combinazione a coefficienti in \mathbb{Q} della base $1, \sqrt{2} + \sqrt{3}, (\sqrt{2} + \sqrt{3})^2, (\sqrt{2} + \sqrt{3})^3$. Infatti $\sqrt{2} = -\frac{9}{2}(\sqrt{2} + \sqrt{3}) + \frac{1}{2}(\sqrt{2} + \sqrt{3})^3$, da cui si ricava anche $\sqrt{3} = (\sqrt{2} + \sqrt{3}) - \sqrt{2} = \frac{11}{2}(\sqrt{2} - \sqrt{3}) - \frac{1}{2}(\sqrt{2} + \sqrt{3})^3$.
- 6.6.2 Si noti che la dimostrazione data per la caratteristica zero non vale in questo caso. Ma nel caso finito basta ricordare che il gruppo moltiplicativo del campo è ciclico. Si conclude.
- 6.6.3 Sia $|F| = p^k$ e sia K il campo di spezzamento del polinomio $x^{p^kn} - x$. Risulta $F \subseteq K$ (basta osservare che ogni $a \in F$ è tale che $a^{p^k} = a$ e quindi soddisfa anche la relazione $a^{p^{kn}} = a$). Ma allora $K = F(\alpha)$ per un opportuno $\alpha \in K$ (cfr. esercizio 6.6.2). Sia $p(x)$ il polinomio minimo di α su F . Allora $p(x)$ è irriducibile e il grado di $p(x)$ è proprio $n = [F(\alpha) : F]$.

Capitolo 7

- 7.1.2 Se entrambi $\alpha + \beta$ e $\alpha\beta$ fossero algebrici, allora α e β risulterebbero radici dell'equazione $x^2 - (\alpha + \beta)x + \alpha\beta$ a coefficienti algebrici, e allora α e β sarebbero algebrici.
- 7.2.2 Sia σ un automorfismo di \mathbb{R} , e siano $a, b \in \mathbb{R}$ tali che $a < b$. Allora $\sigma(a) < \sigma(b)$ (quale proprietà di un automorfismo si sfrutta?), ossia ogni automorfismo di \mathbb{R} conserva l'ordinamento. Supponiamo per assurdo che esista $a \in \mathbb{R}$ tale che $\sigma(a) > a$. Detto q un numero razionale, sicuramente esistente, tale che $\sigma(a) > q > a$, si ha $\sigma(q) = q$. Ma allora si ha una contraddizione, perché $q > a$ ma $\sigma(a) > \sigma(q) = q$.
- 7.2.3 $G(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}) = \{e\}$, e il suo campo fissato è $\mathbb{Q}(\sqrt[3]{2})$. Si noti invece che $I(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q})$ possiede tre elementi.
- 7.3.1 $x^3 + 2x^2 + 5x + 10$. Campo di spezzamento $K = \mathbb{Q}(\sqrt{5}i)$. $G(K, \mathbb{Q}) \cong \mathbb{Z}_2$.
 $x^4 - 7x^2 + 10$. $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. $G(K, \mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
 $x^5 + 2x^4 - 5x^3 - 10x^2 + 6x + 12$. $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. $G(K, \mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
 $x^3 - 1$. $K = \mathbb{Q}(\zeta)$. $\zeta = (-1 + \sqrt{3}i)/2$ radice terza primitiva dell'unità. $G(K, \mathbb{Q}) \cong \mathbb{Z}_2$.
 $x^3 - 7$. $K = (\sqrt[3]{7}, \zeta)$, ζ radice terza primitiva dell'unità. $G(K, \mathbb{Q}) \cong S_3$.
 $x^4 - 5$. $K = \mathbb{Q}(\sqrt[4]{5}, i)$. $G(K, \mathbb{Q}) \cong D_4$ (gruppo delle simmetrie di un quadrato).
- $x^4 - 4x^2 + 2$. $K = \mathbb{Q}(\sqrt{2 + \sqrt{2}})$. $G(K, \mathbb{Q}) \cong \mathbb{Z}_4$.
- 7.3.2 $x^6 + x^4 = 4x^2 - 4 = (x^2 + 2)(x^2 - 2)(x^2 + 1)$. Le sue radici sono $\pm\sqrt{2}$, $\pm i$. Il suo campo di spezzamento è $K = \mathbb{Q}(\sqrt{2}, i)$. Si ha $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$ poiché $i \notin \mathbb{Q}(\sqrt{2})$ (quindi il grado è > 1 , ma ≤ 2 perché i è radice di $x^2 + 1$). In conclusione, $[K : \mathbb{Q}] = 4$, e $G(K, \mathbb{Q}) = \langle i \rangle$. Una base di K su \mathbb{Q} è data da $1, i, \sqrt{2}, i\sqrt{2}$. Ogni $\sigma \in G(K, \mathbb{Q})$ è determinato dalle immagini di i e di $\sqrt{2}$. $\sigma(i)$ può essere $\pm i$, $\sigma(\sqrt{2})$ può essere $\pm\sqrt{2}$. In definitiva si hanno 4 automorfismi: oltre

all'automorfismo identico,

$$\begin{aligned}\sigma_1 : i &\mapsto -i, & \sqrt{2} &\mapsto \sqrt{2} \\ \sigma_2 : i &\mapsto i, & \sqrt{2} &\mapsto -\sqrt{2} \\ \sigma_3 : i &\mapsto -i, & \sqrt{2} &\mapsto -\sqrt{2}.\end{aligned}$$

Sono tutti di periodo 2 (salvo l'automorfismo identico). Quindi $G(K, \mathbb{Q}) \cong V$ (gruppo di Klein). Per il teorema di corrispondenza di Galois, i sottocampi di K sono tutti e soli i campi fissati dai sottogruppi di $G(K, \mathbb{Q})$. Ad esempio, il campo fissato da σ_3 è $\mathbb{Q}(i\sqrt{2})$: basta imporre $a + bi = c\sqrt{2} + di\sqrt{2} = \sigma_3(a + bi + c\sqrt{2} + di\sqrt{2}) = a - bi - c\sqrt{2} + di\sqrt{2}$. Si ricordi che $1, i, \sqrt{2}, i\sqrt{2}$ sono linearmente indipendenti, per ottenere il risultato. Gli altri sottocampi sono $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, oltre naturalmente a K e \mathbb{Q} .

7.3.4

 \mathbb{Z}_2 .

7.3.5 Il polinomio minimo di i su \mathbb{Q} è $x^2 + 1$. $\sigma(i) = \pm i$. Essendo il polinomio minimo di $\sqrt[3]{5}x^3 - 5$, $\sigma(\sqrt[3]{5})$ deve essere una radice di $x^3 - 5$: le radici di $x^3 - 5$ sono $\sqrt[3]{5}$ e $\frac{1}{2}(-1 \pm i\sqrt{3})\sqrt[3]{5}$. Queste ultime non appartengono a K , altrimenti anche $\sqrt[3]{3}$ apparterrebbe a K . Quindi $\sigma(\sqrt[3]{5}) = \sqrt[3]{5}$. Esistono al massimo due automorfismi: quello che manda i in i e $\sqrt[3]{5}$ in $\sqrt[3]{5}$ (ossia l'automorfismo identico) e l'automorfismo σ_2 che manda i in $-i$ e $\sqrt[3]{5}$ in $\sqrt[3]{5}$: queste condizioni determinano effettivamente un automorfismo di K che manda ogni elemento di $K = \{q_0 + q_1\sqrt[3]{5} + q_2(\sqrt[3]{5})^2 + q_3i + q_4i\sqrt[3]{5} + q_5i(\sqrt[3]{5})^2\}$ nel complesso coniugato. Quindi $G(K, \mathbb{Q}) \cong \mathbb{Z}_2$. L'estensione non è galoiana (il gruppo di Galois dell'estensione ha grado 2, mentre l'estensione ha grado 6).

7.3.7 Si tratta del gruppo ciclico di ordine 5. I suoi elementi sono i cinque automorfismi σ_i , $i = 0, \dots, 4$, dove $\sigma_i(\sqrt[3]{5}) = \zeta^i \sqrt[3]{5}$.

7.3.8 $x^4 + 1$ è irriducibile su \mathbb{Q} . I suoi zeri in \mathbb{C} sono $(1 \pm i)/\sqrt{2}$ e $(-1 \pm i)/\sqrt{2}$. Il campo di spezzamento di $x^4 + 1$ è $K = \mathbb{Q}(\frac{1+i}{\sqrt{2}})$ (infatti, posto $a = (1+i)/\sqrt{2}$, tutte le altre radici sono potenze di questa). Quindi $[K : \mathbb{Q}] = 4$. $G(K, \mathbb{Q}) \cong U(\mathbb{Z}_8) = \{\bar{1}_8, \bar{3}_8, \bar{5}_8, \bar{7}_8\}$ rispetto alla moltiplicazione modulo 8. Il campo di spezzamento di $x^3 - 1$ coincide con il campo di spezzamento di $x^4 + 1$.

7.3.9 Il campo di spezzamento di $x^5 - 1$ su \mathbb{Q} è $K = \mathbb{Q}(\zeta)$, dove ζ una radice quinta primitiva dell'unità. Il polinomio minimo soddisfatto da ζ è $x^4 - x^3 + x^2 + x + 1$. Il gruppo di Galois $G(K, \mathbb{Q})$ è isomorfo a \mathbb{Z}_4 , ed è generato dall'automorfismo σ che manda ζ in ζ^2 . L'unico sottogruppo di ordine 2 H di $G(K, \mathbb{Q})$ è il sottogruppo generato da σ^2 . Il sottocampo di $\mathbb{Q}(\zeta)$ fissato da H è $K_H = \mathbb{Q}(\zeta^2 + \zeta^3)$. Il polinomio minimo di $\zeta^2 - \zeta^3$ è $x^2 + x - 1$. Le radici di questo polinomio sono $(-1 \pm \sqrt{5})/2$, quindi $K_H = \mathbb{Q}(\sqrt{5})$. Il polinomio minimo di ζ su K_H è $x^2 + (\zeta^3 + \zeta^2 + 1)x + 1$. Si deduce allora per ζ l'espressione $\zeta = (-1 + \sqrt{5})/4 - \frac{1}{2}i\sqrt{(5 + \sqrt{5})/2}$.

7.3.10 $G(K, T_1(T_2))$ consiste di tutti gli automorfismi di K che fissano gli elementi di $T_1(T_2)$, quindi fisseranno sia gli elementi di T_1 , sia gli elementi di T_2 . Allora $G(K, T_1(T_2)) \subseteq H_1 \cap H_2$. Viceversa, se $\sigma \in H_1 \cap H_2$, lasciando fissi gli elementi di T_1 e gli elementi di T_2 , lascerà fissi gli elementi di $T_1(T_2)$, quindi $H_1 \cap H_2 \subseteq G(K, T_1(T_2))$ e vale l'uguaglianza.

Sia ora $\sigma \in \langle H_1, H_2 \rangle$. È ovvio che σ fissa gli elementi di $T_1 \cap T_2$, quindi $\langle H_1, H_2 \rangle \subseteq G(K, T_1 \cap T_2)$. Viceversa, sia $k \in K$, $k \notin T_1 \cap T_2$: supponiamo $k \notin T_1$. Dato che $T_1 = K_{H_1}$, esiste almeno un elemento $\sigma \in H_1$ tale che $\sigma(k) \neq k$, e quindi k non è lasciato fisso da $H_1 \cap H_2$. Quindi $K_{\langle H_1, H_2 \rangle} \subseteq T_1 \cap T_2$. In definitiva $K_{\langle H_1, H_2 \rangle} = T_1 \cap T_2$. Quindi (per la corrispondenza di Galois), $\langle H_1, H_2 \rangle = G(K, T_1 \cap T_2)$.

- 7.3.11 $[\varphi(K) : F] = [K : F]$ e quindi $\varphi(K) = K$.
- 7.4.2 Il campo di spezzamento K su \mathbb{R} di un polinomio a coefficienti in \mathbb{R} o è \mathbb{R} o è \mathbb{C} . Quindi il suo gruppo di Galois ha ordine 1 o 2. In ogni caso è abeliano e quindi risolubile.
- 7.4.3 Sia G un gruppo finito di ordine n . Allora G è isomorfo (teorema di Cayley) ad un sottogruppo di S_n . S_n è il gruppo di Galois di $F(x_1, x_2, \dots, x_n)$ sul sottocampo S delle funzioni razionali simmetriche. Concludere sfruttando il teorema di Corrispondenza di Galois.

Soluzioni esercizi riassuntivi

1. Se $|G| = 12$, esiste (teorema di Sylow) un sottogruppo H di ordine 4. Allora $t(H)| = 6$, e $|G| \nmid 6$, quindi ...
2. $\pi^2 - 1$ è trascendente su \mathbb{Q} (se fosse algebrico, tale sarebbe anche π^2 e anche la sua radice quadrata, cioè π). È invece algebrico su $\mathbb{Q}(\pi^3)$. Infatti, posto $\alpha = \pi^2 - 1$, dalla $\alpha + 1 = \pi^2$, elevando al cubo, si ha: $\alpha^3 + 3\alpha^2 + 3\alpha + 1 = \pi^6$. Quindi α soddisfa il polinomio $x^3 + 3x^2 + 3x + 1 - \pi^6$, che è a coefficienti in $\mathbb{Q}(\pi^3)$, perché $1 - \pi^6 = (1 - \pi^3)(1 + \pi^3)$.
3. C'è solamente l'omomorfismo nullo. Infatti gli elementi di G hanno tutti periodo finito, e in un omomorfismo vengono mandati in elementi di periodo finito. L'unico elemento di periodo finito di \mathbb{Z} è lo zero.
4. È compatibile rispetto all'addizione, ma non rispetta alla moltiplicazione. Infatti se $x \equiv x'$ (ossia $x = x' + hr$), $y \equiv y'$ (ossia $y = y' + kr$), $h, k \in \mathbb{Z}$, $r \in \mathbb{R}$, risulta $xy = x'y' + (hy' + kx' + hkr)r$, e in genere $hy' + kx' + hkr \notin \mathbb{Z}$. Ad esempio se $r = \pi$, $\frac{\pi}{2} = -\frac{\pi}{2} + 1 \cdot \pi$, $\pi = 0 + 1 \cdot \pi$, ma $\pi^2/2 \not\equiv 0 \pmod{\pi}$.
5. Sia $|K| = p^n$. Supponiamo $p \neq 2$. Fissato $\alpha \in K$, poniamo $A = \{\alpha - x^2 \mid x \in K\}$ e $B = \{z^2 \mid z \in K\}$. Risulta $|A| = |B| = (p^n - 1)/2$, per cui esisterà un elemento che sta contemporaneamente in A e in B : ne segue che $\alpha = x^2 + z^2$ per qualche $x, z \in K$.
Se $p = 2$, l'applicazione $\Phi(x) = x^2$ di F in sé è biunivoca, quindi per ogni $\alpha \in K$ esiste un $x \in K$ tale che $\alpha = x^2$.
6. No, non si può concludere che G non è ciclico, perché in un gruppo ciclico di ordine 100 i generatori sono in numero di $\varphi(100) = 40$, quindi i 40 generatori potrebbero trovarsi tra gli altri 50.
7. Il periodo di g deve essere 8. Infatti essendo $g^{12} \neq 1$, g , vengono esclusi per g i periodi 1, 2, 3, 4, 6, e 12. Essendo poi il gruppo non abeliano, non può essere il periodo 24 (altrimenti il gruppo sarebbe ciclico). L'unica possibilità è quindi 8.
8. Solo la condizione (a).

9. Per induzione sull'ordine del gruppo. Per $|G| = 1$ il risultato è vero. Supponiamo vero il risultato per ogni p -gruppo con ordine $< |G|$. Sappiamo che $Z(G) \neq \{e\}$ ed è risolubile essendo abeliano. $G/Z(G)$ ha ordine $< |G|$, quindi è risolubile per ipotesi. Allora G è tale che contiene un sottogruppo normale $Z(G)$ risolubile e $G/Z(G)$ risolubile: allora è risolubile (cfr. esercizio 5.15.4).
10. \mathbb{Q}/\mathbb{Z} .
11. Siano a_1, a_2, \dots, a_n gli elementi del gruppo. Il gruppo sarà completamente determinato dalla sua tavola di moltiplicazione, ed è chiaro che il numero di tabelle distinte che si possono costruire con gli n elementi a_1, a_2, \dots, a_n sono n^{n^2} . Ovviamente la maggior parte delle tabelle che si possono costruire non forniscono la tavola di moltiplicazione di un gruppo: perché?
12. C'è solamente l'omomorfismo nullo e l'omomorfismo identico.
13. $\mathbb{Q}(\pi^2)$.
14. Il gruppo di Galois di $x^r - 1$ è $U(\mathbb{Z}_r)$, il gruppo di Galois di $x^s - 1$ è $U(\mathbb{Z}_s)$, il gruppo di Galois di $x^{rs} - 1$ è $U(\mathbb{Z}_{rs})$ e $U(\mathbb{Z}_{rs}) \cong U(\mathbb{Z}_r) \times U(\mathbb{Z}_s)$.
15. $91 = 13 \cdot 7$, quindi il minimo n cercato è $n = 13 + 7 = 20$. Così, nel secondo caso il minimo n è $n = 40$. In generale, il più piccolo intero positivo n tale che S_n contenga un elemento di ordine pq , p, q primi è $p + q$. Infatti ricordiamo che l'ordine di un elemento σ di un gruppo simmetrico è dato dal mem delle lunghezze dei suoi cicli disgiunti. Se vogliamo che l'ordine di σ sia pq , il minimo numero di simboli con cui possiamo realizzare un elemento di ordine pq è $p + q$, quando cioè σ è prodotto di un p -ciclo e un q -ciclo disgiunti.
16. Se b è algebrico su F , anche $a = b^n$ è algebrico su F , in quanto prodotto di elementi algebrici (potenza di un elemento algebrico). Viceversa, se a è algebrico su F , anche b è algebrico su F , in quanto radice di un polinomio, $x^n - a$, a coefficienti algebrici.
17. (a) Dati comunque $x, y \in R$, $(x+y)^2 = (x-y)(x+y) = x - xy + yx + y$ (perché?). Dato che anche $(x+y)^2 = x+y$, si ha $xy - yx = 0$. Per $x = y$ si ottiene $x + x = 0$, quindi $xy + yx = 0$ che, assieme alla $xy - yx = 0$ di prima, implica $xy = yx$ per ogni $x, y \in R$ e quindi R è commutativo.
- (b) Supponiamo che R (booleano) contenga più di due elementi: allora, dati comunque due elementi $a \neq 0, b \neq 0, a \neq b$, si ha $ab(a+b) = ab + ba = 0$. Se $b(a+b)$ è diverso da zero, allora a è un divisore dello zero, mentre se $b(a+b) = 0$, allora è b ad essere divisore dello zero perché $a + b \neq a + a = 0$. Abbiamo così provato che ogni anello booleano con almeno tre elementi non è mai un dominio d'integrità.
- (c) Sia P un ideale primo di R . Il quoziente R/P è un dominio d'integrità, che è ancora un anello booleano, perché la proprietà $x^2 = x$ si conserva per omomorfismo. Per quanto visto in (b), R/P contiene due elementi (essendo $R \neq P$, R/P non è ridotto al solo zero), siano essi P e $a+P$, $a \notin P$. Sia I un ideale di R contenente propriamente P , e sia $x \in I$, $x \notin P$. Allora la classe $x+P$ coincide con la classe $a+P$ e $I = R$, per cui P è massimale.
18. \mathbb{Z}_p è sicuramente contenuto nel campo fissato da σ_p , il quale a sua volta coincide con l'insieme delle radici del polinomio $x^p - x$. Quindi ...

19. $G(K, F)$ è un gruppo di ordine 6, e in quanto tale è isomorfo a \mathbb{Z}_6 o a S_3 . In entrambi i casi esiste un solo sottogruppo normale di indice 2. Il risultato segue per il teorema di corrispondenza di Galois.
20. Ricordiamo che se $f(x)$ è un polinomio $\in F[x]$ di grado n e K è il suo campo di spezzamento, allora $G(K, F)$ è un sottogruppo di S_n . Inoltre $|G(K, F)| = [K : F] \leq n!$. Supponiamo $p(x)$ riducibile. Allora si spezzerà nel prodotto di due polinomi di secondo grado. Nel primo caso il campo di spezzamento K avrà grado su \mathbb{Q} minore o uguale a $3! = 6$, nel secondo caso $[K : \mathbb{Q}] \leq 4$. In ogni caso si arriva ad una contraddizione.
21. $\mathbb{Z}_5[x]/(x^3 + 2x + 1)$.

Dati anagrafici degli autori citati nel testo

- ABEL, Niels Henrik, n. Findo 1802, m. Froland 1829.
- AL-KROWARITZMI,¹ Muhammad ibn Musà, n. Bagdad, m. a metà del 9^o secolo.
- BÉZOUT, Étienne, n. Nemours 1730, m. Fontainebleau 1783.
- BOMBELLI, Raffaele, n. Borgopanigale (Bologna) ~ 1526, m. ~ 1572.
- BOOLE, George, n. Lincoln 1815, m. Cork 1864.
- BURNSIDE, William, n. Londra 1852, m. West Wickham (Kent) 1927.
- CANTOR, Georg, n. Pietroburgo 1845, m. Halle 1918.
- CARDANO, Gerolamo, n. Pavia 1501, m. Roma 1576.
- CAUCHY, Augustin Louis, n. Parigi 1789, m. Sceaux, Seine 1857.
- CAYLEY, Arthur, n. Richmond (Surrey) 1821, m. Cambridge 1895.
- DAL FERRO, Scipione, n. Bologna 1465, m. Bologna 1526.
- DIOFANTO (*Διοφαντος*) di Alessandria ~ 250.
- EISENSTEIN, Ferdinand Gotthold Max, n. Berlino 1823, m. Berlino 1852.
- ERATOSTENE, 276-194 a.C.
- EUCLIDE di Alessandria, ~ 350 a.C.
- ETTLERO, Leonhard, n. Basilea 1707, m. Pietroburgo 1783.
- FERRARI, Lodovico, n. Bologna 1522, m. 1565.
- FERMAT, Pierre de, n. Beaumont de Lomagne 1601, m. Castres 1665.
- FIBONACCI, Leonardo (detto Leonardo Pisano), n. Pisa ~ 1175, m. 1235.
- FONTANA, Niccolò (detto Tartaglia), n. Brescia ~ 1499, m. Venezia 1557.
- FROBENIUS, Georg Ferdinand, n. Berlino 1849, m. Charlottenburg 1917.
- GALOIS, Evariste, n. Bourg-la-Reine 1811, m. Parigi 1832.
- GAUSS, Karl Friedrich, n. Brunswick 1777, m. Gottinga 1855.

¹ Ha dato luogo alla parola "algoritmo".

- HAMILTON, William Rowan, Dublino 1805, m. Dublino 1865.
- HERMITE, Charles, n. Dieuze (Lorena) 1822, m. Parigi 1901.
- IPAZIA² ($\Upsilon\piατια$), n. Alessandria d'Egitto 375 (?), m. ivi 415 d.C.
- KLEIN, Felix, n. Dusseldorf 1849, m. Gottinga 1925.
- KRONECKER, Leopold, n. Liegnitz 1823, m. Berlino 1891.
- LAGRANGE, Giuseppe Luigi, n. Torino 1736, m. Parigi 1813.
- LINDEMANN, Ferdinand von, n. Hannover 1852, m. Monaco di Baviera 1939.
- MOIVRE, Abraham de, n. Vitry, Champagne 1667, m. Londra 1754.
- PASCAL, Blaise, n. Clermont-Ferrand 1623, m. Parigi 1662.
- PEANO, Giuseppe, n. Cuneo 1858, m. Torino 1932.
- PELL, John, n. Southwick, Sussex 1611, m. Londra 1685.
- PITAGORA, n. Samo, VI sec. a.C.
- PLATONE, n. Atene 427 a.C., m. Atene 347 a.C.
- RUFFINI, Paolo, n. Valentano (Viterbo) 1765, m. Modena 1822.
- SYLOW, Peter Ludvig Mejdell, n. Cristiania (Oslo) 1832, m. ivi 1918.
- TALETE di Mileto, n. ~ 624-23, m. ~ 548-45 a.C.
- VIÈTE, François, n. Fontenay-le-Comte 1540, m. Parigi 1603.
- WILSON, John, n. Applethwaite, Westmorland 1741, m. Kendal 1793.
- ZERMELO, Ernst, n. Berlino 1871, m. Friburgo (Brisgovia) 1953.

²La prima donna matematica.

Bibliografia

- [1] I.T. Adamson. *Introduction to Field Theory*. Oliver & Boyd, Edinburgh. 1964.
- [2] R.B.J.T. Allenby. *Rings, Fields and Groups. An Introduction to Abstract Algebra*. Edward Arnold, 1983.
- [3] M.A. Armstrong. *Groups and Symmetry*. Undergraduate Texts in Mathematics. Springer Verlag. 1988.
- [4] L.C. Grove, C.T. Benson. *Finite Reflection Groups*. Graduate texts in Mathematics. Springer Verlag, 1985.
- [5] P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul. *Basic Abstract Algebra*. Cambridge University Press. 1986.
- [6] G. Birkhoff, S. Mac Lane. *A Survey of Modern Algebra*. Macmillan Company. 1953.
- [7] N.J. Bloch. *Abstract Algebra with Applications*. Prentice-Hall, Inc.. 1987.
- [8] R. Bombelli. *L'Algebra*. Feltrinelli, Milano. 1966. Introduzione di U. Forti. Prefazione di E. Bortolotti.
- [9] R.P. Burn. *A pathway into number theory*. Cambridge University Press. 1982.
- [10] D.M. Burton. *Elementary Number Theory*. Allyn & Bacon. Boston. 1980.
- [11] L. Childs. *A Concrete Introduction to Higher Algebra*. Undergraduate Texts in Mathematics. Springer Verlag, 1988.
- [12] A. Clark. *Elements of Abstract Algebra*. Dover Publications, New York. 1971.
- [13] P.M. Cohn. *Algebra*. vol. I e vol. II. John Wiley & Sons. 1989.
- [14] M.H. Fenwick. *Introduction to the Galois Correspondence*. Birkhauser. 1991.
- [15] J.B. Fraleigh. *A first course in abstract algebra*. Addison-Wesley. Reading. 1967.
- [16] L. Gaal. *Classical Galois Theory with examples*. Chelsea Publishing Company. New York. 1979.
- [17] J.A. Gallian. *Contemporary Abstract Algebra*. D.C. Heath and Company. 1986.
- [18] L. Gårding, T. Tambour. *Algebra for computer science*. Universitext. Springer Verlag. 1988.
- [19] L.J. Goldstein. *Abstract Algebra: a first course*. Prentice-Hall, New Jersey. 1973.
- [20] R.H. Graham, D.E. Knuth, O. Patashnik. *Concrete Mathematics*. Addison-Wesley Publishing Company, second edition. 1994.

- [21] E. Grosswald. *Representations of Integers as Sums of Squares*. Springer Verlag, 1985.
- [22] C.R. Hadlock. *Field Theory and its Classical Problems*. The Carus Mathematical Monographs 19, Mathematical Association of America, Washington DC, 1978.
- [23] G.H. Hardy, E.M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, Oxford, 1979.
- [24] I.N. Herstein. *Algebra*. Editori Riuniti, 1982.
- [25] N. Jacobson. *Basic Algebra*, vol. I e vol. II. W.H. Freeman and Company, San Francisco, 1974.
- [26] K. Kaftmann. *An Introduction to Discrete Mathematics and its Applications*. Addison Wesley, 1986.
- [27] D.E. Knuth. *The Art of Computer Programming*, Vols. I, 2. Addison-Wesley, 1974, 1981.
- [28] A. Kurosh. *Cours d'Algèbre Supérieure*. Éditions MIR de Moscou, 1973.
- [29] R. Lidl, G. Pilz. *Applied Abstract Algebra*. Undergraduated texts in mathematics. Springer Verlag, 1984.
- [30] L. Lombardo Radice. *Istituzioni di Algebra Astratta*. Feltrinelli, 1965.
- [31] U. Manber. *Introduction to Algorithms. A Creative Approach*. Addison-Wesley, 1989.
- [32] N.H. McCoy. *Introduction to Modern Algebra*. Allyn & Bacon, 1966.
- [33] I. Niven. A simple proof that π is irrational. *Bulletin of the American Mathematical Society*, 53 (1947) p. 509.
- [34] C. Procesi. *Elementi di Teoria degli Anelli*. Decibel, Padova, 1978.
- [35] C. Procesi. *Elementi di Teoria dei Gruppi*. Decibel, Padova, 1976.
- [36] C. Procesi. *Elementi di Teoria di Galois*. Decibel, Padova, 1977.
- [37] P. Ribenboim. *The book of prime number records*. Universitext, Springer Verlag, 1989.
- [38] K.H. Rosen. *Discrete Mathematics and its Applications*. McGraw-Hill, 1995.
- [39] J. Rotman. *Galois Theory*. Universitext, Springer Verlag, 1990.
- [40] D. Schattschneider. The plane symmetry groups: their recognition and notation. *American Mathematical Monthly*, 1978.
- [41] M.R. Schroeder. *Number Theory in Science and Communication*. Springer Verlag, 1990.
- [42] L. Shapiro. *Introduction to Abstract Algebra*. McGraw-Hill, 1973.
- [43] C.C. Sims. *Abstract Algebra. A computational approach*. John Wiley & Sons, 1984.
- [44] K. Spindler. *Algebra with applications*, vol. I e vol. II. Marcel Dekker, 1994.
- [45] D. Stautou, D. White. *Constructive combinatorics*. Springer Verlag, 1986.
- [46] I. Stewart. *Galois Theory*. Chapman & Hall, London-New York, 1989.
- [47] B.L. Van Der Waerden. *Modern Algebra*. Ungar, New York, 1953.

Indice dei simboli

ϵ , 7	$[a]$, 14
\notin , 8	\bar{a} , 14
\emptyset , 8	A/ρ , 15
\subseteq , 8	$f : A \rightarrow B$, 18
\subset , 8	$f(S)$, 19
\subsetneq , 8	$\operatorname{Im} f$, 19
\mathbb{N} , 8, 23	$f^{-1}(T)$, 19
\mathbb{Z} , 8, 42	$g \circ f$, 19
\mathbb{Q} , 8, 56	$f^{-1}(b)$, 20
\mathbb{R} , 8	i_X , 20
\mathbb{C} , 8, 104	2^X , 20
\forall , 8	χ_A , 20
\exists , 8	g_f , 21
$\exists!$, 8	$A \sim B$, 31
\nsubseteq , 8	$\operatorname{Card}(A)$, 31
$\exists!$, 8	\aleph_0 , 31
\Rightarrow , 8	$n!$, 36
\Rightarrow , 8	$S(X)$, 37
\Leftrightarrow , 8	$\binom{n}{k}$, 38
\Leftrightarrow , 8	\mathbb{Z}^+ , 42
$ $, 8	\mathbb{Z}^- , 42
$A \cap B$, 9	$[a]$, 44
$A \cup B$, 9	$a \mid b$, 44
$\bigcup_{\alpha \in \mathcal{X}} A_\alpha$, 9	$a \nmid b$, 44
$\bigcap_{\alpha \in \mathcal{X}} A_\alpha$, 9	$\operatorname{MCD}(a, b)$, 47
\mathcal{CA} , 9	(a, b) , 47
$B \sim A$, 9	$\operatorname{lcm}(a, b)$, 54
$A \times B$, 10	$[a, b]$, 54
$\mathcal{P}(A)$, 10	F_n , 59
$a \varrho b$, 12	Φ , 63
$a \varrho^{-1} b$, 13	$\hat{\Phi}$, 63

- $=$, 65
- \mathbb{Z}_n , 68
- $\varphi(n)$, 85
- $U(\mathbb{R})$, 88
- $U(\mathbb{Z}_n)$, 88
- N_n , 93
- $z\bar{z}$, 105
- $|z|$, 105
- $h_{n,k}$, 107
- \mathbb{K} , 109
- $\mathbb{K}[x]$, 111
- $\deg p(x)$, 112
- $\partial p(x)$, 112
- MCD($f(x), g(x)$), 116
- Δ , 121, 141
- $\Phi_n(x)$, 133
- $\Delta(x_1, x_2, \dots, x_n)$, 150
- $R_1 \oplus R_2$, 153
- \simeq , 153, 242
- $\text{End}(A)$, 157
- $\text{Ker } \varphi$, 159, 246
- $I \leq R$, 160
- R/I , 164
- $I + J$, 165
- IJ , 165
- (a_1, a_2, \dots, a_m) , 172
- $Q(D)$, 178
- $\mathbb{Z}[i]$, 181
- $v(a+ib)$, 181
- $\mathbb{Z}[a]$, 185
- $d(f(x))$, 190
- $N(a+b\sqrt{d})$, 197
- $\text{char } F$, 201
- $M_{nn}(R)$, 207
- $M_n(R)$, 207
- $GL_n(\mathbb{R})$, 207
- $SL_n(\mathbb{R})$, 207
- $O_n(\mathbb{R})$, 207
- $O_n(\mathbb{R})$, 207
- $SO_n(\mathbb{R})$, 207
- $H < G$, 208
- $H \leq G$, 208
- $Z(G)$, 208
- $\langle X \rangle$, 209
- $\langle g \rangle$, 209
- $S(X)$, 212
- S_n , 217
- $\mathcal{O}_\sigma(x)$, 219
- A_n , 224
- D_n , 235
- $a \# b$, 238
- $a \circ b$, 238
- Ha , 238
- $(G : H)$, 240
- $\sigma(g)$, 241
- $H \trianglelefteq G$, 251
- H^π , 253
- G/N , 253
- $N_G(H)$, 256
- $\text{Aut}(G)$, 258
- $\mathbb{Z}(G)$, 259
- G' , 260, 290
- $g * x$, 264
- $\mathcal{O}(x)$, 265
- St_x , 267
- $C(x)$, 268
- c_x , 270
- X_g , 271
- $G_1 \times G_2$, 282
- $G_1 \times G_2 \times \dots \times G_k$, 285
- $G_1 \coprod_\Phi G_2$, 288
- $[x, y]$, 290
- Σ_p , 300
- $[K : F]$, 308
- $F(S)$, 310
- $F(S)$, 310
- \mathbb{A} , 316
- $\mathcal{I}(K, F)$, 348
- $G(K, F)$, 351
- K_G , 352
- $K_{G(K, F)}$, 353
- $G(K, T)$, 355
- K_H , 355

Indice analitico

F-automorfismo, 351

F-monomorfismo, 348

G-insieme, 265

p-gruppo, 275

A

Abel-Ruffini, teorema di, 371

abeliano, gruppo, 206

addizione, 151

affinità, 214

algebrica, struttura, 24

algebricamente chiuso, campo, 319

algebrico:

— ampliamento, 318

— elemento, 312

algoritmo:

— della divisione tra polinomi, 114

— di Euclide, 48

— euclideo delle divisioni successive, 48

alterno, sottogruppo, 221

ampliamento, 307

— algebrico, 318

— finito, 308

anello, 151

— commutativo, 154

— con unità, 154

— degli interi di Gauss, 180

— delle classi resto, 68

— principale, 174

— quoziente, 164

— unitario, 154

angolo, trisezione dell', 347

antisimmetrica, relazione, 16

appartenenza, 8

appartiene, 7

applicazione, 18

— composta, 19

— identica, 20

— inversa, 20

argomento di un numero complesso, 106

assonanza:

— della scelta, 35

— di Zermelo, 35

associati:

— interi, 45

— polinomi, 116

associativa, operazione, 205

aureo, rapporto, 62

automorfismo:

— di Frobenius, 334

— di un gruppo, 258

— interno, 259

azione di un gruppo su un insieme, 264

B

Bézout, identità di, 48

base:

— *b*, rappresentazione in, 100

— decimale, rappresentazione in, 99

billettiva, funzione, 19

binaria, operazione, 23

binomiale, coefficiente, 38

biunivoca, funzione, 19

buon ordinamento:

— principio del, 26

— teorema del, 35

Burnside, teorema di, 271

C

campo, 154, 307

— algebricamente chiuso, 319

— dei numeri algebrici, 316

— dei quozienti, 59, 178

— di spezzamento, 321

— finito, 329

— fissato, 352

cancellazione, leggi di, 46, 216

Cantor, procedimento diagonale di, 33

caratteristica:

— di un anello, 201

— funzione, 20

Cardano, formula di, 139

cardinalità, 31

— inferiore, 34

carte da parati, 296

cartesiano, prodotto, 10

Cassini, identità di, 60

casus irriducibilis, 141

catena, 16

Cauchy, teorema di, 274

Cayley:

— teorema di, 243

— teorema generalizzato di, 280

centralizzante, 268

centro di un gruppo, 208

cerchio, quadratura del, 347

chiave pubblica, sistema di crittografia, 94

chiusa, formula, 28

chiusura algebrica, 320

ciclico:

— gruppo, 211

— sottogruppo, 209

ciclo, 220

ciclotomia, 131

ciclotomico, polinomio, 133

circonferenza, rettificazione della, 347

classe:

— di equivalenza, 14

— laterale, 238

classi:

— coniugate, 229

— resto, anello delle, 68

— equazione delle, 270

codominio, 18

coefficiente:

— binomiale, 38

— direttivo, 112

commutatore, 290

— sottogruppo, 290

compatibile, relazione, 68

complemento, 9

— relativo, 9

complessi, numeri, 104

componente primaria, 301

composta, applicazione, 19

condizione iniziale, 27

congruenza:

— lineare, 75

— modulo n , 17

— relazione di, 67

coniugata, permutazione, 227

coniugati, elementi, 252

coniugato di un numero complesso, 105

contenuto, 122

— propriamente, 9

continuo:

— ipotesi del, 35

— ipotesi generalizzata del, 35

— potenza del, 34

controimmagine, 19

coprimi:

— interi, 47

— polinomi, 117

corpo, 154

— dei quaternioni, 334

corrispondenza, 12

— ben definita, 18

— di Galois, 359

— univoca, 18

costruibile, numero reale, 343

costruzione:

— con riga e compasso, 342

— euclidea, 342

- criterio:
 — di divisibilità, 72
 — di irriducibilità di Eisenstein, 126
- crittografia, 94
- crittologia, 93
- crivello di Eratostene, 91
- cubo, duplicazione del, 347
- D**
- de Moivre, formula di, 107
- decorazioni, 296
- derivata di un polinomio, 329
- derivato, sottogruppo, 260, 290
- diedrale, gruppo, 235
- direttivo, coefficiente, 112
- discriminante, 378
- dell'equazione cubica, 140
- dispari, permutazione, 222
- disuguaglianza triangolare, 106
- divisibilità, 44
- criterio di, 72
- divisione:
 — in \mathbb{Z} , 47
 — tra polinomi, 114
- divisore, 44, 122
- comune, 44
- dello zero, 44
- divisori elementari, 302
- dominio, 18
 — a fattorizzazione unica, 187
 — di integrità, 44, 154
 — euclideo, 180
 — principale, 182
- duplicazione del cubo, 347
- E**
- Eisenstein, criterio di irriducibilità di, 126
- elementi coniugati, 252
- elemento:
 — algebrico, 312
 — di un insieme, 7
 — invertibile, 45
 — neutro, 206
 — primitivo, 310
 — trascendente, 312
 — unità, 45
- endomorfismo di un gruppo abeliano, 137
- epimorfismo:
 — fra auelli, 158
 — tra gruppi, 246
- equazione:
 — delle classi, 270
 — di Pell, 199
- equipotenti, insiemi, 31
- equipotenza, 31
- equivalente, 13
- equivalenza, classe di, 14
- Eratostene, crivello di, 91
- essere contenuto, 8
- estensione, 307
 — di un isomorfismo, 325
 — finita, 308
 — galoisiana, 360
 — normale, 337
 — radicale, 368
 — semplice, 311
 — separabile, 339
- Euclide:
 — algoritmo di, 48
 — numeri di, 66
- euclideo, dominio, 180
- Eulero:
 — funzione di, 85
 — teorema di, 86
- F**
- fattoriale, 36
- fattorizzazione
 — di Fermat, 91
 — unica, 117
 — — dominio a, 187
- Fermat:
 — fattorizzazione di, 91
 — numero di, 93
 — piccolo teorema di, 70
- Fibonacci, numeri di, 59
- fibra, 21
- finita, estensione, 308
- finito, ampliamento, 308
- forma trigonometrica di un numero complesso, 106

formula:

- chiusa, 28
- di Cardano, 139
- di de Moivre, 107
- di Viète, 145
- Frobenius, automorfismo di, 334
- funzione, 18
 - biettiva, 19
 - biunivoca, 19
 - caratteristica, 20
 - di Eulero, 85
 - iniettiva, 19
 - polinomiale, 110
 - razionale, 148
 - razionale intera, 110
 - razionale simmetrica, 148
 - suriettiva, 19
 - simmetrica elementare, 145

G

Galois:

- corrispondenza di, 359
- gruppo di, 352
- teorema di corrispondenza di, 362

galoisiana, estensione, 360

Gauss:

- interi di, 180
 - lemma di, 123
- teorema di, 123

generatori di un ideale, 172

gioco della Torre di Hanoi, 29

grado:

- di un polinomio, 112
- di un'estensione, 308

grafico, 18

grafo, gruppo di, 214

gruppi delle decorazioni, 296

gruppo, 37, 152, 205

- abeliano, 206

- additivo, 152

- ciclico, 211

- cristallografico, 296

- di Galois, 352

- di Galois di un polinomio, 362

- di Klein, 233

- di trasformazioni, 213

- di un grafo, 214

- diedrale, 235
- puntuale, 296
- risolubile, 291
- semplice, 281
- simmetrico, 217

I

ideale:

- bilatero, 160
- destro, 160
- generato da un sottoinsieme, 172
- massimale, 171
- primo, 174
- principale, 174
- sinistro, 160

identica, applicazione, 20

identità:

- di Bézout, 48
- di Cassini, 60

immagine, 18, 19

- inversa, 19

indice di un sottogruppo, 240

induzione matematica, principio di, 22, 23

iniettiva, funzione, 19

insieme, 7

- bene ordinato, 26
- delle parti, 40
- differenza, 9
- finito, 31
- infinito, 31
- numerabile, 31
- parzialmente ordinato, 16
- quoziente, 15
- totalmente ordinato, 16
- vuoto, 8

insiemi equipotenti, 31

integrità, dominio di, 44, 154

interi:

- associati, 45
- coprimi, 47
- di Gauss, 180
- negativi, 42
- positivi, 42
- numeri, 41
- intersezione, 9
- invarianti, 302

inversa:

— applicazione, 20

— relazione, 13

inverso, elemento, 206

invertibile, polinomio, 115, 117

ipotesi:

— del continuo, 35

— generalizzata del continuo, 35

irriducibile:

— elemento, 45

— polinomio, 117

isometria, 213

isomorfismo:

— fra anelli, 153

— tra gruppi, 242

— primo teorema di, 262

— secondo teorema di, 170, 263

isotropia, sottogruppo di, 267

K

Klein, gruppo di, 233

L

Lagrange, teorema di, 240

leggi di cancellazione, 46, 216

lemma di Gauss, 123

lessicografico, ordinamento, 144

lunghezza di un ciclo, 220

M

massimale, ideale, 174

massimo comune divisore, 46, 116

matrice, 12

minimo comune multiplo, 54

minimo, principio del, 26

modulo di un numero complesso, 105

molteplicità di una radice, 118

moltiplicazione, 151

monomorfismo:

— fra anelli, 158

— tra gruppi, 246

movimento rigido, 213

multipla, radice, 118

N

naturali, numeri, 22

neutro, elemento, 206

nilpotente, elemento, 161

non appartiene, 7

norma:

— di un numero complesso, 105

— in $\mathbb{Z}[\sqrt{d}]$, 197

normale, sottogruppo, 251

normalizzante di un sottogruppo in un gruppo, 256

nucleo:

— di un omomorfismo fra anelli, 159

— di un omomorfismo tra gruppi, 246

numerabile, insieme, 31

numeri:

— complessi, 104

— di Euclide, 66

— di Fibonacci, 59

— interi, 41

— naturali, 22

— razionali, 55

numero:

— algebrico, 312

— cardinale, 31

— complesso, coniugato di, 105

— di Fermat, 93

— reale costruibile, 343

— trascendente, 312

O

omomorfismo:

— fra anelli, 158

— tra gruppi, 246

— valutazione, 313

operazione:

— associativa, 205

— binaria, 23

orbita, 219, 265

ordinamento lessicografico, 144

ordine:

— di un elemento, 210

— di un gruppo, 211

— di una radice n -esima dell'unità, 131

— parziale, relazione di, 16

P

pari, permutazione, 222

partizione, 15
 — di un intero, 231
 parzialmente ordinato, insieme, 16
 Pascal, triangolo di, 39
 Peano, postulati di, 22
 Pell, equazione di, 199
 periodo:
 — di un elemento, 210
 — di una radice n -esima dell'unità, 131
 permutazione, 37, 217
 — coniugata, 227
 — dispari, 222
 — pari, 222
 piccolo teorema di Fermat, 70
 poligono:
 — regolare, 373
 — costruibile, 373
 polinomi:
 — associati, 116
 — coprimi, 117
 — in n indeterminate, 143
 — irriducibili su \mathbb{C} , 120
 — irriducibili su \mathbb{Q} , 121
 — irriducibili su \mathbb{R} , 120
 — simmetrici elementari, 145
 polinomiale, funzione, 110
 polinomio, 111, 113
 — ciclotomico, 133
 — generale di grado n , 371
 — inseparabile, 330
 — invertibile, 115, 117
 — irriducibile, 117
 — minimo, 314
 — monico, 116
 — primitivo, 122, 191
 — primo, 117
 — riducibile, 117
 — separabile, 330
 — simmetrico, 144
 postulati di Peano, 22
 potenza, 31
 — del continuo, 34
 — del numerabile, 31
 primitivo, polinomio, 122, 191
 primo:
 — teorema di isomorfismo, 169, 262

— elemento, 45
 — ideale, 174
 — numero, 45
 — polinomio, 117
 principale:
 — anello, 174
 — dominio, 182
 — — ideale, 174
 principio:
 — del buon ordinamento, 26
 — del minimo, 26
 — di induzione matematica, 22, 23
 procedimento diagonale di Cantor, 33
 prodotto, 24
 — cartesiano, 10
 — diretto esterno, 282
 — diretto interno, 283
 — semidiretto, 288
 proiezione canonica, 21
 — — sul quoziente, 164
 proporzione divina, 62
 propriamente contenuto, 9
 proprietà:
 — riflessiva, 13
 — simmetrica, 13
 — transitiva, 13
 prova del nove, 71

Q

quadratura del cerchio, 347
 quaternioni, corpo dei, 334
 quoziente, insieme, 15
 quozienti, campo dei, 59, 178

R

radicale, estensione, 368
 radice:
 — n -esima dell'unità primitiva, 132
 — di un polinomio, 118
 — multipla, 118
 — razionale, 126
 — semplice, 118
 radici n -esime dell'unità, 107
 rapporto aureo, 62
 rappresentazione:
 — in base b , 100
 — in base decimale, 99

razionali, numeri, 55
 relazione, 12
 — antisimmetrica, 16
 — compatibile, 68, 249
 — di congruenza modulo n , 67
 — di equivalenza, 13
 — di equivalenza compatibile con le operazioni, 162
 — di ordine parziale, 16
 — inversa, 13
 — ricorsiva, 27
 reticolo, 296
 rettificazione della circonferenza, 347
 riducibile, polinomio, 117
 riflessiva, proprietà, 13
 risolubile:
 — per radicali, 368
 — gruppo, 291
 Ruffini, teorema di, 117

S
 scelta, assioma della, 35
 secondo teorema di isomorfismo, 170, 263
 semplice:
 — gruppo, 281
 — radice, 118
 separabile, estensione, 339
 simmetrica, proprietà, 13
 simmetrico:
 — gruppo, 217
 — polinomio, 144
 singleton, 10
 sistema di crittografia con chiave pubblica, 94
 somma, 23, 24
 somma diretta, 153
 sottoanello, 155
 — fondamentale, 202
 sottocampo:
 — fondamentale, 201
 — primo, 201
 sottogruppo, 207
 — alterno, 224
 — ciclico, 209
 — commutatore, 290
 — delle traslazioni, 296

— derivato, 260, 290
 — di isotropia, 267
 — di Sylow, 275
 — generato da un sottoinsieme, 209
 — normale, 251
 sottoinsieme, 8
 spezzamento, campo di, 321
 stabilizzatore, 267
 struttura algebrica, 24
 successione radicale, 368
 successivo, 23
 suriettiva, funzione, 19
 Sylow:
 — sottogruppo di, 275
 — teoremi di, 275

T
 Tartaglia, triangolo di, 39
 teorema:
 — cinese del resto, 79
 — del buon ordinamento, 35
 — dell'elemento primitivo, 340
 — di Abel-Ruffini, 371
 — di Burnside, 271
 — di Cauchy, 274
 — di Cayley, 243
 — di Cayley generalizzato, 280
 — di corrispondenza di Galois, 362
 — di Eulero, 86
 — di fattorizzazione unica, 117
 — di Gauss, 123
 — di Lagrange, 240
 — di Ruffini, 117
 — di Wedderburn, 335
 — di Wilson, 90
 — fondamentale dell'algebra, 120, 367
 — fondamentale dell'aritmetica, 52
 — fondamentale di omomorfismo tra anelli, 166
 — fondamentale di omomorfismo tra gruppi, 257
 — fondamentale sui gruppi abeliani finiti, 303
 — fondamentale sui polinomi simmetrici, 145
 — fondamentale sulle funzioni razionali simmetriche, 148

teoremi di Sylow, 275
test di non primalità, 90
torre di Hanoi, gioco della, 29
totalmente ordinato, insieme, 16
transitiva, proprietà, 13
trascendente, elemento, 312
trasformazione affine, 214
trasposizione, 222
triangolo di Pascal, 39
triangolo di Tartaglia, 39
trisezione dell'angolo, 347

U

uguaglianza di insiemi, 8
unione, 9
unità:
— immaginaria, 105
— elemento, 45
universo, 9

V

valore assoluto, 44
valutazione di un dominio euclideo,
180
valutazione: omomorfismo, 313
Viète, formule di, 145

W

Wedderburn, teorema di, 335
Wilson, teorema di, 90

Z

Zermelo, assioma di, 35
zero:
— di un polinomio, 118
— divisore dello, 44



