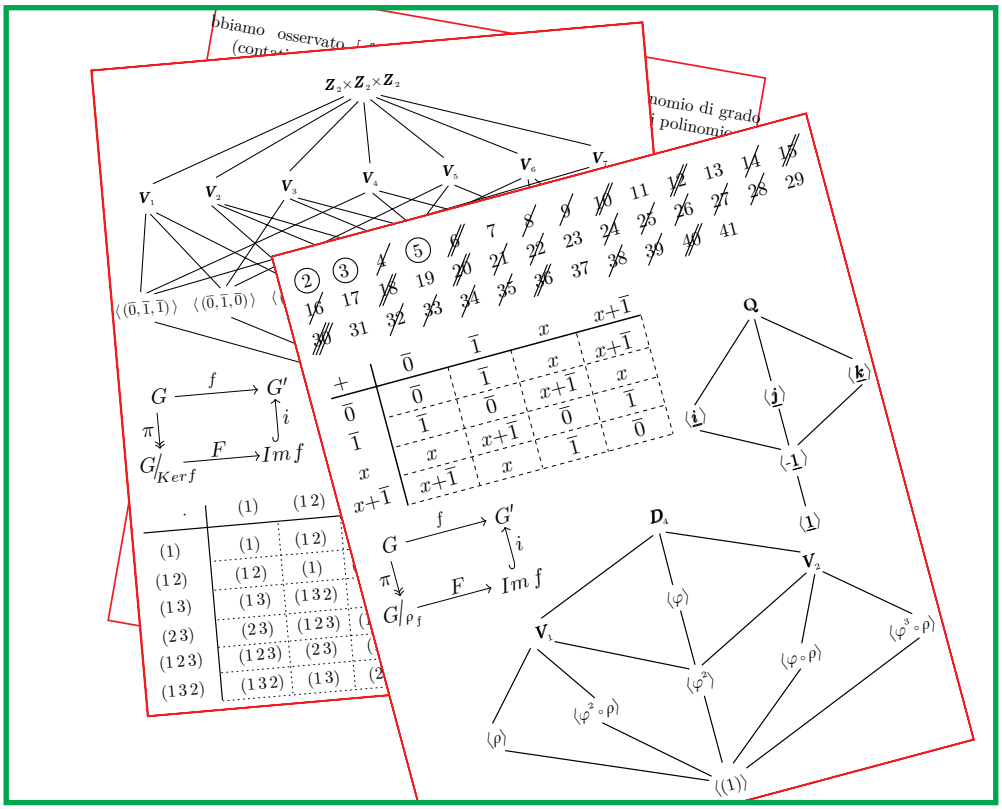
Università degli Studi di Roma "La Sapienza"
Dipartimento di Matematica "G.Castelnuovo"
A.A. 2004-2005

G. CAMPANELLA

APPUNTI DI ALGEBRA 1



Prefazione

Ho raccolto in questo volume gli appunti del modulo di Algebra 1 da me tenuto presso il Dipartimento "G.Castelnuovo" dell'Università "La Sapienza" di Roma negli A.A. 2002-03, 2003-04 e 2004-05.

Ho suddiviso gli argomenti affrontati nel corso in quattro capitoli. Il primo è dedicato alle generalità della teoria degli insiemi, allo studio delle proprietà elementari degli insiemi numerici tradizionali (naturali, interi, razionali, reali e complessi) e ad una schematica presentazione delle principali strutture algebriche (gruppi ed anelli). Il secondo e terzo capitolo studiano le proprietà della fattorizzazione e delle congruenze nell'anello $\boldsymbol{Z}$ degli interi e nell'anello $K[X]$ dei polinomi in una indeterminata ed a coefficienti in un campo K; viene messa in evidenza la stretta analogia algebrica tra le due strutture. Nel quarto ed ultimo capitolo vengono presentate le prime nozioni di teoria dei gruppi, con particolare attenzione allo studio dei gruppi finiti.

Mancano molti importanti argomenti, che trovavano di solito posto in un corso annuale di Algebra: ideali e teoria moltiplicativa degli anelli, estensioni di campi ed elementi di teoria di Galois; si tratta di argomenti che vengono rinviati al modulo di Algebra 2.

Gli esercizi proposti alla fine di ciascun capitolo sono risolti in un volumetto separato, nella cui ultima sezione sono inoltre presentati (sotto forma di esercizi) alcuni complementi e sono raccolti vari esercizi "conclusivi" del corso (recenti prove d'esame o d'esonero).

Desidero ringraziare gli studenti dei corsi di Algebra 1 (A-H) di questi ultimi tre A.A. per l'attenzione con cui hanno seguito la nascita di questi appunti ed in particolare gli studenti A.Appel, L.Belli, V.Capraro, G.Fortuna e G.Franzutti per la cura con cui mi hanno segnalato errori ed imprecisioni.

Giugno 2005

Giulio Campanella

Indice

Capitolo I

Insiemi - applicazioni - relazioni - operazioni - insiemi numerici - cardinalità

Capitolo II

Fattorizzazione e congruenze sugli interi

Capitolo III

Polinomi

Capitolo IV

Gruppi

Capitolo I

INSIEMI - APPLICAZIONI - RELAZIONI - OPERAZIONI - INSIEMI NUMERICI - CARDINALITA'

1. Generalità sugli insiemi

Il concetto di *insieme* è primitivo. Dire "un insieme è una collezione di oggetti" è una tautologia [infatti cos'è una *collezione*, se non un *insieme* di oggetti ?].

Diremo che un insieme A è assegnato quando è possibile stabilire se un oggetto x è *elemento* di A [e si scrive $x \in A$] o non è elemento di A [e si scrive $x \notin A$].

Esiste un solo insieme privo di elementi: è l'*insieme vuoto*, denotato $\emptyset$. Assumiamo inoltre provvisoriamente noti gli insiemi numerici più importanti: $\boldsymbol{N}$, $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$ (cioè l'insieme dei *naturali*, degli *interi*, dei *razionali*, dei *reali* e dei *complessi*); ma su essi torneremo nel paragrafo **5**.

Per descrivere un insieme A:

- se ne possono scrivere gli elementi, elencandoli tra parentesi graffe e separandoli con virgole: ad esempio $A = \{a, b, c, \ ... \}$.

- si può descrivere (sempre tra parentesi graffe) la legge di appartenenza dei suoi elementi. A tale scopo si fa uso di alcuni ben noti *simboli logici*:

- *quantificatori*: $\forall$, $\exists$, $\exists!$, $\nexists$ [cioè *per ogni*, *esiste*, *esiste un unico*, *non esiste*];

- *implicazioni*: $\Longrightarrow$, $\Longleftarrow$, $\Longleftrightarrow$, $\not\Longrightarrow$ [cioè *implica*, *è implicato*, *equivale*, *non implica*];

- *congiunzioni*: $,$, $\wedge$, $\vee$, $\neg$, $\mid$ [cioè *virgola* (o *separatore*), *e*, *oppure*, *non*, *tale che*].

La congiunzione *"non"* è talvolta indicata con $/$ (invece di $\neg$), mentre *"tale che"* è spesso indicata con $:$ (invece di $\mid$).

Ad esempio, l'insieme $\boldsymbol{P}$ dei numeri naturali pari può essere così descritto:

$$\boldsymbol{P} = \{0, 2, 4, 6, 8, \ .... \}, \text{ oppure } \boldsymbol{P} = \{n \in \boldsymbol{N} \mid n = 2x, \ \exists\, x \in \boldsymbol{N}\} = \{2n, \ \forall\, n \in \boldsymbol{N}\}.$$

Definizione 1. *Siano A, B due insiemi. A è detto sottoinsieme di B se, $\forall\, a \in A$, $a \in B$. Si scrive in tal caso $A \subseteq B$ [oppure $B \supseteq A$] e si dice che A è contenuto in B [o che B contiene A].*

Si dice poi che A è contenuto propriamente in B o che B contiene propriamente A [e si scrive $A \subset B$ o $B \supset A$] se $A \subseteq B$ ed $\exists\, b \in B \mid b \notin A$.

Ogni insieme A ammette sempre i due sottoinsiemi $\emptyset$, A, detti sottoinsiemi banali di A. Gli altri (eventuali) sottoinsiemi di A sono detti sottoinsiemi propri.

Osservazione 1. Una *proposizione* $\mathcal{P}$ è un enunciato, per il quale si può stabilire se è vero o falso.

(*i*) Ad ogni proposizione $\mathcal{P}$ resta associata la sua negazione "*non* $\mathcal{P}$" [che si denota usualmente $\neg\mathcal{P}$ oppure $\not\mathcal{P}$]. Ovviamente $\neg\mathcal{P}$ è vera $\Longleftrightarrow$ $\mathcal{P}$ è falsa.

Ad esempio, assegnata la proposizione $A \subseteq B$, la sua negazione $A \not\subseteq B$, è così definita:

$$A \not\subseteq B \iff \exists\, a \in A \mid a \notin B.$$

Più in generale, per scrivere la negazione di $\mathcal{P}$, si procede in questo modo:

- si sostituisce $\forall$ con $\exists$ [e viceversa];

- si sostituisce $\wedge$ con $\vee$ [e viceversa];

- si sostituisce $,$ con $\mid$ [e viceversa];

- si sostituisce ogni affermazione contenuta in $\mathcal{P}$ con la sua opposta.

A titolo di esempio, vogliamo negare la seguente ben nota definizione di *limite di una successione*:

$$\{a_n\} \longrightarrow \alpha \iff \forall \varepsilon > 0\ ,\ \exists m \ \text{(dipendente da } \varepsilon) \ \Big|\ \forall n \geq m\ ,\ |a_n - \alpha| < \varepsilon.$$
$$\{a_n\} \not\longrightarrow \alpha \iff \exists \varepsilon > 0 \ \Big|\ \forall m \ \text{[non dipend. da } \varepsilon]\ ,\ \exists n \geq m \ \Big|\ |a_n - \alpha| \geq \varepsilon.$$

(*ii*) Assegnate due proposizioni $\mathcal{P}$, $\mathcal{Q}$, si consideri la proposizione "$\mathcal{P} \Longrightarrow \mathcal{Q}$" [vera o falsa che sia] e si provi a dimostrarla. Tale proposizione può anche essere dimostrata nella sua *forma contrappositiva* o *per assurdo* [nel seguito spesso abbeviato con PA]: "$\neg\mathcal{Q} \Longrightarrow \neg\mathcal{P}$".

Ciò dipende dal fatto che le due proposizioni "$\mathcal{P} \Longrightarrow \mathcal{Q}$" e "$\neg\mathcal{Q} \Longrightarrow \neg\mathcal{P}$" sono *logicamente equivalenti*, cioè hanno la stessa *tavola di verità*. Per definizione, la tavola di verità di "$\mathcal{P} \Longrightarrow \mathcal{Q}$" è la seguente:

$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P} \Longrightarrow \mathcal{Q}$
V	**V**	**V**
V	**F**	**F**
F	**V**	**V**
F	**F**	**V**

Ne segue, tenuto conto che la tavola di verità di $\neg\mathcal{P}$ è opposta a quella di $\mathcal{P}$ (e lo stesso vale per $\mathcal{Q}$):

$\mathcal{P}$	$\mathcal{Q}$	$\neg\,\mathcal{Q}$	$\neg\,\mathcal{P}$	$\neg\mathcal{Q} \Longrightarrow \neg\mathcal{P}$
V	**V**	**F**	**F**	**V**
V	**F**	**V**	**F**	**F**
F	**V**	**F**	**V**	**V**
F	**F**	**V**	**V**	**V**

Confrontando le due ultime colonne delle due tavole, segue che le due proposizioni sono logicamente equivalenti.

Utilizzando le circonlocuzioni *"condizione necessaria affinché ... "* o *"condizione sufficiente affinché ... "* [abbreviate rispettivamente CN e CS], l'implicazione "$\mathcal{P} \Longrightarrow \mathcal{Q}$" si può anche leggere nella forma:

"CN affinché valga $\mathcal{P}$ è che valga $\mathcal{Q}$" [ovvero "$\mathcal{Q}$ è necessario per $\mathcal{P}$"];

"CS affinché valga $\mathcal{Q}$ è che valga $\mathcal{P}$" [ovvero "$\mathcal{P}$ è sufficiente per $\mathcal{Q}$"].

Definizione 2. *Due insiemi A, B sono detti uguali [e si scrive $A = B$] se hanno gli stessi elementi. Si ha quindi:*

$$A = B \iff A \subseteq B \ \ e \ \ B \subseteq A.$$

A, B sono detti diversi se non sono uguali [e si scrive $A \neq B$].

Osservazione 2. (*i*) Dalla definizione precedente segue, ad esempio, che $\{a, a\} = \{a\}$.

(*ii*) Sia $n \in \boldsymbol{N}$. Se un insieme A è formato da n elementi (a due a due distinti), si scrive $|A| = n$, oppure $\#(A) = n$ e si dice che A *ha cardinalità* n. In particolare, $|\emptyset| = 0$. Un insieme A è detto finito se ha cardinalità n (per qualche $n \in \boldsymbol{N}$); altrimenti è detto *infinito*.

(*iii*) Si noti che abbiamo già utilizzato il simbolo $=$ per *definire* un insieme. In effetti, scrivendo $\boldsymbol{P} = \{0, 2, 4, ...\}$ abbiamo assegnato il nome $\boldsymbol{P}$ all'insieme $\{0, 2, 4, ...\}$. In tal caso è molto frequente sostituire $=$ con $:=$, scrivendo quindi $\boldsymbol{P} := \{0, 2, 4, ...\}$.

In modo analogo, il simbolo $\iff$ può essere anche usato per definire un concetto. In tal caso sarebbe preferibile sostituirlo con $:\iff$ ovvero con $\overset{def}{\iff}$. Ad esempio, avremmo potuto scrivere $\{a_n\} \longrightarrow \alpha \overset{def}{\iff} \forall \varepsilon > 0 \ldots .$.

Definizione 3. *Sia X un insieme e siano A, B sottoinsiemi di X. Sono definiti i seguenti insiemi:*

$$A \cap B = \{x \in X \ :\ x \in A \ \ e \ \ x \in B\},\ \textit{detto intersezione di } A \ e \ B;$$

$A \cup B = \{x \in X \ : \ x \in A \ \ \textit{oppure} \ \ x \in B\}$, *detto unione di* A *e* B;
$A - B = \{x \in X \ : \ x \in A \ \ e \ \ x \notin B\}$, *detto differenza di* A *con* B;
$\mathbf{C}_{X}(A) = \{x \in X \ : \ x \notin A\}$, *detto complementare di* A *in* X.

Osservazione 2. (*i*) Valgono le seguenti ovvie inclusioni:

$$A \cap B \begin{array}{l} \subseteq A \\ \subseteq B \end{array} \subseteq A \cup B.$$

Se $A \cap B = \emptyset$, A, B sono detti *insiemi disgiunti*.

(*ii*) L'intersezione e l'unione si generalizzano in questo modo: se $\{A_i\}_{i \in I}$ è una famiglia di sottoinsiemi di X,

$$\bigcap_{i \in I} A_i = \{x \in X \ : \ x \in A_i, \ \forall\, i \in I\}, \qquad \bigcup_{i \in I} A_i = \{x \in X \ : \ x \in A_i, \ \exists\, i \in I\}$$

(*iii*) Ovviamente $A - B = A \cap \mathbf{C}_{X}(B)$ e si verifica subito che $A - B_2 \subseteq A - B_1$, se $B_1 \subseteq B_2$.

(*iv*) Valgono le seguenti uguaglianze tra sottoinsiemi A, B, C di un insieme X [note come *formule di De Morgan*]:

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C); \qquad (A \cup B) \cap C = (A \cap C) \cup (B \cap C);$$
$$A - (B \cup C) = (A - B) \cap (A - C); \qquad A - (B \cap C) = (A - B) \cup (A - C).$$

Le prime due formule sono conseguenza del fatto che, assegnate tre proposizioni $\mathcal{P}$, $\mathcal{Q}$, $\mathcal{R}$, la proposizione $(\mathcal{P} \wedge \mathcal{Q}) \vee \mathcal{R}$ è logicamente equivalente a $(\mathcal{P} \vee \mathcal{R}) \wedge (\mathcal{Q} \vee \mathcal{R})$, mentre la proposizione $(\mathcal{P} \vee \mathcal{Q}) \wedge \mathcal{R}$ è logicamente equivalente a $(\mathcal{P} \wedge \mathcal{R}) \vee (\mathcal{Q} \wedge \mathcal{R})$. Le ultime due formule discendono dalle prime due e dal fatto che $\neg(\mathcal{P} \wedge \mathcal{Q})$ è logicamente equivalente a $(\neg\mathcal{P}) \vee (\neg\mathcal{Q})$, mentre $\neg(\mathcal{P} \vee \mathcal{Q})$ è logicamente equivalente a $(\neg\mathcal{P}) \wedge (\neg\mathcal{Q})$.

Definizione 4. *Sia* X *un insieme. L'insieme dei sottoinsiemi di* X *è detto insieme delle parti di* X. *È denotato* $\boldsymbol{\mathcal{P}}(X)$.

Osservazione 3. (*i*) Se ad esempio $A = \{1, 2\}$, risulta $\boldsymbol{\mathcal{P}}(A) = \big\{\emptyset, \{1\}, \{2\}, A\big\}$.

(*ii*) Si noti che:

$\boldsymbol{\mathcal{P}}(\emptyset) = \{\emptyset\}$ ha cardinalità 1;
$\boldsymbol{\mathcal{P}}\big(\boldsymbol{\mathcal{P}}(\emptyset)\big) = \big\{\emptyset, \{\emptyset\}\big\}$ ha cardinalità 2;
$\boldsymbol{\mathcal{P}}\Big(\boldsymbol{\mathcal{P}}\big(\boldsymbol{\mathcal{P}}(\emptyset)\big)\Big) = \big\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\big\}$ ha cardinalità 4, ecc..

Proveremo in seguito (cfr. **Prop. 5.6**) che se $|A| = n$, allora $|\boldsymbol{\mathcal{P}}(A)| = 2^n$.

Definizione 5. *Sia* X *un insieme e sia* $\mathfrak{U} = \{A_i\}_{i \in I}$ una famiglia di suoi sottoinsiemi. $\mathfrak{U}$ è detta *ricoprimento di* X se $\bigcup_{i \in I} A_i = X$. $\mathfrak{U}$ è detta *partizione di* X se è un ricoprimento di X e se $A_i \cap A_j = \emptyset$, se $i \neq j$.

Esempi 1. (*i*) In $\boldsymbol{N}$ consideriamo i sottoinsiemi

$$\boldsymbol{P} = 2\boldsymbol{N} := \{2n, \ \forall\, n \in \boldsymbol{N}\}, \quad 3\boldsymbol{N} := \{3n, \ \forall\, n \in \boldsymbol{N}\}, \quad 1 + 2\boldsymbol{N} = \{1 + 2n, \ \forall\, n \in \boldsymbol{N}\}.$$

$\big\{2\boldsymbol{N}, 3\boldsymbol{N}\big\}$ non è un ricoprimento di $\boldsymbol{N}$ [infatti ad esempio $5 \notin 2\boldsymbol{N} \cup 3\boldsymbol{N}$]. Invece $\big\{2\boldsymbol{N}, 1 + 2\boldsymbol{N}\big\}$ è una partizione di $\boldsymbol{N}$ [la partizione "dei pari e dei dispari"].

(*ii*) La famiglia $\mathfrak{U} = \big\{\{1\}, p\boldsymbol{N}, \ \forall\, p \text{ numero primo}\big\}$ è un ricoprimento di $\boldsymbol{N}$ [infatti ogni naturale ≥ 2 è prodotto di primi], ma non è una partizione di $\boldsymbol{N}$ [infatti $p_1 p_2 \in p_1\boldsymbol{N} \cap p_2\boldsymbol{N}$, se p_1, p_2 sono primi distinti].

(*iii*) Ogni insieme X ammette le due seguenti partizioni *banali*:

$$\mathfrak{U} = \big\{\{x\},\ \forall\, x \in X\big\}, \quad \mathfrak{V} = \{X\}.$$

Definizione 6. *Dati due insiemi A, B, si chiama prodotto cartesiano di A e B l'insieme*

$$A\times B = \big\{(a,b),\ \forall\, a \in A,\ \forall\, b \in B\big\}.$$

L'elemento $(a,b) \in A\times B$ è detto coppia (ordinata) formata da a, b.

Osservazione 4. Le seguenti considerazioni sono pressoché ovvie e la loro verifica è lasciata al lettore.

(*i*) È evidente che $(a,b) \neq (b,a)$, se $a \neq b$. Risulta inoltre: $(a,b) = (c,d) \iff a = c$ e $b = d$.

(*ii*) Ovviamente $A\times\emptyset = \emptyset\times B = \emptyset$. Inoltre:

$$A\times B = \emptyset \implies A = \emptyset \text{ oppure } B = \emptyset.$$

(*iii*) Se $|A| = m$ e $|B| = n$, allora $|A\times B| = mn$.

(*iv*) Risulta:

$$(A\times B)\cap(A\times C) = A\times(B\cap C), \qquad (A\times B)\cup(A\times C) = A\times(B\cup C).$$

(*v*) Se $A \subseteq X$ e $B \subseteq Y$, allora $A\times B \subseteq X\times Y$ e si ha:

$$\mathbf{C}_{X\times Y}(A\times B) = \big(\mathbf{C}_X(A)\times Y\big)\cup\big(X\times\mathbf{C}_Y(B)\big).$$

(*vi*) Assegnati n insiemi A_1, A_2, ... , A_n, si definisce loro *prodotto cartesiano* l'insieme

$$A_1\times A_2\times \ldots \times A_n = \big\{(a_1,\, a_2,\, \ldots\, ,\, a_n),\ \forall\, a_i \in A_i\big\}.$$

(*vii*) Se A è un insieme e $n \geq 2$, si scrive A^n in luogo di $\underbrace{A\times A\times \ldots \times A}_{n \text{ volte}}$.

Definizione 7. *Dati due insiemi A, B, si chiama unione disgiunta di A e B l'insieme*

$$A \sqcup B = \big(A\times\{1\}\big)\cup\big(B\times\{2\}\big).$$

Ad esempio, se $A = \{a,b,c\}$ e $B = \{c,d\}$, allora

$$A \sqcup B = \big\{(a,1),\,(b,1),\,(c,1),\,(c,2),\,(d,2)\big\}$$

[mentre $A\cup B = \{a,b,c,d\}$]. Si noti che $A\times\{1\}$ e $B\times\{2\}$ sono in ogni caso disgiunti (indipendentemente da A e B). Se in particolare $|A| = m$ e $|B| = n$, allora $|A \sqcup B| = m + n$.

Nota. *Se $A\cap B = \emptyset$, $A\cup B$ viene (impropriamente) identificato con $A \sqcup B$.*

2 Applicazioni tra insiemi

Definizione 1. *Siano A, B due insiemi. Un'applicazione $f : A \to B$ è una legge che ad ogni elemento $a \in A$ associa uno ed un solo elemento $b \in B$, che è detto immagine di a ed è usualmente denotato $f(a)$.*

Osservazione 1. (*i*) La precedente definizione è ovviamente "tautologica". In effetti non abbiamo detto che cosa sia una "legge". Si noti che potremmo facilmente definire il concetto di applicazione ricorrendo a quello di insieme, ma non insistiamo su tale fatto.

(*ii*) Siano $A = \{a, b, c\}$ e $B = \{1, 2, 3, 4\}$ due insiemi. In base alla precedente definizione, le due seguenti "leggi" f, g non sono applicazioni.

$$f : \begin{cases} a \longrightarrow 1 \\ b \longrightarrow 2 \\ c \quad\ 3 \\ \quad\ 4 \end{cases} \qquad g : \begin{cases} a \longrightarrow 1 \\ a \longrightarrow 2 \\ b \longrightarrow 3 \\ c \longrightarrow 4 \end{cases}$$

[Infatti nella prima l'elemento c non ha alcuna immagine, mentre nella seconda l'elemento a ha due immagini]. Se chiamiamo *corrispondenza da A a B* ogni applicazione da A a $\boldsymbol{\mathcal{P}}(B)$, le due leggi sopra definite rientrano nel concetto di corrispondenza. Risulta infatti:

$$f(a) = \{1\},\ f(b) = \{2\},\ f(c) = \emptyset; \qquad g(a) = \{1, 2\},\ g(b) = \{3\},\ g(c) = \{4\}.$$

(*iii*) Ovviamente due applicazioni $f : A \to B$, $g : A \to B$ sono dette *uguali* [si scrive $f = g$] se risulta $f(a) = g(a)$, $\forall\, a \in A$. Sono quindi diverse [si scrive $f \neq g$] se $\exists\, a \in A \mid f(a) \neq g(a)$.

Definizione 2. *Sia $f : A \to B$ un'applicazione. Per ogni $A' \subseteq A$, l'insieme*

$$f(A') = \{f(a),\ \forall\, a \in A'\}$$

è detto immagine di A' tramite f. In particolare, l'insieme $f(A) =: Im\, f$ [ovvero $Im(f)$] è detto immagine di f. Per ogni $b \in B$, l'insieme

$$f^{-1}(b) = \{a \in A \mid f(a) = b\}$$

è detto controimmagine di b tramite f. Sono sinonimi di controimmagine: fibra, antiimmagine o preimmagine. Più generalmente, per ogni $B' \subseteq B$, l'insieme

$$f^{-1}(B') = \{a \in A \mid f(a) \in B'\}$$

è detto controimmagine di B' tramite f. Ovviamente risulta $f^{-1}(Im\, f) = f^{-1}(B) = A$. Si noti poi che, se $A_1 \subseteq A_2 \subseteq A$, allora $f(A_1) \subseteq f(A_2) \subseteq Im\, f$; se $B_1 \subseteq B_2 \subseteq B$, allora $f^{-1}(B_1) \subseteq f^{-1}(B_2) \subseteq A$.

Definizione 3. *Sia $f : A \to B$ un'applicazione. f è detta iniettiva se risulta, $\forall\, a_1, a_2 \in A$,*

$$f(a_1) = f(a_2) \implies a_1 = a_2$$

[ovvero se: $a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$, cioè se "elementi distinti hanno immagini distinte"].

$f : A \to B$ è detta suriettiva se

$$\forall\, b \in B,\ \exists\, a \in A \mid f(a) = b$$

[ovvero se $Im\, f = B$].

Infine $f : A \to B$ è detta biiettiva se è iniettiva e suriettiva. In tal caso diciamo che A, B sono *in biiezione* o *in corrispndenza biunivoca* tramite f.

Notazioni. Talvolta un'applicazione suriettiva potrà essere indicata utilizzando una freccia a due punte $\twoheadrightarrow$, mentre per un'applicazione iniettiva potrà essere utilizzata una freccia della forma $\hookrightarrow$. Dunque una biiezione potrà essere denotata con una freccia $\rightarrowtail\!\!\!\!\!\twoheadrightarrow$.

Osservazione 2. Si verificano con facilità le seguenti caratterizzazioni [in termini di controimmagine]. Sia $f : A \to B$ un'applicazione.

(*i*) f è iniettiva $\iff f^{-1}(b)$ ha al più un elemento, $\forall\, b \in B$.
(*ii*) f è suriettiva $\iff f^{-1}(b) \neq \emptyset$, $\forall\, b \in B$.
(*iii*) f è biiettiva $\iff f^{-1}(b)$ ha esattamente un elemento, $\forall\, b \in B$.

Osservazione 3. Illustriamo alcune applicazioni "standard".

(*1*) *Applicazione d'inclusione.* Sia $A' \subseteq A$. È definita l'applicazione

$$i : A' \hookrightarrow A \text{ tale che } i(a) = a,\ \forall\, a \in A'.$$

i è detta *applicazione canonica d'inclusione (del sottoinsieme A' di A)* ed è ovviamente iniettiva.

(*2*) *Applicazione identica.* Sia A un insieme. È sempre definita l'applicazione

$$\mathbf{1}_A : A \to A \text{ tale che } \mathbf{1}_A(a) = a,\ \forall\, a \in A.$$

L'applicazione $\mathbf{1}_A$ è detta *applicazione identica* o *identità di A*. È ovviamente biiettiva.

(*3*) *Restrizione di un'applicazione.* Sia $f : A \to B$ un'applicazione e sia $A' \subseteq A$. L'applicazione

$$f_{|_{A'}} : A' \to B \text{ tale che } f_{|_{A'}}(a') = f(a'),\ \forall\, a' \in A'$$

è detta *restrizione di f ad A'*.

(*4*) *Suriettificazione di un'applicazione.* Sia $f : A \to B$ un'applicazione. L'applicazione

$$f_{su} : A \to Im\, f \text{ tale che } f_{su}(a) = f(a),\ \forall\, a \in A$$

è detta *suriettificazione di f*. È ovviamente suriettiva.

(*5*) *Funzione caratteristica di un sottoinsieme.* Sia $A' \subseteq A$. L'applicazione

$$\chi_{A'} : A \to \{0,1\} \text{ tale che } \chi_{A'}(a) = \begin{cases} 0, & \text{se } a \notin A' \\ 1, & \text{se } a \in A', \end{cases} \quad \forall\, a \in A,$$

è detta *funzione caratteristica di A' in A*.

(*6*) *Proiezioni canoniche.* Siano A, B due insiemi. Le due applicazioni

$$p_1 : A \times B \to A \ :\ p_1(a,b) = a, \quad p_2 : A \times B \to B \ :\ p_2(a,b) = b,\ \forall\, (a,b) \in A \times B,$$

sono dette rispettivamente *prima e seconda proiezione canonica (dal prodotto cartesiano $A \times B$)*. Sono ovviamente suriettive.

Osservazione 4. (*i*) Sia $f : A \to B$ un'applicazione e siano $B_1, B_2 \subseteq B$. Si verifica facilmente che

$$f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2); \qquad f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2).$$

(*ii*) Sia $f : A \to B$ un'applicazione e siano $A_1, A_2 \subseteq A$. Si verifica facilmente che

$$f(A_1 \cup A_2) = f(A_1) \cup f(A_2); \qquad f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2).$$

L'ultima inclusione può essere stretta, come nel seguente esempio:
sia $A = \{a_1, a_2\}$, $B = \{1\}$, $f : A \to B$ tale che $f(a_1) = f(a_2) = 1$. Posto $A_1 = \{a_1\}$, $A_2 = \{a_2\}$, allora $f(A_1 \cap A_2) = f(\emptyset) = \emptyset$, mentre $f(A_1) \cap f(A_2) = \{1\}$.

(*iii*) Le formule (*i*) e (*ii*) si generalizzano ad un numero arbitrario di sottoinsiemi:

$$f^{-1}\big(\bigcap_{i\in I} B_i\big) = \bigcap_{i\in I} f^{-1}(B_i), \qquad f^{-1}\big(\bigcup_{i\in I} B_i\big) = \bigcup_{i\in I} f^{-1}(B_i);$$
$$f\big(\bigcup_{i\in I} A_i\big) = \bigcup_{i\in I} f(A_i), \qquad f\big(\bigcap_{i\in I} A_i\big) \subseteq \bigcap_{i\in I} f(A_i).$$

Proposizione 1. *Sia $f : A \to B$ un'applicazione. Risulta:*
(i) Per ogni $A' \subseteq A$, $f^{-1}\big(f(A')\big) \supseteq A'$. Se poi f è iniettiva, risulta sempre $f^{-1}\big(f(A')\big) = A'$.
(ii) Per ogni $B' \subseteq B$, $f\big(f^{-1}(B')\big) \subseteq B'$. Se poi f è suriettiva, risulta sempre $f\big(f^{-1}(B')\big) = B'$.
(iii) Per ogni $A' \subseteq A$, $f\big(f^{-1}\big(f(A')\big)\big) = f(A')$; per ogni $B' \subseteq B$, $f^{-1}\big(f\big(f^{-1}(B')\big)\big) = f^{-1}(B')$.

Dim. (*i*) Risulta, $\forall\, a \in A$: $a \in f^{-1}\big(f(A') \iff f(a) \in f(A')$. Se quindi $a \in A'$, allora $f(a) \in f(A')$ e quindi $a \in f^{-1}\big(f(A')$.

Se poi f è iniettiva, basta verificare che $f^{-1}\big(f(A')\big) \subseteq A'$. Se infatti $a \in f^{-1}\big(f(A')\big)$, allora $f(a) = f(a')$, $\exists\, a' \in A'$. Ma poiché f è iniettiva, $a = a' \in A'$.

Nota. Diamo un esempio di applicazione $f : A \to B$ non iniettiva tale che $f^{-1}\big(f(A')\big) \supset A'$. Si ponga: $A = \{1, 2, 3\}$, $B = \{a, b, c\}$, $f : A \to B$ tale che $f(1) = f(2) = a$, $f(3) = c$. Posto ora $A' = \{1, 3\}$, risulta: $f(A') = \{a, c\}$ e $f^{-1}\big(f(A')\big) = \{1, 2, 3\} \supset A'$.

(*ii*) Risulta: $f\big(f^{-1}(B')\big) = \big\{f(a),\ \forall\, a \in A\ :\ f(a) \in B'\big\} = Im\, f \cap B' \subseteq B'$. Se poi f è suriettiva, allora $Im\, f = B$ e quindi $f\big(f^{-1}(B')\big) = B \cap B' = B'$.

Nota. Diamo un esempio di applicazione $f : A \to B$ non suriettiva tale che $f\big(f^{-1}(B')\big) \subset B'$. Si consideri la stessa applicazione della nota precedente. Posto $B' = \{a, b\}$, risulta: $f^{-1}(B') = \{1, 2\}$ e quindi $f\big(f^{-1}(B')\big) = \{a\} \subset B'$.

(*iii*) Sia $A' \subseteq A$. Da (*ii*), $f\big(f^{-1}\big(f(A')\big)\big) \subseteq f(A')$. Viceversa, da (*i*), $f^{-1}\big(f(A')\big) \supseteq A'$ e, applicando f a tale inclusione, segue che $f\big(f^{-1}\big(f(A')\big)\big) \supseteq f(A')$.

Sia ora $B' \subseteq B$. Da (*i*), $f^{-1}\big(f\big(f^{-1}(B')\big)\big) \supseteq f^{-1}(B')$. Viceversa, da (*ii*), $f\big(f^{-1}(B')\big) \subseteq B'$ e, applicando f^{-1} a tale inclusione, segue che $f^{-1}\big(f\big(f^{-1}(B')\big)\big) \subseteq f^{-1}(B')$.

Definizione 4. *Siano $f : A \to B$ e $g : B \to C$ due applicazioni. Si chiama composizione di f e g o prodotto operatorio di f e g l'applicazione*

$$g \circ f : A \to C \quad \textit{tale che} \quad (g \circ f)(a) = g\big(f(a)\big),\ \ \forall\, a \in A.$$

Osservazione 5. (*i*) Date le tre applicazioni $f : A \to B$, $g : B \to C$ e $h : C \to D$, si verifica facilmente che vale la *proprietà associativa*, cioè: $h \circ (g \circ f) = (h \circ g) \circ f$.

Infatti, $\forall\, a \in A$: $\big(h \circ (g \circ f)\big)(a) = h\big(g(f(a))\big) = \big((h \circ g) \circ f\big)(a)$.

(*ii*) Data $f : A \to B$, risulta: $f \circ \mathbf{1}_A = f$, $\quad \mathbf{1}_B \circ f = f$.

Infatti, $\forall\, a \in A$: $(f \circ \mathbf{1}_A)(a) = f(\mathbf{1}_A(a)) = f(a)$, $\quad (\mathbf{1}_B \circ f)(a) = \mathbf{1}_B(f(a)) = f(a)$.

(*iii*) In generale, $f \circ g \neq g \circ f$. Ad esempio, posto $\begin{cases} f : \boldsymbol{R} \to \boldsymbol{R} \ \big|\ f(x) = x^2,\ \forall\, x \in \boldsymbol{R}, \\ g : \boldsymbol{R} \to \boldsymbol{R} \ \big|\ f(x) = x + 1,\ \forall\, x \in \boldsymbol{R}, \end{cases}$ risulta:

$$(g \circ f)(x) = x^2 + 1, \quad (f \circ g)(x) = (x + 1)^2,\ \ \forall\, x \in \boldsymbol{R},\ \text{e dunque}\ f \circ g \neq g \circ f.$$

(*iv*) Se $f : A \to B$ e $g : B \to C$ sono iniettive [rispett. suriettive], anche $g \circ f : A \to C$ è iniettiva [rispett. suriettiva]. La verifica è lasciata per esercizio.

(*v*) Si noti che ogni applicazione $f : A \to B$ si fattorizza nella forma $f = i \circ f_{su}$, con $f_{su} : A \to Im\, f$ suriettivizzazione di f ed $i : Im\, f \hookrightarrow B$ inclusione canonica (cfr. **Osserv. 3**). Si noti infine, che se f è iniettiva, allora f_{su} è biiettiva.

Proposizione 2. *Sia $f : A \to B$ un'applicazione. Risulta:*

$$f \textit{ è biiettiva} \iff \exists\, g : B \to A \quad \textit{tale che} \quad g \circ f = \mathbf{1}_A \ \textit{ e } \ f \circ g = \mathbf{1}_B.$$

Se tale g esiste, allora è unica ed è detta applicazione inversa di f, denotata f^{-1}.

Dim. ($\Longrightarrow$). Essendo f biiettiva, $\forall\, b \in B$, $\exists!\, a \in A\ :\ f(a) = b$. Si definisce allora

$$g : B \to A \quad \text{tale che} \quad g(b) = a, \ \text{ se } \ f(a) = b.$$

Risulta:

- $\forall\, a \in A\ :\ (g \circ f)(a) = g(f(a)) = g(b) = a = \mathbf{1}_A(a)$, e dunque $g \circ f = \mathbf{1}_A$.
- $\forall\, b \in B\ :\ (f \circ g)(b) = f(g(b)) = f(a) = b = \mathbf{1}_B(b)$, e dunque $f \circ g = \mathbf{1}_B$.

($\Longleftarrow$). Assumiamo che esista g. Verifichiamo che f è iniettiva. Sia $f(a_1) = f(a_2)$. Allora $g(f(a_1)) = g(f(a_2))$, cioè $\mathbf{1}_A(a_1) = \mathbf{1}_A(a_2)$ ovvero $a_1 = a_2$. Verifichiamo ora che f è suriettiva. Per ogni $b \in B$ risulta: $b = \mathbf{1}_B(b) = (f \circ g)(b) = f(g(b))$ e quindi $b \in Im\, f$. Dunque $Im\, f = B$.

Ora verifichiamo l'unicità di g. Sia $g_1 : B \to A$ tale che $g_1 \circ f = \mathbf{1}_A$ e $f \circ g_1 = \mathbf{1}_B$. Si tratta di verificare che $g_1 = g$. Si ha, $\forall\, b \in B$: $b = \mathbf{1}_B(b) = (f \circ g)(b) = (f \circ g_1)(b)$ e dunque $f(g(b)) = f(g_1(b))$. Essendo f iniettiva, allora $g(b) = g_1(b)$, da cui $g = g_1$.

Osservazione 6. Si osserva subito che:

(*i*) $\mathbf{1}_A$ è biiettiva, con inversa se stessa.

(*ii*) Se $f : A \to B$ è biiettiva, anche $f^{-1} : B \to A$ lo è ed ha inversa f.

(*iii*) Se $f : A \to B$ e $g : B \to C$ sono applicazioni biiettive, anche $g \circ f : C \to A$ è biiettiva e risulta $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Infatti si verifica facilmente che $(g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathbf{1}_C$ e $(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathbf{1}_A$.

Notazioni. Dati due insiemi A, B,

$$B^A := \{f : A \to B\}$$

denota l'insieme di tutte le possibili applicazioni da A a B. Si noti in particolare che:

- $B^\emptyset$ ha un solo elemento [cioè l'inclusione canonica $i : \emptyset \hookrightarrow B$];
- $\emptyset^A = \{f : \emptyset \dashrightarrow A\} = \emptyset$, se $A \neq \emptyset$ [in quanto non esistono applicazioni prive di immagini].

Si noti infine che conviene lasciare $\emptyset^\emptyset$ indeterminato [infatti contrastano tra loro due fatti: esiste l'inclusione canonica $i : \emptyset \hookrightarrow \emptyset$, ma non esistono applicazioni prive di immagini].

Ci poniamo ora il problema di contare le applicazioni tra due insiemi finiti.

Proposizione 3. *Siano A, B due insiemi finiti tali che $|A| = m$ e $|B| = n$. Allora $\left|B^A\right| = n^m$.*

Dim. Sia $f \in B^A$. f è completamente individuata se sono assegnati gli elementi $f(a)$, $\forall\, a \in A$. Si noti che un elemento $a \in A$ può essere scelto in $m = |A|$ modi, mentre l'elemento $f(a) \in B$ può essere scelto in $n = |B|$ modi. Si hanno complessivamente $\underbrace{n \cdot n \cdot \ \dots\ \cdot n}_{m} = n^m$ possibili scelte per f. Si conclude che esistono n^m applicazioni da A a B, cioè $\left|B^A\right| = n^m$.

Esempio 1. Sia $A = \{1, 2\}$, $B = \{a, b, c\}$. Ogni $f : A \to B$ è completamente individuata dalla coppia $(f(1), f(2)) \in B \times B$. Gli elementi $f(1), f(2)$ possono essere scelti ciascuno in tre modi diversi. Dunque B^A è formato da $9 = 3^2$ applicazioni, associate alle nove coppie:

$$(a, a),\ (a, b),\ (a, c),\ (b, a),\ (b, b),\ (b, c),\ (c, a),\ (c, b),\ (c, c).$$

Si noti invece che A^B è formato da $8 = 2^3$ applicazioni, associate alle otto terne:

$$(1, 1, 1),\ (1, 1, 2),\ (1, 2, 1),\ (1, 2, 2),\ (2, 1, 1),\ (2, 1, 2),\ (2, 2, 1),\ (2, 2, 2).$$

Proposizione 4. *Siano A, B due insiemi finiti.*

(i) Se $|A| > |B|$, non esistono applicazioni iniettive da A a B.

(ii) Se $|A| < |B|$, non esistono applicazioni suriettive da A a B.

(iii) Se $|A| = |B|$, ogni applicazione iniettiva da A a B è anche suriettiva e ogni applicazione suriettiva da A a B è anche iniettiva.

Dim. Se A, B sono insiemi finiti, valgono i seguenti fatti, intuitivamente ovvi [e su cui torneremo nel paragrafo **6**]:

- se $A \subseteq B$, $|A| \leq |B|$;
- se $A \subseteq B$ e $|A| = |B|$, allora $A = B$.

Sia ora $f : A \to B$ un'applicazione [tra insiemi finiti]. In base alle precedenti osservazioni, si ha:

- $|Im\, f| \leq |B|$ [perché $Im\, f \subseteq B$];
- $|Im\, f| \leq |A|$ [perché $Im\, f = \{f(a_1), \dots, f(a_m)\}$, se $A = \{a_1, \dots, a_m\}$];
- $f : A \to B$ è iniettiva $\iff |Im\, f| = |A|$;

- $f : A \to B$ è suriettiva $\iff |Im\, f| = |B|$.

Si ha quindi:

(*i*) Se $f : A \to B$ è iniettiva, allora $|A| = |Im\, f| \leq |B|$. Se quindi $|A| > |B|$, non esistono applicazioni iniettive da A a B.

(*ii*) Se $f : A \to B$ è suriettiva, allora $|B| = |Im\, f| \leq |A|$. Se quindi $|A| < |B|$, non esistono applicazioni suriettive da A a B.

(*iii*) Sia $|A| = |B|$. Si ha: f è iniettiva $\iff |Im\, f| = |A| \iff |Im\, f| = |B| \iff f$ è suriettiva.

Proposizione 5. *Siano A, B insiemi finiti (non vuoti), con $|A| = m$, $|B| = n$. Sia $1 \leq m \leq n$. Il numero delle applicazioni iniettive da A a B è $n(n-1)...(n-m+1)$.*

Dim. Sia $A = \{a_1, ..., a_m\}$ e sia $f : A \to B$ un'applicazione iniettiva. L'elemento $f(a_1)$ può essere scelto in B in n modi distinti. Per ogni $k = 2, ...m$, risulta che $f(a_k) \in B - \{f(a_1), ..., f(a_{k-1})\}$. Dunque $f(a_k)$ può essere scelto in $n-(k-1)$ modi distinti. Ne segue che le applicazioni iniettive da A a B sono $n(n-1)...(n-m+1)$.

Corollario 1. *Siano A, B insiemi finiti (non vuoti), con la stessa cardinalità $n \geq 1$. Il numero delle applicazioni biettive da A a B è $n(n-1) ... \cdot 2 \cdot 1$.*

Dim. Segue dalla **Prop. 5** e dalla **Prop. 4**(*iii*).

Definizione 5. *Per ogni $n \in \boldsymbol{N}$, $n \geq 1$, il numero $n(n-1) \cdot ... \cdot 2 \cdot 1$ è chiamato n fattoriale ed è denotato $n!$. Si definisce poi $0! = 1$.*

In base al **Cor. 1**, *se A è un insieme finito (non vuoto) formato da $n \geq 1$ elementi, le applicazioni biiettive di A in A [usualmente dette permutazioni di A] sono $n!$.*

Dopo aver affrontato il problema di contare le applicazioni tra insiemi finiti, affrontiamo il problema di contare i sottoinsiemi di una data cardinalità di un insieme finito. Introduciamo la seguente definizione.

Definizione 6. *Sia A un insieme finito con n elementi. Per ogni $k \in \boldsymbol{N}$, tale che $0 \leq k \leq n$, si chiama coefficiente binomiale di n su k il numero dei sottoinsiemi di A formati da k elementi. Tale numero è denotato $\binom{n}{k}$.*

Osservazione 7. Allo scopo di ottenere una formula che calcoli $\binom{n}{k}$ [in funzione di n e k], premettiamo le seguenti elementari osservazioni:

$\binom{n}{0} = 1$ [infatti $\emptyset$ è l'unico sottoinsieme di A con 0 elementi];

$\binom{n}{n} = 1$ [infatti A è l'unico sottoinsieme di A con n elementi];

$\binom{n}{1} = n$ [infatti $\{a_1\}, ..., \{a_n\}$ sono tutti e soli i sottoinsiemi di A con 1 elemento];

$\binom{n}{n-1} = n$ [infatti $A - \{a_1\}, ..., A - \{a_n\}$ sono tutti e soli i sottoinsiemi di A con $n-1$ elementi].

Proposizione 6. *Per ogni n, $k \in \boldsymbol{N}$, tali che $1 \leq k \leq n$, risulta:*

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

Dim. Si fissi in A un arbitrario elemento a_1. Per ogni sottoinsieme B di A formato da k elementi, si hanno due possibili casi: $a_1 \in B$ oppure $a_1 \notin B$.

Se $a_1 \in B$, gli altri $k-1$ elementi di B sono scelti nell'insieme $A - \{a_1\}$, che ha $n-1$ elementi. Dunque si hanno $\binom{n-1}{k-1}$ possibili sottoinsiemi B.

Se $a_1 \notin B$, i k elementi di B vanno scelti in $A - \{a_1\}$. Dunque si hanno $\binom{n-1}{k}$ possibili sottoinsiemi B.

Complessivamente i possibili sottoinsiemi B sono quindi $\binom{n-1}{k-1} + \binom{n-1}{k}$.

Osservazione 8. La proposizione precedente afferma che è possibile calcolare $\binom{n}{k}$ conoscendo i binomiali $\binom{n-1}{\dots}$. Se ordiniamo su righe i binomiali con lo stesso coefficiente "alto" n e su colonne i binomiali con lo stesso coefficiente "basso" k, otteniamo il seguente triangolo, detto *triangolo di Tartaglia*:

$$\binom{0}{0}$$

$$\binom{1}{0} \quad \binom{1}{1}$$

$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$

$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$

$$\binom{k}{0} \quad \binom{k}{1} \quad \dots \quad \dots \quad \dots \quad \binom{k}{k}$$

$$\dots \quad \dots$$

Tenuto conto di **Osserv. 7** e di **Prop. 6**, i valori numerici delle prime righe del triangolo sono

$$\begin{array}{cccccccc}
1 & & & & & & & \\
1 & 1 & & & & & & \\
1 & 2 & 1 & & & & & \\
1 & 3 & 3 & 1 & & & & \\
1 & 4 & 6 & 4 & 1 & & & \\
1 & 5 & 10 & 10 & 5 & 1 & & \\
1 & 6 & 15 & 20 & 15 & 6 & 1 & \\
1 & 7 & 21 & 35 & 35 & 21 & 7 & 1 \\
\dots & \dots & & & & & &
\end{array}$$

Proposizione 7. (*Formula del binomiale*). *Per ogni* $n,\ k \in \boldsymbol{N}$, *tali che* $1 \le k \le n$, *risulta:*

$$\binom{n}{k} = \frac{n(n-1)\ \dots\ (n-k+1)}{k!}.$$

Dim. Sia A un insieme con n elementi e sia B un insieme con k elementi (con $1 \le k \le n$). Conteremo in due modi diversi le applicazioni iniettive da B ad A.

(a) Dalla **Prop. 5**, la cardinalità delle applicazioni iniettive da B ad A è $n(n-1)\dots(n-k+1)$.

(b) Ogni applicazione iniettiva $f : B \to A$ si fattorizza nella forma

$$f = i \circ f_{su} : B \to Im\, f \hookrightarrow A \quad [\text{cfr. } \textbf{Osserv. 5}(v)].$$

$Im\, f$ è un sottoinsieme di k elementi di A: dunque può essere scelto in $\binom{n}{k}$ modi. f_{su} è una biiezione tra B e $Im\, f$: dunque può essere scelta in $k!$ modi. Per f si hanno quindi $\binom{n}{k}\, k!$ possibili scelte.

Dunque si ha: $\binom{n}{k}\, k! = n(n-1)\dots(n-k+1)$, da cui segue la formula cercata.

Osservazione 9. (i) Risulta: $\binom{n}{k} = \frac{n!}{k!\,(n-k)!} = \binom{n}{n-k}$.

Infatti: $\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!} \cdot \frac{(n-k)!}{(n-k)!} = \frac{n!}{k!\,(n-k)!}$. Inoltre: $\binom{n}{n-k} = \frac{n!}{(n-k)!\,(n-(n-k))!} = \frac{n!}{(n-k)!\,k!} = \binom{n}{k}$.

(ii) Il motivo per cui $\binom{n}{k}$ è chiamato *coefficiente binomiale* sta nel fatto che vale la seguente formula [che verrà dimostrata per induzione, cfr. **Prop. 5.7**]:

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

Dunque i coefficienti binomiali sono i coefficienti dello sviluppo della potenza n-sima del binomio $x+y$.

3 Relazioni su un insieme

Definizione 1. *Sia A un insieme non vuoto. Si chiama relazione su A ogni sottoinsieme $\rho \subseteq A\times A$. Se $(a_1, a_2) \in \rho$, si scrive $a_1 \rho a_2$; se invece $(a_1, a_2) \notin \rho$, si scrive $a_1 \not\rho a_2$.*

Osservazione 1. Una relazione ρ su A si identifica ad una corrispondenza di A in A [cioè ad un'applicazione $A \to \boldsymbol{\mathcal{P}}(A)$].

Infatti, ad ogni $\rho \subseteq A\times A$ si associa l'applicazione $F_\rho : A \to \boldsymbol{\mathcal{P}}(A)$ tale che

$$F_\rho(a) = \big\{b \in A \ : \ a\rho b\big\} \in \boldsymbol{\mathcal{P}}(A), \quad \forall\, a \in A.$$

Viceversa, ad ogni $F : A \to \boldsymbol{\mathcal{P}}(A)$ si associa la relazione

$$\rho_{_F} = \big\{(a, b) \in A\times A \ : \ b \in F(a), \ \forall\, a \in A\big\}.$$

Si tratta di verificare che queste due costruzioni sono inverse l'una dell'altra e cioè che:

$$(i) \ \ F_{\rho_{_F}} = F, \ \ \forall\, F : A \to \boldsymbol{\mathcal{P}}(A); \qquad (ii) \ \ \rho_{_{F_\rho}} = \rho, \ \ \forall\, \rho \subseteq A\times A.$$

Infatti:

(i) $F_{\rho_{_F}}(a) = \{b \in A \ : \ a\rho_{_F} b\} = \{b \in A \ : \ (a, b) \in \rho_{_F}\} = \{b \in A \ : \ b \in F(a)\} = F(a)$.

(ii) $a\rho_{_{F_\rho}} b \iff b \in F_\rho(a) \iff a\rho b$. Dunque $\rho_{_{F_\rho}} = \rho$.

Osservazione 2. Su ogni insieme non vuoto sono sempre definite le tre seguenti relazioni:

(i) la *relazione identica*: $a\,\rho\, b \iff a = b, \ \ \forall\, a, b \in A$ [cioè $\rho = \{(a, a), \ \forall\, a \in A\} =: \Delta_{_A}$, detta *diagonale di* A].

(ii) la *relazione caotica*: $a\,\rho\, b \iff a, b \in A$ [cioè $\rho = A\times A$].

(iii) la *relazione vuota*: $a \not\rho b, \ \ \forall\, a, b \in A$ [cioè $\rho = \emptyset$].

Osservazione 3. (i) Se $A = \{a_1, a_2, \ldots, a_n\}$ è un insieme finito, una relazione ρ su A può essere rappresentata in "forma cartesiana" (o "matriciale"), ponendo

$$a_i \times a_j = \begin{cases} 0, & \text{se } \ a_i \not\rho a_j \\ 1, & \text{se } \ a_i \rho\, a_j \,. \end{cases}$$

Ad esempio, se $A = \{a, b, c, d\}$ e $\rho = \{(a, a), (b, b), (c, c), (a, d), (c, d)\}$, allora ρ è rappresentata con la seguente tavola di 0, 1:

ρ	a	b	c	d
a	1	0	0	1
b	0	1	0	0
c	0	0	1	1
d	0	0	0	0

Si noti che le relazioni su un insieme A di cardinalità n sono 2^{n^2}: infatti sono in corrispondenza biunivoca con le matrici quadrate di ordine n formate da soli 0, 1.

(ii) Se A_1 è un sottoinsieme di A e ρ è una relazione su A, resta definita su A_1 la relazione ρ_1 *indotta da* ρ *su* A_1, ponendo $\rho_1 := \rho \cap (A_1\times A_1)$. Dunque: $a\rho_1 b \iff a\rho b, \ \forall\, a, b \in A_1$.

Definizione 2. *Una relazione ρ su A è detta:*

- *riflessiva, se $a\,\rho\, a, \ \ \forall\, a \in A$;*
- *simmetrica, se $a\,\rho\, b \implies b\,\rho\, a, \ \ \forall\, a, b \in A$;*
- *transitiva, se $a\,\rho\, b$ e $b\,\rho\, c \implies a\,\rho\, c, \ \ \forall\, a, b, c \in A$;*
- *antisimmetrica, se $a\,\rho\, b$ e $b\,\rho\, a \implies a = b, \ \ \forall\, a, b \in A$*

- *totale, se risulta* $a \rho b$ *oppure* $b \rho a$, $\forall\, a, b \in A$.

Una relazione riflessiva, simmetrica e transitiva è detta relazione di equivalenza. Una relazione riflessiva e transitiva è detta relazione di pre-ordine. Una relazione riflessiva, antisimmetrica e transitiva è detta relazione di ordine. Infine una relazione di ordine che è anche totale è detta relazione di ordine totale.

Esempi 1. (*i*) La relazione identica è riflessiva, simmetrica, transitiva, antisimmetrica, ma non totale. Dunque è una relazione di equivalenza e di ordine (non totale).

(*ii*) La relazione caotica è riflessiva, simmetrica, transitiva, totale, ma non antisimmetrica. La relazione vuota è simmetrica, antisimmetrica, transitiva [in modo banale], ma non è riflessiva né totale.

(*iii*) La relazione ρ definita in **Osserv. 3** non ha alcuna di queste proprietà.

(*iv*) In $\boldsymbol{N}$ introduciamo la seguente *relazione di divisibilità*: $\forall\, a, b \in \boldsymbol{N}$:

$$a \,|\, b \iff b = at,\ \exists\, t \in \boldsymbol{N},$$

[$a \,|\, b$ si legge: a *divide* b, oppure a *è un divisore di* b, oppure anche b *è un multiplo di* a]. Risulta:

(a) $a \,|\, a$ [infatti $a = a \cdot 1$];

(b) $a \,|\, b,\ b \,|\, c \implies a \,|\, c$ [infatti $b = at,\ c = bs \implies c = ats$];

(c) $a \,|\, b,\ b \,|\, a \implies a = b$ [infatti $b = at,\ a = bs \implies b = bst \implies st = 1 \implies s = 1 \implies b = a$];

(d) $a \,|\, b \not\Longrightarrow b \,|\, a$ [ad esempio $2 \,|\, 4$ ma $4 \not| 2$];

(e) ad esempio $2 \not| 3$ e $3 \not| 2$.

Dunque la relazione di divisibilità in $\boldsymbol{N}$ è una relazione di ordine (non totale).

Osservazione 4. Se ρ è una relazione riflessiva su A, allora $\Delta_A \subseteq \rho$. Se ρ è una relazione simmetrica ed antisimmetrica, allora $\rho \subseteq \Delta_A$. Infatti, per ipotesi $\begin{cases} a \rho b \implies b \rho a, \\ a \rho b,\ b \rho a \implies a = b. \end{cases}$ Ne segue: $a \rho b \implies a = b$, cioè $\rho \subseteq \Delta_A$.

($\boldsymbol{A}$) RELAZIONI DI EQUIVALENZA

Ci occuperemo ora delle *relazioni di equivalenza*, cioè delle relazioni riflessive, simmetriche e transitive.

Definizione 3. *Sia* ρ *una relazione di equivalenza su* A. *Per ogni* $a \in A$, *il sottoinsieme di* A

$$[a] = [a]_\rho := \{x \in A \,:\, a \rho x\}$$

è detto classe di equivalenza di a *modulo* ρ. *Ovviamente, per la simmetria di* ρ, $[a] = \{x \in A \,:\, x \rho a\}$.

Proposizione 1. *Sia* ρ *una relazione di equivalenza su* A. *Si ha:*

(i) $a \in [a],\ \forall\, a \in A$.

(ii) $[a] = [b] \iff a \rho b$.

(iii) $[a] \cap [b] = \emptyset \iff a \not\rho b$.

(iv) Le classi di equivalenza modulo ρ *(a due a due distinte) formano una partizione di* A.

Dim. (*i*) Da $a \rho a$ segue che $a \in [a]$.

(*ii*) ($\implies$). Poiché $b \in [b] = [a]$, allora $a \rho b$.

($\Longleftarrow$). Sia $x \in [a]$. Si ha: $x \rho a$, $a \rho b$ e quindi, per transitività, $x \rho b$, cioè $x \in [b]$. Dunque $[a] \subseteq [b]$. In modo analogo si verifica che $[b] \subseteq [a]$.

(*iii*) Dimostreremo che $[a] \cap [b] \neq \emptyset \iff a \rho b$.

($\Longrightarrow$). Se $x \in [a] \cap [b]$, allora $a \rho x$, $x \rho b$ e quindi (per transitività) $a \rho b$.

($\Longleftarrow$). Segue da (*ii*) e (*i*).

(*iv*) La famiglia

$$\mathfrak{U} = \mathfrak{U}_\rho = \big\{[a],\ \forall\, a \in A\big\},$$

formata da tutte le classi di equivalenza a due a due distinte di A (modulo ρ), è un ricoprimento di A [in base a (*i*)]; inoltre due classi distinte sono disgiunte [in base a (*ii*) e (*iii*)]. Ne segue che $\mathfrak{U}$ è una partizione di A (cfr. **Def. 1.5**).

Osservazione 5. Dalla proposizione precedente segue che ogni relazione di equivalenza ρ induce una partizione $\mathfrak{U}_\rho$.

Vale anche il viceversa. Sia infatti $\mathfrak{U} = \{A_i,\ i \in I\}$ una partizione di A formata da sottoinsiemi non vuoti; possiamo definire su A la seguente relazione $\rho = \rho_{\mathfrak{U}}$:

$$a \rho b \iff a, b \in A_i,\ \exists\, i \in I.$$

Si verifica subito che ρ è una relazione di equivalenza su A. Le classi di equivalenza *modulo* ρ sono gli insiemi $A_i \in \mathfrak{U}$. Si verifichi poi che $\mathfrak{U}_{\rho_{\mathfrak{U}}} = \mathfrak{U}$ e che $\rho_{\mathfrak{U}_\rho} = \rho$.

Definizione 4. *Sia ρ una relazione di equivalenza su A. Si chiama insieme quoziente di A modulo ρ l'insieme $A/_\rho$ formato dalle classi di equivalenza (a due a due distinte) di A modulo ρ, cioè*

$$A/_\rho = \big\{[a],\ \forall\, a \in A\big\}.$$

L'applicazione

$$\pi : A \to A/_\rho,\ \textit{tale che}\ \ \pi(a) = [a],\ \forall\, a \in A,$$

è ovviamente suriettiva ed è chiamata proiezione canonica di A su $A/_\rho$.

Definizione 5. *Ad ogni applicazione $f : A \to B$ resta "canonicamente" associata una relazione ρ_f su A, così definita:*

$$a_1 \rho_f a_2 \iff f(a_1) = f(a_2),\ \ \forall\, a_1, a_2 \in A.$$

Si verifica subito che ρ_f è una relazione di equivalenza su A, detta relazione di equivalenza associata ad f.

Si noti che se f è iniettiva ρ_f è la relazione identica su A (e viceversa). Inoltre, essendo $[a]_{\rho_f} = f^{-1}(f(a))$, $\forall\, a \in A$, risulta subito che

$$A/_{\rho_f} = \big\{f^{-1}(b),\ \forall\, b \in Im(f)\big\}.$$

Proposizione 2. *Sia $f : A \to B$ un'applicazione e sia ρ_f la relazione di equivalenza associata ad f. È ben definita la seguente applicazione*

$$F : A/_{\rho_f} \to B\ \ \textit{tale che}\ \ F([a]) = f(a),\ \ \forall\, [a] \in A/_{\rho_f}.$$

Inoltre F è iniettiva.

Dim. Dimostrare che F è "ben definita", significa dimostrare che la definizione di F non dipende dal rappresentante scelto in ogni classe, cioè che

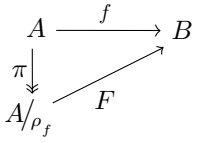
$$[a] = [a_1] \implies F([a]) = F([a_1]).$$

Infatti: $[a] = [a_1] \iff a \rho_f a_1 \iff f(a) = f(a_1) \iff F([a]) = F([a_1])$.

Dalle precedenti implicazioni (lette da destra a sinistra) segue che $F([a]) = F([a_1]) \implies [a] = [a_1]$, cioè che F è iniettiva.

Osservazione 6. (*i*) Si noti che F è l'<u>unica</u> applicazione tale che $F \circ \pi = f$, cioè tale che il

seguente diagramma (di insiemi e applicazioni)



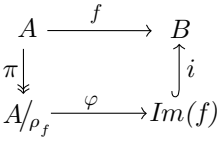
è commutativo [nel senso che "il passaggio da un insieme ad un altro è indipendente da ogni possibile percorso (che usi le applicazioni assegnate)"]. Infatti, se $\tilde{F} : A/_{\rho_f} \to B$ verifica $\tilde{F} \circ \pi = f$, allora $\tilde{F}([a]) = (\tilde{F} \circ \pi)(a) = f(a) = F([a]),\ \forall\, [a] \in A/_{\rho_f}$. Dunque $\tilde{F} = F$.

(*ii*) Si noti che F agisce come f e che F è iniettiva. Dunque F risolve il problema di rendere iniettiva o "iniettivizzare" f [modificandone però l'insieme di definizione].

(*iii*) Risulta: F è suriettiva $\iff$ f è suriettiva. Infatti:

$$F \text{ è suriettiva} \iff \forall\, b \in B,\ \exists\, [a] \in A/_{\rho_f} \text{ tale che } F([a]) = b \iff$$
$$\iff \forall\, b \in B,\ \exists\, a \in A \text{ tale che } f(a) = b \iff f \text{ è suriettiva.}$$

Proposizione 3. (*Teorema di decomposizione delle applicazioni*). *Sia $f : A \to B$ un'applicazione tra insiemi. Esiste un'unica biiezione $\varphi : A/_{\rho_f} \to Im(f)$ tale che $f = i \circ \varphi \circ \pi$, cioè tale che rende commutativo il diagramma:*



[Dunque ogni applicazione si decompone in maniera "standard" nel prodotto operatorio di tre applicazioni: una suriettiva, una biiettiva ed una iniettiva].

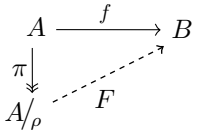
Dim. Dalla **Prop. 2**, è ben definita ed iniettiva un'applicazione $F : A/_{\rho_f} \to B$ tale che $F \circ \pi = f$. Si osservi che $Im\, f = Im\, F$. Pertanto $\varphi := F_{su} : A/_{\rho_f} \to Im\, f$ è biiettiva. Si ha poi, $\forall\, a \in A$:

$$(i \circ \varphi \circ \pi)(a) = (i \circ \varphi)([a]) = i(\varphi([a])) = i(F([a])) = i(f(a)) = f(a).$$

Quindi $f = i \circ \varphi \circ \pi$.

L'unicità di φ è evidente [si verifichi che se $i \circ \psi \circ \pi = i \circ \varphi \circ \pi$, allora $\psi = \varphi$].

Vogliamo ora generalizzare la precedente costruzione. Sono assegnati: un'applicazione $f : A \to B$ ed un'arbitraria relazione di equivalenza ρ su A. Vogliamo determinare in quali ipotesi f *si fattorizza tramite* ρ, cioè quando è definita un'applicazione $F : A/_{\rho} \to B$ tale che $F \circ \pi = f$, ovvero tale che il diagramma



è commutativo. La risposta al problema è fornita dal teorema che segue.

Teorema 1. (*Teorema fondamentale delle applicazioni*). *Sia $f : A \to B$ un'applicazione e sia ρ una relazione di equivalenza su A. Risulta:*

$$\left[\, \exists\, F : A/_{\rho} \to B \text{ tale che } F \circ \pi = f \right] \iff \rho \subseteq \rho_f$$

Se una siffatta applicazione F esiste, essa è unica. Inoltre:

(a) F è iniettiva $\iff$ $\rho = \rho_f$;

(b) F è suriettiva $\iff$ f è suriettiva.

Dim. Si noti che, dovendo essere commutativo il diagramma sopra indicato, F è necessariamente così definita:

$$F([a]) = f(a), \quad \forall\, [a] \in A/_\rho.$$

Ne segue:

$$F \text{ esiste} \iff \text{la precedente definizione è ben posta} \iff$$
$$\iff \big[\, [a_1] = [a_2] \implies F([a_1]) = F([a_2]) \,\big] \iff$$
$$\iff \big[\, a_1 \rho\, a_2 \implies f(a_1) = f(a_2) \,\big] \iff \big[\, a_1 \rho\, a_2 \implies a_1 \rho_f\, a_2 \,\big] \iff \rho \subseteq \rho_f\,.$$

L'unicità di F è evidente: se $\tilde{F} \circ \pi = f$, allora

$$\tilde{F}([a]) = (\tilde{F} \circ \pi)(a) = f(a) = (F \circ \pi)(a) = F([a]), \quad \forall\, [a] \in A/_\rho.$$

(a) F è iniettiva $\iff \big[\, F([a_1]) = F([a_2]) \implies [a_1]) = [a_2] \,\big] \iff$

$$\iff \big[\, f(a_1) = f(a_2) \implies a_1 \rho\, a_2 \,\big] \iff \big[\, a_1 \rho_f\, a_2 \implies a_1 \rho\, a_2 \,\big] \iff \rho_f \subseteq \rho.$$

Poiché, in ogni caso, $\rho \subseteq \rho_f$, allora F è iniettiva $\iff \rho = \rho_f$.

(b) F è suriettiva $\iff \forall\, b \in B,\ \exists\, [a] \in A/_\rho$ tale che $F([a]) = b \iff$

$$\iff \forall\, b \in B,\ \exists\, a \in A \text{ tale che } f(a) = b \iff f \text{ è suriettiva.}$$

Osservazione 7. Per valutare l'utilità e l'importanza dei risultati precedenti, osserviamo quanto segue.

Assegnata una relazione di equivalenza ρ su A, le classi di equivalenza modulo ρ, "nate" come *sottoinsiemi* di A, vengono poi pensate come *elementi* di $A/_\rho$. L'esigenza di dover interpretare come elementi dei sottoinsiemi può provocare qualche difficoltà, soprattutto quando occorra eseguire calcoli su $A/_\rho$. Per tale motivo è senz'altro utile poter identificare $A/_\rho$ con un insieme B, i cui elementi siano meglio individuabili, cioè "più concreti". Dal **Teor. 1** e dalla **Prop. 2** segue immediatamente che basta "cercare" un'applicazione f definita su A e tale che $\rho_f = \rho$, perché allora $Im(f)$ è identificabile (cioè in biiezione) con $A/_\rho$.

La difficoltà nella individuazione di un siffatto "modello concreto" $Im(f)$ di $A/_\rho$ sta nel fatto che l'applicazione f cercata non è assegnata ma va "inventata"!

Verificheremo tali considerazioni su alcuni esempi.

Esempio 1. In $\boldsymbol{Z}$ si introduce la seguente relazione ρ:

$$a\, \rho\, b \iff |a| = |b|, \quad \forall\, a, b \in \boldsymbol{Z}.$$

Si verifica facilmente che ρ è una relazione di equivalenza su A e si ha:

$$[a] = \{a, -a\}, \quad \forall\, a \in \boldsymbol{Z}.$$

Vogliamo descrivere $\boldsymbol{Z}/_\rho$. Definiamo $f : \boldsymbol{Z} \to \boldsymbol{N}$ tale che $f(a) = |a|$, $\forall\, a \in \boldsymbol{Z}$. Ovviamente f è suriettiva. Inoltre $a\, \rho_f\, b \iff |a| = |b| \iff a\, \rho b$. Dunque $\rho_f = \rho$. Pertanto

$$F : \boldsymbol{Z}/_\rho \to \boldsymbol{N} \text{ tale che } F([a]) = |a|, \quad \forall\, [a] \in \boldsymbol{Z}/_\rho,$$

è una biiezione e $\boldsymbol{Z}/_\rho$ può essere identificato con $\boldsymbol{N}$.

Esempio 2. In $\boldsymbol{Z}$ consideriamo la seguente partizione

$$\mathfrak{U} = \big\{\{2n,\, 2n+1\}, \quad \forall\, n \in \boldsymbol{Z}\big\}.$$

Sia ρ la relazione di equivalenza associata ad $\mathfrak{U}$. Si ha:

$$a \rho\, b \iff \exists\, n \in \boldsymbol{Z} \ :\ a, b \in \{2n,\, 2n+1\}.$$

Vogliamo descrivere $\boldsymbol{Z}/_\rho$. Sia $\boldsymbol{P} = \{2n, \ \forall\, n \in \boldsymbol{Z}\}$ l'insieme dei relativi pari. Sia

$$f : \boldsymbol{Z} \to \boldsymbol{P} \text{ tale che, } \quad \forall\, a \in \boldsymbol{Z},\ f(a) = \begin{cases} a, \text{ se } a \text{ è pari,} \\ a - 1, \text{ se } a \text{ è dispari.} \end{cases}$$

Ovviamente f è suriettiva. Se verifichiamo che $\rho_f = \rho$, allora f induce una biiezione tra $\boldsymbol{Z}/_\rho$ e $\boldsymbol{P}$ e quindi $\boldsymbol{P}$ è un "modello concreto" di $\boldsymbol{Z}/_\rho$. Si ha infatti: $a\, \rho_f\, b \iff f(a) = f(b) \iff$

$$\iff \begin{cases} a=b, \text{ se } a, b \text{ sono pari} \\ a-1=b-1, \text{ se } a, b \text{ sono dispari} \\ a=b-1, \text{ se } a \text{ è pari e } b \text{ è dispari} \\ a-1=b, \text{ se } a \text{ è dispari e } b \text{ è pari,} \end{cases} \iff \begin{cases} a=b, \text{ se } a, b \text{ hanno la stessa parità} \\ b=a+1, \text{ se } a \text{ è pari} \\ b=a-1, \text{ se } a \text{ è dispari} \end{cases}$$

$$\iff a, b \in \{2n, 2n+1\},\ \exists\, n \in \boldsymbol{Z} \iff a \,\rho\, b.$$

Esempio 3. Per ogni $t \in \boldsymbol{R}$, $t \geq 0$, sia $\boldsymbol{C}_t$ la circonferenza del piano $\boldsymbol{R}^2$ di centro $O=(0,0)$ e raggio t. La famiglia $\mathfrak{U} = \{\boldsymbol{C}_t,\ \forall\, t \geq 0\}$ è una partizione di $\boldsymbol{R}^2$. Denotata con ρ la relazione di equivalenza associata ad $\mathfrak{U}$, vogliamo determinare un modello concreto di $\boldsymbol{R}^2/_\rho$.

Si osservi che $(x,y) \in \boldsymbol{C}_t \iff \sqrt{x^2+y^2} = t$. Ne segue che, $\forall\,(x,y), (x_1,y_1) \in \boldsymbol{R}^2$,
$(x,y)\rho(x_1,y_1) \iff (x,y), (x_1,y_1) \in \boldsymbol{C}_t,\ \exists\, t \geq 0 \iff$
$\iff \sqrt{x^2+y^2} = t = \sqrt{x_1^2+y_1^2},\ \exists\, t \geq 0 \iff \sqrt{x^2+y^2} = \sqrt{x_1^2+y_1^2}.$

Sia quindi $f : \boldsymbol{R}^2 \to \boldsymbol{R}^{\geq 0}$ la seguente applicazione:

$$f(x,y) = \sqrt{x^2+y^2},\ \ \forall\,(x,y) \in \boldsymbol{R}^2.$$

f è certamente suriettiva. Infatti, $\forall\, a \geq 0$, $f(a,0) = a$. Inoltre $\rho_f = \rho$. Si conclude che l'insieme quoziente $\boldsymbol{R}^2/_\rho$ può essere identificato con la semiretta $\boldsymbol{R}^{\geq 0}$, tramite la biiezione

$$F : \boldsymbol{R}^2/_\rho \to \boldsymbol{R}^{\geq 0}, \text{ tale che } F([(x,y)]_\rho) = \sqrt{x^2+y^2},\ \ \forall\,[(x,y)]_\rho \in \boldsymbol{R}^2/_\rho.$$

($\boldsymbol{B}$) RELAZIONI DI ORDINE

Nella parte restante di questo paragrafo ci occuperemo di insiemi ordinati. Introduciamo la seguente terminologia. Una relazione di ordine (cioè riflessiva, antisimmetrica e transitiva) su un insieme A sarà denotata con $\leq$ [in luogo di ρ]. Ad essa è "naturalmente" associata la corrispondente *relazione di ordine stretta* $<$, così definita:

$$a < b \iff a \leq b \ \text{ e } \ a \neq b.$$

La coppia $(A, \leq)$ è detta *insieme ordinato* (o *parzialmente ordinato*). Se $\leq$ è una relazione di ordine totale, $(A, \leq)$ è detto *insieme totalmente ordinato*. [Si osservi che, se $(A, \leq)$ è totalmente ordinato, si ha: $a \not\leq b \iff b < a$].

Ad esempio, $(\boldsymbol{Z}, \leq)$ è totamente ordinato [rispetto alla relazione: $a \leq b \iff b-a \in \boldsymbol{N}$]. Anche $(\boldsymbol{R}, \leq)$ è totamente ordinato [rispetto alla relazione: $a \leq b \iff b-a \geq 0$]. Invece, se A è un insieme con almeno due elementi, $(\boldsymbol{\mathcal{P}}(A), \subseteq)$ è un insieme ordinato ma non totamente ordinato. Si verifica subito che una relazione d'ordine $\leq$ su A *induce* una relazione d'ordine su ogni sottoinsieme non vuoto $B \subseteq A$. Si noti infine che, tramite $\leq$, è possibile definire su A la relazione $\geq$, detta *relazione opposta di* $\leq$, in questo modo: $a \geq b \iff b \leq a$. Si verifica subito che $\geq$ verifica le stesse proprietà di $\leq$.

Definizione 6. *Sia $(A, \leq)$ un insieme ordinato e sia $S \subseteq A$, $S \neq \emptyset$. Un elemento $s_0 \in S$ è detto minimo di S se $s_0 \leq s$, $\forall\, s \in S$. Se un tale elemento esiste, è unico ed è denotato $min(S)$. Analogamente, un elemento $s_1 \in S$ è detto massimo di S se $s \leq s_1$, $\forall\, s \in S$. Se esiste, è unico ed è denotato $max(S)$. In particolare, se $S = A$, $min(A)$ e $max(A)$ (se esistono) sono rispettivamente detti primo elemento e ultimo elemento di A. Infine, $(A, \leq)$ è detto insieme bene ordinato se ogni sottoinsieme non vuoto di A ammette minimo.*

Ovviamente, ogni insieme bene ordinato è totalmente ordinato [infatti ogni sottoinsieme $\{a, b\} \subseteq A$ ammette minimo], mentre il viceversa è falso [ad esempio $(\boldsymbol{Z}, \leq)$ non è bene ordinato].

Definizione 7. *Sia $(A, \leq)$ un insieme ordinato e sia $S \subseteq A$, $S \neq \emptyset$. Un elemento $a \in A$ è detto minorante di S se $a \leq s$, $\forall\, s \in S$; un elemento $a \in A$ è detto maggiorante di S se $s \leq a$, $\forall\, s \in S$. Denoteremo con $Minor(S)$ [rispett. $Maggior(S)$] l'insieme dei minoranti [rispett. maggioranti] di S. Infine, S è detto limitato inferiormente se $Minor(S) \neq \emptyset$ [cioè se S ha almeno un minorante],*

mentre è detto limitato superiormente se $Maggior(S) \neq \emptyset$ *[cioè se* S *ha almeno un maggiorante].*

Definizione 8. *Sia* $(A, \leq)$ *un insieme ordinato e sia* $S \subseteq A,\ S \neq \emptyset$. *Se* S *è limitato inferiormente, si chiama estremo inferiore di* S *(se esiste) il massimo dei minoranti di* S. *È denotato* $inf(S)$. *Analogamente, se* S *è limitato superiormente, si chiama estremo superiore di* S *(se esiste) il minimo dei maggioranti di* S. *È denotato* $sup(S)$.

Osservazione 8. Poiché $inf(S) = max(Minor(S))$, si ha:

$$x_0 = inf(S) \iff \begin{cases} x_0 \in Minor(S) \\ y \in Minor(S) \implies y \leq x_0 \end{cases} \iff \begin{cases} x_0 \leq s,\ \forall\, s \in S \\ y \not\leq x_0 \implies y \notin Minor(S) \end{cases} \iff$$
$$\iff \begin{cases} x_0 \leq s,\ \forall\, s \in S \\ y \not\leq x_0 \implies \exists\, s_0 \in S\ :\ y \not\leq s_0. \end{cases}$$

Se ora $(A, \leq)$ è totalmente ordinato, dal fatto (già osservato) che $a \not\leq b \iff b < a$, segue che

$$x_0 = inf(S) \iff \begin{cases} x_0 \leq s,\ \forall\, s \in S \\ x_0 < y \implies \exists\, s_0 \in S\ :\ s_0 < y. \end{cases}$$

In modo analogo, si verifica che

$$x_1 = sup(S) \iff \begin{cases} s \leq x_1,\ \forall\, s \in S \\ x_1 \not\leq z \implies \exists\, s_1 \in S\ :\ s_1 \not\leq z. \end{cases}$$

Se poi $(A, \leq)$ è totalmente ordinato, si ha:

$$x_1 = sup(S) \iff \begin{cases} s \leq x_1,\ \forall\, s \in S \\ z < x_1 \implies \exists\, s_1 \in S\ :\ z < s_1. \end{cases}$$

Ad esempio, $(\boldsymbol{R}, \leq)$ è totalmente ordinato. Se denotiamo con $x_0 + \varepsilon$ un arbitrario numero reale $y > x_0$ e con $x_1 - \varepsilon$ un arbitrario numero reale $z < x_1$ [avendo assunto $\varepsilon \in \boldsymbol{R},\ \varepsilon > 0$], si ottengono le ben note definizioni di inf e sup in $\boldsymbol{R}$:

$$x_0 = inf(S) \iff \begin{cases} x_0 \leq s,\ \forall\, s \in S \\ \forall\, \varepsilon > 0,\ \exists\, s_0 \in S\ :\ s_0 < x_0 + \varepsilon, \end{cases}$$
$$x_1 = sup(S) \iff \begin{cases} s \leq x_1,\ \forall\, s \in S \\ \forall\, \varepsilon > 0,\ \exists\, s_1 \in S\ :\ x_1 - \varepsilon < s_1. \end{cases}$$

Osservazione 9. Sia $(A, \leq)$ un insieme ordinato e sia $S \subseteq A,\ S \neq \emptyset$. Si osserva subito che, se $\exists\, min(S)$, allora $inf(S) = min(S)$. Infatti, posto $s_0 = min(S)$, si ha:

- $s_0 \in Minor(S)$ [infatti $s_0 \leq s,\ \forall\, s \in S$];
- se $a \in Minor(S)$, allora $a \leq s_0$; dunque $s_0 = max(Minor(S)) = inf(S)$.

Analogamente, se $\exists\, max(S)$, allora $sup(S) = max(S)$.

Viceversa, può esistere $inf(S)$ senza che esista $min(S)$. Ad esempio, in $(\boldsymbol{R}, \leq)$, denotato con $\boldsymbol{R}^+$ l'insieme dei reali strettamente positivi, risulta: $inf(\boldsymbol{R}^+) = 0$, mentre $min(\boldsymbol{R}^+)$ non esiste.

Come altro esempio, consideriamo l'insieme ordinato $(\boldsymbol{\mathcal{P}}(A), \subseteq)$ [con A insieme avente almeno due elementi]. Ogni sottoinsieme S di $\boldsymbol{\mathcal{P}}(A)$ ammette inf e sup: se infatti $S = \{A_i\}_{i \in I}$, allora

$$inf(S) = \bigcap_{i \in I} A_i\,, \qquad sup(S) = \bigcup_{i \in I} A_i\,.$$

Invece, scelti $a_1, a_2 \in A,\ a_1 \neq a_2$, l'insieme $S = \big\{\{a_1\}, \{a_2\}\big\}$ non ha né massimo né minimo.

Definizione 9. *Sia* $(A, \leq)$ *un insieme ordinato. Per ogni* $a \in A$, *ovviamente* $a \in Minor(\{a\})$ *e* $a \in Maggior(\{a\})$. *Se* $Minor(\{a\}) = \{a\}$ *[cioè* $x \leq a \implies x = a$*], si dice che* a *è un elemento minimale di* A. *Analogamente, se* $Maggior(\{a\}) = \{a\}$ *[cioè* $x \geq a \implies x = a$*], si dice che* a *è un elemento massimale di* A.

Osservazione 10. Se A ha il primo elemento [cioè il minimo] a_0, allora A non ha altri elementi minimali (oltre a_0); analogamente, se A ha l'ultimo elemento [cioè il massimo] a_1, allora A non

ha altri elementi massimali (oltre a_1). Ad esempio $(\boldsymbol{\mathcal{P}}(A), \subseteq)$ ha il primo elemento $[\emptyset]$ e l'ultimo elemento $[A]$: dunque non ha altri elementi minimali o massimali.

Quando un insieme ordinato ammette elementi massimali? Un'importante condizione sufficiente per tale esistenza è il seguente risultato (noto come *Lemma di Zorn*), che ci limitiamo qui ad enunciare. Premettiamo una definizione.

Definizione 10. *Sia $(A, \leq)$ un insieme ordinato. Un sottoinsieme non vuoto S di A è detto catena di A se $\forall\, x, y \in S$ risulta $x \leq y$ oppure $y \leq x$ [cioè se S è totalmente ordinato].*

Teorema 2 (*Lemma di Zorn*). *Sia $(A, \leq)$ un insieme ordinato. Se ogni catena di A ammette un maggiorante, allora A ha almeno un elemento massimale.*

Osservazione 11. Per dimostrare il Lemma di Zorn si fa ricorso ad una *funzione di scelta*. Per definizione, una *funzione di scelta relativa ad una famiglia $\{A_i\}_{i \in I}$ di sottoinsiemi non vuoti di A* è una funzione $\sigma : I \to A$ tale che $\sigma(i) \in A_i$, $\forall\, i \in I$. L'esistenza di una siffatta funzione non è un fatto ovvio (a dispetto dell'apparenza). Per definizione, accettarne l'esistenza significa accettare, nella teoria degli insiemi, l'*Assioma della Scelta*. Si dimostra anzi che l'assioma della scelta è equivalente al Lemma di Zorn, così come al *Teorema di Zermelo* [detto anche *Principio del Buon Ordinamento*: "ogni insieme può essere dotato di una relazione d'ordine, rispetto a cui è bene ordinato"].

A chi voglia approfondire tali questioni segnaliamo il testo di Fontana-Gabelli (citato in Bibliografia).

Una semplice applicazione del Lemma di Zorn è il seguente importante teorema, probabilmente noto dal corso di Algebra Lineare: *ogni K-spazio vettoriale ammette una base.* Dimostreremo tale risultato alla fine del prossimo paragrafo.

4 Operazioni e strutture algebriche

Definizione 1. *Sia A un insieme non vuoto. Ogni applicazione $* : A \times A \to A$ è chiamata operazione (binaria) su A. Per ogni $a_1, a_2 \in A$, si scrive $a_1 * a_2$ in luogo di $*(a_1, a_2)$.*

Sono ben noti vari esempi di operazioni tra insiemi:

- l'addizione e la moltiplicazione sugli insiemi numerici $\boldsymbol{N}$, $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$.
- la moltiplicazione righe per colonne sull'insieme $\mathfrak{M}_n(\boldsymbol{R})$ delle matrici quadrate di ordine n, a valori in $\boldsymbol{R}$.
- l'addizione sull'insieme $\mathfrak{M}_{m,n}(\boldsymbol{R})$ delle matrici ad m righe ed n colonne, a valori in $\boldsymbol{R}$.

Molte operazioni verificano le proprietà indicate nella definizione che segue.

Definizione 2. *Un'operazione $*$ su A è:*

(1) associativa se $(a * b) * c = a * (b * c)$, $\forall\, a, b, c \in A$;

(2) dotata di elemento neutro e se $\exists\, e \in A$ tale che $a * e = a = e * a$, $\forall\, a \in A$;

(3) dotata di reciproco di ogni elemento se $\forall\, a \in A$, $\exists\, a' \in A$ tale che $a * a' = e = a' * a$, $\forall\, a \in A$;

(4) commutativa se $a * b = b * a$, $\forall\, a, b \in A$.

Esempi 1. (*i*) L'addizione $+$ su $\boldsymbol{N}$ verifica le proprietà (*1*), (*2*), (*4*) ma non (*3*).

(*ii*) La moltiplicazione $\cdot$ su $\boldsymbol{N}$ verifica le proprietà (*1*), (*2*), (*4*) ma non (*3*).

(*iii*) L'addizione $+$ su $\boldsymbol{Z}$ (e su $\boldsymbol{Q}$ ed $\boldsymbol{R}$) verifica le proprietà (*1*), (*2*), (*3*) e (*4*).

(*iv*) La moltiplicazione $\cdot$ su $\boldsymbol{Z}$ verifica le proprietà (*1*), (*2*), (*4*) ma non (*3*).

(*v*) La moltiplicazione $\cdot$ su $\boldsymbol{Q}^{\cdot} := \boldsymbol{Q} - \{0\}$ e su $\boldsymbol{R}^{\cdot} := \boldsymbol{R} - \{0\}$ verifica le proprietà (*1*), (*2*), (*3*) e (*4*).

Nota. Negli esempi precedenti relativi all'addizione, l'elemento neutro è 0 ed il reciproco è detto *opposto*; relativamente alla moltiplicazione, l'elemento neutro è 1 ed il reciproco è detto *inverso*.

(*vi*) L'addizione $+$ su $\mathfrak{M}_{m,n}(\boldsymbol{R})$ verifica le proprietà (*1*), (*2*), (*3*) e (*4*).

(*vii*) Indicato con $\mathbf{GL}_n(\boldsymbol{R})$ l'insieme delle matrici quadrate <u>invertibili</u> di ordine $n \geq 2$ (ed a valori in $\boldsymbol{R}$), il prodotto righe per colonne su $\mathbf{GL}_n(\boldsymbol{R})$ verifica le proprietà (*1*), (*2*), (*3*) ma non (*4*). Infatti si ha:

- $(AB)C = (AB)C$, $\forall\, A, B, C \in \mathbf{GL}_n(\boldsymbol{R})$;
- $AI_n = I_nA = A$, $\forall\, A \in \mathbf{GL}_n(\boldsymbol{R})$, con I_n *matrice unità*;
- $A\,A^{-1} = A^{-1}A = I_n$, $\forall\, A \in \mathbf{GL}_n(\boldsymbol{R})$, con A^{-1} *matrice inversa* di A.
- in generale $AB \neq BA$; ad esempio $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

(*viii*) Per ogni insieme non vuoto X, il prodotto operatorio $\circ$ sull'insieme X^X [delle applicazioni di X in sé] verifica le proprietà (*1*) e (*2*), ma non (*3*) e (*4*). Se indichiamo con $\boldsymbol{S}(X)$ l'insieme delle biiezioni di X in sé, il prodotto operatorio $\circ$ [ristretto ad $\boldsymbol{S}(X)$, cfr. **Osserv. 2.6**] verifica anche la proprietà (*3*) [cfr. **Prop. 2.2**].

Definizione 3. *Si chiama gruppo ogni coppia $(A, *)$ tale che A è un insieme non vuoto (detto sostegno del gruppo) ed $*$ è un'operazione su A verificante le proprietà (1), (2), (3), cioè associativa, dotata di elemento neutro e dotata di reciproco di ogni elemento. Un gruppo $(A, *)$ è detto commutativo (o abeliano) se $*$ verifica (4), cioè è commutativa.*

Esempi 2. (*i*) $(\boldsymbol{Z}, +)$, $(\boldsymbol{Q}, +)$, $(\boldsymbol{R}, +)$ ed $(\mathfrak{M}_{m,n}(\boldsymbol{R}), +)$ sono gruppi commutativi. $(\boldsymbol{Q}^{\cdot}, \cdot)$ e $(\boldsymbol{R}^{\cdot}, \cdot)$ sono gruppi commutativi. $\big(\mathbf{GL}_n(\boldsymbol{R}), \cdot\big)$ è un gruppo non commutativo, se $n \geq 2$, detto *gruppo*

generale lineare di ordine n su $\boldsymbol{R}$. Anche $(\boldsymbol{S}(X), \circ)$ è un gruppo, detto *gruppo delle biiezioni di X.*

(*ii*) $(\boldsymbol{N}, +)$, $(\boldsymbol{N}^{\cdot}, \cdot)$ e $(\boldsymbol{Z}^{\cdot}, \cdot)$ non sono gruppi.

(*iii*) Sia X un insieme non vuoto. Su $\boldsymbol{\mathcal{P}}(X)$ sono definite le operazioni $\cup, \cap$ [unione ed intersezione di sottoinsiemi di X]. Entrambe sono associative, commutative e dotate di elemento neutro, ma non sono dotate di reciproco. Dunque $(\boldsymbol{\mathcal{P}}(X), \cup)$ e $(\boldsymbol{\mathcal{P}}(X), \cap)$ non sono gruppi.

Introduciamo su $\boldsymbol{\mathcal{P}}(X)$ la seguente operazione Δ, detta *differenza simmetrica*:

$$A \Delta B = (A - B) \cup (B - A).$$

Per ogni $A, B, C \in \boldsymbol{\mathcal{P}}(X)$, risulta:

- $A \Delta A = \emptyset$;
- $A \Delta \emptyset = \emptyset \Delta A = A$;
- $A \Delta (B \Delta C) = (A \Delta B) \Delta C$;
- $A \Delta B = B \Delta A$.

[Solo la terza proprietà non è banalissima]. Si conclude che $\big(\boldsymbol{\mathcal{P}}(X), \Delta\big)$ è un gruppo commutativo [con neutro $\emptyset$ e reciproco di ogni elemento coincidente con l'elemento stesso].

(*iv*) Siano $(A, *)$ e $(B, \bullet)$ due gruppi. Sul prodotto cartesiano $A \times B$ è definita l'operazione $\cdot$:

$$(a_1, b_1) \cdot (a_2, b_2) = \big(a_1 * a_2, b_1 \bullet b_2\big), \ \forall\, (a_1, b_1), (a_2, b_2) \in A \times B.$$

Si verifica facilmente che $(A \times B, \cdot)$ è un gruppo, detto *prodotto diretto di $(A, *)$ e $(B, \bullet)$.*

Proposizione 1. *In ogni gruppo $(A, *)$:*

(1) L'elemento neutro e è unico.

(2) Il reciproco di ogni elemento a è unico.

(3) Vale la legge di cancellazione $\begin{cases} \text{a sinistra:} & a * b = a * c \implies b = c \\ \text{a destra:} & a * b = c * b \implies a = c. \end{cases}$

(4) Il reciproco di un prodotto è il prodotto dei reciproci, in ordine inverso.

Dim. (*1*) Siano e, e' due elementi neutri di $(A, *)$. Allora

$$\begin{cases} e * e' = e' * e = e' & \text{essendo } e \text{ elemento neutro,} \\ e * e' = e' * e = e & \text{essendo } e' \text{ elemento neutro.} \end{cases}$$

Dunque $e = e'$.

(*2*) Siano a', a'' due reciproci di a. Allora $\begin{cases} a * a' = a' * a = e \\ a * a'' = a'' * a = e. \end{cases}$ Dunque, utilizzando la proprietà associativa ed il fatto che e è elemento neutro:

$$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''.$$

(*3*) Verifichiamo la legge di cancellazione a sinistra [per quella a destra si procede in modo analogo]. Moltiplicando l'uguaglianza $a * b = a * c$ a sinistra per a' [reciproco di a], si ottiene:

$$a' * (a * b) = a' * (a * c) \implies (a' * a) * b = (a' * a) * c \implies e * b = e * c \implies b = c.$$

(*4*) Dimostriamo che $(a * b)' = b' * a'$, $\forall\, a, b \in A$. Per l'unicità del reciproco, basta verificare che:

$$(a * b) * (b' * a') = e = (b' * a') * (a * b).$$

Verifichiamo la prima uguaglianza [per l'altra si procede in modo analogo]. Si ha:

$$(a * b) * (b' * a') = \big((a * b) * b'\big) * a' = \big(a * (b * b')\big) * a' = (a * e) * a' = a * a' = e.$$

In modo analogo si verifica che $(a_1 * a_2 * \ \dots\ * a_n)' = a'_n * \ \dots\ * a'_2 * a'_1$, $\forall\, a_1, a_2, \dots, a_n \in A$.

Definizione 4. *Si chiama sottogruppo di un gruppo $(A, *)$ ogni sottoinsieme non vuoto $B \subseteq A$ tale che $(B, *)$ è un gruppo (rispetto alla stessa operazione $*$ di A, opportunamente ristretta agli elementi di B).*

Esempi 3. (*i*) Ad esempio, $\boldsymbol{Z}$ è un sottogruppo di $(\boldsymbol{Q}, +)$, $\boldsymbol{Z}$ e $\boldsymbol{Q}$ sono sottogruppi di $(\boldsymbol{R}, +)$.

(*ii*) Indicato con $\mathbf{SL}_n(\boldsymbol{R})$ l'insieme delle matrici reali quadrate di ordine n, con *determinante* $= 1$, si può verificare, utilizzando le proprietà dei determinanti, che $\mathbf{SL}_n(\boldsymbol{R})$ è un sottogruppo di $\mathbf{GL}_n(\boldsymbol{R})$.

Definizione 5. *Siano* $(A,*)$ *e* $(B,\bullet)$ *due gruppi. Un'applicazione* $f : A \to B$ *è detta omomorfismo (di gruppi) se risulta:*

$$f(a_1 * a_2) = f(a_1) \bullet f(a_2), \quad \forall\, a_1,\, a_2 \in A.$$

In particolare, un omomorfismo biiettivo è detto isomorfismo. Se esiste un isomorfismo tra $(A,*)$ *e* $(B,\bullet)$*, si dice che* $(A,*)$ *e* $(B,\bullet)$ *sono isomorfi e scrive* $(A,*) \cong (B,\bullet)$*. Un isomorfismo di* $(A,*)$ *in sé è detto automorfismo.*

Esempi 4. (*i*) Si osservi che, indicato con $\boldsymbol{R}^+$ l'insieme dei reali positivi, $(\boldsymbol{R}^+,\cdot)$ è un gruppo [ovvero $\boldsymbol{R}^+$ é un sottogruppo di $(\boldsymbol{R}^{\cdot},\cdot)$]. L'applicazione *logaritmo (naturale)*

$$\lg : (\boldsymbol{R}^+,\cdot) \to (\boldsymbol{R},+)$$

[che associa ad ogni $a > 0$ il suo logaritmo naturale $\lg(a)$] è un isomorfismo di gruppi. Infatti, $\forall\, a,\, b > 0,\ \lg(ab) = \lg(a) + \lg(b)$.

(*ii*) Se X è un insieme finito formato da n elementi (che possiamo identificare con $\{1, 2, \ldots, n\}$), l'insieme $\boldsymbol{S}(X)$ delle biiezioni di X in sé viene usualmente denotato con $\boldsymbol{S}_n$ e $(\boldsymbol{S}_n, \circ)$ è un gruppo, detto *gruppo delle permutazioni su* n *elementi*. Ha $n!$ elementi.

Ogni permutazione $f \in \boldsymbol{S}_n$ invece di essere indicata nella forma

$$f : \begin{array}{l} 1 \longrightarrow f(1) =: f_1 \\ 2 \longrightarrow f(2) =: f_2 \\ \vdots \\ n \longrightarrow f(n) =: f_n \end{array}$$

è preferibilmente indicata nella forma

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f_1 & f_2 & \ldots & f_n \end{pmatrix}.$$

Se quindi $f,\, g \in \boldsymbol{S}_n$, allora

$$g \circ f = \begin{pmatrix} 1 & 2 & \ldots & n \\ g_{f_1} & g_{f_2} & \ldots & g_{f_n} \end{pmatrix}.$$

Se ad esempio $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \in \boldsymbol{S}_4$, allora

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

Nel seguito (cfr. **Cap. IV.3**) troveremo un modo "più economico" per scrivere le permutazioni e calcolarne la composizione.

Osserviamo poi che, nel calcolare $g \circ f$, prima agisce f e poi g. Dunque occorre seguire "a ritroso" l'azione di $g \circ f$ sugli elementi $1, 2, \ldots, n$. Poichè ciò è in contrasto con la nostra abitudine a leggere da sinistra verso destra, scriveremo fg in luogo di $g \circ f$. Dunque

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

Tale "convenzione" sarà adottata nel seguito.

Osservazione 1. Nello studio "astratto" dei gruppi si usa per lo più la *notazione moltiplicativa*. Un gruppo viene indicato con $(G,\cdot)$, il suo elemento neutro con 1 (o 1_G) ed il reciproco di un elemento $g \in G$ con g^{-1} (ed è detto *inverso di* g).

Talvolta però viene anche usata la *notazione additiva* $(G,+)$ [e ciò avviene soprattutto nello studio dei gruppi commutativi]. In tal caso si indica l'elemento neutro con 0 (o 0_G) ed il reciproco di un

elemento $g \in G$ con $-g$ (ed è detto *opposto di* g).

Si osserva facilmente che spesso in uno stesso insieme coesistono almeno due operazioni. Ad esempio, in $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ (ed anche in $\boldsymbol{N}$) sono definite sia l'addizione che la moltiplicazione; in $\mathfrak{M}_n(\boldsymbol{R})$ sono definite l'addizione e la moltiplicazione righe per colonne. Le due operazioni non sono indipendenti, ma sono legate dalle leggi distributive.

Definizione 6. *Si chiama anello ogni terna* $(A, +, \cdot)$ *tale che:* A *è un insieme non vuoto (detto sostegno dell'anello);* $+$ *e* $\cdot$ *sono due operazioni su* A *(dette somma e prodotto di* A*), verificanti i seguenti assiomi:*

- $(A, +)$ *è un gruppo commutativo;*
- $\cdot$ *è associativa:* $(ab)c = a(bc),\ \forall\, a, b, c \in A$ *;*
- *valgono le due leggi distributive tra somma e prodotto*

$$a(b + c) = ab + ac,\ (a + b)c = ac + bc,\ \forall\, a, b, c \in A.$$

Definizione 7. *Un anello* $(A, +, \cdot)$ *è detto unitario se la moltiplicazione* $\cdot$ *ha elemento neutro (detto unità di* A *e denotato* 1 *o* 1_A*), cioè* $a\cdot 1 = 1\cdot a = a,\ \forall\, a \in A$*. Si noti che l'unità, se esiste, è unica (cfr.* **Prop. 1***(1)).*

L'anello A *è detto commutativo se la moltiplicazione* $\cdot$ *è commutativa, cioè* $ab = ba,\ \forall\, a, b \in A$*. L'anello* A *è detto campo se* $(A^{\cdot}, \cdot)$ *è un gruppo commutativo. Dunque un campo è un anello commutativo unitario tale che ogni* $a \in A^{\cdot}$ *ammette inverso* $a^{-1} \in A$*; i campi sono spesso denotati con la lettera* K *(o lettere contigue). Infine, un campo non commutativo (rispetto alla moltiplicazione) è detto corpo.*

Osservazione 2. (*i*) $(\boldsymbol{Z}, +, \cdot)$ è un anello commutativo unitario [abbr. *c.u.*], ma non è un campo. Infatti $(\boldsymbol{Z}^{\cdot}, \cdot)$ non è un gruppo [soltanto 1, -1 ammettono inverso in $\boldsymbol{Z}$]. Invece $(\boldsymbol{Q}, +, \cdot)$ e $(\boldsymbol{R}, +, \cdot)$ sono campi. Infine $(\mathfrak{M}_n(\boldsymbol{R}), +, \cdot)$ è un anello unitario, non commutativo e non corpo se $n \geq 2$.

(*ii*) In ogni anello $(A, +, \cdot)$ risulta:

$$a\cdot 0 = 0\cdot a = 0,\ \forall\, a \in A.$$

Infatti $a\cdot 0 = a(0 + 0) = a\cdot 0 + a\cdot 0$. Dunque $a\cdot 0 + 0 = a\cdot 0 + a\cdot 0$ e, dalla legge di cancellazione (per la somma), segue che $a\cdot 0 = 0$. Analogamente si verifica che $0\cdot a = 0$.

(*iii*) In ogni anello $(A, +, \cdot)$ valgono le tre seguenti regole di calcolo:

$$a(-b) = -(ab) = (-a)b; \qquad (-a)(-b) = ab; \qquad a(b - c) = ab - ac,\ \ \forall\, a, b, c \in A.$$

Per verificare la prima regola, basta osservare che

$$a(-b) + ab = a\big((-b) + b\big) = a\cdot 0 = 0; \qquad (-a)b + ab = \big((-a) + a\big)b = 0\cdot b = 0.$$

Per la seconda [applicando la prima]: $(-a)(-b) = -\big((-a)b\big) = -\big(-(ab)\big) = ab$. Per la terza infine [tenuto conto che si pone, per definizione: $x - y := x + (-y)$], si ha:

$$a(b - c) = a\big(b + (-c)\big) = ab + a(-c) = ab + \big(-(ac)\big) = ab - ac.$$

(*iv*) In un anello $(A, +, \cdot)$ la condizione $ab = 0$ non implica necessariamente $a = 0$ o $b = 0$. Ad esempio, in $\mathfrak{M}_2(\boldsymbol{R})$: $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Tale fatto conduce alla prossima definizione.

Definizione 8. *Un anello* $(A, +, \cdot)$ *è detto integro se risulta,* $\forall\, a, b \in A$*:*

$$ab = 0 \implies a = 0 \ \text{ oppure } \ b = 0.$$

Ne segue che $(A, +, \cdot)$ *è non integro se* $\exists\, a, b \neq 0$ *tali che* $ab = 0$*. Un elemento* $a \in A$ *è detto divisore dello zero o* 0*-divisore di* A *se* $\exists\, b \in A,\ b \neq 0$*, tale che* $ab = 0$*. Ovviamente* 0 *è uno zero-divisore, detto zero divisore banale di* A*. Infine, un anello commutativo unitario ed integro è*

detto dominio d'integrità.

L'anello $(\boldsymbol{Z}, +, \cdot)$ è un dominio d'integrità [ma una dimostrazione più precisa verrà dato nel prossimo paragrafo]. Ogni campo $(K, +, \cdot)$ è un dominio d'integrità [se infatti $a, b \in K$ e $ab = 0$, $a \neq 0$, allora $b = b\cdot 1 = (a^{-1}a)b = a^{-1}(ab) = a^{-1}\cdot 0 = 0$, cioè $b = 0$. Invece $(\mathfrak{M}_n(\boldsymbol{R}), +, \cdot)$ è un anello non integro, come già osservato (per $n = 2$).

Osservazione 3. Sia $(A, +, \cdot)$ un anello unitario. L'insieme degli elementi invertibili

$$\mathcal{U}(A) = \left\{a \in A \,:\, aa' = 1 = a'a,\ \exists\, a' \in A\right\}$$

è un gruppo rispetto al prodotto [verificarlo], detto *gruppo delle unità* o *gruppo degli elementi invertibili di* A.

Ad esempio, $\mathcal{U}(\boldsymbol{Z}) = \{\pm 1\}$, $\mathcal{U}(K) = K^*$, $\forall\, K$ campo, $\mathcal{U}(\mathfrak{M}_n(\boldsymbol{R})) = \mathbf{GL}_n(\boldsymbol{R})$.

Definizione 9. *Si chiama sottoanello di* $(A, +, \cdot)$ *ogni sottoinsieme non vuoto* $B \subseteq A$ *tale che* $(B, +, \cdot)$ *è un anello, rispetto alle stesse operazioni di* A *(ristrette agli elementi di* B*).*

Definizione 10. *Siano* $(A, +, \cdot)$ *e* $(B, +, \cdot)$ *due anelli. Un'applicazione* $f : A \to B$ *è detta omomorfismo (di anelli) se risulta:*

$$f(a_1 + a_2) = f(a_1) + f(a_2), \qquad f(a_1\cdot a_2) = f(a_1)\cdot f(a_2), \quad \forall\, a_1,\, a_2 \in A.$$

In particolare, un omomorfismo biiettivo di anelli è detto isomorfismo ed un isomorfismo dell'anello $(A, +, \cdot)$ *in sé è detto automorfismo.*

Si può facilmente verificare che se $f : A \to B$ è un omomorfismo iniettivo di anelli, l'immagine $f(A)$ è un sottoanello di B isomorfo ad A. Si usa dire in tal caso che f *immerge* A *in* B.

Si può inoltre facilmente verificare (cfr. **Cap. IV**, **Prop. 6.1**) che se $f : A \to B$ è un isomorfismo di anelli [o di gruppi], anche $f^{-1} : B \to A$ è un isomorfismo di anelli [o di gruppi].

Osservazione 4. In $\boldsymbol{Z}$ (come in $\boldsymbol{Q}$ ed $\boldsymbol{R}$) la relazione d'ordine totale $\leq$ è *compatibile* con le due operazioni $+$, $\cdot$, nel senso che, $\forall\, a, b, c \in \boldsymbol{Z}$:

$$a < b \implies a + c < b + c; \quad a < b,\ c > 0 \implies ac < bc.$$

Tale fatto motiva la seguente definizione: un anello $(A, +, \cdot)$ è detto *anello totalmente ordinato* rispetto ad una relazione d'ordine totale $\leq$ su A, se $\forall\, a, b, c \in A$:

(*i*) $a < b \implies a + c < b + c$;

(*ii*) $a < b,\ 0 < c \implies ac < bc$.

Si osserva subito che in un anello totalmente ordinato A risulta:

$$a^2 > 0,\ \forall\, a \in A,\ a \neq 0.$$

Infatti, se $a > 0$, allora $a^2 > 0$; se invece $a < 0$, allora $-a > 0$ e quindi $a^2 = (-a)(-a) > 0$.

Concludiamo il paragrafo richiamando la definizione di K-spazio vettoriale (che presumiamo nota al lettore).

Definizione 11. *Sia* $(K, +, \cdot)$ *un campo. Un insieme non vuoto* V *è detto* K*-spazio vettoriale se è dotato di un'operazione* $+$ *[detta somma], rispetto a cui* $(V, +)$ *è un gruppo commutativo e se è definita un'applicazione* $K \times V \to V$ *[detta moltiplicazione per uno scalare], tale che:*

- $(c + d)\underline{v} = c\underline{v} + d\underline{v}$, $\forall\, c, d \in K$, $\forall\, \underline{v} \in V$;
- $c(\underline{v}_1 + \underline{v}_2) = c\underline{v}_1 + c\underline{v}_2$, $\forall\, c \in K$, $\forall\, \underline{v}_1,\, \underline{v}_2 \in V$;
- $(cd)\underline{v} = c(d\underline{v})$, $\forall\, c, d \in K$, $\forall\, \underline{v} \in V$;
- $1\cdot\underline{v} = \underline{v}$, $\forall\, \underline{v} \in V$.

Gli elementi di V sono detti vettori mentre gli elementi di K sono detti scalari.

È certamente noto al lettore che una *base* $\mathcal{B}$ di un K-spazio vettoriale V è un insieme di vettori linearmente indipendenti [cioè tali che: $\forall\, \underline{v}_1, \dots, \underline{v}_n \in \mathcal{B},\ \sum_{i=1}^{n} c_i \underline{v}_i = \underline{0} \implies c_1 = \dots = c_n = 0$] e tali che il *sottospazio* $\mathfrak{L}(\mathcal{B})$ *generato da* $\mathcal{B}$ coincide con V [$\mathfrak{L}(\mathcal{B})$ è l'insieme di tutti i vettori che si possono scrivere nella forma $\sum_{i=1}^{n} c_i \underline{v}_i$, per opportuni $\underline{v}_1, \dots, \underline{v}_n \in \mathcal{B},\ c_1, \dots, c_n \in K$].

Dimostreremo ora, come applicazione del Lemma di Zorn (cfr. **Teor. 3.2**), il seguente importante risultato.

Teorema 1. *Ogni K-spazio vettoriale V (non nullo) ammette una base.*

Dim. Sia $\mathfrak{A}$ l'insieme di tutti i sottoinsiemi di V formati da vettori linearmente indipendenti. Certamente $\mathfrak{A} \neq \emptyset$ [infatti $\{\underline{v}\} \in \mathfrak{A},\ \forall\, \underline{v} \in V, \underline{v} \neq \underline{0}$] e dunque, poiché $\mathfrak{A} \subset \boldsymbol{\mathcal{P}}(V)$, $(\mathfrak{A}, \subseteq)$ è un insieme ordinato.

Sia ora $\mathcal{S} = \{S_i, i \in I\}$ una catena in $\mathfrak{A}$ (cfr. **Def. 3.10**) e sia $\mathcal{B}_{\mathcal{S}} = \bigcup_{i \in I} S_i$. Risulta subito che $\mathcal{B}_{\mathcal{S}} \in \mathfrak{A}$ (e dunque $\mathcal{B}_{\mathcal{S}}$ è un maggiorante di $\mathcal{S}$). Se infatti $\underline{v}_1, \dots, \underline{v}_t \in \mathcal{B}_{\mathcal{S}},\ \exists\, j \in I$ tale che $\underline{v}_1, \dots, \underline{v}_t \in S_j$: dunque $\underline{v}_1, \dots, \underline{v}_t$ sono linearmente indipendenti.

In base al Lemma di Zorn, $\mathfrak{A}$ possiede almeno un elemento massimale, che denotiamo $\mathcal{B}$. Ovviamente $\mathcal{B}$ è formato da elementi linearmente indipendenti. Se per assurdo $\mathfrak{L}(\mathcal{B}) \neq V,\ \exists\, \underline{v}_0 \in V - \mathfrak{L}(\mathcal{B})$. Allora $\mathcal{B} \cup \{\underline{v}_0\} \in \mathfrak{A}$ e $\mathcal{B} \subset \mathcal{B} \cup \{\underline{v}_0\}$: ciò contraddice la massimalità di $\mathcal{B}$. Si conclude allora che $\mathcal{B}$ è una base di V.

5 Insiemi numerici

In questo paragrafo vogliamo introdurre, con un certo grado di precisione, le strutture numeriche elementari, alcune delle quali peraltro avevamo assunto parzialmente già note nei paragrafi precedenti.

Studieremo quindi:

- ($\boldsymbol{A}$) Numeri naturali e principio d'induzione.
- ($\boldsymbol{B}$) Numeri interi.
- ($\boldsymbol{C}$) Numeri razionali.
- ($\boldsymbol{D}$) Numeri reali (cenno).
- ($\boldsymbol{E}$) Numeri complessi.
- ($\boldsymbol{F}$) Quaternioni.

($\boldsymbol{A}$) NUMERI NATURALI

Definizione 1. *Si chiama terna di Peano ogni terna* $(\boldsymbol{N}, 0, \sigma)$, *dove:*

(i) $\boldsymbol{N}$ *è un insieme non vuoto;*

(ii) 0 *è un elemento di* $\boldsymbol{N}$*;*

(iii) $\sigma : \boldsymbol{N} \to \boldsymbol{N}$ *è un'applicazione verificante i tre seguenti assiomi, detti assiomi di Peano:*

($\boldsymbol{P}_1$) σ *è iniettiva;*

($\boldsymbol{P}_2$) $0 \notin Im(\sigma)$*;*

($\boldsymbol{P}_3$) *Per ogni* $U \subseteq \boldsymbol{N}$ *tale che* $\begin{cases} (\boldsymbol{a}) & 0 \in U, \\ (\boldsymbol{b}) & \sigma(U) \subseteq U, \end{cases}$ *risulta* $U = \boldsymbol{N}$.

L'applicazione σ *è detta applicazione del successivo. Il terzo assioma di Peano* ($\boldsymbol{P}_3$) *è detto principio d'induzione matematica. Si pone usualmente:*

$$\sigma(0) =: 1, \quad \sigma(1) =: 2, \quad \sigma(2) =: 3, \ ...$$

[dove $0, 1, 2, ...$ *vanno al momento interpretati come simboli e non come numeri naturali!]. Per semplicità si scriverà* $\boldsymbol{N}$ *in luogo di* $(\boldsymbol{N}, 0, \sigma)$.

Se una tale terna di Peano $\boldsymbol{N} = (\boldsymbol{N}, 0, \sigma)$ *esiste ed è unica, è detta insieme dei numeri naturali.*

Che una terna di Peano esista non può però essere dimostrato, ma va invece accettato come assioma (detto *assioma dell'infinito*). L'unicità di $(\boldsymbol{N}, 0, \sigma)$ può essere invece facilmente dimostrata in questa forma: *se* $(\boldsymbol{N}, 0, \sigma)$ *e* $(\boldsymbol{N}', 0', \sigma')$ *sono due terne di Peano, esiste un'unica biiezione* $\varphi : \boldsymbol{N} \to \boldsymbol{N}'$ *tale che* $\sigma'(\varphi(n)) = \varphi(\sigma(n)), \ \forall\, n \in \boldsymbol{N}$.

Dunque i numeri naturali sono un concetto primitivo, ma le proprietà della precedente definizione ci consentono di caratterizzarli, prescindendo dalla loro natura.

Osservazione 1. Dall'assioma ($\boldsymbol{P}_3$) segue subito che

($*$) $\qquad n = \sigma\big(\sigma(\ ...\quad \sigma(0)\,)\big), \ \forall\, n \in \boldsymbol{N}^{\cdot} := \boldsymbol{N} - \{0\}.$

Basta osservare che l'insieme $U = \{0, \sigma(0), \sigma(\sigma(0)), \sigma(\sigma(\sigma(0))), ...\}$ verifica le condizioni ($\boldsymbol{a}$) e ($\boldsymbol{b}$) di ($\boldsymbol{P}_3$). Dunque $U = \boldsymbol{N}$. Da ($*$) segue che

($**$) $\qquad n \neq \sigma\big(\sigma(\ ...\quad \sigma(n)\,)\big), \ \forall\, n \in \boldsymbol{N}.$

In base a ($\boldsymbol{P}_2$), $0 \neq \sigma(\sigma\ ...\ \sigma(0))$. Sia $n \in \boldsymbol{N}^{\cdot}$ e [in base a ($*$)] $n = \sigma\big(\sigma(\ ...\quad \sigma(0)\,)\big)$. Se per assurdo fosse $n = \sigma\big(\sigma(\ ...\quad \sigma(n)\,)\big)$, allora $\sigma\big(\sigma(\ ...\quad \sigma(0)\,)\big) = \sigma\big(\sigma(\ ...\quad \sigma(\sigma(\sigma(\ ...\quad \sigma(n)\,)))\,)\big)$. Utilizzando ripetutamente l'iniettività di σ, si otterrebbe $0 = \sigma(\sigma\ ...\ \sigma(0))$, cioè $0 \in Im(\sigma)$: assurdo.

Definizione 2. *In* $\boldsymbol{N}$ *è definita la seguente relazione di diseguaglianza stretta* $<$: $\forall\, n, m \in \boldsymbol{N}$,

$$n < m \iff m = \sigma\big(\sigma(\ ...\quad \sigma(n)\,)\big)$$

[cioè $n < m \iff m$ "è un successivo" di n]. Ad essa resta ovviamente associata la relazione di diseguaglianza debole $\leq$, così definita: $\forall\, n, m \in \boldsymbol{N}$,

$$n \leq m \iff n = m \text{ oppure } n < m.$$

Proposizione 1. *$(\boldsymbol{N}, \leq)$ è un insieme totalmente ordinato, con primo elemento 0.*

Dim. La relazione $\leq$ è riflessiva per definizione. Verifichiamo che è transitiva: se $n < m$ e $m < p$, allora $m = \sigma\big(\sigma(\ \dots\ \ \sigma(n)\,)\big)$, $p = \sigma\big(\sigma(\ \dots\ \ \sigma(m)\,)\big)$ e dunque $p = \sigma\big(\sigma(\ \dots\ \ \sigma(\sigma(\sigma(\ \dots\ \ \sigma(n)\,)))\,)\big)$. Allora $n < p$. [Se fosse $n = m$ o $m = p$, la transitività sarebbe immediata]. Verifichiamo ora che $\leq$ è antisimmetrica. Sia $n \leq m$, $m \leq n$ e, per assurdo, $n \neq m$. Allora $m = \sigma\big(\sigma(\ \dots\ \ \sigma(n)\,)\big)$ e $n = \sigma\big(\sigma(\ \dots\ \ \sigma(m)\,)\big)$, da cui $m = \sigma\big(\sigma(\ \dots\ \ \sigma(\sigma(\sigma(\ \dots\, \sigma(m)\,)))\,)\big)$. Ciò è assurdo in base a (**).

Verifichiamo ora che $\leq$ è totale. Siano $n, m \in \boldsymbol{N}^{\cdot}$, con $n \neq m$. Da (*), se $n = \sigma\big(\sigma(\ \dots\ \ \sigma(0)\,)\big)$ ed $m = \sigma\big(\sigma(\ \dots\ \ \sigma(0)\,)\big)$, confrontando tali scritture segue subito che $n = \sigma\big(\sigma(\ \dots\ \ \sigma(m)\,)\big)$ oppure $m = \sigma\big(\sigma(\ \dots\ \ \sigma(n)\,)\big)$, cioè $n < m$ oppure $m < n$.

Infine, che 0 sia il primo elemento di $\boldsymbol{N}$ è ovvio.

Definizione 3. *Su $\boldsymbol{N}$ è definita la seguente operazione di addizione (o somma) $+ : \boldsymbol{N} \times \boldsymbol{N} \to \boldsymbol{N}$ tale che, $\forall\, n, m \in \boldsymbol{N}$,*

$$n + 0 = n; \quad n + \sigma(m) = \sigma(n + m).$$

Si noti che $n + \sigma(0) = \sigma(n + 0) = \sigma(n)$, cioè $\sigma(n) = n + 1$. È per tale motivo che σ è stata chiamata "applicazione del successivo".

Osservazione 2. (*i*) La precedente definizione di somma è di tipo *induttivo* o *ricorsivo*: per calcolare $n + m$ occorre aver calcolato $n + k$, $\forall\, k < n$. La validità logica di un siffatto tipo di definizione discende dal principio d'induzione. Ma non insistiamo oltre su ciò.

(*ii*) Se $n < m$, $\exists!\, h \in \boldsymbol{N}$ tale che $m = n + h$. Sia infatti ad esempio $m = \sigma(\sigma(\sigma(n)))$. Allora

$$m = \sigma(\sigma(\sigma(n + \sigma(0)))) = \sigma(\sigma(n + \sigma(\sigma(0)))) = \sigma(n + \sigma(\sigma(\sigma(0)))) = n + \sigma(\sigma(\sigma(\sigma(0)))) = n + 4.$$

Veniamo ora all'unicità di h. Assumiamo che sia $m = n + h = n + h'$ e, ad esempio, $h < h'$. Allora $\underbrace{\sigma\big(\sigma(\ \dots\ \ \sigma}_{h}(n)\,)\big) = \underbrace{\sigma\big(\sigma(\ \dots\ \ \sigma}_{h'}(n)\,)\big)$ e, in base all'iniettività di σ, $n = \underbrace{\sigma\big(\sigma(\ \dots\, \sigma}_{h'-h}(n)\,)\big)$. Ciò è assurdo in base a (**). Il naturale h viene denotato usualmente $m - n$.

(*iii*) L'addizione in $\boldsymbol{N}$ verifica la proprietà associativa: $(n + m) + p = n + (m + p)$, $\forall\, m, n, p \in \boldsymbol{N}$. Per verificare tale proprietà si segue un procedimento induttivo. Si ha infatti, posto $p = 1$:

$$(n + m) + 1 = \sigma(n + m) = n + \sigma(m) = n + (m + 1).$$

Allora, posto $p = 2$: $(n+m)+2 = (n+m)+\sigma(1) = \sigma((n+m)+1) = \sigma(n+(m+1)) = n+\sigma(m+1) = n + (m + \sigma(1)) = n + (m + 2)$.

Assumendo quindi $(n+m)+(p-1) = n+(m+(p-1))$, si verifica che $(n+m)+p = n+(m+p)$.

Definizione 4. *Su $\boldsymbol{N}$ è definita la seguente operazione di moltiplicazione (o prodotto) $\cdot : \boldsymbol{N} \times \boldsymbol{N} \to \boldsymbol{N}$ tale che, $\forall\, n, m \in \boldsymbol{N}$,*

$$n \cdot 0 = 0; \quad n \cdot \sigma(m) = n \cdot m + n.$$

In particolare, $n \cdot 1 = n \cdot \sigma(0) = n \cdot 0 + n = 0 + n = n$, cioè $n \cdot 1 = n$. Anche tale definizione è induttiva.

La verifica delle proprietà della somma e del prodotto è, come osservato nella precedente osservazione, piuttosto laboriosa. Ci limitiamo quindi ad elencarne le principali, senza dimostrazione.

Proposizione 2. *Le operazioni di somma e prodotto verificano le seguenti proprietà:*

(1) $(n + m) + p = n + (m + p)$, $\forall\, n, m, p \in \boldsymbol{N}$ (proprietà associativa della somma);

(2) $n+0=n=0+n,\ \forall\, n\in\boldsymbol{N}$ *(esiste l'elemento neutro della somma,* 0*);*
(3) $n+m=m+n,\ \forall\, n,\, m\in\boldsymbol{N}$ *(proprietà commutativa della somma);*
(4) $(nm)p=n(mp),\ \forall\, n,\, m,\, p\in\boldsymbol{N}$ *(proprietà associativa del prodotto);*
(5) $n\cdot 1=n=1\cdot n,\ \forall\, n\in\boldsymbol{N}$ *(esiste l'elemento neutro del prodotto,* 1*);*
(6) $nm=mn,\ \forall\, n,\, m\in\boldsymbol{N}$ *(proprietà commutativa del prodotto);*
(7) $mn=0 \iff m=0$ *oppure* $n=0$*;*
(8) $mn=1 \iff m=n=1$*;*
(9) $\begin{cases}(m+n)p=mp+np,\\ m(n+p)=mn+mp,\end{cases}\quad \forall\, m,\, n,\, p\in\boldsymbol{N}$ *(proprietà distributive a destra e sinistra);*
(10) $m+n_1=m+n_2 \implies n_1=n_2$ *(legge di cancellazione della somma);*
(11) $mn_1=mn_2,\ m\neq 0 \implies n_1=n_2$ *(legge di cancellazione del prodotto);*
(12) $n_1<n_2 \iff n_1+n<n_2+n,\ \forall\, n\in\boldsymbol{N}$*;*
(13) $n_1<n_2 \iff n_1 n<n_2 n,\ \forall\, n\in\boldsymbol{N},\ n\neq 0$*;*
(14) $\forall\, m,\, n\in\boldsymbol{N},\ n\neq 0,\ \exists\, p\in\boldsymbol{N}$ *tale che* $m<np$ *(proprietà archimedea di* $\boldsymbol{N}$*).*

IL PRINCIPIO D'INDUZIONE

Poiché $\sigma(k)=k+1,\ \forall\, k\in\boldsymbol{N}$, l'assioma di Peano $(\boldsymbol{P}_3)$ può essere riformulato in questo modo:

$(\boldsymbol{P}_3)$ *Per ogni* $U\subseteq\boldsymbol{N}$ *tale che* $\begin{cases}(\boldsymbol{a})\ \ 0\in U,\\ (\boldsymbol{b})\ \ k\in U \implies k+1\in U\ \ [\forall\, k\geq 0],\end{cases}$ *risulta* $U=\boldsymbol{N}$.

Dall'assioma $(\boldsymbol{P}_3)$ segue il *"metodo di prova per induzione"*:

Proposizione 3. *Sia* $\mathcal{P}(n)$ *un'affermazione da dimostrare, definita* $\forall\, n\in\boldsymbol{N}$*. Se*

(i) $\mathcal{P}(0)$ *è vera,*

(ii) $\mathcal{P}(k)$ *vera* $\implies \mathcal{P}(k+1)$ *vera* $\quad[\forall\, k\geq 0]$*,*

allora $\mathcal{P}(n)$ *è vera,* $\forall\, n\in\boldsymbol{N}$*.*

La (i) è detta "base induttiva", la (ii) è detta "passo induttivo", l'ipotesi " $\mathcal{P}(k)$ *vera" [in (ii)] è detta "ipotesi induttiva".*

Dim. Posto $U:=\{n\in\boldsymbol{N}\ :\ \mathcal{P}(n)\ \text{è vera}\}$, bisogna verificare che $U=\boldsymbol{N}$.
Poiché vale (i), U verifica la condizione $(\boldsymbol{a})$ di $(\boldsymbol{P}_3)$. Poiché vale (ii), U verifica anche la condizione $(\boldsymbol{b})$ di $(\boldsymbol{P}_3)$. Da $(\boldsymbol{P}_3)$ segue che $U=\boldsymbol{N}$.

Osservazione 3. La base induttiva può essere anche riferita ad un naturale $k_0>0$. In tal caso il passo induttivo (ii) va verificato per ogni $k\geq k_0$.

Il passo induttivo (ii) può essere ovviamente anche formulato in questo modo:
(ii) $\mathcal{P}(k-1)$ vera $\implies \mathcal{P}(k)$ vera $\quad[\forall\, k\geq 1]$.

Esiste una seconda formulazione del principio d'induzione, detta *forma forte* (o *seconda forma*) *del principio d'induzione*:

$(\boldsymbol{P}'_3)$ *Per ogni* $V\subseteq\boldsymbol{N}$ *tale che* $\begin{cases}(\boldsymbol{a})\ \ 0\in V,\\ (\boldsymbol{b}')\ \ \{0,1,\dots,k\}\subseteq V \implies k+1\in V\ \ [\forall\, k\geq 0],\end{cases}$ *risulta* $V=\boldsymbol{N}$.

L'assioma $(\boldsymbol{P}'_3)$ fornisce il seguente *"metodo di prova per induzione forte"*:

Proposizione 4. *Sia* $\mathcal{P}(n)$ *un'affermazione da dimostrare, definita* $\forall\, n\in\boldsymbol{N}$*. Se:*

(i) $\mathcal{P}(0)$ *è vera,*

(ii') $\mathcal{P}(h)$ *vera,* $\forall\, h = 0, 1, \ldots k, \implies \mathcal{P}(k+1)$ *vera* $\quad [\forall\, k \geq 0]$,

allora $\mathcal{P}(n)$ *è vera,* $\forall\, n \in \boldsymbol{N}$.

Dim. Posto $V := \{n \in \boldsymbol{N} \,:\, \mathcal{P}(n) \text{ è vera}\}$, bisogna verificare che $V = \boldsymbol{N}$.

L'insieme V verifica le condizioni $(\boldsymbol{a})$ e $(\boldsymbol{b'})$ di $(\boldsymbol{P}'_3)$, in quanto valgono (i) e (ii). Allora da $(\boldsymbol{P}'_3)$ segue che $V = \boldsymbol{N}$.

Vogliamo ora dimostrare che $(\boldsymbol{P}_3)$ è equivalente a $(\boldsymbol{P}'_3)$. A tale scopo conviene utilizzare un terzo assioma, ad essi equivalente. Tale assioma, detto *principio del minimo* o *principio del buon ordinamento* [abbreviato $\boldsymbol{BO}$] è il seguente:

*(**BO**) Ogni sottoinsieme non vuoto* $T \subseteq \boldsymbol{N}$ *ha un minimo [cioè* $\exists\, t_0 \in T \,:\, t_0 \leq t,\ \forall\, t \in T$, *cfr.* **Def. 4.6***].*

Teorema 1. *I tre assiomi* $(\boldsymbol{P}_3)$, $(\boldsymbol{P}'_3)$ *e* $(\boldsymbol{BO})$ *sono equivalenti.*

Dim. Dimostreremo che $(\boldsymbol{P}'_3) \implies (\boldsymbol{P}_3) \implies (\boldsymbol{BO}) \implies (\boldsymbol{P}'_3)$.

$(\boldsymbol{P}'_3) \implies (\boldsymbol{P}_3)$. Preso un insieme $U \subseteq \boldsymbol{N}$ verificante le condizioni $(\boldsymbol{a})$ e $(\boldsymbol{b})$ di $(\boldsymbol{P}_3)$, bisogna provare che $U = \boldsymbol{N}$. Basta dimostrare che U verifica $(\boldsymbol{b'})$ [perché allora, per $(\boldsymbol{P}'_3)$, $U = \boldsymbol{N}$]. Sia $\{0, 1, \ldots k\} \subseteq U$. In particolare $k \in U$ e quindi, per $(\boldsymbol{b})$, $k+1 \in U$. Dunque U verifica $(\boldsymbol{b'})$.

$(\boldsymbol{P}_3) \implies (\boldsymbol{BO})$. Per assurdo, esista un sottoinsieme non vuoto $T \subseteq \boldsymbol{N}$, privo di minimo. Certo T ha almeno due elementi distinti [altrimenti avrebbe minimo]. Poniamo

$$U := Minor(T) = \{k \in \boldsymbol{N} \,:\, k \leq t,\ \forall\, t \in T\} \quad [\text{cfr. } \textbf{Def. 4.7}].$$

Poiché $T \subseteq \boldsymbol{N}$, allora $0 \in U$ e dunque U verifica la condizione $(\boldsymbol{a})$ di $(\boldsymbol{P}_3)$. Osserviamo ora che $U \neq \boldsymbol{N}$ [se infatti $t_1, t_2 \in T$, con $t_1 < t_2$, allora $t_2 \notin U$]. Ne segue che U non verifica la condizione $(\boldsymbol{b})$ [altrimenti $U = \boldsymbol{N}$, in base a $(\boldsymbol{P}_3)$]. Pertanto esiste $k \in U$ tale che $k+1 \notin U$. Poiché $k \in U$, allora $k \leq t,\ \forall\, t \in T$. Si verifica subito che $k \in T$ [altrimenti, se $k \notin T$, allora $k < t,\ \forall\, t \in T$ e dunque $k+1 \leq t,\ \forall\, t \in T$, da cui $k+1 \in U$: assurdo]. Allora k è il minimo di T: assurdo, per l'ipotesi fatta su T.

$(\boldsymbol{BO}) \implies (\boldsymbol{P}'_3)$. Preso un insieme $V \subseteq \boldsymbol{N}$ verificante le condizioni $(\boldsymbol{a})$ e $(\boldsymbol{b'})$ di $(\boldsymbol{P}'_3)$, bisogna provare che $V = \boldsymbol{N}$. Per assurdo, sia $V \subset \boldsymbol{N}$ e sia $T = \boldsymbol{N} - V$ (non vuoto). Per l'assioma $(\boldsymbol{BO})$, T ha il minimo, diciamo t_0. Poiché $0 \in V$, allora $t_0 \neq 0$ [e dunque $t_0 - 1 \in \boldsymbol{N}$]. L'insieme $\{0, 1, \ldots, t_0 - 1\}$ è contenuto in V [perché t_0 è il minimo di T] e, poiché V verifica $(\boldsymbol{b'})$, allora $t_0 \in V$: assurdo.

Osservazione 4. Una semplice conseguenza del principio del buon ordinamento è la dimostrazione del seguente "ovvio" risultato [peraltro già conseguenza del fatto che $\boldsymbol{N}$ è totalmente ordinato]:

$(*)$ $\quad \nexists\, m \in \boldsymbol{N}$ tale che $0 < m < 1$.

Per verificare tale affermazione, assumiamo per assurdo che $\exists\, m \in \boldsymbol{N}$ tale che $0 < m < 1$. Moltiplicando tale diseguaglianza per m si ottiene

$$0 < m^2 < m \quad \text{e quindi} \quad 0 < m^2 < m < 1.$$

Rimoltiplicando per m: $0 < m^3 < m^2 < m < 1$. Iterando tale procedimento:

$$0 < m^k < m^{k-1} < \ \ldots\ < m^3 < m^2 < m < 1.$$

Ma allora l'insieme $T = \{m^k,\ \forall\, k \geq 0\}$ è privo di minimo: assurdo.

Si noti che, ad esempio, la proprietà archimedea di $\boldsymbol{N}$ [cfr. **Prop. 2**(*14*)] può essere dimostrata

ricorrendo a (∗).

Concludiamo questa parte con alcuni risultati che si dimostrano con il metodo d'induzione.

Proposizione 5. *Per ogni* $n \geq 1$, *si ponga* $S_n := 1 + 2 + 3 + \ ... \ + n = \sum_{k=1}^{n} k$. *Risulta:*

$$S_n = \binom{n+1}{2}, \quad \forall\, n \geq 1.$$

Dim. Per induzione su $n \geq 1$.

Base induttiva. Risulta: $S_1 = \binom{1+1}{2}$ [infatti $S_1 = 1$, $\binom{1+1}{2} = \binom{2}{2} = 1$].

Passo induttivo. Sia $n \geq 1$ e sia $S_n = \binom{n+1}{2}$. Bisogna verificare che $S_{n+1} = \binom{n+2}{2}$.

Infatti $S_{n+1} = S_n + (n+1) = \binom{n+1}{2} + (n+1) = \binom{n+1}{2} + \binom{n+1}{1} = \binom{n+2}{2}$ [cfr. **Prop. 2.6**].

Nota. Tale risulato può essere dimostrato anche senza induzione. Infatti:

$$\begin{aligned} 2S_n &= \big(1 + 2 + \ ... \ + (n-1) + n\big) + \big(n + (n-1) + \ ... \ + 2 + 1\big) = \\ &= [1+n] + [2 + (n-1)] + [3 + (n-2)] + \ ... \ + [(n-1) + 2] + [n+1] = \\ &= \sum_{k=1}^{n} [k + (n-k+1)] = \sum_{k=1}^{n} (n+1) = n(n+1). \end{aligned}$$

Dunque $S_n = \frac{n(n+1)}{2} = \binom{n+1}{2}$.

Proposizione 6. *Sia* A *un insieme finito. Se* $|A| = n$, *allora* $|\boldsymbol{\mathcal{P}}(A)| = 2^n$, $\forall\, n \geq 0$.

Dim. Per induzione su $n \geq 0$.

Base induttiva. Se $|A| = 0$, $|\boldsymbol{\mathcal{P}}(A)| = 2^0$. Infatti se $|A| = 0$, allora $A = \emptyset$ e $|\boldsymbol{\mathcal{P}}(\emptyset)| = |\{\emptyset\}| = 1$.

Passo induttivo. Sia $n \geq 0$ e, $\forall\, B : |B| = n$, sia $|\boldsymbol{\mathcal{P}}(B)| = 2^n$. Per ogni insieme A tale che $|A| = n+1$, proveremo che $|\boldsymbol{\mathcal{P}}(A)| = 2^{n+1}$.

Si fissi un elemento $a_1 \in A$. In $\boldsymbol{\mathcal{P}}(A)$ consideriamo i due sottoinsiemi:

$$\mathfrak{C} = \{B \subseteq A \ : \ B \ni a_1\}, \qquad \mathfrak{D} = \{B \subseteq A \ : \ B \not\ni a_1\}.$$

Ovviamente $\mathfrak{C} \cup \mathfrak{D} = \boldsymbol{\mathcal{P}}(A)$ e $\mathfrak{C} \cap \mathfrak{D} = \emptyset$. Dunque $|\boldsymbol{\mathcal{P}}(A)| = |\mathfrak{C}| + |\mathfrak{D}|$. Si ha:

$\mathfrak{C} = \big\{B_1 \cup \{a_1\},\ \forall\, B_1 \subseteq A - \{a_1\}\big\}$ è in corrispondenza biunivoca con $\boldsymbol{\mathcal{P}}(A - \{a_1\})$;

$\mathfrak{D} = \big\{B \subseteq A - \{a_1\}\big\} = \boldsymbol{\mathcal{P}}(A - \{a_1\})$.

Per ipotesi induttiva, da $|A - \{a_1\}| = n$, segue che $|\mathfrak{C}| = |\mathfrak{D}| = 2^n$. Dunque $|\boldsymbol{\mathcal{P}}(A)| = 2^n + 2^n = 2^{n+1}$.

Proposizione 7. *Per ogni* $x, y \in \boldsymbol{R}$ *e per ogni* $n \geq 0$, *risulta*

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

Dim. Per induzione su $n \geq 0$.

Base induttiva. Risulta: $(x+y)^0 = \sum_{k=0}^{0} \binom{0}{k} x^{0-k} y^k$. Infatti: $(x+y)^0 = 1$, $\sum_{k=0}^{0} \binom{0}{k} x^{0-k} y^k = \binom{0}{0} x^0 y^0 = 1$.

Passo induttivo. Sia $n \geq 1$. Per ipotesi induttiva, sia $(x+y)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-1-k} y^k$. Bisogna verificare che

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

Infatti si ha:

$$\begin{aligned} (x+y)^n &= (x+y)(x+y)^{n-1} = (x+y)\Big(\sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-1-k} y^k\Big) = \\ &= \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-k} y^k + \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-1-k} y^{k+1} = \quad \text{[ponendo } h = k+1\text{]} \end{aligned}$$

$$= \sum_{k=0}^{n-1} \binom{n-1}{k} x^{n-k} y^k + \sum_{h=1}^{n} \binom{n-1}{h-1} x^{n-h} y^h = \quad [\text{ponendo } k = h]$$

$$= \binom{n-1}{0} x^n + \sum_{k=1}^{n-1} \binom{n-1}{k} x^{n-k} y^k + \sum_{k=1}^{n-1} \binom{n-1}{k-1} x^{n-k} y^k + \binom{n-1}{n-1} x^0 y^n =$$

$$= x^n + \sum_{k=1}^{n-1} [\binom{n-1}{k} + \binom{n-1}{k-1}] x^{n-k} y^k + y^n =$$

$$= x^n + \sum_{k=1}^{n-1} \binom{n}{k} x^{n-k} y^k + y^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k .$$

Proposizione 8. *Per ogni $n \geq 1$, si ponga $\Sigma_n := 1 + 3 + 5 + \ ... \ + (2n-1)$ [somma dei primi n numeri dispari]. Risulta: $\Sigma_n = n^2$, $\forall\, n \geq 1$.*

Dim. Presentiamo due dimostrazioni: la prima usa l'induzione tramite la **Prop. 5**; la seconda procede direttamente per induzione.

(**1**). Risulta:

$$\Sigma_n = S_{2n} - \sum_{k=0}^{n} 2k = S_{2n} - 2S_n = \binom{2n+1}{2} - 2\binom{n+1}{2} = \tfrac{(2n+1)2n}{2} - 2\tfrac{(n+1)n}{2} = n^2$$

(**2**). Per induzione su $n \geq 1$.

Base induttiva. Risulta: $\Sigma_1 = 1^2$ [ovvio].

Passo induttivo. Sia $n \geq 1$ e sia $\Sigma_n = n^2$. Dobbiamo verificare che $\Sigma_{n+1} = (n+1)^2$. Infatti:

$$\Sigma_{n+1} = \Sigma_n + (2n+1) = n^2 + (2n+1) = (n+1)^2.$$

Proposizione 9. *Sia $a \in \boldsymbol{R}$. Risulta, $\forall\, n \geq 1$:*

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ ... \ + a + 1).$$

Dim. Per induzione su $n \geq 1$.

Base induttiva. Risulta: $a^1 - 1 = (a-1)\cdot 1$ [ovvio].

Passo induttivo. Sia $n \geq 2$ e sia $a^{n-1} - 1 = (a-1)(a^{n-2} + \ ... \ + a + 1)$. Bisogna verificare che $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ ... \ + a + 1)$. Infatti:

$$a^n - 1 = a^n - a + a - 1 = a(a^{n-1} - 1) + (a-1) = a(a-1)(a^{n-2} + \ ... \ + a + 1) + (a-1) =$$
$$= (a-1)\big[a(a^{n-2} + \ ... \ + a + 1) + 1\big] = (a-1)(a^{n-1} + a^{n-2} + \ ... \ + a + 1).$$

(*B*) NUMERI INTERI

Non ogni equazione della forma $n + X = m$, con $n, m \in \boldsymbol{N}$, è risolubile in $\boldsymbol{N}$: ad esempio non lo è l'equazione $1 + X = 0$. Per rendere risolubile ogni siffatta equazione serve poter operare su insieme numerico più ampio dei naturali, e per questo si introduce l'insieme $\boldsymbol{Z}$ dei *numeri interi*.

Presenteremo $\boldsymbol{Z}$ come insieme quoziente di $\boldsymbol{N}\times\boldsymbol{N}$ modulo un'opportuna relazione d'equivalenza ρ. Poi definiremo in $\boldsymbol{Z}$ le operazioni di addizione e moltiplicazione e ne studieremo le proprietà.

Definizione 5. *In $\boldsymbol{N}\times\boldsymbol{N}$ è definita la seguente relazione d'equivalenza ρ:*

$$(a,b)\rho(c,d) \iff a + d = b + c, \quad \forall\, (a,b),\, (c,d) \in \boldsymbol{N}\times\boldsymbol{N}.$$

Osservazione 5. ρ è una relazione di equivalenza su $\boldsymbol{N}\times\boldsymbol{N}$. Lasciamo per esercizio la verifica delle proprietà riflessiva e simmetrica e verifichiamo soltanto la proprietà transitiva:

$$\text{se } (a,b)\rho(c,d) \text{ e } (c,d)\rho(e,f), \text{ allora } (a,b)\rho(e,f).$$

Da $\begin{cases} a+d=b+c \\ c+f=d+e, \end{cases}$ sommando a membro a membro segue $a+d+c+f=b+c+d+e$, da cui, semplificando $c+d$, risulta $a+f=b+e$, cioè $(a,b)\rho(e,f)$.

Definizione 6. *L'insieme quoziente* $\boldsymbol{Z} := \boldsymbol{N}\times\boldsymbol{N}/_{\rho}$ *è detto insieme dei numeri interi. Un numero intero è quindi una classe di equivalenza modulo* ρ*:*

$$[a,b] := [(a,b)]_{\rho} = \big\{(x,y)\in\boldsymbol{N}\times\boldsymbol{N} \ : \ a+y=b+x\big\}$$

Osservazione 6. Se $a\geq b$, allora $a-b\in\boldsymbol{N}$ [cfr. **Osserv. 2**(*ii*)]. Si ha quindi:

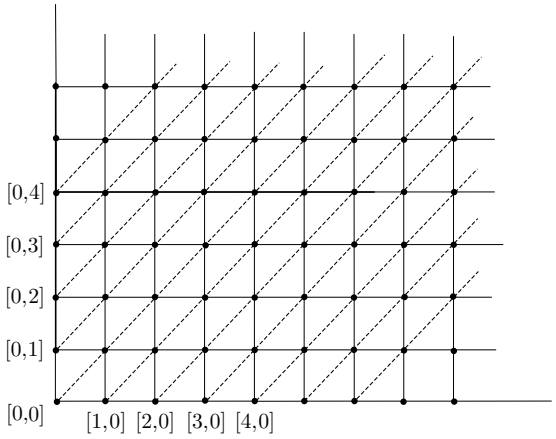
$$[a,b]=\big\{(x,y)\in\boldsymbol{N}\times\boldsymbol{N} \ : \ x=(a-b)+y\big\}=\big\{\big((a-b)+t,t\big), \ \forall\, t\in\boldsymbol{N}\big\}.$$

In particolare, $[a,b]=[a-b,0]$. Se invece $a\leq b$, allora $b-a\in\boldsymbol{N}$. In tal caso:

$$[a,b]=\big\{(x,y)\in\boldsymbol{N}\times\boldsymbol{N} \ : \ y=(b-a)+x\big\}=\big\{\big(t,(b-a)+t\big), \ \forall\, t\in\boldsymbol{N}\big\}.$$

In particolare, $[a,b]=[0,b-a]$.

Le classi di equivalenza sono visualizzate sul "reticolo" $\boldsymbol{N}\times\boldsymbol{N}$ come gli insiemi di punti giacenti sulle "semirette diagonali" uscenti dai due semiassi, come nel seguente disegno.



Dunque $\boldsymbol{Z}=\{\ \dots\ ,[0,n],\ \dots\ ,[0,2],\ [0,1],\ [0,0],\ [1,0],\ [2,0],\ \dots\ ,[n,0],\ \dots\ \}$.

Introduciamo le seguenti notazioni:

$$-n := [0,n],\ \forall\, n\in\boldsymbol{N}; \quad n := [n,0],\ \forall\, n\in\boldsymbol{N}$$

[in particolare $0=[0,0]$]. Ne segue:

$$\boldsymbol{Z}=\boldsymbol{Z}_{+}\cup\{0\}\cup\boldsymbol{Z}_{-}\,,$$

con $\boldsymbol{Z}_{+} := \{n,\ \forall\, n\in\boldsymbol{N},\ n\geq 1\}$ (*interi positivi*), $\boldsymbol{Z}_{-} := \{-n,\ \forall\, n\in\boldsymbol{N},\ n\geq 1\}$ (*interi negativi*).

Osserviamo che $n\in\boldsymbol{Z}_{+} \iff -n\in\boldsymbol{Z}_{-}$ (e viceversa).

Vogliamo ora definire in $\boldsymbol{Z}$ le operazioni di addizione e moltiplicazione.

Definizione 7. *È definita in* $\boldsymbol{Z}$ *l'operazione di addizione o somma* $+:\boldsymbol{Z}\times\boldsymbol{Z}\to\boldsymbol{Z}$ *tale che:*

$$[a,b]+[c,d]=[a+c,b+d], \quad \forall\,[a,b],\,[c,d]\in\boldsymbol{Z}.$$

Osservazione 7. Perché tale definizione sia accettabile, occorre verificare che è ben posta e cioè che non dipende dalla scelta dei rappresentanti nelle classi. Se quindi $[a,b]=[a_1,b_1]$ e $[c,d]=[c_1,d_1]$, bisogna verificare che $[a+c,b+d]=[a_1+c_1,b_1+d_1]$.

Infatti, da $\begin{cases} a+b_1=b+a_1 \\ c+d_1=d+c_1, \end{cases}$ sommando a membro a membro segue $a+c+b_1+d_1=b+d+a_1+c_1$.

Proposizione 10. *L'addizione* $+$ *su* $\boldsymbol{Z}$ *verifica le seguenti proprietà:*

(1) è associativa;

(2) è dotata di elemento neutro, 0*;*
(3) è dotata di opposto $-[a,b]$ *di ogni elemento* $[a,b]$*; risulta* $-[a,b]=[b,a]$*;*
(4) è commutativa.

Ne segue che $(\boldsymbol{Z},+)$ *è un gruppo commutativo. Inoltre, per ogni* $n,\, m \in \boldsymbol{Z}$*, l'equazione* $X+m=n$ *ammette un'unica soluzione in* $\boldsymbol{Z}$*, e cioè l'intero* $x=n+(-m)$ $[=:(n-m)]$.

Dim. [Lasciata per esercizio].

Definizione 8. *È definita in* $\boldsymbol{Z}$ *l'operazione di moltiplicazione o prodotto* $\cdot : \boldsymbol{Z}\times\boldsymbol{Z} \to \boldsymbol{Z}$ *tale che:*

$$[a,b]\cdot[c,d]=[ac+bd, ad+bc], \quad \forall\, [a,b],\, [c,d] \in \boldsymbol{Z}.$$

Osservazione 8. Come per l'addizione, occorre verificare che anche la moltiplicazione è ben definita. Procediamo con due passi successivi:

(a) se $[a,b]=[a_1,b_1]$, allora $[a,b]\cdot[c,d]=[a_1,b_1]\cdot[c,d]$.

(b) se $[c,d]=[c_1,d_1]$, allora $[a_1,b_1]\cdot[c,d]=[a_1,b_1]\cdot[c_1,d_1]$.

Verifichiamo (a). Per ipotesi, $a+b_1=b+a_1$ e dobbiamo verificare che

$(*)$ $\qquad ac+bd+a_1d+b_1c=ad+bc+a_1c+b_1d.$

Si moltiplica l'uguaglianza $a+b_1=b+a_1$ per c e per d. Si ottiene

$$\begin{cases} ac+b_1c=bc+a_1c \\ ad+b_1d=bd+a_1d. \end{cases}$$

Sommando ora le due uguaglianze (incrociando i due membri), si ottiene esattamente $(*)$.

Per verificare (b) si procede in modo del tutto analogo e si ottiene

$(**)$ $\qquad a_1c+b_1d+a_1d_1+b_1c_1=a_1d+b_1c+a_1c_1+b_1d_1.$

Sommando a membro a membro $(*)$ e $(**)$ si ottiene la tesi.

Proposizione 11. *La moltiplicazione* $\cdot$ *su* $\boldsymbol{Z}$ *verifica le seguenti proprietà:*

(1) è associativa;
(2) è distributiva rispetto alla somma [cioè, $\forall\, m,n,p \in \boldsymbol{Z}$*, risulta*

$$(m+n)p=mp+np, \quad m(n+p)=mn+mp];$$

(3) è dotata di elemento neutro, $1=[1,0]$*;*
(4) è commutativa.

Ne segue che $(\boldsymbol{Z},+,\cdot)$ *è un anello commutativo unitario.*

Dim. [Lasciata per esercizio].

Osservazione 9. Vogliamo rimarcare il fatto che il prodotto di due interi negativi è positivo. Siano infatti $[0,n],\, [0,m] \in \boldsymbol{Z}_-$. Risulta:

$$[0,n]\cdot[0,m]=[0\cdot 0+nm, 0\cdot m+n\cdot 0]=[nm,0] \in \boldsymbol{Z}_+.$$

Con analoga dimostrazione si verifica che il prodotto di due interi positivi è positivo.

Concludiamo questa parte illustrando ulteriori proprietà di $\boldsymbol{Z}$.

Valgono ovviamente nell'anello $(\boldsymbol{Z},+,\cdot)$ [come in ogni anello $(A,+,\cdot)$ cfr. **Osserv. 4.2**(ii),(iii)] le seguenti regole di calcolo:

$$n\cdot 0=0=0\cdot n, \quad n(-m)=-nm=(-n)m, \quad m(n-p)=mn-mp, \quad \forall\, n,m,p \in \boldsymbol{Z}.$$

Proposizione 12. $(\boldsymbol{Z},+,\cdot)$ *è un dominio d'integrità. In esso quindi vale la legge di cancellazione del prodotto, cioè:*

$$\text{se } \ ab=ac \ \text{ e } \ a\neq 0, \ \text{allora } \ b=c.$$

Dim. Bisogna verificare che $\boldsymbol{Z}$ è un anello integro, cioè: se $ab = 0$, allora $a = 0$ oppure $b = 0$. Risulta (per opportuni $m, n \in \boldsymbol{N}$):

$$ab = \begin{cases} [mn, 0], & \text{se } a = [m, 0],\ b = [n, 0], \\ [0, mn], & \text{se } a = [0, m],\ b = [n, 0], \\ [0, mn], & \text{se } a = [m, 0],\ b = [0, n], \\ [mn, 0], & \text{se } a = [0, m],\ b = [0, n]. \end{cases}$$

Se quindi $ab = 0$, allora $mn = 0$ e pertanto $m = 0$ oppure $n = 0$, cioè $a = 0$ oppure $b = 0$.

Infine, la validità della legge di cancellazione segue dal fatto che l'anello è integro. Infatti:

$$\begin{matrix} ab = ac \\ a \neq 0 \end{matrix} \implies \begin{matrix} a(b-c) = 0 \\ a \neq 0 \end{matrix} \implies b - c = 0 \implies b = c.$$

Proposizione 13. $(\boldsymbol{Z}, +, \cdot)$ *è un anello totalmente ordinato (cfr.* **Osserv. 4.4***).*

Dim. Definiamo in $\boldsymbol{Z}$ la relazione $<$ ponendo, $\forall\, n, m \in \boldsymbol{Z}$:

$$0 < n \iff n \in \boldsymbol{Z}_+; \quad n < m \iff 0 < m - n \ \ [\text{con } m - n := m + (-n)].$$

Quindi

$$n \leq m \iff n = m \ \text{ oppure } \ n < m.$$

Le verifiche della riflessività, antisimmetria e transitività sono lasciate per esercizio.

Verifichiamo che $\leq$ è totale. Sia $n \not\leq m$. Allora $n - m \notin \boldsymbol{Z}_+ \cup \{0\}$ e dunque $-(n-m) = m - n \in \boldsymbol{Z}_-$. Pertanto $n < m$.

Verifichiamo infine che $\leq$ è compatibile con somma e prodotto. Sia $n < m$. Per ogni $p \in \boldsymbol{Z}$, $(m + p) - (n + p) = m - n > 0$. Allora $n + p < m + p$. Sia ancora $n < m$ e sia $p > 0$. Allora $m - n, p \in \boldsymbol{Z}_+$ e quindi anche $(m - n)p \in \boldsymbol{Z}_+$. Pertanto $np < mp$.

Osservazione 10. (*i*) Per ogni $n \in \boldsymbol{Z}$, si pone

$$|n| = \begin{cases} n, & \text{se } n \geq 0 \\ -n, & \text{se } n < 0. \end{cases}$$

$|n|$ è detto *valore assoluto di* n. Lasciamo per esercizio la verifica dei seguenti fatti: $\forall\, n, m \in \boldsymbol{Z}$,

$$|n + m| \leq |n| + |m|; \qquad |nm| = |n| \cdot |m|$$

[Per verificare l'ultimo risultato, conviene distinguere quattro casi: $n, m \geq 0$; $n, m < 0$; $n \geq 0$, $m < 0$; $n < 0$, $m \geq 0$].

(*ii*) Risulta: $nm = 1 \implies m = n = 1$ oppure $m = n = -1$. Infatti (cfr. **Prop. 2.***(8)*):

$$mn = 1 \implies |mn| = 1 \implies |m| \cdot |n| = 1 \implies |m| = |n| = 1 \implies m = \pm 1,\ n = \pm 1.$$

Poiché m, n non possono avere segni opposti, si conclude che $m = n = 1$ oppure $m = n = -1$.

(*iii*) Vale in $\boldsymbol{Z}$ la proprietà archimedea: $\forall\, m, n \in \boldsymbol{Z}$, con $n \neq 0$, $\exists\, p \in \boldsymbol{Z}$ tale che $m < np$.

Se $m < n$, basta porre $p = 1$.

Sia invece $n \leq m$. Se $n < 0$, si pone $p = -1 - |m|$. Allora:

$$m \leq |m| < 1 + |m| \leq (-n)(1 + |m|) = n(-1 - |m|) = np, \ \text{ cioè } \ m < np.$$

Se invece $n > 0$, si pone $p = 1 + |m|$. Allora:

$$m \leq |m| < 1 + |m| \leq n(1 + |m|) = np, \ \text{ cioè } \ m < np.$$

(*C*) NUMERI RAZIONALI

Non ogni equazione della forma $aX = b$, con $a, b \in \boldsymbol{Z}$, $a \neq 0$, è risolubile in $\boldsymbol{Z}$: ad esempio non lo è l'equazione $2X = 1$. Per rendere risolubile ogni siffatta equazione serve poter operare su insieme numerico più ampio degli interi, e per questo si introduce l'insieme $\boldsymbol{Q}$ dei *numeri razionali*.

Presenteremo $\boldsymbol{Q}$ come insieme quoziente di $\boldsymbol{Z}\times\boldsymbol{Z}^{\cdot}$ modulo un'opportuna relazione d'equivalenza ρ. Poi definiremo in $\boldsymbol{Q}$ le operazioni di addizione e moltiplicazione e ne studieremo le proprietà.

Definizione 9. *In* $\boldsymbol{Z}\times\boldsymbol{Z}^{\cdot}$ *[con* $Z^{\cdot}=\boldsymbol{Z}-\{0\}$*] è definita la seguente relazione d'equivalenza* ρ*:*

$$(a,b)\rho(c,d) \iff ad=bc, \quad \forall\,(a,b),\,(c,d)\in\boldsymbol{Z}\times\boldsymbol{Z}^{\cdot}.$$

Osservazione 11. ρ è una relazione di equivalenza su $\boldsymbol{Z}\times\boldsymbol{Z}^{\cdot}$. Verifichiamo soltanto la proprietà transitiva: se $(a,b)\rho(c,d)$ e $(c,d)\rho(e,f)$, allora $(a,b)\rho(e,f)$.

Infatti, essendo possibile cancellare d $(\neq 0)$:

$$\begin{cases} ad=bc \\ cf=de, \end{cases} \implies \begin{cases} adf=bcf \\ bcf=bde, \end{cases} \implies adf=bde \implies af=be \implies (a,b)\rho(e,f).$$

Definizione 10. *L'insieme quoziente* $\boldsymbol{Q}:=\boldsymbol{Z}\times\boldsymbol{Z}^{\cdot}\big/_{\rho}$ *è detto insieme dei numeri razionali. Un numero razionale è quindi una classe di equivalenza modulo* ρ*:*

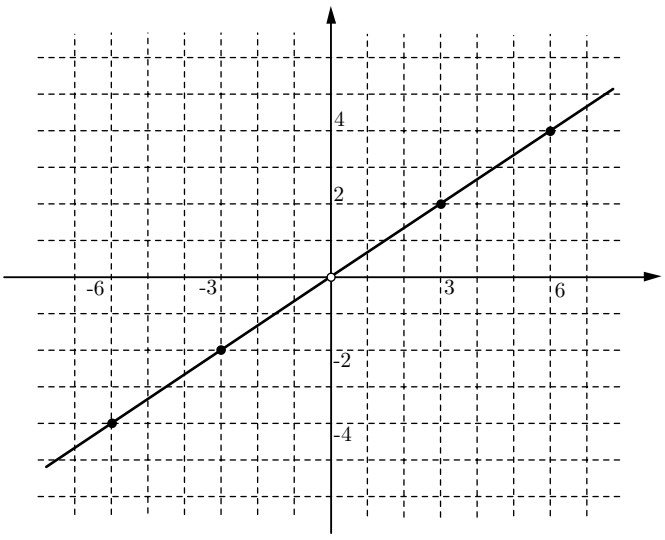
$$[a,b]:=[(a,b)]_{\rho}=\big\{(x,y)\in\boldsymbol{Z}\times\boldsymbol{Z}^{\cdot} \;:\; ay=bx\big\}.$$

$[a,b]$ *è usualmente denotato* $\frac{a}{b}$.

Osservazione 12. La classe $\frac{a}{b}=[a,b]\in\boldsymbol{Q}$ può essere visualizzata nel piano $\boldsymbol{R}^2$ come luogo dei punti a coordinate intere (ma non entrambe nulle) della retta passante per l'origine $(0,0)$ e per il punto (a,b) [di equazione $bX=aY$]. Ad esempio

$$\tfrac{3}{2}=[3,2]=\{(3,2),\,(-3,-2),\,(6,4),\,(-6,-4),\,(9,6),\;\ldots\}$$

come visualizzato nel disegno che segue.



Ora introdurremo in $\boldsymbol{Q}$ le operazioni di addizione e moltiplicazione e ne studieremo le principali proprietà.

Definizione 11. *È definita in* $\boldsymbol{Q}$ *l'operazione di addizione o somma* $+:\boldsymbol{Q}\times\boldsymbol{Q}\to\boldsymbol{Q}$ *tale che:*

$$\tfrac{a}{b}+\tfrac{c}{d}=\tfrac{ad+bc}{bd}, \quad \forall\,\tfrac{a}{b},\,\tfrac{c}{d}\in\boldsymbol{Q}.$$

Osservazione 13. Verifichiamo che tale definizione è ben posta. Se $\frac{a}{b}=\frac{a_1}{b_1}$ e $\frac{c}{d}=\frac{c_1}{d_1}$, bisogna verificare che $\frac{ad+bc}{bd}=\frac{a_1d_1+b_1c_1}{b_1d_1}$, cioè che $(ad+bc)b_1d_1=(a_1d_1+b_1c_1)bd$.

Da $\begin{cases} ab_1 = ba_1 \\ cd_1 = dc_1, \end{cases}$ segue: $(ad+bc)b_1d_1 = ab_1dd_1 + cd_1bb_1 = ba_1dd_1 + dc_1bb_1 = bd(a_1d_1 + b_1c_1)$.

Proposizione 14. *L'addizione $+$ su $\boldsymbol{Q}$ verifica le seguenti proprietà:*

(1) è associativa;
(2) è dotata di elemento neutro, $0 = \frac{0}{1}$;
(3) è dotata di opposto $-\frac{a}{b}$ di ogni elemento $\frac{a}{b}$; risulta $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$;
(4) è commutativa.

Ne segue che $(\boldsymbol{Q}, +)$ è un gruppo commutativo.

Dim. [Lasciata per esercizio].

Definizione 12. *È definita in $\boldsymbol{Q}$ l'operazione di moltiplicazione o prodotto $\cdot : \boldsymbol{Q}\times\boldsymbol{Q} \to \boldsymbol{Q}$ tale che:*

$$\tfrac{a}{b}\cdot\tfrac{c}{d} = \tfrac{ac}{bd}, \quad \forall\, \tfrac{a}{b},\ \tfrac{c}{d} \in \boldsymbol{Q}.$$

Osservazione 14. Verifichiamo che anche la moltiplicazione è ben definita: se $\frac{a}{b} = \frac{a_1}{b_1}$ e $\frac{c}{d} = \frac{c_1}{d_1}$, bisogna verificare che $\frac{ac}{bd} = \frac{a_1c_1}{b_1d_1}$, cioè che $acb_1d_1 = a_1c_1bd$.

Da $\begin{cases} ab_1 = ba_1 \\ cd_1 = dc_1, \end{cases}$ segue, moltiplicando a membro a membro: $acb_1d_1 = bda_1c_1$.

Proposizione 15. *La moltiplicazione $\cdot$ su $\boldsymbol{Q}$ verifica le seguenti proprietà:*

(1) è associativa;
(2) è distributiva rispetto alla somma [cioè, $\forall\, \frac{a}{b},\ \frac{c}{d},\ \frac{e}{f} \in \boldsymbol{Q}$, risulta

$$(\tfrac{a}{b} + \tfrac{c}{d})\tfrac{e}{f} = \tfrac{a}{b}\cdot\tfrac{e}{f} + \tfrac{c}{d}\cdot\tfrac{e}{f}, \quad \tfrac{a}{b}(\tfrac{c}{d} + \tfrac{e}{f}) = \tfrac{a}{b}\cdot\tfrac{c}{d} + \tfrac{a}{b}\cdot\tfrac{e}{f}];$$

(3) è dotata di elemento neutro, $1 = \frac{1}{1}$;
(4) è commutativa.
(5) è dotata di inverso $(\frac{a}{b})^{-1}$ di ogni elemento $\frac{a}{b} \neq 0$; risulta $(\frac{a}{b})^{-1} = \frac{b}{a}$.

Si conclude che $(\boldsymbol{Q}, +, \cdot)$ è un campo.

Dim. [Lasciata per esercizio].

Proposizione 16. *L'applicazione $i : \boldsymbol{Z} \to \boldsymbol{Q}$ tale che $i(a) = \frac{a}{1}$, $\forall\, a \in \boldsymbol{Z}$, è un omomorfismo iniettivo di anelli. Tramite i, $\boldsymbol{Z}$ è identificato ad un sottoanello di $\boldsymbol{Q}$.*

Dim. L'applicazione i è iniettiva. Infatti: $i(a) = i(b) \implies \frac{a}{1} = \frac{b}{1} \implies a\cdot 1 = b\cdot 1 \implies a = b$.
i è un omomorfismo di anelli. Infatti, $\forall\, a, b \in \boldsymbol{Z}$:

$$i(a+b) = \tfrac{a+b}{1} = \tfrac{a}{1} + \tfrac{b}{1} = i(a) + i(b); \qquad i(ab) = \tfrac{ab}{1} = \tfrac{a}{1}\cdot\tfrac{b}{1} = i(a)\cdot i(b)$$

L'insieme $i(\boldsymbol{Z}) \subset \boldsymbol{Q}$ è un sottoanello di $\boldsymbol{Q}$.

Osservazione 15. (*i*) Ogni $\frac{a}{b} \in \boldsymbol{Q}$ si può scrivere nella forma $\frac{a/1}{b/1} = \frac{i(a)}{i(b)}$, cioè come quoziente di interi. Infatti:

$$\tfrac{a}{b} = \tfrac{a}{1}\cdot\tfrac{1}{b} = \tfrac{a}{1}\cdot(\tfrac{b}{1})^{-1} = i(a)\cdot i(b)^{-1} = \tfrac{i(a)}{i(b)}.$$

Per tale motivo $\boldsymbol{Q}$ è detto *campo dei quozienti di* $\boldsymbol{Z}$.

(*ii*) Ogni equazione del tipo $aX = b$, con $a,\, b \in \boldsymbol{Q}$, $a \neq 0$ è risolubile in $\boldsymbol{Q}$ ed ha un'unica soluzione $x = a^{-1}b$.

(*iii*) Il campo $\boldsymbol{Q}$ è totalmente ordinato. Basta infatti definire su $\boldsymbol{Q}$ la seguente relazione $<$:

$$0 < \tfrac{a}{b} \iff ab \in \boldsymbol{Z}_+; \quad \tfrac{a}{b} < \tfrac{c}{d} \iff 0 < \tfrac{c}{d} - \tfrac{a}{b}, \quad \forall\, \tfrac{a}{b},\ \tfrac{c}{d} \in \boldsymbol{Q}$$

e quindi

$$\tfrac{a}{b} \le \tfrac{c}{d} \iff \tfrac{a}{b} = \tfrac{c}{d} \text{ oppure } \tfrac{a}{b} < \tfrac{c}{d}, \quad \forall\, \tfrac{a}{b},\, \tfrac{c}{d} \in \boldsymbol{Q}.$$

Si verifica che $\le$ è una relazione totale su $\boldsymbol{Q}$, compatibile con le due operazioni di $\boldsymbol{Q}$.

(*D*) NUMERI REALI [Cenno]

Non ogni equazione della forma $X^2 = q$, con $q \in \boldsymbol{Q}$, $q > 0$, è risolubile in $\boldsymbol{Q}$: ad esempio non lo è l'equazione $X^2 = 2$ (come verificheremo in **Cap. II, Prop. 3.4**). Per risolvere questa ed altre equazioni si introduce l'insieme $\boldsymbol{R}$ dei *numeri reali*. Non definiremo compiutamente $\boldsymbol{R}$, ma ci limiteremo a presentare per sommi capi la definizione di $\boldsymbol{R}$ che utilizza le successioni di Cauchy.

Ricordiamo che una successione $\{x_n\}$ in un insieme A è l'immagine di un'applicazione $f : \boldsymbol{N} \to A$. Assumiamo inoltre nota la definizione di *convergenza di una successione* [cfr. **Osserv. 1.1**(i)].

Definizione 13. *Sia $\{x_n\}$ una successione in $\boldsymbol{Q}$. La successione $\{x_n\}$ è detta successione di Cauchy se* $\forall\, \varepsilon > 0,\ \exists\, n_\varepsilon \in \boldsymbol{N}$ *tale che* $|x_n - x_m| < \varepsilon,\ \forall\, n, m \ge n_\varepsilon$.

Si può verificare facilmente che ogni successione in $\boldsymbol{Q}$ che converge in $\boldsymbol{Q}$ [cioè convergente ad un numero razionale] è anche una successione di Cauchy; il viceversa è in generale falso.

Definizione 14. *Denotato con $\mathfrak{C}$ l'insieme delle successioni di Cauchy in $\boldsymbol{Q}$, si introduce su $\mathfrak{C}$ la seguente relazione $\sim$:* $\forall\, \{x_n\}, \{y_n\} \in \mathfrak{C}$,

$$\{x_n\} \sim \{y_n\} \iff \{x_n - y_n\} \text{ converge a } 0$$

[e scriveremo, brevemente, $\{x_n - y_n\} \to 0$].

Si verifica facilmente che $\sim$ è una relazione di equivalenza su $\mathfrak{C}$. L'insieme quoziente $\mathfrak{C}/_{\sim}$ è detto insieme dei numeri reali, denotato $\boldsymbol{R}$. Un numero reale verrà quindi denotato con $[\{x_n\}]$ o $[\{x_n\}]_\sim$, in quanto classe di equivalenza di $\{x_n\}$ modulo $\sim$.

In $\boldsymbol{R}$ si introducono le due operazioni:

$$+ : \boldsymbol{R}\times\boldsymbol{R} \to \boldsymbol{R} \text{ tale che } [\{x_n\}] + [\{y_n\}] = [\{x_n + y_n\}],\ \forall\, [\{x_n\}], [\{y_n\}] \in \boldsymbol{R};$$

$$\cdot : \boldsymbol{R}\times\boldsymbol{R} \to \boldsymbol{R} \text{ tale che } [\{x_n\}]\cdot[\{y_n\}] = [\{x_n \cdot y_n\}],\ \forall\, [\{x_n\}], [\{y_n\}] \in \boldsymbol{R}.$$

Bisogna ovviamente verificare che le due operazioni sono ben definite. Si verifica poi che $(\boldsymbol{R}, +, \cdot)$ è un campo.

Si può facilmente verificare che $(\boldsymbol{R}, +, \cdot)$ contiene $\boldsymbol{Q}$ come sottoanello (o, per meglio dire, come *sottocampo*). Infatti $\boldsymbol{Q}$ si identifica al sottoinsieme di $\boldsymbol{R}$

$$\big\{[\{q\}],\ \forall\, \{q\} \text{ successione costante di valore } q \in \boldsymbol{Q}\big\}.$$

Considerato un numero reale $\alpha = [\{x_n\}]$, diremo che $\alpha \ge 0$ se la successione di Cauchy $\{x_n\}$ è equivalente ad una successione di Cauchy $\{y_n\}$ formata da razionali non negativi. Diremo poi che $\alpha \ge \beta \iff a - \beta \ge 0$.

Con tale relazione di diseguaglianza $\ge$, si può verificare che $(\boldsymbol{R}, +, \cdot)$ è un campo totalmente ordinato. Si noti che in $\boldsymbol{R}$ [come in $\boldsymbol{Q}$ e, più generalmente, come in ogni anello totalmente ordinato $(A, +, \cdot)$, cfr. **Osserv. 4.4**] risulta: $\alpha^2 > 0,\ \forall\, \alpha \ne 0$.

(*E*) NUMERI COMPLESSI

Nel campo $\boldsymbol{R}$, l'equazione $X^2 + 1 = 0$, non ha soluzioni [infatti un quadrato non è mai negativo]. Cerchiamo allora un insieme contenente $\boldsymbol{R}$ e contenente una soluzione (almeno) della precedente

equazione. Otterremo l'insieme $\boldsymbol{C}$ dei *numeri complessi*.

Definizione 15. *Sia i un simbolo verificante la condizione $i^2 = -1$. L'insieme delle espressioni formali $a + ib$, $\forall\, a, b \in \boldsymbol{R}$ è detto insieme dei numeri complessi ed è denotato $\boldsymbol{C}$. Per ogni numero complesso $z = a + ib \in \boldsymbol{C}$,*

a è detta parte reale di z, denotata $\mathcal{R}e(z)$;
b è detta parte immaginaria di z, denotata $\mathcal{I}m(z)$.
Imponendo la regola $0\, i = 0$, si ottiene che, $\forall\, r \in \boldsymbol{R}$, $r = r + 0i \in \boldsymbol{C}$. Dunque $\boldsymbol{R} \subset \boldsymbol{C}$.

L'insieme $\boldsymbol{C}$ può essere identificato con il piano $\boldsymbol{R}^2$ [che prende il nome di *piano di Gauss* (o *piano di Argand-Gauss*), tramite la biiezione

$$z = a + ib \in \boldsymbol{C} \longrightarrow (a, b) \in \boldsymbol{R}^2;$$

In particolare $\boldsymbol{R}$ (come sottoinsieme di $\boldsymbol{C}$) coincide con l'*asse x* di $\boldsymbol{R}^2$.

Definizione 16. *Si definiscono su $\boldsymbol{C}$ le due seguenti operazioni di addizione e moltiplicazione:*

$$+ : \boldsymbol{C}\times\boldsymbol{C} \to \boldsymbol{C} \quad \text{tale che} \quad (a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2),$$
$$\cdot : \boldsymbol{C}\times\boldsymbol{C} \to \boldsymbol{C} \quad \text{tale che} \quad (a_1 + ib_1)\cdot(a_2 + ib_2) = (a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1),$$

$\forall\, a_1 + ib_1,\ a_2 + ib_2 \in \boldsymbol{C}$.

Osservazione 16. Nell'identificazione tra $\boldsymbol{C}$ ed $\boldsymbol{R}^2$, la somma di due numeri complessi corrisponde alla somma di vettori di $\boldsymbol{R}^2$.

Il prodotto di due numeri complessi coincide con l'usuale moltiplicazione "polinomiale" delle due espressioni formali $a_1 + ib_1$, $a_2 + ib_2$, con l'ulteriore regola: $i^2 = -1$.

Proposizione 17. *$(\boldsymbol{C}, +, \cdot)$ è un campo ed un $\boldsymbol{R}$-spazio vettoriale di dimensione 2.*

Dim. [Lasciata per esercizio]. Si noti che: $0 = 0 + i0$ è l'elemento neutro della somma; $1 = 1 + 0i$ è l'elemento neutro del prodotto; $-z = -a - ib$ è l'opposto di $z = a + ib$; per ogni numero complesso $z = a + ib \neq 0$, $z^{-1} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$ è l'inverso di z. Infine, $\{1, i\}$ è una base di $\boldsymbol{C}$ come $\boldsymbol{R}$-spazio vettoriale.

Definizione 17. *Per ogni numero complesso $z = a + ib$,*

$\overline{z} := a - ib$ è detto coniugato di z;
$z\,\overline{z} = a^2 + b^2$ è detto norma di z; si tratta di un numero reale ≥ 0, denotato $\mathcal{N}(z)$;
$|z| := \sqrt{z\,\overline{z}} = \sqrt{a^2 + b^2}$ è detto modulo di z; si tratta di un numero reale ≥ 0.

Osservazione 17. Nell'identificazione tra $\boldsymbol{C}$ ed $\boldsymbol{R}^2$, $\overline{z}$ è il simmetrico di z rispetto all'*asse x*. In base al teorema di Pitagora, $|z|$ è la distanza tra 0 e z [cioè tra l'origine $O = (0, 0)$ ed il punto (a, b), se $z = a + ib$].

Proposizione 18. *Risulta, $\forall\, z,\ z_1,\ z_2 \in \boldsymbol{C}$:*

(i) $\overline{\overline{z}} = z$; $\quad \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$; $\quad \overline{z_1 \cdot z_2} = \overline{z_1}\cdot\overline{z_2}$; $\quad z = \overline{z} \iff z \in \boldsymbol{R}$;
(ii) $|z_1 z_2| = |z_1|\cdot|z_2|$;
(iii) $|z_1 + z_2| \leq |z_1| + |z_2|$.

Dim. La (*i*) e la (*ii*) sono del tutto ovvie; per la (*iii*) basta ricordare che in un triangolo la lunghezza di un lato è minore o uguale alla somma della lunghezza degli altri due.

Osservazione 18. (*i*) Sia $\alpha : \boldsymbol{C} \to \mathfrak{M}_2(\boldsymbol{R})$ l'applicazione così definita:

$$\alpha(z) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathfrak{M}_2(\boldsymbol{R}), \quad \forall\, z = a + ib \in \boldsymbol{C}.$$

Si verifica facilmente che α è un omomorfismo iniettivo di anelli. Ne segue che $\boldsymbol{C}$ è identificable ad un sottoinsieme di $\mathfrak{M}_2(\boldsymbol{R})$.

(*ii*) $\boldsymbol{C}$ non può essere totalmente ordinato in modo che il suo ordinamento sia compatibile con quello di $\boldsymbol{R}$. Infatti, in $\boldsymbol{R}$, $-1 < 0$ e quindi in $\boldsymbol{C}$ deve risultare $i^2 < 0$. Ma si è già osservato che in ogni anello totalmente ordinato ogni quadrato è positivo [cfr. **Osserv. 4.4**].

Ci occuperemo ora della *rappresentazione trigonometrica* dei numeri complessi.

Ad ogni numero complesso non nullo $z = a + ib \in \boldsymbol{C}^{\cdot}$ resta associata una coppia (ρ, ϑ_0) di numeri reali, così definiti:

- $\rho = |z|$ è il *modulo* di z [già definito in **Def. 17**];

- $\vartheta_0 \in [0, 2\pi)$ è la misura in radianti dell'angolo (orientato in verso antiorario) di vertice $O = (0,0)$ tra l'*asse x* (positivamente orientato) e la semiretta $O\,z$. È detto *argomento principale di z*. Dalla trigonometria

$$\begin{cases} a = \rho \cos \vartheta_0 \\ b = \rho \sin \vartheta_0. \end{cases}$$

Osservazione 19. Sia $z = a + ib \in \boldsymbol{C}^{\cdot}$. Abbiamo già osservato che

$$\rho = |z| = \sqrt{a^2 + b^2}.$$

Relativamente a ϑ_0, si ha:

$$\vartheta_0 = \begin{cases} \arccos \frac{a}{\sqrt{a^2+b^2}}\,, & \text{se } b \geq 0 \\ 2\pi - \arccos \frac{a}{\sqrt{a^2+b^2}}\,, & \text{se } b < 0. \end{cases}$$

Infatti, $\forall\, \vartheta_0 \in [0, 2\pi)$ risulta: $a = \rho \cos \vartheta_0$, cioè $\cos \vartheta_0 = \frac{a}{\rho}$. Ne segue:

- se $\vartheta_0 \in [0, \pi]$, cioè se $b \geq 0$, allora $\vartheta_0 = \arccos \frac{a}{\rho} = \arccos \frac{a}{\sqrt{a^2+b^2}}$;

- se $\vartheta_0 \in (\pi, 2\pi)$, cioè se $b < 0$, allora [usando la seconda determinazione della funzione arccos cioè la funzione $f(x) = 2\pi - \arccos(x)$] si ottiene: $\vartheta_0 = 2\pi - \arccos \frac{a}{\rho} = 2\pi - \arccos \frac{a}{\sqrt{a^2+b^2}}$.

Abbiamo così costruito un'applicazione

$$\Phi : \boldsymbol{C}^{\cdot} \to \boldsymbol{R}^+ \times [0, 2\pi) \quad \text{tale che} \quad \Phi(z) = (\rho, \vartheta_0), \quad \forall\, z \in \boldsymbol{C}^{\cdot},$$

con ρ, ϑ_0 definiti come nella precedente osservazione.

Tale applicazione Φ è biiettiva. Per dimostrarlo ne costruiremo l'inversa. Poniamo

$$\Psi : \boldsymbol{R}^+ \times [0, 2\pi) \to \boldsymbol{C}^{\cdot} \quad \text{tale che} \quad \Psi(\rho, \vartheta_0) = \rho\big(\cos \vartheta_0 + i \sin \vartheta_0\big), \quad \forall\, (\rho, \vartheta_0) \in \boldsymbol{R}^+ \times [0, 2\pi).$$

Si tratta ora di verificare che risulta:

$$\Psi \circ \Phi = \mathbf{1}_{\boldsymbol{C}^{\cdot}}\,, \qquad \Phi \circ \Psi = \mathbf{1}_{\boldsymbol{R}^+ \times [0, 2\pi)}\,.$$

[Le semplici verifiche sono lasciate al lettore].

Abbiamo dunque ottenuto che, $\forall\, z \in \boldsymbol{C}^{\cdot}$, $\exists!(\rho, \vartheta_0) \in \boldsymbol{R}^+ \times [0, 2\pi)$ tale che

$$z = \rho\big(\cos \vartheta_0 + i \sin \vartheta_0\big).$$

Tale espressione è detta *espressione trigonometrica di z*.

Osservazione 20. La biiezione $\Psi : \boldsymbol{R}^+ \times [0, 2\pi) \to \boldsymbol{C}^{\cdot}$ può essere estesa ad un'applicazione [suriettiva ma non iniettiva]

$$\psi : \boldsymbol{R}^+ \times \boldsymbol{R} \to \boldsymbol{C}^{\cdot} \quad \text{tale che} \quad \psi(\rho, \vartheta) = \rho\big(\cos \vartheta + i \sin \vartheta\big), \quad \forall\, (\rho, \vartheta) \in \boldsymbol{R}^+ \times \boldsymbol{R}.$$

Ne segue che ogni $z \in \boldsymbol{C}^{\cdot}$ si scrive nella forma

$$z = \rho\big(\cos \vartheta + i \sin \vartheta\big),$$

ancora detta *espressione trigonometrica di z*; ϑ è detto *argomento di z*. Tale espressione non è però unica per z.

Ricordato che le funzioni cos e sin sono funzioni periodiche (di periodo 2π), si verifica facilmente che, $\forall\, z_1 = \rho_1\big(\cos\vartheta_1 + i\sin\vartheta_1\big)$, $z_2 = \rho_2\big(\cos\vartheta_2 + i\sin\vartheta_2\big) \in \boldsymbol{C}^*$, si ha:

$$z_1 = z_2 \iff \rho_1 = \rho_2 \ \text{ e } \ \vartheta_2 = \vartheta_1 + 2k\pi,\ \exists\, k \in \boldsymbol{Z}.$$

Proposizione 19. *(i) Siano* $z_1 = \rho_1\big(cos\vartheta_1 + i\,sin\vartheta_1\big)$, $z_2 = \rho_2\big(cos\vartheta_2 + i\,sin\vartheta_2\big) \in \boldsymbol{C}^*$. *Risulta:*

$$z_1 z_2 = \rho_1\rho_2\big(cos(\vartheta_1 + \vartheta_2) + i\,sin(\vartheta_1 + \vartheta_2)\big).$$

(ii) (Formula di De Moivre). Sia $z = \rho\big(cos\vartheta + i\,sin\vartheta\big) \in \boldsymbol{C}^*$. *Per ogni* $n \in \boldsymbol{Z}$, *risulta:*

$$z^n = \rho^n\big(cos\, n\vartheta + i\,sin\, n\vartheta\big)$$

Dim. (*i*) Si ha: $z_1 z_2 = \rho_1\rho_2\big(\cos\vartheta_1 + i\sin\vartheta_1\big)\big(\cos\vartheta_2 + i\sin\vartheta_2\big) =$

$$= \rho_1\rho_2\big[(\cos\vartheta_1\cos\vartheta_2 - \sin\vartheta_1\sin\vartheta_2) + i(\sin\vartheta_1\cos\vartheta_2 + \cos\vartheta_1\sin\vartheta_2)\big]$$
$$= \rho_1\rho_2\big(\cos(\vartheta_1 + \vartheta_2) + i\sin(\vartheta_1 + \vartheta_2)\big).$$

(*ii*) Se $n > 0$, segue subito da (*i*). Se $n = 0$, $\rho^0(\cos 0 + i\sin 0) = 1 = z^0$. Sia $n < 0$. Si osservi che, posto $w := \rho^{-1}\big(\cos(-\vartheta) + i\sin(-\vartheta)\big)$, risulta da (*i*) che $w = z^{-1}$. Allora

$$z^n = (z^{-1})^{|n|} = (\rho^{-1})^{|n|}\big(\cos(|n|(-\vartheta)) + \sin(|n|(-\vartheta))\big) = \rho^n\big(\cos n\vartheta + i\sin n\vartheta\big).$$

Si noti che, posto $\mathrm{e}^{i\vartheta} := \cos\vartheta + i\sin\vartheta$, $\forall\,\vartheta \in \boldsymbol{R}$ [nota come *identità di Eulero*], l'espressione trigonometrica $z = \rho(cos\vartheta + i\sin\vartheta)$ diventa

$$z = \rho\,\mathrm{e}^{i\vartheta},$$

nota come *espressione esponenziale di* z. La formula di De Moivre diventa:

$$z^n = \rho^n\,\mathrm{e}^{in\vartheta},\quad \forall\, n \in \boldsymbol{Z}.$$

Concludiamo questa sezione sui numeri complessi, introducendo la definizione di *radice n-sima di un numero complesso.*

Definizione 18. *Sia* $z \in \boldsymbol{C}$ *e sia* $n \in \boldsymbol{N}$. *Si chiama radice n-sima di* z *ogni* $\alpha \in \boldsymbol{C}$ *tale che* $\alpha^n = z$. *Denotiamo con* $\sqrt[n]{z} = \big\{\alpha \in \boldsymbol{C} \,:\, \alpha^n = z\big\}$ *l'insieme delle radici n-sime di* z. *Si tratta delle soluzioni dell'equazione* $X^n = z$.

Osservazione 21. Sia $z = r(\cos t + i\sin t) \neq 0$, con $r > 0$ e $t \in [0, 2\pi)$. Denotiamo con $\alpha = \rho(\cos\vartheta + i\sin\vartheta)$ un arbitrario numero complesso $[\neq 0]$, al momento non noto. Poiché, in base alla formula di de Moivre, $\alpha^n = \rho^n(\cos n\vartheta + i\sin n\vartheta)$, allora:

$$\alpha^n = z \iff \rho^n = r \ \text{ e } \ n\vartheta = t + 2k\pi,\ \exists\, k \in \boldsymbol{Z} \iff \rho = \sqrt[n]{r} \ \text{ e } \ \vartheta = \tfrac{t+2k\pi}{n},\ \exists\, k \in \boldsymbol{Z}.$$

Essendo le funzioni cos e sin periodiche di periodo 2π, allora

$$\sqrt[n]{z} = \big\{\sqrt[n]{r}\big(\cos\tfrac{t+2k\pi}{n} + i\sin\tfrac{t+2k\pi}{n}\big),\ \ \forall\, k \in \boldsymbol{Z}\big\}.$$

Si può verificare che, $\forall\, h, k \in \{0, 1, \dots, n-1\}$, con $h \neq k$, gli argomenti $\frac{t+2h\pi}{n}$ e $\frac{t+2k\pi}{n}$ non differiscono per multipli interi di 2π. Viceversa, $\forall\, h \in \boldsymbol{Z}$, esiste un unico $r \in \{0, 1, \dots, n-1\}$, tale che $\frac{t+2h\pi}{n} = \frac{t+2r\pi}{n} + 2q\pi$ [basta dividere h per n: si ottiene $h = nq + r$, con $0 \leq r < n$, cfr. **Cap. II.1**]. Dunque

$$\sqrt[n]{z} = \big\{\sqrt[n]{r}\big(\cos\tfrac{t+2k\pi}{n} + i\sin\tfrac{t+2k\pi}{n}\big),\ \ \forall\, k = 0, 1, \dots, n-1\big\}.$$

Concludiamo che $\sqrt[n]{z}$ è formato esattamente da n numeri complessi distinti, che hanno lo stesso modulo [cioè $\sqrt[n]{r}$] e dunque (pensati in $\boldsymbol{R}^2$) giacciono su una stessa circonferenza di centro l'origine 0 e raggio $\sqrt[n]{r}$. Sono ottenuti l'uno dall'altro con una rotazione antioraria di angolo multiplo di $\frac{2\pi}{n}$. Quindi sono i vertici di un poligono regolare n-latero, inscritto in una circonferenza di raggio $\sqrt[n]{r}$.

Se in particolare consideriamo il numero complesso $1 = \cos 0 + i\sin 0$, otteniamo l'insieme delle *radici n-sime dell'unità*:

$$\sqrt[n]{1} = \big\{\cos\tfrac{2k\pi}{n} + i\sin\tfrac{2k\pi}{n},\ \ \forall\, k = 0, 1, \dots, n-1\big\},$$

che è comunemente denotato $\boldsymbol{C}_n$. Per indicare le radici n-sime dell'unità si usa la seguente notazione:

$$\zeta_{n,k} := \cos\tfrac{2k\pi}{n} + i\sin\tfrac{2k\pi}{n}, \quad \forall\, n \geq 1, \quad \forall\, k = 0, 1, \ldots, n-1.$$

In particolare, si pone:

$$\zeta_n := \zeta_{n,1} = \cos\tfrac{2\pi}{n} + i\sin\tfrac{2\pi}{n}.$$

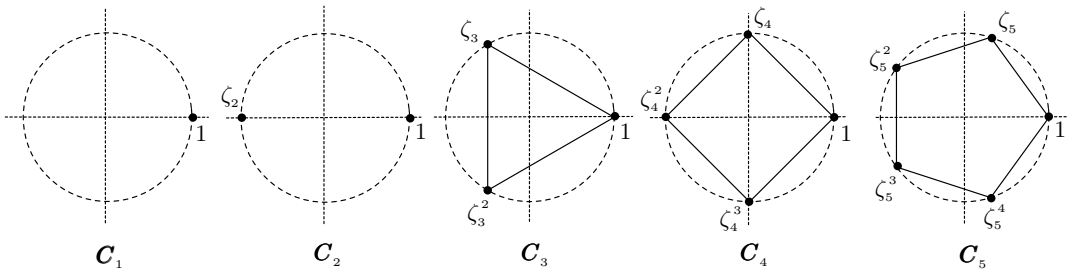
In base alla formula di De Moivre, risulta: $\zeta_n^{\,k} = \zeta_{n,k}$. Dunque

$$\boldsymbol{C}_n = \left\{\zeta_n^{\,k}, \quad \forall\, k = 0, 1, \ldots, n-1\right\} = \left\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\,n-1}\right\}.$$

A titolo di esempio, scriviamo tutte le radici n-sime, con $1 \leq n \leq 5$. Risulta:

$$\boldsymbol{C}_1 = \{1\}, \quad \boldsymbol{C}_2 = \{1, \zeta_2\}, \quad \boldsymbol{C}_3 = \left\{1, \zeta_3, \zeta_3^2\right\}, \quad \boldsymbol{C}_4 = \left\{1, \zeta_4, \zeta_4^2, \zeta_4^3\right\}, \quad \boldsymbol{C}_5 = \left\{1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4\right\},$$

con $\zeta_2 = -1$, $\zeta_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $\zeta_4 = i$, $\zeta_5 = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$.



$\boldsymbol{C}_1$ $\boldsymbol{C}_2$ $\boldsymbol{C}_3$ $\boldsymbol{C}_4$ $\boldsymbol{C}_5$

Osservazione 22. Sia $z \in \boldsymbol{C}^{\cdot}$ e sia $\alpha_0 \in \sqrt[n]{z}$. Verifichiamo che risulta:

$$\sqrt[n]{z} = \alpha_0 \boldsymbol{C}_n \quad [= \left\{\alpha_0, \alpha_0\zeta_n, \alpha_0\zeta_n^2, \ldots, \alpha_0\zeta_n^{\,n-1}\right\}].$$

Infatti, $\forall\, k = 0, 1, \ldots, n-1$, si ha:

$$(\alpha_0\zeta_n^{\,k})^n = \alpha_0^{\,n}(\zeta_n^{\,k})^n = \alpha_0^{\,n}(\zeta_n^{\,n})^k = z \cdot 1^k = z.$$

Dunque $\alpha_0\zeta_n^{\,k} \in \sqrt[n]{z}$ e pertanto $\alpha_0\boldsymbol{C}_n \subseteq \sqrt[n]{z}$.

Si osservi ora che (in base a **Prop. 19**(i)) $\alpha_0\zeta_n$ è ottenuto ruotando α_0 di un angolo di $\frac{2\pi}{n}$ radianti intorno all'origine (in verso antiorario). Analogamente, $\alpha_0\zeta_n^{\,2}$ è ottenuto nello stesso modo da $\alpha_0\zeta_n$, e così via. Ne segue che gli n numeri complessi di $\alpha_0\boldsymbol{C}_n$ sono a due a due distinti e dunque "riempono" tutto $\sqrt[n]{z}$. Si conclude che $\sqrt[n]{z} = \alpha_0\boldsymbol{C}_n$.

($\boldsymbol{F}$) QUATERNIONI

Abbiamo osservato che $\boldsymbol{C}$ è un campo contenente $\boldsymbol{R}$ ed è un $\boldsymbol{R}$-spazio vettoriale di dimensione (finita) 2. Potremmo chiederci se esistono campi K contenenti $\boldsymbol{C}$ e che sono al tempo stesso $\boldsymbol{R}$-spazi vettoriali di dimensione finita > 2. Tale problema di ricerca di "strutture ipercomplesse" è stato attivamente studiato (e risolto) nella seconda metà dell'ottocento.

Nel 1843 W. Hamilton ha determinato un corpo (cioè un campo non commutativo) contenente $\boldsymbol{C}$ ed avente dimensione 4 come $\boldsymbol{R}$-spazio vettoriale. Si tratta del *corpo dei quaternioni*, che adesso definiremo. Successivamente, G. Frobenius ha dimostrato che non esistono altri corpi (e quindi campi) contenenti $\boldsymbol{C}$ che siano $\boldsymbol{R}$-spazi vettoriali di dimensione finita, chiudendo così il problema cui si è accennato. Esistono comunque altre strutture ipercomplesse contenenti i quaternioni e di dimensione finita su $\boldsymbol{R}$. Si tratta degli *ottetti di Cayley*, che sono corpi non associativi di dimensione 8 su $\boldsymbol{R}$.

Definizione 19. *Si chiama quaternione (reale), relativo a due numeri complessi $z, w \in \boldsymbol{C}$, la matrice quadrata [di ordine 2 ed a valori in $\boldsymbol{C}$]:*

$$\boldsymbol{h}(z, w) = \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \in \mathfrak{M}_2(\boldsymbol{C}).$$

L'insieme $\boldsymbol{H} = \{\boldsymbol{h}(z, w), \ \forall\, z, w \in \boldsymbol{C}\} \subset \mathfrak{M}_2(\boldsymbol{C})$ è detto insieme dei quaternioni(reali).

Poiché $\boldsymbol{H} \subset \mathfrak{M}_2(\boldsymbol{C})$ e poiché $\mathfrak{M}_2(\boldsymbol{C})$ è un anello [rispetto alla somma ed al prodotto righe per

colonne], ha senso esaminare la struttura algebrica di $\boldsymbol{H}$ [rispetto a tali operazioni].

Proposizione 20. $(\boldsymbol{H},+,\cdot)$ *è un corpo. Inoltre* $\boldsymbol{C}$ *è identificabile ad un sottoanello di* $\boldsymbol{H}$.

Dim. Occorre innnazitutto verificare che la somma ed il prodotto di due quaternioni è un quaternione. Infatti, $\forall\, z_1,\, w_1,\, z_2,\, w_2 \in \boldsymbol{C}$, si ha:

$$\boldsymbol{h}(z_1,w_1)+\boldsymbol{h}(z_2,w_2)=\boldsymbol{h}(z_1+z_2,w_1+w_2);$$
$$\boldsymbol{h}(z_1,w_1)\cdot\boldsymbol{h}(z_2,w_2)=\boldsymbol{h}(z_1z_2-w_1\overline{w_2},\, z_1w_2+w_1\overline{z_2}).$$

Risulta poi:

- $\underline{\mathbf{0}} := \boldsymbol{h}(0,0)=\begin{pmatrix}0&0\\0&0\end{pmatrix}$ è elemento neutro della somma;
- $\boldsymbol{h}(-z,-w)$ è l'opposto di $\boldsymbol{h}(z,w)$;
- valgono le proprietà associative della somma e del prodotto;
- $\underline{\mathbf{1}} := \boldsymbol{h}(1,0)=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ è elemento neutro del prodotto;
- valgono le proprietà distributive tra la somma ed il prodotto.
- $\boldsymbol{h}(i,0)\,\boldsymbol{h}(0,1)\neq\boldsymbol{h}(0,1)\,\boldsymbol{h}(i,0)$.

È così verificato che $(\boldsymbol{H},+,\cdot)$ è un anello unitario non commutativo.

Verifichiamo che $(\boldsymbol{H}^{\cdot},\cdot)$ è un gruppo, cioè che ogni $\boldsymbol{h}(z,w)\neq\underline{\mathbf{0}}$ ammette inverso in $\boldsymbol{H}$. Risulta:

$$det\big(\boldsymbol{h}(z,w)\big)=\begin{vmatrix} z & w\\ -\overline{w} & \overline{z}\end{vmatrix}=z\,\overline{z}+w\overline{w}=\mathcal{N}(z)+\mathcal{N}(w)>0.$$

Allora la matrice $\boldsymbol{h}(z,w)$ è invertibile in $\mathfrak{M}_2(\boldsymbol{C})$ e risulta:

$$\boldsymbol{h}(z,w)^{-1}=\tfrac{1}{det(\boldsymbol{h}(z,w))}\begin{pmatrix}\overline{z}&-w\\ \overline{w}&z\end{pmatrix}=\boldsymbol{h}\big(\tfrac{\overline{z}}{det(\boldsymbol{h}(z,w))},\,\tfrac{-w}{det(\boldsymbol{h}(z,w))}\big)\in\boldsymbol{H}.$$

Resta ora da verificare che esiste un omomorfismo iniettivo $f:\boldsymbol{C}\to\boldsymbol{H}$. Si ponga

$$f(z)=\boldsymbol{h}(a,b),\quad \forall\, z=a+ib\in\boldsymbol{C}.$$

Si verifica facilmente che f è iniettiva e che f è un omomorfismo di anelli, cioè:

$$f(z_1+z_2)=f(z_1)+f(z_2),\qquad f(z_1\cdot z_2)=f(z_1)\cdot f(z_2),\quad \forall\, z_1,\, z_2\in\boldsymbol{C}.$$

Alternativamente, si può osservare che $f=i\circ\alpha$ dove $\alpha:\boldsymbol{C}\to\mathfrak{M}_2(\boldsymbol{R})$ è l'omomorfismo definito in **Osserv. 18**(i), mentre $i:\mathfrak{M}_2(\boldsymbol{R})\to\mathfrak{M}_2(\boldsymbol{C})$ è l'inclusione canonica. Essendo α ed i omomorfismi iniettivi, anche f lo è.

Proposizione 21. $\boldsymbol{H}$ *è un* $\boldsymbol{R}$*-spazio vettoriale di dimensione* 4.

Dim. $\boldsymbol{H}$ è dotato di struttura di $\boldsymbol{R}$-spazio vettoriale. Basta definire la seguente moltiplicazione per uno scalare:

$$a\,\boldsymbol{h}(z,w)=\boldsymbol{h}(a,0)\,\boldsymbol{h}(z,w)=\boldsymbol{h}(az,aw),\quad \forall\, a\in\boldsymbol{R},\quad \forall\boldsymbol{h}(z,w)\in\boldsymbol{H},$$

e verificare gli assiomi di spazio vettoriale.

A questo punto è sufficiente verificare che ogni $\boldsymbol{h}(z,w)\in\boldsymbol{H}$ si può scrivere in modo unico come combinazione lineare, a coefficienti in $\boldsymbol{R}$, dei seguenti quattro quaternioni:

$$\underline{\mathbf{1}}=\boldsymbol{h}(1,0),\quad \underline{\boldsymbol{i}}=\boldsymbol{h}(i,0),\quad \underline{\boldsymbol{j}}=\boldsymbol{h}(0,1),\quad \underline{\boldsymbol{k}}=\boldsymbol{h}(0,i).$$

Infatti, $\forall\, z=a+ib,\ w=c+id\in\boldsymbol{C}$, risulta:

$$\boldsymbol{h}(z,w)=\begin{pmatrix}a+ib&c+id\\-c+id&a-ib\end{pmatrix}=\begin{pmatrix}a&0\\0&a\end{pmatrix}+\begin{pmatrix}ib&0\\0&-ib\end{pmatrix}+\begin{pmatrix}0&c\\-c&0\end{pmatrix}+\begin{pmatrix}0&id\\id&0\end{pmatrix}=$$
$$=a\begin{pmatrix}1&0\\0&1\end{pmatrix}+b\begin{pmatrix}i&0\\0&-i\end{pmatrix}+c\begin{pmatrix}0&1\\-1&0\end{pmatrix}+d\begin{pmatrix}0&i\\i&0\end{pmatrix}=a\underline{\mathbf{1}}+b\,\underline{\boldsymbol{i}}+c\,\underline{\boldsymbol{j}}+d\,\underline{\boldsymbol{k}}.$$

Verificare l'"unicità della scrittura è un semplice esercizio.

Proposizione 22. *L'insieme* $\mathbf{Q}:=\{\pm\underline{\mathbf{1}},\,\pm\underline{\boldsymbol{i}},\,\pm\underline{\boldsymbol{j}},\,\pm\underline{\boldsymbol{k}}\}$ *forma un gruppo rispetto al prodotto, detto gruppo delle unità dei quaternioni.*

Dim. Poiché l'associatività già vale in $\boldsymbol{H}$, è sufficiente verificare che $\mathbf{Q}$ è chiuso rispetto al prodotto e che ogni elemento di $\mathbf{Q}$ ammette inverso in $\mathbf{Q}$.

Ciò può essere fatto per verifica diretta. Si osserva che $\underline{\mathbf{1}}$ funge (ovviamente) da elemento neutro in $\mathbf{Q}$ e che gli elementi $\underline{\boldsymbol{i}}$, $\underline{\boldsymbol{j}}$, $\underline{\boldsymbol{k}}$ sono legati dalle seguenti relazioni:

$$\underline{\boldsymbol{i}}^2 = \underline{\boldsymbol{j}}^2 = \underline{\boldsymbol{k}}^2 = -\underline{\mathbf{1}}, \quad \underline{\boldsymbol{i}}\,\underline{\boldsymbol{j}} = -\underline{\boldsymbol{j}}\,\underline{\boldsymbol{i}} = \underline{\boldsymbol{k}}, \quad \underline{\boldsymbol{j}}\,\underline{\boldsymbol{k}} = -\underline{\boldsymbol{k}}\,\underline{\boldsymbol{j}} = \underline{\boldsymbol{i}}, \quad \underline{\boldsymbol{k}}\,\underline{\boldsymbol{i}} = -\underline{\boldsymbol{i}}\,\underline{\boldsymbol{k}} = \underline{\boldsymbol{j}}.$$

Si può allora scrivere la tavola moltiplicativa di $\mathbf{Q}$.

$\cdot$	$\underline{\mathbf{1}}$	$\underline{\boldsymbol{i}}$	$\underline{\boldsymbol{j}}$	$\underline{\boldsymbol{k}}$	$-\underline{\mathbf{1}}$	$-\underline{\boldsymbol{i}}$	$-\underline{\boldsymbol{j}}$	$-\underline{\boldsymbol{k}}$
$\underline{\mathbf{1}}$	$\underline{\mathbf{1}}$	$\underline{\boldsymbol{i}}$	$\underline{\boldsymbol{j}}$	$\underline{\boldsymbol{k}}$	$-\underline{\mathbf{1}}$	$-\underline{\boldsymbol{i}}$	$-\underline{\boldsymbol{j}}$	$-\underline{\boldsymbol{k}}$
$\underline{\boldsymbol{i}}$	$\underline{\boldsymbol{i}}$	$-\underline{\mathbf{1}}$	$\underline{\boldsymbol{k}}$	$-\underline{\boldsymbol{j}}$	$-\underline{\boldsymbol{i}}$	$\underline{\mathbf{1}}$	$-\underline{\boldsymbol{k}}$	$\underline{\boldsymbol{j}}$
$\underline{\boldsymbol{j}}$	$\underline{\boldsymbol{j}}$	$-\underline{k}$	$-\underline{\mathbf{1}}$	$\underline{\boldsymbol{i}}$	$-\underline{\boldsymbol{j}}$	$\underline{\boldsymbol{k}}$	$\underline{\mathbf{1}}$	$-\underline{\boldsymbol{i}}$
$\underline{\boldsymbol{k}}$	$\underline{\boldsymbol{k}}$	$\underline{\boldsymbol{j}}$	$-\underline{\boldsymbol{i}}$	$-\underline{\mathbf{1}}$	$-\underline{k}$	$-\underline{\boldsymbol{j}}$	$\underline{\boldsymbol{i}}$	$\underline{\mathbf{1}}$
$-\underline{\mathbf{1}}$	$-\underline{\mathbf{1}}$	$-\underline{\boldsymbol{i}}$	$-\underline{\boldsymbol{j}}$	$-\underline{k}$	$\underline{\mathbf{1}}$	$\underline{\boldsymbol{i}}$	$\underline{\boldsymbol{j}}$	$\underline{\boldsymbol{k}}$
$-\underline{\boldsymbol{i}}$	$-\underline{\boldsymbol{i}}$	$\underline{\mathbf{1}}$	$-\underline{k}$	$\underline{\boldsymbol{j}}$	$\underline{\boldsymbol{i}}$	$-\underline{\mathbf{1}}$	$\underline{\boldsymbol{k}}$	$-\underline{\boldsymbol{j}}$
$-\underline{\boldsymbol{j}}$	$-\underline{\boldsymbol{j}}$	$\underline{\boldsymbol{k}}$	$\underline{\mathbf{1}}$	$-\underline{\boldsymbol{i}}$	$\underline{\boldsymbol{j}}$	$-\underline{k}$	$-\underline{\mathbf{1}}$	$\underline{\boldsymbol{i}}$
$-\underline{k}$	$-\underline{k}$	$-\underline{\boldsymbol{j}}$	$\underline{\boldsymbol{i}}$	$\underline{\mathbf{1}}$	$\underline{\boldsymbol{k}}$	$\underline{\boldsymbol{j}}$	$-\underline{\boldsymbol{i}}$	$-\underline{\mathbf{1}}$

6 Cardinalità di insiemi

Definizione 1. *Due insiemi X, Y sono detti equipotenti (e si scrive $X \sim Y$) se esiste un'applicazione biiettiva $f : X \to Y$. La relazione $\sim$ è detta relazione di equipotenza.*

Osservazione 1. La relazione di equipotenza $\sim$ è una relazione di equivalenza (nella famiglia di tutti gli insiemi). Infatti:

- $X \sim X$ [tramite la biiezione identica $\mathbf{1}_X$];

- $X \sim Y \implies Y \sim X$ [se $f : X \to Y$ è biiettiva, anche $f^{-1} : Y \to X$ lo è];

- $X \sim Y$, $Y \sim Z \implies X \sim Z$ [se $f : X \to Y$, $g : Y \to Z$ sono biiettive, anche $g \circ f : X \to Z$ lo è].

Definizione 2. *La classe di equivalenza modulo $\sim$ di un insieme X è detta cardinalità di X, o numero cardinale di X, o potenza di X. È denotata $Card(X)$ o $|X|$.*

Sono detti numeri cardinali finiti le seguenti cardinalità:

$$0 := Card(\emptyset),\ 1 := Card(\{0\}),\ 2 := Card(\{0,1\}),\ \dots,\ k := Card(\{0,1,\dots,k-1\}),\ \dots$$

per ogni $k \in \boldsymbol{N}$. Un insieme X è detto finito se la sua cardinalità è un numero cardinale finito [cioè se X è equipotente a $\{0,1,\dots,k-1\}$, $\exists\, k \in \boldsymbol{N}$]. Altrimenti X è detto infinito.

Ovviamente $\boldsymbol{N}$ è un insieme infinito. La sua cardinalità è detta cardinalità del numerabile, spesso denotata $\aleph_0$ [che si legge "alef-zero" ($\aleph$ è la prima lettera dell'alfabeto ebraico)]. Dunque $Card(\boldsymbol{N}) = |\boldsymbol{N}| = \aleph_0$. Infine, un insieme X è detto numerabile se $|X| = |\boldsymbol{N}|$ (ovvero $X \sim \boldsymbol{N}$).

Osservazione 2. (*i*) Due numeri cardinali finiti k_1, k_2 con $k_1 \neq k_2$ (come numeri naturali) sono ovviamenti distinti (come numeri cardinali). Infatti non può esistere alcuna biiezione tra gli insiemi $\{0,1,\dots,k_1-1\}$ e $\{0,1,\dots,k_2-1\}$ (cfr. **Prop. 2.4**).

(*ii*) Ogni insieme numerabile X può essere scritto come una successione di elementi distinti. Se infatti $f : \boldsymbol{N} \to X$ è una biiezione, posto $f(i) = x_i$, $\forall\, i \in \boldsymbol{N}$, allora $X = Im(f) = \{x_0, x_1, x_2, \dots, x_k, \dots\}$.

Definizione 3. *Denotiamo con $\boldsymbol{Card}$ la famiglia di tutte le cardinalità. Introduciamo su $\boldsymbol{Card}$ la seguente relazione $\leq$:*

$$|X| \leq |Y| \iff \exists\, h : X \to Y \ \textit{iniettiva}.$$

Si verifica subito che tale definizione è ben posta e cioè che, se $|X| = |X_1|$ e $|Y| = |Y_1|$, allora:

$$|X| \leq |Y| \iff |X_1| \leq |Y_1|.$$

Siano infatti $f : X \to X_1$ e $g : Y \to Y_1$ due biiezioni. Se esiste un'applicazione iniettiva $h : X \to Y$, anche $g \circ h \circ f^{-1} : X_1 \to Y_1$ è iniettiva. Analogamente, se $h_1 : X_1 \to Y_1$ è iniettiva, anche $g^{-1} \circ h_1 \circ f : X \to Y$ è iniettiva.

È subito visto che $\leq$ è riflessiva e transitiva [infatti la composizione di due applicazioni iniettive è iniettiva]. Si può dimostrare che $\leq$ è anche antisimmetrica [e dunque che $\leq$ è una relazione d'ordine su $\boldsymbol{Card}$]. Tale fatto (non banalissimo) è noto come *teorema di Schroeder-Bernstein*, che ci limitiamo ad enunciare.

Teorema 1. (*Schroeder-Bernstein*). *La relazione $\leq$ è antisimmetrica. In altri termini: se esistono un'applicazione iniettiva $f : X \to Y$ ed un'applicazione iniettiva $g : Y \to X$, allora esiste una*

biiezione $h : X \to Y$.

Risulta subito:

$$0 < 1 < 2 < 3 < \ .... \ < k < k+1 < \ .... \ < |\boldsymbol{N}|.$$

A questo punto dovremmo porci alcune domande:

($\boldsymbol{A}$) $|\boldsymbol{N}|$ è la minima cardinalità infinita ?

($\boldsymbol{B}$) Esistono altre cardinalità infinite (oltre $|\boldsymbol{N}|$) ? E quali sono le cardinalità di $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$?

($\boldsymbol{C}$) $(\boldsymbol{Card}, \leq)$ è totalmente ordinato ? È bene ordinato ?

Prima di rispondere a queste domande definiamo le seguenti operazioni su $\boldsymbol{Card}$.

Definizione 4. *Siano* $\alpha = |A|$, $\beta = |B|$ *due numeri cardinali.*

Si chiama somma di α, β *il numero cardinale* $\alpha + \beta := |A \sqcup B|$ *[dove* $A \sqcup B$ *denota l'unione disgiunta di* A, B, *cfr.* **Def. 1.7***].*

Si chiama prodotto di α, β *il numero cardinale* $\alpha\beta := |A \times B|$.

Si chiama potenza di base α *ed esponente* β *il numero cardinale* $\alpha^\beta := |A^B|$ *[dove* A^B *denota l'insieme delle applicazioni da* B *ad* A*].*

Osservazione 3. (*i*) Per accettare le precedenti definizioni, occorre verificare che sono ben poste, e cioè che, se $|A| = |A_1|$ e $|B| = |B_1|$, allora

$$|A \sqcup B| = |A_1 \sqcup B_1|, \quad |A \times B| = |A_1 \times B_1|, \quad |A^B| = |A_1^{B_1}|$$

Se infatti $f : A \to A_1$ e $g : B \to B_1$ sono biiezioni, anche le tre seguenti applicazioni:

$$F : A \sqcup B \to A_1 \sqcup B_1 \ \big| \ F(a,1) = (f(a),1), \ F(b,2) = (g(b),2), \ \ \forall\, (a,1),(b,2) \in A \sqcup B;$$

$$G : A \times B \to A_1 \times B_1 \ \big| \ G(a,b) = (f(a), g(b)), \ \ \forall\, (a,b) \in A \times B;$$

$$H : A^B \to A_1^{B_1} \ \big| \ H(h) = f \circ h \circ g^{-1}, \ \ \forall\, h \in A^B,$$

sono biiezioni.

(*ii*) Si osservi che $\alpha^0 = |A|^{|\emptyset|} = \big|A^\emptyset\big| = 1$ [in quanto $A^\emptyset = \{\emptyset \hookrightarrow A\}$]. Analogamente, $0^\alpha = 0$, se $\alpha \neq 0$ [mentre 0^0 è indeterminato].

Andrebbero ora enunciate e verificate le usuali proprietà della somma, del prodotto e dell'elevamento a potenza, che estendono analoghe proprietà dei numeri naturali.

Non insistiamo su tutto ciò. Segnaliamo invece che, operando con cardinalità infinite, nascono subito semplici questioni di "calcolo", ad esempio le seguenti: quanto valgono $|\boldsymbol{N}|+|\boldsymbol{N}|$, $|\boldsymbol{N}|\cdot|\boldsymbol{N}|$, $|\boldsymbol{N}|^{|\boldsymbol{N}|}$? Ad esse, almeno, saremo presto in grado di rispondere.

La proposizione che segue risponde (affermativamente) alla prima domanda che ci eravamo posti (problema ($\boldsymbol{A}$)).

Proposizione 1. *Risulta:*

(**1**). *Se* X *è un insieme infinito,* X *contiene un sottoinsieme numerabile.*

(**2**). *Un sottoinsieme di un insieme numerabile è finito o numerabile.*

Ne segue che $|\boldsymbol{N}|$ *è la cardinalità minima infinita.*

Dim.

(**1**). Sia X infinito. Si scelga $x_0 \in X$. Poiché $X - \{x_0\} \neq \emptyset$, si può scegliere $x_1 \in X - \{x_0\}$. Analogamente, poiché $X - \{x_0, x_1\} \neq \emptyset$, si può scegliere $x_2 \in X - \{x_0, x_1\}$. Procedendo in questo modo si ottiene il sottoinsieme numerabile $Y = \{x_0, x_1, x_2, \ \ldots\ , x_k, \ \ldots\ \} \subseteq X$.

(**2**). Segue subito da (**1**) e dal **Teor. 1**. Sia infatti $|X| = |\boldsymbol{N}|$ ed $Y \subseteq X$. Ovviamente $|Y| \leq |X|$. Se Y non è finito, da (**1**) segue che $|Y| \geq |\boldsymbol{N}|$. Per antisimmetria, da $|X| = |\boldsymbol{N}| \leq |Y| \leq |X|$, segue che $|Y| = |X| = |\boldsymbol{N}|$.

L'ultima affermazione discende immediatamente da (**1**).

Nota. La (**2**) può essere dimostrata anche senza ricorrere al **Teor. 1**, ma semplicemente come conseguenza di **Osserv. 1**(*ii*). Sia infatti $X = \{x_0, x_1, x_2, \ ... \ \}$ e sia $Y \subseteq X$. Se Y non è finito, allora Y è una sottosuccessione $\{x_{n_0}, x_{n_1}, x_{n_2}, \ ... \ \}$ di X (formata da elementi tutti distinti). Dunque Y è un insieme numerabile.

Chiarito quindi che $|\boldsymbol{N}|$ è la minima cardinalità infinita, per cominciare ad affrontare il problema (***B***) dobbiamo far luce sulle proprietà del numerabile, dimostrando il seguente importante teorema.

Terema 2. (*Teorema Fondamentale del Numerabile*). *Sia* $\{X_n\}_{n\geq 0}$ *una famiglia numerabile di insiemi numerabili. L'insieme* $X = \bigcup_{n\geq 0} X_n$ *è numerabile.*

Dim. (***a***) Facciamo (provvisoriamente) l'ulteriore ipotesi che gli insiemi X_n siano a due a due disgiunti. Posto, $\forall\, n \geq 0$:

$$X_n = \{x_{n,0}, x_{n,1}, x_{n,2}, \ ... \ , x_{n,k}, \ ...\},$$

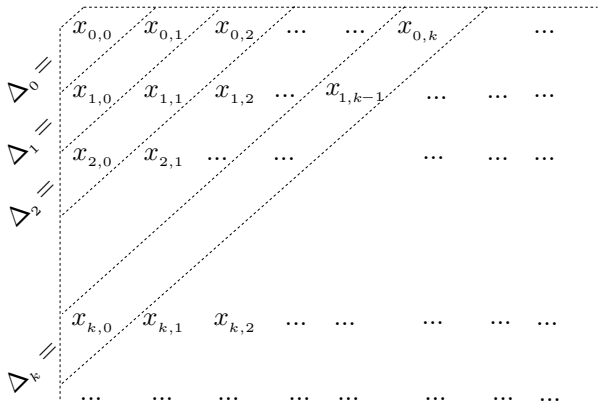
allora

$$X = \{x_{n,k}, \ \forall\, n \geq 0, \ \forall\, k \geq 0\}.$$

Per ogni $k \geq 0$, si ponga

$$\Delta_k := \{x_{k,0}, x_{k-1,1}, \ ... \ , x_{1,k-1}, x_{0,k}\}.$$

Tale insieme, detto *k-sima diagonale di Cantor di* X, è formato da $k+1$ elementi di X. Ovviamente $\{\Delta_k\}_{k\geq 0}$ è una partizione di X. La ragione del nome "*k-sima diagonale*" attribuito a Δ_k è evidente dalla seguente scrittura di X.



Possiamo ora ordinare X in questo modo:

- ogni Δ_k viene ordinato rispetto al "secondo indice crescente" [cioè verso l'alto nel precedente disegno].
- gli elementi di Δ_k precedono quelli di Δ_{k+1}, $\forall\, k \geq 0$.

Dunque X è la seguente successione

$$\{\underbrace{x_{0,0}}, \underbrace{x_{1,0}, x_{0,1}}, \underbrace{x_{2,0}, x_{1,1}, x_{0,2}}, \ .... \ , \underbrace{x_{k,0}, \ ... ... \ , x_{0,k}}, \ ..... \ \}.$$

Ne segue che X è numerabile. Il procedimento di ordinamento sopra illustrato è noto come *ordinamento diagonale di Cantor*.

(***b***) Lasciamo ora cadere l'ipotesi che gli insiemi X_n siano a due a due disgiunti. Poniamo:

$Y_0 := X_0$ [insieme numerabile];
$Y_1 := X_1 - X_0$ [insieme finito o numerabile];
$Y_2 := X_2 - (X_0 \cup X_1)$ [insieme finito o numerabile];
...
$Y_k := X_k - (X_0 \cup \ ... \ \cup X_{k-1})$ [insieme finito o numerabile];
...

Allora $X = \bigcup_{k\geq 0} Y_k$ e gli Y_k sono a due a due disgiunti. Se qualche Y_k è finito, lo possiamo includere in un insieme numerabile $\tilde{Y}_k$ ottenuto aggiungendo a Y_k un'infinità numerabile di *indeterminate* $z_{k,t}$, $\forall t > |Y_k|$, e tali indeterminate sono a due a due distinte (in quanto hanno indici diversi). Allora $X \subseteq \bigcup_{k\geq 0} \tilde{Y}_k$ e, in base ad $(\boldsymbol{a})$, $\big|\bigcup_{k\geq 0} \tilde{Y}_k\big| = |\boldsymbol{N}|$. Dalla **Prop. 1(2)**, X è finito o numerabile. Ma X non è finito (in quanto contiene $Y_0 = X_0$). Dunque X è numerabile.

Corollario 1. *L'unione X di un numero finito o di un'infinità numerabile di insiemi X_k finiti o numerabili è un insieme finito o numerabile.*

Dim. L'ordinamento diagonale di Cantor può essere applicato anche nel caso in cui sia assegnato un numero finito di insiemi (finiti o numerabili) e ci permette di concludere che X è un sottoinsieme di un insieme numerabile: dnque è un insieme finito o numerabile.

Osservazione 4. (*i*) $\boldsymbol{Z}$ è numerabile. Infatti $\boldsymbol{Z} = \boldsymbol{N} \cup (-\boldsymbol{N})$, cioè $\boldsymbol{Z}$ è unione di due insiemi numerabili.

(*ii*) $\boldsymbol{Q}$ è numerabile. Infatti, per ogni $n \geq 1$, si ponga $\boldsymbol{Q}_n := \big\{\frac{a}{n},\ \forall\, a \in \boldsymbol{Z}\big\}$. Certo $\boldsymbol{Q}_n$ è numerabile [infatti è in corrispondenza biunivoca con $\boldsymbol{Z}$]. Inoltre $\boldsymbol{Q} = \bigcup_{n\geq 1} \boldsymbol{Q}_n$ [si osservi che ogni razionale può essere scritto con denominatore positivo]. Si conclude che $\boldsymbol{Q}$ è numerabile.

(*iii*) Siano X, Y due insiemi numerabili. Dal **Cor. 1**, anche $X \sqcup Y$ è numerabile [infatti $X \sqcup Y = (X\times\{1\}) \cup (Y\times\{2\})$ e $X\times\{1\} \sim X$, $Y\times\{2\} \sim Y$ (entrambi numerabili)].

Anche $X\times Y$ è numerabile [infatti $X\times Y = \bigcup_{y\in Y} X\times\{y\}$ e $X\times\{y\} \sim X$].

Ne segue, applicando tali considerazioni a $X = Y = \boldsymbol{N}$, che

$$|\boldsymbol{N}|+|\boldsymbol{N}| = |\boldsymbol{N}|, \quad |\boldsymbol{N}|\cdot|\boldsymbol{N}| = |\boldsymbol{N}|.$$

Dimostreremo ora una classica caratterizzazione degli insiemi infiniti, dovuta a Dedekind. Premettiamo un lemma (anch'esso di Dedekind), utile anche per altri risultati.

Lemma 1. *Se X è un insieme infinito ed Y è un insieme finito o numerabile, risulta: $X \cup Y \sim X$. Ne segue subito che, se α è un numero cardinale infinito e β è un numero cardinale finito o numerabile, risulta: $\alpha + \beta = \alpha$.*

Dim. Affermiamo che non è restrittivo supporre che X ed Y siano disgiunti. Se infatti fosse $X \cap Y \neq \emptyset$, potremmo sostituire Y con $Y_1 := Y - X$; risulterebbe in tal caso:

$$Y_1 \text{ è finito o numerabile, } X \cap Y_1 = \emptyset \text{ e } X \cup Y_1 = X \cup Y.$$

Assumiamo quindi direttamente che sia $X \cap Y = \emptyset$.

Poiché X è infinito, X contiene un sottoinsieme numerabile X_1. In base al **Cor. 1**, $X_1 \cup Y$ è numerabile e dunque esiste una biiezione $f : X_1 \cup Y \to X_1$. Definiamo l'applicazione

$$g : X \cup Y \to X \text{ tale che } g(x) = \begin{cases} x, & \text{se } x \in X - X_1 \\ f(x), & \text{se } x \in X_1 \cup Y. \end{cases}$$

Si noti che g è ottenuta "incollando" f con l'identità $\mathbf{1}_{X-X_1}$. Poichè tali applicazioni sono biiettive e definite su insiemi disgiunti, anche g è biiettiva. Ne segue che $X \cup Y \sim X$ (tramite g).

Teorema 3. (*Dedekind*). *Un insieme è infinito $\iff$ è in corrispondenza biunivoca con un suo sottoinsieme proprio.*

Dim. ($\Longrightarrow$). Essendo X infinito, X contiene un sottoinsieme numerabile X_1. Due casi sono possibili:

$$(*)\ X - X_1 \text{ è finito;} \qquad (**)\ X - X_1 \text{ è infinito.}$$

Nel caso (∗), allora $X = (X - X_1) \cup X_1$ è numerabile (dal **Cor. 1**). Dunque esiste una biiezione $f : X \to \boldsymbol{N}$. Indicato con $\boldsymbol{P}$ l'insieme dei naturali pari, l'insieme $Y := f^{-1}(\boldsymbol{P})$ è un sottoinsieme proprio di X e l'applicazione $f_{\big|_{Y,su}} : Y \to \boldsymbol{P}$ [restrizione di f ad Y, suriettivizzata] è ovviamente biiettiva. Si consideri poi l'applicazione

$$g : \boldsymbol{P} \to \boldsymbol{N} \text{ tale che } g(2n) = n, \ \forall\, 2n \in \boldsymbol{P}.$$

Ovviamente g è biiettiva e quindi è anche biiettiva la composizione

$$f^{-1} \circ g \circ f_{\big|_{Y,su}} : Y \to \boldsymbol{P} \to \boldsymbol{N} \to X.$$

Pertanto X è in corrispondenza biunivoca con il suo sottoinsieme proprio Y.

Nel caso (∗∗), risulta, in base al **Lemma 1**, che $(X - X_1) \cup X_1 \sim X - X_1$. Dunque esiste una biiezione $f : X - X_1 \to (X - X_1) \cup X_1 = X$. Si conclude che X è in corrispondenza biunivoca con il suo sottoinsieme proprio $X - X_1$.

($\Longleftarrow$). Sia X in corrispondenza biunivoca con un suo sottoinsieme proprio Y e sia $f : X \to Y$ una biiezione. L'applicazione

$$i \circ f : X \to Y \hookrightarrow X$$

è ovviamente iniettiva. Se per assurdo X fosse finito, in base a **Prop. 2.4**(*iii*), $i \circ f$ sarebbe anche suriettiva. Per ogni $x \in X$ esisterebbe $x_1 \in X$ tale che $i \circ f(x_1) = x$. Ne seguirebbe che $x = i\big(f(x_1)\big) = f(x_1) \in Y$. Pertanto $X \subseteq Y$, mentre $Y \subset X$: assurdo. Si conclude che X è infinito.

Il seguente teorema, dovuto a Cantor, risponde alla prima domanda del problema (***B***).

Teorema 4. (*Cantor*). *Per ogni insieme X risulta:* $|X| < |\boldsymbol{\mathcal{P}}(X)|$.

Dim. Sia $i : X \to \boldsymbol{\mathcal{P}}(X)$ l'applicazione così definita: $i(x) = \{x\}, \ \forall\, x \in X$. Poiché i è iniettiva, $|X| \leq |\boldsymbol{\mathcal{P}}(X)|$.

Per assurdo sia $|X| = |\boldsymbol{\mathcal{P}}(X)|$. In tal caso esiste una biiezione $f : X \to \boldsymbol{\mathcal{P}}(X)$. [Si noti che, $\forall\, x \in X$, $f(x)$ è un sottoinsieme di X]. Definiamo il seguente sottoinsieme di X:

$$X_f := \{x \in X \ : \ x \notin f(x)\}.$$

In base alla suriettività di f, risulta: $X_f = f(y), \ \exists\, y \in X$. Ci sono due possibilità per y: $y \in X_f$ oppure $y \notin X_f$.

Se $y \in X_f$, allora $y \notin f(y)$, cioè $y \notin X_f$: assurdo. Se $y \notin X_f$, allora $y \in f(y)$, cioè $y \in X_f$: assurdo.

In ogni caso si è pervenuti ad un assurdo. Si conclude che $|X| \neq |\boldsymbol{\mathcal{P}}(X)|$ e dunque che $|X| < |\boldsymbol{\mathcal{P}}(X)|$.

Teorema 5. (*Cantor*). *Risulta:* $|\boldsymbol{R}| = |\boldsymbol{\mathcal{P}}(\boldsymbol{N})|$.

Dal **Teor. 4** segue allora che $|\boldsymbol{N}| < |\boldsymbol{R}|$. La cardinalità di $\boldsymbol{R}$ è detta *cardinalità del continuo*, spesso denotata $\aleph$ ["alef"]. Dunque $|\boldsymbol{R}| = Card(\boldsymbol{R}) = \aleph$.

La dimostrazione del **Teor. 5** verrà suddivisa in tre passi successivi:

(**1**) $\boldsymbol{R} \sim [0, 1)$,

(**2**) $[0, 1) \sim \boldsymbol{2^N}$,

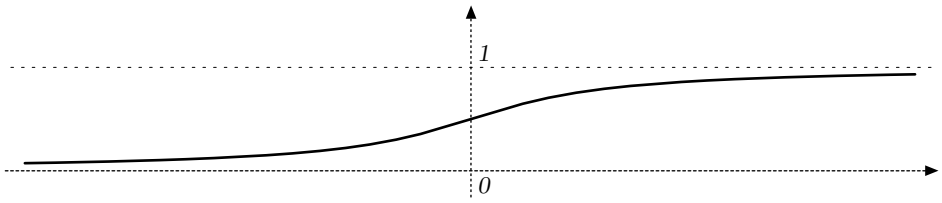
(**3**) $\boldsymbol{2^N} \sim \boldsymbol{\mathcal{P}}(\boldsymbol{N})$,

dove $[0, 1) = \{x \in \boldsymbol{R} \ : \ 0 \leq x < 1\}$ è un intervallo chiuso-aperto di $\boldsymbol{R}$ e $\boldsymbol{2^N} = \big\{f : \boldsymbol{N} \to \{0, 1\}\big\}$ è l'insieme di tutte le successioni formate dai soli 0 ed 1.

Da (**1**), (**2**), (**3**) per transitività segue subito che $\boldsymbol{R} \sim \boldsymbol{\mathcal{P}}(\boldsymbol{N})$.

Dim. (1). Si osserva subito che $\boldsymbol{R} \sim (0, 1) = \{x \in \boldsymbol{R} \ : \ 0 < x < 1\}$.

Infatti una biiezione $f : \boldsymbol{R} \to (0,1)$ è ad esempio ottenibile dal grafico di una funzione continua crescente $y = f(x),\ \forall\, x \in \boldsymbol{R}$, avente asintoti orizzontali nelle rette $y = 0$ ed $y = 1$ [ad esempio la funzione $f(x) = \frac{1}{2} + \frac{1}{\pi}\, arctg(x),\ \forall\, x \in \boldsymbol{R}$].



Per concludere basta quindi costruire una biiezione $g : [0,1) \to (0,1)$.

Sia $\mathbf{S} = \{\frac{1}{n},\ \forall\, n \geq 2\}$. Poiché $\mathbf{S}$ è numerabile, anche $\mathbf{S} \cup \{0\}$ è numerabile: dunque esiste una biiezione $\gamma : \mathbf{S} \cup \{0\} \to \mathbf{S}$ [ad esempio $\gamma(0) = \frac{1}{2},\ \gamma(\frac{1}{k}) = \frac{1}{k+1},\ \forall\, k \geq 2$]. Si definisce allora

$$g : [0,1) \to (0,1) \ \text{ tale che } \ g(x) = \begin{cases} x, & \text{se } x \in [0,1) - \big(\mathbf{S} \cup \{0\}\big), \\ \gamma(x), & \text{se } x \in \mathbf{S} \cup \{0\}. \end{cases}$$

Per costruzione, g è una biiezione tra $[0,1)$ e $(0,1)$. Si conclude che $f^{-1} \circ g : [0,1) \to \boldsymbol{R}$ è una biiezione.

Dim. (2). Verificheremo alla fine di **Cap. II.2** che:

ogni numero reale $x \in [0,1)$ *si può scrivere in modo unico in base* 2, *cioè nella forma*

$$x = 0 + \tfrac{a_1}{2} + + \tfrac{a_2}{2^2} + \tfrac{a_3}{2^3} + \ \ldots\ + \tfrac{a_k}{2^k} + \ \ldots .\ ,$$

dove $\{a_1,\, a_2,\, a_3,\, \ldots\, ,\, a_k\, ,\, \ldots\, \}$ *è una successione di* 0, 1, *non definitivamente* $= 1$.

Scriveremo in tal caso $x = 0, (a_1,\, a_2,\, \ldots\, ,\, a_k\, ,\, \ldots\,)_2$.

Indichiamo con $(\mathbf{2^N})^*$ l'insieme di tutte le successioni di 0, 1, non definitivamente $= 1$ e poniamo $Y := \mathbf{2^N} - (\mathbf{2^N})^*$. Ovviamente Y è l'insieme di tutte le successioni di 0, 1, definitivamente $= 1$. Y è un insieme numerabile [infatti, $\forall\, k \geq 0$, è finito l'insieme delle successioni di $\mathbf{2^N}$ aventi tutti 1 a partire dal k-simo elemento della successione: dunque Y è unione di un'infinità numerabile di insiemi finiti]. Da quanto sopra affermato, $[0,1) \sim (\mathbf{2^N})^*$, tramite la biiezione

$$x \in [0,1) \longrightarrow \{a_1,\, a_2,\, a_3,\, \ldots\, ,\, a_k\, ,\, \ldots\, \} \in (\mathbf{2^N})^* .$$

Inoltre, in base al **Lemma 1**, $\mathbf{2^N} = (\mathbf{2^N})^* \cup Y \sim (\mathbf{2^N})^*$. Dunque $[0,1) \sim \mathbf{2^N}$.

Dim. (3). Dimostremo un risultato più generale:

per ogni insieme X, *risulta:* $\mathbf{2}^X \sim \boldsymbol{\mathcal{P}}(X)$.

Per ogni sottoinsieme $Y \subseteq X$, sia χ_Y la funzione caratteristica di Y in X [cfr. **Osserv. 2.3**(v)]. Ovviamente $\chi_Y \in \mathbf{2}^X$. Dunque è definita l'applicazione

$$\chi : \boldsymbol{\mathcal{P}}(X) \to \mathbf{2}^X \ \text{ tale che } \ \chi(Y) = \chi_Y\, , \ \forall\, Y \in \boldsymbol{\mathcal{P}}(X).$$

Per ogni $f \in \mathbf{2}^X$, $f^{-1}(1) = \{x \in X \ :\ f(x) = 1\} \in \boldsymbol{\mathcal{P}}(X)$. Dunque è definita l'applicazione

$$\psi : \mathbf{2}^X \to \boldsymbol{\mathcal{P}}(X) \ \text{ tale che } \ \psi(f) = f^{-1}(1),\ \forall\, f \in \mathbf{2}^X .$$

Si constata facilmente che le due applicazioni sono inverse l'una dell'altra. Dunque $\mathbf{2}^X \sim \boldsymbol{\mathcal{P}}(X)$.

Corollario 2. (*Cantor*). *Risulta:* $\boldsymbol{R}^n \sim \boldsymbol{R}$, $\forall\, n \geq 1$. *Ne segue in particolare che* $\boldsymbol{C} \sim \boldsymbol{R}$.

Dim. Nella dimostrazione useremo due semplici fatti:

$(*)$ $A_1 \sim A_2,\ B_1 \sim B_2 \implies A_1 \times B_1 \sim A_2 \times B_2$ [già notato in **Osserv. 3**(i)];

$(**)$ $X \sim Y \implies \boldsymbol{\mathcal{P}}(X) \sim \boldsymbol{\mathcal{P}}(Y)$ [se infatti $f : X \to Y$ è una biiezione, è una biiezione anche l'applicazione $F : \boldsymbol{\mathcal{P}}(X) \to \boldsymbol{\mathcal{P}}(Y)$ tale che $F(X_1) = f(X_1),\ \forall\, X_1 \in \boldsymbol{\mathcal{P}}(X)$].

Da $(*)$ segue che è sufficiente verificare che $\boldsymbol{R} \sim \boldsymbol{R}^2$ [perché allora $\boldsymbol{R} \sim \boldsymbol{R}^2 \sim \boldsymbol{R}^3 \sim \ \ldots\ \sim \boldsymbol{R}^n$]. Dalla dimostrazione del **Teor. 5** e da $(*)$ segue che $\boldsymbol{R}^2 = \boldsymbol{R} \times \boldsymbol{R} \sim \mathbf{2^N} \times \mathbf{2^N}$. Se verifichiamo che

$(\bullet)$ $\qquad\qquad \mathbf{2^N} \times \mathbf{2^N} \ \sim \mathbf{2^{N \sqcup N}}$

e teniamo conto del fatto che $\boldsymbol{\mathcal{P}(N \sqcup N) \sim \mathcal{P}(N)}$ [ciò segue da (**) e dal fatto che $\boldsymbol{N \sqcup N \sim N}$], allora possiamo concludere che

$$\boldsymbol{R^2 \sim 2^N \times 2^N \sim 2^{N \sqcup N} \sim \mathcal{P}(N \sqcup N) \sim \mathcal{P}(N) \sim R}.$$

Resta da verificare (•).

Ricordato che $\boldsymbol{N \sqcup N = (N \times \{1\}) \cup (N \times \{2\})}$, ad ogni $\boldsymbol{f \in 2^{N \sqcup N}}$ restano associate le due applicazioni

$$\boldsymbol{f_1 : N \to \{0,1\}} \text{ tale che } \boldsymbol{f_1(n) = f(n,1)}, \quad \boldsymbol{f_2 : N \to \{0,1\}} \text{ tale che } \boldsymbol{f_2(n) = f(n,2)}.$$

[f_1, f_2 sono identificabili rispettivamente con le restrizioni $\boldsymbol{f\big|_{N \times \{1\}}}$ e $\boldsymbol{f\big|_{N \times \{2\}}}$]. Resta quindi definita l'applicazione

$$\boldsymbol{\Phi : 2^{N \sqcup N} \to 2^N \times 2^N} \text{ tale che } \boldsymbol{\Phi(f) = (f_1, f_2)}, \ \ \boldsymbol{\forall\, f \in 2^{N \sqcup N}}.$$

Si verifica facilmente che Φ ammette la seguente inversa:

$$\boldsymbol{\Psi : 2^N \times 2^N \to 2^{N \sqcup N}} \text{ tale che } \boldsymbol{\Psi(f,g) = F}, \text{ con } \begin{cases} \boldsymbol{F(n,1) = f(n)} \\ \boldsymbol{F(n,2) = g(n)}, \end{cases} \quad \boldsymbol{\forall\, n \in N}.$$

In tal modo l'affermazione (•) è verificata.

Osservazione 5. Chiarito che $\boldsymbol{|N| < |R| = 2^{|N|}}$, si pone "naturalmente" la seguente questione:

ci sono cardinalità intermedie tra $\boldsymbol{|N|}$ *ed* $\boldsymbol{|R|}$ *?*

A tale questione fu subito ipotizzata (dallo stesso Cantor) una risposta negativa, nota come *ipotesi del continuo* o *congettura di Cantor* o *I problema di Hilbert* (1900). L'ipotesi del continuo è stata poi formulata in questa forma più generale (detta *ipotesi generalizzata del continuo*):

assegnato un numero cardinale α*, non esiste alcun numero cardinale* β *tale che* $\alpha < \beta < 2^{\alpha}$.

Nel 1938 K. Godel ha dimostrato che l'ipotesi del continuo (anche nella sua forma generalizzata) è *consistente* con gli assiomi della teoria degli insiemi [cioè non porta a contraddizioni]. Nel 1963 P.Cohen ha poi dimostrato che l'ipotesi del continuo è *indipendente* dagli assiomi della teoria degli insiemi: ciò significa che anche ritenere possibile l'esistenza di cardinalità intermedie non porta a contraddizioni.

Oggi l'ipotesi del continuo è comunemente accettata tra gli assiomi della teoria degli insiemi.

Osservazione 6. Il **Teorema 4** comporta che non esista in $\boldsymbol{\mathcal{C}ard}$ una cardinalità massima, mentre ovviamente 0 è la cardinalità minima.

Nel 1904 E. Zermelo ha dimostrato che $(\boldsymbol{\mathcal{C}ard}, \leq)$ è bene ordinato (cfr. **Def. 3.6**). Poiché ogni insieme bene ordinato è totalmente ordinato, otteniamo che anche le risposte alle domande del nostro problema $(\boldsymbol{C})$ sono affermative.

Osservazione 7. Accettare $\boldsymbol{\mathcal{C}ard}$ come un insieme, così come accettare come insieme l'*insieme di tutti gli insiemi* porta ad un'immediata contraddizione, nota come *Paradosso di Cantor* (1899).

Infatti, se indichiamo con $\mathbf{U}$ l'insieme di tutti gli insiemi, allora $Card(\mathbf{U}) < Card(\mathcal{P}(\mathbf{U}))$ (in base al **Teor. 4**). Ma $\mathcal{P}(\mathbf{U})$ è formato da insiemi e dunque $\mathcal{P}(\mathbf{U}) \subseteq \mathbf{U}$. Ne segue che $Card(\mathcal{P}(\mathbf{U})) \leq Card(\mathbf{U})$. Le due diseguaglianze sono contraddittorie.

Ciononostante, in questi apppunti abbiamo "sfidato il paradosso", utilizzando l'espressione $\boldsymbol{\mathcal{C}ard}$ per denotare la "famiglia di tutte le cardinalità". Lo abbiamo fatto per evidenti ragioni di semplicità e di comodità di linguaggio.

Allo studente interessato ad una panoramica introduttiva sulle teorie assiomatiche della *teoria degli insiemi* consigliamo la lettura dell'appendice **A.2** del testo di Fontana-Gabelli, citato in bibliografia.

7. Esercizi del Capitolo I

1.1. Si assumano note le tavole di verità della negazione $(\neg)$ di una proposizione, dell'unione $(\vee)$, dell'intersezione $(\wedge)$ e dell'implicazione $(\Longrightarrow)$ di due proposizioni.

(*i*) Assegnate due proposizioni $\mathcal{P}$, $\mathcal{Q}$, verificare che le due proposizioni

$$\neg(\mathcal{P} \vee \mathcal{Q}) \ \text{ e } \ (\neg\mathcal{P}) \wedge (\neg\mathcal{Q})$$

sono logicamente equivalenti, cioè hanno la stessa tavola di verità.

(*ii*) Assegnate tre proposizioni $\mathcal{P}$, $\mathcal{Q}$, $\mathcal{R}$ verificare che sono logicamente equivalenti le due proposizioni

$$\mathcal{P} \wedge (\mathcal{Q} \vee \mathcal{R}) \ \text{ e } \ (\mathcal{P} \wedge \mathcal{Q}) \vee (\mathcal{P} \wedge \mathcal{R}).$$

(*iii*) Assegnate due proposizioni $\mathcal{P}$, $\mathcal{Q}$, verificare che sono logicamente equivalenti le due proposizioni

$$\mathcal{P} \not\Longrightarrow \mathcal{Q} \ \text{ e } \ \mathcal{P} \wedge \neg\mathcal{Q}.$$

* * * * * * * * *

1.2. Sono assegnati tre insiemi A, B, C.

(*i*) Verificare che $A - (B - C) = (A - B) \cup (A \cap C)$.

(*ii*) Verificare che $(A - B) - C = A - (B \cup C)$.

(*iii*) Verificare che $(A - B) - C \subseteq A - (B - C)$ e che tale inclusione può essere propria.

* * * * * * * * *

1.3. Sono assegnati tre insiemi A, B, C.

(*i*) Verificare che $(A \cup B) - C = (A - C) \cup (B - C)$ e che $(A \cap B) - C = (A - C) \cap (B - C)$.

(*ii*) Verificare che $A \cap (B - C) = (A \cap B) \cap (A - C)$.

(*iii*) Determinare un insieme T tale che $A \cup (B - C) = (A \cup B) \cap T$.

* * * * * * * * *

1.4. Sia $f : \boldsymbol{Z} \to \boldsymbol{Z}$ l'applicazione così definita: $f(x) = x^2 + 1, \ \ \forall\, x \in \boldsymbol{Z}$.

(*i*) Verificare che f non è né iniettiva né suriettiva.

(*ii*) Determinare un sottoinsieme $A \subseteq \boldsymbol{Z}$ tale che la restrizione $f_{|_A}$ sia iniettiva. Si scelga A *massimale* rispetto a questa proprietà.

(*iii*) Posto $\boldsymbol{P} = 2\boldsymbol{N} = \{0, 2, 4, \dots\}$ (naturali pari) e $\boldsymbol{D} = \boldsymbol{N} - 2\boldsymbol{N} = \{1, 3, 5, \dots\}$ (naturali dispari), calcolare $f^{-1}(\boldsymbol{P})$ e $f^{-1}(\boldsymbol{D})$.

(*iv*) Determinare gli insiemi $f^{-1}(f(\boldsymbol{N}))$, $f^{-1}(f(\boldsymbol{P}))$ e $f^{-1}(f(\boldsymbol{D}))$.

* * * * * * * * *

1.5. Sia $f : \boldsymbol{Z} \to \boldsymbol{Z}$ la seguente applicazione:

$$f(n) = \begin{cases} n+1, \ \text{se} \ \ n \ \ \text{è dispari} \\ n-1, \ \text{se} \ \ n \ \ \text{è pari,} \end{cases} \qquad \forall\, n \in \boldsymbol{Z}.$$

(*i*) Verificare che f è iniettiva.

(*ii*) Verificare che f è suriettiva.

(*iii*) Determinare un'espressione di f^{-1}.

* * * * * * * * *

1.6. Assegnate le applicazioni $f : A \to B$, $g : B \to C$, è definita la loro composizione $g \circ f : A \to C$.

(*i*) Verificare che se $g \circ f$ è iniettiva, anche f è iniettiva.

(*ii*) Verificare che se $g \circ f$ è suriettiva, anche g è suriettiva.

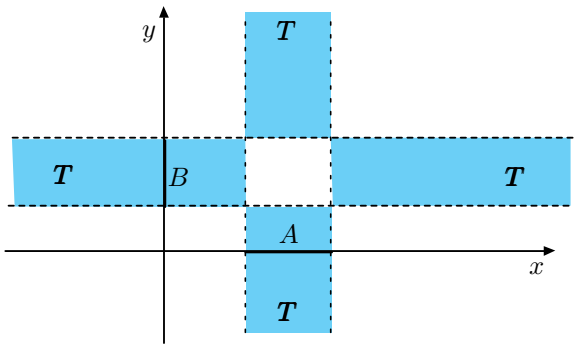
(*iii*) Verificare che se $g \circ f$ è iniettiva ed f è suriettiva, anche g è iniettiva.

(*iv*) Verificare che se $g \circ f$ è suriettiva e g è iniettiva, anche f è suriettiva.

(*v*) Nell'ipotesi che $|A| = |C| = 2$, $|B| = 3$, determinare esempi di applicazioni f, g tali che $g \circ f$ sia biiettiva, ma g non sia iniettiva e f non sia suriettiva.

* * * * * * * * *

1.7. Siano A, B intervalli limitati, scelti rispettivamente sull'*asse* x e sull'*asse* y di un riferimento cartesiano del piano $\boldsymbol{R}^2$. Sia $\boldsymbol{T}$ l'insieme formato dall'unione delle quattro "semistrisce" evidenziate in figura e sia $\boldsymbol{S}$ l'insieme $(A\times B)\cup\big(\mathbf{C}_{\boldsymbol{R}}(A)\times\mathbf{C}_{\boldsymbol{R}}(B)\big)$.



(*i*) Esprimere $\boldsymbol{T}$, in funzione di A, B, come unione di due prodotti cartesiani.

(*ii*) Esprimere $\boldsymbol{S}$, in funzione di A, B, come intersezione di due insiemi $\boldsymbol{S}_1$, $\boldsymbol{S}_2$.

* * * * * * * * *

1.8. Sia $f:\boldsymbol{R}\to\boldsymbol{R}$ l'applicazione così definita:

$$f(x)=[x],\ \forall\, x\in\boldsymbol{R}\quad [\text{dove } [x] \text{ denota la } \textit{parte intera di } x, \text{ cioè il massimo intero } \le x].$$

Posto $A=2\boldsymbol{N}=\{0,\,2,\,4,\,6,\,8,\,\dots\}$, individuare gli insiemi $f^{-1}\big(f(A)\big)$ e $f\big(f^{-1}(A)\big)$.

* * * * * * * * *

1.9. Sono assegnati in $\boldsymbol{R}$ gli intervalli $[0,1)$ e $(-\infty,1]$. Determinare una biiezione tra i due intervalli, utilizzando opportunamente il grafico di un'iperbole di $\boldsymbol{R}^2$.

* * * * * * * * *

1.10. Posto $\boldsymbol{R}^{\cdot}=\boldsymbol{R}-\{0\}$, sia $f:\boldsymbol{R}^{\cdot}\to\boldsymbol{R}$ l'applicazione così definita:

$$f(x)=1-\tfrac{1}{x},\ \forall\, x\in\boldsymbol{R}^{\cdot}.$$

(*i*) Verificare che f è iniettiva e calcolare $Im(f)$.

(*ii*) Posto $X=\boldsymbol{R}-\{0,1\}$, verificare che la restrizione $g:=f_{|X}:X\to X$ è una biiezione.

(*iii*) Verificare che $g^3=\mathbf{1}_X$. Dedurne l'inversa di g.

* * * * * * * * *

1.11. [*Esonero 8/4/03*] Sono assegnate due funzioni f e g, di dominio e codominio $\boldsymbol{Z}$, definite nel modo seguente: $\forall\, x\in\boldsymbol{Z}$,

$$f(x)=2x+3,\quad g(x)=\begin{cases}\frac{x}{2}+1, & \text{se } x \text{ è pari}\\ \frac{x+3}{2}+1, & \text{se } x \text{ è dispari.}\end{cases}$$

(*i*) Verificare se tali funzioni sono iniettive o suriettive.

(*ii*) Calcolare i prodotti operatori $f\circ g$ e $g\circ f$ e verificare se questi sono funzioni iniettive o suriettive.

* * * * * * * * *

1.12. [*Esame 10/6/03*] Sia $f:\boldsymbol{Q}\to\boldsymbol{Q}$ l'applicazione così definita:

$$f(x)=2-\tfrac{x-1}{2},\ \forall\, x\in\boldsymbol{Q}.$$

(*i*) Verificare che f è biunivoca.

(*ii*) Esprimere f come composizione di tre applicazioni biunivoche non identiche $g_i:\boldsymbol{Q}\to\boldsymbol{Q}$, in modo che $f=g_1\circ g_2\circ g_3$.

Calcolare poi f^{-1}, ${g_i}^{-1}$ [con $i=1,2,3$] e verificare che $f^{-1}={g_3}^{-1}\circ{g_2}^{-1}\circ{g_1}^{-1}$.

* * * * * * * * *

1.13. È assegnata la funzione $f:(0,\frac{\pi}{2})\to\boldsymbol{R}$ tale che $f(t)=\sin t\,\cos t,\ \forall\, t\in(0,\frac{\pi}{2})$.
Assumendo noti grafico e proprietà della funzione seno:

(*i*) Calcolare $Im(f)$;

(*ii*) Verificare che f non è iniettiva;

(*iii*) Calcolare l'insieme quoziente A di $(0, \frac{\pi}{2})$ modulo la relazione di equivalenza ρ_f associata ad f e stabilire una biiezione tra l'insieme quoziente A ed un opportuno intervallo della retta.

* * * * * * * * *

1.14. Sia ρ la seguente relazione su $\boldsymbol{R}$:

$$x \,\rho\, y \iff x - y \in \boldsymbol{Z}.$$

(*i*) Verificare che ρ è una relazione di equivalenza su $\boldsymbol{R}$ e che $[x]_\rho = x + \boldsymbol{Z} := \{x+n,\ \forall\, n \in \boldsymbol{Z}\},\ \forall\, x \in \boldsymbol{R}$.

(*ii*) Verificare che $\boldsymbol{R}/_\rho$ è in corrispondenza biunivoca con l'intervallo $[0, 1)$.

* * * * * * * * *

1.15. Sia ρ una relazione di equivalenza su un insieme A e σ una relazione di equivalenza su un insieme B. È definita su $A \times B$ la seguente relazione $\mathfrak{R}$:

$$(a, b)\, \mathfrak{R}\, (a_1, b_1) \iff a \,\rho\, a_1 \ \text{ e } \ b \,\sigma\, b_1.$$

(*i*) Verificare che $\mathfrak{R}$ è una relazione di equivalenza su $A \times B$.

(*ii*) Verificare che l'insieme quoziente $A \times B/_{\mathfrak{R}}$ è in corrispondenza biunivoca con $A/_\rho \times B/_\sigma$.

* * * * * * * * *

1.16. In $\boldsymbol{R}^{2\,*} := \boldsymbol{R}^2 - \{(0, 0)\}$ si introduce la seguente relazione ρ

$$(a, b)\rho(c, d) \iff det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 0.$$

(*i*) Verificare che ρ è una relazione di equivalenza su $\boldsymbol{R}^{2\,*}$. Perché ρ non può essere estesa ad $\boldsymbol{R}^2$?

(*ii*) Verificare che la classe di equivalenza $[(a, b)]_\rho$ è formata dai punti della retta $\mathbf{r}$ per $(0, 0)$ e (a, b) [privata del punto $(0, 0)$].

(*iii*) A quale configurazione geometrica corrisponde l'insieme quoziente $\boldsymbol{R}^{2\,*}/_\rho$?

* * * * * * * * *

1.17. Sia $f : \boldsymbol{Z} \to \boldsymbol{Z}$ l'applicazione così definita:

$$f(x) = x, \text{ se } |x| < 10; \quad f(x) = 10, \text{ se } |x| \geq 10.$$

(*i*) Verificare che f non è inietttiva né suriettiva.

(*ii*) Determinare $f^{-1}(10)$.

(*iii*) Descrivere la relazione ρ_f indicandone le classi di equivalenza.

(*iv*) Verificare che l'insieme quoziente $\boldsymbol{Z}/_{\rho_f}$ è in corrispondenza biunivoca con l'insieme $\{1, 2, \ldots, 20\}$.

* * * * * * * * *

1.18. [*Esame 2/2/04*] È assegnata la funzione $f : \boldsymbol{R}^2 \to \boldsymbol{R}$ tale che

$$f(x, y) = \begin{cases} \sqrt{xy}, \text{ se } xy \geq 0, \\ -\sqrt{-xy}, \text{ se } xy < 0. \end{cases}$$

(*i*) Verificare che f è suriettiva e non iniettiva.

(*ii*) Calcolare la controimmagine $f^{-1}(r),\ \forall\, r \in \boldsymbol{R}$.

(*iii*) Verificare che la relazione di equivalenza ρ_f associata ad f coincide con la seguente relazione ρ di $\boldsymbol{R}^2$: $\forall\, (x, y), (x_1, y_1) \in \boldsymbol{R}^2$,

$$(x, y)\rho(x_1, y_1) \iff xy = x_1 y_1.$$

(*iv*) Determinare una biiezione tra l'insieme quoziente $\boldsymbol{R}^2/_{\rho_f}$ e l'insieme $\Gamma = \{(t, |t|),\ \forall\, t \in \boldsymbol{R}\}$.

* * * * * * * * *

1.19. [*Esonero 8/4/03*] Sull'insieme $A = \boldsymbol{Z} \times \boldsymbol{Z} \times \boldsymbol{Z}^\cdot$ [con $\boldsymbol{Z}^\cdot = \boldsymbol{Z} - \{0\}$] sono definite le relazioni ρ_1, ρ_2, ponendo, $\forall\, (a, b, c), (a_1, b_1, c_1) \in A$:

$$(a, b, c)\, \rho_1\, (a_1, b_1, c_1) \iff abc_1 = a_1 b_1 c; \ \ (a, b, c)\, \rho_2\, (a_1, b_1, c_1) \iff (a + b)c_1 = (a_1 + b_1)c.$$

(*i*) Verificare che ρ_1, ρ_2 sono relazioni di equivalenza su A.

(*ii*) Utilizzando il teorema fondamentale delle applicazioni, verificare che gli insiemi quozienti $A/_{\rho_1}$ ed $A/_{\rho_2}$ sono in corrispondenza biunivoca con l'insieme $\boldsymbol{Q}$ dei razionali.

(*iii*) Descrivere esplicitamente una biiezione $F : A/_{\rho_1} \to A/_{\rho_2}$.

* * * * * * * * *

1.20. Nell'insieme $\boldsymbol{Z}^{\cdot} = \boldsymbol{Z} - \{0\}$ si consideri la partizione $\mathfrak{F}$ formata dai seguenti quattro insiemi:

$\mathbf{P}_+ = \{2, 4, 6, 8, ...\}$ [pari positivi], $\mathbf{P}_- = \{-2, -4, -6, -8, ...\}$ [pari negativi],

$\mathbf{D}_+ = \{1, 3, 5, 7, ...\}$ [dispari positivi], $\mathbf{D}_- = \{-1, -3, -5, -7, ...\}$ [dispari negativi].

Denotata con ρ la relazione di equivalenza su $\boldsymbol{Z}^{\cdot}$ corrispondente ad $\mathfrak{F}$, si descriva ρ e si determini un'applicazione suriettiva $f : \boldsymbol{Z}^{\cdot} \to \{\pm 1, \pm 2\}$ tale che $\rho_f = \rho$.

* * * * * * * * *

1.21. Come è noto, la relazione di divisibilità in $\boldsymbol{Z}$ è così definita:

$$\forall\, a, b \in \boldsymbol{Z},\ a \,\big|\, b \iff b = ah,\ \exists\, h \in \boldsymbol{Z}.$$

Indicheremo sempre con $\big|$ sia la relazione di divisibilità ristretta a $\boldsymbol{N}$ [cioè $a \,\big|\, b \iff b = ah,\ \exists\, h \in \boldsymbol{N}$], che quella ristretta a $\boldsymbol{N}^{\cdot} = \boldsymbol{N} - \{0\}$ [cioè $a \,\big|\, b \iff b = ah,\ \exists\, h \in \boldsymbol{N}^{\cdot}$].

(*i*) Verificare che $(\boldsymbol{Z}, \big|)$, è un insieme *pre-ordinato*, [cioè che la relazione $\big|$ è riflessiva e transitiva], ma non simmetrica né antisimmetrica.

(*ii*) Verificare che $(\boldsymbol{N}, \big|)$ è un insieme ordinato, non totalmente, e che ammette un primo ed un ultimo elemento.

(*iii*) Verificare che $(\boldsymbol{N}^{\cdot}, \big|)$ è un insieme ordinato (non totalmente) e calcolare eventuali massimo, minimo, estremo inferiore ed estremo superiore dei due suoi seguenti sottoinsiemi:

$$2^{\boldsymbol{N}} = \{2^h,\ \forall\, h \in \boldsymbol{N}\}, \quad \boldsymbol{T} = \{2, 3, 6\}.$$

* * * * * * * * *

1.22. Sia $(A, \leq)$ un insieme ordinato.

(*i*) Verificare che, se $(A, \leq)$ è bene ordinato, allora è totalmente ordinato.

(*ii*) Verificare che, se $(A, \leq)$ è un insieme *finito* totalmente ordinato, allora $(A, \leq)$ è bene ordinato.

(*iii*) Indicare un insieme ordinato infinito $(A, \leq)$ che sia totalmente ordinato ma non bene ordinato.

* * * * * * * * *

1.23. Sia $A = \{a, b, c\}$ un insieme con tre elementi distinti e sia $\boldsymbol{\mathcal{P}}(A)$ il suo insieme delle parti.

(*i*) Verificare che $(\boldsymbol{\mathcal{P}}(A), \subseteq)$ è un insieme ordinato, non bene ordinato né totalmente ordinato, dotato di primo ed ultimo elemento.

(*ii*) Determinare i minoranti ed i maggioranti di $\{a\}$.

(*iii*) È vero che $sup(\{S\}) = S,\ \forall\, S \in \boldsymbol{\mathcal{P}}(A)$?

* * * * * * * * *

1.24. Verificare che in un anello unitario $(A, +, \cdot)$ l'unità 1_A è unica.

* * * * * * * * *

1.25. Sia A' un sottoinsieme non vuoto di un anello $(A, +, \cdot)$. Verificare che

$$A' \text{ è un sottoanello di } A \iff A' - A' \subseteq A' \text{ e } A' \cdot A' \subseteq A'.$$

* * * * * * * * *

1.26. Sia $f : A \to B$ un omomorfismo dall'anello $(A, +, \cdot)$ all'anello $(B, +, \cdot)$.

(*i*) Verificare che $f(0_A) = 0_B$.

(*ii*) Verificare che $f(-a) = -f(a),\ \forall\, a \in A$.

(*iii*) Verificare che $f(A)$ è un sottoanello di B.

* * * * * * * * *

1.27. Siano $(A, +, \cdot)$ e $(B, +, \cdot)$ due anelli unitari; sia $f : A \to B$ un omomorfismo di anelli.

(*i*) Verificare che nei due seguenti esempi **non** è verificata la condizione $f(1_A) = 1_B$ [si dirà che tali omomorfismi *non sono unitari*]:

(*a*) $0 : A \to B$ tale che $0(a) = 0_B,\ \forall\, a \in A$.

(*b*) $f : \boldsymbol{R} \to \mathfrak{M}_2(\boldsymbol{R})$ tale che $f(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, $\forall\, a \in \boldsymbol{R}$.

(*ii*) Verificare che, se f è suriettivo, f è un omomorfismo unitario, cioè $f(1_A) = 1_B$.

(*iii*) Verificare che, se $f \neq 0$ e B è un anello integro, f è un omomorfismo unitario, cioè $f(1_A) = 1_B$.

* * * * * * * * *

1.28. Sia $f : A \to B$ un omomorfismo di anelli unitari.

(*i*) Verificare che se f è unitario risulta $f\big(\mathcal{U}(A)\big) \subseteq \mathcal{U}(B)$ [dove $\mathcal{U}(A)$ e $\mathcal{U}(B)$ denotano rispettivamente i gruppi degli elementi invertibili di A e B].

(*ii*) La precedente inclusione può essere stretta?

(*iii*) Se f non è unitario, l'inclusione di (*i*) è sempre vera?

* * * * * * * * *

1.29. Assegnato un insieme non vuoto X e indicate con $\Delta, \cap$ rispettivamente la differenza simmetrica e l'intersezione di sottoinsiemi di X, verificare che la terna $(\boldsymbol{\mathcal{P}}(X), \Delta, \cap)$ è un anello commutativo, unitario e non integro (se $|X| \geq 2$). Tale anello è noto come l'*algebra di Boole di* X.

* * * * * * * * *

1.30. Utilizzando il seguente fatto: $\nexists\, k \in \boldsymbol{N}$ tale che $0 < k < 1$, dimostrare la validità della *proprietà archimedea* in $\boldsymbol{N}$:

$$\forall\, m,\, n \in \boldsymbol{N},\ n \neq 0,\ \exists\, p \in \boldsymbol{N} \text{ tale che } m < np.$$

* * * * * * * * *

1.31. [*Esonero 8/4/03*] Utilizzando il principio di induzione si dimostri che, per ogni numero naturale positivo n, risulta:

$$1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1) = \tfrac{(2n)!}{2^n \cdot n!}.$$

* * * * * * * * *

1.32. Per ogni intero $n \geq 1$, denotiamo con $\mathfrak{P}_n$ un insieme di n rette del piano in "posizione generica" [cioè non parallele tra loro e non incidenti a tre a tre]. Dimostrare per induzione su $n \geq 1$ che $\mathfrak{P}_n$ ripartisce il piano in $1 + \binom{n+1}{2}$ regioni disgiunte.

* * * * * * * * *

1.33. Siano x, y numeri reali. Dimostrare che, $\forall\, n \geq 0$, vale la seguente formula:

$$\sum_{k=0}^{n} (x + ky) = \tfrac{1}{2}(n+1)(2x + ny).$$

* * * * * * * * *

1.34. Si consideri la *successione di Fibonacci* F [che è definita "ricorsivamente" in questo modo:

$$F(0) = 0,\ F(1) = 1,\ F(k) = F(k-2) + F(k-1),\ \forall\, k \geq 2].$$

Fissati due numeri reali x, y, si definisca ricorsivamente la seguente successione $\boldsymbol{a}$:

$$\boldsymbol{a}(0) = x,\ \boldsymbol{a}(1) = y,\ \boldsymbol{a}(k) = \boldsymbol{a}(k-2) \cdot \boldsymbol{a}(k-1),\ \forall\, k \geq 2].$$

Verificare, per induzione *forte* su n, che

$$\boldsymbol{a}(n) = x^{F(n-1)}\, y^{F(n)},\ \forall\, n \geq 1.$$

* * * * * * * * *

1.35. Sono assegnate in forma ricorsiva le seguenti successioni $\{a_n\}$ e $\{b_n\}$:

$$a_1 = 1,\ a_n = n + a_{n-1},\ \ \forall\, n \geq 2; \qquad b_1 = 1,\ b_n = n \cdot b_{n-1},\ \ \forall\, n \geq 2.$$

Determinare *formule chiuse* di tali successioni [cioè formule che permettano di calcolare il termine n-simo senza aver calcolato i precedenti].

* * * * * * * * *

1.36. [*Esonero 8/4/03*] È assegnato il numero complesso $z = \frac{1}{4} + \frac{i}{4}$.

(*i*) Determinare la rappresentazione trigonometrica di $\frac{1}{z}$.

(*ii*) Calcolare le radici quinte di $\frac{1}{z}$. Quale di queste radici ha sia la parte reale che la parte immaginaria negative ?

* * * * * * * * *

1.37. (*i*) Calcolare le quattro radici complesse quarte di -2.

(*ii*) Usando (*i*), determinare le otto radici complesse ottave di 4 e disegnarle nel piano $\boldsymbol{R}^2$.

* * * * * * * * *

1.38. [*Esame 10/6/03*] È assegnato il numero complesso $z = -2 - 2i$. Determinare in forma trigonometrica i numeri complessi $z^{3/4}$ e $z^{4/3}$ e disegnarli nel piano di Argand-Gauss.

* * * * * * * * *

1.39. Determinare la struttura algebrica dei seguenti sottoinsiemi del campo $\boldsymbol{C}$ dei numeri complessi:

(*i*) $\{z = a + i\,b \in \boldsymbol{C} :\ a = b\}$. (*ii*) $\{z \in \boldsymbol{C} :\ \mathcal{N}(z) = 1\}$.

(*iii*) $\{z = a + i\,b \in \boldsymbol{C} :\ a, b \in \boldsymbol{Q}\}$. (*iv*) $\{z = a + i\,b \in \boldsymbol{C} :\ a, b \in \boldsymbol{Z}\}$.

* * * * * * * * *

1.40. (*i*) Sia $\varphi : \boldsymbol{C} \to \boldsymbol{C}$ l'applicazione così definita: $\varphi(z) = \overline{z},\ \forall\, z \in \boldsymbol{C}$. Verificare che φ è un isomorfismo del campo $\boldsymbol{C}$ in sé.

(*ii*) Posto $\boldsymbol{C}^{\cdot} = \boldsymbol{C} - \{0\}$, sia $f : \boldsymbol{C}^{\cdot} \to \boldsymbol{C}^{\cdot}$ l'applicazione così definita: $f(z) = \frac{1}{z},\ \forall\, z \in \boldsymbol{C}^{\cdot}$.

(*a*) f è un isomorfismo del gruppo $(\boldsymbol{C}^{\cdot}, \cdot)$ in sé ?

(*b*) Determinare gli eventuali $z \in \boldsymbol{C}^{\cdot}$ 'fissati' da f (cioè per cui $f(z) = z$).

(*c*) Verificare che f 'fissa' il sottoinsieme $\boldsymbol{U} = \{z \in \boldsymbol{C} :\ \mathcal{N}(z) = 1\}$ (cioè $f(\boldsymbol{U}) \subseteq \boldsymbol{U}$).

* * * * * * * * *

1.41. È assegnato il numero complesso $z = 3 - 4\,i$.

(*i*) Calcolare, facendo ricorso alla formula di De Moivre, i numeri complessi z^2 e $\frac{1}{z}$.

(*ii*) Calcolare le radici seconde e le radici quarte di z, esprimendole senza far ricorso alle funzioni seno e coseno.

* * * * * * * * *

1.42. Sia R un dominio d'integrità e sia $\equiv$ la relazione su $R \times R^{\cdot}$ così definita:

$$(a, b) \equiv (c, d) \iff ad - bc = 0.$$

(*i*) Si verifichi che $\equiv$ è una relazione di equivalenza su $R \times R^{\cdot}$.

Denotato con $K = R \times R^{\cdot}/_{\equiv}$ l'insieme quoziente di $R \times R^{\cdot}$ modulo $\equiv$ e con $\frac{a}{b}$ la classe di equivalenza di (a, b) modulo $\equiv$, sono definite in K le due operazioni

$$+ : K \times K \to K \ \text{ tale che } \ \tfrac{a}{b} + \tfrac{c}{d} = \tfrac{ad+bc}{bd},\ \ \forall\, \tfrac{a}{b},\, \tfrac{c}{d} \in K,$$
$$\cdot : K \times K \to K \ \text{ tale che } \ \tfrac{a}{b} \cdot \tfrac{c}{d} = \tfrac{ac}{bd},\ \ \forall\, \tfrac{a}{b},\, \tfrac{c}{d} \in K.$$

(*ii*) Verificare che $+,\ \cdot$ sono ben poste e che $(K, +, \cdot)$ è un campo. Tale campo viene chiamato *campo dei quozienti di* R e viene spesso denotato $\mathbf{Q}(R)$.

(*iii*) Sia $i : R \to K$ l'applicazione così definita:

$$i(a) = \tfrac{a}{1},\ \ \forall\, a \in R.$$

Verificare che i è un omomorfismo iniettivo di anelli. i è detto *immersione canonica* di R nel suo campo dei quozienti K.

* * * * * * * * *

1.43. Verificare che l'insieme delle successioni a valori in $\boldsymbol{R}$ e l'insieme delle successioni a valori in $\boldsymbol{N}$ hanno la cardinalità del continuo.

* * * * * * * * *

1.44. Indicato con $\boldsymbol{R}[X_1, X_2, \ldots, X_n]$ l'anello dei polinomi a coefficienti in $\boldsymbol{R}$, nelle n indeterminate $X_1, X_2, \ldots, X_n$ (cfr. **Cap. III.1**), verificare che $\boldsymbol{R}[X_1, X_2, \ldots, X_n] \sim \boldsymbol{R}$.

* * * * * * * * *

1.45. Verificare che l'insieme delle funzioni reali di variabile reale ha cardinalità superiore a quella del continuo.

* * * * * * * * *

Appendice 1

Numeri di Fibonacci

Definizione 1. *Si chiama n-simo numero di Fibonacci il numero naturale F_n definito per ricorsività nel seguente modo:*

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2}\,, \ \forall\, n \geq 2.$$

Chiameremo successione di Fibonacci la successione $\{F_n\}$ dei numeri di Fibonacci. Risulta subito, con semplici calcoli:

$$F_2 = 1, \quad F_3 = 2, \quad F_4 = 3, \quad F_5 = 5, \quad F_6 = 8, \quad F_7 = 13, \quad F_8 = 21, \quad \textit{ecc.}$$

Vogliamo ottenere una *formula chiusa* per la successione di Fibonacci, cioè un'espressione che permetta di calcolare ogni termine F_n della successione, senza conoscerne i precedenti. Si noti che, in generale, per ottenere la formula chiusa di una successione ricorsiva non esistono regole, ma si procede ad intuito, per tentativi.

Proposizione 1. *Per ogni $n \geq 1$ risulta:*

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

Dim. Si fa la seguente ipotesi:

$$F_n = X^n, \quad \forall\, n \geq 0,$$

per un'opportuna quantità numerica X da determinare. Se tale ipotesi verrà soddisfatta, la parte ricorsiva della definizione di numero di Fibonacci implica che risulti:

$$(*) \qquad X^n = X^{n-1} + X^{n-2}.$$

Dividendo (*) per X^{n-2}, si ottiene $X^2 = X + 1$. Le soluzioni di tale equazione sono i due numeri complessi

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

I numeri α e β verificano ovviamente l'equazione (*), ma le successioni $\{\alpha^n\}$ e $\{\beta^n\}$ non verificano le condizioni iniziali della definizione di numero di Fibonacci. Dunque **non** si può concludere che $F_n = \alpha^n$ oppure $F_n = \beta^n$.

Tuttavia si osserva che, $\forall\, r, s \in \boldsymbol{R}$, la combinazioni lineari $G_{rs}(n) = r\,\alpha^n + s\,\beta^n$ verificano (*). Infatti (essendo $\alpha^2 = \alpha + 1$, $\beta^2 = \beta + 1$):

$$G_{rs}(n) = r\,\alpha^n + s\,\beta^n = r\,\alpha^{n-2}\alpha^2 + s\,\beta^{n-2}\beta^2 = r\,\alpha^{n-2}(\alpha+1) + s\,\beta^{n-2}(\beta+1) =$$
$$= r\,\alpha^{n-1} + s\,\beta^{n-1} + r\,\alpha^{n-2} + s\,\beta^{n-2} = G_{rs}(n-1) + G_{rs}(n-2).$$

Si tratta allora di individuare eventuali numeri reali r, s tali che $G_{rs}(0) = 0$ e $G_{rs}(1) = 1$. Se tali numeri esistono, allora $F_n = G_{rs}(n)$, $\forall\, n \geq 0$.

Il sistema $\begin{cases} G_{rs}(0) = 0 \\ G_{rs}(1) = 1 \end{cases}$ equivale a $\begin{cases} r\,\alpha^0 + s\,\beta^0 = 0 \\ r\,\alpha^1 + s\,\beta^1 = 1 \end{cases}$ cioè a $\begin{cases} r + s = 0 \\ \alpha + s\beta = 1. \end{cases}$ Tale sistema ammette l'unica soluzione $r = \frac{1}{\sqrt{5}}$, $s = -r = -\frac{1}{\sqrt{5}}$. Dunque

$$F_n = \tfrac{1}{\sqrt{5}}\left(\alpha^n - \beta^n\right) = \tfrac{1}{\sqrt{5}} \left[\left(\tfrac{1+\sqrt{5}}{2} \right)^n - \left(\tfrac{1-\sqrt{5}}{2} \right)^n \right].$$

Osservazione 1. Il numero complesso $\alpha = \frac{1+\sqrt{5}}{2}$ è noto col nome di *sezione aurea* o *numero d'oro*. È stato introdotto dai matematici greci dell'antichità come il rapporto più armonioso tra la base (lato lungo) e l'altezza (lato corto) di un rettangolo. Precisamente, indicata con a la misura della base e

con b la misura dell'altezza di un rettangolo $\mathfrak{R}$, tale rettangolo soddisfa alle *condizioni di massima armonia* se verifica la *"divina proporzione"* $\frac{a}{b} = \frac{a+b}{a}$ [cioè il rapporto tra lato lungo e lato corto coincide con quello tra la somma dei lati ed il lato lungo]. Si noti che risolvendo la divina proporzione si ottiene l'equazione di secondo grado $(\frac{a}{b})^2 = \frac{a}{b} + 1$, che ammette come unica soluzione positiva proprio la sezione aurea α.

Capitolo II

FATTORIZZAZIONE E CONGRUENZE SUGLI INTERI

1. La divisione euclidea

Teorema 1. (*Divisione euclidea in* $\boldsymbol{Z}$). *Siano* $a, b \in \boldsymbol{Z},\ b \neq 0$. *Esiste un'unica coppia* $(q, r) \in \boldsymbol{Z}\times\boldsymbol{Z}$ *tale che*

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

q, r sono rispettivamente il quoziente ed il resto della divisione euclidea, mentre a, b ne sono rispettivamente il dividendo e il divisore.

Dim. (*Esistenza*). Distinguiamo due casi: $b > 0$ e $b < 0$.

$\boldsymbol{b > 0}$. Si ponga:

$$\mathbf{S} := (a - b\boldsymbol{Z}) \cap \boldsymbol{N} = \{a - bx \geq 0,\ x \in \boldsymbol{Z}\}.$$

Si ha: $\mathbf{S} \neq \emptyset$. Infatti, posto ad esempio $x := -|a|$, si verifica che $a - bx = a + b|a| \geq 0$ [infatti: $b \geq 1 \implies |a|b \geq |a| \implies |a|b \geq |a| \geq -a \implies |a|b + a \geq 0$].

Per il principio del buon ordinamento (cfr. **Cap. I. 5**), $\mathbf{S}$ ha un minimo, che denotiamo r. Se $r = a - bq$ con $q \in \boldsymbol{Z}$, segue subito che $a = bq + r$ e resta quindi soltanto da verificare che $0 \leq r < |b|$.

Poiché $r \in \mathbf{S}$, allora $r \geq 0$. Per assurdo, sia $r \not< |b| = b$ e dunque $r \geq b$. Allora $0 \leq r - b = a - bq - b = a - b(q + 1)$ e quindi $r - b \in \mathbf{S}$. Ma $r - b < r$ e ciò contraddice la minimalità di r in $\mathbf{S}$: assurdo. Si conclude che $0 \leq r < |b|$.

$\boldsymbol{b < 0}$. Allora $-b > 0$. Dal caso precedente, $\exists\, q_1, r_1 \in \boldsymbol{Z}$ tali che $a = (-b)q_1 + r_1,\ 0 \leq r_1 < |-b| = |b|$. Quindi $a = b(-q_1) + r_1$, con $0 \leq r_1 < |b|$.

(*Unicità*). Assumiamo che risulti

$$a = bq + r = bq_1 + r_1, \ \text{ con } \ 0 \leq r < |b|,\ 0 \leq r_1 < |b|.$$

Bisogna verificare che $q = q_1,\ r = r_1$.

Dalla precedente uguaglianza segue subito che $q = q_1 \iff r = r_1$. Assumiamo, per assurdo, che sia $r \neq r_1$ e ad esempio poniamo $r < r_1$. Essendo $\begin{cases} 0 \leq r \\ r_1 < |b|, \end{cases}$ cioè $\begin{cases} -r \leq 0 \\ r_1 < |b|, \end{cases}$ sommando a membro a membro si ottiene $r_1 - r < |b|$. Ma allora

$$|b| \cdot |q - q_1| = |b(q - q_1)| = |r_1 - r| < |b|$$

e quindi, semplificando $|b|$, $|q - q_1| < 1$, cioè $q = q_1$ [in base alla **Prop. I.5.2(11)**]. Ne segue che $r = r_1$, contro l'ipotesi.

Osservazione 1. Esiste la seguente *"variante"* della divisione euclidea: $\forall\, a, b \in \boldsymbol{Z},\ b \neq 0$, esiste un'unica coppia $(q_1, r_1) \in \boldsymbol{Z}\times\boldsymbol{Z}$ tale che

$$a = bq_1 + r_1, \quad -\tfrac{|b|}{2} < r_1 \leq \tfrac{|b|}{2}.$$

Se infatti q, r sono tali che $a = bq + r$ e $0 \leq r < |b|$, basta porre:

- se $0 \leq r \leq \frac{|b|}{2}$: $\quad q_1 := q, \quad r_1 := r$
- se $\frac{|b|}{2} < r < |b|$: $\begin{cases} q_1 := q + 1 \ \text{ ed } \ r_1 := r - b, & \text{se } \ b > 0, \\ q_1 := q - 1 \ \text{ ed } \ r_1 := r + b, & \text{se } \ b < 0. \end{cases}$

Ad esempio, posto $a = 19$, $b = -7$, risulta:

$19 = (-7)(-2) + 5$ [divisione euclidea *"tradizionale"*], $19 = (-7)(-3) + (-2)$ [*"variante"*].

È evidente che è possibile anche esprimere (q, r) in funzione di (q_1, r_1). Ne segue che l'unicità e l'esistenza di (q_1, r_1) sono conseguenza del **Teor. 1**.

Si noti che q_1 è l'intero più prossimo al numero razionale $\frac{a}{b}$. Infatti $\frac{a}{b} = q_1 + \frac{r_1}{b}$ e $|\frac{r_1}{b}| \leq \frac{1}{2}$.

Di tale variante della divisione eucidea in $\boldsymbol{Z}$ faremo uso per calcolare quoziente e resto della divisione euclidea nell'anello $\boldsymbol{Z}[i]$ degli interi di Gauss [cfr. **Prop. III.5.1**].

2. Divisibilità e Massimo Comun Divisore

Definizione 1. *Siano* $a, b \in \boldsymbol{Z}$. *Si chiama relazione di divisibilità in* $\boldsymbol{Z}$ *la relazione* $|$ *così definita:*

$$a \,|\, b \iff b = ac,\ \exists\, c \in \boldsymbol{Z}.$$

Si legge: " a *divide* b*" oppure "* a *è un divisore di* b*" oppure ancora "* b *è un multiplo di* a*". Se* a *non divide* b*, si scrive:* $a \not| b$.

Osservazione 1. Per ogni $n \in \boldsymbol{Z}$, sia $n\boldsymbol{Z} := \{nx,\ \forall\, x \in \boldsymbol{Z}\}$. Risulta:

$$a \,|\, b \iff a\boldsymbol{Z} \supseteq b\boldsymbol{Z}.$$

[Infatti: $(\Longrightarrow)$: $a \,|\, b \implies b = ac,\ \exists\, c \in \boldsymbol{Z} \implies b \in a\boldsymbol{Z} \implies b\boldsymbol{Z} \subseteq a\boldsymbol{Z}$.
$(\Longleftarrow)$: $b\boldsymbol{Z} \subseteq a\boldsymbol{Z} \implies b = b\cdot 1 \in a\boldsymbol{Z} \implies b = ac,\ \exists\, c \in \boldsymbol{Z} \implies a \,|\, b$.]

Osservazione 2. La relazione $|$ è riflessiva e transitiva; non è né simmetrica né antisimmetrica. Dunque è soltanto una relazione di pre-ordine su $\boldsymbol{Z}$ (cfr. **Def. I. 3.2**). Si ha infatti:

- $a|a,\ \forall\, a \in \boldsymbol{Z}$ [infatti $a = a\cdot 1$];
- $a|b,\ b|c \implies a|c,\ \forall\, a, b, c \in \boldsymbol{Z}$ [infatti, se $b = ax,\ c = by,$ allora $c = (ax)y = a(xy)$];
- $2 \,|\, 4$ ma $4 \not| 2$ [non simmetrica];
- $2 \,|\, -2,\ -2 \,|\, 2$ ma $2 \neq -2$ [non antisimmetrica].

Osservazione 3. (*i*) Ogni $a \in \boldsymbol{Z}$ ammette sempre i quattro divisori $\pm a, \pm 1,$ detti *divisori banali* di a. Gli altri eventuali divisori di a sono detti *divisori propri* di a.

(*ii*) Risulta:

- $a \,|\, 0,\ \forall\, a \in \boldsymbol{Z}$ [infatti $0 = a\cdot 0$];
- $1 \,|\, a,\ \forall\, a \in \boldsymbol{Z}$ [infatti $a = 1\cdot a$];
- $0 \,|\, a \iff a = 0$ $\left[\begin{array}{l}(\Rightarrow):\ a = 0\cdot c \implies a = 0\\ (\Leftarrow):\ 0 \,|\, 0 \text{ (ovvio)}\end{array}\right]$;
- $a \,|\, 1 \iff a = \pm 1$ $\left[\begin{array}{l}(\Rightarrow):\ 1 = a\cdot c \implies a = \pm 1\\ (\Leftarrow):\ \pm 1 \,|\, 1 \text{ (ovvio)}\end{array}\right]$.

Proposizione 1. (*i*) $a \,|\, b \iff ac \,|\, bc,\ \forall\, c \in \boldsymbol{Z} \iff ac \,|\, bc,\ \exists\, c \in \boldsymbol{Z}^{\cdot}$ $[= \boldsymbol{Z} - \{0\}]$.
(*ii*) $a \,|\, b$ *e* $a \,|\, c \iff a \,|\, bx + cy,\ \forall\, x, y \in \boldsymbol{Z}$.

Dim. (*i*) Se $a \,\big|\, b$ e $b = ax$, alllora $bc = acx,\ \forall\, c \in \boldsymbol{Z}$, cioè $ac \,|\, bc,\ \forall\, c \in \boldsymbol{Z}$.

Se $ac \,\big|\, bc,\ \forall\, c \in \boldsymbol{Z}$, ovviamente $ac \,\big|\, bc,\ \exists\, c \in \boldsymbol{Z}^{\cdot}$.

Se $ac \,\big|\, bc,\ \exists\, c \in \boldsymbol{Z}^{\cdot}$, allora $bc = acx$, cioè $(b - ax)c = 0$. Allora $b - ax = 0$, cioè $a \,|\, b$.

(*ii*) $(\Longrightarrow)$. $b = ar,\ c = as \implies bx + cy = arx + asy = a(rx + sy) \implies a \,|\, bx + cy$.
$(\Longleftarrow)$. $a \,\big|\, b\cdot 1 + c\cdot 0$ e quindi $a \,\big|\, b$; $a \,\big|\, b\cdot 0 + c\cdot 1$ e quindi $a \,\big|\, c$.

Osservazione 4. Esaminiamo più in dettaglio la *non antisimmetria* della relazione $\big|$. Introduciamo la seguente definizione.

Definizione. Siano $a, b \in \boldsymbol{Z}^{\cdot}$. a e b sono detti *associati* (e si scrive $a \sim b$) se $a \,\big|\, b$ e $b \,\big|\, a$.

[Si può facilmente osservare che $\sim$ è una relazione di equivalenza su $\boldsymbol{Z}^{\cdot}$]. Verifichiamo ora che

$$a \sim b \iff b = \pm a$$

$(\Longrightarrow)$. $a \sim b \implies b = ax,\ a = by,\ \exists\, x, y \in \boldsymbol{Z} \implies a = axy \implies 1 = xy$ [essendo $a \neq 0$] $\implies x = \pm 1 \implies b = \pm a$.

($\Longleftarrow$). Ovviamente $\pm a \,|\, a$ e $a \,|\, \pm a$. Dunque $a \sim \pm a$.

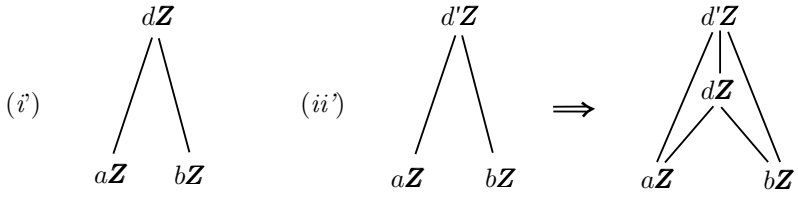
Definizione 2. *Siano $a, b \in \boldsymbol{Z}$, non entrambi nulli. Si chiama massimo comun divisore di a, b (abbreviato MCD) ogni eventuale intero $d \geq 1$ tale che*

$$(i)\ \ d \,|\, a \ \text{ e } d \,|\, b; \qquad (ii)\ \ \text{se } d' \,|\, a \ \text{ e } d' \,|\, b, \ \text{allora } d' \,|\, d.$$

Il MCD di a, b viene denotato con $MCD(a, b)$ o semplicemente (a, b) o anche $GCD(a, b)$ [da "Greatest Common Divisor"] . Per brevità riscriveremo le condizioni (i) e (ii) nella forma:

$$(i)\ \ d \,\Big|\, \begin{matrix} a \\ b \end{matrix}; \qquad (ii)\ \ d' \,\Big|\, \begin{matrix} a \\ b \end{matrix} \implies d' \,|\, d.$$

Osservazione 5. Dall'**Osserv. 1** segue che (i) e (ii) possono essere visualizzate nella forma:



[dove i segmenti tracciati corrispondono a inclusioni "verso l'alto"]. Ne segue che il MCD corrisponde al più piccolo insieme del tipo $n\boldsymbol{Z}$ contenente $a\boldsymbol{Z}$ e $b\boldsymbol{Z}$.

Osservazione 6. Si noti che, se si applicano le condizioni (i) e (ii) della precedente **Def. 2** ad $a = b = 0$, risulta $MCD(0, 0) = 0$. Si preferisce però di solito considerare *non definito* $MCD(0, 0)$. Infatti ogni naturale n è un divisore di 0 e sembra quindi paradossale affermare che 0 è il "più grande" divisore comune di 0 e 0.

Teorema 1. ($\textit{Esistenza ed unicità del } MCD$). *Siano $a, b \in \boldsymbol{Z}$ non entrambi nulli. $MCD(a, b)$ esiste ed è unico.*

Dim. (Esistenza). Poniamo:

$$\mathbf{S} := (a\boldsymbol{Z} + b\boldsymbol{Z}) \cap \boldsymbol{N}^{\cdot} = \{ax + by > 0, \ \ \forall\, x, y \in Z\}.$$

Osserviamo che $\mathbf{S} \neq \emptyset$. Infatti: se $a > 0$, allora $a = a \cdot 1 + b \cdot 0 \in \mathbf{S}$; se invece $a < 0$, allora $-a = a \cdot (-1) + b \cdot 0 \in \mathbf{S}$; se $a = 0$ e $b > 0$, allora $b \in \mathbf{S}$; se infine $a = 0$ e $b < 0$, allora $-b \in \mathbf{S}$.

Dal principio del buon ordinamento segue che $\mathbf{S}$ ha un minimo: sia tale minimo $d := ax_0 + by_0$ (con $x_0, y_0 \in \boldsymbol{Z}$). Certo $d \geq 1$ (perché $d \in \mathbf{S}$); vogliamo verificare che $d = MCD(a, b)$, cioè che:

$$(*)\ \ d \,\Big|\, \begin{matrix} a \\ b \end{matrix} \quad \text{e} \quad (**)\ \ d' \,\Big|\, \begin{matrix} a \\ b \end{matrix} \implies d' \,|\, d.$$

($*$): preso un qualsiasi intero $ax + by \in a\boldsymbol{Z} + b\boldsymbol{Z}$, lo si divida per d: $\exists\, q, r \in \boldsymbol{Z}$ tali che

$$ax + by = dq + r, \quad 0 \leq r < d.$$

Allora: $r = ax - by - (ax_0 + by_0)q = a(x - x_0 q) + b(y - y_0 q)$.

Se fosse $r > 0$, allora $r \in \mathbf{S}$. Poiché $r < d$, ciò contraddice la minimalità di d in $\mathbf{S}$. Dunque $r = 0$. Allora $d \,|\, ax + by, \ \ \forall\, x, y \in \boldsymbol{Z}$. Segue (cfr. **Prop. 1**(ii)) che $d \,\Big|\, \begin{matrix} a \\ b \end{matrix}$.

($**$): da $d' \,\Big|\, \begin{matrix} a \\ b \end{matrix}$ segue che $d' \,|\, ax_0 + by_0$, cioè $d' \,|\, d$.

(Unicità). Se $d, \tilde{d}$ sono due MCD di a, b, allora:

$d \,|\, \tilde{d}$ [infatti, essendo $\tilde{d} = MCD(a, b)$, da $d \,\Big|\, \begin{matrix} a \\ b \end{matrix}$ segue che $d \,|\, \tilde{d}$];

$\tilde{d} \,|\, d$ [infatti, essendo $d = MCD(a, b)$, da $\tilde{d} \,\Big|\, \begin{matrix} a \\ b \end{matrix}$ segue che $\tilde{d} \,|\, d$].

Ne segue che $d \sim \tilde{d}$. Poiché $d, \tilde{d} \geq 1$, allora $d = \tilde{d}$.

Proposizione 2. *Sia $a \neq 0$. Se $a \,|\, b$, allora $MCD(a,b) = |a|$. Ne segue in particolare:*
(i) $MCD(a, \pm a) = |a|$ (infatti $a \,|\, \pm a$).
(ii) $MCD(a, 0) = |a|$ (infatti $a \,|\, 0$).
(iii) $MCD(\pm 1, a) = 1$ (infatti $\pm 1 \,|\, a$).

Dim. Sia $b = ac$. Si ha: $|a| \,\Big|\, \begin{matrix} a \\ ac \end{matrix}$. Se poi $d' \,\Big|\, \begin{matrix} a \\ ac \end{matrix}$, allora $d' \,|\, a$ e quindi $d' \,|\, |a|$. Si conclude che $|a|$ è il MCD di a, $b = ac$.

Il seguente risultato estende la proposizione precedente.

Proposizione 3. *Siano $a, b, c \in \boldsymbol{Z}$, con $a \neq 0$ e $(b,c) \neq (0,0)$. Si ha*
$$MCD(ab, ac) = |a|\, MCD(b,c).$$

Dim. Si ponga: $d := MCD(b,c)$, $d_1 := MCD(ab, ac)$. Dimostreremo che $d_1 = |a| \cdot d$, cioè che
$$(*) \quad |a| \cdot d \,|\, d_1, \qquad (**) \quad d_1 \,\Big|\, |a| \cdot d.$$
(*): $d \,\Big|\, \begin{matrix} b \\ c \end{matrix} \implies ad \,\Big|\, \begin{matrix} ab \\ ac \end{matrix} \implies |a|d \,\Big|\, \begin{matrix} ab \\ ac \end{matrix} \implies |a|d \,|\, d_1$.

(**): poiché $a \,\Big|\, \begin{matrix} ab \\ ac \end{matrix}$ allora $a \,|\, d_1$, cioè $d_1 = at$, $\exists t \in \boldsymbol{Z}$. Allora: $at \,\Big|\, \begin{matrix} ab \\ ac \end{matrix} \implies t \,\Big|\, \begin{matrix} b \\ c \end{matrix} \implies t \,|\, d \implies at \,|\, ad \implies at \,\Big|\, |a|d$, cioè $d_1 \,\Big|\, |a|d$.

Corollario 1. *Se $MCD(a,b) = d$, allora $MCD(\frac{a}{d}, \frac{b}{d}) = 1$.*

Dim. Si ha: $d = MCD(a,b) = MCD(\frac{a}{d}\, d, \frac{b}{d}\, d) = |d|\, MCD(\frac{a}{d}, \frac{b}{d}) = d\, MCD(\frac{a}{d}, \frac{b}{d})$, cioè $d = d\, MCD(\frac{a}{d}, \frac{b}{d})$. Semplificando d, si ha la tesi.

Definizione 3. *Siano $a, b \in \boldsymbol{Z}$ non entrambi nulli. a, b sono detti coprimi (o relativamente primi) se $MCD(a,b) = 1$.*

Il seguente fondamentale risultato segue subito dalla dimostrazione dell'esistenza del MCD.

Corollario 2. (*Identità di Bézout*). *Siano $a, b \in \boldsymbol{Z}$ non entrambi nulli. Se $d = MCD(a,b)$, esistono $x_0, y_0 \in \boldsymbol{Z}$ tali che*
$$d = ax_0 + by_0 \quad \textit{[identità di Bézout per } a, b\textit{]}.$$

Dim. Cfr. **Teor. 1** (Esistenza).

Osservazione 7. (*i*) La coppia (x_0, y_0) che realizza l'identità di Bézout per a, b *non* è *unica*, anzi ne esistono infinite. Infatti $\forall\, c \in \boldsymbol{Z}$,
$$a(x_0 + bc) + b(y_0 - ac) = d + abc - bac = d.$$
Dunque anche $(x_0 + bc, y_0 - ac)$ realizza un'identità di Bézout per a, b.

(*ii*) Se $1 = ar + bs$ (per opportuni $r, s \in \boldsymbol{Z}$), allora $MCD(a,b) = 1$.

Infatti, posto $d = MCD(a,b)$, da $d \,\Big|\, \begin{matrix} a \\ b \end{matrix}$ segue che $d \,\Big|\, ar + bs = 1$ e dunque $d = 1$.

Corollario 3. (*Lemma di Euclide*) *[abbreviato EU]. Siano a, b, $c \in \boldsymbol{Z}$. Se $a \,|\, bc$ e $MCD(a,b) = 1$, allora $a \,|\, c$.*

Dim. Sia $1 = a\cdot r + b\cdot s$ [identità di Bézout per a, b]. Sia $bc = at,\ \exists\, t \boldsymbol{Z}$. Allora:

$$c = c\cdot 1 = c(ar + bs) = acr + bcs = acr + ats = a(cr + ts).$$

Dunque $a \,|\, c$.

Esercizio 1. Siano $a,\ b,\ c \in \boldsymbol{Z}$ tali che $(ab, c) \neq (0, 0)$. Risulta:

$$MCD(ab, c) = 1 \iff MCD(a, c) = MCD(b, c) = 1$$

Soluzione. ($\Longrightarrow$). Sia $d_1 := MCD(a, c)$. Risulta: $d_1 \Big| \begin{matrix} a \\ c \end{matrix} \implies d_1 \Big| \begin{matrix} ab \\ c \end{matrix} \implies d_1 \,|\, 1 \implies d_1 = 1$. In modo analogo si verifica che $MCD(b, c) = 1$.

($\Longleftarrow$). Sia $d := MCD(ab, c)$. Se dimostreremo che $MCD(d, a) = 1$, allora, in base al Lemma di Euclide (EU), da $d \,|\, ab$ e $MCD(d, a) = 1$, segue che $d \,|\, b$. Ma allora: $d \Big| \begin{matrix} b \\ c \end{matrix} \implies d \,|\, 1 \implies d = 1$.

Resta quindi da verificare che $MCD(d, a) = 1$. Sia $d' := MCD(d, a)$. Allora:

$d' \Big| \begin{matrix} a \\ d \,|\, c \end{matrix} \implies d' \Big| \begin{matrix} a \\ c \end{matrix} \implies d' \,|\, 1 \implies d' = 1$, cioè $MCD(d, a) = 1$.

Sappiamo che il MCD esiste, ma non abbiamo ancora un modo per calcolarlo, né un modo per ottenere un'identità di Bézout. Il metodo per ottenere MCD e identità di Bézout è l'*algoritmo euclideo delle divisioni successive*, che ora descriviamo. Premettiamo un risultato.

Proposizione 4. *Siano $a,\ b, \in \boldsymbol{Z}$, con $b \neq 0$. Sia $a = bq + r$, con $0 \leq r < |b|$. Risulta:*

$$MCD(a, b) = MCD(b, r).$$

Dim. Siano $d := MCD(a, b)$ e $d_1 := MCD(b, r)$. Bisogna dimostrare che:

$$(*)\ \ d \,|\, d_1 \quad \text{e} \quad (**)\ \ d_1 \,|\, d.$$

Infatti:

$(*)$: $d \Big| \begin{matrix} a \\ b \end{matrix} \implies d \,\big|\, a - bq = r \implies d \Big| \begin{matrix} r \\ b \end{matrix} \implies d \,|\, d_1$.

$(**)$: $d_1 \Big| \begin{matrix} b \\ r \end{matrix} \implies d_1 \,\big|\, bq + r = a \implies d_1 \Big| \begin{matrix} a \\ b \end{matrix} \implies d_1 \,|\, d$.

ALGORITMO EUCLIDEO DELLE DIVISIONI SUCCESSIVE

Siano $a,\ b \in \boldsymbol{Z}$. Se uno dei due interi è nullo (ad esempio $b = 0$), l'algoritmo non è necessario, in quanto $MCD(a, 0) = |a| = a\cdot(\pm 1) + b\cdot 0$.

Siano quindi $a,\ b \in \boldsymbol{Z}^{\cdot}$ ed assumiamo che $a \geq b > 0$. Al fine di calcolare il MCD, tale assunzione non è restrittiva: se infatti a o b non fosse positivo, potrebbe essere sostituito dal rispettivo opposto [infatti $MCD(a, b) = MCD(\pm a, \pm b)$]; se non fosse $a \geq b$, i due interi potrebbero essere scambiati tra loro [infatti $MCD(a, b) = MCD(b, a)$].

L'algoritmo euclideo delle divisioni successive consiste in una successione finita di divisioni euclidee, in modo che il divisore ed il resto (se non nullo) diventino rispettivamente dividendo e divisore della divisione successiva. Il procedimento si interrompe non appena si ottiene il primo resto nullo. Dunque l'algoritmo è articolato nei seguenti passi:

($\mathbf{1}^o$) $a = bq_1 + r_1,\ 0 \leq r_1 < b$. Se $r_1 > 0$, si procede con il passo successivo.

($\mathbf{2}^o$) $b = r_1 q_2 + r_2,\ 0 \leq r_2 < r_1$. Se $r_2 > 0$, si procede con il passo successivo.

($\mathbf{3}^o$) $r_1 = r_2 q_3 + r_3,\ 0 \leq r_3 < r_2$. Se $r_3 > 0$, si procede con il passo successivo.

.
.
.

Risulta quindi: $b > r_1 > r_2 > r_3 > \ldots$. Pertanto $\exists\, n \in \boldsymbol{N}$ tale che $r_n > 0$ e $r_{n+1} = 0$. Ciò significa che gli ultimi due passi dell'algoritmo sono

$(\boldsymbol{n}^o)$ $r_{n-2} = r_{n-1}\, q_n + r_n,\ 0 < r_n < r_{n-1}$.

$(\boldsymbol{n+1}^o)$ $r_{n-1} = r_n\, q_{n+1} + 0$.

Dalla **Prop. 4** segue:

$$MCD(a,b) = MCD(b,r_1) = MCD(r_1,r_2) = MCD(r_2,r_3) = \ldots = MCD(r_{n-1},r_n) = MCD(r_n,0) = r_n.$$

Dunque $r_n = MCD(a,b)$. Il MCD è quindi l'ultimo resto non nullo dell'algoritmo.

Per ottenere un'identità di Bézout si procede in questo modo. Si isolano gli n resti ottenuti nelle divisioni successive, a partire da r_1. Per ricordarsi di non eseguire semplificazioni numeriche, si conviene di scrivere tra parentesi quadre gli interi a, b ed i resti r_k. Si ottengono pertanto le seguenti uguaglianze:

$(\boldsymbol{1}^o)$ $[r_1] = [a] - q_1[b]$.

$(\boldsymbol{2}^o)$ $[r_2] = [b] - q_2[r_1]$.

$(\boldsymbol{3}^o)$ $[r_3] = [r_1] - q_3[r_2]$.

.

.

.

$(\boldsymbol{n}^o)$ $[r_n] = [r_{n-2}] - q_n[r_{n-1}]$.

Si osserva subito che, $\forall\, k = 1, 2, \ldots n$, $[r_k]$ è "combinazione lineare" di $[r_{k-1}]$ e $[r_{k-2}]$ (convenendo in particolare di porre $r_0 = b$, $r_{-1} = a$). A partire da $k = 2$ (se $r_2 \neq 0$), con successive sostituzioni si può quindi esprimere ogni $[r_k]$ come combinazione lineare di $[a]$ e $[b]$, con coefficienti che sono funzioni di $q_1, \ldots, q_k$.

In conclusione, si otterrà $[r_n]$ in funzione di $[a]$, $[b]$. Eliminando le parentesi quadre, si ottiene, come richiesto, un'identità di Bézout relativa ad a, b (con $a \geq b > 0$).

Esempio 1. Calcolare MCD e un'identità di Bézout per $a = -123$, $b = -39$.

Si ha: $123 > 39 > 0$. Risulta:

$$\begin{array}{rl} \underline{123} = \underline{39}\cdot 3 + \underline{6} & \qquad [6] = [123] - [39]\cdot 3 \\ \underline{39} = \underline{6}\cdot 6 + \underline{3} & \qquad [3] = [39] - [6]\cdot 6 \\ \underline{6} = \underline{3}\cdot 2 + 0. & \end{array}$$

Dunque $MCD(123, 39) = 3$ e

$$[3] = [39] - ([123] - [39]\cdot 3)\cdot 6 = [39] - 6[123] + 18[39] = -6[123] + 19[39].$$

Da ciò segue $3 = -6\cdot 123 + 19\cdot 39$ ed, essendo $a = -123$, $b = -39$, si ottiene l'identità di Bézout

$$3 = 6\cdot a - 19\cdot b.$$

Esempio 2. Calcolare MCD e un'identità di Bézout per $a = -336$, $b = 115$.

Si ha: $336 > 115 > 0$. Risulta:

$$\begin{array}{rl} \underline{336} = \underline{115}\cdot 2 + \underline{106} & \qquad [106] = [336] - [115]\cdot 2 \\ \underline{115} = \underline{106}\cdot 1 + \underline{9} & \qquad [9] = [115] - [106]\cdot 1 \\ \underline{106} = \underline{9}\cdot 11 + \underline{7} & \qquad [7] = [106] - [9]\cdot 11 \\ \underline{9} = \underline{7}\cdot 1 + \underline{2} & \qquad [2] = [9] - [7]\cdot 1 \\ \underline{7} = \underline{2}\cdot 3 + \underline{1} & \qquad [1] = [7] - [2]\cdot 3 \\ \underline{2} = \underline{1}\cdot 2 + 0. & \end{array}$$

Dunque $MCD(336, 115) = 1$ e

$[9] = [115] - \big([336] - [115]\cdot 2\big) = -[336] + [115]\cdot 3$;

$[7] = [336] - [115]\cdot 2 - \big(-[336] + [115]\cdot 3\big)\cdot 11 = [336]\cdot 12 + [115]\cdot(-35)$;

$[2] = -[336] - [115]\cdot 3 - [336]\cdot 12 + [115]\cdot 35 = [336]\cdot(-13) + [115]\cdot 18$;

$[1] = [336]\cdot 12 + [115]\cdot(-35) - \big([336]\cdot(-13) + [115]\cdot 18\big)\cdot 3 = [336]\cdot 51 + [115]\cdot(-149)$.

Da ciò segue $1 = 51\cdot 336 - 149\cdot 115$ ed, essendo $a = -336,\ b = 115,$ si ottiene l'identità di Bézout

$$1 = -51\cdot a - 149\cdot b.$$

Un altro importante algoritmo che utilizza le divisioni euclidee è quello che ci consente di rappresentare ogni naturale (e, più in generale ogni numero reale) in base $b \geq 2$. Dedicheremo la parte finale di questo paragrafo alla descrizione di tale algoritmo.

SCRITTURA DI UN NATURALE IN BASE $b \geq 2$

Proposizione 5. *Sia* $b \geq 2$ *un naturale fissato. Ogni* $a \in \boldsymbol{N}$ *si scrive in modo unico nella forma*

$$(*) \qquad a = \sum_{t=0}^{n} r_t\, b^t \quad \text{con} \quad \begin{cases} n \geq 0 \\ r_t \in \boldsymbol{N} \ \text{ e } \ 0 \leq r_t < b, \ \ \forall\, t = 0, \ldots, n \\ r_n \neq 0, \quad \text{se } \ a \neq 0. \end{cases}$$

Tale espressione di a *è detta espansione di* a *in somma di potenze di* b.

Dim. (*Esistenza*). Si procede per induzione forte su $a \geq 0$.

$\boldsymbol{a = 0}$. Si ha: $0 = 0\cdot b^0$ e dunque la formula $(*)$ è verificata.

$\boldsymbol{a \geq 0}$. Assumiamo che, $\forall\, q \in \boldsymbol{N}$ tale che $0 \leq q \leq a,\ q$ si scriva in forma $(*)$. Sia $a+1 = bq + r$ [divisione euclidea], con $0 \leq r < b$. Si osservi che (essendo $a+1,\ b,\ r \geq 0$) $q \geq 0$. Inoltre (essendo $b \geq 2$) $q \leq a$. Si può applicare a q l'ipotesi induttiva:

$$q = \sum_{s=0}^{m} r_s\, b^s, \quad \text{con } \ 0 \leq r_s < b.$$

Allora

$$a + 1 = bq + r = \sum_{s=0}^{m} r_s\, b^{s+1} + r = r + r_0 b + \ \ldots\ + r_m\, b^{m+1} \quad \text{[espressione di tipo } (*)\text{]}.$$

(*Unicità*). Sia $a = \sum_{i=0}^{n} r_i\, b^i = \sum_{j=0}^{m} s_j\, b^j$, con $n \leq m$ [per fissare le idee]. Si ha, da tali uguaglianze:

$$a = r_0 + bq_1 = s_0 + bq_2, \ \text{ con } \ 0 \leq r_0, s_0 < b.$$

Per l'unicità del resto e del quoziente della divisione euclidea di a per b, si ottiene $r_0 = s_0$ e $q_1 = q_2$, cioè:

$$r_1 + r_2 b + \ \ldots\ + r_n b^{n-1} = s_1 + s_2 b + \ \ldots\ + s_m\, b^{m-1}.$$

Procedendo in modo analogo, si perviene a $r_i = s_i,\ \forall\, i = 0, \ldots n$. Se per assurdo fosse $n < m$, si avrebbe:

$$0 = s_{n+1} b + \ \ldots\ + s_m\, b^{m-n}.$$

In tal caso, essendo $s_m > 0$ ed ogni altro $s_k \geq 0$, il secondo membro sarebbe > 0: assurdo. Si conclude che $n = m$ e quindi le due espressioni coincidono.

Se $b = 10$ e $a \in \boldsymbol{N}$, le cifre di a nella numerazione araba (o decimale) sono esattamente i coefficienti che intervengono nell'espansione $(*)$ di a come somma di potenze di 10. Ad esempio:

$$a = 1270 = 1\cdot 10^3 + 2\cdot 10^2 + 7\cdot 10^1 + 0\cdot 10^0.$$

Scriveremo: $1270 = (1,\, 2,\, 7,\, 0)_{10}$.

Definizione 4. *Si chiama scrittura di* a *in base* b *la successione* $\{r_n,\, r_{n-1},\, \ldots, r_0\}$ *dei coefficienti dell'espansione* $(*)$ *di* a *come somma di potenze di* b. *Scriveremo:*

$$a = \big(r_n,\, r_{n-1},\, \ldots, r_0\big)_b.$$

Ad esempio:

$0 \in \boldsymbol{N}$ *si scrive in base* b *nella forma* $(0)_b$;
$b \in \boldsymbol{N}$ *si scrive in base* b *nella forma* $(1,\, 0)_b$;

$b^2 \in \boldsymbol{N}$ *si scrive in base* b *nella forma* $(1,\,0,\,0)_b$, *ecc.*

Per scrivere in base b un qualsiasi naturale a si procede con il seguente algoritmo:

$$\begin{aligned}
&a = bq_0 + r_0, && 0 \le r_0 < b;\\
&q_0 = bq_1 + r_1, && 0 \le r_1 < b;\\
&q_1 = bq_2 + r_2, && 0 \le r_2 < b;\\
&\cdot\\
&\cdot\\
&\cdot\\
&q_{n-2} = bq_{n-1} + r_{n-1}, && 0 \le r_{n-1} < b;\\
&q_{n-1} = b\cdot 0 + r_n, && 0 < r_n = q_{n-1} < b.
\end{aligned}$$

Si noti che $a > q_0 > q_1 > q_2 > \ ...$ e dunque l'algoritmo termina [con $q_n = 0$]. Basta ora inserire l'espressione di ogni q_k in quella di q_{k-1}, a partire dalla prima divisione. Si ottiene:

$$a = b^2 q_1 + br_1 + r_0 = b^3 q_2 + b^2 r_2 + b\,r_1 + r_0 = \ ... \ = b^n r_n + b^{n-1} r_{n-1} + \ ... \ + b^2 r_2 + b\,r_1 + r_0.$$

Dunque: $a = \big(r_n,\, r_{n-1},\, ...,\, r_2,\, r_1,\, r_0\big)_b$.

Ad esempio: $1270 = (1,\,2,\,7,\,0)_{10} = (5,\,5,\,1,\,4)_6 = (4,\,15,\,6)_{16} = (12,\,70)_{100}$.

Infatti:

$$\begin{cases} 1270 = 211\cdot 6 + 4\\ 211 = 35\cdot 6 + 1\\ 35 = 5\cdot 6 + 5\\ 5 = 0\cdot 6 + 5 \end{cases}\uparrow \qquad \begin{cases} 1270 = 79\cdot 16 + 6\\ 79 = 4\cdot 16 + 15\\ 4 = 0\cdot 16 + 4 \end{cases}\uparrow \qquad \begin{cases} 1270 = 12\cdot 100 + 70\\ 12 = 0\cdot 100 + 12 \end{cases}\uparrow$$

Osservazione 8. Vogliamo rimarcare, come conseguenza della **Prop. 5** applicata a $b = 2$, che ogni $a \in \boldsymbol{N}$ si scrive in modo unico come somma di potenze decrescenti di 2. Ad esempio

$$15 = (1,\,1,\,1,\,1)_2 = 2^3 + 2^2 + 2^1 + 2^0, \quad 22 = (1,\,0,\,1,\,1,\,0)_2 = 2^4 + 2^2 + 2^1, \ \text{ecc.}$$

Tale considerazione sarà utilizzata nell'**Osserv. 6.2** di questo capitolo.

SCRITTURA DI UN NUMERO REALE IN BASE $b \ge 2$

Ogni numero reale $x > 0$ è somma della sua *parte intera* $[x]$ e della sua *parte frazionaria* $\alpha := x - [x] \in [0, 1)$. [Si ricorda che la parte intera di un numero reale x è il massimo intero $\le x$.]

In base b $(b \ge 2)$ la parte intera $[x]$ si scrive come visto sopra. Vediamo ora come si scrive in base b la parte frazionaria α di x. Per ogni $\alpha \in [0, 1)$, è noto che

$$\alpha = 0, c_1 c_2 c_3 ... c_k \ ... \iff \alpha = \tfrac{c_1}{10} + \tfrac{c_2}{10^2} + \tfrac{c_3}{10^3} + \ ... \ + \tfrac{c_k}{10^k} + \ ... \ = \sum_{k=1}^{\infty} \tfrac{c_k}{10^k}.$$

Se ora $b \ge 2$ è una base assegnata, per esprimere α in base b, basta determinare una successione $\{a_k\}_{k\ge 1}$ tale che

$$\alpha = \sum_{k=1}^{\infty} \tfrac{a_k}{b^k} \quad \text{e} \quad a_k \in \{0,\,1,\,...\,,\,b-1\}.$$

Si scriverà allora: $\alpha = 0, \big(a_1,\, a_2,\, a_3,\, ...\ \big)_b$.

Per determinare le "cifre" a_k si procede in questo modo:

da $\alpha = \sum_{k=1}^{\infty} \frac{a_k}{b^k}$ segue che $b\alpha = a_1 + \sum_{k=2}^{\infty} \frac{a_k}{b^{k-1}}$. La parte intera e la parte frazionaria di $b\alpha$ sono rispettivamente

$$[b\alpha] = a_1 \quad \text{e} \quad b\alpha - a_1, \ \text{ con } \ a_1 \in \{0,\,1,\ ...\, b-1\}.$$

Se $b\alpha - a_1 = 0$, allora $\alpha = \frac{a_1}{b}$ e dunque $\alpha = 0, (a_1,\, 0,\, 0,\, ...\ )_b$: il procedimento ha termine. Se invece $b\alpha - a_1 \ne 0$, si ha:

$$b(b\alpha - a_1) = a_2 + \sum_{k=3}^{\infty} \frac{a_k}{b^{k-2}}.$$

La parte intera e la parte frazionaria di $b(b\alpha - a_1)$ sono rispettivamente

$$[b(b\alpha - a_1)] = a_2 \quad \text{e} \quad b(b\alpha - a_1) - a_2, \ \text{con} \ \ a_2 \in \{0,\ 1,\ \ldots\, b-1\}.$$

Come prima, se $b(b\alpha - a_1) - a_2 = 0$, allora $\alpha = \frac{a_1}{b} + \frac{a_2}{b^2}$ e dunque $\alpha = 0, (a_1,\ a_2,\ 0,\ \ldots\ )_b$ ed il procedimento ha termine. Se invece $b(b\alpha - a_1) - a_2 \neq 0$, si procede come visto sopra.
Naturalmente il procedimento può essere infinito.

A titolo d'esempio, scriviamo in base $b = 5$ i due numeri reali $\alpha = \frac{76}{100} = 0,76$ e $\beta = \frac{75}{100} = 0,75$. Si ha:

$$\begin{aligned}
&\alpha = 0,76 = \tfrac{a_1}{5} + \tfrac{a_2}{25} + \tfrac{a_3}{125} + \ \ldots\ ;\\
&5\alpha = 3,80 = a_1 + \tfrac{a_2}{5} + \tfrac{a_3}{25} + \ \ldots\ \Longrightarrow\ a_1 = 3;\\
&5\alpha - a_1 = 0,80 = \tfrac{a_2}{5} + \tfrac{a_3}{25} + \ \ldots\ ;\\
&5(5\alpha - a_1) = 4,0 = a_2 + \tfrac{a_3}{5} + \ \ldots\ \Longrightarrow\ a_2 = 4;\\
&5(5\alpha - a_1) - a_2 = 0. \quad \text{Dunque} \ \ \alpha = 0, (3,\ 4)_5\,.
\end{aligned}$$

Si ha:

$$\begin{aligned}
&\beta = 0,75 = \tfrac{a_1}{5} + \tfrac{a_2}{25} + \tfrac{a_3}{125} + \ \ldots\ ;\\
&5\beta = 3,75 = a_1 + \tfrac{a_2}{5} + \tfrac{a_3}{25} + \ \ldots\ \Longrightarrow\ a_1 = 3;\\
&5\beta - a_1 = 0,75 = \tfrac{a_2}{5} + \tfrac{a_3}{25} + \ \ldots\ ;\\
&5(5\beta - a_1) = 3,75 = a_2 + \tfrac{a_3}{5} + \ \ldots\ \Longrightarrow\ a_2 = 3;\\
&5(5\beta - a_1) - a_2 = 0,75 = \tfrac{a_3}{5} + \ \ldots\ ;\\
&5(5(5\beta - a_1) - a_2) = 3,75 = a_3 + \tfrac{a_4}{5} + \ \ldots\ \Longrightarrow\ a_3 = 3.
\end{aligned}$$

Si noti che i coefficienti a_k si ripetono costantemente e quindi il procedimento non ha termine. Dunque $\beta = 0, (3,\ 3,\ 3,\ 3,\ \ldots..\ )_5$.

Osservazione 9. I due seguenti numeri scritti in base b:

$$\begin{aligned}
&\alpha_1 = 0, \big(a_1,\ a_2,\ \ldots\,,\ a_{k-1},\ a_k,\ b-1,\ b-1,\ b-1,\ \ldots\ \big)_b,\\
&\alpha_2 = 0, \big(a_1,\ a_2,\ \ldots\,,\ a_{k-1},\ a_k+1,\ 0,\ 0,\ 0,\ \ldots\ \big)_b
\end{aligned}$$

(nell'ipotesi che $a_k < b-1$) coincidono.

Infatti, posto $\beta = \sum_{i=1}^{k-1} \frac{a_i}{b^i}$ ed assunto come noto (dai corsi di Analisi Matematica) il fatto che $\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$, se $0 < x < 1$, si ha:

$$\begin{aligned}
\alpha_1 &= \beta + \tfrac{a_k}{b^k} + \sum_{i=k+1}^{\infty} \tfrac{b-1}{b^i} = \beta + \tfrac{a_k}{b^k} + \tfrac{b-1}{b^{k+1}} \left(1 + \tfrac{1}{b} + \tfrac{1}{b^2} + \ \ldots\ \right) =\\
&= \beta + \tfrac{a_k}{b^k} + \tfrac{b-1}{b^{k+1}} \tfrac{1}{1-\frac{1}{b}} = \beta + \tfrac{a_k}{b^k} + \tfrac{b-1}{b^{k+1}} \tfrac{b}{b-1} = \beta + \tfrac{a_k}{b^k} + \tfrac{1}{b^k} = \beta + \tfrac{a_k+1}{b^k} = \alpha_2.
\end{aligned}$$

Ad esempio, in base $b = 10$, si ha: $0,29999\ \ldots\ = 0,3$. In base $b = 2$, si ha:

$$0, (1,\ 0,\ 0,\ 1,\ 1,\ 1,\ 1,\ 1,\ \ \ldots\ )_2 = 0, (1,\ 0,\ 1)_2 = \tfrac{5}{8}.$$

Si può facilmente verificare che, assegnati i numeri reali $\alpha = \sum_{k=1}^{\infty} \frac{a_k}{b^k}$, $\alpha' = \sum_{k=1}^{\infty} \frac{a'_k}{b^k} \in (0,1]$, se le successioni $\{a_k\}$, $\{a'_k\}$ non sono definitivamente nulle o definitivamente $= b-1$, da $\alpha = \alpha'$ segue che $a_k = a'_k$, $\forall\, k \geq 1$. Dunque possiamo concludere che esiste una biiezione tra l'intervallo $[0,1)$ e l'insieme delle successioni a valori interi compresi tra 0 e $b-1$, non definitivamente uguali a $b-1$. Tale risultato è già stato utilizzato, con $b = 2$ in **Cap. I**, **Teor. 6.5(2)**.

3. Numeri primi. Teorema Fondamentale dell'Aritmetica

Definizione 1. *Sia* $p \in \boldsymbol{Z}$, $p \geq 2$. p *è detto numero primo se* p *ha soltanto i quattro divisori banali* $\pm 1, \pm p$ *(cioè* p *non ha divisori propri). Pertanto:*

$$p \text{ è un numero primo} \iff \big[p = xy \text{ e } x \neq \pm 1 \implies y = \pm 1\big].$$

Lemma 1. *Sia* $p \in \boldsymbol{Z}$, $p \geq 2$. *Si ha:*

$$p \text{ è un numero primo} \iff \big[p \,|\, xy \text{ e } p \nmid x \implies p \,|\, y\big].$$

[Si noti che tale enunciato è logicamente equivalente a $\big[p \,|\, xy \implies p \,|\, x \text{ o } p \,|\, y\big]$. *In altri termini:* p *è un numero primo* $\iff$ *"dividendo il prodotto di due fattori, divide almeno un fattore"].*

Dim. ($\implies$). Sia p un numero primo. Assumiamo che $p \,|\, xy$ e $p \nmid x$. Dimostreremo che $p \,|\, y$.

Si tratta di una conseguenza del Lemma di Euclide (cfr. **Cor. 2.3**). Sia $d := MCD(p, x)$. Poiché $d \,|\, p$, allora $d = 1$ oppure $d = p$. Se fosse $d = p$, allora $d = p \,|\, x$, contro l'ipotesi. Dunque $d = 1$. Pertanto: $p \,|\, xy$, $MCD(p, x) = 1 \overset{EU}{\implies} p \,|\, y$.

($\impliedby$). Sia $p = xy$ e $x \neq \pm 1$. Dimostreremo che $y = \pm 1$.

Da $p = xy$ segue che $p \,|\, xy$. Se $p \,|\, x$ allora $x = pr$ ($\exists\, r \in \boldsymbol{Z}$) e quindi $p = pry$, da cui $ry = 1$ e quindi $y = \pm 1$. Se $p \nmid x$, per ipotesi $p \,|\, y$. Allora $y = ps$ ($\exists\, s \in \boldsymbol{Z}$) e quindi $p = xps$. Ne segue $xs = 1$ e quindi $x = \pm 1$: assurdo. Dunque $y = \pm 1$.

Corollario 1. *Sia* $p \in \boldsymbol{Z}$, $p \geq 2$. *Si ha:*

$$p \text{ è un numero primo} \iff \big[p \,|\, x_1 x_2 \dots x_n \implies p \,|\, x_i,\ \exists\, x_i\ (1 \leq i \leq n)\big].$$

Dim. ($\impliedby$). È un'ovvia conseguenza del **Lemma 1**, con $n = 2$.

($\implies$). Se p è un primo e $p \,|\, x_1 x_2 \dots x_n$, allora $p \,|\, x_1(x_2 \dots x_n)$. Ne segue: $p \,|\, x_1$ oppure $p \,|\, x_2 \dots x_n$. Se $p \nmid x_1$, allora $p \,|\, x_2 \dots x_n = x_2(x_3 \dots x_n)$ e quindi $p \,|\, x_2$ oppure $p \,|\, x_3 \dots x_n$. Iterando tale procedimento si conclude che $p \,|\, x_i,\ \exists\, x_i\ (1 \leq i \leq n)\big]$.

Vogliamo ora estendere il concetto di numero primo ad un qualsiasi dominio d'integrità.

Osservazione 1. Sia $(A, +, \cdot)$ un dominio d'integrità, cioè un anello commutativo unitario ed integro (cfr. **Cap. I.4**). Risulta:

(*i*) In $(A, +, \cdot)$ valgono le *leggi di cancellazione (a sinistra e a destra)*:

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

[infatti: $0 = ab - ac = a(b - c) \implies b - c = 0 \implies b = c$; in modo analogo si verifica l'altra formula].

(*ii*) Gli elementi invertibili di $(A, +, \cdot)$ formano un gruppo rispetto al prodotto, denotato $\mathcal{U}(A)$ (cfr. **Osserv. I.4.3**).

(*iii*) In $(A, +, \cdot)$ si definisce (come in $\boldsymbol{Z}$) la *relazione di divisibilità* $\,|\,$:

$$a \,|\, b \iff b = ax,\ \exists\, x \in A.$$

Tale relazione è riflessiva e transitiva (come in $\boldsymbol{Z}$). In $A^{\cdot}$ è quindi definita la seguente relazione $\sim$:

$$a \sim b \iff a \,|\, b \text{ e } b \,|\, a.$$

Si dice in tal caso che a, b sono *elementi associati*. Si può facilmente verificare che $\sim$ è una relazione di equivalenza su $A^{\cdot}$. Inoltre si verifica subito che $a \sim b \iff b = au$, $\exists\, u \in \mathcal{U}(A)$.
Infine, dalla relazione di divisibilità segue, $\forall\, a \in A^{\cdot}$, la *relazione di congruenza modulo* a:

$$x \equiv_a y \iff a \,|\, x - y.$$

Si tratta, come facilmente si verifica, di una relazione di equivalenza su A.

(*iv*) Non è detto che in $(A, +, \cdot)$ esista il MCD di due elementi non entrambi nulli di A. [In effetti, in $\boldsymbol{Z}$ l'esistenza del MCD segue dall'esistenza della divisione euclidea]. Ci limitiamo qui ad informare il lettore che un esempio di dominio d'integrità in cui non sempre è definito il MCD di due elementi (non nulli) è l'anello $\boldsymbol{Z}[\sqrt{-3}]$ (cfr. **Cap. III.5**).

Definizione 2. *Sia* $(A, +, \cdot)$ *un dominio d'integrità. Sia* $a \in A,\ a \neq 0$ *e* $a \notin \mathcal{U}(A)$.
L'elemento a *è detto primo se* $a \,|\, xy$ *e* $a \nmid x \implies a \,|\, y$. *L'elemento* a *è detto irriducibile se* $a = xy$ *e* $x \notin \mathcal{U}(A) \implies y \in \mathcal{U}(A)$.

Proposizione 1. *In un dominio d'integrità* $(A, +, \cdot)$ *ogni elemento primo è anche irriducibile.*

Dim. [Si tratta dell'implicazione ($\Longleftarrow$) del precedente **Lemma 1**]. Sia a un elemento primo, $a = xy$ e $x \notin \mathcal{U}(A)$. Dimostreremo che $y \in \mathcal{U}(A)$.

Da $a = xy$ segue che $a \,|\, xy$. Se $a \,|\, x$ si ha: $x = ar\ (\exists\, r \in A) \implies a = ary \implies ry = 1 \implies y \in \mathcal{U}(A)$. Se $a \nmid x$, allora $a \,|\, y$. Dunque $y = as\ (\exists\, s \in A) \implies a = xas \implies xs = 1 \implies x \in \mathcal{U}(A)$: assurdo. Dunque $y \in \mathcal{U}(A)$.

Osservazione 2. Il viceversa della proposizione precedente è in generale falso. Otterremo in **Cap. III.5** un esempio di dominio d'integrità con un elemento irriducibile ma non primo.

Si noti che, per conformarci alla tradizione, abbiamo chiamato *numero primo* in $\boldsymbol{Z}$ ogni *elemento irriducibile* (e positivo) di $\boldsymbol{Z}$. Ma in effetti, in base al **Lemma 1**, elementi irriducibili ed elementi primi di $\boldsymbol{Z}$ si identificano. Come vedremo nel prossimo **Cap. III.2**, lo stesso è vero anche nell'anello dei polinomi $K[X]$.

Teorema 1. (*Teorema Fondamentale dell'Aritmetica* (in $\boldsymbol{N}$)).
(1) Ogni naturale $n \geq 2$ *è prodotto di un numero finito di numeri primi.*
(2) Se per ogni $n \geq 2$ *poniamo:*

$$n = p_1^{h_1} p_2^{h_2} \dots p_s^{h_s}\ ,\ \ con\ \begin{cases} s \geq 1 \\ p_1,\ \dots\ , p_s\ \ primi\ distinti \\ h_1,\ \dots\ , h_s \geq 1, \end{cases}$$

tale scrittura è unica a meno dell'ordine dei fattori.

Dim. (*1*) Per *induzione forte* su $n \geq 2$.

$\boldsymbol{n = 2}$ (base induttiva). Risulta: $2 = 2$ (2 è primo).

$\boldsymbol{n \geq 3}$. Assumiamo vero che ogni naturale h, tale che $2 \leq h < n$, sia prodotto di un numero finito di primi. Dimostriamo che lo stesso vale per n.

Se n è primo, non c'è nulla da dimostrare. Sia n non primo. Allora $n = ab$, con $1 < a, b < n$. Per ipotesi induttiva: $a = p_1 \dots p_s\,,\ b = p_{s+1} \dots p_t$. Si conclude che $p = ab = p_1 \dots p_s\, p_{s+1} \dots p_t$.

(*2*) Siano

$$n = p_1^{h_1} p_2^{h_2} \dots p_s^{h_s} = q_1^{k_1} q_2^{k_2} \dots q_t^{k_t}$$

due diverse espressioni di n come prodotto di primi distinti. Bisogna verificare che:

$$s = t; \quad \{p_1,\ \dots\ , p_s\} = \{q_1,\ \dots\ , q_t\}; \quad \text{se } p_i = q_j\,,\ h_i = k_j\,.$$

Per ogni $i = 1, \dots, s,\ p_i \,|\, n$. In base al **Cor. 1**, $p_i \,|\, q_j$ (e dunque $p_i = q_j$), $\exists j :\ 1 \leq j \leq t$. Ne segue che $\{p_1,\ \dots\ , p_s\} \subseteq \{q_1,\ \dots\ , q_t\}$. Si verifica in modo analogo l'inclusione opposta: dunque $\{p_1,\ \dots\ , p_s\} = \{q_1,\ \dots\ , q_t\}$ (e $s = t$).

Per semplificare le notazioni, assumiamo $p_i = q_i$ ($\forall\, i = 1, \dots, s$). Allora:

$$n = p_1^{h_1} p_2^{h_2} \dots p_s^{h_s} = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}\,.$$

Bisogna verificare che $h_i = k_i\,,\ \ \forall\, i = 1, \dots, s$. Se per assurdo fosse $h_1 > k_1$, allora, semplificando il fattore $p_1^{k_1}$, si avrebbe

$$p_1^{h_1 - k_1} p_2^{h_2} \dots p_s^{h_s} = p_2^{k_2} \dots p_s^{k_s}\,.$$

Dunque $p_1 \,|\, p_j$, $\exists\, j \neq 1$: assurdo. In modo analogo si verifica che $h_1 \not< k_1$ e dunque $h_1 = k_1$. Nello stesso modo si verifca che anche $h_2 = k_2, \ldots, h_s = k_s$.

Corollario 2. (*Teorema Fondamentale dell'Aritmetica* (in $\boldsymbol{Z}$)). *Sia* $a \in \boldsymbol{Z}$, $a \neq 0$, $a \neq \pm 1$. *L'intero* a *si scrive in modo unico (a meno dell'ordine dei fattori) nella forma*

$$a = \pm p_1^{h_1} p_2^{h_2} \ldots p_s^{h_s},$$

dove: $s \geq 1$, $p_1, \ldots, p_s$ *sono numeri primi distinti,* $h_1, \ldots, h_s \geq 1$, *e vale il segno* $+$ *se* $a \in \boldsymbol{Z}_+$, *vale il segno* $-$ *se* $a \in \boldsymbol{Z}_-$.

Dim. Basta applicare il precedente **Teor. 1** ad $|a|$.

Corollario 3. *Siano* $a, b \in \boldsymbol{Z}$, $a, b \neq 0, \pm 1$. *Se*

$$a = \pm p_1^{h_1} p_2^{h_2} \ldots p_s^{h_s}, \quad b = \pm p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$$

con $p_1, \ldots, p_s$ *numeri primi e* $h_i, k_i \geq 0$, *allora*

$$MCD(a,b) = p_1^{d_1} p_2^{d_2} \ldots p_s^{d_s}, \ \text{con } d_i := min\{h_i, k_i\} \quad (\forall\, i = 1, \ldots, s).$$

Nota. Si osservi che, avendo assunto $h_i, k_i \geq 0$, è stato possibile esprimere a, b come prodotto degli stessi primi [ad esempio, posto $a = 12$, $b = 15$, allora $a = 2^2 3^1 5^0$, $b = 2^0 3^1 5^1$].

Dim. Poniamo $d := p_1^{d_1} p_2^{d_2} \ldots p_s^{d_s}$. Dobbiamo verificare che $d = MCD(a,b)$.

Certamente $d \,\Big|\, \begin{matrix} a \\ b \end{matrix}$. Sia ora $d' \in \boldsymbol{Z}$ tale che $d' \,\Big|\, \begin{matrix} a \\ b \end{matrix}$. Allora $a = d't$, $b = d's$. Dunque

$$\begin{aligned} p_1^{h_1} \ldots p_s^{h_s} = d't &\implies d' = p_1^{r_1} \ldots p_s^{r_s}, \ \text{con } r_i \leq h_i, \\ p_1^{k_1} \ldots p_s^{k_s} = d's &\implies d' = p_1^{r_1} \ldots p_s^{r_s}, \ \text{con } r_i \leq k_i. \end{aligned}$$

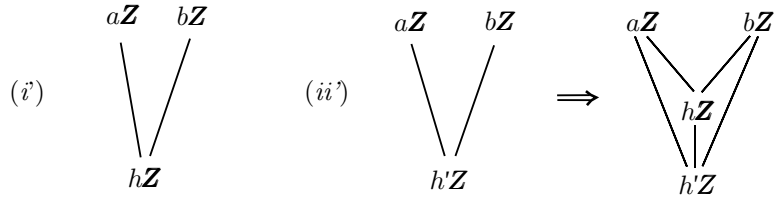
Ne segue che ogni $r_i \leq min\{h_i, k_i\} = d_i$. Dunque $d' \,|\, d$.

Osservazione 3. Il teorema Fondamentale dell'Aritmetica è conseguenza del teorema di esistenza del MCD: infatti la dimostrazione dell'unicità utilizza il **Lemma 1** (che è a sua volta un corollario dell'identità di Bézout e quindi del teorema di esistenza del MCD). Pertanto non è logicamente corretto assumere come *definizione* di MCD la *regola di calcolo* espressa nel precedente **Cor. 3**.

Definizione 3. *Siano* $a, b \in \boldsymbol{Z}$. *Si chiama minimo comune multiplo (abbreviato mcm) di* a, b *ogni eventuale intero* $h \geq 0$ *tale che*

$$(i) \ \begin{matrix} a \\ b \end{matrix} \Big| \, h; \qquad (ii) \ \begin{matrix} a \\ b \end{matrix} \Big| \, h' \implies h \,|\, h'.$$

Osservazione 4. Le precedenti condizioni (i) e (ii) possono essere visualizzate nella forma:



Da (ii) segue subito che $h\boldsymbol{Z} \supseteq ab\boldsymbol{Z}$ [infatti $\begin{matrix} a \\ b \end{matrix} \Big| \, ab$ e quindi $h \,|\, ab$]. Inoltre risulta:

$$h\boldsymbol{Z} = a\boldsymbol{Z} \cap b\boldsymbol{Z}.$$

Infatti: da (i'), $h\boldsymbol{Z} \subseteq a\boldsymbol{Z} \cap b\boldsymbol{Z}$; viceversa, se $t \in a\boldsymbol{Z} \cap b\boldsymbol{Z}$, allora $\begin{matrix} a \\ b \end{matrix} \Big| \, t$. Da (ii), $h \,|\, t$, cioè $t \in h\boldsymbol{Z}$; dunque $a\boldsymbol{Z} \cap b\boldsymbol{Z} \subseteq h\boldsymbol{Z}$.

Dalla precedente uguaglianza segue subito che $mcm(a,0) = 0$, $mcm(a, \pm 1) = |a|$. Infine, se

$h = mcm(a,b) = 0$, allora $a = 0$ o $b = 0$ [infatti, se fosse $ab \neq 0$, allora $h\boldsymbol{Z} \supseteq ab\boldsymbol{Z} \supset 0\boldsymbol{Z} = 0$].

Proposizione 2. *Siano* $a, b \in \boldsymbol{Z}$, $a, b \neq 0, \neq \pm 1$. *Se*

$$a = \pm p_1^{h_1} p_2^{h_2} \dots p_s^{h_s}, \quad b = \pm p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$$

con $h_i, k_i \geq 0$, *allora*

$$mcm(a,b) = p_1^{D_1} p_2^{D_2} \dots p_s^{D_s}, \ \text{con} \ D_i = max\{h_i, k_i\}.$$

Dim. Posto: $h := p_1^{D_1} p_2^{D_2} \dots p_s^{D_s}$, dobbiamo verificare che $h = mcm(a,b)$.

Certamente $\begin{matrix} a \\ b \end{matrix} \Big| h$. Sia ora $h' \in \boldsymbol{Z}$ tale che $\begin{matrix} a \\ b \end{matrix} \Big| h'$ e quindi $h' = at = bm$, $\exists\, t, m \in \boldsymbol{Z}$. Dunque

$$h' = at = \pm p_1^{h_1} p_2^{h_2} \dots p_s^{h_s}\, t, \quad h' = bm = \pm p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}\, m$$

e quindi, in base al teorema Fondamentale dell'Aritmetica, h' ammette come fattore $p_1^{D_1} \dots p_s^{D_s}$, cioè $h' = p_1^{D_1} \dots p_s^{D_s}\, n$, ovvero $h \,\big|\, h'$.

Corollario 4. *Siano* $a, b \in \boldsymbol{Z}$, *non entrambi nulli. Risulta:*

$$|ab| = MCD(a,b) \cdot mcm(a,b).$$

Dim. Assumiamo $a, b \neq 0, \pm 1$. In tal caso, siano

$$|a| = p_1^{h_1} \dots p_s^{h_s}, \quad |b| = p_1^{k_1} \dots p_s^{k_s}, \quad \text{con} \quad h_i, k_i \geq 0$$

Sia $d_i := min\{h_i, k_i\}$, $D_i := max\{h_i, k_i\}$. Allora $h_i + k_i = d_i + D_i$ e quindi:

$$|ab| = |a| \cdot |b| = p_1^{h_1+k_1} \dots p_s^{h_s+k_s} = p_1^{d_1+D_1} \dots p_s^{d_s+D_s} = \left(p_1^{d_1} \dots p_s^{d_s}\right) \cdot \left(p_1^{D_1} \dots p_s^{D_s}\right) =$$
$$= MCD(a,b) \cdot mcm(a,b).$$

Se $a = 0$ (e quindi $b \neq 0$), allora: $|ab| = 0$ e $MCD(0,b) \cdot mcm(0,b) = |b| \cdot 0 = 0$. Se $a = \pm 1$ (o $b = \pm 1$), allora: $|ab| = |b|$ e $MCD(\pm 1, b) \cdot mcm(\pm 1, b) = 1 \cdot |b| = |b|$. Si è quindi osservato che la formula è verificata in ogni caso.

Osservazione 5. L'unicità e l'esistenza del mcm seguono dalla formula della **Prop. 2** (una volta nota l'esistenza e l'unicità del MCD). La formula del **Cor. 4** consente ovviamente il calcolo immediato del mcm se è noto il MCD (e viceversa).

Proposizione 3 (*Euclide*). *Esistono infiniti numeri primi.*

Dim. Per assurdo, assumiamo che l'insieme $\boldsymbol{\mathcal{P}}$ dei numeri primi sia finito e poniamo

$$\boldsymbol{\mathcal{P}} = \{p_1, p_2, \dots, p_N\}.$$

Consideriamo il numero naturale $a := \left(\prod_{i=1}^{N} p_i\right) + 1$. Poiché $a \geq 2$, in base al **Teor. 1**, $\exists\, p_j \in \boldsymbol{\mathcal{P}}$ tale che $p_j \,\big|\, a$. Dunque $a = \left(\prod_{i=1}^{N} p_i\right) + 1 = p_j\, t$, da cui $1 = p_j\, t - \prod_{i=1}^{N} p_i = p_j \left(t - \prod_{i \neq j} p_i\right)$ e quindi $p_j \,\big|\, 1$: assurdo.

Proposizione 4 (*Pitagora*). *Per ogni primo* p, $\sqrt{p} \notin \boldsymbol{Q}$.

Dim. Per assurdo, sia $\sqrt{p} \in \boldsymbol{Q}$. Dunque $\sqrt{p} = \frac{r}{s}$, con $MCD(r,s) = 1$. Ne segue $p = \frac{r^2}{s^2}$ e quindi $r^2 = p\, s^2$. Applichiamo a tale intero il teorema Fondamentale dell'Aritmetica: il primo p ha esponente pari (perché r^2 è un quadrato) ma ha anche esponente dispari (perché s^2 è un quadrato). Segue un assurdo.

Concludiamo il paragrafo con due algoritmi: il *Crivello di Eratostene* ed il *metodo "standard" di*

fattorizzazione. Il primo serve a scrivere tutti i numeri primi $\leq n$ (naturale assegnato); il secondo fornisce un metodo per fattorizzare un naturale n come prodotto di primi.

Premettiamo il seguente lemma, che verrà utilizzato in entrambi gli algoritmi.

Lemma 2. *Sia n un numero naturale non primo, $n \geq 4$. n ammette un divisore positivo proprio $\leq [\sqrt{n}\,]$ [dove $[x]$ denota la parte intera di un numero reale $x > 0$; si tratta, come già osservato, del massimo intero $\leq x$].*

Dim. Sia $n = ab$, con $a, b \in \boldsymbol{N}$, tali che $2 \leq a, b < n$. Se $a \leq [\sqrt{n}\,]$, non c'è nulla da dimostrare. Se invece $a > [\sqrt{n}\,]$, risulta: $a - 1 \geq [\sqrt{n}\,] \implies a \geq 1 + [\sqrt{n}\,] > \sqrt{n} \implies a > \sqrt{n}$. Dunque: $n = ab > \sqrt{n}\, b \implies b < \frac{n}{\sqrt{n}} = \sqrt{n} \implies b \leq [\sqrt{n}\,]$.

CRIVELLO DI ERATOSTENE

Assegnato un naturale n, tale algoritmo permette di scrivere tutti i numeri primi $\leq n$. L'idea è semplicissima: si scrive la lista ordinata di tutti i naturali k tali che $2 \leq k \leq n$ e poi si cancellano da tale lista i numeri non primi. Descriviamo i passi dell'algoritmo:

1°. Si evidenzia il primo elemento della lista (cioè $k = 2$) e si cancellano dalla lista i suoi multipli.

2°. Nella lista rimasta si evidenzia il primo elemento non già evidenziato (cioè $k = 3$) e si cancellano dalla lista i suoi multipli.

3°. Si procede in modo analogo, evidenziando il primo elemento h non già evidenziato e cancellandone poi i multipli ancora presenti.

Il procedimento può essere interrotto non appena $h > [\sqrt{n}\,]$: i numeri rimasti nella lista (evidenziati o meno) sono tutti primi. Infatti, sia k un elemento presente nella lista, con $h \leq k \leq n$. In base al **Lemma 2**, se k non fosse primo, ammetterebbe un fattore $t \leq [\sqrt{k}\,]$. Poiché $[\sqrt{k}\,] \leq [\sqrt{n}\,] < h$, allora $t < h$ e dunque k sarebbe già stato eliminato, in quanto multiplo di t. Dunque k non è presente nella lista: assurdo. I primi cercati sono dunque tutti i numeri presenti nella lista rimasta.

A titolo d'esempio, cerchiamo i primi ≤ 41 $([\sqrt{41}\,] = 6)$.

②	③	~~4~~	⑤	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~
~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29
~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~	41		

I primi ≤ 41 sono: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41.

METODO "STANDARD" DI FATTORIZZAZIONE

Sia n un naturale ≥ 2. Vogliamo determinare tutti i primi $p_1 \leq p_2 \leq \ \ldots\ \leq p_N$ tali che $n = \prod_{i=1}^{N} p_i$. Procediamo con i seguenti passi:

1°. Si ponga $I_1 := \{k \in \boldsymbol{N} \ : \ 2 \leq k \leq [\sqrt{n}\,]\} = \boldsymbol{N} \cap \big[2, [\sqrt{n}\,]\big]$.

In base al **Lemma 2**, se nessun intero $k \in I_1$ è un divisore di n, allora n è primo e l'algoritmo termina a questo punto. Altrimenti, sia $k_1 \in I_1$ il minimo divisore di n. Si noti che k_1 è primo [altrimenti, se $t \,\big|\, k_1$, con $2 \leq t < k_1$, allora $t \,\big|\, k_1 \,\big|\, n$, e ciò contraddice la minimalità di k_1 come divisore di n]. Si ponga $n_1 := \frac{n}{k_1}$.

2°. Si ponga $I_2 := \{k \in \boldsymbol{N} \ : \ k_1 \leq k \leq [\sqrt{n_1}\,]\} = \boldsymbol{N} \cap \big[k_1, [\sqrt{n_1}\,]\big]$.

Se nessun intero $k \in I_2$ è un divisore di n_1, allora n_1 è primo [si noti che, $\forall\, h \ : \ 2 \leq h < k_1$, $h \not| n_1$ (altrimenti $h \,\big|\, n$, contro l'ipotesi di minimalità di k_1)]. In tal caso $n = k_1 n_1$ (prodotto di primi) e l'algoritmo termina a questo punto. Altrimenti, sia $k_2 \in I_2$ il minimo divisore di n_1. Si noti che

k_2 è primo [altrimenti k_2 avrebbe un divisore $t < k_1$; quindi $t \,|\, k_2 \,|\, n_1 \,|\, n$, contro la minimalità di k_1 come divisore di n]. Si ponga $n_2 := \frac{n_1}{k_2}$.

3°. Si procede in modo analogo: se $h \geq 3$, posto $I_h := \boldsymbol{N} \cap \big[k_{h-1}, [\sqrt{n_{h-1}}]\big]$, si cerca un eventuale minimo divisore k_h di n_{h-1}. Se tale divisore non esiste, n_{h-1} è primo e $n = k_1 k_2 \ldots k_{h-1} n_{h-1}$ (prodotto di primi cercato). Se invece k_h esiste, si costruisce l'intervallo I_{h+1}.

Si osserva che gli intervalli I_h si restringono al crescere di h. Dunque l'algoritmo termina in uno di questi due modi: o non esiste alcun divisore di n_{h-1} in I_h, ovvero $k_{h-1} \not\leq \sqrt{n_{h-1}}$, cioè $I_h = \emptyset$. Chiariamo queste due eventualità nei due esempi che seguono.

Esempio 1. Fattorizzare $n = 136$.

Risulta:

$$\begin{array}{llll} [\sqrt{136}] = 11 & I_1 = [2,11] \cap \boldsymbol{N} & k_1 = 2 & n_1 = \frac{136}{2} = 68 \\ [\sqrt{68}] = 8 & I_2 = [2,8] \cap \boldsymbol{N} & k_2 = 2 & n_2 = \frac{68}{2} = 34 \\ [\sqrt{34}] = 5 & I_3 = [2,5] \cap \boldsymbol{N} & k_3 = 2 & n_3 = \frac{34}{2} = 17 \\ [\sqrt{17}] = 4 & I_4 = [2,4] \cap \boldsymbol{N} & \nexists\, k_4. & \end{array}$$

Ne segue che $136 = 2{\cdot}2{\cdot}2{\cdot}17$.

Esempio 2. Fattorizzare $n = 210$.

Risulta:

$$\begin{array}{llll} [\sqrt{210}] = 14 & I_1 = [2,14] \cap \boldsymbol{N} & k_1 = 2 & n_1 = \frac{210}{2} = 105 \\ [\sqrt{105}] = 10 & I_2 = [2,10] \cap \boldsymbol{N} & k_2 = 3 & n_2 = \frac{105}{3} = 35 \\ [\sqrt{35}] = 5 & I_3 = [3,5] \cap \boldsymbol{N} & k_3 = 5 & n_3 = \frac{35}{5} = 7 \\ [\sqrt{7}] = 2 & I_4 = [5,2] \cap \boldsymbol{N} = \emptyset. & & \end{array}$$

Ne segue che $210 = 2{\cdot}3{\cdot}5{\cdot}7$.

Osservazione 6. Esistono altri (e decisamente più efficienti) algoritmi di fattorizzazione in primi di un numero naturale. Ne descriveremo due in un'appendice in fondo a questo capitolo. Si tratta del *metodo di fattorizzazione di Fermat* e del *metodo di fattorizzazione di Draim*.

4. Congruenze sugli interi

Definizione 1. *Sia* $n \geq 2$. *Si chiama relazione di congruenza modulo* n *la seguente relazione su* $\boldsymbol{Z}$. *Presi comunque* $a, b \in \boldsymbol{Z}$:

$$a \equiv b \ (mod\ n) \iff n \,|\, a - b.$$

Si dice in tal caso che a *è conguente (o congruo)* a b *modulo* n. *In luogo di* $a \equiv b \ (mod\ n)$ *si può anche scrivere* $a \equiv b \ (n)$ *oppure* $a \equiv_n b$.

Osservazione 1. $\equiv_n$ è una relazione di equivalenza su $\boldsymbol{Z}$. Risulta infatti:

- $a \equiv a \ (mod\ n), \ \forall\, a \in \boldsymbol{Z}$ [infatti $n \,|\, a - a = 0$];
- $a \equiv b \ (mod\ n) \implies b \equiv a \ (mod\ n)$ [infatti $n \,|\, a - b \implies n \,|\, b - a$];
- $a \equiv b \ (mod\ n), \ b \equiv c \ (mod\ n) \implies a \equiv c \ (mod\ n)$ [infatti $a - b = nr, \ b - c = ns$ (con $r, s \in \boldsymbol{Z}$) $\implies a - c = (a - b) + (b - c) = n(r + s) \implies n \,|\, a - c$].

Osservazione 2. La precedente definizione di congruenza può anche essere estesa ai casi $n = 1$, $n = 0$, $n < 0$. Si ha:

(a) $a \equiv b \ (mod\ 1) \iff 1 \,|\, a - b \iff a - b \in \boldsymbol{Z}$. Dunque $\equiv_1$ è la relazione caotica.

(b) $a \equiv b \ (mod\ 0) \iff 0 \,|\, a - b \iff a - b = 0$. Dunque $\equiv_0$ è la relazione identica.

(c) Sia $n < 0$. $a \equiv b \ (mod\ n) \iff n \,|\, a - b \iff |n| \,|\, a - b$. Dunque $\equiv_n$ coincide con $\equiv_{|n|}$.

Definizione 2. *L'insieme quoziente* $\boldsymbol{Z}/_{\equiv_n}$ *è detto insieme delle classi resto modulo* n. *E' denotato usualmente* $\boldsymbol{Z}_n$. *I suoi elementi sono detti classi resto modulo* n. *Per ogni* $a \in \boldsymbol{Z}$, *la classe resto di* a *modulo* n *è denotata* $\overline{a}$ *(oppure* $[a]$*). Risulta:*

$$\overline{a} = a + n\boldsymbol{Z} = \{a + nt, \ \forall\, t \in \boldsymbol{Z}\}.$$

Proposizione 1. *Risulta:*

$$a \equiv b \ (mod\ n) \iff a, b \text{ hanno lo stesso resto, se divisi per } n.$$

Ne segue:

$$\boldsymbol{Z}_n = \{\overline{0}, \overline{1}, \ ....\ , \overline{n-1}\}.$$

Dim. ($\implies$). Sia $a \equiv b \ (mod\ n)$ e quindi $a - b = nt, \ \exists\, t \in \boldsymbol{Z}$. Se

$$a = nq + r, \ 0 \leq r < n; \quad b = nq_1 + r_1, \ 0 \leq r_1 < n,$$

bisogna verificare che $r = r_1$. Da $0 \leq r < n, \ -n < -r_1 \leq 0$, segue, sommando membro a membro, che $-n < r - r_1 < n$. Si ha: $nt = a - b = n(q - q_1) + r - r_1$, da cui $r - r_1 = n(t - q + q_1)$. Dunque $n \,|\, r - r_1$. Da $n \,|\, r - r_1$ e $-n < r - r_1 < n$, segue che $r - r_1 = 0$.

($\Longleftarrow$). Sia $a = nq + r$ e $b = nq_1 + r$. Allora $a - b = n(q - q_1)$ e quindi $n \,|\, a - b$, cioè $a \equiv b \ (mod\ n)$.

L'ultima affermazione è ovvia. Infatti $\forall\, \overline{a} \in \boldsymbol{Z}_n$ risulta: $\overline{a} = \overline{r}$, se $a = nq + r, \ 0 \leq r < n$, ed i possibili resti della divisione per n sono $0, 1, \ ... \ , n - 1$.

Si noti ad esempio che $\overline{n} = \overline{0}$, $\overline{n+1} = \overline{1}$, $\overline{-1} = \overline{n-1}$, ecc..

Proposizione 2. *La relazione* $\equiv_n$ *è compatibile con le operazioni di somma e prodotto in* $\boldsymbol{Z}$. *Ne segue che* $(\boldsymbol{Z}_n, +, \cdot)$ *è un anello commutativo unitario.*

Dim. Siano $a \equiv a_1 \ (mod\ n)$ e $b \equiv b_1 \ (mod\ n)$. Bisogna verificare che:

$$a + b \equiv a_1 + b_1 \ (mod\ n) \quad \text{e} \quad a \cdot b \equiv a_1 \cdot b_1 \ (mod\ n)$$

Se infatti $a - a_1 = nt, \ b - b_1 = ns$, allora $a + b - (a_1 - b_1) = n(t + s)$ e dunque $a + b \equiv a_1 + b_1 \ (mod\ n)$. Inoltre:

$$a\cdot b - a_1\cdot b_1 = a\cdot b - a\cdot b_1 + a\cdot b_1 - a_1\cdot b_1 = a(b-b_1) + (a-a_1)b_1 = ans + ntb_1 = n(as+tb_1).$$

Dunque $a\cdot b \equiv a_1\cdot b_1 \ (mod\ n)$.

Sono quindi ben definite in $\boldsymbol{Z}_n$ le due operazioni:

$$\overline{a} + \overline{b} = \overline{a+b}, \quad \overline{a}\cdot\overline{b} = \overline{a\cdot b}, \quad \forall\, \overline{a},\, \overline{b} \in \boldsymbol{Z}_n.$$

Verifichiamo che $(\boldsymbol{Z}_n, +)$ è un gruppo commutativo. Si ha:

- $(\overline{a}+\overline{b})+\overline{c} = \overline{a}+(\overline{b}+\overline{c}), \quad \forall\, \overline{a},\, \overline{b},\, \overline{c} \in \boldsymbol{Z}_n;$
- $\overline{a}+\overline{0} = \overline{a} = \overline{0}+\overline{a}, \quad \forall\, \overline{a} \in \boldsymbol{Z}_n;$
- $\overline{a}+\overline{-a} = \overline{0} = \overline{-a}+\overline{a}, \quad \forall\, \overline{a} \in \boldsymbol{Z}_n;$
- $\overline{a}+\overline{b} = \overline{b}+\overline{a}, \quad \forall\, \overline{a},\, \overline{b} \in \boldsymbol{Z}_n.$

[Le verifiche sono lasciate per esercizio]. Valgono inoltre le seguenti proprietà [anch'esse lasciate per esercizio]:

- $(\overline{a}\cdot\overline{b})\cdot\overline{c} = \overline{a}\cdot(\overline{b}\cdot\overline{c}), \quad \forall\, \overline{a},\, \overline{b},\, \overline{c} \in \boldsymbol{Z}_n;$
- $\overline{a}\cdot(\overline{b}+\overline{c}) = \overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}, \quad (\overline{a}+\overline{b})\cdot\overline{c} = \overline{a}\cdot\overline{c}+\overline{b}\cdot\overline{c}, \quad \forall\, \overline{a},\, \overline{b},\, \overline{c} \in \boldsymbol{Z}_n;$
- $\overline{a}\cdot\overline{b} = \overline{b}\cdot\overline{a}, \quad \forall\, \overline{a},\, \overline{b} \in \boldsymbol{Z}_n.$
- $\overline{a}\cdot\overline{1} = \overline{a} = \overline{1}\cdot\overline{a}, \quad \forall\, \overline{a} \in \boldsymbol{Z}_n.$

Si conclude che $(\boldsymbol{Z}_n, +, \cdot)$ è un anello commutativo unitario.

Osservazione 3. In generale $\boldsymbol{Z}_n$ non è un dominio d'integrità. Ad esempio, in $\boldsymbol{Z}_4$, $\overline{2}\cdot\overline{2} = \overline{0}$ (e $\overline{2} \neq \overline{0}$). In generale non vale la legge di cancellazione. Ad esempio, ancora in $\boldsymbol{Z}_4$, $\overline{2}\cdot\overline{2} = \overline{2}\cdot\overline{0}$, ma $\overline{2} \neq \overline{0}$.

La legge di cancellazione vale però in qualche caso, come illustrato nella proposizione che segue.

Proposizione 3. *Sia $\overline{a}\cdot\overline{c} = \overline{b}\cdot\overline{c}$ in $\boldsymbol{Z}_n$. Se $(c,n) = 1$ allora $\overline{a} = \overline{b}$.*
[Nota. D'ora in poi useremo la notazione $(-,-)$ in luogo di $MCD(-,-)$.]

Dim. Risulta: $\overline{a}\cdot\overline{c} = \overline{b}\cdot\overline{c}$ in $\boldsymbol{Z}_n \iff ac \equiv bc \ (mod\ n) \iff (a-b)c \equiv 0 \ (mod\ n) \iff n \,\big|\, (a-b)c$. Da $n \,\big|\, (a-b)c$ e $(n,c) = 1$ segue (in base a *EU*) che $n \,\big|\, a-b$, cioè $\overline{a} = \overline{b}$ in $\boldsymbol{Z}_n$.

Cerchiamo gli elementi invertibili di $\boldsymbol{Z}_n$.

Proposizione 4. $\overline{a} \in \mathcal{U}(\boldsymbol{Z}_n) \iff (a,n) = 1$.

Dim. ($\Longrightarrow$). Sia $\overline{a} \in \mathcal{U}(\boldsymbol{Z}_n)$: $\overline{a}\cdot\overline{x} = \overline{1}$ ($\exists\, \overline{x} \in \boldsymbol{Z}_n$). Allora: $ax \equiv 1 \ (mod\ n) \implies n \,\big|\, ax-1 \implies ax - 1 = ns$ ($\exists\, \overline{s} \in \boldsymbol{Z}_n$) $\implies 1 = ax - ns \implies (a,n) = 1$ [cfr. **Osserv. 2.7**(*ii*)]

($\Longleftarrow$). Sia $(a,n) = 1$. Allora $1 \overset{Bez}{=} ar + ns$, $\exists\, r, s \in \boldsymbol{Z}$ e quindi $\overline{1} = \overline{a}\cdot\overline{r} + \overline{n}\cdot\overline{s} = \overline{a}\cdot\overline{r} + \overline{0} = \overline{a}\cdot\overline{r}$. Dunque $\overline{a} \in \mathcal{U}(\boldsymbol{Z}_n)$ (con $\overline{a}^{\,-1} = \overline{r}$).

Definizione 3. *Se $ar \equiv 1 \ (mod\ n)$ si dice che r è un inverso aritmetico di a modulo n.*
Da **Prop. 4** *segue ovviamente che un inverso aritmetico di a modulo n esiste $\iff (a,n) = 1$. Si verifica subito, in tal caso, che c'è un unico inverso aritmetico di a compreso tra 1 ed $n-1$. [Se infatti $ar \equiv 1 \equiv as \ (mod\ n)$ allora $n \,\big|\, r-s$ e quindi $r = s$, se $1 \leq r, s < n$].*

Corollario 1. *Sia $n \geq 2$. Le seguenti condizioni sono equivalenti:*

(i) $\boldsymbol{Z}_n$ *è un campo.*

(ii) $\boldsymbol{Z}_n$ *è un anello integro.*

(iii) n *è un numero primo.*

Dim. $(i) \Longrightarrow (ii)$ è ovvia.

$(ii) \Longrightarrow (iii)$. Per assurdo, n non sia primo. Dunque $n = ab$, con $2 \leq a, b < n$. Allora $\overline{0} = \overline{n} = \overline{a}\cdot\overline{b}$, con $\overline{a}, \overline{b} \neq \overline{0}$. Ma $\boldsymbol{Z}_n$ è integro: assurdo.

$(iii) \Longrightarrow (i)$. Poiché $\boldsymbol{Z}_n$ è un anello commutativo unitario, basta verificare che $\mathcal{U}(\boldsymbol{Z}_n) = \boldsymbol{Z}_n^{\cdot}$ (cfr. **Cap. I.4, Def. 7**).

Certo $\mathcal{U}(\boldsymbol{Z}_n) \subseteq \boldsymbol{Z}_n^{\cdot}$. Viceversa, $\forall\, \overline{a} \in \boldsymbol{Z}_n^{\cdot}$ risulta $a \not\equiv 0 \ (mod\ n)$ e quindi, essendo n primo, $(a, n) = 1$. Dalla **Prop. 4** segue che $\overline{a} \in \mathcal{U}(\boldsymbol{Z}_n)$.

Nota. Abbiamo ottenuto un'infinità di campi finiti: sono i campi $\boldsymbol{Z}_p$, $\forall\, p$ primo.

Osservazione 4. Si noti che se $a \equiv b \ (mod\ n)$, allora $a^t \equiv b^t \ (mod\ n)$, $\forall\, t \geq 1$.

Tale affermazione può essere facilmente verificata osservando che se (in $\boldsymbol{Z}_n$) $\overline{a} = \overline{b}$, allora $\overline{a}^{\,t} = \overline{b}^{\,t}$ e quindi $a^t \equiv b^t \ (mod\ n)$. Altrimenti, si verifichi che, $\forall\, t \geq 1$, $a - b \,\big|\, a^t - b^t$ [da cui: $n \,\big|\, a - b \Longrightarrow n \,\big|\, a^t - b^t$].

Della precedente **Osserv. 4** faremo ora uso per dimostrare alcuni ben noti **criteri di divisibilità**, rispetto ai seguenti naturali:

$$3,\ 9,\ 11,\ \text{potenze di } 2,\ \text{potenze di } 5,\ \text{potenze di } 10.$$

Poi dimostreremo un criterio di divisibilità rispetto ad un qualsiasi naturale $h \geq 2$.

Sia $n \in \boldsymbol{N}$; nel seguito assumeremo che

$$n = \sum_{k=0}^{t} a_k 10^k = \big(a_t,\, a_{t-1},\, \ldots.\, ,\, a_1,\, a_0\big)_{10}$$

siano rispettivamente l'espansione di n in somma di potenze di 10 e la scrittura decimale di n.

(A) **Criteri di divisibilità per 3 e per 9.**

Risulta: $n \equiv \sum_{k=0}^{t} a_k \ (mod\ 9)$ *e* $(mod\ 3)$. *Ne segue:*

$$9 \,\big|\, n \iff 9 \,\Big|\, \sum_{k=0}^{t} a_k \quad e \quad 3 \,\big|\, n \iff 3 \,\Big|\, \sum_{k=0}^{t} a_k\,.$$

Dim. Dimostriamo il risultato soltanto per $mod\ 9$ (per $mod\ 3$ è del tutto analogo). Risulta: $10 \equiv 1 \ (mod\ 9)$. Allora $10^k \equiv 1^k = 1 \ (mod\ 9)$ ($\forall\, k \geq 0$). Ne segue:

$$n = \sum_{k=0}^{t} a_k 10^k \equiv \sum_{k=0}^{t} a_k 1 = \sum_{k=0}^{t} a_k \ (mod\ 9).$$

Infine: $9 \,\big|\, n \iff n \equiv 0 \ (mod\ 9) \iff \sum_{k=0}^{t} a_k \equiv 0 \ (mod\ 9) \iff 9 \,\Big|\, \sum_{k=0}^{t} a_k\,.$

Corollario 2. *("La prova del nove"). Siano* $n_1, n_2 \in \boldsymbol{N}$, *con*

$$n_1 = \big(a_t,\, a_{t-1},\, \ldots.\, ,\, a_1,\, a_0\big)_{10}, \quad n_2 = \big(b_s,\, b_{s-1},\, \ldots.\, ,\, b_1,\, b_0\big)_{10}, \quad n_1 n_2 = \big(c_r,\, c_{r-1},\, \ldots.\, ,\, c_1,\, c_0\big)_{10}.$$

Allora:

$$\sum_{\ell=0}^{r} c_\ell \equiv \Big(\sum_{k=0}^{t} a_k\Big)\Big(\sum_{h=0}^{s} b_h\Big) \ \ (mod\ 9).$$

Dim. In base al criterio (A), si ha:

$$n_1 \equiv \sum_{k=0}^{t} a_k \ (mod\ 9), \quad n_2 \equiv \sum_{h=0}^{s} b_h \ (mod\ 9), \quad n_1\, n_2 \equiv \sum_{\ell=0}^{r} c_\ell \ (mod\ 9).$$

Poiché la relazione di congruenza è compatibile con il prodotto (cfr. **Prop. 2**), allora:

$$\sum_{\ell=0}^{r} c_\ell \equiv n_1 n_2 \equiv \Big(\sum_{k=0}^{t} a_k\Big)\Big(\sum_{h=0}^{s} b_h\Big) \ \ (mod\ 9).$$

Note. (i). Vale ovviamente anche la *prova del tre* [più debole].

(*ii*). La *prova del nove* vale anche relativamente all'addizione.

Corollario 3. *Per ogni* $n = \sum_{k=0}^{t} a_k 10^k \in \boldsymbol{N}$, *si ponga:* $\tilde{n} = \sum_{k=0}^{t} a_{t-k} 10^k$ *[ad esempio, se* $a = 1234$, $\tilde{a} = 4321$*; se* $b = 1230$, $\tilde{b} = 321$*]. Per ogni* $n \in \boldsymbol{N}$ *risulta:*

$$9 \,\big|\, \tilde{n} - n.$$

Dim. Risulta: $\tilde{n} - n = \sum_{k=0}^{t} (a_{t-k} - a_k) 10^k$. Inoltre $\sum_{k=0}^{t} (a_{t-k} - a_k) = \sum_{k=0}^{t} a_{t-k} - \sum_{k=0}^{t} a_k = 0$. Poiché

$$\tilde{n} - n \equiv \sum_{k=0}^{t} (a_{t-k} - a_k) = 0 \ (mod\ 9),$$

si conclude che $9 \,\big|\, \tilde{n} - n$.

(*B*) **Criterio di divisibilità per 11**.

Risulta: $n \equiv \sum_{k=0}^{t} (-1)^k a_k \ (mod\ 11)$. *Ne segue:*

$$11 \,\big|\, n \iff 11 \,\Big|\, \sum_{k=0}^{t} (-1)^k a_k .$$

Dim. Risulta: $10 \equiv -1 \ (mod\ 11)$. Ne segue $10^k \equiv (-1)^k$, $\forall\, k \geq 0$. Allora:

$$n = \sum_{k=0}^{t} a_k 10^k \equiv \sum_{k=0}^{t} a_k (-1)^k = \sum_{k=0}^{t} (-1)^k a_k \ (mod\ 11).$$

Infine: $11 \,\big|\, n \iff n \equiv 0 \ (mod\ 11) \iff \sum_{k=0}^{t} (-1)^k a_k \equiv 0 \ (mod\ 11) \iff 11 \,\Big|\, \sum_{k=0}^{t} (-1)^k a_k$.

(*C*) **Criteri di divisibilità per 2^s e per 5^s, $\forall\, s \geq 1$**.

Sia $n = \sum_{k=0}^{t} a_k 10^k$ *e sia* s *tale che* $1 \leq s \leq t$. *Risulta:*

$$2^s \,\big|\, n \iff \big(a_{s-1},\ ....\ , a_1,\ a_0\big)_{10} \equiv 0 \ (mod\ 2^s); \quad 5^s \,\big|\, n \iff \big(a_{s-1},\ ....\ , a_1,\ a_0\big)_{10} \equiv 0 \ (mod\ 5^s).$$

Dim. Dimostriamo il risultato soltanto per $mod\ 2^s$ (per $mod\ 5^s$ è del tutto analogo). Si osserva subito che $2^s \,\big|\, 10^k$, $\forall\, k \geq s$ e dunque $10^k \equiv 0 \ (mod\ 2^s)$, $\forall\, k \geq s$. Se quindi $1 \leq s \leq t$:

$$n = \big(a_0 + \ ... \ + a_{s-1} 10^{s-1}\big) + \big(a_s 10^s + \ ... \ + a_t 10^t\big) \equiv a_0 + \ ... \ + a_{s-1} 10^{s-1} + 0 + \ ... \ + 0 \ \ (mod\ 2^s).$$

Allora: $2^s \,\big|\, n \iff n \equiv 0 \ (mod\ 2^s) \iff \sum_{k=0}^{s-1} a_k 10^k \equiv 0 \ (mod\ 2^s) \iff 2^s \,\Big|\, \sum_{k=0}^{s-1} a_k 10^k \iff$

$$\iff 2^s \,\big|\, \big(a_{s-1},\ ....\ , a_1,\ a_0\big)_{10}.$$

Nota. I primi casi del precedente criterio sono ben noti:

$2 \,\big|\, n \iff a_0$ è pari;

$4 \,\big|\, n \iff a_1 a_0$ è un multiplo di $4 \iff a_1 a_0 = 00,\ 04,\ 08,\ 12,\ ...\ ,\ 92,\ 96$;

$5 \,\big|\, n \iff a_0 = 0,\ 5$;

$25 \,\big|\, n \iff a_1 a_0 = 00,\ 25,\ 50,\ 75$.

(*D*) **Criterio di divisibilità per 10^s, $\forall\, s \geq 1$**.

Sia $n = \sum_{k=0}^{t} a_k 10^k$ *e sia* s *tale che* $1 \leq s \leq t$. *Risulta:*

$$10^s \,\big|\, n \iff a_{s-1} = \ .... \ = a_0 = 0.$$

Dim. Ovviamente $10^k \equiv 0 \ (mod\ 10^s)$, $\forall\, k \geq s$. Allora

$$n \equiv a_0 + \ ... \ + a_{s-1} 10^{s-1} = \big(a_{s-1},\ ....\ , a_1,\ a_0\big)_{10} \ (mod\ 10^s).$$

Pertanto: $10^s \,|\, n \iff n \equiv 0 \ (mod\ 10^s) \iff \left(a_{s-1},\ \ldots.\ ,\ a_1,\ a_0\right)_{10} \equiv 0 \ (mod\ 10^s) \iff$

$\iff \left(a_{s-1},\ \ldots.\ ,\ a_1,\ a_0\right)_{10} = 0$ [perché $\left(a_{s-1},\ \ldots.\ ,\ a_1,\ a_0\right)_{10} < 10^s$] $\iff a_{s-1} = \ldots. = a_0 = 0.$

Il seguente risultato, dovuto a Pascal (1654), fornisce un criterio di divisibilità rispetto ad un qualsiasi naturale $h \geq 2$.

Proposizione 4. *Sia* $n = \sum_{k=0}^{t} a_k 10^k$ *e sia* $h \geq 2$. *Supponiamo che:*

$$10 \equiv r_1 \ (mod\ h) \quad e \quad 10\, r_{k-1} \equiv r_k \ (mod\ h), \quad \forall\, k = 2, \ldots, t.$$

Allora: $h \,|\, n \iff h \,|\, \sum_{k=0}^{t} a_k r_k$ *[con* $r_0 = 1$*].*

Dim. Dalle ipotesi:

$$\begin{aligned} &10^2 \equiv 10\, r_1 \equiv r_2 \ (mod\ h),\\ &10^3 \equiv 10\, r_2 \equiv r_3 \ (mod\ h),\\ &\ldots\\ &10^t \equiv 10\, r_{t-1} \equiv r_t \ (mod\ h). \end{aligned}$$

Ne segue che [avendo posto $r_0 = 1$]:

$$n = \sum_{k=0}^{t} a_k 10^k \equiv a_0 + \sum_{k=1}^{t} a_k\, r_k = \sum_{k=0}^{t} a_k r_k \ (mod\ h).$$

Pertanto: $h \,|\, n \iff n \equiv 0 \ (mod\ h) \iff \sum_{k=0}^{t} a_k r_k \equiv 0 \ (mod\ h) \iff h \,|\, \sum_{k=0}^{t} a_k r_k$.

Ad esempio, posto $n = 1925$ ed $h = 7$, si osserva facilmente che $h \,|\, n$. Infatti risulta:

$$r_1 = 3,\ r_2 = 2,\ r_3 = 6, \ \text{quindi} \ \sum_{k=0}^{t} a_k r_k = 5 + 2{\cdot}3 + 2{\cdot}9 + 1{\cdot}6 = 35 \ \text{ e } \ 7 \,|\, 35.$$

Concludiamo il paragrafo con una classica caratterizzazione dei numeri primi, che fornisce un *"test di primalità"*, cioè un criterio per riconoscere se un numero naturale n è primo.

Teorema 1. (*Teorema di Wilson, 1770*). *Sia* $n \geq 2$. *Risulta:*

$$n \text{ è primo} \iff (n-1)! \equiv -1 \ (mod\ n).$$

Dim. ($\Longleftarrow$). Per ipotesi, $n \,|\, 1 + (n-1)!$ Per assurdo, n non sia primo. Allora $\exists\, c \in \boldsymbol{N}$ tale che $1 < c < n$ e $c \,|\, n$. Quindi $c \,|\, 1 + (n-1)!$, cioè $1 + (n-1)! = ch$, $\exists\, h \in \boldsymbol{N}$. Poiché $(n-1)! = 2{\cdot}\ldots.{\cdot}c{\cdot}\ldots{\cdot}(n-1)$, allora $1 = ch - (n-1)! = ch - 2{\cdot}\ldots.{\cdot}c{\cdot}\ldots{\cdot}(n-1) = ck$, $\exists\, k \in \boldsymbol{N}$. Quindi $c \,|\, 1$: assurdo. Pertanto n è primo.

($\Longrightarrow$). Sia $n := p$ un numero primo. Bisogna dimostrare che $(p-1)! \equiv -1 \ (mod\ p)$.

Se $p = 2, 3$, la tesi è di immediata verifica. Assumiamo $p \geq 5$. Per ottenere la tesi, basta dimostrare che $(p-2)! \equiv 1 \ (mod\ p)$ [infatti ne segue subito che $(p-1)! = (p-1)(p-2)! \equiv p - 1 \equiv -1 \ (mod\ p)$]. Dimostriamo quindi che $\overline{2}{\cdot}\overline{3}\ldots.{\cdot}\overline{p-2} = \overline{1}$ (in $\boldsymbol{Z}_p$). Poniamo

$$\boldsymbol{H} = \{\overline{2},\ \overline{3},\ \ldots.\ ,\ \overline{p-2}\}.$$

Ovviamente $\boldsymbol{H}$ è formato da un numero pari di classi (diciamo $2t$), ciascuna delle quali è invertibile. Per ogni $\overline{a} \in \boldsymbol{H}$, consideriamone l'inversa $\overline{a}^{-1}$. Osserviamo che $\overline{1}^{-1} = \overline{1}$ e che $\overline{p-1}^{-1} = \overline{p-1}$ [infatti $(p-1)(p-1) = p^2 - 2p + 1 \equiv 1 \ (mod\ p)$]: ne segue (per l'unicità dell'inverso) che $\overline{a}^{-1} \in \boldsymbol{H}$. Ora verifichiamo che $\overline{a}^{-1} \neq \overline{a}$, $\forall\, \overline{a} \in \boldsymbol{H}$.

Se infatti per assurdo fosse $\overline{a}^{-1} = \overline{a}$, allora $a^2 \equiv 1 \ (mod\ p)$ e dunque $p \,|\, (a-1)(a+1)$. Se $p \,|\, a - 1$, allora $a - 1 = pt$ e $2 \leq a \leq p - 2$, da cui $1 \leq a - 1 \leq p - 3$, cioè $1 \leq pt < p - 3$: escluso.

Se invece $p \mid a+1$, allora $a+1 = ps$ e $2 \leq a \leq p-2$, da cui $3 \leq a+1 \leq p-1$, cioè $3 \leq ps \leq p-1$: escluso. Dunque p divide un prodotto ma nessuno dei due fattori: assurdo.

Concludiamo che gli elementi di $\boldsymbol{H}$ possono essere ripartiti in t insiemi $\{\overline{a}_i, \overline{b}_i\}$, ciascuno formato da un elemento $\overline{a}_i$ e dal suo inverso $\overline{b}_i = \overline{a}_i^{-1}$. Si ha quindi:

$$\overline{2}\cdot\overline{3}\,....\cdot\overline{p-2} = \overline{a}_1\cdot\overline{b}_1\cdot\overline{a}_2\cdot\overline{b}_2\cdot\ ....\ \cdot a_t\cdot\overline{b}_t = \overline{1}\cdot\overline{1}\cdot\ ....\ \cdot\overline{1} = \overline{1}^{\,t} = \overline{1}\ \ (\text{in } \boldsymbol{Z}_p).$$

5. Equazioni congruenziali lineari

Definizione 1. *Si chiama equazione congruenziale lineare modulo n un'equazione del tipo*

$$aX \equiv b \ (mod\ n) \quad [\text{ovvero, più brevemente, } \ aX \equiv b \ (n)\,],$$

con $a, b \in \boldsymbol{Z}$, $n \geq 2$ ed $a \notin n\boldsymbol{Z}$. Una sua soluzione [se esiste] è un intero x tale che $ax \equiv b \ (mod\ n)$. Un'equazione congruenziale lineare è detta compatibile se ammette una soluzione; altrimenti è detta incompatibile. È evidente che se x è una soluzione, anche $x + nh$ ($\forall\, h \in \boldsymbol{Z}$) è una soluzione della stessa equazione.

Si noti che ogni equazione congruenziale lineare $aX \equiv b \ (mod\ n)$ si trasforma in modo naturale nell'equazione lineare $\overline{a}X = \overline{b}$, con coefficienti in $\boldsymbol{Z}_n$. Ovviamente, x è soluzione dell'equazione $aX \equiv b \ (mod\ n) \iff \overline{x}$ è soluzione dell'equazione $\overline{a}X = \overline{b}$.

Proposizione 1. *L'equazione $aX \equiv b \ (mod\ n)$ è compatibile $\iff (a, n) \,|\, b$.*

Dim. $aX \equiv b \ (mod\ n)$ è compatibile $\iff \exists\, x \in \boldsymbol{Z}$ tale che $ax \equiv b \ (n) \iff \exists\, x, y \in \boldsymbol{Z}$ tali che $ax - b = ny \iff$ l'equazione $aX - nY = b$ ammette una soluzione intera (cioè in $\boldsymbol{Z}\times\boldsymbol{Z}$).

Per concludere basta allora dimostrare il seguente lemma.

Lemma 1. *L'equazione $aX - nY = b$ ammette soluzioni in $\boldsymbol{Z}\times\boldsymbol{Z} \iff (a, n) \,|\, b$.*

Dim. (**Lemma 1**). Si ponga $d := (a, n)$.

($\Longrightarrow$). Sia $(x, y) \in \boldsymbol{Z}\times\boldsymbol{Z}$ tale che $ax - ny = b$. Da $d \,\Big|\, \begin{matrix} a \\ n \end{matrix}$ segue che $d \,|\, ax - ny = b$.

($\Longleftarrow$). Supponiamo che $d = (a, n) \overset{Bez}{=} ar + ns$. Per ipotesi $d \,|\, b$, cioè $b = db_1$, $\exists\, b_1 \in \boldsymbol{Z}$. Allora $b = db_1 = arb_1 + nsb_1$. Ne segue che $(rb_1, -sb_1)$ è una soluzione intera di $aX - nY = b$.

Osservazione 1. Sia $aX \equiv b \ (n)$, con $d := (a, n) \,|\, b$. Tale equazione è compatibile (in base a **Prop. 1**). Una sua soluzione si ottiene schematicamente con questa procedura:

$$\begin{aligned} &d = (a, n) \overset{Bez}{=} ar + ns; \\ &d \,|\, b \implies b = db_1; \\ &b = db_1 = ab_1r + nb_1s \equiv a(b_1r) \ (mod\ n). \end{aligned}$$

Dunque $x = b_1r$ è una soluzione dell'equazione.

Definizione 2. *Siano $aX \equiv b \ (mod\ n)$ e $a_1X \equiv b_1 \ (mod\ n_1)$ due equazioni congruenziali lineari. Tali equazioni sono dette equivalenti $\iff$ hanno le stesse soluzioni $\iff$ $\big[\ \forall\, x \in \boldsymbol{Z}$, risulta: $n \,|\, ax - b \iff n_1 \,|\, a_1x - b_1\big]$.*

Proposizione 2. *(i) Se $(a, n) = 1$, l'equazione $aX \equiv b \ (mod\ n)$ è equivalente a $X \equiv ba' \ (mod\ n)$, con a' inverso aritmetico di a $(mod\ n)$.*

(ii) Se l'equazione $aX \equiv b \ (mod\ n)$ è compatibile, essa è equivalente a $\frac{a}{d}X \equiv \frac{b}{d} \ (mod\ \frac{n}{d})$, con $d = (a, n)$.

Dim. (*i*) Essendo $aa' \equiv 1 \ (mod\ n)$, risulta $1 = aa' + nr$, $\exists\, r \in \boldsymbol{Z}$. Bisogna verificare che $n \,|\, ax - b \iff n \,|\, x - ba'$, $\forall\, x \in \boldsymbol{Z}$.

($\Longrightarrow$). $n \,|\, ax - b \implies ax - b = ns \implies aa'x - ba' = a'ns \implies (1 - nr)x - ba' = a'ns \implies$
$\implies x - ba' = n(rx + a's) \implies n \,|\, x - ba'$.

($\Longleftarrow$). $n \,|\, x - ba' \implies x - ba' = nt \implies ax - aba' = ant \implies ax - (1 - nr)b = ant \implies$

$\implies ax - b = n(at - rb) \implies n \,|\, ax - b.$

(*ii*) Se $n \,|\, ax-b$, allora $\frac{n}{d} \,|\, \frac{a}{d}\, x - \frac{b}{d}$ (essendo $\frac{n}{d},\ \frac{a}{d},\ \frac{b}{d} \in \boldsymbol{Z}$). Viceversa, se $\frac{n}{d} \,|\, \frac{a}{d}\, x - \frac{b}{d}$, moltiplicando per d si ottiene $n \,|\, ax - b$.

Proposizione 3. *(i) Sia $aX \equiv b\ (mod\ n)$ un'equazione congruenziale lineare compatibile (e quindi $d := (a, n) \,|\, b$) e sia x_0 una sua soluzione. Si ha:*

(1) $x_0 + \frac{n}{d}h$ è una soluzione, $\forall\, h \in \boldsymbol{Z}$.

(2) Ogni soluzione è del tipo $x_0 + \frac{n}{d}h$ (per un opportuno $h \in \boldsymbol{Z}$).

(3) Se $h_1, h_2 \in \boldsymbol{Z}$ sono tali che $0 \le h_1 \ne h_2 < d$, le due soluzioni $x_0 + \frac{n}{d}h_1$ e $x_0 + \frac{n}{d}h_2$ non sono congruenti $(mod\ n)$.

(4) Per ogni $h \in \boldsymbol{Z}$, $\exists!\, r$ tale che $0 \le r < d$ e $x_0 + \frac{n}{d}h \equiv x_0 + \frac{n}{d}r\ (mod\ n)$.

Dai punti precedenti segue che un insieme "massimale" (cioè non estendibile) di soluzioni a due a due non congruenti dell'equazione $aX \equiv b\ (mod\ n)$ è dato da:

$$\left\{x_0,\ x_0 + \tfrac{n}{d},\ x_0 + 2\tfrac{n}{d},\ \ \dots\ ,\ x_0 + (d-1)\tfrac{n}{d}\right\}.$$

Un tale insieme di soluzioni è detto sistema completo di soluzioni dell'equazione $aX \equiv b\ (mod\ n)$.

Le corrispondenti classi resto forniscono l'insieme di tutte le d soluzioni (a due a due distinte) dell'equazione lineare $\overline{a}X = \overline{b}$ in $\boldsymbol{Z}_n$.

Dim. (*1*) Osservato che $\frac{a}{d} \in \boldsymbol{Z}$, $a(x_0 + \frac{n}{d}h) = ax_0 + a\frac{n}{d}h = ax_0 + \frac{a}{d}\, nh \equiv ax_0 \equiv b\ (mod\ n)$. Dunque $x_0 + \frac{n}{d}h$ è una soluzione di $aX \equiv b\ (mod\ n)$.

(*2*) Sia x una soluzione: $ax \equiv b\ (mod\ n)$. Allora $a(x - x_0) \equiv b - b \equiv 0\ (mod\ n)$. Quindi: $n \,|\, a(x - x_0)$, da cui $\frac{n}{d} \,|\, \frac{a}{d}(x - x_0)$. Poiché $\left(\frac{n}{d},\ \frac{a}{d}\right) = 1$, dal Lemma di Euclide $\frac{n}{d} \,|\, x - x_0$. Allora $x - x_0 = \frac{n}{d}h$, $\exists\, h \in \boldsymbol{Z}$, da cui $x = x_0 + \frac{n}{d}h$.

(*3*) Essendo $0 \le h_1 \ne h_2 < d$, allora: $0 \le h_1 < d$, $-d < -h_2 \le 0$ e quindi, sommando membro a membro, $-d < h_1 - h_2 < d$. Poiché inoltre $h_1 - h_2 \ne 0$, allora $d \nmid h_1 - h_2$.

Se per assurdo $x_0 + \frac{n}{d}h_1 \equiv x_0 + \frac{n}{d}h_2\ (mod\ n)$, allora $n \,|\, \frac{n}{d}(h_1 - h_2)$, cioè $n(h_1 - h_2) = nds$, da cui $h_1 - h_2 = ds$, cioè $d \,|\, h_1 - h_2$: assurdo.

(*4*) Sia $h = dq + r$, con $0 \le r < d$. Allora: $x_0 + \frac{n}{d}h = x_0 + \frac{n}{d}(dq + r) = x_0 + nq + \frac{n}{d}r \equiv x_0 + \frac{n}{d}r\ (mod\ n)$. L'unicità di r discende da (*3*).

Osservazione 2. Per risolvere un'equazione congruenziale lineare compatibile $aX \equiv b\ (mod\ n)$, si può procedere seguendo due vie diverse:

(*A*): utilizzando i due risultati della **Prop. 2**. In tal modo l'equazione assegnata viene trasformata in un'equazione del tipo $X \equiv b'\ (mod\ n')$, la cui generica soluzione è data dall'insieme $b' + n'\boldsymbol{Z}$.

(*B*): utilizzando l'**Osserv. 1** per determinare una soluzione. Si usa poi la formula di **Prop. 3** per scrivere un sistema completo di soluzioni.

Come messo in luce dall'esempio che segue, le soluzioni ottenute con i due procedimenti possono presentarsi in forma diversa, ma in realtà "globalmente" si tratta delle stesse soluzioni.

Esempio 1. Risolvere l'equazione $15X \equiv 12\ (mod\ 21)$.

Poiché $3 = (15, 21) \,|\, 12$, l'equazione è compatibile. Ne otterremo le soluzioni seguendo i due metodi (*A*) e (*B*).

(*A*) L'equazione data è equivalente a $5X \equiv 4\ (mod\ 7)$. Un inverso aritmetico di 5 $(mod\ 7)$ è 3 [infatti $5 \cdot 3 \equiv 1\ (mod\ 7)$]. Allora $5X \equiv 4\ (mod\ 7)$ è equivalente a $X \equiv 4 \cdot 3\ (mod\ 7)$, cioè $X \equiv 5\ (mod\ 7)$ Pertanto le soluzioni sono date dall'insieme

$$5 + 7\boldsymbol{Z} = \{5 + 7h,\ \ \forall\, h \in \boldsymbol{Z}\}.$$

(*B*) Risulta:

$$3 = (15, 21) \overset{Bez}{=} 15 \cdot 3 + 21 \cdot (-2),$$
$$3 \,|\, 12 \quad [12 = 3 \cdot 4],$$

$$12 = 15\cdot 12 + 21\cdot(-8) \equiv 15\cdot 12 \ (mod\ 21).$$

Una soluzione è quindi $x_0 = 12$. Un sistema completo di soluzioni è quindi

$$\{12,\ 12+\tfrac{21}{3},\ 12+2\tfrac{21}{3}\} = \{12,\ 19,\ 26\}_{\equiv_{21}} = \{12,\ 19,\ 5\}.$$

Le soluzioni sono pertanto date dall'unione dei tre insiemi:

$$\big(5+21\boldsymbol{Z}\big)\cup\big(12+21\boldsymbol{Z}\big)\cup\big(19+21\boldsymbol{Z}\big) \qquad [=5+7\boldsymbol{Z}\,].$$

Veniamo ora allo studio di *sistemi* di equazioni congruenziali lineari, della forma:

$$(*) \qquad \begin{cases} a_1X \equiv b_1\ (mod\ n_1) \\ a_2X \equiv b_2\ (mod\ n_2) \\ : \\ a_sX \equiv b_s\ (mod\ n_s). \end{cases}$$

Un tale sistema è detto *compatibile* se esiste $x \in \boldsymbol{Z}$ tale che $\begin{cases} a_ix \equiv b_i\ (mod\ n_i) \\ \forall\, i = 1,\ ...\ ,\ s\ . \end{cases}$

Osservazione 3. Se il sistema $(*)$ è compatibile, ogni singola equazione deve esserlo. Allora $(a_i, n_i)\,\big|\,b_i$, $\forall\, i = 1,\ ...\ ,\ s$. Il viceversa è però falso: ad esempio il sistema

$$\begin{cases} 2X \equiv 4\ (mod\ 6) \\ 2X \equiv 2\ (mod\ 6) \end{cases}$$

è formato da due equazioni compatibili ma non è compatibile [altrimenti si avrebbe, per transitività, $4 \equiv 2\ (mod\ 6)$]. Dimostreremo che se le singole equazioni sono compatibili e se i moduli n_i sono a due a due coprimi, allora il sistema è compatibile. Ma prima di dimostrare tale risultato (cfr. **Teor. 2**), dobbiamo introdurre e risolvere sistemi di equazioni congruenziali particolari, detti *sistemi "cinesi"*.

Definizione 3. *Un sistema cinese di s equazioni congruenziali lineari è un sistema del tipo:*

$$(**) \qquad \begin{cases} X \equiv c_1\ (mod\ r_1) \\ X \equiv c_2\ (mod\ r_2) \\ : \\ X \equiv c_s\ (mod\ r_s), \end{cases} \qquad \textit{con } r_1,\ ...\ ,\ r_s \textit{ a due a due coprimi.}$$

Teorema 1. (*Teorema Cinese del resto* - 1^a **formulazione**). *Ogni sistema cinese $(**)$ è compatibile ed ha un'unica soluzione $(mod\ r_1r_2...\ r_s)$.*

Dim. (*Unicità della soluzione*). Siano x, y due soluzioni del sistema $(**)$: va dimostrato che $x \equiv y\ (mod\ r_1r_2...\ r_s)$.

Da $\begin{cases} x \equiv c_i \equiv y\ (r_i) \\ \forall\, i = 1,\ ...,\ s, \end{cases}$ segue che $r_i\,\big|\,x-y$, $\forall\, i = 1,\ ...,\ s$. In particolare, $r_1\big|\,x-y$ e dunque $x-y = r_1t_1$. In base a EU, da $r_2\big|\,x-y = r_1t_1$ e $(r_1, r_2) = 1$, segue: $r_2\big|\,t_1 \implies t_1 = r_2t_2 \implies x-y = r_1r_2t_2$. Ancora in base a EU, da $r_3\big|\,x-y = r_1r_2t_2$ e $(r_1r_2, r_3) = 1$ [cfr. **Eserc. 2.1**], segue: $r_3\big|\,t_2 \implies t_2 = r_3t_3 \implies x-y = r_1r_2r_3t_3$.

Proseguendo in questo modo si conclude che $x-y = r_1r_2\ ....\ r_s\ t_s$, cioè $x \equiv y\ (mod\ r_1r_2...\ r_s)$.

(*Esistenza della soluzione*). Non è restrittivo assumere che risulti $0 \le c_i < r_i$, $\forall\, i = 1, ..., s$. In tal caso la s-pla $(c_1,\ ...\ , c_s)$ appartiene ad un insieme di cardinalità $n := \prod_{i=1}^{s} r_i$.

Per ogni intero k tale che $0 \le k < n$, $\exists!\, k_i \in \boldsymbol{Z}$ tale che $k_i \equiv k\ (mod\ r_i)$ e $0 \le k_i < r_i$. L'intero k definisce quindi la s-pla $\tilde{k} = (k_1,\ ...\ , k_s)$. Si verifica subito che se $\tilde{k} = \tilde{k'}$, allora $k = k'$. Infatti, essendo $k \equiv k_i = k'_i \equiv k'\ (mod\ r_i)$, allora [con la stessa dimostrazione svolta per l'unicità] $k \equiv k'\ (mod\ n)$ e dunque [essendo $0 \le k,\, k' < n$] $k = k'$.

Le s-ple $\tilde{k}$ sono quindi a due a due distinte e sono complessivamente n. Tra esse c'è anche la s-pla $(c_1, \dots, c_s)$. Dunque k è soluzione del sistema $(**)$, se $\tilde{k} = (c_1, \dots, c_s)$.

La precedente dimostrazione non è costruttiva. Vogliamo quindi fornire un metodo per il calcolo della soluzione per sistemi cinesi. Per semplicità ci limitiamo però ad illustrare il procedimento per sistemi di 2 o 3 equazioni.

(a) È assegnato il sistema cinese di due equazioni

$$(\bullet) \qquad \begin{cases} X \equiv c_1 \ (mod\ r_1) \\ X \equiv c_2 \ (mod\ r_2), \end{cases} \qquad \text{con} \ \ (r_1, r_2) = 1.$$

Associamo a $(\bullet)$ i due seguenti sistemi cinesi:

$$(\circ) \quad \begin{cases} X \equiv 1 \ (mod\ r_1) \\ X \equiv 0 \ (mod\ r_2), \end{cases} \qquad (\circ\circ) \quad \begin{cases} X \equiv 0 \ (mod\ r_1) \\ X \equiv 1 \ (mod\ r_2). \end{cases}$$

Da $1 = (r_1, r_2) \overset{Bez}{=} ar_1 + br_2$, segue subito che:

- br_2 è una soluzione di $(\circ)$: infatti $\begin{cases} br_2 \equiv 1 \ (mod\ r_1) \\ br_2 \equiv 0 \ (mod\ r_2), \end{cases}$
- ar_1 è una soluzione di $(\circ\circ)$: infatti $\begin{cases} ar_1 \equiv 0 \ (mod\ r_1) \\ ar_1 \equiv 1 \ (mod\ r_2). \end{cases}$

Consideriamo ora l'intero $x = c_1(br_2) + c_2(ar_1)$. Verifichiamo che x è soluzione di $(\bullet)$. Infatti:

$$\begin{cases} x \equiv c_1 br_2 \equiv c_1 \cdot 1 = c_1 \ (mod\ r_1) \\ x \equiv c_2 ar_1 \equiv c_2 \cdot 1 = c_2 \ (mod\ r_2). \end{cases}$$

Abbiamo così dimostrato che $(\bullet)$ ammette una soluzione.

(b) È assegnato il sistema cinese di tre equazioni

$$(\bullet\bullet) \qquad \begin{cases} X \equiv c_1 \ (mod\ r_1) \\ X \equiv c_2 \ (mod\ r_2) \\ X \equiv c_3 \ (mod\ r_3), \end{cases} \qquad \text{con} \ \ (r_1, r_2) = (r_1, r_3) = (r_2, r_3) = 1.$$

Gli associamo i tre seguenti sistemi cinesi:

$$(\circ) \quad \begin{cases} X \equiv 1 \ (mod\ r_1) \\ X \equiv 0 \ (mod\ r_2) \\ X \equiv 0 \ (mod\ r_3), \end{cases} \qquad (\circ\circ) \quad \begin{cases} X \equiv 0 \ (mod\ r_1) \\ X \equiv 1 \ (mod\ r_2) \\ X \equiv 0 \ (mod\ r_3), \end{cases} \qquad (\circ\circ\circ) \quad \begin{cases} X \equiv 0 \ (mod\ r_1) \\ X \equiv 0 \ (mod\ r_2) \\ X \equiv 1 \ (mod\ r_3). \end{cases}$$

Da $1 = (r_1, r_2 r_3) \overset{Bez}{=} r_1 \cdot a_1 + r_2 r_3 \cdot b_1$, segue che $b_1 r_2 r_3$ è soluzione di $(\circ)$.
Da $1 = (r_2, r_1 r_3) \overset{Bez}{=} r_2 \cdot a_2 + r_1 r_3 \cdot b_2$, segue che $b_2 r_1 r_3$ è soluzione di $(\circ\circ)$.
Da $1 = (r_3, r_1 r_2) \overset{Bez}{=} r_3 \cdot a_3 + r_1 r_2 \cdot b_3$, segue che $b_3 r_1 r_2$ è soluzione di $(\circ\circ\circ)$.
Posto allora $x = c_1 b_1 r_2 r_3 + c_2 b_2 r_1 r_3 + c_3 b_3 r_1 r_2$, si verifica che x è una soluzione del sistema $(\bullet\bullet)$.

Osservazione 4. Per risolvere il sistema cinese $(**)$ si può procedere seguendo due vie diverse.

(A) Si segue l'idea sviluppata nei precedenti algoritmi: calcolate le identità di Bézout

$$\begin{aligned} 1 &= (r_1, r_2 r_3 \dots r_s) = a_1 \cdot r_1 + b_1 \cdot r_2 r_3 \dots r_s, \\ 1 &= (r_2, r_1 r_3 \dots r_s) = a_2 \cdot r_2 + b_2 \cdot r_1 r_3 \dots r_s, \\ &\vdots \\ 1 &= (r_s, r_1 r_2 \dots r_{s-1}) = a_s \cdot r_s + b_s \cdot r_1 r_3 \dots r_{s-1}, \end{aligned}$$

allora $x := \sum_{i=1}^{s} c_i b_i r_1 \dots \not{r_i} \dots r_s$ è l'unica soluzione di (**).

(B) Si consideri la generica soluzione della prima equazione: $x = c_1 + r_1 t_1, \ \forall t_1 \in \boldsymbol{Z}$. La si sostituisce nella seconda equazione, ottenendo l'equazione $c_1 + r_1 t_1 \equiv c_2 \ (r_2)$ [nell'incognita t_1]. Si risolve tale congruenza, ottenendo $t_1 = d_1 + r_2 t_2, \ \forall t_2 \in \boldsymbol{Z}$. La si inserisce nella precedente espressione di x, ottenendo $x = c_1 + r_1 d_1 + r_1 r_2 t_2$.

Si sostituisce tale espressione nella terza equazione del sistema, si risolve l'equazione [in t_2] e si inserisce la generica soluzione $t_2 = d_2 + t_3 r_3$ nell'ultima espressione di x, ottenendo $x = c_1 + r_1 d_1 + r_1 r_2 t_2 + r_1 r_2 r_3 t_3$.

Procedendo in tal modo, dopo un numero finito di passi si ottiene l'unica soluzione del sistema.

Esempio 2. Risolvere il seguente sistema cinese:

$$\begin{cases} X \equiv 3\ (5) \\ X \equiv 4\ (7) \\ X \equiv 4\ (11). \end{cases}$$

Si noti che $(5,7) = (5,11) = (7,11) = 1$. Dunque i moduli sono a due a due coprimi e quindi il sistema è compatibile. Ne otterremo le soluzioni seguendo i due metodi (A) e (B).

(A) Si ha:

$$1 = (5,77) \overset{Bez}{=} 5\cdot 31 + 77\cdot(-2) = 5\cdot 31 + (-154),$$
$$1 = (7,55) \overset{Bez}{=} 7\cdot 8 + 55\cdot(-1) = 7\cdot 8 + (-55),$$
$$1 = (11,35) \overset{Bez}{=} 11\cdot 16 + 35\cdot(-5) = 11\cdot 16 + (-175).$$

Allora: $x = 3(-154)+4(-55)+4(-175) = -1382$. Poiché $-1382 \equiv 158\ (mod\ 385)$, l'unica soluzione del sistema è $x = 158\ (mod\ 385)$.

(B) La prima equazione ha generica soluzione $x = 3 + 5t_1$. Inserendo tale valore nella seconda equazione: $3 + 5t_1 \equiv 4\ (7) \implies 5t_1 \equiv 1\ (7) \implies t_1 \equiv 3\ (7) \implies t_1 = 3 + 7t_2$. Allora

$$x = 3 + 5(3 + 7t_2) = 18 + 35t_2.$$

Inserendo tale valore nella terza equazione: $18 + 35t_2 \equiv 4\ (11) \implies 7 + 2t_2 \equiv 4\ (11) \implies 2t_2 \equiv 8\ (11) \implies t_2 \equiv 48\ (11) \implies t_2 \equiv 4\ (11) \implies t_2 = 4 + 11t_3$. Allora

$$x = 18 + 35t_2 = 18 + 35(4 + 11t_3) = 158 + 385t_3.$$

L'unica soluzione del sistema è quindi, come prima, $x = 158\ (mod\ 385)$.

Torniamo ora al più generale problema della risoluzione di un sistema di tipo (*), con moduli a due a due coprimi (cfr. **Osserv. 3**).

Teorema 2. *Assegnato il sistema di equazioni congruenziali lineari*

$$(*) \qquad \begin{cases} a_1 X \equiv b_1\ (mod\ n_1) \\ : \\ a_s X \equiv b_s\ (mod\ n_s), \end{cases}$$

con $d_i := (a_i, b_i) \,\big|\, b_i$, $\forall\, i = 1, \ldots s$, *e con* $(n_i, n_j) = 1$, $\forall\, i \neq j$, *tale sistema è equivalente ad un sistema cinese del tipo:*

$$(**) \qquad \begin{cases} X \equiv c_1\ (mod\ n_1') \\ : \\ X \equiv c_s\ (mod\ n_s'), \end{cases}$$

con $n_i' := \frac{n_i}{d_i}$, $\forall\, i = 1, \ldots s$. *Ne segue che* $(*)$ *ha un'unica soluzione* $mod\ \prod_{i=1}^{s} n_i'$.

Dim. Dalla **Prop. 2**(ii) segue che $a_i X \equiv b_i\ (n_i)$ è equivalente a $\frac{a_i}{d_i} X \equiv \frac{b_i}{d_i}\ \left(mod\ \frac{n_i}{d_i}\right)$. Dunque $(*)$ è equivalente al sistema

$$(\bullet) \qquad \begin{cases} \frac{a_i}{d_i} X \equiv \frac{b_i}{d_i}\ \left(mod\ \frac{n_i}{d_i}\right) \\ \forall\, i = 1, \ldots s. \end{cases}$$

Poiché $\left(\frac{a_i}{d_i}, \frac{n_i}{d_i}\right) = 1$, esiste un inverso aritmetico di $\frac{a_i}{d_i}\ mod\ \frac{n_i}{d_i}$, che denotiamo α_i. Dalla **Prop. 2**(i) segue che $(\bullet)$ è equivalente al sistema

$$(\bullet\bullet) \qquad \begin{cases} X \equiv \frac{b_i}{d_i}\,\alpha_i\ (mod\ n_i') \\ \forall\, i = 1, \ldots s, \end{cases}$$

che è il sistema cinese $(**)$ cercato.

Esempio 3. Risolvere il seguente sistema di equazioni congruenziali lineari:

$$\begin{cases} 6X \equiv 8\ (10) \\ 9X \equiv 15\ (21) \\ 2X \equiv 8\ (11). \end{cases}$$

Si noti che $(10,21) = (10,11) = (21,11) = 1$ e che $(6,10) \,|\, 8,\ (9,21) \,|\, 1,\ (2,11) \,|\, 8.$ Pertanto il sistema assegnato è compatibile ed è equivalente ad un sistema cinese. Si ha:

$6X \equiv 8\ (10)$ è equivalente a $3X \equiv 4\ (5)$ e $9X \equiv 15\ (21)$ è equivalente a $3X \equiv 5\ (7)$. Dunque il sistema assegnato è equivalente a

$$\begin{cases} 3X \equiv 4\ (5) \\ 3X \equiv 5\ (7) \\ 2X \equiv 8\ (11). \end{cases}$$

Poiché $3{\cdot}2 \equiv 1\ (5),\ 3{\cdot}5 \equiv 1\ (7),\ 2{\cdot}6 \equiv 1\ (11),$ allora il sistema diventa equivalente al sistema cinese

$$\begin{cases} X \equiv 8\ (5) \\ X \equiv 4\ (7) \\ X \equiv 4\ (11). \end{cases}$$

A questo punto va risolto il sistema. Ma lo abbiamo già fatto nel precedente **Esempio 2**. L'unica soluzione del sistema asegnato è quindi $x = 158\ (mod\ 385)$.

Cosa si può dire sulla compatibilità di un sistema a moduli non coprimi? In generale non è compatibile. Vale il seguente risultato relativo ad un sistema "di tipo cinese" di due equazioni.

Proposizione 4. *Dato il sistema di due equazioni*

$$(\bullet) \qquad \begin{cases} X \equiv a\ (mod\ n) \\ X \equiv b\ (mod\ m), \end{cases} \qquad con\ \ d := (m,n),$$

risulta: $(\bullet)$ *è compatibile* $\iff d \,|\, a-b.$

In tal caso ha un'unica soluzione modulo $mcm(m,n)$.

Dim. $(\bullet)$ è compatibile $\iff \exists\, x \in \boldsymbol{Z} : \begin{cases} n \,|\, x-a, \\ m \,|\, x-b \end{cases} \iff \exists\, x,t,s \in \boldsymbol{Z} : \begin{cases} x-a = tn, \\ x-b = ms \end{cases} \iff$

$\iff \exists\, t,s \in \boldsymbol{Z} : a-b = sm-tn \iff$ l'equazione $mX-nY = a-b$ ha una soluzione in $\boldsymbol{Z}\times\boldsymbol{Z} \iff$

$\iff$ [cfr. **Lemma 1**] $(m,n) \,|\, a-b \iff d \,|\, a-b.$

Sia ora $(\bullet)$ compatibile e siano $x,\ y$ due sue soluzioni. Allora

$$\begin{cases} x \equiv a\ (n) \\ x \equiv b\ (m), \end{cases} \quad \begin{cases} y \equiv a\ (n) \\ y \equiv b\ (m), \end{cases} \quad \text{da cui} \quad \begin{cases} x \equiv y\ (n) \\ x \equiv y\ (m), \end{cases}$$

cioè $\begin{matrix} n \\ m \end{matrix} \Big| x-y.$ Allora $mcm(m,n) \,|\, x-y,$ cioè $x \equiv y\ \big(mod\ mcm(m,n)\big).$

Esempio 4. Verificare che il sistema $\begin{cases} X \equiv 3\ (mod\ 10) \\ X \equiv 5\ (mod\ 6) \end{cases}$ è compatibile e calcolarne l'unica soluzione $(mod\ 30)$.

Si ha: $(10,6) = 2 \,|\, 3-5.$ Dunque il sistema è compatibile. Dalla prima equazione: $x = 3+10t.$ Sostituendo nella seconda: $3+10t \equiv 5\ (6) \implies 4t \equiv 2\ (6) \implies 2t \equiv 1\ (3) \implies t \equiv 2\ (3) \implies t = 2+3s.$ Allora $x = 3+10(2+3s) = 23+30s.$ L'unica soluzione è $x = 23\ (mod\ 30).$

Veniamo ora ad una diversa formulazione del teorema cinese del resto. Occorre premettere una

definizione.

Definizione 4. *Siano* $(A, +, \cdot)$ *e* $(B, +, \cdot)$ *due anelli [c. u.]. Sul prodotto cartesiano* $A \times B$ *si introduce una struttura di anello [c. u.], con le seguenti operazioni:*

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2), \quad (a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2).$$

Si verifica facilmente che $(A \times B, +, \cdot)$ *è un anello [c. u.], detto prodotto diretto di* A, B. *In modo analogo si definisce il prodotto diretto* $A_1 \times A_2 \times \ldots \times A_n$ *di* n *anelli* $A_1, A_2, \ldots, A_n$.

Teorema 3. (*Teorema Cinese del resto - 2ª* **formulazione**). *Se* r, s *sono interi relativamente primi, sussiste l'isomorfismo di anelli*

$$\boldsymbol{Z}_{rs} \cong \boldsymbol{Z}_r \times \boldsymbol{Z}_s .$$

Tale risultato può essere formulato in modo più completo, in questo modo:

Siano $r, s \geq 2$. *Risulta:*

(1) L'applicazione $F : \boldsymbol{Z}_{rs} \to \boldsymbol{Z}_r \times \boldsymbol{Z}_s$ *tale che* $F(\overline{x}) = \left(\overline{x}_r, \overline{x}_s\right)$, $\forall\, \overline{x} \in \boldsymbol{Z}_{rs}$, *è un omomorfismo di anelli [con* $\overline{x}_r$ *(rispett.* $\overline{x}_s$*) si è denotata la classe resto di* x $(mod\, r)$ *(rispett.* $(mod\, s)$*)].*

(2) Sono condizioni equivalenti:

(i) F *è biiettiva (cioè un isomorfismo di anelli).*

(ii) $(r, s) = 1$.

(iii) ogni sistema di equazioni congruenziali del tipo

$$\begin{cases} X \equiv a \ (mod\, r) \\ X \equiv b \ (mod\, s) \end{cases}$$

ammette una ed una sola soluzione $(mod\, rs)$.

Dim. (*1*) Verifichiamo che F è ben definita, cioè che: $\overline{x} = \overline{y}$ (in $\boldsymbol{Z}_{rs}$) $\implies F(\overline{x}) = F(\overline{y})$.

Infatti, se $rs \,\big|\, x - y$, allora $\begin{matrix} r \\ s \end{matrix} \,\Big|\, x - y$ e quindi $\overline{x}_r = \overline{y}_r$, $\overline{x}_s = \overline{y}_s$, cioè $F(\overline{x}) = F(\overline{y})$.

Verifichiamo ora che F è un omomorfismo di anelli. Si ha infatti:

$$F(\overline{x} + \overline{y}) = F(\overline{x + y}) = \left(\overline{x + y}_{\,r}, \overline{x + y}_{\,s}\right) = \left(\overline{x}_r + \overline{y}_r, \overline{x}_s + \overline{y}_s\right) = F(\overline{x}) + F(\overline{y})$$

ed in modo analogo si verifica che $F(\overline{x} \cdot \overline{y}) = F(\overline{x}) \cdot F(\overline{y})$.

(*2*) Osserviamo preliminarmente che $|\boldsymbol{Z}_{rs}| = rs = |\boldsymbol{Z}_r \times \boldsymbol{Z}_s|$. Ne segue che F è biiettiva $\iff$ F è iniettiva $\iff$ F è suriettiva.

(*i*) $\implies$ (*ii*). Per assurdo, sia $d := (r, s) > 1$. Posto $h := mcm(r, s)$, allora $h = \frac{rs}{d}$ e $1 \leq h < rs$. Ne segue che $\overline{h} \neq \overline{0}$, in $\boldsymbol{Z}_{rs}$. Poiché $\begin{matrix} r \\ s \end{matrix} \,\Big|\, h$, allora $\overline{h}_r = \overline{0}_r$, $\overline{h}_s = \overline{0}_s$ e quindi $F(\overline{h}) = (\overline{0}_r, \overline{0}_s)$. Poiché ovviamente anche $F(\overline{0}) = (\overline{0}_r, \overline{0}_s)$, allora F non è iniettiva: assurdo.

(*ii*) $\implies$ (*iii*). È il teorema cinese del resto nella 1ª formulazione, relativo a sistemi di due equazioni.

(*iii*) $\implies$ (*i*). Basta dimostrare che F è suriettiva. Per ogni $\left(\overline{a}_r, \overline{b}_s\right) \in \boldsymbol{Z}_r \times \boldsymbol{Z}_s$, si consideri il sistema

$$\begin{cases} X \equiv a \ (mod\, r) \\ X \equiv b \ (mod\, s). \end{cases}$$

Per ipotesi tale sistema ammette una soluzione x $(mod\, rs)$. Si ha: $F(\overline{x}) = \left(\overline{x}_r, \overline{x}_s\right) = \left(\overline{a}_r, \overline{b}_s\right)$. Dunque F è suriettiva.

Corollario 1. *Se* $r_1, \ldots, r_t$, *sono interi a due a due coprimi, risulta:*

$$\boldsymbol{Z}_{r_1 \cdots r_t} \cong \boldsymbol{Z}_{r_1} \times \ .... \ \times \boldsymbol{Z}_{r_t} .$$

Tale risultato viene riformulato in questo modo:

Siano $r_1, \ldots, r_t \geq 2$. *Risulta:*

(1) L'applicazione $F : \boldsymbol{Z}_{r_1 \cdots r_t} \to \boldsymbol{Z}_{r_1} \times \ .... \ \times \boldsymbol{Z}_{r_t}$ *tale che* $F(\overline{x}) = \left(\overline{x}_{r_1}, \ldots, \overline{x}_{r_t}\right)$, $\forall\, \overline{x} \in \boldsymbol{Z}_{r_1 \cdots r_t}$, *è un omomorfismo di anelli.*

(2) Sono condizioni equivalenti:

(i) F *è biiettiva (cioè un isomorfismo di anelli).*

(ii) $r_1, \dots, r_t$, *sono a due a due coprimi.*

(iii) ogni sistema di equazioni congruenziali del tipo

$$\begin{cases} X \equiv a_i \ (mod\, r_i) \\ \forall\, i = 1, \dots t \end{cases}$$

ammette una ed una sola soluzione $(mod \prod_{i=1}^{t} r_i)$.

Dim. La dimostrazione di *(1)* è esattamente la stessa del **Teorema 3**. Le implicazioni $(ii) \Longrightarrow (iii)$ e $(iii) \Longrightarrow (i)$ sono del tutto analoghe a quelle dimostrate nello stesso teorema.

$(i) \Longrightarrow (ii)$. Assumiamo, per assurdo, che, ad esempio, $d := (r_1, r_2) > 1$. Allora $h := mcm(r_1, r_2) < r_1 r_2$. Ne segue che, posto $x := h\, r_3 \dots r_t$, risulta $\overline{x} \neq \overline{0}$ in $\boldsymbol{Z}_{r_1 \cdots r_t}$ e $r_i \,\big|\, x$, $\forall\, i = 1, \dots, t$. Allora $\overline{x}_{r_i} = \overline{0}$ in $\boldsymbol{Z}_{r_i}$ e dunque $F(\overline{x}) = F\overline{0})$. Ciò contraddice l'iniettività di F.

Osservazione 6. Il teorema cinese del resto, nella sua formulazione $\boldsymbol{Z}_{rs} \cong \boldsymbol{Z}_r \times \boldsymbol{Z}_s$, se $(r, s) = 1$, si presta a semplificare vari calcoli aritmetici.

Ad esempio, vogliamo calcolare le ultime due cifre di $n = 827^{\,7}$.

Poiché le ultime due cifre di n sono il resto della divisione di n per 100, basta calcolare una soluzione in $[0, 99]$ della congruenza $X \equiv 827^{\,7}\ (mod\, 100)$.

Sussiste un isomorfismo $F : \boldsymbol{Z}_{100} \longrightarrow \boldsymbol{Z}_4 \times \boldsymbol{Z}_{25}$. Allora

$$F(\overline{827}) = \left(\overline{827}_4, \overline{827}_{25}\right) = \left(\overline{3}_4, \overline{2}_{25}\right) \text{ e quindi } F(\overline{827^{\,7}}) = F(\overline{827}^{\,7}) = \left(\overline{827}_4, \overline{827}_{25}\right)^7 = \left(\overline{3}_4^7, \overline{2}_{25}^7\right).$$

Si ha:

$$3^7 = 3 \cdot 3^3 \cdot 3^3 = 3 \cdot 27 \cdot 27 \equiv 3 \cdot 3 \cdot 3 \equiv 3\ (mod\, 4), \quad 2^7 = 4 \cdot 32 \equiv 4 \cdot 7 = 28 \equiv 3\ (mod\, 25)$$

e dunque $F(\overline{827}^{\,7}) = \left(\overline{3}_4, \overline{3}_{25}\right)$.

Sia ora $\overline{x} \in \boldsymbol{Z}_{100}$ tale che $F(\overline{x}) = \left(\overline{3}_4, \overline{3}_{25}\right)$. Per ottenere $\overline{x}$ basta risolvere il sistema cinese

$$\begin{cases} X \equiv 3\ (mod\, 4) \\ X \equiv 3\ (mod\, 25). \end{cases}$$

Si ha: $x = 3 + 25t \implies 3 + 25t \equiv 3\ (4) \implies 25t \equiv 0\ (4) \implies t \equiv 0\ (4) \implies t = 4s$. Allora $x = 3 + 100s$. Pertanto $827^{\,7} \equiv 3\ (mod\, 100)$. Le ultime due cifre di $827^{\,7}$ sono $0, 3$.

6. Piccolo teorema di Fermat. Il teorema di Eulero-Fermat

Teorema 1. *(Piccolo Teorema di Fermat (1640) -* 1^a **formulazione***) [abbr.* PTF_1*]. Sia* p *un numero primo. Risulta, per ogni* $a \in \boldsymbol{Z}$*,*

$$a^p \equiv a \ (mod\ p).$$

La dimostrazione fa uso del seguente lemma.

Lemma 1. *Sia* p *un numero primo. Per ogni* $x, y \in \boldsymbol{Z}$*:*

$$(x+y)^p \equiv x^p + y^p \ (mod\ p).$$

Dim. (Lemma 1). Si noti che, se p è primo, $p \,\big|\, \binom{p}{k}$, $\forall\, k = 1, \dots, p-1$. Si ha quindi:

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k + y^p = x^p + y^p + p(\ \dots\ ) \equiv x^p + y^p \ (mod\ p).$$

Dim. (PTF_1). Distinguiamo due casi: $a \geq 0$, $\quad a < 0$.

$\boldsymbol{a \geq 0}$. Per induzione su a.

Base induttiva: sia $a = 0$. $0^p \equiv 0 \ (mod\ p)$ è ovvio.

Passo induttivo: sia $a \geq 0$ ed assumiamo che $a^p \equiv a \ (mod\ p)$. Dimostriamo che $(a+1)^p \equiv a+1 \ (mod\ p)$. Si ha, per il lemma e l'ipotesi induttiva: $(a+1)^p \equiv a^p + 1^p \equiv a+1 \ (mod\ p)$.

$\boldsymbol{a < 0}$. Poiché $-a > 0$, $(-a)^p \equiv -a \ (mod\ p)$. Si ha (dal lemma e dal caso precedente):

$$0 = 0^p = \big(a + (-a)\big)^p \equiv a^p + (-a)^p \equiv a^p + (-a) \ (mod\ p), \text{ cioè } a \equiv a^p \ (mod\ p).$$

Corollario 1. (*Piccolo Teorema di Fermat -* 2^a **formulazione**) [abbr. PTF_2]. *Siano* $a, p \in \boldsymbol{Z}$*, con* $(a,p) = 1$*. Se* p *è primo, risulta:*

$$a^{p-1} \equiv 1 \ (mod\ p).$$

[Dunque $\overline{a}^{\,p-1} = \overline{1}$, $\forall\, \overline{a} \in \boldsymbol{Z}_p^{\cdot}$*].*

Dim. Dal PTF_1, $a^p \equiv a \ (mod\ p)$, cioè $p \,\big|\, a^p - a = a(a^{p-1} - 1)$. Poiché $(p,a) = 1$, segue da EU che $p \,\big|\, a^{p-1} - 1$, cioè $a^{p-1} \equiv 1 \ (mod\ p)$.

Osservazione 1. Se p non è primo, la conclusione del PTF (in entrambe le formulazioni) è in generale falsa. Ad esempio, se $p = 4$ ed $a = 3$, risulta: $a^{p-1} \not\equiv 1$, $a^p \not\equiv a \ (mod\ 4)$.

Anche il viceversa del PTF è falso: ad esempio risulta: $5^{4-1} \equiv 1 \ (mod\ 4)$, ma 4 non è primo.

Osservazione 2. In forma contrappositiva, il PTF_2 può enunciarsi in questo modo:

Siano $a, n \in \boldsymbol{Z}$*, con* $(a,n) = 1$*. Se* $a^{n-1} \not\equiv 1 \ (mod\ n)$*, allora* n *non è primo.*

Questa formulazione è utile come "*test di non primalità*". Supponiamo infatti di voler sapere se un naturale n è o non è primo. Si può ovviamente assumere n dispari e $n \geq 3$.

Si può scegliere come base $a = 2$. Se $2^{n-1} \not\equiv 1 \ (mod\ n)$, allora n non è primo; se invece $2^{n-1} \equiv 1 \ (mod\ n)$, non si può decidere nulla.

Si scelga in tal caso come base il più piccolo numero primo successivo a 2 e relativamente primo con n: dunque $a = 3$ (se $(3,n) = 1$). Se $3^{n-1} \not\equiv 1 \ (mod\ n)$, n non è primo. Se invece $3^{n-1} \equiv 1 \ (mod\ n)$, non si può concludere nulla, ma si può scegliere $a = 5$ (se $(5,n) = 1$) e verificare se $5^{n-1} \equiv 1 \ (mod\ n)$.

[Si noti che è inutile verificare se $4^{n-1} \equiv 1 \ (mod\ n)$. Infatti $4^{n-1} = 2^{n-1} \cdot 2^{n-1}$ ed, essendo $2^{n-1} \equiv 1 \ (mod\ n)$, allora $4^{n-1} \equiv 1 \ (mod\ n)$. Da ciò segue che è inutile scegliere come base a un numero non primo].

Il procedimento sopra descritto ovviamente non può aver termine se n è primo.

Si noti infine che per calcolare $a^{n-1}\ (mod\ n)$ conviene procedere in questo modo:

- si scrive l'intero $n-1$ come somma di potenze decrescenti di 2 (cfr. **Osserv. 2.8**):

$$n-1 = 2^{k_1} + 2^{k_2} + \ ...\ + 2^{k_s}, \text{ con } k_1 > k_2 > \ ...\ > k_s \geq 1 \text{ [si osservi che } n-1 \text{ è pari].}$$

- si calcolano $(mod\ n)$ le potenze $a = a^{2^0}, a^{2^1}, a^{2^2}, \ ...\ , a^{2^{k_1}}$, nell'ordine indicato, tenendo conto del fatto che $a^{2^i} \equiv (a^{2^{i-1}})^2\ (mod\ n)$.

A questo punto, si utilizza il fatto che $a^{n-1} = \left(a^{2^{k_1}}\right)\cdot\left(a^{2^{k_2}}\right)\cdot\ ...\ \cdot\left(a^{2^{k_s}}\right)$ e si riduce tale uguaglianza *modulo* n.

Esempio 1. Vogliamo verificare che $n = 341$ non è primo.

Risulta: $n-1 = 340 = 2^8 + 2^6 + 2^4 + 2^2$. Scelta come base $a = 2$, si ha:

$$\begin{aligned}
&2^{2^0} = 2 \equiv 2\ (mod\ 341),\\
&2^{2^1} \equiv (2)^2 \equiv 4\ (mod\ 341),\\
&2^{2^2} \equiv (4)^2 \equiv 16\ (mod\ 341),\\
&2^{2^3} \equiv (16)^2 \equiv 256\ (mod\ 341),\\
&2^{2^4} \equiv (256)^2 \equiv 64\ (mod\ 341),\\
&2^{2^5} \equiv (64)^2 \equiv 4\ (mod\ 341),\\
&2^{2^6} \equiv (4)^2 \equiv 16\ (mod\ 341),\\
&2^{2^7} \equiv (16)^2 \equiv 256\ (mod\ 341),\\
&2^{2^8} \equiv (256)^2 \equiv 64\ (mod\ 341).
\end{aligned}$$

Ne segue che $2^{340} = 2^{2^8}\cdot 2^{2^6}\cdot 2^{2^4}\cdot 2^{2^2} \equiv 64\cdot 16\cdot 64\cdot 16 = 16^2\cdot 64^2 \equiv 256\cdot 4 = 1024 \equiv 1\ (mod\ 341)$.

Nulla si può quindi decidere sulla "non primalità" di 341, ma si può passare alla base $a = 3$. Si ha:

$$\begin{aligned}
&3^{2^0} = 3 \equiv 3\ (mod\ 341),\\
&3^{2^1} \equiv (3)^2 \equiv 9\ (mod\ 341),\\
&3^{2^2} \equiv (9)^2 \equiv 81\ (mod\ 341),\\
&3^{2^3} \equiv (81)^2 \equiv 82\ (mod\ 341),\\
&3^{2^4} \equiv (82)^2 \equiv 245\ (mod\ 341),\\
&3^{2^5} \equiv (245)^2 \equiv 9\ (mod\ 341),\\
&3^{2^6} \equiv (9)^2 \equiv 81\ (mod\ 341),\\
&3^{2^7} \equiv (81)^2 \equiv 82\ (mod\ 341),\\
&3^{2^8} \equiv (82)^2 \equiv 245\ (mod\ 341).
\end{aligned}$$

Ne segue che $3^{340} = 3^{2^8}\cdot 3^{2^6}\cdot 3^{2^4}\cdot 3^{2^2} \equiv 245\cdot 81\cdot 245\cdot 81 \equiv 56\ (mod\ 341)$. Poiché $3^{340} \not\equiv 1\ (mod\ 341)$, allora 341 non è primo. [In effetti sappiamo che $11 \,|\, 343$. Dunque $341 = 11\cdot 31$].

Ora descriveremo un risultato analogo al PTF_2, ma valido *modulo* un naturale n non necessariamente primo: è il *teorema di Eulero-Fermat* (cfr. **Teorema 2**). Premettiamo la definizione di *funzione di Eulero* ed una formula per il suo calcolo.

Definizione 1. *Per ogni $n \geq 1$, si denota con $\boldsymbol{U}_n$ l'insieme*

$$\boldsymbol{U}_n = \{k \in \boldsymbol{Z} \ :\ 1 \leq k \leq n \ \text{ e } \ (k,n) = 1\}.$$

Si chiama funzione di Eulero l'applicazione $\varphi : \boldsymbol{N}^\cdot \to \boldsymbol{N}^\cdot$ tale che $\varphi(n) = |\boldsymbol{U}_n|$, $\forall\, n \in \boldsymbol{N}^\cdot$. [Dunque $\varphi(n)$ è il numero dei naturali $\leq n$ e primi con n.]

Osservazione 3. Per ogni $n \geq 2$, risulta: $\varphi(n) = \left|\mathcal{U}(\boldsymbol{Z}_n)\right|$. Infatti è noto che

$$\mathcal{U}(\boldsymbol{Z}_n) = \left\{\overline{a} \in \boldsymbol{Z}_n \ :\ 1 \leq a < n \ \text{ e } \ (a,n) = 1\right\}.$$

Si noti che: $\varphi(1) = 1$ (perché $\boldsymbol{U}_1 = \{1\}$); $\varphi(2) = 1$ (perché $\boldsymbol{U}_2 = \{1\}$); $\varphi(3) = 2$ (perché $\boldsymbol{U}_3 = \{1,2\}$); per ogni primo p, $\varphi(p) = p-1$ (perché $\boldsymbol{U}_p = \{1,2,\ ...\ ,p-1\}$). Si tratta ora di

calcolare $\varphi(n)$, $\forall\, n \geq 1$.

Proposizione 1. *Se* $n = p_1^{r_1} \dots p_s^{r_s}$, *risulta:*

$$\varphi(n) = \big(p_1^{r_1} - p_1^{r_1-1}\big) \cdot \dots \cdot \big(p_s^{r_s} - p_s^{r_s-1}\big).$$

Dim. Basterà dimostrare i due seguenti risultati:

(A) Se $(r,s) = 1$, $\varphi(rs) = \varphi(r)\cdot\varphi(s)$.

(B) Se p è primo, $\varphi(p^r) = p^r - p^{r-1}$ $(\forall\, r \geq 1)$.

Per dimostrare (A) abbiamo bisogno del seguente lemma.

Lemma 2. *Sia* $f : A \to B$ *un isomorfismo di anelli commutativi unitari. Allora* $f\big(\mathcal{U}(A)\big) = \mathcal{U}(B)$.

Dim. Lemma 2. Osserviamo che $f(1_A) = 1_B$. Infatti, essendo f suriettiva, $\forall\, b \in B$, $\exists\, a \in A$ tale che $f(a) = b$. Allora $b = f(a) = f(a\cdot 1_A) = f(a)\cdot f(1_A) = b\cdot f(1_A) = f(1_A)\cdot b$, cioè $b\cdot f(1_A) = b = f(1_A)\cdot b$. Dunque $f(1_A)$ è l'unico elemento neutro in B (rispetto al prodotto), cioè $f(1_A) = 1_B$.

Verifichiamo che $f\big(\mathcal{U}(A)\big) \subseteq \mathcal{U}(B)$. Per ogni $a \in \mathcal{U}(A)$ [con $aa' = 1_A$] si ha: $1_B = f(1_A) = f(aa') = f(a)f(a')$. Dunque $f(a) \in \mathcal{U}(B)$.

Verifichiamo che $\mathcal{U}(B) \subseteq f\big(\mathcal{U}(A)\big)$. Per ogni $b \in \mathcal{U}(B)$ [con $bb' = 1_B$] si ha: se $b = f(a)$ e $b' = f(a')$, allora $f(1_A) = 1_B = bb' = f(a)f(a') = f(aa')$: ne segue che (essendo f iniettiva) $1_A = aa'$. Quindi $a \in \mathcal{U}(A)$ e $b \in f\big(\mathcal{U}(A)\big)$

Dim. (A). Sia $(r,s) = 1$. Dal teorema Cinese del Resto (cfr. **Teor. 5.3**), $F : \boldsymbol{Z}_{rs} \to \boldsymbol{Z}_r \times \boldsymbol{Z}_s$ è un isomorfismo di anelli. Dal precedente **Lemma 2**, F trasforma $\mathcal{U}(\boldsymbol{Z}_{rs})$ in $\mathcal{U}(\boldsymbol{Z}_r \times \boldsymbol{Z}_s)$. Ora verifichiamo che $\mathcal{U}(\boldsymbol{Z}_r \times \boldsymbol{Z}_s) = \mathcal{U}(\boldsymbol{Z}_r) \times \mathcal{U}(\boldsymbol{Z}_s)$. Infatti:

$(\overline{a},\overline{b}) \in \mathcal{U}(\boldsymbol{Z}_r \times \boldsymbol{Z}_s) \iff (\overline{a},\overline{b})\cdot(\overline{c},\overline{d}) = (\overline{1}_r, \overline{1}_s)$, $\exists\, c,d \in \boldsymbol{Z} \iff \overline{a}\cdot\overline{c} = \overline{1}_r$ e $\overline{b}\cdot\overline{d} = \overline{1}_s \iff$

$\iff \overline{a} \in \mathcal{U}(\boldsymbol{Z}_r)$ e $\overline{b} \in \mathcal{U}(\boldsymbol{Z}_s) \iff (\overline{a},\overline{b}) \in \mathcal{U}(\boldsymbol{Z}_r) \times \mathcal{U}(\boldsymbol{Z}_s)$.

Ne segue: $\varphi(rs) = \big|\mathcal{U}(\boldsymbol{Z}_{rs})\big| = \big|\mathcal{U}(\boldsymbol{Z}_r \times \boldsymbol{Z}_s)\big| = \big|\mathcal{U}(\boldsymbol{Z}_r) \times \mathcal{U}(\boldsymbol{Z}_s)\big| = \big|\mathcal{U}(\boldsymbol{Z}_r)\big|\cdot\big|\mathcal{U}(\boldsymbol{Z}_s)\big| = \varphi(r)\cdot\varphi(s)$.

Nota. Se $r_1, \dots r_s$ sono a due a due coprimi, risulta: $\varphi(r_1 \cdot \dots \cdot r_s) = \prod_{i=1}^{s} \varphi(r_i)$.

Dim. (B). Per definizione, $\varphi(p^r) = \big|\boldsymbol{U}_{p^r}\big|$. Si ha:

$$\boldsymbol{U}_{p^r} = \big\{k \in \boldsymbol{Z} \text{ tali che } 1 \leq k \leq p^r,\ (k,p^r) = 1\big\}.$$

Si ha: $(k,p^r) = 1 \iff (k,p) = 1$. Ne segue: $(k,p^r) \neq 1 \iff (k,p) \neq 1 \iff (k,p) = p \iff k \in p\boldsymbol{Z}$. Pertanto:

$$\boldsymbol{U}_{p^r} = \big\{k \in \boldsymbol{Z} \,:\, 1 \leq k \leq p^r,\ k \notin p\boldsymbol{Z}\big\} = \big\{1, 2, \dots, p^r\big\} - \big\{ph,\ \forall\, h = 1, \dots, p^{r-1}\big\}.$$

Allora $\varphi(p^r) = \big|\boldsymbol{U}_{p^r}\big| = p^r - p^{r-1}$.

Teorema 2. *(Teorema di Eulero-Fermat). Sia* $n \geq 2$ *e sia* $a \in \boldsymbol{Z}$ *tale che* $(a,n) = 1$. *Risulta:,*

$$a^{\varphi(n)} \equiv 1 \ (mod\ n).$$

[Dunque $\overline{a}^{\,\varphi(n)} = \overline{1}$, $\forall\, \overline{a} \in \mathcal{U}(\boldsymbol{Z}_n)$*].*

Dim. (*J. Ivory, 1806*). Denotiamo con $t_1, \dots, t_{\varphi(n)}$ i naturali compresi tra 1 ed n, relativamente primi con n. Poiché $(a,n) = 1$, anche $at_1, \dots, at_{\varphi(n)}$ sono relativamente primi con n. Inoltre sono a due a due non congruenti *mod* n. Se infatti $at_i \equiv at_j$ $(mod\ n)$, allora $n \,\big|\, t_i - t_j$ (da *EU*) e dunque $t_i - t_j = 0$. Ne segue che

$$\big\{\overline{t_1}, \dots, \overline{t_{\varphi(n)}}\big\} = \mathcal{U}(\boldsymbol{Z}_n) = \big\{\overline{at_1}, \dots, \overline{at_{\varphi(n)}}\big\}.$$

Pertanto, moltiplicando gli elementi dei due insiemi,

$$\overline{t_1} \cdot \dots \cdot \overline{t_{\varphi(n)}} = \overline{at_1} \cdot \dots \cdot \overline{at_{\varphi(n)}} = \overline{a}^{\,\varphi(n)}\, \overline{t_1} \cdot \dots \cdot \overline{t_{\varphi(n)}}$$

e, semplificando i fattori $\overline{t}_i$, si ottiene $\overline{1} = \overline{a}^{\varphi(n)}$, cioè $a^{\varphi(n)} \equiv 1 \ (mod\ n)$.

Osservazione 4. Si noti che con la stessa dimostrazione si può dimostrare anche il PTF_2.

Corollario 2. *Sia $n \geq 2$ e sia $a \in \boldsymbol{Z}$ tale che $(a, n) = 1$. Un inverso aritmetico a' di a modulo n è dato da $a^{\varphi(n)-1}$.*

Dim. Infatti $a \cdot a^{\varphi(n)-1} = a^{\varphi(n)} \equiv 1 \ (mod\ n)$.

Il teorema di Eulero-Fermat è un utile strumento per risolvere problemi aritmetici, come negli esempi che seguono. Si noti che, utilizzando soltanto il teorema Cinese del Resto (come fatto in **Osserv. 5.6**) i calcoli sarebbero molto più laboriosi.

Esempio 2. Usando il teorema di Eulero-Fermat, calcolare le ultime due cifre di $n = 81^{82}$.

Si tratta di risolvere la congruenza $81^{82} \equiv X \ (mod\ 100)$.

Si ha: $(81, 100) = 1$ e $\varphi(100) = \varphi(4) \cdot \varphi(25) = 2 \cdot 20 = 40$. Allora, in base al teorema di Eulero-Fermat, $81^{40} = 81^{\varphi(100)} \equiv 1 \ (mod\ 100)$. Dunque

$$81^{82} = \left(81^{40}\right)^2 \cdot 81^2 \equiv 1^2 \cdot 81^2 = 6561 \equiv 61 \ (mod\ 100).$$

Le ultime due cifre di 81^{82} sono $6, 1$.

Esempio 3. Usando il teorema di Eulero-Fermat, calcolare le ultime tre cifre di $n = 7^{827}$.

Si tratta di risolvere la congruenza $7^{827} \equiv X \ (mod\ 1000)$.

Si ha: $(7, 1000) = 1$ e $\varphi(1000) = \varphi(8) \cdot \varphi(125) = 4 \cdot 100 = 400$. Allora, in base al teorema di Eulero-Fermat, $7^{400} \equiv 1 \ (mod\ 1000)$. Allora $7^{827} = (7^{400})^2 \cdot 7^{27} \equiv 1^2 \cdot 7^{27} \ (mod\ 1000)$. Si tratta quindi di calcolare $7^{27} \ (mod\ 1000)$.

Essendo $27 = 2^4 + 2^3 + 2 + 1$, allora $7^{27} \equiv 7^{16} \cdot 7^8 \cdot 7^2 \cdot 7 \ (mod\ 1000)$. Si ha:

$$\begin{aligned} &7 \equiv 7 \ (mod\ 1000), \\ &7^2 \equiv 49 \ (mod\ 1000), \\ &7^4 \equiv 401 \ (mod\ 1000), \\ &7^8 \equiv (401)^2 \equiv 801 \ (mod\ 1000), \\ &7^{16} \equiv (801)^2 \equiv 601 \ (mod\ 1000). \end{aligned}$$

Poiché $601 \cdot 801 \equiv 401 \ (mod\ 1000)$ e $49 \cdot 7 \equiv 343 \ (mod\ 1000)$, allora $7^{27} \equiv 401 \cdot 343 \equiv 543 \ (mod\ 1000)$.

Si conclude che le ultime tre cifre di 7^{827} sono $5, 4, 3$.

7. Esercizi del Capitolo II

2.1. (*i*) Estendere la definizione di MCD al caso di un numero finito di interi $a_1, \dots, a_n$, con $n \geq 2$.
(*ii*) Assegnati tre interi non nulli a, b, c, verificare che $MCD(a, b, c) = MCD(a, MCD(b, c))$.
(*iii*) Verificare che se gli interi a, b, c sono a due a due coprimi, allora $MCD(ab, ac, bc) = 1$.
(*iv*) Se $MCD(a, b, c) = 1$, è vero che $MCD(ab, ac, bc) = 1$?
(*v*) Se $MCD(a, b, c) = 1$, determinare un'identità di Bézout, del tipo $1 = ax+by+cz$, con $x, y, z \in \boldsymbol{Z}$.

* * * * * * * * *

2.2. (*i*) Sia p un numero primo. Sia $a \in \boldsymbol{N}$ tale che $1 \leq a < p^2$. Quali a sono privi di inverso aritmetico *mod* p^2?
(*ii*) Siano n, m interi ≥ 2, tali che $n \,|\, m$. Sia $a \in \boldsymbol{N}$ tale che $1 \leq a < n$. Verificare che se a ha inverso aritmetico *mod* m lo ha anche *mod* n. È vero che se a ha inverso aritmetico *mod* n lo ha anche *mod* m ?

* * * * * * * * *

2.3. Risolvere l'equazione congruenziale lineare $121\,X \equiv 22 \ (mod\ 33)$, indicandone un sistema completo di soluzioni *mod* 33.

* * * * * * * * *

2.4. Posto $n = 9, 10, 11, 12, 13, 14, 15, 16$, risolvere l'equazione congruenziale lineare

$$6\,X \equiv 9 \ (mod\ n),$$

indicandone, se compatibile, la totalità delle soluzioni ed un sistema completo di soluzioni *mod* n.

* * * * * * * * *

2.5. Risolvere il seguente sistema 'cinese' di equazioni congruenziali lineari

$$\begin{cases} X \equiv 2 \ (mod\ 5) \\ X \equiv 1 \ (mod\ 3) \\ X \equiv 6 \ (mod\ 14) \\ X \equiv 5 \ (mod\ 11). \end{cases}$$

* * * * * * * * *

2.6. Risolvere il seguente sistema di equazioni congruenziali lineari

$$\begin{cases} 18\,X \equiv 12 \ (mod\ 30) \\ 7\,X \equiv 4 \ (mod\ 9) \\ 28\,X \equiv 14 \ (mod\ 98). \end{cases}$$

* * * * * * * * *

2.7. Verificare se il seguente sistema di equazioni congruenziali lineari è compatibile:

$$\begin{cases} 2\,X \equiv 8 \ (mod\ 9) \\ 2\,X \equiv 6 \ (mod\ 15). \end{cases}$$

* * * * * * * * *

2.8. [*Esonero 8/4/03*] Determinare, se esistono, i valori $a \in \boldsymbol{Z}$ per cui il seguente sistema ammette soluzione:

$$\begin{cases} 6425\,X \equiv 7 \ \ mod\ 12 \\ 8614\,X \equiv 3 \ \ mod\ 7 \\ 3\,X \equiv a \ \ mod\ 8. \end{cases}$$

Per tali valori calcolare le soluzioni stesse.

* * * * * * * * *

2.9. [*Esame 1/7/03*] Al variare di $a \in \boldsymbol{N}$, $0 \leq a < 15$, sono assegnati i seguenti sistemi di congruenze:

$$\begin{cases} 2X \equiv 5 \ (mod\ 7) \\ X \equiv 4 \ (mod\ 9) \\ 4X \equiv a \ (mod\ 15). \end{cases}$$

Determinare gli eventuali a per cui il sistema è compatibile e scriverne la generica soluzione.

* * * * * * * * *

2.10. [*Esame 15/6/04*] È assegnato il seguente sistema di equazioni congruenziali lineari, dipendente da due parametri $a, b \in \boldsymbol{Z}$:

$$\begin{cases} aX \equiv \ 3 \ (mod\ 5) \\ 3X \equiv b \ (mod\ 8). \end{cases}$$

(*i*) Determinare per quali $a, b \in \boldsymbol{Z}$ il sistema è compatibile.

(*ii*) Per siffatti valori scrivere la generica soluzione del sistema, in funzione dei parametri a, b ed eventualmente di loro inversi aritmetici a', b'.

* * * * * * * * *

2.11. [*Esonero 8/4/03*] Sia $f : \boldsymbol{Z}_{18} \to \boldsymbol{Z}_6 \times \boldsymbol{Z}_3$ l'applicazione così definita:

$$f(\overline{x}_{18}) = (\overline{x}_6, \overline{x}_3), \ \forall\, \overline{x}_{18} \in \boldsymbol{Z}_{18} \ \text{ [dove } \overline{x}_k \text{ denota la classe resto } \overline{x} \text{ in } \boldsymbol{Z}_k, \ \forall\, k \geq 2].$$

(*i*) Verificare che f è ben definita.

(*ii*) Determinare $Im(f)$ e calcolare $f^{-1}((\overline{0}_6, \overline{0}_3)),\ f^{-1}((\overline{1}_6, \overline{2}_3))$.

(*iii*) Sia $g : \boldsymbol{Z}_6 \to \boldsymbol{Z}_{18}$ tale che: $g(\overline{x}_6) = \overline{x}_{18}, \forall\, \overline{x}_6 \in \boldsymbol{Z}_6$. g è ben definita? g è iniettiva?

* * * * * * * * *

2.12. Utilizzando il teorema Cinese del Resto, verificare che le ultime tre cifre di $n = 46^{14}$ sono $6, 5, 6$.

* * * * * * * * *

2.13. Determinare, se esiste, il minimo intero $n > 0$ tale che 7123^n abbia come ultima cifra 1.

* * * * * * * * *

2.14. Considerati i numeri naturali $734^h,\ \forall\, h \geq 2,$ determinare le possibili ultime due cifre di tali numeri.

* * * * * * * * *

2.15. È assegnato il numero naturale $n = 133^{42}$.

(*i*) Usando il teorema di Eulero-Fermat, calcolare le ultime due cifre di n.

(*ii*) Usando il teorema Cinese del Resto, calcolare le ultime tre cifre di n.

* * * * * * * * *

2.16. Sia $n \geq 2$. Verificare che ogni elemento non nullo di $\boldsymbol{Z}_n$ è o un elemento invertibile o uno zero-divisore di $\boldsymbol{Z}_n$.

* * * * * * * * *

2.17. Utilizzando opportunamente la relazione di congruenza $mod\ 3$, verificare che esiste un'unica terna di numeri primi della forma

$$(n,\ n-2,\ n-4), \ \text{ con } \ n \in \boldsymbol{N}.$$

* * * * * * * * *

2.18. Dimostrare che esistono infiniti primi congruenti a $3\ mod\ 4$.

Suggerimento. Per assurdo, l'insieme A dei primi congruenti a $3\ mod\ 4$ sia finito. Poniamo

$$A = \{p_1 = 3,\ p_2 = 7,\ p_3,\ \dots,\ p_n\}.$$

Posto inoltre $P = \prod_{i=1}^{n} p_i\,,\ Q = 4P - 1,$ verificare preliminarmente che:

$$(a)\ \ Q \ \text{ non è primo;} \quad (b)\ \ \exists\, p_k \in A \ \text{ tale che } \ p_k \,\big|\, Q.$$

* * * * * * * * *

Appendice 2

Metodi di fattorizzazione in prodotti di primi

Ci proponiamo di determinare la fattorizzazione in primi di un naturale n, che assumeremo dispari e ≥ 3. Descriveremo due algoritmi. Il primo è attribuito a Fermat.

Definizione 1. *Poniamo,* $\forall\, n \geq 3$*:*

$$\boldsymbol{\mathcal{A}}_n := \{(a,b) \in \boldsymbol{N}\times\boldsymbol{N} \ \ \textit{tali che} \ \ ab = n,\ 1 \leq a \leq b\}.$$

Osservazione 1. (*i*) Risulta: $\boldsymbol{\mathcal{A}}_n \neq \emptyset$ [infatti $(1,n) \in \boldsymbol{\mathcal{A}}_n$].

(*ii*) Risulta: $\boldsymbol{\mathcal{A}}_n = \{(1,n)\} \iff n$ è primo [ovvio].

(*iii*) $\boldsymbol{\mathcal{A}}_n$ è un insieme finito [infatti, $\forall\,(a,b) \in \boldsymbol{\mathcal{A}}_n,\ 1 \leq a,b \leq n$].

(*iv*) $\boldsymbol{\mathcal{A}}_n$ è un insieme totalmente ordinato rispetto alla seguente relazione:

$$(a,b) \leq (a_1,b_1) \iff b-a \leq b_1-a_1, \ \ \forall\,(a,b),\,(a_1,b_1) \in \boldsymbol{\mathcal{A}}_n$$

[Verifichiamo che $\leq$ è una relazione d'ordine totale su $\boldsymbol{\mathcal{A}}_n$:

- la riflessività e la transitività di $\leq$ sono ovvie.

- $\leq$ è *antisimmetrica*: sia infatti $(a,b) \leq (a_1,b_1)$ e $(a_1,b_1) \leq (a,b)$. Allora $b-a = b_1-a_1$. Se per assurdo fosse $a < a_1$, si avrebbe $\frac{n}{a} > \frac{n}{a_1}$, cioè $b > b_1$. Allora $b_1-a_1 < b-a$: assurdo. Analogamente si esclude che sia $a_1 < a$. Dunque $a_1 = a$ e quindi $b_1 = b$, cioè $(a,b) = (a_1,b_1)$.

- $\leq$ è *totale*: se infatti $(a,b) \not\leq (a_1,b_1)$, allora $b-a \not\leq b_1-a_1$ e quindi $b_1-a_1 < b-a$, da cui $(a_1,b_1) \leq (a,b)$.

Si noti che $(a,b) \leq (1,n), \ \ \forall\,(a,b) \in \boldsymbol{\mathcal{A}}_n$: dunque $(1,n)$ è l'ultimo elemento di $\boldsymbol{\mathcal{A}}_n$.]

Assumiamo per il momento di saper calcolare il primo elemento di $\boldsymbol{\mathcal{A}}_n$, che denoteremo $(\tilde{a},\tilde{b})$. Con lo stesso procedimento potremo poi calcolare il primo elemento di $\boldsymbol{\mathcal{A}}_{\tilde{a}}$ e di $\boldsymbol{\mathcal{A}}_{\tilde{b}}$ e così via, finché ci ridurremo ad insiemi di tipo $\boldsymbol{\mathcal{A}}_{p_i}$, con p_i primo. Tutti i primi p_i ottenuti forniranno la fattorizzazione richiesta di n.

Allo scopo di calcolare gli elementi di $\boldsymbol{\mathcal{A}}_n$ (ed in particolare il primo elemento), introduciamo la seguente definizione.

Definizione 2. *Poniamo,* $\forall\, n \geq 3$*:*

$$\boldsymbol{\mathcal{B}}_n := \{(x,y) \in \boldsymbol{N}\times\boldsymbol{N} \ \ \textit{tali che} \ \ 0 \leq y < x \ \ \textit{e} \ \ x^2 - y^2 = n\}.$$

Osservazione 2. (*i*) Verifichiamo che gli insiemi $\boldsymbol{\mathcal{A}}_n$, $\boldsymbol{\mathcal{B}}_n$ sono in corrispondenza biunivoca. Allo scopo definiamo le due applicazioni:

$$\varphi : \boldsymbol{\mathcal{A}}_n \to \boldsymbol{\mathcal{B}}_n \ \text{ tale che } \ \varphi((a,b)) = \left(\tfrac{b+a}{2},\, \tfrac{b-a}{2}\right), \ \ \forall\,(a,b) \in \boldsymbol{\mathcal{A}}_n$$

[si noti che, essendo n dispari, anche a,b lo sono e dunque $\frac{b+a}{2},\, \frac{b-a}{2} \in \boldsymbol{N}$. Inoltre si ha: $0 \leq \frac{b-a}{2} < \frac{b+a}{2}$ e $(\frac{b+a}{2})^2 - (\frac{b-a}{2})^2 = ab = n$. Dunque $\varphi((a,b)) \in \boldsymbol{\mathcal{B}}_n$];

$$\psi : \boldsymbol{\mathcal{B}}_n \to \boldsymbol{\mathcal{A}}_n \ \text{ tale che } \ \psi((x,y)) = \big(x-y,\, x+y\big), \ \ \forall\,(x,y) \in \boldsymbol{\mathcal{B}}_n$$

[si noti che $1 \leq x-y \leq x+y$; inoltre $(x+y)(x-y) = x^2 - y^2 = n$. Dunque $\psi((x,y)) \in \boldsymbol{\mathcal{A}}_n$].

Lasciamo per esercizio la verifica che φ, ψ sono l'una inversa dell'altra.

(*ii*) L'ordinamento totale di $\boldsymbol{\mathcal{A}}_n$ si trasforma tramite φ in un ordinamento totale di $\boldsymbol{\mathcal{B}}_n$, che è così definito:

$$(x,y) \leq (x_1,y_1) \iff x \leq x_1 \iff y \leq y_1.$$

Infatti: $(x,y) \leq (x_1,y_1) \iff \psi((x,y)) \leq \psi((x_1,y_1)) \iff (x-y, x+y) \leq (x_1-y_1, x_1+y_1) \iff x+y-(x-y) \leq x_1+y_1-(x_1-y_1) \iff 2y \leq 2y_1 \iff y \leq y_1 \iff y^2 \leq y_1^2 \iff y^2+n \leq y_1^2+n \iff x^2 \leq x_1^2 \iff x \leq x_1$.

Per ottenere gli elementi di $\boldsymbol{\mathcal{A}}_n$ (ed in particolare il primo, che denoteremo $(\tilde{a},\tilde{b})$), basterà calcolare gli elementi di $\boldsymbol{\mathcal{B}}_n$ (ed in particolare il primo elemento $(\tilde{x},\tilde{y})$) e poi trasformarli nei corrispondenti di $\boldsymbol{\mathcal{A}}_n$.

Proposizione 1. *Sia* $x_0 :=$ *minimo intero* $\geq \sqrt{n}$. *Per ogni* $(x,y) \in \boldsymbol{N}\times\boldsymbol{N}$, *risulta:*

$$(x,y) \in \boldsymbol{\mathcal{B}}_n \iff y = \sqrt{x^2-n} \ \text{ e } \ x_0 \leq x \leq \tfrac{n+1}{2}.$$

Dim. ($\Longrightarrow$). Sia $(x,y) \in \boldsymbol{\mathcal{B}}_n$. Allora

($*$) $y^2 = x^2 - n > 0 \ \Rightarrow \ y = \sqrt{x^2-n}$;

($**$) essendo $(a,b) \leq (1,n)$, $\forall\,(a,b) \in \boldsymbol{\mathcal{A}}_n$, allora $(x,y) = \varphi((a,b)) \leq \varphi((1,n)) = (\frac{n+1}{2}, \frac{n-1}{2})$ e quindi $x \leq \frac{n+1}{2}$.

($***$) $x^2 = n + y^2 \geq n$ e quindi $x \geq \sqrt{n}$. Allora $x \geq x_0$.

Da ($*$), ($**$) e ($***$) segue l'implicazione ($\Longrightarrow$).

($\Longleftarrow$). Sia $(x,y) \in \boldsymbol{N}\times\boldsymbol{N}$ tale che $y = \sqrt{x^2-n}$ e $x_0 \leq x \leq \frac{n+1}{2}$. Allora

($*$) $y^2 = x^2 - n \ \Rightarrow \ x^2 - y^2 = n$.

($**$) $0 \leq y$ è ovvio.

($***$) $y = \sqrt{x^2-n} < \sqrt{x^2} = x$: dunque $y < x$.

Da ($*$), ($**$) e ($***$) segue che $(x,y) \in \boldsymbol{\mathcal{B}}_n$.

La **Prop. 1** consente di determinare $\boldsymbol{\mathcal{B}}_n$: tra gli interi $x = x_0 + h \in [x_0, \frac{n+1}{2}]$, si scelgono quelli per cui $(x_0+h)^2 - n$ è un quadrato. Allora $\boldsymbol{\mathcal{B}}_n$ è formato dalle coppie $\big(x_0+h, \sqrt{(x_0+h)^2-n}\big)$, per ogni x_0+h scelto. In particolare, la prima coppia ottenuta (corrispondente al valore minimo possibile di h) è il primo elemento di $\boldsymbol{\mathcal{B}}_n$ [che poi corrisponde al primo elemento $(\tilde{a},\tilde{b})$ di $\boldsymbol{\mathcal{A}}_n$].

Osservazione 3. Si noti che il metodo di fattorizzazione di Fermat è più efficiente rispetto al metodo di fattorizzazione standard (cfr. **Cap. II.2**). Ciò dipende dal fatto che i due fattori $\tilde{a}$ e $\tilde{b}$ sono sensibilmente inferiori a $n_1 = \frac{n}{k_1}$ e portano quindi ad una semplificazione più rapida del problema.

Esempio 1. Fattorizzare $n = 375$ con il metodo di Fermat.

Si ha: $x_0 =$ minimo intero $\geq \sqrt{375} = 19,\ldots$ e dunque $x_0 = 20$.

Si considerano gli interi compresi tra 20 e $\frac{376}{2} = 188$ e si cerca il primo $h \geq 0$ tale che $(20+h)^2 - 375$ è un quadrato.

Sia $h = 0$. $(20+0)^2 - 375 = 25 = 5^2$: è un quadrato. Dunque $(20,5)$ è il primo elemento di $\boldsymbol{\mathcal{B}}_{375}$. Ad esso corrisponde $(15,25) \in \boldsymbol{\mathcal{A}}_{375}$. Dunque $375 = 15\cdot 25$.

Ora bisogna calcolare i primi elementi di $\boldsymbol{\mathcal{A}}_{15}$ ed $\boldsymbol{\mathcal{A}}_{25}$.

Consideriamo $\boldsymbol{\mathcal{A}}_{15}$. Risulta: $\sqrt{15} = 4,\ldots$ e quindi $x_0 = 4$. Cerchiamo il primo $h \geq 0$ tale che $(4+h)^2 - 15$ è un quadrato. Per $h = 0$, $(4+0)^2 - 15 = 1 = 1^2$: è un quadrato. Allora $(4,1)$ è il primo elemento di $\boldsymbol{\mathcal{B}}_{15}$ e ad esso corrisponde $(3,5) \in \boldsymbol{\mathcal{A}}_{15}$ [infatti $15 = 3\cdot 5$].

Consideriamo $\boldsymbol{\mathcal{A}}_{25}$. Risulta: $\sqrt{25} = 5$ e quindi $x_0 = 5$; inoltre $(5+0)^2 - 25 = 0 = 0^2$: è un quadrato. Allora il primo elemento di $\boldsymbol{\mathcal{B}}_{25}$ è $(5,0)$ e ad esso corrisponde $(5,5)$, primo elemento di $\boldsymbol{\mathcal{A}}_{25}$ [infatti $25 = 5\cdot 5$].

Poiché $(3,5)$ e $(5,5)$ sono coppie di primi, il procedimento è terminato e si ha

$$375 = 15{\cdot}25 = (3{\cdot}5){\cdot}(5{\cdot}5) = 3{\cdot}5{\cdot}5{\cdot}5.$$

Esempio 2. Fattorizzare $n = 85$ con il metodo di Fermat.

Si ha: $\sqrt{85} = 9, ...$ e dunque $x_0 = 10$.

Si ha: $10^2 - 85 = 15$ (non quadrato); $11^2 - 85 = 36 = 6^2$ (quadrato). Allora $(11,6) \in \boldsymbol{\mathcal{B}}_{85}$ e quindi $(5,17) \in \boldsymbol{\mathcal{A}}_{85}$.

5, 17 sono primi e quindi il procedimento termina: $85 = 5{\cdot}17$.

Esempio 3. Fattorizzare $n = 13485$ con il metodo di Fermat.

Si ha: $\sqrt{13485} = 116, ...$ e dunque $x_0 = 117$.

Si ha: $117^2 - n$ non quadrato; $118^2 - n$ non quadrato; $119^2 - n = 26^2$ (quadrato). Allora $(119,26) \in \boldsymbol{\mathcal{B}}_n$ e quindi $(93,145) \in \boldsymbol{\mathcal{A}}_n$.

Si può verificare con il metodo di Fermat (o, ovviamente, direttamente) che $93 = 3{\cdot}31$ e $145 = 5{\cdot}29$. Si conclude che

$$n = 13485 = 93{\cdot}145 = (3{\cdot}31){\cdot}(5{\cdot}29) = 3{\cdot}5{\cdot}29{\cdot}31.$$

Un altro algoritmo per la fattorizzazione di un naturale in primi è dovuto a N.A.Draim ($\sim$ 1950). Draim [capitano della marina statunitense] non ha mai pubblicato il suo algoritmo, che invece è stato divulgato da J.H.Davenport [cfr. *The Higher Arithmetic*, Cambridge Univ. Press (1982)].

Sia n un naturale dispari e ≥ 3. Si ponga $n_1 = m_1 = n$. L'algoritmo consiste nel creare due successioni di naturali $\{n_k\}$, $\{m_k\}$ così definite: denotati con q_k ed r_k rispettivamente il quoziente ed il resto della divisione euclidea di n_k per $2k+1$, cioè

$$(*) \qquad n_k = (2k+1)\, q_k + r_k\,, \ \forall\, k \geq 1,$$

si ponga, $\forall\, k \geq 2$:

$$m_k = m_{k-1} - 2q_{k-1}\,, \quad n_k = m_k + r_{k-1}\,.$$

Da tali definizioni segue facilmente che, $\forall\, k \geq 2$:

$$(**) \qquad n_k = k\,n - (2k+1) \sum_{t=1}^{k-1} q_t\,,$$

$$(***) \qquad m_k = n - 2 \sum_{t=1}^{k-1} q_t\,.$$

Da $(*)$, $(**)$ e dal fatto che $MCD(k, 2k+1) = 1$, segue subito che

$$r_k = 0 \iff 2k+1 \,\big|\, n.$$

Se quindi $r_k = 0$ e $r_1, ..., r_{k-1} > 0$, allora $2k+1$ è il minimo fattore (necessariamente primo) di n. In tal caso da $(**)$ segue che

$$k\,n = (2k+1) \sum_{t=1}^{k} q_t\,.$$

Tenuto conto di tale uguaglianza e dell'espressione di m_{k+1} [dedotta da $(***)$], si ottiene

$$m_{k+1} = n - 2 \sum_{t=1}^{k} q_t = n - 2\tfrac{kn}{2k+1} = \tfrac{n}{2k+1}.$$

Dunque n è prodotto dei due fattori $2k+1$, m_{k+1} (di cui il secondo non è necessariamente primo). Si applica ora l'algoritmo sopra esposto ad m_{k+1} e, dopo un numero finito di passi, si perverrà ad una completa fattorizzazione di n.

Tenuto conto del **Lemma 3.2** (cioè del fatto che ogni non primo $n \geq 4$ ammette un fattore $\leq [\sqrt{n}\,]$), le successioni $\{n_k\}$, $\{m_k\}$ andranno al più calcolate fino al massimo indice k tale che $2k+1 \leq [\sqrt{n}\,]$ ovvero fino al minimo indice k tale che $r_k = 0$, mentre $r_1, ..., r_{k-1} > 0$.

Esempio 4. Fattorizzare $n = 85$ con il metodo di Draim.

Risulta:

$$n_1 = 85 = 3\cdot 28 + 1, \quad q_1 = 28, \quad r_1 = 1.$$

Ne segue:

$$m_2 = 85 - 2q_1 = 29, \quad n_2 = m_2 + r_1 = 30.$$

Risulta:

$$n_2 = 30 = 5\cdot 6 + 0, \quad q_2 = 6, \quad r_2 = 0.$$

Essendo $r_2 = 0$, il fattore minimo di $n = 85$ è 5 e l'altro fattore è $m_3 = m_2 - 2q_2 = 17$ (anch'esso primo). Il procedimento quindi termina con $85 = 5\cdot 17$.

Esempio 5. Fattorizzare $n = 13485$ con il metodo di Draim.

Risulta:

$$n_1 = 13485 = 3\cdot 4495 + 0, \quad q_1 = 4495, \quad r_1 = 0$$

e si conclude che n è fattorizzato da $3,\ 4495$.

Riapplichiamo il procedimento a $n_1 = 4495$ Risulta:

$$n_1 = 4495 = 3\cdot 1498 + 1, \quad q_1 = 1498, \quad r_1 = 1$$

e quindi

$$m_2 = 4495 - 2q_1 = 1499, \quad n_2 = m_2 + r_1 = 1500.$$

Risulta:

$$n_2 = 1500 = 5\cdot 300 + 0, \quad q_2 = 300, \quad r_2 = 0.$$

Allora $m_3 = m_2 - 2q_2 = 899$ e pertanto n è fattorizzato da $3,\ 5,\ 899$.

Riapplichiamo ora il procedimento a $n_1 = 899$. In questo caso i calcoli si rivelano piuttosto laboriosi, ma sappiamo che le successioni $\{n_k\}$, $\{m_k\}$ andranno al più calcolate per $2k+1 \leq [\sqrt{899}] = 29$, cioè per $k \leq 14$. Si può verificare che:

$$\{m_k\}_{k\geq 1} = \{899, 301, 181, 129, 101, 83, 71, 61, 53, 49, 43, 41, 37, 35, 31\},$$
$$\{n_k\}_{k\geq 1} = \{899, 303, 184, 131, 106, 90, 83, 69, 54, 65, 45, 63, 50, 58\},$$
$$\{r_k\}_{k\geq 1} = \{2, 3, 2, 5, 7, 12, 8, 1, 16, 2, 22, 13, 23, 0\}.$$

Poiché r_{14} è il primo resto nullo, si può concludere che 899 è fattorizzato da $2\cdot 14+1 = 29$, $m_{15} = 31$ (primo). Pertanto $13485 = 3\cdot 5\cdot 29\cdot 31$.

Capitolo III

POLINOMI

1. Polinomi e funzioni polinomiali

Definizione 1. *Sia K un campo. Si chiama polinomio a coefficienti in K ogni espressione del tipo:*

$$P = P(X) = a_0 + a_1X + a_2X^2 + \ .... \ + a_nX^n = \sum_{i=0}^{n} a_i X^i .$$

Si tratta di una somma formale di addendi $a_i X^i$, con $a_i \in K$, detti monomi di P. In particolare, a_i è detto i-esimo coefficiente di P (o coefficiente di grado i); a_0 è detto anche termine noto di P. X è un simbolo, detto indeterminata (o incognita) del polinomio P. Si assume che X verifichi le seguenti identità:

$$X^0 = 1, \quad X^1 = X, \quad 0X = 0, \ 1X = X.$$

Si conviene inoltre di identificare $P = \sum_{i=0}^{n} a_i X^i$ con $P + 0X^{n+1} + \ .... \ + 0X^m$, $\forall m > n$.

Il polinomio $0 + 0X + \ ... \ + 0X^n$ ($\forall n \geq 0$) è detto polinomio nullo ed è denotato con 0.
L'insieme dei polinomi a coefficienti in K e nell'indeterminata X è denotato con $K[X]$.

Definizione 2. *Sia $P = \sum_{k=0}^{n} a_k X^k \in K[X]$ un polinomio non nullo. Si chiama grado di P il numero naturale $\partial P = deg(P) := max\{k \ : \ a_k \neq 0\}$. Il coefficiente a_k tale che $k = \partial P$ è detto coefficiente direttore di P. Se il coefficiente direttore di P è 1, P è detto monico.*

Osservazione 1. I polinomi di grado 0 sono tutti e soli gli elementi di $K^{\cdot}$ $\left[= K - \{0\}\right]$ e sono detti (*polinomi*) *costanti*.

Il polinomio nullo 0 non ha grado (in base alla definizione precedente), ma, per ragioni che saranno chiarite dalla successiva **Osserv. 2**(*ii*), converremo di attribuirgli grado $-\infty$ [e dunque $\partial 0 = -\infty$].

Definizione 3. *Due polinomi $P = \sum_{i=0}^{n} a_i X^i$, $Q = \sum_{j=0}^{m} b_j X^j \in K[X]$ sono detti uguali se hanno lo stesso grado e se $a_k = b_k$, $\forall k = 0, 1, \ ..., \partial P \ [= \partial Q]$. Si scrive in tal caso $P = Q$.*

Proposizione 1. *L'insieme $K[X]$ è un anello rispetto alle operazioni di somma $+$ e prodotto $\cdot$ così definite: $\forall P = \sum_{i=0}^{n} a_i X^i$, $Q = \sum_{j=0}^{m} b_j X^j \in K[X]$,*

$$P + Q = \sum_{t=0}^{N} (a_t + b_t) X^t, \ \ con \ \ N = max(n, m),$$

$$P \cdot Q = \sum_{k=0}^{n+m} c_k X^k, \ \ con \ \ c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

[in particolare: $c_0 = a_0b_0$, $c_1 = a_0b_1 + a_1b_0$, $c_2 = a_0b_2 + a_1b_1 + a_2b_0$, ... , $c_{n+m} = a_nb_m$].
Inoltre l'anello $(K[X], +, \cdot)$ è un dominio d'integrità.

Dim. $(K[X], +)$ è un gruppo commutativo. Ha elemento neutro 0 e l'opposto di $P = \sum_{k=0}^{n} a_k X^k$ è

$-P = \sum_{k=0}^{n} (-a_k)X^k$. Si può infatti verificare che, $\forall\, P,\, Q,\, R \in K[X]$:

$$(P+Q)+R = P+(Q+R),$$
$$P+0 = P = 0+P,$$
$$P+(-P) = 0 = (-P)+P,$$
$$P+Q = Q+P.$$

Il prodotto $P\cdot Q$ sopra definito è ottenuto estendendo la seguente moltiplicazione tra monomi:

$$aX^i \cdot bX^i = abX^{i+j}.$$

Infatti $(\sum_{i=0}^{n} a_i X^i)(\sum_{j=0}^{m} b_j X^j) = \sum_{j=0}^{m}(\sum_{i=0}^{n} a_i X^i)b_j X^j = \sum_{j=0}^{m}\sum_{i=0}^{n} a_i b_j X^{i+j} = \sum_{k=0}^{n+m}(\sum_{i=0}^{k} a_i\, b_{k-i})X^k$ (dopo aver raccolto i coefficienti rispetto alle potenze crescenti di X). Si può facilmente verificare che:

$$(P\cdot Q)\cdot R = P\cdot(Q\cdot R),$$
$$P\cdot(Q+R) = P\cdot Q + P\cdot R, \quad (P+Q)\cdot R = P\cdot R + Q\cdot R,$$
$$P\cdot Q = Q\cdot P \ \text{ e } \ 1\cdot P = P$$

e pertanto $K[X]$ è un anello commutativo unitario. Resta da verificare che $K[X]$ è un anello integro, cioè che $P\cdot Q = 0 \implies P = 0 \ \vee \ Q = 0$. Se per assurdo $P, Q \neq 0$ e se a_n, b_m sono i coefficienti direttori risp. di P, Q, allora $P\cdot Q$ avrebbe coefficiente direttore $a_n b_m$. Ma $P\cdot Q = 0$ e dunque $a_n b_m = 0$, mentre $a_n, b_m \neq 0$: assurdo.

Osservazione 2. (*i*) In base alla definizione di prodotto risulta: $X\cdot X = X^2$ e, più generalmente, $X^n\cdot X^m = X^{n+m}$, $\forall\, n, m \geq 0$. Inoltre $a\cdot X^i = aX^i$, $\forall\, a \in K$ e $\forall\, i \geq 0$. Ne segue (eseguendo somme e prodotti in $K[X]$) che $a_0 + a_1\cdot X + \ \ldots\ + a_n\cdot X^n$ coincide con il polinomio $\sum_{i=0}^{n} a_i X^i$ (inteso come somma formale).

(*ii*) Dalle definizioni di somma e di prodotto di polinomi e dalla definizione di grado segue che, $\forall\, P, Q \in K[X]$:

$$\partial(P+Q) \leq max\{\partial P, \partial Q\}, \qquad \partial(P\cdot Q) = \partial P + \partial Q.$$

[Tali formule valgono anche se P o Q è il polinomio nullo. Basta accettare le seguenti regole di calcolo: $-\infty + n = -\infty$, $\forall\, n \in \boldsymbol{N}$, $-\infty + (-\infty) = -\infty$].

(*iii*) Risulta: $\mathcal{U}(K[X]) = K^{\cdot}$. Verifichiamo tale uguaglianza.

($\subseteq$). Se $P\cdot Q = 1$, da (*ii*) segue che $0 = \partial 1 = \partial P + \partial Q$. Quindi $\partial P = \partial Q = 0$ e pertanto $P, Q \in K^{\cdot}$.

($\supseteq$). $\forall\, a \in K^{\cdot}$, a ammette per inverso il polinomio (costante) $\frac{1}{a}$. Dunque $a \in \mathcal{U}(K[X])$.

Osservazione 3. È possibile definire polinomi a coefficienti su un anello A (anziché su un campo K). Per essi valgono inalterate le precedenti definizioni di grado, di somma e di prodotto [ovviamente, per definire somme e prodotti si fa ricorso alla somma ed al prodotto in A].

L'insieme dei polinomi a coefficienti in A è un anello, denotato $A[X]$. Si verifica subito che $A[X]$ è risp. commutativo, unitario ed integro $\iff$ A lo è. Se infine A è un dominio d'integrità, resta ancora valida la formula $\partial(P\cdot Q) = \partial P + \partial Q$. Ne segue subito che $\mathcal{U}(A[X]) = \mathcal{U}(A)$.

Osservazione 4. Assegnato un campo K, denoteremo con $\mathcal{S}_K$ l'insieme delle *successioni definitivamente nulle* a valori in K. [Una successione $\underline{a} = (a_0, a_1, a_2, \ldots\ldots\ )$ a valori in K è detta *definitivamente nulla* se $\exists\, n \in \boldsymbol{N}$ tale che $a_t = 0$, $\forall\, t > n$.]

Si osserva subito che la seguente applicazione

$$\mathcal{S}_K \longrightarrow K[X] \ \text{ tale che } \ \underline{a} = (a_0, \ \ldots\ , a_n, 0, 0, 0, \ \ldots\ldots\ ) \longrightarrow \sum_{i=0}^{n} a_i X^i,$$

è una biiezione. [Si noti in particolare che

$$(0, 0, 0, 0, \ \ldots\ ) \longrightarrow 0, \quad (1, 0, 0, 0, \ \ldots\ ) \longrightarrow 1, \quad (0, 1, 0, 0, \ \ldots\ ) \longrightarrow X,$$
$$(0, 0, 1, 0, \ \ldots\ ) \longrightarrow X^2, \quad (0, 0, 0, 1, \ \ldots\ ) \longrightarrow X^3, \ \text{ ecc.}].$$

Sussistendo tale biiezione, i polinomi di $K[X]$ potranno essere identificati con le successioni definita-

mente nulle (di $\mathcal{S}_K$).

Definizione 4. *Sia K un campo e sia $P = \sum_{i=0}^{n} a_i X^i \in K[X]$. Si chiama funzione polinomiale su K associata a P l'applicazione*

$$\Phi_P : K \to K \quad \text{tale che} \quad \Phi_P(x) = \sum_{i=0}^{n} a_i x^i, \quad \forall\, x \in K.$$

Osservazione 5. Le funzioni polinomiali su K sono particolari applicazioni di K in sé. Indicato con K^K l'insieme di tutte le applicazioni di K in sé, indichiamo con $\mathcal{F}_K$ il suo sottoinsieme delle applicazioni polinomiali su K.

Osserviamo che K^K è dotato di struttura di anello commutativo unitario, rispetto alle due seguenti operazioni di somma $+$ e prodotto $\cdot$:

$$(f+g)(x) = f(x) + g(x), \quad \forall\, x \in K, \qquad \forall\, f, g \in K^K;$$
$$(f \cdot g)(x) = f(x) \cdot g(x), \quad \forall\, x \in K, \qquad \forall\, f, g \in K^K.$$

In particolare, gli elementi neutri rispetto a $+$ e a $\cdot$ sono rispettivamente l'applicazione costante nulla $\mathbf{0} : K \to K$ e l'applicazione costante $\mathbf{1} : K \to K$ (che non va confusa con l'applicazione identica $\mathbf{1}_K$ di K). Le verifiche degli assiomi di anello sono un semplice esercizio.

Anche $\mathcal{F}_K$ è dotato di struttura di anello commutativo unitario [rispetto alle stesse operazioni di K^K: dunque $\mathcal{F}_K$ è un sottoanello di K^K]. Risulta infatti, $\forall\, x \in K$:

$$\big(\Phi_P + \Phi_Q\big)(x) = \Phi_P(x) + \Phi_Q(x) = P(x) + Q(x) = (P+Q)(x) = \Phi_{P+Q}(x),$$
$$\big(\Phi_P \cdot \Phi_Q\big)(x) = \Phi_P(x) \cdot \Phi_Q(x) = P(x) \cdot Q(x) = (P \cdot Q)(x) = \Phi_{PQ}(x).$$

Dunque $\Phi_P + \Phi_Q = \Phi_{P+Q}$, $\Phi_P \cdot \Phi_Q = \Phi_{PQ}$ [la somma ed il prodotto di due funzioni polinomiali è una funzione polinomiale]. In particolare, $\Phi_0 = \mathbf{0}$ e $\Phi_1 = \mathbf{1}$ [applicazioni costanti].

La verifica degli assiomi di anello è lasciata per esercizio.

Proposizione 2. *Sia K un campo. L'applicazione*

$$\Phi : K[X] \to \mathcal{F}_K \quad \text{tale che} \quad \Phi(P) = \Phi_P, \quad \forall\, P \in K[X]$$

è un omomorfismo suriettivo di anelli.

Dim. Φ è suriettiva per definizione di $\mathcal{F}_K$. Bisogna verificare che, $\forall\, P, Q \in K[X]$, si ha:

$$\Phi(P+Q) = \Phi(P) + \Phi(Q), \quad \Phi(P \cdot Q) = \Phi(P) \cdot \Phi(Q).$$

Infatti: $\Phi(P+Q) = \Phi_{P+Q} = \Phi_P + \Phi_Q = \Phi(P) + \Phi(Q)$, $\Phi(P \cdot Q) = \Phi_{PQ} = \Phi_P \cdot \Phi_Q = \Phi(P) \cdot \Phi(Q)$.

Osservazione 6. Se il campo K è finito, Φ non può essere iniettiva. Infatti $Card(K[X]) = \infty$ [perché $K[X]$ contiene gli infiniti polinomi distinti X^n, $\forall\, n \in \boldsymbol{N}$]. D'altra parte $\mathcal{F}_K \subseteq K^K$ e quindi $Card(\mathcal{F}_K) \leq Card(K^K) = |K|^{|K|} < \infty$.

Ad esempio, se $K = \boldsymbol{Z}_p$ (p primo), il polinomio $P = X(X-\overline{1})(X-\overline{2})\ldots(X-\overline{p-1}) \in \boldsymbol{Z}_p[X]$ è non nullo [in quanto ha grado p], mentre $\Phi_P = \mathbf{0}$. Infatti, $\forall\, \overline{a} \in \boldsymbol{Z}_p$,

$$\Phi_P(\overline{a}) = P(\overline{a}) = \overline{a}(\overline{a}-\overline{1})(\overline{a}-\overline{2})\ldots(\overline{a}-\overline{p-1}) = \overline{0}$$

[in quanto uno dei fattori è necessariamente $\overline{0}$].

Dimostreremo nel prossimo paragrafo che se K è un campo infinito, l'applicazione Φ è biiettiva (e dunque è un isomorfismo). In tale ipotesi, i polinomi si identificano con le funzioni polinomiali. Tale risultato è noto come *principio d'identità dei polinomi*.

Concluderemo il paragrafo definendo i polinomi a più indeterminate.

Definizione 5. *Siano X, Y due indeterminate sul campo K. Un polinomio $P = P(X,Y)$ a*

coefficienti in K, *nelle indeterminate* X, Y *è una somma formale del tipo:*

$$P = P(X,Y) = a_{00} + a_{10}X + a_{01}Y + a_{20}X^2 + a_{11}XY + a_{02}Y^2 + a_{30}X^3 + a_{21}X^2Y + a_{12}XY^2 + a_{03}Y^3 + \\ + ... + a_{n0}X^n + a_{n-1\,1}X^{n-1}Y + \ ... \ + a_{0n}Y^n,$$

con $n \geq 0$ *e* $a_{ij} \in K$ $(0 \leq i, j \leq n)$. *Per brevità si scrive* $P = \sum_{i+j=0}^{n} a_{ij}X^iY^j$. *I suoi addendi sono detti monomi di* P. *L'insieme di tali polinomi è denotato* $K[X,Y]$.

Più in generale, assegnate n *indeterminate* $X_1, \ldots, X_n$, *si chiama polinomio a coefficienti in* K, *nelle indeterminate* $X_1, \ldots, X_n$, *ogni somma formale*

$$P = P(X_1, \ldots, X_n) = \sum_{i_1+\ldots+i_n=0}^{N} a_{i_1 \ldots i_n} X_1^{\,i_1} \ldots X_n^{\,i_n}.$$

L'insieme di tali polinomi è denotato con $K[X_1, \ldots, X_n]$.

Osservazione 7. In $K[X,Y]$ (o in $K[X_1, \ldots, X_n]$) si definiscono [usando le usuali regole di calcolo] le due operazioni di somma e prodotto. Si conviene in particolare che le indeterminate commutino a due a due [dunque $YX = XY$, ecc.].

In $K[X_1, \ldots, X_n]$ si introduce la seguente definizione di *grado*: se $M = aX_1^{\,i_1} \ldots X_n^{\,i_n}$ è un monomio del polinomio P, si definisce *grado del monomio* M: $\partial M = \sum_{k=1}^{n} i_k$. Si pone quindi:

$$\partial P = max\{\partial M, \ \forall\, M = \text{ monomio di } P\}.$$

Osservazione 8. Le considerazioni svolte nell'osservazione precedente restano valide, più generalmente, se il campo K viene sostituito da un anello A. Si può poi verificare che se A è un dominio d'integrità, anche $A[X_1, \ldots, X_n]$ è un dominio d'integrità e che risulta:

$$\mathcal{U}(A[X_1, \ldots, X_n]) = \mathcal{U}(A).$$

A tale scopo basta far riferimento all'**Osserv. 3** e verificare che

$$(*) \qquad A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n],$$

da cui segue:

$$A[X_1, \ldots, X_n] = A[X_1][X_2][X_3] \ldots [X_n].$$

Verifichiamo la formula $(*)$ per $n = 2$, nella forma: $A[X,Y] = A[X][Y]$.

$(\subseteq)$. Assegnato $P \in A[X,Y]$, si raccolgono tutti i monomi di P aventi lo stesso esponente in Y. Risulterà quindi:

$$P = \sum_{j=0}^{d_Y} a_j(X)Y^j,$$

con $a_j(X) \in A[X]$ e con d_Y grado di P come polinomio di $A[X][Y]$. Dunque $A[X,Y] \subseteq A[X][Y]$.

$(\supseteq)$. Ogni $P = \sum_{j=0}^{d} a_j(X)Y^j \in A[X][Y]$ è ovviamente anche un polinomio in $A[X,Y]$.

Ad esempio, assegnato $P = 1 + X^3 + Y^3 + 2XY^2 + X^2Y^2 - 2X^3Y \in \boldsymbol{Z}[X,Y]$, tale polinomio si riscrive, come elemento di $\boldsymbol{Z}[X][Y]$ nella forma:

$$P = (1 + X^3) + (-2X^3)Y + (2X + X^2)Y^2 + Y^3.$$

Si osservi che P ha grado 4 come polinomio in $\boldsymbol{Z}[X,Y]$ ed ha grado 3 come polinomio in $\boldsymbol{Z}[X][Y]$.

2. Divisibilità in K[X]

Esiste una notevole analogia tra le proprietà algebriche di $\boldsymbol{Z}$ e quelle di $K[X]$. Tutto nasce dal fatto che, come in $\boldsymbol{Z}$, anche in $K[X]$ vale il teorema della divisione con resto.

Teorema 1. (*Divisione con resto in* $K[X]$). *Siano* $F, G \in K[X]$, $G \neq 0$. *Esiste un'unica coppia di polinomi* $Q, R \in K[X]$ *tali che*

$$F = GQ + R, \quad \partial R < \partial G.$$

Q ed R sono detti rispettivamente quoziente e resto della divisione di F per G. F e G sono detti rispettivamente dividendo e divisore.

Dim. (*Esistenza*). Distinguiamo due casi: $F = 0$ e $F \neq 0$.

(a) $F = 0$. Basta in tal caso porre $Q = R = 0$. Si ottiene: $F = 0 = G\cdot 0 + 0$, con $\partial R = \partial 0 = -\infty < \partial G$.

(b) $F \neq 0$ (e dunque $\partial F \geq 0$). Se $\partial F < \partial G$, basta porre $Q = 0$, $R = F$ e si ottiene $F = G\cdot 0 + F$, con $\partial R = \partial F < \partial G$. Assumeremo quindi $\partial F \geq \partial G$ e procederemo per *induzione forte* su $\partial F \geq 0$.

Base induttiva. Sia $\partial F = 0$, cioè $F = a \in K^{\cdot}$. In tal caso anche $\partial G = 0$ e dunque $G = b \in K^{\cdot}$. Basta quindi porre $Q = \frac{a}{b}$, $R = 0$ e si ottiene: $F = a = b\cdot\frac{a}{b} + 0$, con $\partial R = -\infty < 0 = \partial G$.

Passo induttivo. Sia $\partial F = n \geq 1$ ed assumiamo vero l'asserto per ogni polinomio $\tilde{F}$ tale che $\partial\tilde{F} < n$. Dunque per ogni siffatto polinomio $\exists\, \tilde{Q}, \tilde{R} \in K[X]$ tali che $\tilde{F} = G\tilde{Q} + \tilde{R}$ e $\partial\tilde{R} < \partial G$. Poniamo:

$$F = \sum_{i=0}^{n} a_i X^i, \quad G = \sum_{j=0}^{m} b_j X^j, \text{ con } m = \partial G \leq \partial F = n.$$

Poiché $b_m \neq 0$, possiamo definire il polinomio $\tilde{F} := F - \frac{a_n}{b_m} X^{n-m} G$. Ovviamente $\partial\tilde{F} \leq n$. Ma risulta

$$\tilde{F} = a_0 + \ \ldots\ + \cancel{a_n X^n} - \tfrac{a_n}{b_m} X^{n-m} b_0 - \ \ldots\ - \cancel{\tfrac{a_n}{b_m} X^{n-m} b_m X^m}$$

e dunque $\partial\tilde{F} < n$. Per ipotesi induttiva, $\exists\, \tilde{Q}, \tilde{R}$ tali che $\tilde{F} = G\tilde{Q} + \tilde{R}$ e $\partial\tilde{R} < \partial G$. Allora:

$$F = \tilde{F} + \tfrac{a_n}{b_m} X^{n-m} G = G\big(\tilde{Q} + \tfrac{a_n}{b_m} X^{n-m}\big) + \tilde{R}.$$

Basta quindi porre $Q = \tilde{Q} + \frac{a_n}{b_m} X^{n-m}$, $R = \tilde{R}$ e si ha la tesi.

Nota (1). Il procedimento induttivo sopra descritto riprende la ben nota regola di divisione tra polinomi. Si ha infatti:

$$\begin{array}{l|l} a_n X^n + \ \ldots\ldots\ldots\ + a_0 & b_m X^m + \ldots\ldots\ + b_0 \\ \hline \frac{a_n}{b_m} X^{n-m}\big(b_m X^m + \ldots + b_0\big) & \frac{a_n}{b_m} X^{n-m} + \ldots\ldots \\ \hline \quad \tilde{F} & \\ \quad \ldots\ldots\ldots & \end{array}$$

Dunque $Q_1 := \frac{a_n}{b_m} X^{n-m}$ è il primo addendo del quoziente Q, mentre $\tilde{F}$ è il secondo dividendo della divisione di F per G.

Nota (2). Il procedimento sopra illustrato vale anche in $\boldsymbol{Z}[X]$ [o, più generalmente in ogni $A[X]$, con A dominio d'integrità], a condizione che il divisore G sia un polinomio monico [cioè $b_m = 1$], o più generalmente che abbia coefficiente direttore invertibile.

(*Unicità*). Supponiamo che risulti:

$$F = GQ + R, \text{ con } \partial R < \partial G \text{ e } F = GQ_1 + R_1, \text{ con } \partial R_1 < \partial G.$$

Dimostreremo che $Q = Q_1$ e $R = R_1$.

Se $Q = Q_1$, allora $R = R_1$ [essendo $GQ + R = GQ_1 + R_1$]. Per assurdo, supponiamo $Q \neq Q_1$. Da $GQ + R = GQ_1 + R_1$ segue $R - R_1 = G(Q_1 - Q)$ e quindi

$$\partial(R - R_1) = \partial G + \partial(Q_1 - Q) \geq \partial G \text{ [in quanto } Q_1 - Q \neq 0].$$

Ma $\partial(R - R_1) \leq max\{\partial R, \partial(-R_1)\} = max\{\partial R, \partial R_1\} < \partial G$: assurdo.

Come in $\boldsymbol{Z}$ [ed in ogni dominio d'integrità], anche in $K[X]$ è definita la *relazione di divisibilità*, con proprietà del tutto simili a quella definita in $\boldsymbol{Z}$.

Definizione 1. *In $K[X]$ è definita la seguente relazione di divisibilità* $\big|$: $\forall F, G \in K[X]$,

$$F \,\big|\, G \iff G = FH, \ \exists H \in K[X].$$

Osservazione 1. (*i*) $F \,\big|\, G \iff F\,K[X] \supseteq G\,K[X]$.

(*ii*) $F \,\big|\, 0$ e $1 \,\big|\, F$, $\forall F \in K[X]$;
$0 \,\big|\, F \iff F = 0$; $F \,\big|\, 1 \iff F \in \mathcal{U}(K[X])$ [$= K^{\cdot}$].

(*iii*) La relazione $\big|$ è riflessiva e transitiva, non simmetrica né antisimmetrica.

(*iv*) ogni F ammette i seguenti divisori: c, cF, $\forall c \in K^{\cdot}$ [infatti $F = c(\frac{1}{c}F) = \frac{1}{c}(cF)$]. Sono detti *divisori banali* di F.

(*v*) $F \,\big|\, G \iff FH \,\big|\, GH$, $\forall H \in K[X]^{\cdot}$.

(*vi*) $F \,\Big|\, \begin{matrix} G_1 \\ G_2 \end{matrix} \iff F \,\big|\, A_1G_1 + A_2G_2$, $\forall A_1, A_2 \in K[X]$.

Definizione 2. *Siano $F, G \in K[X]$, con $F, G \neq 0$. Si dice che F, G sono polinomi associati (e si scrive $F \sim G$) se $F \,\big|\, G$ e $G \,\big|\, F$.*

Osservazione 2. (*i*) $F \sim G \iff G = cF$, $\exists c \in K^{\cdot}$. Infatti:

($\Longrightarrow$). $\begin{matrix} G = FH_1 \\ F = GH_2 \end{matrix} \implies G = G(H_2H_1) \implies H_2H_1 = 1 \implies G = cF$, con $c = H_2 \in K^{\cdot}$.

($\Longleftarrow$). da $G = cF$ segue $F \,\big|\, G$ ma anche $F = \frac{1}{c}\,G$ e quindi $G \,\big|\, F$. Dunque $F \sim G$.

(*ii*) $\sim$ è una relazione di equivalenza su $K[X]$ (ovvio). Per ogni $F \in K[X]$, la classe di equivalenza di F modulo $\sim$ è

$$[F]_{\sim} = \{cF, \ \forall c \in K^{\cdot}\}.$$

Si noti che se $F \neq 0$, $[F]_{\sim}$ contiene un unico polinomio monico. Se infatti $F = \sum_{k=0}^{n} a_k X^k$ e $a_n \neq 0$, l'unico polinomio monico in $[F]_{\sim}$ è $\frac{1}{a_n}F$.

Definizione 3. (*Massimo comun divisore*). *Siano $F, G \in K[X]$, non entrambi nulli. Si chiama massimo comun divisore di F, G ogni eventuale polinomio <u>monico</u> $D \in K[X]$ tale che*

$$(i)\ D \,\Big|\, \begin{matrix} F \\ G \end{matrix}; \qquad (ii)\ D' \,\Big|\, \begin{matrix} F \\ G \end{matrix} \implies D' \,\big|\, D.$$

Un tale polinomio D viene usualmente denotato con $MCD(F, G)$, oppure con $GCD(F, G)$ o, più semplicemente, con (F, G).

Nota. Si potrebbe anche lasciar cadere l'ipotesi che D sia monico. In tal caso il MCD sarà però unico solo "a meno di polinomi associati".

Teorema 2. *Il MCD di due polinomi non entrambi nulli in $K[X]$ esiste ed è unico.*

Dim. L'<u>unicità</u> si dimostra come fatto in $\boldsymbol{Z}$. Per l'<u>esistenza</u> si modifica lievemente la corrispondente dimostrazione fatta in $\boldsymbol{Z}$. Precisamente, assegnati $F, G \in K[X]$ non entrambi nulli, sia

$$\mathbf{S} := \boldsymbol{N} \cap \{\partial(AF + BG), \ \ \forall\, A,\, B \in K[X]\}.$$

Certo $\mathbf{S} \neq \emptyset$ [se ad esempio $F \neq 0$, allora $\partial F = \partial(1F + 0G) \in \mathbf{S}$]. In base al principio del Buon Ordinamento (cfr. **Cap. I.5**), $\mathbf{S}$ ha minimo. Sia $D = A_0F + B_0G$ tale che ∂D è un minimo in $\mathbf{S}$. Si può assumere D monico [dividendolo eventualmente per il suo coefficiente direttore]. Dimostreremo che D è un MCD di F, G, verificando le condizioni (i) e (ii) di **Def. 3**.

(i) Per ogni $A, B \in K[X]$, dividiamo per D il polinomio $AF + BG$. Si ha: $AF + BG = DQ + R$, con $\partial R < \partial D$. Si ha:

$$R = AF + BG - DQ = AF + BG - A_0FQ - B_0GQ = (A - A_0Q)F + (B - B_0Q)G.$$

Se fosse $R \neq 0$, allora $\partial R \in \mathbf{S}$ e ciò contraddice la minimalità di ∂D in $\mathbf{S}$. Dunque $R = 0$. Ne segue che $D \,\big|\, AF + BG, \ \ \forall\, A, B \in K[X]$. Da **Osserv. 1**$(vi)$, $D \,\Big|\, \begin{matrix} F \\ G \end{matrix}$.

(ii) Se $D' \,\Big|\, \begin{matrix} F \\ G \end{matrix}$, allora $F = D'A'$, $G = D'B'$ e quindi $D = (A_0A' + B_0B')D'$, cioè $D' \,\big|\, D$.

Corollario 1. (*Identità di Bézout*). *Siano $F, G \in K[X]$, non entrambi nulli. Se $D = MCD(F, G)$, esistono $A, B \in K[X]$ tali che*

$$D = AF + BG \quad \textit{[identità di Bézout per } F, G\textit{]}.$$

Dim. Ovvia conseguenza della dimostrazione dell'esistenza del MCD.

Corollario 2. (*Lemma di Euclide*) *[abbreviato EU]. Siano $F, G, H \in K[X]$. Se $F \,\big|\, GH$ e $MCD(F, G) = 1$, allora $F \,\big|\, H$.*

Dim. Sia $GH = FN$ e $1 = AF + BG$. Allora $H = AFH + BGH = F(AH + BN)$. Dunque $F \,\big|\, H$.

Per il calcolo del MCD si usa l'*algoritmo euclideo delle divisioni successive* (identico a quello che vale in $\boldsymbol{Z}$). Si basa sul seguente risultato.

Proposizione 1. *Siano $F, G \in K[X]$, con $G \neq 0$. Se $F = GQ + R$, con $\partial R < \partial G$, si ha: $MCD(F, G) = MCD(G, R)$.*

Dim. [Si procede come in $\boldsymbol{Z}$]. Posto $D := MCD(F, G)$ e $D_1 := MCD(G, R)$, si tratta di verificare che $D \,\big|\, D_1$ e $D_1 \,\big|\, D$. Essendo D, D_1 monici, allora $D = D_1$.

L'algoritmo delle divisioni successive opera in questo modo: sono assegnati $F, G \in K[X]$ tali che $\partial F \geq \partial G \geq 0$. Risulta:

$$\begin{aligned}
&F = GQ_1 + R_1, \ \ \partial R_1 < \partial G;\\
&G = R_1Q_2 + R_2, \ \ \partial R_2 < \partial R_1;\\
&R_1 = R_2Q_3 + R_3, \ \ \partial R_3 < \partial R_2;\\
&\vdots\\
&R_{n-2} = R_{n-1}Q_n + R_n, \ \ \partial R_n < \partial R_{n-1};\\
&R_{n-1} = R_nQ_{n+1} + 0.
\end{aligned}$$

Allora: $MCD(F, G) = MCD(G, R_1) = MCD(R_1, R_2) = \ \ldots \ = MCD(R_n, 0) = R_n$ (a meno di polinomi associati).

Osservazione 3. Come in $\boldsymbol{Z}$, si può ottenere dall'algoritmo precedente un'identità di Bézout per F, G. Posto $[R_k] = [R_{k-2}] - [R_{k-1}]\,Q_k, \ \ \forall\, k = 1, \ldots, n$ [e posto $R_0 := G$, $R_{-1} := F$], basterà esprimere $[R_n]$ in funzione $[F]$ e $[G]$.

Come in ogni dominio d'integrità, anche in $K[X]$ sono definite le nozioni di elemento primo ed

elemento irriducibile (cfr. **Cap. II, Def. 3.2**).

Definizione 4. *Un polinomio* $P \in K[X]$ *di grado* ≥ 1 *è detto irriducibile se ammette soltanto divisori banali, ovvero ammette soltanto fattorizzazioni banali [cioè fattorizzazioni in cui uno dei fattori è invertibile]. Pertanto:* P *è irriducibile* $\iff \big[P = FG \text{ e } F \notin K^{\cdot} \implies G \in K^{\cdot}\big]$. *Inoltre,* P *è detto riducibile se non è irriducibile.*

Un polinomio $P \in K[X]$ *di grado* ≥ 1 *è detto primo se:*

$$P \,\big|\, FG \text{ e } P \not| F \implies P \,\big|\, G$$

[dunque P *è primo* $\iff$ *dividendo un prodotto, divide almeno un fattore].*

Come in ogni dominio d'integrità, ogni polinomio primo è anche irriducibile. Come in $\boldsymbol{Z}$, vale anche in $K[X]$ il viceversa. Infatti vale il seguente risultato.

Proposizione 2. *Ogni polinomio irriducibile in* $K[X]$ *è anche primo. [Il viceversa è ovviamente vero].*

Dim. Sia $P \in K[X]$ irriducibile. Supponiamo che $P \,\big|\, FG$ e $P \not| F$: proveremo che $P \,\big|\, G$.

Come in $\boldsymbol{Z}$, si tratta di una conseguenza del lemma di Euclide. Sia $D := MCD(P, F)$. Poiché $D \,\big|\, P$ e P è irriducibile, allora $D = 1$ oppure $D \sim P$. Se fosse $D \sim P$, allora $P \,\big|\, D$. Ma $D \,\big|\, F$ e quindi, per transitività, $P \,\big|\, F$: escluso, per ipotesi. Dunque $D = 1$. Da *EU,* segue che $P \,\big|\, G$.

Osservazione 4. Le precedenti definizioni di polinomio irriducibile e polinomio primo sussistono anche in $A[X]$, con A dominio d'integrità. [Infatti anche $A[X]$ è un dominio d'integrità, cfr. **Osserv. 1.3**]. Non è però in generale vero che in $A[X]$ ogni polinomio irriducibile è anche primo. (cfr. **Cap. II, Osserv. 3.2**). Dimostreremo comunque che in $\boldsymbol{Z}[X]$ ogni polinomio irriducibile è primo (cfr. la successiva **Osserv. 3.9**).

Vale infine l'analogo del teorema Fondamentale dell'Aritmetica, detto *teorema di fattorizzazione unica* in $K[X]$. La dimostrazione (che verrà omessa) è perfettamente analoga a quella fatta in $\boldsymbol{Z}$. Basta procedere per induzione (forte) sul grado dei polinomi.

Teorema 3. ($K[X]$ *è un dominio a fattorizzazione unica*).

(**1**) *Ogni polinomio* $F \in K[X], \partial F \geq 1$ *è prodotto di un numero finito di polinomi irriducibili (o primi).*

(**2**) *Posto* $F = \prod_{i=1}^{s} P_i^{r_i}$, *con* $\begin{cases} s \geq 1, \\ P_1, \ldots, P_s \text{ polinomi irriducibili a due a due non associati,} \\ r_1, \ldots, r_s \geq 1, \end{cases}$

tale espressione è unica, a meno dell'ordine dei fattori P_i *ed a meno di polinomi ad essi associati.*

Osservazione 5. Si dice che un dominio d'integrità A è un *dominio a fattorizzazione unica* (abbreviato *UFD*) se:

(**1**) Ogni elemento $a \in A^{\cdot} - \mathcal{U}(A)$ è prodotto di un numero finito di elementi irriducibili.

(**2**) Tale fattorizzazione (come prodotto di elementi irriducibili) è unica, a meno dell'ordine e di fattori ad essi associati.

Il precedente **Teor. 3** può sinteticamente essere enunciato nella forma: $K[X]$ è un *UFD*. Analogamente, il teorema Fondamentale dell'Aritmetica si può enunciare nella forma: $\boldsymbol{Z}$ è un *UFD*.

Esempio 1. Verifichiamo che $X^2 - 2 \in \boldsymbol{Q}[X]$ è irriducibile.

Per assurdo, $X^2-2=FG$ ammetta in $\boldsymbol{Q}[X]$ fattorizzazione non banale FG. Necessariamente $\partial F=\partial G=1$, F, G. Si noti che in $\boldsymbol{R}[X]$ sussiste la fattorizzazione: $X^2-2=(X-\sqrt{2})(X+\sqrt{2})$ e che i quattro polinomi F, G, $X-\sqrt{2}$, $X+\sqrt{2}$ sono irriducibili in $\boldsymbol{R}[X]$ (in quanto di grado 1). Allora, dal fatto che $\boldsymbol{R}[X]$ è un *UFD,* segue ad esempio che $F\sim X-\sqrt{2}$, cioè

$$F=a(X-\sqrt{2})=aX-a\sqrt{2},\ \text{con}\ a\in\boldsymbol{R}^{\cdot}.$$

Poiché $F\in\boldsymbol{Q}[X]$, allora a, $-a\sqrt{2}\in\boldsymbol{Q}$ e dunque $\sqrt{2}\in\boldsymbol{Q}$: assurdo. Analoga conclusione si ottiene se $F\sim X+\sqrt{2}$.

Osservazione 6. In analogia a quanto visto in $\boldsymbol{Z}$, assegnati due polinomi F, $G\in K[X]$, si chiama *minimo comune multiplo di* F, G un eventuale polinomio monico $H=mcm(F,G)\in K[X]$, tale che

$$(i)\ \begin{matrix}F\\G\end{matrix}\Big|\,H\ ;\qquad (ii)\ \begin{matrix}F\\G\end{matrix}\Big|\,H'\implies H\,|\,H'.$$

L'esistenza ed unicità del *mcm* segue subito dal **Teor. 3**. Posto infatti

$$F=\prod_{i=1}^{t}P_i^{\,r_i},\ G=\prod_{i=1}^{t}P_i^{\,s_i},\ \text{con i}\ P_i\ \text{irriducibili e}\ r_i,s_i\geq 0,$$

si può verificare (cfr. **Prop. II. 3.2**) che $H\sim\prod_{i=1}^{t}P_i^{\,D_i}$, con $D_i=max(r_i,s_i)$. Analogamente, se $D=MCD(F,G)$, risulta $D\sim\prod_{i=1}^{t}P_i^{\,d_i}$, con $d_i=min(r_i,s_i)$. Ne segue (cfr. **Cor. II. 3.4**) che

$$FG\sim MCD(F,G)\,mcm(F,G).$$

Veniamo ora al concetto di *zero* o *radice* di un polinomio.

Definizione 5. *Sia $P\in K[X]$ e sia $\alpha\in K$. α è detto zero (o radice) di P se $P(\alpha)=0$.*

Proposizione 3. *(Teorema di Ruffini). α è uno zero di $P\iff X-\alpha\,|\,P$.*

Dim. ($\Longrightarrow$). Dal **Teor. 1**, $P=(X-\alpha)\,Q+R$, con $\partial R\leq 0$. Per ipotesi, $P(\alpha)=0$ e dunque $0=P(\alpha)=(\alpha-\alpha)\,Q(\alpha)+R=0+R=R$. Ne segue che $X-\alpha\,|\,P$.

($\Longleftarrow$). Da $X-\alpha\,|\,P$, $P=(X-\alpha)\,G$. Quindi $P(\alpha)=(\alpha-\alpha)\,G(\alpha)=0$.

Nota. Si può anche assumere che lo zero α di P appartenga ad un campo $L\supseteq K$. In tal caso si ha: *α è uno zero di $P\iff X-\alpha\,|\,P$ <u>in</u> $L[X]$.*

Definizione 6. *Sia $P\in K[X]$, sia $\alpha\in K$ e sia $t\in\boldsymbol{N}$. α è detto zero di molteplicità t di P se risulta: $(X-\alpha)^t\,|\,P$, ma $(X-\alpha)^{t+1}\not|\,P$. In particolare, uno zero di molteplicità 0 non è uno zero di P. Inoltre, se uno zero ha molteplicità 1 è detto semplice, se ha molteplicità ≥ 2 è detto multiplo.*

Proposizione 4. *Sia $P\in K[X]$, con $n=\partial P\geq 0$. Gli zeri di P sono al più n, contati con la rispettiva molteplicità.*

Dim. Per induzione forte su $n=\partial P\geq 0$.

$\boldsymbol{n=0}$. In tal caso $P=c\neq 0$ e quindi non esistono zeri di P, cioè gli zeri di P sono al più 0.

$\boldsymbol{n\geq 1}$. Supponiamo vero il risultato per ogni polinomio in $K[X]$ di grado $<n$ e dimostriamo il teorema per P.

Sia α uno zero di P, con molteplicità $t\geq 1$. Dunque P ha t zeri uguali ad α e $P=(X-\alpha)^tQ$, con $0\leq\partial Q=n-t<n$. Sia β un altro zero di P, $\beta\neq\alpha$. Poiché $0=P(\beta)=(\beta-\alpha)^tQ(\beta)$, allora $Q(\beta)=0$, cioè β è uno zero di Q. Per ipotesi induttiva, applicata a Q, Q ha al più $n-t$ zeri (contati con la rispettiva molteplicità). Ne segue che P ha al più $t+(n-t)=n$ zeri (contati con la rispettiva molteplicità).

Corollario 3. *(Principio d'identità dei polinomi). Se K è un campo <u>infinito</u>, l'applicazione*

$$\Phi : K[X] \to \mathcal{F}_K \quad \textit{tale che} \quad \Phi(P) = \Phi_P \quad \textit{[cfr.} \ \textbf{Prop. 1.2}\textit{]}$$

è un isomorfismo (di anelli).

Dim. C'è solo da verificare che Φ è iniettiva, e cioè che: $\Phi(P) = \Phi(Q) \implies P = Q$.
Φ è un omomorfismo e dunque $\Phi_{P-Q} = \Phi_P - \Phi_Q = \mathbf{0}$. Ne segue che, $\forall\, c \in K$: $0 = \Phi_{P-Q}(c) = (P-Q)(c)$. Il polinomio $P - Q$ ha quindi infiniti zeri. Allora $P - Q = 0$ [altrimenti, in base a **Prop. 4**, $P - Q$ avrebbe al più $\partial(P - Q)$ zeri].

Osservazione 7. (*i*) Si noti che il teorema di Ruffini e la **Prop. 4** valgono (con la stessa dimostrazione) anche per ogni anello $A[X]$, con A dominio d'integrità. Ne segue che il principio d'identità dei polinomi (**Cor. 3**) vale anche per ogni anello $A[X]$, con A dominio d'integrità <u>infinito</u> [ad esempio $\boldsymbol{Z}[X]$].

(*ii*) Dal teorema di Ruffini discende il seguente risultato:

Siano $F, G \in K[X]$, con F irriducibile. Se F, G hanno in comune uno zero α, in un campo $L \supseteq K$, allora $F \,|\, G$.

Dimostriamo tale risultato. Osserviamo che F è unico, a meno di una costante non nulla in K. Se infatti $\tilde{F}$ è un polinomio irriducibile in $K[X]$, di grado minimo tale che $\tilde{F}(\alpha) = 0$, e se $F = \tilde{F}\tilde{Q} + \tilde{R}$, con $\partial\tilde{R} < \partial\tilde{F}$, segue subito che $\tilde{R}(\alpha) = 0$ e quindi $R = 0$. Poiché F è irriducibile, allora $\tilde{Q} = c \in K^{\cdot}$. Dividendo G per F, si ottiene $G = FQ + R$, con $\partial R < \partial F$. Poiché $R(\alpha) = 0$, allora $R = 0$, cioè $F \,|\, G$.

Nota. Seguiremo di solito la convenzione di indicare i polinomi in $\boldsymbol{Z}[X]$ con lettere minuscole, mentre quelli in $K[X]$ con lettere maiuscole. Ciò sarà utile nel seguito, quando confronteremo polinomi in $\boldsymbol{Z}[X]$ con polinomi in $\boldsymbol{Q}[X]$.

Osservazione 8. *Ricerca di eventuali zeri razionali di polinomi in $\boldsymbol{Z}[X]$.* Sia $f = \sum_{i=0}^{n} a_i X^i \in \boldsymbol{Z}[X]$. Sia $\alpha = \frac{r}{s} \in \boldsymbol{Q}$, con $(r, s) = 1$. Dimostriamo la seguente affermazione:

$$(*) \qquad f(\alpha) = 0 \implies r \,|\, a_0 \ \text{ e } \ s \,|\, a_n.$$

Ne segue che gli eventuali zeri razionali di f vanno cercati tra le frazioni $\frac{r}{s}$ [con $(r, s) = 1$] il cui numeratore divide il termine noto di f ed il cui denominatore divide il coefficiente direttore di f.

Dimostriamo $(*)$. Da $f(\alpha) = 0$, segue $\sum_{i=0}^{n} a_i \frac{r^i}{s^i} = 0$. Allora (moltiplicando per s^n):

$$a_0 s^n + a_1 s^{n-1} r + \ .... \ + a_{n-1} s r^{n-1} + a_n r^n = 0.$$

Ne segue, per opportuni $h, k \in \boldsymbol{Z}$:

$$\begin{cases} 0 = a_0 s^n + rh \\ 0 = sk + a_n r^n \end{cases} \quad \text{e quindi} \quad \begin{cases} r \,|\, a_0 s^n \\ s \,|\, a_n r^n. \end{cases}$$

Poiché $(r, s) = 1$, allora $(r, s^n) = (s, r^n) = 1$ e quindi (da *EU*) $r \,|\, a_0$ e $s \,|\, a_n$.

Ad esempio, cerchiamo gli eventuali zeri razionali del polinomio

$$f = X^5 + 40X^3 + 80X^2 + 90X - 31 \in \boldsymbol{Z}[X].$$

Se $\alpha = \frac{r}{s}$ è uno zero razionale di f, allora $\begin{cases} r \,|\, -31 \\ s \,|\, 1. \end{cases}$

Dunque $r \in \{\pm 1, \pm 31\}$, $s \in \{\pm 1\}$ e quindi $\alpha \in \{\pm 1, \pm 31\}$.

Ma $f(1),\ f(-1),\ f(31),\ f(-31) \neq 0$ (come facilmente si verifica) . Quindi f non ha zeri razionali.

3. Polinomi irriducibili

Esamineremo l'irriducibilità dei polinomi in $\boldsymbol{C}[X]$, $\boldsymbol{R}[X]$, $\boldsymbol{Q}[X]$ e $\boldsymbol{Z}[X]$. Ma cominciamo con alcuni semplici risultati sull'irriducibilità, di carattere generale, validi cioè in $K[X]$, con K campo qualsiasi.

Proposizione 1. *Sia K un campo. Sia $F \in K[X]$.*

(1) $\partial F = 1 \implies F$ è irriducibile in $K[X]$.

(2) Sia $\partial F \geq 2$.

(a) F irriducibile in $K[X] \implies F$ non ha zeri in K.

(b) F non ha zeri in $K \implies F$ non ha fattori di grado 1 in $K[X]$.

(3) Sia $2 \leq \partial F \leq 3$. F è irriducibile in $K[X] \iff F$ non ha zeri in K.

(4) Sia $\partial F \geq 4$. F non ha zeri in $K \not\Longrightarrow F$ è irriducibile.

Dim. (*1*). Sia $\partial F = 1$ e sia $F = GH$. Poiché $\partial G + \partial H = 1$, allora $\partial G = 0$ oppure $\partial H = 0$, cioè $G \in K^\cdot$ oppure $H \in K^\cdot$. Dunque GH è una fattorizzazione banale di F.

(*2a*). Per assurdo, $\exists\, \alpha \in K \ : \ F(\alpha) = 0$. Allora $X - \alpha \,\big|\, F$, cioè $F = (X - \alpha)G$, con $\partial G = \partial F - 1 \geq 1$. Dunque F non è irriducibile: assurdo.

(*2b*). Per assurdo, $aX + b \,\big|\, F$, con $a, b \in K$, $a \neq 0$. Allora $F = (aX + b)G$, e quindi $F(-\frac{b}{a}) = 0$. F ha quindi lo zero $-\frac{b}{a} \in K$: assurdo.

(*3*). ($\Longrightarrow$). È già stato dimostrato (cfr. *(2a)*).

($\Longleftarrow$). Da (*2b*), F non ha fattori di grado 1. Sia $F = GH$. Se nessuno dei fattori G, H è costante, allora $\partial G, \partial H \geq 2$ e dunque $\partial F = \partial G + \partial H \geq 4$: assurdo. Ne segue che la fattorizzazione è banale e dunque F è irriducibile.

(*4*). Ad esempio $F = (X^2 + 1)^2 \in \boldsymbol{Q}[X]$ non ha zeri in $\boldsymbol{Q}$ ma è ovviamente riducibile [in quanto $F = (X^2 + 1)(X^2 + 1)$].

Proposizione 2. *Siano k, K due campi, con $k \subset K$. Sia $F \in k[X]$ (e quindi $F \in K[X]$). Risulta:*

(1) F irriducibile in $K[X] \implies F$ irriducibile in $k[X]$.

(2) F irriducibile in $k[X] \not\Longrightarrow F$ irriducibile in $K[X]$.

Dim. (*1*). Sia $F = GH$, con $G, H \in k[X]$. Poiché tale fattorizzazione sussiste anche in $K[X]$, allora è banale, cioè $G \in K^\cdot$ (oppure $H \in K^\cdot$). Ma allora $G \in k^\cdot$ [infatti si ha: $K^\cdot \cap k[X] = k^\cdot$], oppure $H \in k^\cdot$. Dunque F è irriducibile su k.

(*2*). Se ad esempio $k = \boldsymbol{Q}$, $K = \boldsymbol{R}$ ed $F = X^2 - 2$, allora F è irriducibile in $\boldsymbol{Q}[X]$, ma non in $\boldsymbol{R}[X]$ [cfr. il precedente **Esempio 1**].

Osservazione 1. Se confrontiamo l'irriducibilità in $\boldsymbol{Z}[X]$ con quella in $\boldsymbol{Q}[X]$, la situazione descritta nella **Prop. 2** curiosamente si ribalta. Sia infatti $f \in \boldsymbol{Z}[X]$ (e quindi $f \in \boldsymbol{Q}[X]$). Risulta:

(1) f irriducibile in $\boldsymbol{Q}[X] \not\Longrightarrow f$ irriducibile in $\boldsymbol{Z}[X]$.

(2) f irriducibile in $\boldsymbol{Z}[X] \implies f$ irriducibile in $\boldsymbol{Q}[X]$.

Per la (*1*) basta osservare che $f = 2X - 2$ è irriducibile in $\boldsymbol{Q}[X]$ ma non in $\boldsymbol{Z}[X]$: infatti $f = 2(X - 1)$ e tale fattorizzazione non è banale [in quanto i polinomi 2, $X - 1$ non sono invertibili in $\boldsymbol{Z}[X]$]. L'affermazione (*2*) è il *Teorema di Gauss* [cfr. il successivo **Teor. 2**].

Osservazione 2. Per valutare l'irriducibilità di un polinomio $F \in K[X]$, può essere utile trasformare F applicandogli un *automorfismo* di $K[X]$ (cioè un omomorfismo biiettivo di $K[X]$ in se

stesso, cfr. **Def. I.4.10**). Vale infatti il seguente risultato:

(∗) *Se* $\varphi : K[X] \to K[X]$ *è un automorfismo di anelli, risulta,* $\forall\, P \in K[X]$*:*

$$P \text{ è irriducibile } \iff \varphi(P) \text{ è irriducibile.}$$

Premettiamo due osservazioni, valide per ogni automorfismo φ di $K[X]$:

(*1*) $\varphi(K) = K$.

Per ogni $c \in K^\cdot$, risulta: $1 = \varphi(1) = \varphi(c\,c^{-1}) = \varphi(c)\,\varphi(c^{-1})$ e dunque $\varphi(c) \in \mathcal{U}(K[X]) = K^\cdot$. Poiché inoltre $\varphi(0) = 0$, allora $\varphi(K) \subseteq K$. Viceversa, poiché anche φ^{-1} è un automorfismo (cfr. **Prop. IV.6.1**), allora $\varphi^{-1}(K) \subseteq K$. Ne segue che $K = \varphi\big(\varphi^{-1}(K)\big) \subseteq \varphi(K)$. Dunque $\varphi(K) = K$.

(*2*) $\partial\,\varphi(X) = 1$ *e* φ *conserva il grado dei polinomi.*

Da (*1*), $\partial\,\varphi(X) \geq 1$ e, per assurdo, sia $\partial\,\varphi(X) \geq 2$. Per ogni polinomio $P = \sum_{i=0}^{n} a_i X^i$ di grado $n \geq 1$, $\varphi(P) = \sum_{i=0}^{n} \varphi(a_i)\varphi(X)^i$ e dunque $\partial\,\varphi(P) = \partial\,\varphi(X)^n = n \cdot \partial\,\varphi(X) \geq 2n \geq 2$. Dunque $Im(\varphi)$ non conterrebbe polinomi di grado 1: assurdo, in quanto φ è suriettiva. Ne segue quindi che $\partial\,\varphi(X) = 1$ e dunque $\partial\,\varphi(P) = \partial\,P$, cioè φ conserva il grado dei polinomi.

Possiamo ora verificare la precedente affermazione (∗). Se $P = FG$, allora $\varphi(P) = \varphi(F)\,\varphi(G)$. Poiché $\partial\,\varphi(F) = \partial F$ e $\partial\,\varphi(G) = \partial G$, allora FG è una fattorizzazione banale di $P \iff \varphi(F)\varphi(G)$ è una fattorizzazione banale di $\varphi(P)$]. Dunque P è irriducibile $\iff \varphi(P)$ lo è.

I più semplici automorfismi φ di $K[X]$, sono quelli per cui risulta $\varphi_{|_K} = \mathbf{1}_K$. Essi vengono detti *sostituzioni lineari* (o K*-automorfismi*) di $K[X]$. Se $\varphi : K[X] \to K[X]$ è una sostituzione lineare e se $f := \varphi(X) = aX + b$ (con $a, b \in K$, $a \neq 0$), allora φ è completamente individuata da f. Infatti

$$\varphi\big(\sum_{i=0}^{n} a_i X^i\big) = \sum_{i=0}^{n} a_i\,(aX + b)^i, \quad \forall\, \sum_{i=0}^{n} a_i X^i \in K[X]$$

[si dice in tal caso che φ è associata ad f e si scrive $\varphi = \varphi_f$]. Si verifica con facilità che l'inversa di una sostituzione lineare è una sostituzione lineare. Precisamente, se φ è associata ad $f = aX + b$, allora φ^{-1} è associata a $g = \frac{1}{a}X - \frac{b}{a}$ [infatti $\varphi^{-1}(\varphi(X)) = \varphi^{-1}(aX + b) = a(\frac{1}{a}X - \frac{b}{a}) + b = X$].

Talvolta, volendo verificare se un polinomio $P \in K[X]$ è irriducibile, si applica ad esso una sostituzione lineare φ e si indaga sull'irriducibilità di $\varphi(P)$. Se ad esempio si verifica che $\varphi(P)$ ammette la fattorizzazione non banale $\varphi(P) = FG$, allora P ammette la fattorizzazione non banale $P = \varphi^{-1}(F)\varphi^{-1}(G)$.

Si noti infine che, se A è un dominio d'integrità, ogni sostituzione lineare associata ad un polinomio monico $X + a$ è un automorfismo di $A[X]$ (la cui inversa è la sostituzione lineare associata a $X - a$). Dunque per valutare l'irriducibilità di F può essere conveniente trasformare F in $F(X + a)$, scegliendo opportunamente $a \in A$ [come faremo nel successivo **Esempio 2**].

(***A***) IRRIDUCIBILITA' IN $\boldsymbol{C}[X]$.

Enunciamo (senza dimostrazione) il seguente teorema, noto come *Teorema Fondamentale dell'Algebra*. Si tratta di un risultato fondamentale della Matematica, la cui prima dimostrazione è dovuta a Gauss (1799). Delle varie dimostrazioni di tale risultato, le più elementari utilizzano semplici strumenti di Analisi Matematica (come il teorema di Weierstrass). Per una dimostrazione rinviamo ai testi di Algebra segnalati in bibliografia (ad esempio *Fontana-Gabelli*).

Teorema 1. *(Teorema Fondamentale dell'Algebra) [abbr. TFA]. Ogni polinomio non costante in* $\boldsymbol{C}[X]$ *ha almeno uno zero in* $\boldsymbol{C}$.

Corollario 1. *Sia* $F \in \boldsymbol{C}[X]$. F *è irriducibile* $\iff \partial F = 1$.

Dim. ($\Longleftarrow$). Segue dalla **Prop. 1**(*1*).

($\Longrightarrow$). Sia $\partial F \geq 2$. Dal *TFA*, $\exists\, \alpha \in \boldsymbol{C}$ tale che $F(\alpha) = 0$. Dal teorema di Ruffini, $X - \alpha \,\big|\, F$ ed

$X-\alpha$ è un divisore proprio di F. Ne segue che F è riducibile.

(***B***) IRRIDUCIBILITA' IN $\boldsymbol{R}[X]$.

Proposizione 3. *Sia* $F \in \boldsymbol{R}[X]$. *Risulta:*

$$F \text{ è irriducibile (in } \boldsymbol{R}[X]) \iff \partial F = 1 \text{ oppure } \partial F = 2 \text{ e } \Delta_F < 0,$$

dove $\Delta_F := b^2 - 4ac$, *se* $F = aX^2 + bX + c$. *Il numero reale* Δ_F *è detto discriminante di* F.

Per dimostrare tale proposizione faremo uso dei due seguenti lemmi.

Lemma 1. *Sia* $F = aX^2 + bX + c \in \boldsymbol{R}[X]$, $a \neq 0$. *Si ha:*

$$F \text{ è riducibile (in } \boldsymbol{R}[X]) \iff \Delta_F \geq 0.$$

Dim. ($\Longrightarrow$). Se F è riducibile, è prodotto di due fattori di grado 1:

$$F = (b_0 + b_1X)(c_0 + c_1X) = b_0c_0 + (b_0c_1 + b_1c_0)X + b_1c_1X^2.$$

Allora $\Delta_F = (b_0c_1 + b_1c_0)^2 - 4b_0c_0b_1c_1 = (b_0c_1 - b_1c_0)^2 \geq 0$.

($\Longleftarrow$). Sia $F = aX^2 + bX + c$ con $\Delta_F \geq 0$. Si consideri il numero reale $x := \frac{-b+\sqrt{\Delta_F}}{2a}$. Con semplici calcoli si verifica che $F(x) = ax^2 + bx + c = \ ... \ = 0$.
Dunque F ha uno zero in $\boldsymbol{R}$ e pertanto (in base a **Prop. 1(*3*)**) F è riducibile (in $\boldsymbol{R}[X]$).

Lemma 2. *Sia* $F \in \boldsymbol{R}[X]$, *con* $\partial F \geq 3$. F *è sempre riducibile (in* $\boldsymbol{R}[X]$*).*

Dim. Sia $F = \sum_{i=0}^{n} a_i X^i \in \boldsymbol{R}[X]$, con $n = \partial F \geq 3$. Dal *TFA*, $\exists\, \alpha \in \boldsymbol{C}$ tale che $F(\alpha) = 0$. Se $\alpha \in \boldsymbol{R}$, dalla **Prop. 1(*2*)** segue che F è riducibile e la tesi è dimostrata.
Sia invece $\alpha \in \boldsymbol{C} - \boldsymbol{R}$. In tal caso $\overline{\alpha} \neq \alpha$. Verifichiamo che anche $F(\overline{\alpha}) = 0$. Infatti:

$$F(\overline{\alpha}) = \sum_{i=0}^{n} a_i \overline{\alpha}^{\,i} = \sum_{i=0}^{n} \overline{a}_i \overline{\alpha}^{\,i} = \overline{\sum_{i=0}^{n} a_i \alpha^{\,i}} = \overline{0} = 0.$$

Ne segue che $X - \alpha \,\big|\, F$ e che $X - \overline{\alpha} \,\big|\, F$ (in $\boldsymbol{C}[X]$). Allora anche $(X-\alpha)(X-\overline{\alpha}) \,\big|\, F$ (in $\boldsymbol{C}[X]$). Si ha:

$$G := (X-\alpha)(X-\overline{\alpha}) = X^2 - 2\mathcal{R}e(\alpha)X + \mathcal{N}(\alpha),$$

e dunque $G \in \boldsymbol{R}[X]$.

Si ponga ora (sempre in $\boldsymbol{C}[X]$) $F = GH$, con $H = \sum_{j=0}^{n-2} \alpha_j X^j \in \boldsymbol{C}[X]$ [si noti che $\partial H = \partial F - 2 \geq 3-2 = 1$]. Se dimostriamo che $H \in \boldsymbol{R}[X]$, otterremo che F è riducibile in $\boldsymbol{R}[X]$ (con fattorizzazione non banale GH), come richiesto. Per semplificare le notazioni, poniamo $G := X^2 + aX + b$ (con $a = -\mathcal{R}e(\alpha)$, $b = \mathcal{N}(\alpha)$). Da $F = GH$, segue che:

$$a_0 = b\alpha_0, \quad a_1 = b\alpha_1 + a\alpha_0, \quad a_2 = b\alpha_2 + a\alpha_1 + \alpha_0, \quad ...., \quad a_{n-2} = b\alpha_{n-2} + a\alpha_{n-3} + \alpha_{n-4}.$$

Allora

$$\alpha_0 = \tfrac{a_0}{b} \in \boldsymbol{R}, \quad \alpha_1 = \tfrac{a_1 - a\alpha_0}{b} \in \boldsymbol{R}, \quad \alpha_2 = \tfrac{a_2 - a\alpha_1 - \alpha_0}{b} \in \boldsymbol{R}, \quad .... \ , \ \alpha_{n-2} = \tfrac{a_{n-2} - a\alpha_{n-3} - \alpha_{n-4}}{b} \in \boldsymbol{R}.$$

Dunque $H \in \boldsymbol{R}[X]$, come richiesto.

Siamo ora in grado di concludere la dimostrazione di **Prop. 3**.

Dim. (Prop. 3) ($\Longrightarrow$). Sia F irriducibile. Dal **Lemma 2**, $1 \leq \partial F \leq 2$. Se $\partial F = 2$, dal **Lemma 1** segue che $\Delta_F < 0$.

($\Longleftarrow$). Se $\partial F = 1$, F è irriducibile (dalla **Prop. 1(*1*)**). Se $\partial F = 2$ e $\Delta_F < 0$, F è irriducibile (dal **Lemma 1**).

($\boldsymbol{C}$) IRRIDUCIBILITA' IN $\boldsymbol{Q}[X]$.

Sia $F \in \boldsymbol{Q}[X]$. Dalla **Prop. 2(*1*)** segue che se F è irriducibile in $\boldsymbol{R}[X]$, allora lo è anche in $\boldsymbol{Q}[X]$. In base a **Prop. 3**, sono quindi irriducibili in $\boldsymbol{Q}[X]$ tutti i polinomi F tali che $\partial F = 2$ e $\Delta_F < 0$. Ma ce ne sono molti altri: ad esempio $F = X^2 - 2$ è irriducibile in $\boldsymbol{Q}[X]$ anche se $\Delta_F = 8 > 0$.

Invece di confrontare l'irriducibilità in $\boldsymbol{Q}[X]$ con quella in $\boldsymbol{R}[X]$, si rivelerà più conveniente confrontarla con quella in $\boldsymbol{Z}[X]$. In effetti, come facilmente si osserva (cfr. il successivo **Lemma 3**), ogni polinomio in $\boldsymbol{Q}[X]$ coincide, a meno di una costante moltiplicativa in $\boldsymbol{Q}$, con un polinomio in $\boldsymbol{Z}[X]$. Vale poi, come vedremo, il seguente risultato (*Teorema di Gauss*): *se un polinomio $f \in \boldsymbol{Z}[X]$ è irriducibile in $\boldsymbol{Z}[X]$, lo è anche in $\boldsymbol{Q}[X]$.*

Studieremo quindi i legami tra l'irriducibilità in $\boldsymbol{Z}[X]$ e in $\boldsymbol{Q}[X]$.

Definizione 1. *Sia $f = \sum_{i=0}^{n} a_i X^i \in \boldsymbol{Z}[X]$, $\partial f \geq 1$. Si chiama contenuto di f (o content di f) il numero naturale $c(f) = c_f := MCD(a_0, a_1, \ldots, a_n)$. Se $\partial f = 0$ e $f = c \in \boldsymbol{Z}^*$, si pone $c(f) = |c|$. Se $c(f) = 1$, f è detto primitivo.*

Osservazione 3. Assegnato $f = \sum_{i=0}^{n} a_i X^i \in \boldsymbol{Z}[X]$, $f \neq 0$, risulta ovviamente che

$$f = c(f)\, f_*, \quad \text{con} \quad f_* = \sum_{i=0}^{n} \tfrac{a_i}{c(f)} X^i$$

polinomio primitivo [infatti $MCD\big(\frac{a_0}{c(f)}, \ldots, \frac{a_n}{c(f)}\big) = 1$]. Inoltre, la scrittura di un polinomio come prodotto di un numero naturale per un polinomio primitivo è unica, come ora verificheremo.

Sia infatti $f = a\, f_1 = b\, f_2$, con $a, b \geq 1$ e f_1, f_2 polinomi primitivi. Si ha:

$$c(f) = \begin{cases} c(af_1) = |a|\, c(f_1) = a \cdot 1 = a \\ c(bf_2) = |b|\, c(f_2) = b \cdot 1 = b. \end{cases}$$

Dunque $a = b$ e pertanto $f_1 = f_2$.

Proposizione 4. (*Lemma di Gauss* - 1^a **formulazione**). *Siano $f, g \in \boldsymbol{Z}[X]^*$. Se f, g sono primitivi, anche il loro prodotto fg è primitivo.*

Dim. Siano $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{j=0}^{m} b_j X^j \in \boldsymbol{Z}[X]$ polinomi primitivi (non nulli).

Per assurdo, fg non sia primitivo: dunque esiste un primo p tale che $p \,|\, c(fg)$. Per definizione di prodotto, $fg = \sum_{s=0}^{n+m} c_s X^s$, con $c_s = \sum_{t=0}^{s} a_t b_{s-t}$. Poiché f, g sono primitivi:

$$\begin{cases} \exists\, h \ \text{ tale che } \ p \,|\, a_0, p \,|\, a_1, \ldots, p \,|\, a_{h-1}, p \nmid a_h, \ \text{ con } \ 0 \leq h \leq n; \\ \exists\, k \ \text{ tale che } \ p \,|\, b_0, p \,|\, b_1, \ldots, p \,|\, b_{k-1}, p \nmid b_k, \ \text{ con } \ 0 \leq k \leq m. \end{cases}$$

Consideriamo il coefficiente c_{h+k} di fg:

$$c_{h+k} = \underbrace{a_0 b_{h+k} + \ \ldots \ + a_{h-1} b_{k+1}}_{\alpha} + a_h b_k + \underbrace{a_{h+1} b_{k-1} + \ldots \ + a_{h+k} b_0}_{\beta}.$$

Dunque $c_{h+k} = \alpha + a_h b_k + \beta$. Per definizione di h, k: $p \,|\, \alpha$ e $p \,|\, \beta$. Inoltre, per ipotesi, $p \,|\, c_{h+k}$. Ne segue che $p \,|\, a_h b_k$ e quindi (essendo p primo) $p \,|\, a_h$ oppure $p \,|\, b_k$: assurdo.

Nota. Vale anche il viceversa: *se fg è primitivo, anche f, g sono primitivi.*

Se infatti, per assurdo ad esempio f non fosse primitivo, esisterebbe un primo p tale che $p \,|\, a_i$, $\forall\, i = 0, \dots, n$. Ma allora $p \,|\, c_s$, $\forall\, s = 0, \dots, n+m$, e dunque $c(fg) \neq 1$: assurdo.

Corollario 2. (*Lemma di Gauss - 2ª* **formulazione**). *Siano* $f, g \in \boldsymbol{Z}[X]^{\cdot}$. *Risulta:*

$$c(fg) = c(f)c(g).$$

Dim. Risulta: $f = c(f)\, f_*$, $g = c(g)\, g_*$, con f_*, g_* primitivi. Ne segue:

$$fg = \begin{cases} c(f)c(g)\, f_* g_* \\ c(fg)\, (fg)_* \end{cases} \quad (\text{con } (fg)_* \text{ primitivo}).$$

Dal Lemma di Gauss (1ª formulazione) $f_* g_*$ è primitivo. Ne segue, per unicità di scrittura (cfr. **Osserv. 3**) che $c(f)c(g) = c(fg)$.

Veniamo ora allo studio dei legami tra polinomi in $\boldsymbol{Q}[X]$ e in $\boldsymbol{Z}[X]$.

Lemma 3. *Sia* $F \in \boldsymbol{Q}[X]^{\cdot}$. *Esistono* $q \in \boldsymbol{Q}$ *ed* $f \in \boldsymbol{Z}[X]$ *primitivo, con* $\partial f = \partial F$ *e* $F = qf$.

Dim. Se $\partial F = 0$, basta porre $q = F$ e $f = 1$. Sia quindi $\partial F \geq 1$. Se $F = \sum_{i=0}^{n} \frac{a_i}{b_i} X^i$ e $m := mcm(b_0, \dots, b_n)$, allora, posto $a'_i = \frac{a_i\, m}{b_i}$, si ha:

$$F = \sum_{i=0}^{n} \frac{a'_i}{m} X^i = \tfrac{1}{m}\, \tilde{f}, \text{ con } \tilde{f} = \sum_{i=0}^{n} a'_i\, X^i \in \boldsymbol{Z}[X].$$

Se $\tilde{f} = c(\tilde{f})\, \tilde{f}_*$, con $f := \tilde{f}_* \in \boldsymbol{Z}[X]$ primitivo, allora:

$$F = \tfrac{c(\tilde{f})}{m}\, f = qf, \text{ con } q = \tfrac{c(\tilde{f})}{m} \in \boldsymbol{Q} \text{ e } \partial f = \partial F.$$

Nota. q ed f sono unici a meno del segno. Sia infatti $F = \frac{a}{b}\, f = \frac{a_1}{b_1}\, f_1$, con f, f_1 primitivi in $\boldsymbol{Z}[X]$. Allora $ab_1 f = ba_1\, f_1$ e quindi $|ab_1| = |a_1 b|$. Ne segue che $\frac{a_1}{b_1} = \pm\frac{a}{b}$ e quindi $f_1 \pm f$.

Teorema 2. (*Teorema di Gauss*). *Sia* $f \in \boldsymbol{Z}[X]^{\cdot}$. *Se* f *si fattorizza in* $\boldsymbol{Q}[X]$, *allora* f *si fattorizza in* $\boldsymbol{Z}[X]$ *con fattori degli stessi gradi, cioè:*

se $f = GH$, *con* $G, H \in \boldsymbol{Q}[X]$, $\exists\, g, h \in \boldsymbol{Z}[X]$ *tali che* $f = gh$ *e* $\partial g = \partial G$, $\partial h = \partial H$.

Ne segue: se f *è irriducibile in* $\boldsymbol{Z}[X]$, *allora è irriducibile anche in* $\boldsymbol{Q}[X]$.

Dim. L'ultima affermazione è una semplice conseguenza della prima. Se infatti per assurdo f fosse riducibile in $\boldsymbol{Q}[X]$, $\exists\, G, H \in \boldsymbol{Q}[X]$ tali che $f = GH$, con $\partial G, \partial H \geq 1$. Ma allora $\exists\, g, h \in \boldsymbol{Z}[X]$ tali che $f = gh$, con $\partial g, \partial h \geq 1$. Dunque f non sarebbe irriducibile in $\boldsymbol{Z}[X]$: assurdo.

Dimostriamo ora la prima parte del teorema.

(a) Assumiamo provvisoriamente f primitivo.

In base al **Lemma 3**,

$G = q_1\, g$, $H = q_2\, h$, con $q_1, q_2 \in \boldsymbol{Q}$ e $g, h \in \boldsymbol{Z}[X]$ polinomi primitivi, con $\partial g = \partial G$ e $\partial h = \partial H$.

Allora $f = GH = (q_1 q_2) gh$. Se $q_1 q_2 = \frac{a}{b}$ (con $a, b \in \boldsymbol{Z}$), allora $bf = agh \in \boldsymbol{Z}[X]$. Quindi $|b|\, c(f) = |a|\, c(gh)$. Essendo f primitivo (per assunzione) e g, h primitivi, allora $|b| = |a|$ (in base al Lemma di Gauss) e quindi $q_1 q_2 = \pm 1$. Dunque $f = \pm gh = (\pm g)h$. Ovviamente $\pm g, h \in \boldsymbol{Z}[X]$ e $\partial(\pm g) = \partial g$. La tesi è quindi dimostrata (nelle attuali ipotesi).

(b) Rimuoviamo l'ipotesi di primitività per f.

Sia $f = cf_*$, con $c = c(f) \in \boldsymbol{N}^{\cdot}$ e $f_* \in \boldsymbol{Z}[X]$ primitivo. Si ha: $f_* = \frac{1}{c}\, f = \frac{1}{c}\, GH = (\frac{1}{c}\, G)H$. Essendo f_* primitivo, da (a) segue che $f_* = gh$, con $f, g \in \boldsymbol{Z}[X]$ primitivi e con $\partial g = \partial(\frac{1}{c}\, G) = \partial G$, $\partial h = \partial H$. Ne segue che $f = cf_* = c(gh) = (cg)h$, con $cg, h \in \boldsymbol{Z}[X]$ e $\partial(cg) = \partial(g) = \partial G$, $\partial h = \partial H$. Il teorema è così dimostrato.

Esempio 1. Assegnato il polinomio $f = 3X^4 + 30X^2 + 72 \in \boldsymbol{Z}[X]$, supponiamo di sapere che ammette in $\boldsymbol{Q}[X]$ la fattorizzazione

$$f = GH, \text{ con } G = 2X^2+8, \quad H = \tfrac{3}{2}X^2+9.$$

Usando le idee sviluppate nella precedente dimostrazione, vogliamo determinare $g, h \in \boldsymbol{Z}[X]$ tali che $f = gh$, $\partial g = 2$, $\partial h = 2$. Si ha:

$$f = 3f_*, \text{ con } f_* = X^4+10X^2+24.$$

Allora

$$f_* = (\tfrac{1}{3}G)H = \big(\tfrac{2}{3}X^2+\tfrac{8}{3}\big)\big(\tfrac{3}{2}X^2+9\big).$$

Si ha: $\frac{1}{3}G = \frac{2}{3}X^2+\frac{8}{3} = \frac{2}{3}(X^2+4)$, $H = \frac{3}{2}(X^2+6)$. Dunque

$$f_* = (\tfrac{1}{3}G)H = \tfrac{2}{3}(X^2+4)\cdot\tfrac{3}{2}(X^2+6) = (X^2+4)(X^2+6).$$

Pertanto $f = 3f_* = 3(X^2+4)(X^2+6) = (3X^2+12)(X^2+6)$. Dunque $g = 3X^2+12$, $h = X^2+6$.

Osservazione 4. Sia $f \in \boldsymbol{Z}[X]^\cdot$. Abbiamo già osservato (cfr. **Osserv. 1**) che:

$$f \text{ irriducibile in } \boldsymbol{Q}[X] \not\Longrightarrow f \text{ irriducibile in } \boldsymbol{Z}[X].$$

Infatti ad esempio $f = aX$ (con $a \in \boldsymbol{Z}$, $a \neq 0, \pm 1$) è irriducibile in $\boldsymbol{Q}[X]$, ma ammette fattorizzazione non banale $a\cdot X$ in $\boldsymbol{Z}[X]$.

La non irriducibilità in $\boldsymbol{Z}[X]$ dipende dal fatto che f non è primitivo. Dimostreremo nella proposizione che segue che se f è primitivo e irriducibile in $\boldsymbol{Q}[X]$, allora è irriducibile in $\boldsymbol{Z}[X]$. Tale fatto rappresenta un "inverso parziale" del teorema di Gauss.

Proposizione 5. *Sia $f \in \boldsymbol{Z}[X]^\cdot$. Se f è primitivo ed è irriducibile in $\boldsymbol{Q}[X]$, allora è anche irriducibile in $\boldsymbol{Z}[X]$.*

Dim. Sia $f = gh$, con $g, h \in \boldsymbol{Z}[X]$. Tenuto conto che $\mathcal{U}(\boldsymbol{Z}[X]) = \{\pm 1\}$, bisogna verificare che (ad esempio) $g = \pm 1$. Poiché f è primitivo, anche g, h lo sono (cfr. *Nota* di **Prop. 4**). Essendo f irriducibile in $\boldsymbol{Q}[X]$, allora gh è una fattorizzazione banale in $\boldsymbol{Q}[X]$ e dunque, ad esempio, g è costante. Ma g è anche primitivo e quindi $g = \pm 1$, come richiesto.

Il seguente corollario riassume i legami tra l'irriducibilità in $\boldsymbol{Q}[X]$ e in $\boldsymbol{Z}[X]$.

Corollario 3. *Sia $F \in \boldsymbol{Q}[X]^\cdot$ e sia $F = q\,f$, con $q \in \boldsymbol{Q}$, $f \in \boldsymbol{Z}[X]$ primitivo e $\partial f = \partial F$. Risulta:*

$$F \text{ è irriducibile in } \boldsymbol{Q}[X] \iff f \text{ è irriducibile in } \boldsymbol{Z}[X].$$

Dim. ($\Longrightarrow$). Poiché $f \sim F$ (in $\boldsymbol{Q}[X]$) ed F è irriducibile in $\boldsymbol{Q}[X]$, anche f lo è. Essendo f primitivo, dalla **Prop. 5** segue che f è irriducibile in $\boldsymbol{Z}[X]$.

($\Longleftarrow$). Essendo f irriducibile in $\boldsymbol{Z}[X]$, dal teorema di Gauss segue che f è irriducibile in $\boldsymbol{Q}[X]$. Essendo $F \sim f$, segue che anche F è irriducibile in $\boldsymbol{Q}[X]$.

(*D*) IRRIDUCIBILITA' IN $\boldsymbol{Z}[X]$.

Sia $f \in \boldsymbol{Z}[X]^\cdot$. Elenchiamo quattro risultati relativi all'irriducibilità di f, dimostrati sino ad ora:

(*1*) f non primitivo $\Longrightarrow$ f riducibile su $\boldsymbol{Z}$ [infatti $c(f)\,f_*$ è una fattorizzazione non banale].

(*2*) f primitivo e irriducibile su $\boldsymbol{Q}$ $\Longrightarrow$ f irriducibile su $\boldsymbol{Z}$ [segue dalla **Prop. 5**].

(*3*) Sia f primitivo e $\partial f \geq 2$.

- (*a*) f irriducibile su $\boldsymbol{Z}$ $\Longrightarrow$ f non ha zeri in $\boldsymbol{Q}$.
- (*b*) f non ha zeri in $\boldsymbol{Q}$ $\Longrightarrow$ f non ha fattori di grado 1 in $\boldsymbol{Z}[X]$.

[(*a*) segue dal **Teor. 2** e da **Prop. 1***(2 a)*; (*b*) segue da **Prop. 1***(2 b)*: se f non ha fattori di grado 1 in $\boldsymbol{Q}[X]$, non ne ha neppure in $\boldsymbol{Z}[X]$].

(*4*) Sia f primitivo e $2 \leq \partial f \leq 3$. Si ha:

$$f \text{ è irriducibile su } \boldsymbol{Z} \iff f \text{ non ha zeri in } \boldsymbol{Q}.$$

[segue da **Prop. 1***(3)* e **Cor. 3**].

Per polinomi $f \in \boldsymbol{Z}[X]$ con $\partial f \leq 3$, è quindi molto semplice verificare se sono irriducibili (in base a (*4*) e ad **Osserv. 2.8**). Per polinomi di grado ≥ 4, il problema è più difficile e occorrono nuovi risultati. Il risultato nuovo più importante è la seguente condizione sufficiente d'irriducibilità, dovuta a F. Eisenstein.

Teorema 3. *(Criterio di Eisenstein). Sia $f \in \boldsymbol{Z}[X]$ un polinomio primitivo, con $n = \partial f \geq 1$. Sia $f = \sum_{k=0}^{n} a_k X^k$. Se $\exists p$ primo verificante le seguenti condizioni (dette "di Eisenstein"):*

$$p \,|\, a_0,\ p \,|\, a_1,\ \ldots\ ,\ p \,|\, a_{n-1},\ p \nmid a_n \ \text{ e } \ p^2 \nmid a_0,$$

allora f è irriducibile in $\boldsymbol{Z}[X]$.

Dim. Per assurdo, f sia riducibile in $\boldsymbol{Z}[X]$. Dunque f ammette una fattorizzazione non banale $f = gh$, con $g, h \in \boldsymbol{Z}[X]$, $1 \leq \partial g, \partial h < n = \partial f$. Assumiamo

$$g = \sum_{i=0}^{r} b_i X^i,\ \ h = \sum_{j=0}^{s} c_j X^j,\ \text{ con } \ 1 \leq r = \partial g < n,\ 1 \leq s = \partial h < n,\ r + s = n.$$

Da $f = gh$ segue in particolare che $a_0 = b_0 c_0$. Poiché p è primo e $p \,|\, a_0$, allora $p \,|\, b_0$ oppure $p \,|\, c_0$. Poiché $p^2 \nmid a_0$, allora p non divide entrambi. Assumiamo ad esempio che $p \,|\, b_0$ e quindi che $p \nmid c_0$.

Si osserva che p non divide tutti i coefficienti $b_0, \ldots, b_r$ [ad esempio $p \nmid b_r$, in quanto altrimenti $p \,|\, b_r c_s = a_n$, mentre $p \nmid a_n$]. Assumiamo quindi che

$$p \,|\, b_0,\ p \,|\, b_1,\ \ldots\ ,\ p \,|\, b_{i-1},\ p \nmid b_i \quad (\exists\, i \leq r).$$

Si ha: $a_i = b_0 c_i + b_1 c_{i-1} + \ldots + b_{i-1} c_1 + b_i c_0$. Poiché $i < n$, allora $p \,|\, a_i$. Inoltre $p \,|\, b_0 c_i,\ \ldots\ ,\ p \,|\, b_{i-1} c_1$. Ne segue che $p \,|\, b_i c_0 \,\big[= a_i - b_0 c_i - \ \ldots\ - b_{i-1} c_1\big]$. Ma $p \nmid b_i$ e $p \nmid c_0$: assurdo.

Osservazione 5. Il criterio di Eisenstein non è una *CN* per l'irriducibilità: esistono cioè polinomi irriducibili $f \in \boldsymbol{Z}[X]$ per i quali non esiste alcun primo p verificante le condizioni di Eisenstein.

Ad esempio, consideriamo $f = X^2 + 2X + 4 \in \boldsymbol{Z}[X]$. Poiché $\partial f = 2$ e $\Delta_f = 4 - 16 < 0$, f è irriducibile in $\boldsymbol{R}[X]$ e quindi in $\boldsymbol{Q}[X]$; poiché f è primitivo, allora è anche irriducibile in $\boldsymbol{Z}[X]$. L'unico primo che potrebbe verificare le tre condizioni di Eisenstein è $p = 2$. Ma non le verifica tutte, in quanto $p^2 = 4 \,|\, a_0 = 4$ (mentre $p^2 \nmid a_0$, secondo il criterio di Eisenstein).

Un altro esempio più semplice: ogni polinomio $f = p^2 + qX$ (con p, q primi distinti) è irriducibile in $\boldsymbol{Z}[X]$, ma non sono verificate le condizioni di Eisenstein.

Esempio 2. Come applicazione del criterio di Eisenstein, verifichiamo che, per ogni primo p, il polinomio

$$f = X^{p-1} + X^{p-2} + \ \ldots\ . + X + 1 \in \boldsymbol{Z}[X]$$

è irriducibile in $\boldsymbol{Z}[X]$.

Osservato che $X^p - 1 = (X - 1) f$, applichiamo a tale identità polinomiale la sostituzione lineare

$$\varphi : \boldsymbol{Z}[X] \to \boldsymbol{Z}[X] \ \text{ tale che } \ \varphi(X) = X + 1 \quad \text{(cfr. \textbf{Osserv. 2}).}$$

Si ottiene: $(X+1)^p - 1 = (X + 1 - 1)\,\varphi(f)$, cioè

$$\Big[\sum_{k=0}^{p} \tbinom{p}{k} X^k\Big] - 1 = X\,\varphi(f), \ \text{ da cui } \ \cancel{\tbinom{p}{0}} + \sum_{k=1}^{p} \tbinom{p}{k} X^k \cancel{- 1} = X\,\varphi(f) \ \text{ e quindi } \ \sum_{k=1}^{p} \tbinom{p}{k} X^{k-1} = \varphi(f).$$

Al polinomio

$$\varphi(f) = \tbinom{p}{1} + \tbinom{p}{2} X + \ \ldots\ . + \tbinom{p}{p-1} X^{p-2} + X^{p-1}$$

si può applicare il criterio di Eisenstein, relativamente a p. Infatti:

$$p \,|\, \tbinom{p}{1},\ p \,|\, \tbinom{p}{2},\ \ldots\ ,\ p \,|\, \tbinom{p}{p-1},\ p \nmid 1 \ \text{ e } \ p^2 \nmid \tbinom{p}{1}.$$

Allora $\varphi(f)$ è irriducibile in $\boldsymbol{Z}[X]$ e quindi anche f lo è.

Nota. Si osservi che, se $p > 0$ non è primo, il polinomio $f = X^{p-1}+X^{p-2}+ .... +X+1 \in \boldsymbol{Z}[X]$ è invece sempre riducibile. Sia infatti $p = rs$, con $r \geq s \geq 2$. Posto $g = X^{s-1}+X^{s-2}+ .... +X+1 \in \boldsymbol{Z}[X]$, risulta subito:

$$f = g + X^s g + X^{2s} g + ... + X^{(r-1)s} g$$

e dunque $g \mid f$. Pertanto f è riducibile.

Osservazione 6. Illustriamo ora un secondo risultato sulla irriducibilità in $\boldsymbol{Z}[X]$, che potremmo chiamare *"verifica diretta"* e che è ragionevole applicare solo se f ha grado relativamente basso e ≥ 4.

Sia dunque $f \in \boldsymbol{Z}[X]$ un polinomio primitivo e privo di zeri razionali, con $n = \partial f \geq 4$. Siano g, h due polinomi non noti, di gradi rispettivamente $t, n-t$, con $2 \leq t \leq n-t$. Si consideri il sistema di equazioni ottenuto da $f = gh$ (uguagliandone i coefficienti di ugual grado). Si tratta di un sistema di $n+1$ equazioni polinomiali di gradi ≤ 2, avente per incognite i coefficienti di g, h. Di tale sistema si cercano le eventuali soluzioni intere. Se non ne esistono, f non ammette alcuna fattorizzazione di gradi $t, n-t$.

Se per nessuna coppia $(t, n-t)$, con $2 \leq t \leq [\frac{n}{2}]$, il sistema sopra considerato ammette soluzioni intere, f è irriducibile in $\boldsymbol{Z}[X]$. In caso contrario, f è riducibile e le soluzioni di un sistema permettono di scrivere i fattori g, h di f.

Cerchiamo di chiarire il tutto con due esempi.

Esempio 3. Verificare che $f = X^4 + X^3 + 1 \in \boldsymbol{Z}[X]$ è irriducibile in $\boldsymbol{Z}[X]$.

Cominciamo col verificare se f ha zeri razionali. Conveniamo di indicare con a_i i coefficienti di f. Se $\alpha = \frac{r}{s}$ è uno zero razionale di f (con $(r,s) = 1$), allora $r \mid a_0 = 1$ e $s \mid a_4 = 1$. Pertanto $r = \pm 1$ e $s = \pm 1$. Dunque $\alpha = \pm 1$. Ma $f(1) = 3 \neq 0$ e $f(-1) = 1 \neq 0$: dunque f non ha zeri razionali.

Se è riducibile, f può soltanto ammettere una fattorizzazione del tipo $f = gh$, con $\partial g = \partial h = 2$. Poniamo

$$g = b_0 + b_1 X + b_2 X^2, \quad h = c_0 + c_1 X + c_2 X^2 \in \boldsymbol{Z}[X].$$

Poiché $a_4 = b_2 c_2 = 1$, non è restrittivo assumere (eventualmente cambiando segno a g ed h) che $b_2 = c_2 = 1$. Poiché $a_0 = b_0 c_0 = 1$, necessariamente $b_0 = c_0 = \pm 1$. Dunque g, h possono essere riscritti, più semplicemente, nella forma:

$$g = X^2 + aX \pm 1, \quad h = X^2 + bX \pm 1$$

[scegliendo o i due segni superiori o i due segni inferiori]. Se scegliamo i due segni superiori $+$:

$$X^4 + X^3 + 1 = (X^2 + aX + 1)(X^2 + bX + 1) = X^4 + (a+b)X^3 + (ab+2)^2 + (a+b)X + 1,$$

da cui, uguagliando i coefficienti di ugual grado, si ottiene il sistema:

$$\begin{cases} 1 = 1 \\ 1 = a + b \\ 0 = ab + 2 \\ 0 = a + b \\ 1 = 1. \end{cases}$$

Tale sistema è incompatibile (essendo $1 = a + b = 0$). Scegliamo ora i due segni inferiori $-$. Si ha:

$$X^4 + X^3 + 1 = (X^2 + aX - 1)(X^2 + bX - 1) = X^4 + (a+b)X^3 + (ab-2)^2 - (a+b)X + 1,$$

da cui segue il sistema:

$$\begin{cases} 1 = 1 \\ 1 = a + b \\ 0 = ab - 2 \\ 0 = a + b \\ 1 = 1, \end{cases}$$

anch'esso incompatibile. Si conclude che f è irriducibile in $\boldsymbol{Z}[X]$.

Esempio 4. Verificare che il polinomio $f = X^5 + X^4 + 2X^3 - 1 \in \boldsymbol{Z}[X]$ è prodotto di un polinomio

di grado 3 ed uno di grado 2, entrambi irriducibili.

Gli eventuali zeri razionali $\alpha = \frac{r}{s} \in \boldsymbol{Q}$ di f sono ± 1 (come nell'esempio precedente). Ma $f(1),\ f(-1) \neq 0$. Dunque f non ha fattori di grado 1.

Si noti che, se determiniamo una fattorizzazione $f = gh$, con $\partial g = 2$ e $\partial h = 3$, allora $g,\ h$ sono necessariamente irriducibili (non potendo possedere fattori di grado 1).

Come nell'esempio precedente, essendo f monico, si può assumere che anche $g,\ h$ lo siano. Inoltre, essendo $a_0 = -1$ il termine noto di f, allora $b_0 c_0 = -1$. Si hanno quindi due casi:

$$(b_0,\ c_0) = (-1, 1), \quad (b_0,\ c_0) = (1, -1).$$

1^{o}*caso*: $(b_0,\ c_0) = (-1, 1)$. Allora:

$$\begin{aligned} f &= (X^2 + aX - 1)(X^3 + bX^2 + cX + 1) = \\ &= X^5 + (a+b)X^4 + (c + ab - 1)X^3 + (1 + ac - b)X^2 + (a - c)X - 1. \end{aligned}$$

Si ottiene il sistema:

$$\begin{cases} a + b = 1 \\ c + ab - 1 = 2 \\ 1 + ac - b = 0 \\ a - c = 0, \end{cases} \quad \text{da cui} \quad \begin{cases} c = a \\ b = 1 - a \\ a + a(1 - a) = 3 \\ 1 + a^2 - 1 + a = 0. \end{cases}$$

La terza equazione del sistema non ha soluzioni (reali) e dunque il sistema è incompatibile.

2^{o}*caso*: $(b_0,\ c_0) = (1, -1)$. Allora:

$$\begin{aligned} f &= (X^2 + aX + 1)(X^3 + bX^2 + cX - 1) = \\ &= X^5 + (a+b)X^4 + (c + ab + 1)X^3 + (-1 + ac + b)X^2 + (-a + c)X - 1. \end{aligned}$$

Si ottiene il sistema:

$$\begin{cases} a + b = 1 \\ c + ab + 1 = 2 \\ -1 + ac + b = 0 \\ -a + c = 0, \end{cases} \quad \text{da cui} \quad \begin{cases} c = a \\ b = 1 - a \\ 2a - a^2 = 1 \\ a^2 = a. \end{cases}$$

Dalle ultime due equazioni: $a = 1$ e quindi $b = 0,\ c = 1$. Il polinomio f è quindi riducibile e si fattorizza in questo modo: $f = (X^2 + X + 1)(X^3 + X - 1)$.

Osservazione 7. Il terzo risultato sulla irriducibilità in $\boldsymbol{Z}[X]$, che chiameremo *"verifica mod p"*, consiste nell'applicare la verifica diretta non ad un polinomio $f \in \boldsymbol{Z}[X]$ ma alla sua *riduzione mod p* $\overline{f} \in \boldsymbol{Z}_p[X]$. Introduciamo la seguente definizione

Definizione. Sia p un primo e sia $\varphi_p : \boldsymbol{Z}[X] \to \boldsymbol{Z}_p[X]$ l'applicazione (suriettiva) così definita:

$$\varphi_p\big(\sum_{i=0}^{n} a_i X^i\big) = \sum_{i=0}^{n} \overline{a}_i X^i, \text{ con } \overline{a}_i = [a_i]_p \text{ classe resto di } a_i \ \textit{mod p}.$$

[φ_p estende ai polinomi la proiezione canonica $\boldsymbol{Z} \to \boldsymbol{Z}_p$]. Per accorciare le notazioni, scriveremo $\varphi_p(f) = \overline{f}$, con $\overline{f} = \sum_{i=0}^{n} \overline{a}_i X^i$, se $f = \sum_{i=0}^{n} a_i X^i$; diremo che $\overline{f}$ è *la riduzione di f mod p*.

Verifichiamo che φ_p è un omomorfismo di anelli. Si ha:

$$(*)\ \varphi_p(f+g) = \overline{f+g} = \overline{\sum_{i=0}^{n}(a_i + b_i)X^i} = \sum_{i=0}^{n}(\overline{a_i} + \overline{b}_i)X^i = \sum_{i=0}^{n} \overline{a_i} X^i + \sum_{i=0}^{n} \overline{b}_i X^i = \overline{f} + \overline{g} = \varphi_p(f) + \varphi_p(g).$$

$(**)$ Se $fg = \sum_{k=0}^{n+m} c_k X^k = \sum_{k=0}^{n+m} \big(\sum_{i=0}^{k} a_i\, b_{k-i}\big)X^k$, allora:

$$\varphi_p(fg) = \overline{fg} = \sum_{k=0}^{n+m} \overline{c_k} X^k = \sum_{k=0}^{n+m} \big(\sum_{i=0}^{k} \overline{a_i}\ \overline{b_{k-i}}\big)X^k = \big(\sum_{i=0}^{n} \overline{a_i} X^i\big)\big(\sum_{j=0}^{m} \overline{b_j} X^j\big) = \overline{f}\,\overline{g} = \varphi_p(f)\varphi_p(g).$$

Ovviamente $\partial \overline{f} \leq \partial f$. Inoltre:

$$\partial \overline{f} = \partial f \iff p \nmid d_f \quad [\text{dove } d_f = a_n \text{ denota il coefficiente direttore di } f]$$

[infatti: $\partial\overline{f} = \partial f \iff \overline{a_n} \neq \overline{0} \iff p \not| a_n \iff p \not| d_f$].

Il criterio di irriducibilità *mod p* si basa sul seguente risultato.

Proposizione 6. *Sia p un numero primo e sia $f \in \boldsymbol{Z}[X]$ un polinomio primitivo tale che $p \not| d_f$ [coefficiente direttore di f]. Se $\overline{f}$ è irriducibile (in $\boldsymbol{Z}_p[X]$), allora f è irriducibile (in $\boldsymbol{Z}[X]$).*

Dim. Abbiamo già osservato che $\partial\overline{f} = \partial f$. Sia $\overline{f}$ irriducibile e per assurdo f riducibile. Allora $f = gh$, con $\partial g, \partial h < \partial f$. Poiché φ_p è un omomorfismo, $\overline{f} = \overline{g}\overline{h}$, con $\partial\overline{g} \leq \partial g < \partial\overline{f}$ e $\partial\overline{h} \leq \partial h < \partial\overline{f}$. Ma allora $\overline{f}$ è riducibile: assurdo.

Osservazione 8. (*i*) La proposizione precedente non si inverte: se $\overline{f}$ è riducibile, non è detto che f sia riducibile.
Ad esempio $f = X^2 + 1 \in \boldsymbol{Z}[X]$ è riducibile *mod* 2 [essendo $\overline{f} = X^2 + \overline{1} = (X + \overline{1})^2$ in $\boldsymbol{Z}_2[X]$], ma f è irriducibile in $\boldsymbol{Z}[X]$.

(*ii*) Per verificare l'irriducibilità di f *mod p* si procede in questo modo.
Si sceglie il minimo primo p tale che $p \not| d_f$. Posto $\overline{f} = \varphi_p(f)$, si opera con verifica diretta su $\overline{f} \in \boldsymbol{Z}_p[X]$. Se ogni possibile sistema, ottenuto da un'eventuale fattorizzazione $\overline{f} = \overline{g}\overline{h}$, è incompatibile su $\boldsymbol{Z}_p$, allora $\overline{f}$ è irriducibile e quindi (in base a **Prop. 6**) f è irriducibile su $\boldsymbol{Z}$. Se invece almeno uno di tali sistemi è compatibile, $\overline{f}$ è riducibile e quindi (in base a (*i*)) il procedimento non porta ad alcuna conclusione. In tal caso si può scegliere il più piccolo primo successivo a p (ma che non divida d_f) e ripetere il ragionamento.

Si noti che questo metodo offre un vantaggio rispetto alla "verifica diretta", in quanto l'eventuale incompatibilità dei sistemi può essere dedotta piuttosto facilmente (anche per tentativi), visto che i coefficienti variano in un insieme finito ($\boldsymbol{Z}_p$) e non in $\boldsymbol{Z}$.

Vogliamo infine rilevare che, se $\overline{f} \in \boldsymbol{Z}_p[X]$ non ammette una fattorizzazione con una coppia di polinomi di gradi $t, n-t$, allora una fattorizzazione con polinomi degli stessi gradi non è lecita neppure per $f \in \boldsymbol{Z}[X]$. Operando quindi la riduzione *mod q* [dove q è un altro primo tale che $q \not| d_f$] si può evitare di esaminare la possibilità di una fattorizzazione di $\overline{f} \in \boldsymbol{Z}_q[X]$ con polinomi di gradi $t, n-t$.

Esempio 5. Verificare se $f = X^5 - X + 1 \in \boldsymbol{Z}[X]$ è irriducibile.

Si osserva subito che f non ha zeri razionali. Infatti $f(1), f(-1) \neq 0$.
Si scelga $p = 2$ ($2 \not| 1$). Allora $f = X^5 + X + \overline{1} \in \boldsymbol{Z}_2[X]$. Osserviamo che $\overline{f}$ non ha zeri in $\boldsymbol{Z}_2$ (infatti $\overline{f}(\overline{0}), \overline{f}(\overline{1}) \neq \overline{0}$). Assumiamo

$$\overline{f} = \overline{g}\,\overline{h}, \text{ con } \overline{g} = \sum_{i=0}^{3} b_i X^i,\ \overline{h} = \sum_{j=0}^{2} c_j X^j \in \boldsymbol{Z}_2[X].$$

Poiché $\overline{1} = d_{\overline{f}} = b_3 \cdot c_2$, si può assumere $b_3 = c_2 = \overline{1}$. Relativamente al termine noto a_0 di $\overline{f}$, si ha $a_0 = \overline{1} = b_0 c_0$. Ne segue $b_0 \neq \overline{0}$ e $c_0 = b_0^{-1}$. Essendo $p = 2$, necessariamente $b_0 = c_0 = \overline{1}$. Pertanto

$$\begin{aligned}\overline{f} &= X^5 + X + \overline{1} = (X^3 + aX^2 + bX + \overline{1})(X^2 + cX + \overline{1}) = \\ &= X^5 + (a+c)X^4 + (b + ac + \overline{1})X^3 + (\overline{1} + bc + a)X^2 + (b+c)X + \overline{1}.\end{aligned}$$

Ne segue:

$$\begin{cases} a + c = \overline{0} \\ b + ac + \overline{1} = \overline{0} \\ \overline{1} + bc + a = \overline{0} \\ b + c = \overline{1}, \end{cases} \quad \text{da cui} \quad \begin{cases} a = c \\ b = c + \overline{1} \\ c + \overline{1} + c^2 + \overline{1} = \overline{0} \\ \overline{1} + c(c + \overline{1}) + c = \overline{0} \end{cases} \quad \text{e quindi} \quad \begin{cases} a = c \\ b = c + \overline{1} \\ c + c^2 = \overline{0} \\ c^2 + \overline{1} = \overline{0}. \end{cases}$$

Pertanto: $c = \overline{1},\ a = \overline{1},\ b = \overline{0}$ e quindi

$$\overline{f} = X^5 + X + \overline{1} = (X^3 + X^2 + bX + \overline{1})(X^2 + X + \overline{1}) \in \boldsymbol{Z}_2[X].$$

Il procedimento non ha portato a nessuna conclusione. Scegliamo allora $p = 3$ ($3 \not| 1$). Allora

$$\overline{f} = X^5 + \overline{2}X + \overline{1} \in \boldsymbol{Z}_3[X].$$

Si verifica che $\overline{f}$ non ha zeri in $\boldsymbol{Z}_3$ e si pone:

$$\overline{f} = \overline{g}\,\overline{h}, \text{ con } \overline{g} = \sum_{i=0}^{3} b_i X^i,\ \overline{h} = \sum_{j=0}^{2} c_j X^j \in \boldsymbol{Z}_3[X].$$

Come prima, $\overline{1} = b_3 c_2$, e quindi $b_3 = c_2 = \overline{1}$. Come prima, $a_0 = \overline{1} = b_0 c_0$ e quindi $b_0 \neq \overline{0}$, $c_0 = b_0^{-1}$. Ma ora b_0 può assumere i valori $\overline{1}, \overline{2}$ e conseguentemente si hanno due possibilità:

$$(b_0, c_0) = (\overline{1}, \overline{1}), \qquad (b_0, c_0) = (\overline{2}, \overline{2}).$$

$1^o caso$: $(b_0, c_0) = (\overline{1}, \overline{1})$. Allora:

$$\overline{f} = X^5 + \overline{2}X + \overline{1} = (X^3 + aX^2 + bX + \overline{1})(X^2 + cX + \overline{1}).$$

Se ne deduce il sistema

$$\begin{cases} a + c = \overline{0} \\ b + ac + \overline{1} = \overline{0} \\ \overline{1} + bc + a = \overline{0} \\ b + c = \overline{2}, \end{cases} \text{ da cui: } \begin{cases} a = \overline{2}c \\ b = \overline{2} + \overline{2}c \\ \overline{2} + \overline{2}c + \overline{2}c^2 + \overline{1} = \overline{0} \\ \overline{1} + \overline{2}c + \overline{2}c^2 + \overline{2}c = \overline{0}, \end{cases} \begin{cases} a = \overline{2}c \\ b = \overline{2} + \overline{2}c \\ \cancel{\overline{2}}(\overline{c}^2 + c) = \overline{0} \\ \overline{1} + c + \overline{2}c^2 = \overline{0}, \end{cases} \begin{cases} a = \overline{2}c \\ b = \overline{2} + \overline{2}c \\ (\overline{c}^2 + c) = \overline{0} \\ c^2 + \overline{1} = \overline{0}. \end{cases}$$

Ma non esiste $c \in \boldsymbol{Z}_3$ tale che $c^2 + \overline{1} = \overline{0}$. Dunque il sistema è incompatibile.

$2^o caso$: $(b_0, c_0) = (\overline{2}, \overline{2})$. In tal caso:

$$\overline{f} = X^5 + \overline{2}X + \overline{1} = (X^3 + aX^2 + bX + \overline{2})(X^2 + cX + \overline{2}).$$

Se ne deduce il sistema

$$\begin{cases} a + c = \overline{0} \\ b + ac + \overline{2} = \overline{0} \\ \overline{2} + bc + \overline{2}a = \overline{0} \\ \overline{2}(b + c) = \overline{2}, \end{cases} \text{ da cui: } \begin{cases} a = \overline{2}c \\ b = \overline{1} + \overline{2}c \\ \cancel{\overline{1}} + \overline{2}c + 2c^2 + \cancel{\overline{2}} = \overline{0} \\ \overline{2} + c + \overline{2}c^2 + c = \overline{0} \end{cases} \text{ e quindi } \begin{cases} c^2 + c = \overline{0} \\ \overline{1} + c + c^2 = \overline{0}. \end{cases}$$

Ma allora $\overline{1} = \overline{0}$: il sistema è incompatibile.

Si conclude che $\overline{f} \in \boldsymbol{Z}_3[X]$ è irriducibile e quindi anche $f \in \boldsymbol{Z}[X]$ lo è.

Osservazione 9. Come già anticipato in **Osserv. 2.4**, possiamo verificare che:

in $\boldsymbol{Z}[X]$ ogni polinomio irriducibile è anche primo.

Dimostriamo preliminarmente la seguente affermazione:

(∗) *Se P è irriducibile in $\boldsymbol{Z}[X]$ e $F \in \boldsymbol{Z}[X]$, si ha: $P \mid F$ in $\boldsymbol{Q}[X] \implies P \mid F$ in $\boldsymbol{Z}[X]$.*

Infatti, sia $F = PH$, con $H \in \boldsymbol{Q}[X]$. Allora $H = q\,h$, con $q = \frac{a}{b} \in \boldsymbol{Q}$ e $h \in \boldsymbol{Z}[X]$ primitivo. Ne segue: $bF = aPH$ e quindi

$$|b|c(F) = |a|c(P)c(h) = |a|$$

[essendo P, h primitivi]. Dunque $c(F) = \frac{|a|}{|b|} = \pm q$, cioè $q = \pm c(F) \in \boldsymbol{Z}$. Ne segue che $H = qh \in \boldsymbol{Z}[X]$ e quindi $P \mid F$ in $\boldsymbol{Z}[X]$.

Sia ora P irriducibile in $\boldsymbol{Z}[X]$ e siano $F, G \in \boldsymbol{Z}[X]$ tali che $P \mid FG$, $P \nmid F$: vogliamo verificare che $P \mid G$ in $\boldsymbol{Z}[X]$.

Da (∗) segue che $P \nmid F$ in $\boldsymbol{Q}[X]$. Poiché P è irriducibile in $\boldsymbol{Q}[X]$ [per il teorema di Gauss], allora è anche primo in $\boldsymbol{Q}[X]$. Quindi $P \mid G$ in $\boldsymbol{Q}[X]$ e quindi [per (∗)] anche in $\boldsymbol{Z}[X]$. Allora P è primo in $\boldsymbol{Z}[X]$.

Concludiamo il paragrafo segnalando il seguente importante risultato (anch'esso attribuito a Gauss).

Teorema 4. *Se A è un UFD, anche $A[X]$ è un UFD.*

Da tale teorema discende in particolare che $\boldsymbol{Z}[X]$ è un *UFD* e che sono *UFD* tutti gli anelli

$A[X_1, X_2, \dots, X_n]$, con A *UFD*. Infatti $A[X_1, X_2, \dots, X_n] = A[X_1][X_2] \dots [X_n]$.

Osservazione 10. L'affermazione provata in **Osserv. 9** [cioè che in $\boldsymbol{Z}[X]$ ogni polinomio irriducibile è primo] è immediata conseguenza del **Teor. 4** e del seguente semplice risultato:

Se A è un UFD, ogni elemento irriducibile di A è primo.

Sia infatti $p \in A$ un elemento iriducibile e assumiamo che $p \mid xy$. Dunque $xy = pz$, $\exists\, z \in A$. Scriviamo x, y come prodotto di elementi irriducibili: $x = p_1 p_2 \dots p_t$, $y = q_1 q_2 \dots q_s$. Allora $pz = p_1 p_2 \dots p_t q_1 q_2 \dots q_s$. In base all'unicità di scrittura di un elemento come prodotto di irriducibili, p coincide (a meno di elementi associati) con uno dei fattori p_i di x o con uno dei fattori q_j di y. Dunque $p \mid x$ oppure $p \mid y$ e pertanto p è primo.

4. Congruenze in K[X]

Definizione 1. *Sia* $P \in K[X]^{\cdot}$. *Si chiama relazione di congruenza modulo* P *la relazione* $\equiv_P$ *su* $K[X]$ *così definita:*

$$F \equiv_P G \iff P \,|\, F - G, \quad \forall\, F, G \in K[X].$$

Lemma 1. *La relazione* $\equiv_P$ *è una relazione di equivalenza su* $K[X]$, *compatibile con le due operazioni dell'anello.*

Dim. Basta dimostrare le seguenti (ovvie) proprietà:

(*i*) $F \equiv_P F$.

(*ii*) $F \equiv_P G \implies G \equiv_P F$.

(*iii*) $F \equiv_P G,\ G \equiv_P H \implies G \equiv_P H$.

(*iv*) Se $F \equiv_P F_1,\ G \equiv_P G_1$, allora: $F + G \equiv_P F_1 + G_1, \quad F \cdot G \equiv_P F_1 \cdot G_1$.

Nota. Si osservi, a proposito dell'ultima congruenza, che $FG - F_1G_1 = FG \pm FG_1 - F_1G_1 = F(G - G_1) + G_1(F - F_1)$. Dunque $P \,|\, FG - F_1G_1$, se $P \,\Big|\, \begin{matrix} F - F_1 \\ G - G_1 \end{matrix}$.

Osservazione 1. Denoteremo con $[F]$ (o $[F]_P$ o anche $\overline{F}$) la classe di equivalenza di F *mod* P, detta *classe di congruenza di* F *mod* P. Ovviamente risulta: $[F] = F + P\,K[X]$.

Si osservi inoltre che se P è una costante non nulla (cioè $\partial P = 0$), allora $\equiv_P$ è la relazione caotica su $K[X]$ (cioè $F \equiv_P G,\ \forall\, F, G \in K[X]$). In tal caso esiste un'unica classe di congruenza *mod* P: l'insieme $K[X]$.

Proposizione 1. *Sia* $\partial P \geq 1$. *L'insieme quoziente* $K[X]/_{\equiv_P}$ *è un anello commutativo unitario, rispetto alle due seguenti operazioni:*

$$[F] + [G] := [F + G], \quad [F] \cdot [G] := [F \cdot G], \quad \forall\, F, G \in K[X]/_{\equiv_P}.$$

Dim. Le due operazioni sono ben definite in base al Lemma precedente. Le verifiche degli assiomi di anello sono un semplice esercizio. Si noti che $[P] = [0]$ è elemento neutro della somma e $[1]$ è elemento neutro del prodotto.

Osservazione 2. (*i*) Sia $\partial P \geq 1$. Consideriamo la seguente applicazione:

$$i : K \to K[X]/_{\equiv_P} \quad \text{tale che} \quad i(a) = [a], \quad \forall\, a \in K.$$

Si verifica subito che i è un omomorfismo di anelli [infatti $i(a + b) = [a + b] = [a] + [b]$ e $i(a \cdot b) = [a \cdot b] = [a] \cdot [b]$] e che i è iniettivo [infatti, se $[a] = [b]$, allora $P \,|\, a - b$. Se fosse $a - b \neq 0$, $1 \leq \partial P \leq \partial(a - b) = 0$: assurdo]. Diremo quindi che K *si immerge in* $K[X]/_{\equiv_P}$ *tramite* i. Si usa perciò scrivere a in luogo di $[a]$ (come elemento di $K[X]/_{\equiv_P}$).

(*ii*) Per ogni $F = \sum_{i=0}^{n} a_i X^i \in K[X]$ risulta, in $K[X]/_{\equiv_P}$:

$$[F] = \sum_{i=0}^{n} [a_i][X]^i = \sum_{i=0}^{n} a_i [X]^i.$$

Se poniamo $x := [X]$, allora $[F] = \sum_{i=0}^{n} a_i x^i$. Scriveremo anche $F(x)$ in luogo di $[F]$. Dunque in $K[X]/_{\equiv_P}$ risulta: $F(x) = \sum_{i=0}^{n} a_i x^i$.

Se, in particolare, si assume $P = \sum_{i=0}^{p} p_i X^i$, con $p = \partial P \geq 1$, allora $0 = [P] = P(x) = \sum_{i=0}^{p} p_i x^i$. Diremo perciò che *$x$ è uno zero (simbolico) di P in $K[X]/_{\equiv_P}$*.

Sia, ad esempio, $P = X^2 - 2X + 2 \in \boldsymbol{Q}[X]$. Nell'anello $\boldsymbol{Q}[X]/_{\equiv_P}$ vale la relazione $P(x) = 0$, cioè $x^2 - 2x + 2 = 0$ e quindi $x^2 = 2x - 2$.

Scelto ad esempio $F = X^3 - 1 \in \boldsymbol{Q}[X]$, risulta:

$$[F] = F(x) = x^3 - 1 = x(2x-2) - 1 = 2x^2 - 2x - 1 = 2(2x-2) - 2x - 1 = 2x - 5$$

e dunque $[F] = [2X - 5]$. Abbiamo così determinato nella classe di congruenza di F un rappresentante di grado $< \partial P$. Tale fatto non è casuale, come viene chiarito dal lemma che segue.

Lemma 2. *Sia $p = \partial P \geq 1$. Per ogni $[F] \in K[X]/_{\equiv_P}$, esiste un unico $R \in K[X]$ tale che $\partial R < p$ e $[F] = [R]$. R è detto residuo canonico di F modulo P.*

Dim. Si divida F per P. Risulta: $F = PQ + R$, con $\partial R < \partial P$. Poiché $P \,\big|\, F - R$, allora $[F] = [R]$.

Per provare l'unicità di R, si assuma che esista $\tilde{R} \in K[X]$ tale che $\partial \tilde{R} < \partial P$ e $[F] = [\tilde{R}]$. Allora $P \,\big|\, F - \tilde{R}$, cioè $F = \tilde{R} + P\tilde{Q}$. Per l'unicità del quoziente e del resto della divisione, $\tilde{R} = R$.

Proposizione 2. *Sia $p = \partial P \geq 1$. Risulta:*

$$K[X]/_{\equiv_P} = \Big\{ \sum_{i=0}^{p-1} a_i x^i, \quad \forall\, a_0, a_1, \dots, a_{p-1} \in K \Big\}, \quad \text{con } x = [X].$$

Inoltre: $\sum_{i=0}^{p-1} a_i x^i = \sum_{i=0}^{p-1} b_i x^i \iff a_i = b_i, \ \forall\, i = 0, \dots, p-1$. In $K[X]/_{\equiv_P}$ allle usuali regole di calcolo tra polinomi si aggiungono le semplificazioni indotte dall'uguaglianza:

$$P(x) = 0, \ \text{cioè} \ \sum_{i=0}^{p} p_i x^i = 0, \ \text{se} \ P = \sum_{i=0}^{p} p_i X^i.$$

Dim. Dal **Lemma 2**, $\forall\, [F] \in K[X]/_{\equiv_P}$ risulta: $[F] = [R]$, con $\partial R < p$. Se $R = \sum_{i=0}^{p-1} a_i X^i$, allora $[F] = \sum_{i=0}^{p-1} a_i x^i$. Se $\sum_{i=0}^{p-1} a_i x^i = \sum_{i=0}^{p-1} b_i x^i$, allora $P \,\big|\, \sum_{i=0}^{p-1} (a_i - b_i) X^i$. Per ragioni di grado, $\sum_{i=0}^{p-1} (a_i - b_i) X^i$ è il polinomio nullo e quindi $a_i = b_i, \ \forall\, i = 0, \dots, p-1$.

Infine, se $P = \sum_{i=0}^{p} p_i X^i$, allora in $K[X]/_{\equiv_P}$ vale l'uguaglianza $P(x) = 0$, cioè $\sum_{i=0}^{p} p_i x^i = 0$.

Osservazione 3. $K[X]/_{\equiv_P}$ viene anche denotato $K[X]/_{(P)}$ o $K[X]/_{\langle P \rangle}$ o $K[X]/_{PK[X]}$ o anche $K[x \,\big|\, P(x) = 0]$.

Esempio 1. Sia $P = X^3 - 1 \in \boldsymbol{Q}[X]$. Risulta:

$$\boldsymbol{Q}[X]/_{(X^3-1)} = \boldsymbol{Q}[x \,\big|\, x^3 = 1] = \big\{ a + bx + cx^2, \ \forall\, a, b, c \in \boldsymbol{Q};\ x^3 = 1 \big\}.$$

Verifichiamo ad esempio che $x^2(x^2+1) = x + x^2$. Infatti:

$$x^2(x^2+1) = x^4 + x^2 = x(x^3) + x^2 = x \cdot 1 + x^2 = x + x^2$$

Osserviamo che tale anello non è integro: infatti $x - 1$, $x^2 + x + 1$ sono elementi non nulli, ma $(x-1)(x^2+x+1) = x^3 - 1 = 0$.

Proposizione 3. *Sia $P \in K[X]$, con $p = \partial P \geq 1$. Risulta:*

$$K[X]/_{(P)} \ \textit{è un campo} \iff P \ \textit{è irriducibile in} \ K[X].$$

Altrimenti, $K[X]/_{(P)}$ *è un anello non integro.*

Dim. ($\Longrightarrow$). Se per assurdo P fosse riducibile, allora $P = FG$, con $1 \le \partial F, \partial G < p$. Allora $0 = P(x) = F(x)G(x)$, con $F(x), G(x) \neq 0$. Ciò è assurdo perché $K[X]/_{(P)}$ è un campo.

Si noti che abbiamo così dimostrato anche l'ultima affermazione.

($\Longleftarrow$). Sia P irriducibile. Poiché $K[X]/_{(P)}$ è un anello commutativo unitario, basta verificare che ogni suo elemento $[F]$ non nullo è invertibile. Poiché $[F] \neq [0]$, $F \not\equiv 0 \ (mod\ P)$ e quindi $P \not| F$. Risulta $MCD(P, F) = 1$ [se per assurdo fosse $D := MCD(P, F) \neq 1$, allora $D \sim P$ (in quanto P è irriducibile) e pertanto $P \,|\, D \,|\, F$: assurdo]. In base all'identità di Bézout, $1 = PA + FB$ (con $A, B \in K[X]$). Allora $1 = [1] = [PA + FB] = 0 + [F][B]$. Dunque $[F]$ è invertibile, con inverso $[B]$.

Esempio 2. Sia $P = X^3 - 2 \in \boldsymbol{Q}[X]$. P è ovviamente irriducibile in $\boldsymbol{Q}[X]$. Dunque

$$\boldsymbol{Q}[X]/_{(X^3-2)} = \boldsymbol{Q}[x \,|\, x^3 = 2] = \left\{a + bx + cx^2,\ \forall\, a,\, b,\, c \in \boldsymbol{Q};\ x^3 = 2\right\}$$

è un campo. Vogliamo ad esempio calcolare l'inverso di x^2 in tale campo. Possiamo seguire due strade:

(*i*) Usiamo l'identità di Bézout (relativa a X^2 e $X^3 - 2$ in $\boldsymbol{Q}[X]$). Si ha:

$$1 = \tfrac{X}{2}\,(X^2) - \tfrac{1}{2}\,(X^3 - 2).$$

Allora $1 = [1] = \frac{x}{2}\,x^2 - \frac{1}{2}\,0$, cioè $x^2 \cdot \frac{x}{2} = 1$. Dunque $(x^2)^{-1} = \frac{x}{2}$.

(*ii*) Determiniamo $a, b, c \in \boldsymbol{Q}$ verificanti l'uguaglianza $x^2(a + bx + cx^2) = 1$ (in $\boldsymbol{Q}[x \,|\, x^3 = 2]$). Si ha:

$$1 = ax^2 + bx^3 + cx^4 = ax^2 + 2b + 2cx \ \text{ e dunque } \ a = c = 0,\ 2b = 1.$$

Quindi $1 = x^2(0 + \frac{1}{2}x + 0x^2) = x^2\frac{x}{2}$ e pertanto $(x^2)^{-1} = \frac{x}{2}$.

[Si noti che $x^3 = 2 \implies \frac{x^3}{2} = 1 \implies x^2\frac{x}{2} = 1 \implies (x^2)^{-1} = \frac{x}{2}$.]

Osservazione 4. Sia $P \in K[X]$ un polinomio irriducibile di grado $\partial P = p \ge 1$ e sia L un campo tale che

$$K \subset L \ \text{ e } \ \exists\, \alpha \in L \,\big|\, P(\alpha) = 0.$$

Vogliamo verificare che il campo $K[X]/_{(P)}$ è un sottocampo di L.

Sia $f : K[X] \to L$ l'applicazione così definita:

$$f(F) = F(\alpha),\ \ \forall\, F \in K[X].$$

Verifichiamo che la relazione di equivalenza ρ_f associata ad f coincide con $\equiv_P$. Infatti:

- Se $F \equiv_P G$, allora $F - G = PQ$ e quindi $F(\alpha) - G(\alpha) = P(\alpha)Q(\alpha) = 0$, cioè $F \rho_f G$.

- Sia $F \rho_f G$, cioè $F(\alpha) = G(\alpha)$. Sia $F - G = PQ + R$, con $\partial R < p$. Se $R = 0$, allora $F \equiv_P G$, come richiesto. Altrimenti, per assurdo, sia $R \neq 0$. Si ha:

$$0 = F(\alpha) - G(\alpha) = P(\alpha)Q(\alpha) + R(\alpha) = 0 + R(\alpha) \ \text{ e dunque } \ R(\alpha) = 0.$$

Essendo P irriducibile e $0 \le \partial R < p$, allora $(R, P) = 1$ e dunque sussiste in $K[X]$ un'identità di Bézout $1 = AR + BP$, che, valutata in α, fornisce l'assurdo: $1 = A(\alpha)R(\alpha) + B(\alpha)P(\alpha) = 0 + 0 = 0$.

Ne segue che $K[X]/_{\rho_f} = K[X]/_{\equiv_P} = K[X]/_{(P)}$. In base a **Cap. I**, **Prop. 3.2**, l'applicazione

$$\varphi : K[X]/_{(P)} \to L \ \text{ tale che } \ \varphi([F]) = F(\alpha),\ \ \forall\, [F] \in K[X]/_{(P)},$$

è iniettiva. Inoltre

$$Im\,\varphi = Im\, f = \left\{F(\alpha),\ \ \forall\, F \in K[X]\right\} = \left\{\sum_{i=0}^{p-1} a_i\,\alpha^i,\ \ \forall\, a_0,\ \dots,\ a_{p-1} \in K\right\}$$

Infine φ è un omomofismo di anelli. Infatti

$$\varphi([F] + [G]) = \varphi([F + G]) = (F + G)(\alpha) = F(\alpha) + G(\alpha) = \varphi([F]) + \varphi([G])$$

Analogamente si verifica che $\varphi([F] \cdot [G]) = \varphi([F]) \cdot \varphi([G])$.

Si conclude che il campo $K[X]/_{(P)}$ è isomorfo ad $Im\,\varphi$, che è quindi un sottocampo di L, usualmente denotato $K[\alpha]$ (o $K(\alpha)$) e chiamato *estensione algebrica semplice di* K *tramite* α.

Ad esempio, poiché il polinomio $X^3-2 \in \boldsymbol{Q}[X]$ ammette in $\boldsymbol{R}$ lo zero $\sqrt[3]{2}$, il campo $\boldsymbol{Q}[X]/_{(X^3-2)}$ (già considerato in **Esempio 2**) si identifica al sottocampo di $\boldsymbol{R}$

$$\boldsymbol{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4}, \ \ \forall\, a,\, b,\, c \in \boldsymbol{Q}\}.$$

Esempio 3. Il polinomio $P = X^2+1$ è irriducibile in $\boldsymbol{Q}[X]$ ed in $\boldsymbol{R}[X]$. Determiniamo i campi $\boldsymbol{Q}[X]/_{(X^2+1)}$ e $\boldsymbol{R}[X]/_{(X^2+1)}$.

(*a*) Risulta: $\boldsymbol{Q}[X]/_{(X^2+1)} = \boldsymbol{Q}[x \,|\, x^2 = -1] = \{a + bx, \ \forall\, a,\, b \in \boldsymbol{Q};\ x^2 = -1\}$.

Tenuto conto che $i \in \boldsymbol{C}$ è uno zero di X^2+1, tale campo è identificabile al sottocampo di $\boldsymbol{C}$

$$\boldsymbol{Q}[i] = \{a + i\,b, \ \ \forall\, a,\, b \in \boldsymbol{Q}\}$$

[si tratta dei numeri complessi "a componenti razionali"].

(*b*) Risulta: $\boldsymbol{R}[X]/_{(X^2+1)} = \boldsymbol{R}[x \,|\, x^2 = -1] = \{a + bx, \ \forall\, a,\, b \in \boldsymbol{R};\ x^2 = -1\}$.

L'applicazione $f : \boldsymbol{R}[X] \to \boldsymbol{C}$ tale che $f(F) = F(i), \ \forall\, F \in \boldsymbol{C}[X]$, è suriettiva [infatti $z = a + ib = f(a + bX), \ \forall\, z \in \boldsymbol{C}$]. Pertanto f induce l'isomorfismo

$$\varphi : \boldsymbol{R}[X]/_{(X^2+1)} \to \boldsymbol{C} \ \text{ tale che } \ \varphi(a + bx) = a + b\,i, \ \ \forall\, a + bx \in \boldsymbol{R}[X]/_{(X^2+1)},$$

e dunque $\boldsymbol{C} = \boldsymbol{R}[i]$ è estensione algebrica semplice di $\boldsymbol{R}$ tramite i.

Esempio 4. Sia $P = aX + b \in K[X]$ un polinomio di grado 1. Allora

$$K[X]/_{(aX+b)} = K.$$

Ciò discende subito dalla **Prop. 2**, ma può anche essere verificato tramite l'**Osserv. 4**. Infatti $P(-\frac{b}{a}) = 0$ e l'applicazione

$$f : K[X] \to K \ \text{ tale che } \ f(F) = F(-\tfrac{b}{a})$$

è suriettiva [in quanto $f(c) = c, \ \forall\, c \in K$]. Dunque f induce l'isomorfismo

$$\varphi : K[X]/_{(aX+b)} \to K \ \text{ tale che } \ \varphi([F]) = F(-\tfrac{b}{a}), \ \ \forall\, [F] \in K[X]/_{(aX+b)}.$$

Si noti che $F = (aX + b)Q + F(-\frac{b}{a})$ e dunque $[F] = F(-\frac{b}{a})$. Pertanto $\varphi = \mathbf{1}_K$.

Esempio 5. Il polinomio $f = X^2 + X + \overline{1} \in \boldsymbol{Z}_2[X]$ è irriducibile in $\boldsymbol{Z}_2[X]$ [infatti non ha zeri in $\boldsymbol{Z}_2$, essendo $f(\overline{0}) = f(\overline{1}) = \overline{1} \neq \overline{0}$]. Allora $\boldsymbol{Z}_2[X]/_{(X^2+X+\overline{1})}$ è un campo. Risulta:

$$\boldsymbol{Z}_2[X]/_{(X^2+X+\overline{1})} = \boldsymbol{Z}_2[x \,|\, x^2 + x + \overline{1} = \overline{0}] = \{a + bx, \ \forall\, a,\, b \in \boldsymbol{Z}_2;\ x^2 = x + \overline{1}\} = \{\overline{0},\, \overline{1},\, x,\, x + \overline{1}\}.$$

Le tavole delle due operazioni di tale campo sono le seguenti:

$+$	$\overline{0}$	$\overline{1}$	x	$x+\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	x	$x+\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$x+\overline{1}$	x
x	x	$x+\overline{1}$	$\overline{0}$	$\overline{1}$
$x+\overline{1}$	$x+\overline{1}$	x	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{1}$	x	$x+\overline{1}$
$\overline{1}$	$\overline{1}$	x	$x+\overline{1}$
x	x	$x+\overline{1}$	$\overline{1}$
$x+\overline{1}$	$x+\overline{1}$	1	x

Denotato con K il campo ottenuto, si osserva subito che il polinomio $f = X^2+X+\overline{1}$ si fattorizza in $K[X]$ con due polinomi di grado 1 (e quindi ha due zeri in K). Infatti risulta: $f = (X+x)(X+x+\overline{1})$. [si noti che x è "per costruzione" uno zero di f in $K[X]$; l'altro zero $x + \overline{1}$ si ottiene dividendo f per $X + x$].

5. Introduzione agli anelli di interi quadratici

Come in $K[X]$, anche in $\boldsymbol{Z}[X]$ la relazione di congruenza *modulo* P (con $P \in \boldsymbol{Z}[X]$, $\partial P \geq 1$) è una relazione di equivalenza compatibile con le due operazioni di $\boldsymbol{Z}[X]$ [verificare]. Allora $\boldsymbol{Z}[X]/_{\equiv_P}$ è un anello commutativo unitario, usualmente denotato $\boldsymbol{Z}[X]/_{(P)}$ (o $\boldsymbol{Z}[X]/_{\langle P \rangle}$ o $\boldsymbol{Z}[X]/_{P\,\boldsymbol{Z}[X]}$).

Osservazione 1. $\boldsymbol{Z}[X]/_{(P)}$ "contiene" $\boldsymbol{Z}$ come sottoanello, nel senso che l'applicazione

$$i : \boldsymbol{Z} \to \boldsymbol{Z}[X]/_{(P)} \text{ tale che } i(a) = [a], \quad \forall\, a \in \boldsymbol{Z},$$

è un omomorfismo iniettivo di anelli. Infatti si ha:

$i(a+b) = [a+b] = [a] + [b] = i(a) + i(b)$, $i(a \cdot b) = [a \cdot b] = [a] \cdot [b] = i(a) \cdot i(b)$,
se $i(a) = i(b)$, allora $[a] = [b]$ e quindi $P \,|\, a - b$; per ragioni di grado, $a - b = 0$.

Si può quindi porre, in $\boldsymbol{Z}[X]/_{(P)}$, $[a] = a$, $\forall\, a \in \boldsymbol{Z}$, e pertanto, posto $x = [X]$, risulta

$$\boldsymbol{Z}[X]/_{(P)} = \{F(x),\ \forall\, F \in \boldsymbol{Z}[X];\ P(x) = 0\} =: \boldsymbol{Z}[x \,|\, P(x) = 0].$$

Osservazione 2. Verifichiamo che $\boldsymbol{Z}[X]/_{(P)}$ è un dominio d'integrità $\iff$ P è irriducibile.

L'implicazione ($\Longrightarrow$) si dimostra come in **Prop. 4.3**. Verifichiamo l'implicazione ($\Longleftarrow$). In base a **Osserv. 3.9**, se P è irriducibile è anche primo (in $\boldsymbol{Z}[X]$). Sia $[F][G] = 0$ e sia $[F] \neq 0$. Allora $P \,|\, FG$ e $P \not| F$. Ne segue che $P \,|\, G$, cioè $[G] = 0$. Dunque $\boldsymbol{Z}[X]/_{(P)}$ è integro.

Osservazione 3. Supponiamo che $P \in \boldsymbol{Z}[X]$ sia un polinomio monico di grado $p = \partial P \geq 1$. Ricordiamo (cfr. **Teor. 2.1**, *Nota 2*) che la divisione con resto vale anche in $\boldsymbol{Z}[X]$ a patto che il divisore sia monico. Pertanto, $\forall\, F \in \boldsymbol{Z}[X]$, risulta:

$$F = PQ + R, \quad \text{con } Q,\, R \in \boldsymbol{Z}[X] \text{ e } \partial R < p.$$

Dunque $[F] = [R]$. R è detto *residuo canonico di* F *modulo* P. Risulta quindi:

$$\boldsymbol{Z}[X]/_{(P)} = \Big\{ \sum_{i=0}^{p-1} a_i x^i,\ \forall\, a_0,\ a_1,\ \dots,\ a_{p-1} \in \boldsymbol{Z};\ P(x) = 0 \Big\}$$

e la scrittura di ogni elemento è unica (cfr. **Prop. 4.2**).

Si noti che se P non è monico, è molto più complicato determinare "buoni rappresentanti" per le classi di congruenza. A titolo di esempio si può verificare che, posto $P = 2X - 1$ e scelto $F = 2X^3 + 4X + 5$, allora $[F] \neq [a]$ e $[F] \neq [a + bX]$, $\forall\, a, b \in \boldsymbol{Z}$, mentre ad esempio $[F] = [X^2 + 7]$.

Osservazione 4. Supponiamo ora che P sia un polinomio monico e irriducibile in $\boldsymbol{Z}[X]$. Intendiamo verificare che:

(*i*) $\boldsymbol{Z}[X]/_{(P)}$ è un sottoanello del campo $\boldsymbol{Q}[X]/_{(P)}$.

(*ii*) $\boldsymbol{Z}[X]/_{(P)}$ non è mai un campo.

Relativamente ad (*i*), osserviamo che P è irriducibile in $\boldsymbol{Q}[X]$ (dal teorema di Gauss) e quindi (cfr. **Prop. 4.3**) $\boldsymbol{Q}[X]/_{(P)}$ è un campo. Si verifica facilmente che l'applicazione

$$\varphi : \boldsymbol{Z}[X]/_{(P)} \to \boldsymbol{Q}[X]/_{(P)} \quad \text{tale che } \varphi\big([F]_{\boldsymbol{Z}}\big) = [F]_{\boldsymbol{Q}},\ \ \forall\, [F]_{\boldsymbol{Z}} \in \boldsymbol{Z}[X]/_{(P)},$$

[con $[F]_{\boldsymbol{Z}} := F + P\,\boldsymbol{Z}[X]$ e $[F]_{\boldsymbol{Q}} := F + P\,\boldsymbol{Q}[X]$] è ben definita ed è un omomorfismo iniettivo [si utilizzi l'affermazione ($*$) di **Osserv. 3.9**]. Si noti poi che un sottoanello di un campo è sempre un dominio d'integrità.

Relativamente a (*ii*), basta verificare che, $\forall\, a \in \boldsymbol{Z}$, $a \neq 0$, $a \neq \pm 1$, $a = [a]$ non è invertibile in $\boldsymbol{Z}[X]/_{(P)}$. Infatti a, pensato in $\boldsymbol{Q}[X]/_{(P)}$, ha per inverso $\frac{1}{a}$. Se a fosse invertibile in $\boldsymbol{Z}[X]/_{(P)}$,

avrebbe per inverso $\frac{1}{a}$, ma $\frac{1}{a} \notin \boldsymbol{Z}[X]/_{(P)}$.

Esamineremo in dettaglio gli anelli $\boldsymbol{Z}[X]/_{(P)}$, con $P = X^2 - d$ polinomio irriducibile in $\boldsymbol{Z}[X]$. Tali anelli sono detti *anelli di interi quadratici*.

Si osservi (cfr. **Osserv. 4.4**) che l'applicazione

$$\varphi : \boldsymbol{Z}[X]/_{(X^2-d)} \to \boldsymbol{C} \text{ tale che } \varphi(a+bx) = a + b\sqrt{d}, \ \forall\, a, b \in \boldsymbol{Z},$$

è un omomorfismo iniettivo di anelli. Pertanto, tramite φ, l'anello $\boldsymbol{Z}[X]/_{(X^2-d)}$ si identifica con la sua immagine, usualmente denotata $\boldsymbol{Z}[\sqrt{d}]$:

$$\boldsymbol{Z}[\sqrt{d}] = Im\,\varphi = \{a + b\sqrt{d}, \ \forall\, a, b \in \boldsymbol{Z}\}.$$

Si noti che se $d \geq 2$ e $P = X^2 - d$ è irriducibile, l'anello $\boldsymbol{Z}[\sqrt{d}]$ è un sottoanello (integro) di $\boldsymbol{R}$. Se invece $d < 0$, $\boldsymbol{Z}[\sqrt{d}]$ è un sottoanello (integro) di $\boldsymbol{C}$.

Osservazione 5. In ogni anello $\boldsymbol{Z}[\sqrt{d}]$ sono definiti il *coniugato* $\overline{z}$ e la *norma* $\mathcal{N}(z)$ di ogni elemento $z = a + b\sqrt{d}$, ponendo

$$\overline{z} := a - b\sqrt{d}, \ \ \mathcal{N}(z) := z\,\overline{z} = a^2 - db^2.$$

(*i*) Si verifica con semplici calcoli che $\mathcal{N}(z_1 z_2) = \mathcal{N}(z_1)\mathcal{N}(z_2)$, $\forall\, z_1, z_2 \in \boldsymbol{Z}[\sqrt{d}]$. [Basta porre $z_1 = a_1 + b_1\sqrt{d}$, $z_2 = a_2 + b_2\sqrt{d}$ ed eseguire il calcolo delle norme].

(*ii*) Se $d < 0$, $\sqrt{d} = i\sqrt{-d}$ e $\mathcal{N}(z)$ coincide con l'usuale norma in $\boldsymbol{C}$, $\forall\, z \in \boldsymbol{Z}[\sqrt{d}]$. Dunque $\mathcal{N}(z) \geq 0$ e risulta:

$$z \in \mathcal{U}(\boldsymbol{Z}[\sqrt{d}]) \iff \mathcal{N}(z) = 1.$$

Verifichiamo tale affermazione. ($\Longrightarrow$): $zw = 1 \implies 1 = \mathcal{N}(zw) = \mathcal{N}(z)\mathcal{N}(w) \implies \mathcal{N}(z) = \mathcal{N}(w) = 1$. ($\Longleftarrow$): $\mathcal{N}(z) = 1 \implies z\,\overline{z} = 1 \implies z \in \mathcal{U}(\boldsymbol{Z}[\sqrt{d}])$.

(*iii*) Se $d < 0$ e $\mathcal{N}(z) = p$ è un numero primo, allora z è irriducibile. Infatti, se $z = z_1 z_2$, allora $p = \mathcal{N}(z_1)\mathcal{N}(z_2)$ e dunque $\mathcal{N}(z_1) = 1$ oppure $\mathcal{N}(z_2) = 1$, cioè z_1 o z_2 è invertibile.

Tra gli anelli $\boldsymbol{Z}[\sqrt{d}]$ è importante l'*anello degli interi di Gauss* $\boldsymbol{Z}[i] = \boldsymbol{Z}[\sqrt{-1}] = \boldsymbol{Z}[X]/_{(X^2+1)}$. Dimostreremo che in $\boldsymbol{Z}[i]$ vale il teorema della divisione con resto e ne trarremo le dovute conseguenze.

Si osserva subito che in $\boldsymbol{Z}[i]$ risulta: $\mathcal{N}(z) = a^2 + b^2$, $\forall\, z = a + ib \in \boldsymbol{Z}[i]$. Inoltre

$$\mathcal{N}(z) = 1 \iff a^2 + b^2 = 1 \iff \begin{cases} a = \pm 1 \\ b = 0 \end{cases} \text{ o } \begin{cases} a = 0 \\ b = \pm 1 \end{cases} \iff z = \pm 1 \text{ o } z = \pm i,$$

e quindi, tenuto conto di **Osserv. 5**(*ii*),

$$\mathcal{U}(\boldsymbol{Z}[i]) = \{1, -1, i, -i\}.$$

Proposizione 1. (*Divisione con resto in* $\boldsymbol{Z}[i]$). *Siano* $z, w \in \boldsymbol{Z}[i]$, $w \neq 0$. *Esistono* $q, r \in \boldsymbol{Z}[i]$ *tali che*

$$z = wq + r \ \text{ e } \ \mathcal{N}(r) < \mathcal{N}(w).$$

[Si noti che non viene richiesta l'unicità di q, r*.]*

Dim. Sia $z = a + ib$ e $w = c + id \neq 0$. Poiché $\boldsymbol{Z}[i] \subset \boldsymbol{Q}[i]$ e $\boldsymbol{Q}[i]$ è un campo, si può considerare in $\boldsymbol{Q}[i]$ l'elemento $\frac{z}{w}$. Risulta:

$$\frac{z}{w} = \frac{z\,\overline{w}}{w\,\overline{w}} = \frac{(a+ib)(c-id)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + i\,\frac{bc-ad}{c^2+d^2}.$$

Denotiamo rispettivamente con $\alpha, \beta \in \boldsymbol{Z}$ i due interi più prossimi rispettivamente a

$$\frac{ac+bd}{c^2+d^2} = \mathcal{R}e(\tfrac{z}{w}), \quad \frac{bc-ad}{c^2+d^2} = \mathcal{I}m(\tfrac{z}{w}).$$

[*Nota*: se $n \in \boldsymbol{Z}$ e $q = n + \frac{1}{2}$, <u>per convenzione</u> assumeremo che l'intero più vicino a q sia $n+1$].

Si noti che $\left|\alpha - \mathcal{R}e(\frac{z}{w})\right| \leq \frac{1}{2}$, $\left|\beta - \mathcal{I}m(\frac{z}{w})\right| \leq \frac{1}{2}$. Si pone:

$$q := \alpha + i\,\beta \in \boldsymbol{Z}[i], \quad r := (\tfrac{z}{w} - q)w = z - wq \in \boldsymbol{Z}[i].$$

Ovviamente: $wq + r = z$. Resta quindi solo da verificare che $\mathcal{N}(r) < \mathcal{N}(w)$. Si ha:

$$\mathcal{N}(r) = \mathcal{N}\big((\tfrac{z}{w} - q)w\big) = \mathcal{N}(\tfrac{z}{w} - q)\mathcal{N}(w)$$

e

$$\mathcal{N}(\tfrac{z}{w} - q) = \big(\mathcal{R}e(\tfrac{z}{w}) - \alpha\big)^2 + \big(\mathcal{I}m(\tfrac{z}{w}) - \beta\big)^2 \leq \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2}.$$

Allora $\mathcal{N}(r) \leq \frac{1}{2}\mathcal{N}(w) < \mathcal{N}(w)$ [essendo $w \neq 0$ e quindi $\mathcal{N}(w) > 0$].

Esempio 1. Vogliamo dividere $z = 1 + i$ per $w = -1 + i$. Si ha:

$$\tfrac{z}{w} = \tfrac{(1+i)(-1-i)}{(-1+i)(-1-i)} = -\tfrac{-(1+i)^2}{2} = \tfrac{1-1+2i}{2} = -i.$$

Allora: $\alpha = 0,\ \beta = -1,\ q = -i,\ r = (\frac{z}{w} - q)w = (-i + i)w = 0$. Dunque

$$1 + i = (-1 + i)(-i) + 0.$$

Esempio 2. Dividere $z = 1 + 2i$ per $w = 1 - i$. Si ha:

$$\tfrac{z}{w} = \tfrac{(1+2i)(1+i)}{(1-i)(1+i)} = \tfrac{-1+3i}{2} = -\tfrac{1}{2} + \tfrac{3}{2}\,i.$$

Allora: $\alpha = 0,\ \beta = 2,\ q = 2i,\ r = (\frac{z}{w} - q)w = (-\frac{1}{2} + \frac{3}{2}i - 2i)(1 - i) = -1$. Dunque

$$1 + 2i = (1 - i)(2i) - 1.$$

Nota. Si sarebbe anche potuto scegliere ad esempio $\alpha = -1,\ \beta = 1$, ottenendo quindi $q_1 = -1 + i,\ r_1 = (\frac{z}{w} - q_1)w = 1$. Dunque $1 + 2i = (1 - i)(-1 + i) + 1$.

Come si vede, quoziente e resto non sono unici.

Segnaliamo che la validità del teorema della divisione con resto in $\boldsymbol{Z}[i]$ implica le seguenti importanti conseguenze (come già visto per $\boldsymbol{Z}$ e $K[X]$):

(**1**) in $\boldsymbol{Z}[i]$ è definito il MCD.
(**2**) esiste in $\boldsymbol{Z}[i]$ un'identità di Bézout (relativa al MCD).
(**3**) vale in $\boldsymbol{Z}[i]$ il lemma di Euclide.
(**4**) in $\boldsymbol{Z}[i]$ ogni elemento irriducibile è primo (e viceversa).
(**5**) $\boldsymbol{Z}[i]$ è un *UFD*.

Ciò che avviene in $\boldsymbol{Z}[i]$ non avviene però in tutti gli anelli $\boldsymbol{Z}[\sqrt{d}]$. Dimostreremo ora che ad esempio in $\boldsymbol{Z}[\sqrt{-3}]$ esistono elementi irriducibili ma non primi e che $\boldsymbol{Z}[\sqrt{-3}]$ non è un *UFD*.

Osserviamo preliminarmente che $\mathcal{U}\big(\boldsymbol{Z}[\sqrt{-3}]\big) = \{\pm 1\}$. Infatti, in base a **Osserv. 5**(*ii*), posto $z = a + b\sqrt{-3}$:

$$z \in \mathcal{U}\big(\boldsymbol{Z}[\sqrt{-3}]\big) \iff \mathcal{N}(z) = 1 \iff a^2 + 3b^2 = 1 \iff a = \pm 1,\ b = 0 \iff z = \pm 1.$$

Proposizione 2. *In* $\boldsymbol{Z}[\sqrt{-3}]$ *l'elemento* $z = 1 + \sqrt{-3}$ *è irriducibile ma non primo. Ne segue che* $\boldsymbol{Z}[\sqrt{-3}]$ *non è un UFD.*

Dim. Verifichiamo che z non è primo: poiché $\mathcal{N}(z) = z\overline{z} = 4$, allora $z \,\big|\, 4$ e dunque $z \,\big|\, 2 \cdot 2$. Basterà allora verificare che $z \not| 2$ [e da ciò segue che z non è primo]. Se per assurdo $z \,\big|\, 2$, allora

$$2 = z(a + b\sqrt{-3}) = (1 + \sqrt{-3})(a + b\sqrt{-3}) = (a - 3b) + (a + b)\sqrt{-3}.$$

Ne segue $\begin{cases} 2 = a - 3b \\ a + b = 0, \end{cases}$ da cui $a = \frac{1}{2}$: assurdo.

Verifichiamo che z è irriducibile. Posto $z = z_1 z_2$, bisogna verificare che uno dei due fattori è invertibile, cioè che ha norma 1. Si ha: $4 = \mathcal{N}(z) = \mathcal{N}(z_1)\mathcal{N}(z_2)$. Ne segue:

$$\begin{cases} \mathcal{N}(z_1) = 2 \\ \mathcal{N}(z_2) = 2 \end{cases} \quad \text{oppure} \quad \begin{cases} \mathcal{N}(z_1) = 1 \text{ (oppure } 4) \\ \mathcal{N}(z_2) = 4 \text{ (oppure } 1). \end{cases}$$

Ma in $\boldsymbol{Z}[\sqrt{-3}]$ non esistono elementi di norma 2. Infatti l'equazione $a^2 + 3b^2 = 2$ non ha soluzioni intere, come subito si osserva. Si conclude quindi che $\mathcal{N}(z_1) = 1$ oppure $\mathcal{N}(z_2) = 1$.

È noto che in un *UFD* ogni elemento irriducibile è primo (cfr. **Osserv. 4.10**). Ne segue che $\boldsymbol{Z}[\sqrt{-3}]$ non è un *UFD*. Ma vogliamo comunque individuare due differenti fattorizzazioni (con elementi irriducibili) di uno stesso elemento di $\boldsymbol{Z}[\sqrt{-3}]$.

Dalla precedente dimostrazione segue che in $\boldsymbol{Z}[\sqrt{-3}]$ tutti gli elementi aventi norma 4 sono irriducibili. Cerchiamo tali elementi. Posto $z = a + b\sqrt{-3}$, si ha:

$$\mathcal{N}(z) = 4 \iff a^2 + 3b^2 = 4 \iff \begin{cases} a^2 = b^2 = 1 \text{ oppure} \\ a^2 = 4,\ b = 0 \end{cases} \iff \begin{cases} z = \pm 1 \pm \sqrt{-3} \text{ oppure} \\ z = \pm 2. \end{cases}$$

In $\boldsymbol{Z}[\sqrt{-3}]$ l'elemento 4 ammette le due seguenti fattorizzazioni in elementi irriducibili:

$$4 = 2 \cdot 2, \qquad 4 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Poiché 2 non è associato né con $1 + \sqrt{-3}$ né con $1 + \sqrt{-3}$, le due fattorizzazioni di 4 sono diverse.

6. Esercizi del Capitolo III

3.1. Sono assegnati in $\boldsymbol{Q}[x]$ i due polinomi

$$F(X) = X^6 + 4X^5 + 2X^4 - 8X^3 - 7X^2 + 4X + 4, \quad G = X^3 + X^2 + X + 1.$$

Calcolare il $MCD(F, G)$ e scrivere un'identità di Bézout relativa a F e G.

* * * * * * * * *

3.2. Dei due polinomi F e G dell'esercizio precedente (pensati in $\boldsymbol{Z}[X]$), calcolare gli zeri razionali con le relative molteplicità.

* * * * * * * * *

3.3. (*i*) Eseguire la divisione con resto tra i due polinomi

$$F = \overline{2}X^5 + X^3 + \overline{4}X, \quad G = \overline{5}X^2 + \overline{1} \in \boldsymbol{Z}_7[X].$$

(*ii*) È possibile eseguire la divisione con resto tra gli stessi polinomi in $\boldsymbol{Z}_6[X]$?

* * * * * * * * *

3.4. (*i*) Determinare un'identità di Bézout per i due polinomi

$$F = X^4 + X^2 + \overline{1}, \quad G = X^3 + X + \overline{1} \in \boldsymbol{Z}_2[X].$$

(*ii*) Determinare un'identità di Bézout per gli stessi polinomi pensati in $\boldsymbol{Z}_3[X]$.

* * * * * * * * *

3.5. Sia $\varphi : \boldsymbol{Z}[X] \to \boldsymbol{Z}[X]$ un automorfismo di anelli.

(*i*) Verificare che φ induce l'identità su $\boldsymbol{Z}$, cioè $\varphi_{\big|_{\boldsymbol{Z}}} = \mathbf{1}_{\boldsymbol{Z}}$.

(*ii*) Verificare che il polinomio $\varphi(X)$ ha grado 1.

(*iii*) Dedurre da (*ii*) che φ fissa il grado dei polinomi, cioè $\partial\big(\varphi(P)\big) = \partial P, \ \forall\, P \in \boldsymbol{Z}[X]$.

* * * * * * * * *

3.6. Sia $F \in \boldsymbol{R}[X]$ un polinomio di grado dispari ed a coefficienti in $\boldsymbol{R}$. Verificare che F ammette un numero dispari di zeri reali, contati con la rispettiva molteplicità.

* * * * * * * * *

3.7. Sia A un anello commutativo con unità e sia $F = \sum_{i=0}^{n} a_i X^i \in A[X]$. Si chiama *polinomio derivato di* F il polinomio

$$F' = \tfrac{dF}{dX} = a_1 + 2a_2X + 3a_3X^2 + \ \ldots\ + na_nX^{n-1}.$$

[Se $A = \boldsymbol{R}$, $\frac{dF}{dX}$ coincide con la derivata di F, intesa come funzione di variabile reale].

(*i*) Verificare le usuali proprietà della derivazione: $\forall\, F, G \in A[X], \ \forall\, a \in A$,

$$\tfrac{d(aF)}{dX} = a\,\tfrac{dF}{dX}; \quad \tfrac{d(F+G)}{dX} = \tfrac{dF}{dX} + \tfrac{dG}{dX}; \quad \tfrac{d(FG)}{dX} = F\,\tfrac{dG}{dX} + G\,\tfrac{dF}{dX}.$$

(*ii*) Sia $F \in \boldsymbol{C}[X]$ e sia α uno zero di F. Verificare che:

α è uno zero multiplo di F [cioè uno zero con molteplicità ≥ 2] $\iff$ α è uno zero di $\frac{dF}{dX}$.

* * * * * * * * *

3.8. Sia K un campo e siano $F, G \in K[X]$ polinomi di grado positivo. Verificare che:

F, G hanno un fattore comune (non costante) $\iff$ $\exists\, A, B \in K[X]$ tali che $AF = BG$, con $0 \leq \partial A < \partial G$ e $0 \leq \partial B < \partial F$.

* * * * * * * * *

3.9. Sia K un campo e siano $F = \sum_{i=0}^{n} a_i X^i$, $G = \sum_{j=0}^{m} b_j X^j \in K[X]$, rispettivamente di gradi $n, m \geq 1$. Sia V il K-spazio vettoriale dei polinomi in $K[X]$ aventi grado $\leq n + m - 1$, e si consideri in V la base (canonica) $\{1, X, X^2, X^3, \ \ldots\ , X^{n+m-1}\}$. [Si noti, che, rispetto a tale base,

le coordinate di un polinomio in V sono i suoi coefficienti]. La matrice delle coordinate [rispetto a tale base] dei seguenti polinomi di V:

$$F,\ XF,\ X^2F,\ \dots,\ X^{m-1}F,\ G,\ XG,\ X^2G,\ \dots,\ X^{n-1}G$$

è detta *matrice di Sylvester di* F, G. Si tratta di una matrice quadrata di ordine $n+m$. Il suo determinante è detto *risultante di* F, G ed è denotato $Ris(F,G)$. Dunque

$$Ris(F,G) = det \begin{pmatrix} a_0 & a_1 & a_2 & & & & a_n & 0 & & & 0 \\ 0 & a_0 & a_1 & a_2 & & & & a_n & 0 & & 0 \\ 0 & 0 & a_0 & a_1 & a_2 & & & & a_n & 0 & 0 \\ \vdots & & & & & & & & & & \\ \vdots & & & & & & & & & & \\ 0 & & & & 0 & a_0 & a_1 & a_2 & & & a_n \\ b_0 & b_1 & b_2 & & & & & b_m & 0 & & 0 \\ 0 & b_0 & b_1 & b_2 & & & & & b_m & 0 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 & & & & & b_m & 0 \\ \vdots & & & & & & & & & & \\ \vdots & & & & & & & & & & \\ 0 & 0 & 0 & 0 & b_0 & b_1 & b_2 & & & & b_m \end{pmatrix}.$$

Verificare che:

$$F,\ G \text{ hanno un fattore comune (non costante)} \iff Ris(F,G) = 0.$$

* * * * * * * * *

3.10. È assegnato il polinomio $F = X^3 + X^2 + X + 1 \in \boldsymbol{Q}[X]$. Applicando ad F l'automorfismo

$$T : \boldsymbol{Q}[X] \to \boldsymbol{Q}[X] \text{ tale che } T(P(X)) = P(X-1),\ \forall\, P(X) \in \boldsymbol{Q}[X],$$

verificare che F è riducibile e determinarne una fattorizzazione non banale.

* * * * * * * * *

3.11. Verificare che il polinomio $X^4 + 1 \in \boldsymbol{Z}_3[X]$ è riducibile e scriverne una fattorizzazione.

* * * * * * * * *

3.12. Verificare che il polinomio $X^4 + 1 \in \boldsymbol{Z}[X]$ è irriducibile.

* * * * * * * * *

3.13. Fattorizzare il polinomio $X^6 - X^4 - X^2 + 1 \in \boldsymbol{Z}[X]$.

* * * * * * * * *

3.14. Verificare (usando il criterio di Eisenstein) che il polinomio $X^4 - X^3 + X^2 - X + 1 \in \boldsymbol{Z}[X]$ è irriducibile.

* * * * * * * * *

3.15. Verificare (usando la riduzione in $\boldsymbol{Z}_2[X]$) che il polinomio $X^4 - 3X^3 + 3X^2 - 3X + 9 \in \boldsymbol{Z}[X]$ è irriducibile.

* * * * * * * * *

3.16. È assegnato il polinomio $f = X^4 + 3X^3 + 2X^2 + X - 1 \in \boldsymbol{Z}[X]$.

(*i*) Fattorizzare f in $\boldsymbol{Q}[X]$ con fattori irriducibili.

(*ii*) Fattorizzare f in $\boldsymbol{R}[X]$ con fattori irriducibili.

(*iii*) Fattorizzare f in $\boldsymbol{C}[X]$ con fattori irriducibili.

(*iv*) Fattorizzare f in $\boldsymbol{Z}_3[X]$ con fattori irriducibili.

* * * * * * * * *

3.17. (*i*) Verificare che il polinomio $f = X^5 + \overline{2}X + \overline{1} \in \boldsymbol{Z}_3[X]$ è irriducibile in $\boldsymbol{Z}_3[X]$.

(*ii*) Calcolare l'inverso di X^3 nel campo $\boldsymbol{Z}_3[X]/_{(f)}$.

* * * * * * * * *

3.18. [*Esonero 3/6/03*] È assegnato in $\boldsymbol{Q}[X]$ il polinomio $f = X^4 - X^3 + 3X^2 - X + 2$.

(*i*) Verificare che f è riducibile in $\boldsymbol{Q}[X]$.

(*ii*) Verificare se l'elemento $\overline{X} \in \boldsymbol{Q}[X]/_{(f)}$ ammette inverso.

(*iii*) Determinare un divisore dello zero (non nullo) in $\boldsymbol{Q}[X]/_{(f)}$.

(*iv*) Verificare che nessun elemento $a\overline{X} + b \in \boldsymbol{Q}[X]/_{(f)}$ è un divisore dello zero (non nullo).

* * * * * * * * *

3.19. [*Esonero 3/6/03*] Per ogni $a \in \boldsymbol{Z}_5$, si considerino i polinomi $f_a = X^3 + \overline{2}X + a \in \boldsymbol{Z}_5[X]$.

(*i*) Fattorizzare ogni f_a come prodotto di polinomi irriducibili.

(*ii*) Scelto un polinomio f_a irriducibile, determinare l'inverso di $\overline{X}$ nel campo $\boldsymbol{Z}_5[X]/_{(f_a)}$.

* * * * * * * * *

3.20. [*Esame 10/6/03*] Nell'insieme $\boldsymbol{Q}[X]$ dei polinomi a coefficienti razionali si introduce la seguente relazione ρ: $\forall\, f, g \in \boldsymbol{Q}[X]$,

$$f \,\rho\, g \iff \text{i termini noti di } f \text{ e } g \text{ hanno la stessa parte intera.}$$

[*Nota*. La parte intera $[x]$ di un numero reale x è il massimo intero n tale che $n \leq x$].

(*i*) Verificare che ρ è una relazione di equivalenza su $\boldsymbol{Q}[X]$.

(*ii*) Descrivere le classi di equivalenza modulo ρ dei polinomi $\frac{1}{2} + X$ e $X + X^2$.

(*iii*) Verificare che l'insieme quoziente $\boldsymbol{Q}[X]/_{\rho}$ è in corrispondenza biunivoca con $\boldsymbol{Z}$. Esplicitare una biiezione tra i due insiemi.

* * * * * * * * *

3.21. [*Esame 10/6/03*] (*i*) Verificare che i due polinomi $f = X^2 + \overline{1}$, $g = X^2 + \overline{2}X + \overline{2} \in \boldsymbol{Z}_3[X]$ sono irriducibili.

(*ii*) Determinare gli elementi dei due campi $\boldsymbol{Z}_3[X]/(f)$, $\boldsymbol{Z}_3[X]/(g)$ e scrivere la tavola moltiplicativa del secondo.

(*iii*) Verificare che tali campi sono isomorfi, esplicitando un isomorfismo tra essi.

* * * * * * * * *

3.22. [*Esame 10/6/03*] In $\boldsymbol{Z}_5[X]$ è assegnato il polinomio

$$f = X^6 + X^5 + X^4 + \overline{3}X^3 + X^2 + X + \overline{1}.$$

(*i*) Verificare che f è prodotto di due polinomi irriducibili di grado 3.

(*ii*) Determinare la cardinalità dell'anello $\boldsymbol{Z}_5[X]/(f)$ ed indicarne un eventuale divisore dello zero.

(*iii*) Determinare la classe del polinomio $(f - X - \overline{1})^4$ in $\boldsymbol{Z}_5[X]/(f)$.

* * * * * * * * *

3.23. [*Esame 1/7/03*] (*i*) Stabilire, motivando la risposta, quali tra i seguenti anelli sono campi e quali non lo sono.

$$K_1 = \boldsymbol{Q}[X]/_{(X^4+X^3+X^2+X+1)}, \quad K_2 = \boldsymbol{Z}_2[X]/_{(X^3+X^2+X+\overline{1})},$$
$$K_3 = \boldsymbol{C}[X]/_{(X^4-2\pi X^2+\pi^2+4)}, \quad K_4 = \boldsymbol{Z}_7[X]/_{(X^3+\overline{4})}.$$

(*ii*) Stabilire inoltre quali tra tali anelli contengono divisori dello zero e, in questo caso, indicarne esplicitamente una coppia.

* * * * * * * * *

3.24. [*Esame 1/7/03*] In $\boldsymbol{Z}_5[X]$ è assegnato il polinomio $f = X^2 + X + \overline{1}$.

(*i*) Verificare che f è irriducibile in $\boldsymbol{Z}_5[X]$.

(*ii*) Posto $\alpha = X + (f)$, elencare tutti gli elementi del campo $K = \boldsymbol{Z}_5[X]/_{(f)}$ e determinare gli eventuali elementi di K che non sono quadrati (in K).

(*iii*) Determinare una fattorizzazione non banale del polinomio $X^2 - \overline{2}\alpha \in K[X]$.

* * * * * * * * *

3.25. [*Esame 23/9/03*] Consideriamo le due classi di congruenza $[X^3 + X^2]$ e $[X + 2]$ dell'anello quoziente $\boldsymbol{Q}[X]/_{(X^3-X^2-X+1)}$.

Per ognuna delle due classi si stabilisca, motivando la risposta, se si tratta di un elemento invertibile o di un divisore dello zero. Nel caso in cui l'elemento sia invertibile, si trovi esplicitamente l'inverso e si faccia la verifica del risultato ottenuto.

* * * * * * * * *

3.26. [*Esame 2/2/04*] Si considerino le classi dell'elemento $X^2+x+\overline{3}$ nei due anelli quoziente

$$A = \boldsymbol{Z}_5[X]/_{(X^3+\overline{2}X+\overline{2})}, \quad B = \boldsymbol{Z}_5[X]/_{(X^3+\overline{3}X+\overline{2})}.$$

In particolare, se si tratta di un divisore dello zero, si determini una classe non nulla $[f(X)] \in A$ (o $\in B$) tale che $[f(X)]\cdot[X^2+X+\overline{3}] = [\overline{0}]$; se si tratta di un elemento invertibile, se ne determini l'inverso.

* * * * * * * * *

3.27. Assegnato il polinomio $f = X^5+\overline{1} \in \boldsymbol{Z}_7[X]$, determinarne una fattorizzazione come prodotto di polinomi irriducibili (in $\boldsymbol{Z}_7[X]$).

* * * * * * * * *

3.28. (*i*) Verificare che il gruppo degli elementi invertibili dell'anello $\boldsymbol{Z}[i]$ degli interi di Gauss coincide con il gruppo delle radici complesse quarte dell'unità.

(*ii*) Sia $z \in \boldsymbol{Z}[i]$. Verificare che, se $\mathcal{N}(z)$ è un numero primo, z è irriducibile (in $\boldsymbol{Z}[i]$).

(*iii*) Verificare che l'elemento $z=3$ è irriducibile (in $\boldsymbol{Z}[i]$). Dedurne che la (*ii*) non si inverte.

(*iv*) Fattorizzare $z=5$ come prodotto di elementi irriducibili di $\boldsymbol{Z}[i]$.

* * * * * * * * *

3.29. [*Esonero 3/6/03*] Sono assegnati in $\boldsymbol{Z}[i]$ i due interi di Gauss

$$z = 4+2i, \quad w = 3-i.$$

(*i*) Determinare il massimo comun divisore $MCD(z,w)$.

(*ii*) Scrivere z come prodotto di interi di Gauss irriducibili.

* * * * * * * * *

3.30. Sono assegnati in $\boldsymbol{Z}[i]$ i due interi di Gauss $z_1 = 4+3i$, $z_2 = 3-2i$.

(*i*) Calcolare $MCD(z_1, z_2)$, utilizzando l'algoritmo euclideo delle divisioni successive.

(*ii*) Scrivere l'identità di Bézout per z_1, z_2.

(*iii*) Determinare $mcm(z_1, z_2)$.

(*iv*) Verificare che l'elemento z_1 non è primo.

(*v*) Scrivere una fattorizzazione di z_1 come prodotto di elementi irriducibili.

* * * * * * * * *

3.31. Si consideri il dominio d'integrità $\boldsymbol{Z}[\sqrt{-2}] = \{a+b\sqrt{-2},\ \forall\, a,\, b \in \boldsymbol{Z}\}$.

(*i*) Determinare $\mathcal{U}(\boldsymbol{Z}[\sqrt{-2}])$.

(*ii*) Osservato che in $\boldsymbol{Z}[\sqrt{-2}]$ risulta

$$9 = 3\cdot 3 = (1+2\sqrt{-2})(1-2\sqrt{-2}),$$

dire se da tale uguaglianza si può concludere che $\boldsymbol{Z}[\sqrt{-2}]$ non è un UFD.

* * * * * * * * *

3.32. Sia $p \in \boldsymbol{N}$ un numero primo tale che $p \equiv 3\ (mod\ 4)$. Verificare che p è irriducibile in $\boldsymbol{Z}[i]$.

Nota. Tale risultato fornisce esempi di elementi irriducibili in $\boldsymbol{Z}[i]$ a norma non prima.

Suggerimento: verificare preliminarmente che, $\forall\, a \in \boldsymbol{Z}$, risulta $a \equiv 0\ (mod\ 4)$ oppure $a \equiv 1\ (mod\ 4)$; dedurne che in $\boldsymbol{Z}$ la somma di due quadrati non è mai congruente a $3\ (mod\ 4)$.

* * * * * * * * *

3.33. [Proposto dallo studente V.Capraro]. (*i*) Sia $\widetilde{\ }\colon K[X] \to K[X]$ l'applicazione così definita:

$$\widetilde{F} = \sum_{i=0}^{n} a_{n-i} X^i, \ \ \forall\, F = \sum_{i=0}^{n} a_i X^i \in K[X]$$

[dunque $\widetilde{\ }$ trasforma il coefficiente direttore di P nel termine noto di $\widetilde{F}$, ecc.]. Sia ora $P \in K[X]$, con $\partial P = n \geq 1,\ a_0 \neq 0$. Risulta:

$$P \text{ è irriducibile } \iff \widetilde{P} \text{ è irriducibile.}$$

(*ii*) Tenuto conto di (*i*), scrivere una diversa versione del criterio di irriducibilità di Eisenstein.

* * * * * * * * *

3.34. [Proposto dallo studente V.Capraro]. Sia $f = \sum_{i=0}^{n} a_i X^i \in \boldsymbol{Z}[X]$, con $n = \partial f \geq 1$. Sia p un primo tale che $p \nmid a_n$. Sia $\overline{f} \in Z_p[X]$ la riduzione di $f \ mod\ p$ e sia $A = Z_p[X]/_{(f)}$.

Verificare che se $\big(\prod_{\alpha \in A^\cdot} \alpha\big)^2 \neq 0$, allora f è irriducibile in $\boldsymbol{Z}[X]$.

* * * * * * * * *

3.35. Sia K un campo e sia $P \in K[X]$, con $n = \partial P \geq 1$. Sia $A = K[X]/_{(P)}$ e sia $\overline{F} = F + PK[X]$ un suo elemento non nullo [dunque $F \notin PK[X]$]. Verificare che le seguenti condizioni sono equivalenti:

(*a*) $\overline{F}$ è uno zero-divisore in A;

(*b*) $\overline{F}$ non è invertibile in A;

(*c*) $MCD(F, P) \neq 1$.

* * * * * * * * *

Appendice 3

Le formule di Cardano e di Ferrari

Abbiamo osservato [cfr. **Cap. III, Teor. 3.1**] che ogni polinomio di grado n in $\boldsymbol{C}[X]$ ammette n zeri (contati con la relativa molteplicità). In particolare, ogni polinomio di grado 2

$$aX^2 + bX + c \in \boldsymbol{C}[X]$$

ammette i due zeri

$$\gamma_1 = \frac{-b+\sqrt{b^2-4ac}}{2a}, \quad \gamma_2 = \frac{-b-\sqrt{b^2-4ac}}{2a}$$

[dove $\sqrt{b^2-4ac}$ rappresenta una delle due radici quadrate del numero complesso b^2-4ac]. Diremo che le espressioni di γ_1, γ_2 scritte sopra sono le *formule di risoluzione per radicali* dell'equazione polinomiale generale di grado 2.

Un famoso risultato - il *Teorema di Abel - Ruffini* (1824) - afferma che, se $n \geq 5$, non esistono *formule risolutive per radicali* della generica equazione polinomiale di grado n, cioè non esistono formule che consentano di scrivere gli zeri del polinomio

$$a_0 + a_1X + \ ... \ + a_nX^n \in \boldsymbol{C}[X] \ \ (n \geq 5)$$

tramite espressioni algebriche dipendenti da $a_0, a_1, \ ... \ , a_n$ e da loro radici (quadrate e non). Invece, per i gradi $n = 3$ e $n = 4$, esistono formule risolutive per radicali, dovute agli *algebristi italiani* del 1500 (Cardano, Tartaglia, Del Ferro, Ferrari, Bombelli, ecc.).

In questa appendice presenteremo la formula di G. Cardano, che fornisce gli zeri dei polinomi di grado 3 a coefficienti in $\boldsymbol{C}$ o in $\boldsymbol{R}$, ed accenneremo alla formula di L. Ferrari, relativa agli zeri dei polinomi di grado 4.

Non è restrittivo supporre, ai fini della ricerca degli zeri, che i polinomi in questione siano monici. Inoltre, è sempre possibile, con un'opportuna sostituzione lineare, fare in modo che il polinomio assegnato [di grado $n = 3$ o $n = 4$] sia trasformato in un polinomio monico dello stesso grado, ma privo del termine di grado $n-1$. Infatti si verifica facilmente che la sostituzione lineare $X \longrightarrow X - \frac{a}{3}$ su $\boldsymbol{C}[X]$ trasforma il polinomio

$$X^3 + aX^2 + bX + c$$

nel cosiddetto *polinomio incompleto associato*

$$X^3 + pX + q, \ \text{ con } \ \begin{cases} p = b - \frac{a}{3} \\ q = \frac{2a^3}{27} - \frac{ab}{3} + c; \end{cases}$$

mentre la sostituzione lineare $X \longrightarrow X - \frac{a}{4}$ su $\boldsymbol{C}[X]$ trasforma il polinomio

$$X^4 + aX^3 + bX^2 + cX + d$$

nel polinomio incompleto associato

$$X^4 + pX^2 + qX + r, \ \text{ con } \ \begin{cases} p = -\frac{3a^4}{256} + \frac{a^2b}{16} - \frac{ac}{4} + d \\ q = \frac{a^3}{8} - \frac{ab}{2} + c \\ r = -\frac{3a^2}{8} + b. \end{cases}$$

Basterà quindi determinare le soluzioni dei polinomi incompleti e poi "traslarle" con la sostituzione lineare in precedenza applicata [cioè $X \longrightarrow X - \frac{a}{3}$ o $X \longrightarrow X - \frac{a}{4}$].

(*A*) *Le formule di Cardano in* $\boldsymbol{C}[X]$

Tali formule [presentate da Cardano (nel 1545), ma probabilmente dovute a Del Ferro e Tartaglia] forniscono i tre zeri del generico polinomio incompleto

$$P = X^3 + pX + q \in \boldsymbol{C}[X].$$

Per ottenerle, si consideri la seguente ovvia identità in $\boldsymbol{C}$:

$$(u+v)^3 - 3uv(u+v) - (u^3+v^3) = 0.$$

Confrontando tale identità con l'espressione del polinomio P, si ha subito che:

$$u+v \text{ è uno zero di } P \iff (u,v) \text{ è soluzione del seguente sistema } (\bullet) \begin{cases} -3uv = p \\ -(u^3+v^3) = q. \end{cases}$$

Ovviamente le soluzioni del sistema $(\bullet)$ verificano il seguente sistema $(\bullet\bullet)$ $\begin{cases} u^3+v^3 = -q \\ u^3 v^3 = -\frac{p^3}{27}. \end{cases}$ Viceversa, le soluzioni (u,v) di $(\bullet\bullet)$ tali che $uv = -\frac{p}{3}$ sono soluzioni di $(\bullet)$.

Tenuto conto [come facilmente si verifica] che la soluzione (x,y) di un sistema (a valori in $\boldsymbol{C}$) del tipo $\begin{cases} X+Y = \alpha \\ XY = \beta \end{cases}$ è formata dai due zeri x, y del polinomio $X^2 - \alpha X + \beta \in \boldsymbol{C}[X]$, segue che:

$$(u,v) \text{ è soluzione di } (\bullet\bullet) \iff u^3,\ v^3 \text{ sono i due zeri del polinomio } X^2 + qX - \tfrac{p^3}{27} \in \boldsymbol{C}[X].$$

Gli zeri di quest'ultimo polinomio sono:

$$\gamma_1 = -\tfrac{q}{2} + \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}}, \quad \gamma_2 = -\tfrac{q}{2} - \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}}.$$

Indicata con $\alpha_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ una delle tre radici terze di γ_1, le tre radici terze di γ_1 sono

$$\alpha_1, \quad \alpha_1\zeta_3, \quad \alpha_1\zeta_3^2,$$

con

$$\zeta_3 = \cos\tfrac{2\pi}{3} + i\sin\tfrac{2\pi}{3} = \tfrac{1}{2}(-1+i\sqrt{3}), \quad \zeta_3^2 = \cos\tfrac{4\pi}{3} + i\sin\tfrac{4\pi}{3} = \tfrac{1}{2}(-1-i\sqrt{3})$$

[radici primitive terze dell'unità]. Analogamente, posto $\alpha_2 = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$, le tre radici terze di γ_2 sono

$$\alpha_2, \quad \alpha_2\zeta_3, \quad \alpha_2\zeta_3^2.$$

Mentre $(\bullet\bullet)$ ha le nove soluzioni $(\alpha_1\zeta_3^{\,i}, \alpha_2\zeta_3^{\,j})$ [con $0 \le i, j \le 2$], le soluzioni di $(\bullet)$ [dovendo verificare la condizione $uv = -\frac{p}{3}$] sono esattamente tre:

$$(\alpha_1, \alpha_2), \quad (\alpha_1\zeta_3, \alpha_2\zeta_3^2), \quad (\alpha_1\zeta_3^2, \alpha_2\zeta_3).$$

Abbiamo così ottenuto le seguenti *formule di Cardano*, cioè le espressioni dei tre zeri (complessi) del polinomio $P = X^3 + pX + q \in \boldsymbol{C}[X]$:

$$\alpha_1 + \alpha_2 = \sqrt[3]{-\tfrac{q}{2} + \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}}} + \sqrt[3]{-\tfrac{q}{2} - \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}}};$$

$$\alpha_1\zeta_3 + \alpha_2\zeta_3^2 = \tfrac{1}{2}(-1+i\sqrt{3})\sqrt[3]{-\tfrac{q}{2} + \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}}} + \tfrac{1}{2}(-1-i\sqrt{3})\sqrt[3]{-\tfrac{q}{2} - \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}}};$$

$$\alpha_1\zeta_3^2 + \alpha_2\zeta_3 = \tfrac{1}{2}(-1-i\sqrt{3})\sqrt[3]{-\tfrac{q}{2} + \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}}} + \tfrac{1}{2}(-1+i\sqrt{3})\sqrt[3]{-\tfrac{q}{2} - \sqrt{\tfrac{q^2}{4} + \tfrac{p^3}{27}}}.$$

Nota. Tali formule, così come la loro dimostrazione, non sono quelle di Cardano, ma sono una loro rielaborazione, dovuta essenzialmente ad Eulero, circa 200 anni dopo. In effetti, ai tempi di Cardano, i numeri complessi non erano ancora noti!

(B) *Le formule di Cardano in $\boldsymbol{R}[X]$*

Assumiamo che un generico polinomio monico di grado 3 in $\boldsymbol{R}[X]$ si trasformi nel polinomio incompleto

$$P = X^3 + pX + q \in \boldsymbol{R}[X].$$

È noto che delle tre radici complesse, date dalle precedenti formule di Cardano, almeno una è reale [in quanto ogni polinomio di grado dispari in $\boldsymbol{R}[X]$ ha almeno uno zero reale]. Vale inoltre il seguente semplice risultato, che lasciamo come esercizio:

($*$) se $z, w \in \boldsymbol{C}$ e $zw,\ z+w \in \boldsymbol{R}$, allora $\overline{z} = w$ [e quindi $\overline{w} = z$]

[si ponga $z = a+ib$, $w = c+id$ e si proceda alla verifica].

Chiameremo *discriminante di* P il numero reale

$$\Delta = -(27\,q^2 + 4\,p^3)$$

[si noti che ha segno opposto al segno del radicando di γ_1 e γ_2]. Pertanto:

(*i*) Se $\Delta < 0$, $\alpha_1 + \alpha_2$ è un numero reale. Inoltre, dalle formule di Cardano si rileva subito che gli altri due zeri $\alpha_1\zeta_3 + \alpha_2\zeta_3^2$ e $\alpha_1\zeta_3^2 + \alpha_2\zeta_3$ sono coniugati tra loro e dunque non sono reali. Si conclude che P ha un solo zero reale e due zeri complessi coniugati.

(*ii*) Se $\Delta = 0$, dalle formule di Cardano segue che

$$\begin{aligned} \alpha_1 + \alpha_2 &= 2\sqrt[3]{-\tfrac{q}{2}}\,; \\ \alpha_1\zeta_3 + \alpha_2\zeta_3^2 &= \sqrt[3]{-\tfrac{q}{2}}\,(\zeta_3 + \zeta_3^2) = -\sqrt[3]{-\tfrac{q}{2}}\,; \\ \alpha_1\zeta_3^2 + \alpha_2\zeta_3 &= \sqrt[3]{-\tfrac{q}{2}}\,(\zeta_3^2 + \zeta_3) = -\sqrt[3]{-\tfrac{q}{2}}\,. \end{aligned}$$

In tal caso si hanno tre radici reali, di cui due coincidenti.

(*iii*) Se $\Delta > 0$ [noto come *"casus irriducibilis"*], le tre radici $\alpha_1 + \alpha_2$, $\alpha_1\zeta_3 + \alpha_2\zeta_3^2$, $\alpha_1\zeta_3^2 + \alpha_2\zeta_3$ sono apparenti numeri complessi [in quanto sono rappresentate con un radicando negativo]. Ma almeno una di esse è un numero reale. Se ad esempio $\alpha_1 + \alpha_2 \in \boldsymbol{R}$, allora [essendo $\alpha_1\alpha_2 = -\frac{p}{3} \in \boldsymbol{R}$], da $(*)$ segue che $\overline{\alpha_1} = \alpha_2$ e quindi

$$\overline{\alpha_1\zeta_3 + \alpha_2\zeta_3^2} = \overline{\alpha_1}\,\overline{\zeta_3} + \overline{\alpha_2}\,\overline{\zeta_3^2} = \alpha_2\zeta_3^2 + \alpha_1\zeta_3, \text{ cioè } \alpha_1\zeta_3 + \alpha_2\zeta_3^2 \in \boldsymbol{R}.$$

Analogamente si verifica che anche $\alpha_1\zeta_3^2 + \alpha_2\zeta_3 \in \boldsymbol{R}$. Dunque i tre "apparenti" zeri complessi sono in realtà numeri reali. Si può poi facilmente verificare che i tre zeri sono a due a due distinti.

Si noti che le formule di Cardano sono in questo caso di poca utilità, in quanto forniscono la rappresentazione dei tre zeri reali in forma "apparente" complessa. Né c'è modo [come dimostrato da R. Bombelli nel 1572] di trovarne un'espressione "per radicali" non complessa.

(*C*) ***La formula di Ferrari*** (cenno)

È assegnato un polinomio incompleto di grado 4

$$P = X^4 + pX^2 + qX + r \in \boldsymbol{C}[X].$$

Se $q = 0$, il polinomio è "biquadratico" e dunque è facilmente risolubile. Assumiamo dunque $q \neq 0$. Si può dimostrare, utilizzando il seguente *polinomio risolvente cubico di Lagrange* ad esso associato

$$L = X^3 + 2pX^2 + (p^2 - 4r)X - q^2 \in \boldsymbol{C}[X],$$

che è possibile fattorizzare P nel prodotto di due polinomi monici di grado 2, che è poi facile risolvere. Precisamente, detto α uno zero del risolvente cubico L [che si può ottenere con le formule di Cardano] e posto $\beta = \sqrt{\alpha}$, risulta che

$$P = \big(X^2 + \beta X + \tfrac{p+\alpha}{2} - \tfrac{q}{2\beta}\big)\big(X^2 - \beta X + \tfrac{p+\alpha}{2} + \tfrac{q}{2\beta}\big).$$

Determinando gli zeri di questi polinomi di grado 2 in $\boldsymbol{C}[X]$, si ottengono le *formule di Ferrari*, che rappresentano i quattro zeri complessi di P.

Capitolo IV

GRUPPI

1. Sottogruppi di un gruppo

Per la definizione di gruppo e le prime proprietà facciamo riferimento a **Cap. I.4**. Per indicare un gruppo utilizzeremo nel seguito la notazione moltiplicativa. È noto che in un gruppo $G = (G, \cdot)$:

- è unico l'elemento neutro $1 = 1_G$;
- è unico l'inverso g^{-1} di ogni $g \in G$;
- valgono le leggi di cancellazione a destra e a sinistra:

$$g\,g_1 = g\,g_2 \implies g_1 = g_2; \quad g_1\,g = g_2\,g \implies g_1 = g_2;$$

- se, $\forall\, g_1,\, g_2 \in G,\ g_1\,g_2 = g_2\,g_1,\ G$ è un gruppo *abeliano* (o *commutativo*).

È noto che un omomorfismo di gruppi $\varphi : (G, \cdot) \to (G', \bullet)$ è un'applicazione verificante le condizioni:

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \bullet \varphi(g_2), \quad \forall\, g_1,\, g_2 \in G.$$

Si verifica facilmente che

$$\varphi(1_G) = 1_{G'}; \quad \varphi(g^{-1}) = \varphi(g)^{-1}, \quad \forall\, g \in G.$$

Definizione 1. *Si chiama ordine del gruppo $(G, \cdot)$ la cardinalità $|G|$ di G.*

Definizione 2. *Un omomorfismo biiettivo è detto isomorfismo; un omomorfismo iniettivo è detto monomorfismo; un omomorfismo suriettivo è detto epimorfismo. Un omomorfismo di $(G, \cdot)$ in sé* è detto *endomorfismo* ed un endomorfismo biiettivo è detto *automorfismo*. Scriveremo $G \cong G'$ per indicare che esiste un isomorfismo tra i gruppi G e G'.

Osservazione 1. (*i*) Sia $g_0 \in G$ un fissato elemento. L'applicazione

$$g_0\,\_ : G \to G \ \text{ tale che } \ x \to g_0\,x, \quad \forall\, x \in G,$$

è biiettiva [ha infatti inversa $g_0^{-1}\,\_$] ma non è in generale un endomorfismo di G [infatti si ha: $g_0\,\_(xy) = g_0\,xy$, mentre $g_0\,\_(x) \cdot g_0\,\_(y) = g_0\,x\,g_0\,y$].

(*ii*) Sia $g_0 \in G$ un fissato elemento. L'applicazione

$$\gamma := \gamma_{g_0} : G \to G \ \text{ tale che } \ \gamma(x) = g_0\,x\,g_0^{-1}, \quad \forall\, x \in G,$$

è un automorfismo di G, detto *automorfismo interno di G (associato a g_0)*. Infatti si ha:

$$\gamma(xy) = g_0\,xy\,g_0^{-1} = g_0\,x\,(g_0^{-1}g_0)\,y\,g_0^{-1} = (g_0\,x\,g_0^{-1})(g_0\,y\,g_0^{-1}) = \gamma(x)\,\gamma(y);$$

$$\big(\gamma_{g_0^{-1}} \circ \gamma_{g_0}\big)(x) = \gamma_{g_0^{-1}}\big(g_0\,x\,g_0^{-1}\big) = g_0^{-1}\big(g_0\,x\,g_0^{-1}\big)\,(g_0^{-1})^{-1} = (g_0^{-1}g_0)\,x\,(g_0^{-1}g_0) = x = \mathbf{1}_G(x).$$

Quindi $\gamma_{g_0^{-1}} \circ \gamma_{g_0} = \mathbf{1}_G$ [identità di G]. Analogamente si verifica che $\gamma_{g_0} \circ \gamma_{g_0^{-1}} = \mathbf{1}_G$.

Ne segue che γ_{g_0} è biiettiva (con inversa $\gamma_{g_0^{-1}}$).

(*iii*) Se $\varphi : (G, \cdot) \to (G', \bullet)$ e $\psi : (G', \bullet) \to (G'', *)$ sono omomorfismi, anche $\psi \circ \varphi : (G, \cdot) \to (G'', *)$ è un omomorfismo. Infatti

$$(\psi\circ\varphi)(g_1\cdot g_2)=\psi\big(\varphi(g_1)\bullet\varphi(g_2)\big)=\psi\big(\varphi(g_1)\big)*\psi\big(\varphi(g_2)\big)=(\psi\circ\varphi)(g_1)*(\psi\circ\varphi)(g_2).$$

Veniamo ora ai sottogruppi, ricordandone per prima cosa la definizione.

Definizione 3. *Sia $(G,\cdot)$ un gruppo e sia H un sottoinsieme non vuoto di G. H è un sottogruppo di G (e si scrive $H\leq G$) se $(H,\cdot)$ è un gruppo (rispetto alla stesssa operazione $\cdot$ di G, ristretta ad $H\times H$). Ovviamente G e $\{1\}$ sono sottogruppi di G, detti sottogruppi banali di G. Se infine $H\subset G$, si può scrivere $H<G$ in luogo di $H\leq G$.*

Osservazione 2. Sia $H\subseteq G$, $H\neq\emptyset$. Risulta:

$$H\leq G\iff\begin{cases}H\cdot H\subseteq H\\ 1_G\in H\\ H^{-1}\subseteq H.\end{cases}$$

Verifichiamo tale affermazione.

($\Longrightarrow$). Poiché la restrizione $\cdot\big|_{H\times H}$ è un'operazione su H verificante i tre assiomi della definizione di gruppo, si ha: $H\cdot H\subseteq H$ [ovvio]; $1_H=1_G$ [infatti, $\forall\, h\in H$: $h=1_H\cdot h=1_G\cdot h\implies 1_H=1_G$]; $H^{-1}\subseteq H$ [infatti, se h' è l'inverso di h in H, allora $hh'=1_G=hh^{-1}\implies h'=h^{-1}$. Dunque $h^{-1}\in H$].

($\Longleftarrow$). Da $H\cdot H\subseteq H$ segue che $\cdot\big|_{H\times H}$ è un'operazione su H. Tale operazione è associativa (perché lo è $\cdot$); 1_G è elemento neutro in H e, $\forall\, h\in H$, $h^{-1}\in H$ è l'inverso di h in H.

Le tre precedenti condizioni, che assicurano che un sottoinsieme è un sottogruppo, possono essere "compattate" in un'unica condizione.

Proposizione 1. *Sia $H\subseteq G$, $H\neq\emptyset$. Risulta: $H\leq G\iff H\cdot H^{-1}\subseteq H$.*

Dim. ($\Longrightarrow$). Segue dall'osservazione precedente: poiché $H^{-1}\subseteq H$, allora $H\cdot H^{-1}\subseteq H\cdot H\subseteq H$.

($\Longleftarrow$). Essendo $H\neq\emptyset$, esiste un elemento $h\in H$. Allora $1_G=h\,h^{-1}\in H\cdot H^{-1}\subseteq H$. Dunque $1_G\in H$. Inoltre, $\forall\, h\in H$: $1h^{-1}\in H\cdot H^{-1}\subseteq H$ e dunque $h^{-1}\in H$. Pertanto $H^{-1}\subseteq H$. Infine, $\forall\, h,k\in H$: $k^{-1}\in H^{-1}\subseteq H$ e dunque $hk=h(k^{-1})^{-1}\in H\cdot H^{-1}\subseteq H$, da cui $H\cdot H\subseteq H$. Si è così verificato che $H\leq G$.

Osservazione 3. (*i*) Vediamo ora come si scrivono le equivalenze di **Osserv. 2** e di **Prop. 1**, in notazione additiva. Sia $(G,+)$ un gruppo e sia $H\subseteq G$, $H\neq\emptyset$. Risulta:

$$H\leq G\iff\begin{cases}H+H\subseteq H\\ 0_G\in H\\ -H\subseteq H\end{cases}\iff H-H\subseteq H.$$

(*ii*) Risulta: se $H\leq G$ e $K\leq H$, allora $K\leq G$ [cioè *"un sottogruppo di un sottogruppo di un gruppo è un sottogruppo del gruppo"*]. Inoltre, se $H,K\leq G$ e $K\subseteq H$, allora $K\leq H$. Le verifiche sono immediate.

Esempi 1. (*i*) Assegnato $(\boldsymbol{Z},+)$, tutti i sottoinsiemi $n\boldsymbol{Z}$ [$:=\{nx,\ \forall\, x\in\boldsymbol{Z}\}$] sono sottogruppi di $\boldsymbol{Z}$, $\forall\, n\in\boldsymbol{Z}$. Infatti: $n\boldsymbol{Z}-n\boldsymbol{Z}=\{nx-ny,\ \forall\, x,y\in\boldsymbol{Z}\}\subseteq n\boldsymbol{Z}$. Si noti che $0\boldsymbol{Z}=\{0\}$, $1\boldsymbol{Z}=\boldsymbol{Z}=(-1)\boldsymbol{Z}$ e che $n\boldsymbol{Z}=(-n)\boldsymbol{Z}$, $\forall\, n\in\boldsymbol{Z}$. Infine, $n\boldsymbol{Z}\leq m\boldsymbol{Z}\iff m\,\big|\,n$.

(*ii*) Assegnato il gruppo $\big(\mathbf{GL}_2(\boldsymbol{R}),\cdot\big)$ (cfr. **Cap. I.4 Esempio 2**), i due seguenti sottoinsiemi:

$$H_1=\Big\{\begin{pmatrix}1&k\\0&1\end{pmatrix},\ \forall\, k\in\boldsymbol{Z}\Big\},\quad H_2=\big\{A\in\mathfrak{M}_2(\boldsymbol{Z})\ :\ det(A)=1\big\}$$

sono sottogruppi di $\mathbf{GL}_2(\boldsymbol{R})$. Infatti:

(1) $\forall\, h,k \in \boldsymbol{Z}$: $\begin{pmatrix}1 & h\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}^{-1} = \begin{pmatrix}1 & h\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & -k\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & h-k\\ 0 & 1\end{pmatrix} \in H_1$.

(2) È noto che, $\forall\, A, B \in \mathfrak{M}_2(\boldsymbol{R})$, risulta $det(AB) = det(A)det(B)$. Inoltre, $\forall\, A \in \mathbf{GL}_2(\boldsymbol{R})$, risulta $det(A^{-1}) = \frac{1}{det(A)}$. Infine, se $A = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathfrak{M}_2(\boldsymbol{Z})$ e $det(A) = 1$, allora $A^{-1} = \begin{pmatrix}d & -b\\ -c & a\end{pmatrix} \in \mathfrak{M}_2(\boldsymbol{Z})$. Quindi, $\forall\, A, B \in H_2$, risulta

$$AB^{-1} \in \mathfrak{M}_2(\boldsymbol{Z}) \text{ e } det(A\,B^{-1}) = det(A)\,\tfrac{1}{det(B)} = 1\cdot\tfrac{1}{1} = 1.$$

Dunque $AB^{-1} \in H_2$ e pertanto $H_2 \leq \mathbf{GL}_2(\boldsymbol{R})$.

Si noti infine che $H_1 \subset H_2$ e dunque $H_1 < H_2$ Il gruppo H_2 viene usualmente denotato $\mathbf{SL}_2(\boldsymbol{Z})$, detto *gruppo speciale lineare di ordine* 2 *su* $\boldsymbol{Z}$.

Osservazione 4. Se $H, K \leq G$, anche $H \cap K \leq G$ (semplice verifica). Più generalmente, se $\{H_i\}_{i\in I}$ è una famiglia non vuota di sottogruppi di G, anche $\bigcap_{i\in I} H_i \leq G$.

Invece non è detto che l'insieme $H \cup K$ sia un sottogruppo di G (se H, K lo sono). Infatti, se $h \in H - K$ e $k \in K - H$, non è detto che $hk \in H \cup K$. Considerato ad esempio il gruppo $(\boldsymbol{Z}, +)$, $2\boldsymbol{Z} \cup 3\boldsymbol{Z}$ non è un sottogruppo di $(\boldsymbol{Z}, +)$ [infatti $2 + 3 \notin 2\boldsymbol{Z} \cup 3\boldsymbol{Z}$, mentre $2, 3 \in 2\boldsymbol{Z} \cup 3\boldsymbol{Z}$].

Definizione 4. *Sia G un gruppo e sia S un suo sottoinsieme non vuoto. Si chiama sottogruppo generato da S il sottogruppo*

$$\langle\, S\,\rangle := \bigcap_{H\leq G, H\supseteq S} H$$

*[cioè l'intersezione dei sottogruppi di G contenenti S. Poiché almeno G verifica le due condizioni "$H \leq G$, $H \supseteq S$", allora $\langle\, S\,\rangle$ è ben definito, ed è un sottogruppo (per l'***Osserv. 4***)]. Si tratta quindi del più piccolo sottogruppo di G contenente S.*

Vogliamo descrivere gli elementi di $\langle\, S\,\rangle$. Serve la seguente definizione.

Definizione 5. *Sia $(G, \cdot)$ un gruppo e sia $g \in G$. Per ogni $t \in \boldsymbol{Z}$, si definisce potenza t-sima di g l'elemento*

$$g^t := \begin{cases} 1, & \text{se } t = 0,\\ g \cdot\ldots\cdot g \ \ [t \text{ volte}], & \text{se } t > 0\\ g^{-1}\cdot\ldots\cdot g^{-1} \ \ [-t \text{ volte}], & \text{se } t < 0.\end{cases}$$

Si verifica facilmente che $g^{t+s} = g^t g^s$, $\forall\, t, s \in \boldsymbol{Z}$, e che $g^{-t} = (g^{-1})^t = (g^t)^{-1}$, $\forall\, t \in \boldsymbol{Z}$.

Analogamente, in $(G, +)$, si definisce multiplo t-simo di g l'elemento

$$tg := \begin{cases} 0, & \text{se } t = 0,\\ g + \ldots\ldots + g \ \ [t \text{ volte}], & \text{se } t > 0,\\ (-g) + \ldots\ldots + (-g) \ \ [-t \text{ volte}], & \text{se } t < 0.\end{cases}$$

Ovviamente $(t + s)g = tg + sg$, $\forall\, t, s \in \boldsymbol{Z}$, e $(-t)g = t(-g) = -(tg)$, $\forall\, t \in \boldsymbol{Z}$.

Proposizione 2. *Sia $(G, \cdot)$ un gruppo e sia $S = \{g\} \subseteq G$. Risulta:*

$$\langle\{g\}\rangle = \{g^t,\ \forall\, t \in \boldsymbol{Z}\}.$$

Nota. Per semplificare le notazioni si scriverà $\langle\, g\,\rangle$ al posto di $\langle\{g\}\rangle$.

Dim. Per definizione, $\langle\, g\,\rangle = \bigcap_{H\leq G, g\in H} H$. Si ponga $H_0 := \{g^t,\ \forall\, t \in \boldsymbol{Z}\}$. Basterà verificare che:

$(*)$ $H_0 \leq G$; $(**)$ se $H \leq G$ e $g \in H$, allora $H_0 \subseteq H$.

Per verificare $(*)$ basta dimostrare che $H_0 \cdot H_0^{-1} \subseteq H_0$. Infatti, $\forall\, t, s \in \boldsymbol{Z}$: $g^t (g^s)^{-1} = g^{t-s} \in H_0$.

Per verificare $(**)$ basta osservare che, essendo $g \in H$ e $H \leq G$, allora $g^t \in H$, $\forall\, t \in \boldsymbol{Z}$. Dunque $H_0 \subseteq H$.

Definizione 5. *Un sottogruppo H di G è detto ciclico se risulta $H = \langle h \rangle$, $\exists\, h \in H$. L'elemento h è detto generatore di H.*

Esempi 2. Diamo due esempi di sottogruppi ciclici.

(i) In $(\boldsymbol{Z}, +)$, il sottogruppo $n\boldsymbol{Z}$ è un sottogruppo ciclico, $\forall\, n \in \boldsymbol{Z}$ [infatti $n\boldsymbol{Z} = \{nt,\ \forall\, t \in \boldsymbol{Z}\} = \langle n \rangle$]. Si può facilmente verificare che $(\boldsymbol{Z}, +)$ ammette soltanto sottogruppi ciclici (cfr. la successiva **Prop. 2.2**).

(ii) In $\big(\mathbf{GL}_2(\boldsymbol{R}), \cdot\big)$ il sottogruppo H_1 definito in **Esempi 1**(ii) è ciclico. Infatti si ha:

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^t,\ \forall\, t \in \boldsymbol{Z} \right\} = \left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix},\ \forall\, t \in \boldsymbol{Z} \right\} = H_1.$$

Proposizione 3. *Sia $(G, \cdot)$ un gruppo e sia S un sottoinsieme non vuoto di G. Posto $S^{-1} = \{s^{-1},\ \forall\, s \in S\}$, risulta:*

$$\langle S \rangle = \{ \prod_{i=1}^{r} s_i,\ \forall\, r \geq 1,\ \ \forall\, s_i \in S \cup S^{-1} \}.$$

Dim. Si ponga $H_0 = \{ \prod_{i=1}^{r} s_i,\ \forall\, r \geq 1,\ \ \forall\, s_i \in S \cup S^{-1} \}$. Si tratta di verificare che

$(*)$ $H_0 \leq G$; $\qquad$ $(**)$ se $H \leq G$ e $S \subseteq H$, allora $H_0 \subseteq H$.

La $(**)$ è ovvia. Verifichiamo la $(*)$. Si ha infatti:

$\forall \prod_{i=1}^{r} s_i\,,\ \prod_{j=1}^{s} t_j \in H_0$, risulta: $\prod_{i=1}^{r} s_i \prod_{j=1}^{s} t_j = s_1 \dots s_r t_1 \dots t_s \in H_0$;

$1_G = s\, s^{-1} \in H_0$;

$\forall \prod_{i=1}^{r} s_i \in H_0$, risulta: $\big(\prod_{i=1}^{r} s_i\big)^{-1} = s_r^{-1} \dots s_2^{-1} s_1^{-1} \in H_0$.

Osservazione 5. Se gli elementi di $S \cup S^{-1}$ commutano tra loro, allora

$$\langle S \rangle = \big\{ s_1^{t_1} \dots s_n^{t_n},\ \forall\, s_1, \dots, s_n \in S \text{ [a due a due distinti]},\ \forall\, t_1, \dots, t_n \in \boldsymbol{Z} \big\}.$$

Infatti, $\forall\, x \in \langle S \rangle$, i fattori di x possono essere commutati in modo da avvicinare i fattori uguali. Dunque $x = s_1^{t_1} \dots s_n^{t_n}$.

Se invece gli elementi di S non commutano, la determinazione di $\langle S \rangle$ è più complicata, come verificheremo nel successivo esempio.

Esempi 3. (i) In $\big(\mathbf{GL}_2(\boldsymbol{R}), \cdot\big)$, sia $S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\}$. Risulta:

$$\langle S \rangle = \left\{ \begin{pmatrix} 2^t & 0 \\ 0 & 2^s \end{pmatrix},\ \forall\, t, s \in \boldsymbol{Z} \right\}$$

[si noti infatti che i due generatori commutano].

(ii) Sempre in $\big(\mathbf{GL}_2(\boldsymbol{R}), \cdot\big)$, sia $S = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}$. Si noti che le due matrici $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ di S non commutano tra loro (cioè $AB \neq BA$). Il sottogruppo $\langle S \rangle$ è formato da elementi del tipo:

$$C = A^{h_1} B^{k_1} A^{h_2} B^{k_2} \dots A^{h_r} B^{k_r},\ \text{ con } h_i, k_j \in \boldsymbol{Z}.$$

Si noti che, poiché $det(A) = det(B) = 1$, allora $det(C) = 1$, $\forall\, C \in \langle S \rangle$. Dunque $\langle S \rangle \leq \mathbf{SL}_2(\boldsymbol{Z})$. Si osservi infine che, stante l'insoddisfacente rappresentazione degli elementi di S, non possiamo

facilmente stabilire se $\langle S \rangle$ sia o meno un sottogruppo proprio di $\mathbf{SL}_2(\boldsymbol{Z})$.

Osservazione 6. Un sottogruppo ciclico $\langle g \rangle$ di G è evidentemente abeliano [infatti $g^t \cdot g^s = g^{t+s} = g^{s+t} = g^s \cdot g^t$] ed è al più numerabile [infatti $|\{g^t,\ \forall t \in \boldsymbol{Z}\}| \leq |\boldsymbol{Z}|$]. Sono quindi esempi di sottogruppi non ciclici tutti i sottogruppi non abeliani di un gruppo (necessariamente non abeliano) e tutti i sottogruppi (anche abeliani) di cardinalità superiore al numerabile. Ad esempio, è non ciclico il sottogruppo $\mathbf{SL}_2(\boldsymbol{Z})$ di $\mathbf{GL}_2(\boldsymbol{R})$ [non abeliano, cfr. **Esempi 3**(*ii*)].

Un esempio di sottogruppo abeliano, numerabile e non ciclico è il seguente. Sia H l'insieme delle matrici diagonali a valori razionali in $\mathbf{GL}_2(\boldsymbol{R})$:

$$H = \Big\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix},\ \forall a, b \in \boldsymbol{Q},\ ab \neq 0 \Big\}$$

Si verifica facilmente che $H < \mathbf{GL}_2(\boldsymbol{R})$ [infatti $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} \frac{a}{c} & 0 \\ 0 & \frac{b}{d} \end{pmatrix} \in H$], che H è commutativo e che è numerabile. Ma H non è ciclico. Se infatti, per assurdo, $A = \begin{pmatrix} q_1 & 0 \\ 0 & q_2 \end{pmatrix}$ fosse un generatore di H, con $q_1 = \frac{r}{s}$, allora $A^t = \begin{pmatrix} \frac{r^t}{s^t} & 0 \\ 0 & q_2^{\,t} \end{pmatrix},\ \forall t \in \boldsymbol{Z}$. Scelto allora $q \in \boldsymbol{Q}^{\cdot}$, con $q \neq \frac{r^t}{s^t},\ \forall t \in \boldsymbol{Z}$, risulterebbe $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix} \in H - \langle A \rangle$.

Nota. Un altro (e più semplice) esempio è dato dal sottogruppo $(\boldsymbol{Q}, +)$ di $(\boldsymbol{R}, +)$ [verificare]. Vari altri esempi di sottogruppi finiti non ciclici (ed abeliani) saranno visti nei paragrafi successivi.

Definizione 6. *Siano H, K sottogruppi di $(G, \cdot)$. Si chiama prodotto di H e K l'insieme*

$$HK = \big\{hk,\ \forall h \in H,\ \forall k \in K\big\}.$$

Scrivendo $HK = KH$, si intende che sono verificate le due condizioni:

$$\begin{cases} \forall hk \in HK,\ \exists h_1 \in H,\ \exists k_1 \in K \ \text{ tali che } \ hk = k_1 h_1, \\ \forall kh \in KH,\ \exists h_2 \in H,\ \exists k_2 \in K \ \text{ tali che } \ kh = h_2 k_2 \end{cases}$$

[cioè che H, K commutano "globalmente" (ma non necessariamente "elemento per elemento")]. Si dice in tal caso che H, K sono sottogruppi permutabili.

Proposizione 4. Siano H, K sottogruppi di $(G, \cdot)$. Risulta:

(*i*) Se $(G, \cdot)$ è commutativo, HK è un sottogruppo di G.

(*ii*) HK è un sottogruppo di $G \iff HK = KH$.

(*iii*) Se HK è un sottogruppo di G, allora $HK = \langle H \cup K \rangle$.

Dim. (*i*) Risulta:

- $1 = 1 \cdot 1 \in HK$;
- $\forall hk,\ h_1 k_1 \in HK$: $hk(h_1 k_1) = h(kh_1)k_1 = h(h_1 k)k_1 = (hh_1)(kk_1) \in HK$;
- $\forall hk \in HK$: $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1} \in HK$.

(*ii*) ($\Longrightarrow$). Verifichiamo che $HK \subseteq KH$. Sia $hk \in HK$. Allora (essendo HK un gruppo): $(hk)^{-1} = k^{-1}h^{-1} \in HK$. Dunque $k^{-1}h^{-1} = h_1 k_1 \in HK$. Allora $hk = \big((hk)^{-1}\big)^{-1} = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} \in KH$. Verifichiamo ora che $KH \subseteq HK$. Sia $kh \in KH$: poiché $h^{-1}k^{-1} \in HK$, allora $kh = (h^{-1}k^{-1})^{-1} \in HK$.

($\Longleftarrow$). Bisogna verificare che $\forall hk,\ h_1 k_1 \in HK$, risulta: $(hk)(h_1 k_1)^{-1} \in HK$. Infatti:

$$(hk)(h_1 k_1)^{-1} = hkk_1^{-1}h_1^{-1} = h(kk_1^{-1})h_1^{-1} = hk_2 h_1^{-1} = h(k_2 h_1^{-1}) = h(h_2 k_3) = (hh_2)k_3 \in HK.$$

(*iii*) Certo $H, K \subset HK$ [infatti $h = h\,1 \in HK,\ \forall h \in H$ e $k = 1\,k \in HK,\ \forall k \in K$]. Ne segue che $H \cup K \subset HK$ e quindi $\langle H \cup K \rangle \leq HK$, essendo $HK \leq G$.

Se poi $L \leq G$ e $L \supseteq H \cup K$, allora $L \supseteq H$, $L \supseteq K$ e dunque $L \supseteq HK$. Si conclude quindi che

$\langle H \cup K \rangle = HK$.

Concludiamo il paragrafo con un semplice esercizio.

Esercizio 1. Sia $(G, \cdot)$ un gruppo abeliano e sia $n \geq 1$.
(i) Verificare che l'insieme $G^n = \{g^n,\ \forall\, g \in G\}$ è un sottogruppo di G.
(ii) Verificare che l'applicazione

$$\varphi_n : G \to G \ \text{ tale che } \ \varphi_n(g) = g^n, \ \ \forall\, g \in G,$$

è un omomorfismo di G in sé, avente per immagine G^n.

Soluzione. (i) Risulta:

(a) $1 \in G^n$. Infatti $1 = \overbrace{1 \,.....\, 1}^{n \text{ volte}} \in G^n$.

(b) $\forall\, g^n \in G^n$: $(g^n)^{-1} = (g \,....\, g)^{-1} = g^{-1} .... \, g^{-1} = (g^{-1})^n \in G^n$.

(c) $\forall\, g^n,\, h^n \in G^n$: $g^n h^n = \overbrace{g \,.....\, g}^{n}\, \overbrace{h \,.....\, h}^{n} = gh \overbrace{g \,.....\, g}^{n-1}\, \overbrace{h \,.....\, h}^{n-1} = \ .... \ = \overbrace{gh \,.....\, gh}^{n} = (gh)^n$.

(ii) Risulta, $\forall\, g,\, h \in G$:

$$\varphi_n(gh) = (gh)^n = \overbrace{gh \,...\, gh}^{n} = g^n h^n = \varphi_n(g)\varphi_n(h).$$

Inoltre: $Im(\varphi_n) = \left\{g^n,\ \forall\, g \in G\right\} = G^n$.

Nota. Se G non è abeliano, G^n non è in generale un sottogruppo di G. Si può infatti verificare che ad esempio $\mathbf{SL}_2(\boldsymbol{Z})^2$ non è un sottogruppo di $\mathbf{SL}_2(\boldsymbol{Z})$. [Si scelgano in $\mathbf{SL}_2(\boldsymbol{Z})$ le due matrici A, B considerate nell'esercizio precedente e si verifichi che $\nexists\, C \in \mathbf{SL}_2(\boldsymbol{Z})$ tale che $A^2B^2 = C^2$].

2. Gruppi ciclici

Definizione 1. *Un gruppo* $(G,\cdot)$ *è detto ciclico se* $\exists\, g \in G$ *tale che* $G = \langle g \rangle$. *L'elemento* g *è detto generatore di* G. *Ovviamente un gruppo ciclico è abeliano [cfr.* **Osserv. 1.6***].*

Un esempio importante di gruppo ciclico è $(\boldsymbol{Z},+)$. Infatti [cfr. **Esempi 1.2**(i)] $\boldsymbol{Z} = \langle 1 \rangle$ $[= \langle -1 \rangle\,]$. Per esaminare la struttura dei gruppi ciclici è opportuno introdurre la nozione di *periodo di un elemento*.

Definizione 2. *Sia* $(G,\cdot)$ *un gruppo, con elemento neutro* $1 = 1_G$. *Per ogni* $g \in G$, *consideriamo le potenze positive di* g. *Si hanno due possibilità:*

$$\exists\, t > 0 \ \text{ tale che } \ g^t = 1, \ \text{ oppure } \ g^t \neq 1, \ \forall\, t > 0.$$

Si chiama periodo di g *(e si denota* $\circ(g)$*) il minimo intero* $t > 0$ *(se esiste) tale che* $g^t = 1$. *Se tale intero non esiste, si dice che* g *ha periodo infinito (e si scrive* $\circ(g) = \infty$*).*

Si noti che $\circ(g) = 1 \iff g = 1_G$. *In notazione additiva,* $\circ(g) = t$ *se* t *è il minimo intero positivo (se esiste) tale che* $tg = 0$; *altrimenti* $\circ(g) = \infty$.

Osservazione 1. Sia $\circ(g) = n$. Risulta, $\forall\, h \in \boldsymbol{Z}$: $g^h = 1 \iff n \,\big|\, h$.

Dimostriamo tale affermazione.

($\Longrightarrow$). Se $h = nq + r$, con $0 \leq r < n$, allora $1 = g^h = g^{nq} \cdot g^r = (1^q) g^r = g^r$ e quindi $g^r = 1$. Per la minimalità di n, si conclude che $r = 0$ e dunque $n \,\big|\, h$.

($\Longleftarrow$). Se $h = ns$, $g^h = (g^n)^s = (1^s) = 1$.

Proposizione 1. *Sia* G *un gruppo e sia* $g \in G$. *Si ha:*

(i) Se $\circ(g) = n$, $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ *e tali elementi sono a due a due distinti. Vale anche il viceversa.*

(ii) Se $\circ(g) = \infty$, $\big(\langle g \rangle, \cdot\big) \cong (\boldsymbol{Z},+)$.

Dim. (i) Si ha: $\langle g \rangle = \{g^t,\ \forall\, t \in \boldsymbol{Z}\}$. Se $t = nq + r$, con $0 \leq r < n$, allora

$$g^t = g^{nq+r} = (g^n)^q \cdot g^r = 1^q \cdot g^r = g^r.$$

Dunque $\langle g \rangle \subseteq \{1 = g^0, g, g^2, \ldots, g^{n-1}\}$. L'inclusione opposta è ovvia.

Verifichiamo che gli elementi $1, g, g^2, \ldots, g^{n-1}$ sono a due a due distinti. Sia infatti $g^h = g^k$, con $0 \leq h \leq k < n$. Allora $1 = g^k (g^h)^{-1} = g^k g^{-h} = g^{k-h}$. Dall'**Osserv. 1**, $n \,\big|\, k - h$; inoltre $0 \leq k - h < n$. Ne segue che $k - h = 0$, cioè $h = k$.

Verifichiamo che tale risultato si inverte. Se $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ (elementi a due a due distinti), allora $g^n = g^t$, $\exists\, t :\ 0 \leq t \leq n-1$. Dunque $g^{n-t} = 1$, con $1 \leq n - t \leq n$. Per ipotesi, $g, g^2, \ldots, g^{n-1} \neq 1$. Dunque $n - t = n$, cioè $t = 0$. Quindi $g^n = 1$ cioè $\circ(g) = n$.

(ii) Si consideri l'applicazione

$$\varphi : \boldsymbol{Z} \to \langle g \rangle \ \text{ tale che } \ \varphi(h) = g^h, \ \forall\, h \in \boldsymbol{Z}.$$

φ è ovviamente suriettiva. Inoltre è iniettiva: se $g^h = g^k$ (con $h \geq k$), allora $g^{h-k} = g^h (g^k)^{-1} = 1$. Essendo ora $\circ(g) = \infty$, allora $h - k = 0$, cioè $h = k$.

Resta da verificare che φ è un omomorfismo di gruppi. Infatti

$$\varphi(h+k) = g^{h+k} = g^h \cdot g^k = \varphi(h) \cdot \varphi(k).$$

Si conclude che $\varphi : \boldsymbol{Z} \to \langle g \rangle$ è un isomorfismo.

Osservazione 2. Sia $(G,\cdot)$ un gruppo ciclico, con $G = \langle g \rangle$. Dalla proposizione precedente segue:

- se $\circ(g) = \infty$, $(G,\cdot) \cong (\boldsymbol{Z},+)$;

- se $\circ(g) = n \in \boldsymbol{N}$, $|G| = n$ (e viceversa).

Vogliamo ora verificare che due gruppi ciclici dello stesso ordine n sono isomorfi. Siano infatti $G = \langle g \rangle$ e $H = \langle h \rangle$, con $\circ(g) = \circ(h) = n$; si osserva subito che l'applicazione

$$\varphi : G \to H \text{ tale che } \varphi(g^t) = h^t, \ \forall\, t = 0, 1, \dots, n-1,$$

è biiettiva. Inoltre si ha: $\varphi(g^m) = h^m$, $\forall\, m \in \boldsymbol{Z}$ [infatti, se $m = nq + r$, $0 \leq r < n$, allora $\varphi(g^m) = \varphi(g^r) = h^r = h^m$]. Quindi:

$$\varphi(g^r g^s) = \varphi(g^{r+s}) = h^{r+s} = \varphi(g^r)\varphi(g^s), \ \forall\, r, s \in \boldsymbol{Z},$$

cioè φ è un isomorfismo tra G ed H.

Scriveremo talvolta $G = \langle g \,|\, g^n = 1 \rangle$ per indicare che G è un gruppo ciclico finito di ordine n [ovvero che G è generato da un elemento di periodo n]. In notazione additiva un gruppo ciclico finito di ordine n può essere indicato nella forma $\langle g \,|\, ng = 0 \rangle$.

Per ogni $n \geq 2$, il gruppo $(\boldsymbol{Z}_n, +)$ costituisce un esempio di gruppo ciclico di ordine n (con notazione additiva). Infatti si ha: $\circ(\overline{1}) = n$ [essendo $n\,\overline{1} = \overline{1} + \ \dots\ + \overline{1} = \overline{n} = \overline{0}$, mentre $t\,\overline{1} = \overline{t} \neq \overline{0}$, $\forall\, t = 1, \dots, n-1$]. Ne segue che $\boldsymbol{Z}_n = \langle \overline{1} \rangle$.

Un altro esempio di gruppo ciclico di ordine n (con notazione moltiplicativa) è il *gruppo delle radici n-sime dell'unità*, che denoteremo $\boldsymbol{C}_n$ [invece di $\sqrt[n]{1}$, cfr. **Cap. I.5**]. È noto che

$$\boldsymbol{C}_n = \sqrt[n]{1} = \{ z \in \boldsymbol{C} \mid z^n = 1 \} = \{ \zeta_{n,k}, \ \forall\, k = 0, 1, \dots, n-1 \},$$

con $\zeta_{n,k} = \cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n}$. È altresì noto che, posto $\zeta_n := \zeta_{n,1} = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$, risulta $\zeta_{n,k} = \zeta_n^{\,k}$. Dunque

$$\boldsymbol{C}_n = \{ \zeta_n^{\,k}, \ \forall\, k = 0, 1, \dots, n-1 \}.$$

Tenuto conto di **Prop. 1**(i), segue che

$$\boldsymbol{C}_n = \langle \zeta_n \rangle$$

e che $\circ(\zeta_n) = n$ [infatti $\zeta_n^{\,n} = 1$, mentre $\zeta_n^{\,k} \neq 1$, $\forall\, k = 0, 1, \dots, n-1$]. Si noti inoltre che $\boldsymbol{C}_n$ è un sottogruppo del gruppo $(\boldsymbol{C}^{\cdot}, \cdot)$ [in quanto l'operazione è la stessa].

Infine si ha, $\forall\, n \geq 1$, $(\boldsymbol{Z}_n, +) \cong (\boldsymbol{C}_n, \cdot)$, tramite l'isomorfismo

$$\varphi : \boldsymbol{Z}_n \to \boldsymbol{C}_n \text{ tale che } \varphi(\overline{k}) = \zeta_n^{\,k}, \ \forall\, \overline{k} = \overline{0}, \overline{1}, \dots, \overline{n-1}.$$

Appurato che, a meno di isomorfismi, esiste un unico gruppo ciclico infinito e, $\forall\, n \geq 1$, un unico gruppo ciclico di ordine n, affronteremo ora due questioni relative ai gruppi ciclici:

(**A**) *Come sono fatti i sottogruppi di un gruppo ciclico?*

(**B**) *Quali e quanti sono i generatori di un gruppo ciclico?*

Per rispondere a tali questioni è utile il seguente lemma.

Lemma 1. *Sia $(G, \cdot)$ un gruppo e sia $g \in G$ un elemento di periodo finito, diciamo $\circ(g) = n$. Per ogni $t \in \boldsymbol{Z}$, risulta:*

$$\circ(g^t) = \tfrac{n}{(n,t)}.$$

Ne segue in particolare che in un gruppo ciclico finito di ordine n, ogni elemento ha come periodo un divisore di n.

Dim. Si ponga: $\circ(g^t) = m$, $(n, t) = d$, $n = dn_1$, $t = dt_1$. Ne segue che $(n_1, t_1) = 1$. Bisogna dimostrare che $m = \frac{n}{d}$ $(= n_1)$ e cioè:

$$(*) \ \ m \,|\, n_1 \quad \text{e} \quad (**) \ \ n_1 \,|\, m.$$

$(*)$: $(g^t)^{n_1} = (g^{dt_1})^{n_1} = (g^n)^{t_1} = 1^{t_1} = 1$. Dall'**Osserv. 1** segue che $m \,|\, n_1$.

$(**)$: $(g^t)^m = 1 = g^{tm}$. Dall'**Osserv. 1**, $n \,|\, tm$, cioè $dn_1 \,|\, dt_1 m$, da cui $n_1 \,|\, t_1 m$. Essendo $(n_1, t_1) = 1$, da *EU* segue che $n_1 \,|\, m$.

L'ultima affermazione è ovvia conseguenza della formula.

Affrontiamo ora la prima questione (problema (**A**)).

Proposizione 2. *Ogni sottogruppo di un gruppo ciclico è un gruppo ciclico.*

Dim. Sia $(G,\cdot)$ un gruppo ciclico generato dall'elemento g. Sia H un sottogruppo di G.

Se $H=\{1\}$, allora $H=\langle 1\rangle$ (è ciclico). Sia quindi $H\neq\{1\}$. Si osserva subito che $\exists\, s>0$ tale che $g^s\in H$ [se infatti $H\ni g^v$, con $v<0$, allora $H\ni (g^v)^{-1}=g^{-v}$, con $-v>0$]. Si ponga $t:=min\{s>0 \mid g^s\in H\}$. Vogliamo verificare che $H=\langle g^t\rangle$.

L'inclusione $\langle g^t\rangle\subseteq H$ è ovvia (in quanto $g^t\in H$). Viceversa, dimostriamo che $H\subseteq\langle g^t\rangle$.

Sia $g^m\in H$ e sia $m=tq+r$, $0\leq r<t$. Si ha: $g^r=g^{m-tq}=g^m\cdot(g^t)^{-q}\in H$. Se fosse $r>0$, allora $g^r\notin H$ (per la minimalità di t): dunque $r=0$ e pertanto $g^m=g^{tq}=(g^t)^q\in\langle g^t\rangle$. Dunque $H\subseteq\langle g^t\rangle$.

Nota. La dimostrazione vale (utilizzando la notazione additiva) anche per $(\boldsymbol{Z},+)$ ed invitiamo lo studente a riscriverla per questo caso. Dunque i sottogruppi di $(\boldsymbol{Z},+)$ sono tutti e soli del tipo $n\boldsymbol{Z}$, $\forall\, n\geq 0$, cfr. **Esempi 1.1**(i).

Proposizione 3. *Sia $G=\langle g \mid g^n=1\rangle$ un gruppo ciclico di ordine n. Risulta:*

(i) Per ogni sottogruppo H di G, $|H|\,\big|\,n$.

(ii) Per ogni divisore positivo k di n, $\exists!\, H\leq G$ tale che $|H|=k$.

Dim. (i). Sia $H\leq G$. In base a **Prop. 2**, H è ciclico. Dunque $H=\langle g^t\rangle$, $\exists\, t\geq 0$. In base a **Prop. 1**(i) e a **Lemma 1**, $|H|=\circ(g^t)=\frac{n}{(t,n)}$. Dunque $|H|\,\big|\,n$.

(ii) Sia k un divisore positivo di n. Risulta:

$$|\langle g^{n/k}\rangle|=\circ(g^{n/k})=\frac{n}{(n,n/k)}=\frac{n}{n/k}=k$$

e dunque $\langle g^{n/k}\rangle$ è un sottogruppo di G di ordine k.

Sia ora H un arbitrario sottogruppo di G di ordine k: bisogna verificare che $H=\langle g^{n/k}\rangle$. Dalla dimostrazione di **Prop. 2**, segue che $H=\langle g^m\rangle$, con $m:=$ *minimo esponente positivo tale che* $g^m\in H$. Si ha:

$$k=|H|=\circ(g^m)=\frac{n}{(n,m)}.$$

Se verifichiamo che $(n,m)=m$, allora $k=\frac{n}{m}$ e dunque $m=\frac{n}{k}$, cioè $H=\langle g^{n/k}\rangle$, come richiesto.

Sia $n=mq+r$, con $0\leq r<m$. Allora $1=g^n=g^{mq}\cdot g^r$ e dunque $g^r=(g^m)^{-q}\in H$. Per la minimalità di m, segue che $r=0$ e dunque $m\,\big|\,n$, cioè $(n,m)=m$.

Nota. La proprietà (ii) [cioè *esiste un solo sottogruppo per ogni divisore dell'ordine di* G] caratterizza i gruppi ciclici finiti. Vale infatti il seguente risultato [per il quale rinviamo al testo di A. Machì (cfr. bibliografia) oppure all'**Esercizio 4.19**]:

Se G è un gruppo finito che per ogni divisore positivo d di $|G|$ ammette al più un solo sottogruppo di ordine d, allora G è ciclico.

Osservazione 3. Sia $G=\langle g \mid g^n=1\rangle$ un gruppo ciclico di ordine n. Abbiamo appena dimostrato che i sottogruppi di G (tutti ciclici) sono in corrispondenza biunivoca con i divisori positivi di n. Precisamente, se $k\,\big|\,n$, $\langle g^{n/k}\rangle$ è l'unico sottogruppo di G di ordine k.

Si osservi poi che, se $h\,\big|\,k$ (e $k\,\big|\,n$), allora $\langle g^{n/h}\rangle$ è a sua volta sottogruppo di $\langle g^{n/k}\rangle$. Infatti $\langle g^{n/k}\rangle$ è ciclico di ordine k e h è un divisore di k: dunque $\langle (g^{n/k})^{k/h}\rangle=\langle g^{n/h}\rangle$ è un suo sottogruppo.

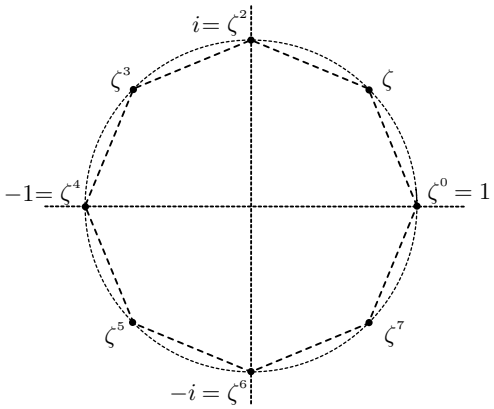
Si osservi infine che se $n=p_1^{r_1}\dots p_s^{r_s}$, il numero dei divisori positivi di n è dato da $(r_1+1)\dots(r_s+1)$ [infatti i divisori positivi di n sono tutti e soli del tipo $p_1^{h_1}\dots p_s^{h_s}$, con $0\leq h_i\leq r_i$, $\forall\, i=1,\dots,s$].

Tenuto conto di questi fatti, non è difficile determinare la totalità dei sottogruppi di G, con le relative relazioni di inclusione, cioè il *reticolo dei sottogruppi di* G.

Esempi 1. (*i*) Determiniamo il reticolo dei sottogruppi di $\boldsymbol{C}_8$.

Sia $\zeta = \zeta_8 = \cos\frac{2\pi}{8} + i\sin\frac{2\pi}{8} = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{1}{\sqrt{2}} + i\,\frac{1}{\sqrt{2}}$. Allora

$$\boldsymbol{C}_8 = \langle\,\zeta\,\rangle = \{1,\, \zeta,\, \zeta^2 = i,\, \zeta^3,\, \zeta^4 = -1,\, \zeta^5,\, \zeta^6 = -i,\, \zeta^7\}.$$



Poichè i divisori positivi di 8 sono 1, 2, 4, 8, $\boldsymbol{C}_8$ ha i seguenti sottogruppi:

$$\langle\,\zeta^{8/1}\,\rangle = \langle\,1\,\rangle = \{1\};$$
$$\langle\,\zeta^{8/2}\,\rangle = \langle\,\zeta^4\rangle = \langle\,-1\,\rangle = \{1, -1\} \quad [\cong \boldsymbol{C}_2];$$
$$\langle\,\zeta^{8/4}\,\rangle = \langle\,\zeta^2\rangle = \langle\,i\,\rangle = \{1,\, i,\, -1,\, -i\} \quad [\cong \boldsymbol{C}_4];$$
$$\langle\,\zeta^{8/8}\,\rangle = \langle\,\zeta\,\rangle = \boldsymbol{C}_8.$$

Poiché $1 \,|\, 2 \,|\, 4 \,|\, 8$, il reticolo dei sottogruppi di $\boldsymbol{C}_8$ è il seguente:

$$\begin{array}{c} \boldsymbol{C}_8 = \langle\,\zeta\,\rangle \\ | \\ \langle\,\zeta^2\,\rangle \\ | \\ \langle\,\zeta^4\,\rangle \\ | \\ \{1\} = \langle\,\zeta^8\,\rangle \end{array}$$

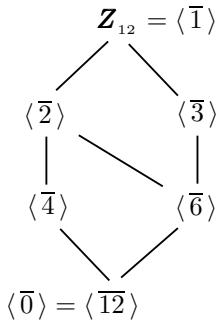
(*ii*) Determiniamo ora il reticolo dei sottogruppi di $(\boldsymbol{Z}_{12}, +)$.

I divisori positivi di 12 sono 1, 2, 3, 4, 6, 12. I corrispondenti sottogruppi sono:

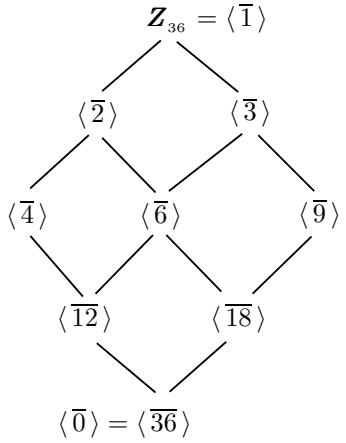
$$\langle\,\tfrac{12}{1}\,\overline{1}\,\rangle = \langle\,\overline{0}\,\rangle = \{\overline{0}\};$$
$$\langle\,\tfrac{12}{2}\,\overline{1}\,\rangle = \langle\,\overline{6}\,\rangle = \{\overline{0},\, \overline{6}\} \quad [\cong \boldsymbol{Z}_2];$$
$$\langle\,\tfrac{12}{3}\,\overline{1}\,\rangle = \langle\,\overline{4}\,\rangle = \{\overline{0},\, \overline{4},\, \overline{8}\} \quad [\cong \boldsymbol{Z}_3];$$
$$\langle\,\tfrac{12}{4}\,\overline{1}\,\rangle = \langle\,\overline{3}\,\rangle = \{\overline{0},\, \overline{3},\, \overline{6},\, \overline{9}\} \quad [\cong \boldsymbol{Z}_4];$$
$$\langle\,\tfrac{12}{6}\,\overline{1}\,\rangle = \langle\,\overline{2}\,\rangle = \{\overline{0},\, \overline{2},\, \overline{4},\, \overline{6},\, \overline{8},\, \overline{10}\} \quad [\cong \boldsymbol{Z}_6];$$
$$\langle\,\tfrac{12}{12}\,\overline{1}\,\rangle = \langle\,\overline{1}\,\rangle = \boldsymbol{Z}_{12}.$$

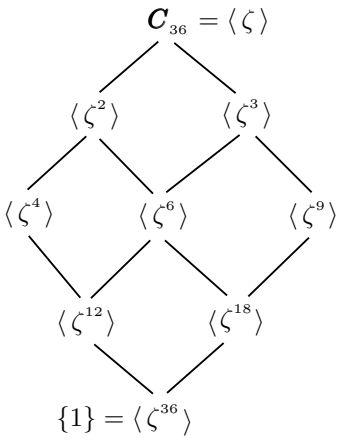
Tra i divisori positivi di 12 sussistono le seguenti relazioni di divisibilità: $1 \,|\, 2 \,\Big|\, \begin{matrix} 4 \\ 6 \end{matrix} \,\Big|\, 12$, $1 \,|\, 3 \,|\, 6 \,|\, 12$.

Conseguentemente, il reticolo dei sottogruppi di $\boldsymbol{Z}_{12}$ è:



(*iii*) Senza ulteriori commenti scriviamo il reticolo dei sottogruppi di $(\boldsymbol{Z}_{36}, +)$ e $(\boldsymbol{C}_{36}, \cdot)$.





Veniamo ora al <u>problema (**B**)</u>: determinare e contare i generatori di un gruppo ciclico.

Relativamente al gruppo ciclico infinito $(\boldsymbol{Z}, +)$, risulta:

$$\boldsymbol{Z} = \langle 1 \rangle = \langle -1 \rangle, \text{ mentre, } \forall\, n \neq \pm 1,\ \langle n \rangle = n\boldsymbol{Z} \subset \boldsymbol{Z}.$$

Dunque $(\boldsymbol{Z}, +)$ ha soltanto due generatori: 1, -1.

Proposizione 4. *Sia* $G = \langle g \,|\, g^n = 1 \rangle$ *un gruppo ciclico di ordine* n. *Risulta,* $\forall\, t = 1, \ldots, n$:

$$\langle g^t \rangle = G \iff (t, n) = 1.$$

Dim. Essendo $|G| = n$, in base al **Lemma 1**,

$$g^t \text{ è un generatore di } G \iff \circ(g^t) = n \iff \tfrac{n}{(n,t)} = n \iff (n, t) = 1.$$

Segue dalla proposizione precedente che il numero dei generatori di $G = \langle g \,|\, g^n = 1 \rangle$ è

$\varphi(n) = \#\{t \in \boldsymbol{N} \,:\, 1 \leq t \leq n,\ (t, n) = 1\}$ [*funzione di Eulero*, cfr. **Cap. II**, **Def. 6.1**].

Ad esempio i generatori di $\boldsymbol{Z}_{12}$ sono quattro [perché $\varphi(12) = 4$], cioè: $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$.

Definizione 3. *I generatori del gruppo* $\boldsymbol{C}_n$ *sono detti radici primitive* n*-sime dell'unità. Se quindi* $\boldsymbol{C}_n = \langle \zeta_n \rangle$, ζ_n^k *è una radice primitiva* n*-sima di* $1 \iff \circ(\zeta_n^k) = n \iff (n, k) = 1$. *In particolare* ζ_n *è sempre una radice primitiva* n*-sima di* 1.

Esempi 2. Elenchiamo le radici primitive per i gruppi $\boldsymbol{C}_1, \boldsymbol{C}_2, \ldots, \boldsymbol{C}_6$. Risulta:

$\boldsymbol{C}_1 = \{1\}$. L'unica radice primitiva 1-sima dell'unità è 1;

$\boldsymbol{C}_2 = \{1, -1\}$. L'unica radice primitiva seconda dell'unità è -1;

$\boldsymbol{C}_3 = \{1, \zeta_3, \zeta_3^{\,2}\}$. Le radici primitive terze dell'unità sono $\zeta_3, \zeta_3^{\,2}$;

$\boldsymbol{C}_4 = \{1, i, -1, -i\}$. Le radici primitive quarte dell'unità sono $i, -i$;

$\boldsymbol{C}_5 = \{1, \zeta_5, \zeta_5^{\,2}, \zeta_5^{\,3}, \zeta_5^{\,4}\}$. Le radici primitive quinte dell'unità sono $\zeta_5, \zeta_5^{\,2}, \zeta_5^{\,3}, \zeta_5^{\,4}$;

$\boldsymbol{C}_6 = \{1, \zeta_6, \zeta_6^{\,2}, \zeta_6^{\,3}, \zeta_6^{\,4}, \zeta_6^{\,5}\}$. Le radici primitive seste dell'unità sono $\zeta_6, \zeta_6^{\,5}$.

Osservazione 4. Sia $\zeta = \zeta_n^{\,k} \in \boldsymbol{C}_n$. Se $\circ(\zeta) = d$ [in $\boldsymbol{C}_n$], risulta: $\zeta \in \boldsymbol{C}_d$ e ζ è una radice primitiva d-sima dell'unità. Infatti, da $\circ(\zeta) = d$ segue che

$$\zeta^d = 1 \text{ e } \zeta, \zeta^2, \dots, \zeta^{d-1} \neq 1.$$

Dunque $\boldsymbol{C}_d = \langle\zeta\rangle$, cioè ζ è una radice primitiva d-sima dell'unità.

Ad esempio, $\zeta_6^{\,4} \in \boldsymbol{C}_6$ ha periodo $\circ(\zeta_6^{\,4}) = \frac{6}{(4,6)} = \frac{6}{2} = 3$. Dunque $\zeta_6^{\,4}$ è una radice primitiva terza dell'unità. Infatti

$$\zeta_6^{\,4} = \cos\tfrac{2\pi}{6}\,4 + i\sin\tfrac{2\pi}{6}\,4 = \cos\tfrac{4\pi}{3} + i\sin\tfrac{4\pi}{3} = \zeta_3^{\,2}.$$

Dalle considerazioni precedenti segue che se, $\forall\, h \geq 1$, denotiamo con $\mathfrak{P}_h$ l'insieme delle radici primitive h-sime dell'unità (in $\boldsymbol{C}_h$), risulta:

$$\boldsymbol{C}_n = \bigsqcup_{d\,|n,\, d>0} \mathfrak{P}_d.$$

Ad esempio, $\boldsymbol{C}_6 = \mathfrak{P}_1 \cup \mathfrak{P}_2 \cup \mathfrak{P}_3 \cup \mathfrak{P}_6$, con

$$\mathfrak{P}_1 = \{1\}, \quad \mathfrak{P}_2 = \{-1\}, \quad \mathfrak{P}_3 = \{\zeta_3, \zeta_3^{\,2}\}, \quad \mathfrak{P}_6 = \{\zeta_6, \zeta_6^{\,5}\}.$$

L'osservazione precedente fa intuire che è possibile contare, in un gruppo ciclico di ordine n, il numero di elementi aventi periodo d (con d divisore positivo di n).

Proposizione 5. *Sia $G = \langle\, g \,|\, g^n = 1\,\rangle$ un gruppo ciclico di ordine n. Sia d un divisore positivo di n. Risulta:*

$$\#\{g^t \in G \mid \circ(g^t) = d\} = \varphi(d).$$

Ne segue che, $\forall\, n \geq 1$, risulta: $n = \sum_{d\,|n,\, d>0} \varphi(d)$.

Dim. Sia $n = dn_1$. Si ha:

$$\#\{g^t \in G \mid \circ(g^t) = d\} = \#\{t \mid 1 \leq t \leq n \text{ e } \tfrac{n}{(t,n)} = d\} =$$
$$\#\{t \mid 1 \leq t \leq n \text{ e } n = d(t,n)\} = \#\{t \mid 1 \leq t \leq dn_1 \text{ e } n_1 = (t, n_1 d)\}.$$

Gli elementi t di tale insieme verificano la condizione $n_1 \,|\, t$. Dunque $t = n_1 t_1$. Perciò:

$$\#\{g^t \in G \mid \circ(g^t) = d\} = \#\{n_1 t_1 \mid 1 \leq n_1 t_1 \leq dn_1 \text{ e } n_1 = (n_1 t_1, n_1 d)\} =$$
$$\#\{t_1 \mid \tfrac{1}{n_1} \leq t_1 \leq d \text{ e } 1 = (t_1, d)\} = \#\{t_1 \mid 1 \leq t_1 \leq d \text{ e } 1 = (t_1, d)\} = \varphi(d).$$

L'ultima affermazione è evidente: basta ripartire G in sottoinsiemi di elementi aventi lo stesso periodo e sommare le cardinalità di ciascuno di tali sottoinsiemi.

Ad esempio, in $(\boldsymbol{Z}_{12}, +)$ gli elementi di periodo 6 sono due [in quanto $\varphi(6) = 2$]. Tali elementi verificano la condizione $6 = \frac{12}{(k,12)}$, cioè $(k, 12) = 2$, con $0 \leq k \leq 11$. Si tratta quindi di $\overline{2}, \overline{10}$.

Elenchiamo i periodi degli elementi di $\boldsymbol{Z}_{12}$:

$$\circ(\overline{0}) = 1; \quad \circ(\overline{6}) = 2; \quad \circ(\overline{4}) = \circ(\overline{8}) = 3; \quad \circ(\overline{3}) = \circ(\overline{9}) = 4;$$
$$\circ(\overline{2}) = \circ(\overline{10}) = 6; \quad \circ(\overline{1}) = \circ(\overline{5}) = \circ(\overline{7}) = \circ(\overline{11}) = 12.$$

3. Il gruppo delle permutazioni

Posto $X = \{1, 2, \dots, n\}$, è noto che l'insieme $\boldsymbol{S}_n = \boldsymbol{S}(X)$, delle biiezioni di X in sé, è un gruppo di ordine $n!$, detto *gruppo delle permutazioni su X* o *gruppo simmetrico su n elementi*, rispetto al prodotto operatorio $\circ$. Precisamente, considerate le due permutazioni

$$\sigma = \begin{pmatrix} 1 & 2 & \dots. & n \\ \sigma_1 & \sigma_2 & \dots. & \sigma_n \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & \dots. & n \\ \tau_1 & \tau_2 & \dots. & \tau_n \end{pmatrix} \in \boldsymbol{S}_n,$$

risulta:

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & \dots. & n \\ \tau_1 & \tau_2 & \dots. & \tau_n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \dots. & n \\ \sigma_1 & \sigma_2 & \dots. & \sigma_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots. & n \\ \tau_{\sigma_1} & \tau_{\sigma_2} & \dots. & \tau_{\sigma_n} \end{pmatrix}.$$

Ci sembra però più conveniente (cfr. **Cap. I, Esempi 4.4**) scrivere $\sigma\tau$ in luogo di $\tau \circ \sigma$. Seguiremo questa convenzione. Ad esempio, se

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}, \ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix} \in \boldsymbol{S}_5,$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}.$$

Definizione 1. *Sia $\sigma \in \boldsymbol{S}_n$ e sia k un intero tale che $1 \leq k \leq n$. σ è detto ciclo o k-ciclo o ciclo di lunghezza k se $\exists\, c_1, c_2, \dots, c_k \in X$, a due a due distinti, tali che*

$$\sigma(c_1) = c_2,\ \sigma(c_2) = c_3,\ \dots.\ ,\ \sigma(c_k) = c_1 \quad e \quad \sigma(x) = x,\ \forall\, x \in X,\ x \neq c_1, c_2, \dots, c_k\,.$$

Tale k-ciclo σ è usualmente denotato $(c_1, c_2, \dots, c_k)$, ovvero, più semplicemente, $(c_1\, c_2 \dots c_k)$. Ad esempio, la permutazione $\sigma\tau \in \boldsymbol{S}_5$ sopra considerata è il 5-ciclo $(1, 2, 3, 4, 5)$ [denotato anche $(1\,2\,3\,4\,5)$]. I 2-cicli vengono anche chiamati trasposizioni. Diremo infine, per brevità, che $c_1, \dots, c_k$ sono "elementi" del ciclo $(c_1\, c_2 \dots c_k)$.

Osservazione 1. (*i*) Sia $2 \leq k \leq n$. Ogni k-ciclo di $\boldsymbol{S}_n$ può essere scritto in k modi diversi. Infatti risulta:

$$(c_1\, c_2\, c_3 \dots c_k) = (c_2\, c_3 \dots c_k\, c_1) = \dots. = (c_k\, c_1\, c_2\, c_3 \dots c_{k-1}).$$

La permutazione identica $\mathbf{1}_X$, elemento neutro di $\boldsymbol{S}_n$, è un 1-ciclo, ed anzi è l'unico 1-ciclo di $\boldsymbol{S}_n$. Si può rappresentare con n scritture diverse, cioè $\mathbf{1}_X = (k),\ \forall\, k \in X\,]$. Due cicli di lunghezza ≥ 2 sono detti *disgiunti* se gli elementi di X che intervengono in un ciclo sono tutti diversi da quelli che intervengono nell'altro ciclo.

(*ii*) Non ogni permutazione $\sigma \in \boldsymbol{S}_n$ è un ciclo; però "contiene" almeno un ciclo [nel senso che $\gamma = (c_1, \dots, c_k)$ è detto *ciclo di* σ se $\sigma\big|_{\{c_1, \dots, c_k\}} = \gamma\big|_{\{c_1, \dots, c_k\}}$]. Ad esempio la permutazione $\sigma \in \boldsymbol{S}_5$ sopra considerata non è un ciclo, ma contiene i due cicli $(1\,3)$, $(2\,4\,5)$. In effetti σ è prodotto di tali cicli, in quanto risulta $\sigma = (1\,3)(2\,4\,5)$.

Proposizione 1. *Ogni permutazione non identica $\sigma \in \boldsymbol{S}_n$ è il prodotto dei suoi cicli disgiunti.*

Dim. Se $\sigma = \mathbf{1}_X$, allora $\sigma = (1)$. Sia $\sigma \neq \mathbf{1}_X$ e siano $\gamma_1, \dots, \gamma_t$ tutti i cicli (a due a due disgiunti) di σ. Bisogna verificare che risulta: $\sigma = \gamma_1 \dots \gamma_t$, cioè che, $\forall\, x \in X$, risulta $\sigma(x) = (\gamma_1 \dots \gamma_t)(x)$.

Se x non appartiene ad alcuno dei cicli γ_i, allora $\sigma(x) = x = (\gamma_1 \dots \gamma_t)(x)$. Altrimenti, sia γ_i l'unico k-ciclo di σ contenente x. Allora:

$$\gamma_i = \big(x,\, \sigma(x),\, \sigma^2(x),\, \dots, \sigma^{k-1}(x)\big).$$

Si ha:

$$(\gamma_1 \dots \gamma_t)(x) = (\gamma_t \circ \dots \circ \gamma_1)(x) = (\gamma_t \circ \dots \circ \gamma_i)(x) = (\gamma_t \circ \dots \circ \gamma_{i+1})(\sigma(x)) = \dots = \sigma(x)$$

[in quanto x non appartiene ai cicli $\gamma_1, \dots, \gamma_{i-1}$ e $\sigma(x)$ non appartiene ai cicli $\gamma_{i+1}, \dots, \gamma_t$]. Dunque

$\sigma = \gamma_1 ... \gamma_t$.

Osservazione 2. (*i*) Due cicli disgiunti di $\boldsymbol{S}_n$ commutano. Siano infatti $\gamma_1 = (c_1\, c_2\, ...\, c_k)$ e $\gamma_2 = (d_1\, d_2\, ...\, d_h)$ due cicli disgiunti di $\boldsymbol{S}_n$. Si tratta di verificare che

$$(\gamma_1\gamma_2)(x) = (\gamma_2\gamma_1)(x), \ \forall\, x \in X.$$

Se $x \in X - \{c_1, ..., c_k, d_1, ..., d_h\}$, allora $\gamma_1(x) = \gamma_2(x) = x$ e dunque $(\gamma_1\gamma_2)(x) = (\gamma_2\gamma_1)(x) = x$. Se invece $x \in \{c_1, ..., c_k\}$, si ha:

$$(\gamma_1\gamma_2)(x) = (\gamma_2 \circ \gamma_1)(x) = \gamma_2(\gamma_1(x)) = \gamma_1(x) \ \text{ [perché } \gamma_1(x) \notin \{d_1, ..., d_h\}],$$
$$(\gamma_2\gamma_1)(x) = (\gamma_1 \circ \gamma_2)(x) = \gamma_1(\gamma_2(x)) = \gamma_1(x) \ \text{ [perché } x \notin \{d_1, ..., d_h\}].$$

Se infine $x \in \{d_1, ..., d_h\}$, si ottiene ancora, con analoghe considerazioni, che $(\gamma_1\gamma_2)(x) = (\gamma_2\gamma_1)(x)$.

(*ii*) Ogni k-ciclo $(k \geq 2)$ è sempre esprimibile come prodotto di $k-1$ 2-cicli (non disgiunti). Infatti:

$$(c_1\, c_2\, ...\, c_k) = (c_1\, c_2)(c_1\, c_3) ... (c_1\, c_k).$$

(*iii*) Si verifica facilmente che l'inverso del k-ciclo $(c_1\, c_2\, ...\, c_{k-1}\, c_k)$ è il k-ciclo $(c_k\ c_{k-1}\ ...\ c_2\, c_1)$.

Proposizione 2. *(i) Il periodo di un k-ciclo di $\boldsymbol{S}_n$ è k.*
(ii) Il periodo di una permutazione $\sigma \in \boldsymbol{S}_n$ è il minimo comune multiplo delle lunghezze dei suoi cicli disgiunti.

Dim. (*i*) Sia $\gamma = (c_1\, c_2\, ...\, c_k)$ un k-ciclo di $\boldsymbol{S}_n$. Si ha:

$$\gamma^k(c_1) = \gamma^{k-1}(c_2) = \ ... \ = \gamma(c_k) = c_1, \quad \gamma^k(c_2) = \gamma^{k-1}(c_3) = \ ... \ = \gamma^2(c_k) = \gamma(c_1) = c_2,$$

e, quindi, procedendo analogamente, $\gamma^k(c_i) = c_i$, $\forall\, i = 1, ..., k$.

Infine, $\gamma^k(x) = x$, $\forall\, x \in X - \{c_1\ ...\ c_k\}$. Dunque $\gamma^k = \mathbf{1}_X$. Inoltre, $\forall\, h \,\big|\, 1 \leq h < k$, si ha che $\gamma^h(c_1) = c_{h+1} \neq c_1$. Dunque $\gamma^h \neq \mathbf{1}_X$. Si conclude che $\circ(\gamma) = k$.

(*ii*) Sia $\sigma = \gamma_1 ... \gamma_t$ (prodotto di cicli disgiunti) e sia k_i la lunghezza del ciclo γ_i $(1 \leq i \leq t)$. Sia $n := \circ(\sigma)$ e sia $m := mcm(k_1, ..., k_t)$. Bisogna verificare che $n \,\big|\, m$ e $m \,\big|\, n$.

Tenuto conto di (*i*) e di **Osserv. 2**(*i*), si ha:

$$\sigma^m = (\gamma_1 ... \gamma_t)^m = \gamma_1^{\,m} ... \gamma_t^{\,m} = \mathbf{1}_X ... \mathbf{1}_X = \mathbf{1}_X \ \text{ e dunque } n \,\big|\, m.$$

Viceversa, da $\circ(\sigma) = n$ e da **Osserv. 2**(*i*), segue:

$$\mathbf{1}_X = \sigma^n = \gamma_1^{\,n} ... \gamma_t^{\,n}.$$

Se verifichiamo che ogni $\gamma_i^{\,n} = \mathbf{1}_X$, allora $k_i = \circ(\gamma_i) \,\big|\, n$ e dunque $mcm(k_1, ..., k_t) \,\big|\, n$, cioè $m \,\big|\, n$.

Sia quindi $x \in X$. Se x non appartiene al ciclo γ_i, allora $\gamma_i^{\,n}(x) = x$; se invece x appartiene a γ_i, allora non appartiene agli altri cicli γ_j. Pertanto $x = \sigma^n(x) = (\gamma_1^{\,n} ... \gamma_t^{\,n})(x) = \gamma_i^{\,n}(x)$, cioè $\gamma_i^{\,n}(x) = x$. Pertanto $\gamma_i^{\,n} = \mathbf{1}_X$, come richiesto.

Dalla **Prop. 1** e dall'**Osserv. 2**(*ii*), segue che ogni permutazione è prodotto di un numero finito di trasposizioni (o 2-cicli). Tale scrittura non è però unica. Ad esempio la permutazione

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix} \in \boldsymbol{S}_5$$

può essere scritta nella forma $\sigma = (1\,2)(3\,4)$ ma anche nella forma $\sigma = (3\,5)(2\,1)(5\,3)(3\,4)$ [come facilmente si verifica]. Ciò che si conserva è la "parità" del numero delle trasposizioni di ogni prodotto, come sarà ora dimostrato.

Proposizione 3. *Sia σ una permutazione di $\boldsymbol{S}_n$, esprimibile come prodotto di trasposizioni nelle due seguenti forme:*

$$\sigma = \gamma_1 .... \gamma_t = \delta_1 .... \delta_s .$$

Risulta: $t \equiv s \ (mod\ 2)$. Dunque il numero dei fattori di σ è sempre pari o sempre dispari.

Dim. La permutazione σ definisce la seguente applicazione:

$$\Phi_\sigma : \boldsymbol{Z}[X_1, \dots X_n] \to \boldsymbol{Z}[X_1, \dots X_n] \text{ tale che } \begin{array}{l} X_i \to X_{\sigma_i}, \ \forall i = 1, \dots, n, \\ c \to c, \ \forall c \in \boldsymbol{Z}. \end{array}$$

Si può verificare che Φ_σ è un isomorfismo dell'anello $\boldsymbol{Z}[X_1, \dots X_n]$ in sé (con inversa l'applicazione $\Phi_{\sigma^{-1}}$), detto *scambio di variabili associato a* σ.

Risulta, $\forall \sigma, \tau \in \boldsymbol{S}_n$: $\Phi_{\sigma\circ\tau} = \Phi_\sigma \circ \Phi_\tau$. Infatti

$$\Phi_{\sigma\circ\tau} : X_i \to X_{\sigma_{\tau_i}}, \qquad \Phi_\sigma \circ \Phi_\tau : X_i \to X_{\tau_i} \to X_{\sigma_{\tau_i}}.$$

Si consideri ora in $\boldsymbol{Z}[X_1, \dots X_n]$ il polinomio

$$P := \prod_{1\le h<k\le n} (X_h - X_k) = (X_1 - X_2)(X_1 - X_3) \dots (X_1 - X_n)(X_2 - X_3) \dots (X_2 - X_n) \dots (X_{n-1} - X_n).$$

Si può verificare che:

($*$) $\Phi_\gamma(P) = -P$, per ogni trasposizione $\gamma = (i\,j) \in \boldsymbol{S}_n$.

Verifichiamo l'affermazione ($*$) su un esempio. Posto $\gamma = (1\,3) \in \boldsymbol{S}_4$:

$$P = (X_1 - X_2)(X_1 - X_3)(X_1 - X_4)(X_2 - X_3)(X_2 - X_4)(X_3 - X_4);$$
$$\Phi_\gamma(P) = (X_3 - X_2)(X_3 - X_1)(X_3 - X_4)(X_2 - X_1)(X_2 - X_4)(X_1 - X_4) =$$
$$= [-(X_2 - X_3)][-(X_1 - X_3)](X_3 - X_4)[-(X_1 - X_2)](X_2 - X_4)(X_1 - X_4) = (-1)^3 P = -P.$$

Accettando provvisoriamente l'affermazione ($*$), possiamo concludere facilmente la dimostrazione. Infatti:

$$\Phi_\sigma(P) = \begin{cases} \Phi_{\gamma_1 \dots \gamma_t}(P) = \Phi_{\gamma_t} \circ \dots \circ \Phi_{\gamma_1}(P) = -\big(- \dots - (P)\big) = (-1)^t P \\ \Phi_{\delta_1 \dots \delta_s}(P) = \Phi_{\delta_s} \circ \dots \circ \Phi_{\delta_1}(P) = -\big(- \dots - (P)\big) = (-1)^s P. \end{cases}$$

Da $(-1)^t P = (-1)^s P$, segue che $t \equiv s \ (mod\ 2)$.

Resta da verificare l'affermazione ($*$). Si osserva subito che ogni permutazione $\gamma = (i, j)$ si può esprimere come prodotto di un numero dispari di *trasposizioni ad interi consecutivi*. Infatti, supposto $i < j$, risulta:

$$\gamma = (i, j) = \underbrace{(i, i+1)(i+1, i+2) \dots (j-2, j-1)}(j-1, j)\,\underbrace{(j-2, j-1) \dots (i+1, i+2)(i, i+1)}.$$

Ad esempio, in $\boldsymbol{S}_n$, con $n \ge 7$:

$$(2\,7) = \underbrace{(2\,3)(3\,4)(4\,5)(5\,6)}(6\,7)\,\underbrace{(5\,6)(4\,5)(3\,4)(2\,3)}.$$

Si osserva ora che, se $\delta = (i, i+1)$ è una trasposizione ad interi consecutivi, allora $\Phi_\delta(P) = -P$. Infatti Φ_δ trasforma il fattore $X_i - X_{i+1}$ di P nel suo opposto, mentre, $\forall (h, k) \ne (i, i+1)$, con $h < k$, $\Phi_\delta(X_h - X_k)$ è ancora un fattore di P [infatti $\Phi_\delta(X_h - X_k) = X_{\delta(h)} - X_{\delta(k)}$, con $\delta(h) < \delta(k)$].

Si conclude che, per ogni trasposizione γ: $\Phi_\gamma(P) = \underbrace{-\big(- \dots - (P)\big)}_{\text{num. dispari}} = -P$.

Definizione 2. *Una permutazione $\sigma \in \boldsymbol{S}_n$ è detta di classe pari se è esprimibile come prodotto di un numero pari di trasposizioni. Altrimenti è detta di classe dispari. L'insieme delle permutazioni di classe pari è denotato $\boldsymbol{A}_n$.*

Osservazione 3. (i) Se una permutazione $\sigma \in \boldsymbol{S}_n$ è prodotto di t cicli $\gamma_1, \dots, \gamma_t$, aventi lunghezze rispettivamente $k_1, \dots, k_t$, la parità di σ è data dalla parità del numero $\sum_{i=1}^{t} (k_i - 1)$ [infatti γ_i è prodotto di $k_i - 1$ trasposizioni (cfr. **Osserv. 2**(ii))].

(ii) Ci chiediamo come, assegnata una permutazione $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma_1 & \sigma_2 & \dots & \sigma_n \end{pmatrix} \in \boldsymbol{S}_n$, se ne possa individuare la parità *direttamente*, cioè senza ricorrere alla sua scrittura come prodotto di cicli.

Per ogni $k = 1, \dots n$, si pone

$$I(\sigma, k) := \#\big\{\sigma_j : \ j > k \ \text{ e } \ \sigma_j < \sigma_k\big\}$$

[in particolare quindi $I(\sigma, n) = 0$]. Si pone poi:

$$I(\sigma) := I(\sigma, 1) + \ \dots \ + I(\sigma, n-1)$$

[detto *numero delle inversioni di* σ]. Si potrebbe verificare che:

$$\sigma \text{ è di classe pari } \iff I(\sigma) \text{ è un numero pari.}$$

Ad esempio, sia $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 5 & 3 & 4 & 2 \end{pmatrix} \in \boldsymbol{S}_6$. Si ha:

$$I(\sigma,1) = 5,\ I(\sigma,2) = 0,\ I(\sigma,3) = 3,\ I(\sigma,4) = 1,\ I(\sigma,5) = 1,$$

e quindi $I(\sigma) = 5+0+3+1+1 = 10$. Pertanto σ è di classe pari. Infatti risulta

$$\sigma = (1\,6\,2)(3\,5\,4) = (1\,6)(1\,2)(3\,5)(3\,4).$$

Proposizione 4. *Per ogni $n \geq 2$, $\boldsymbol{A}_n$ è un sottogruppo di $\boldsymbol{S}_n$ avente ordine $\frac{n!}{2}$. È detto gruppo alterno su n elementi.*

Dim. Se $\sigma, \tau \in \boldsymbol{A}_n$, anche $\sigma\tau \in \boldsymbol{A}_n$ [come σ e τ, anche $\sigma\tau$ è prodotto di un numero pari di trasposizioni]. $(1) \in \boldsymbol{A}_n$ [è prodotto di 0 trasposizioni]. Se $\sigma \in \boldsymbol{A}_n$, anche $\sigma^{-1} \in \boldsymbol{A}_n$. Se infatti $\sigma = \gamma_1 .... \gamma_{2t}$, allora

$$\sigma^{-1} = (\gamma_1 .... \gamma_{2t})^{-1} = (\gamma_{2t} \circ .... \circ \gamma_1)^{-1} = \gamma_1^{-1} \circ .... \circ \gamma_{2t}^{-1} = \gamma_1 \circ .... \circ \gamma_{2t} = \gamma_{2t} .... \gamma_1.$$

[Si noti che ogni trasposizione coincide con la propria inversa, avendo periodo 2].

Resta da verificare che $|\boldsymbol{A}_n| = \frac{n!}{2}$. A tale scopo, si fissi un'arbitraria trasposizione $\gamma_0 \in \boldsymbol{S}_n$. Si osserva subito che, $\forall\, \sigma \in \boldsymbol{S}_n$, $\gamma_0\sigma$ ha parità opposta alla parità di σ. Posto $\boldsymbol{B}_n := \boldsymbol{S}_n - \boldsymbol{A}_n$ [insieme delle permutazioni dispari], si consideri la partizione $\{\boldsymbol{A}_n, \boldsymbol{B}_n\}$ di $\boldsymbol{S}_n$. Si consideri poi la biiezione

$$\gamma_0 \_ : \boldsymbol{S}_n \to \boldsymbol{S}_n \quad \text{[cfr. } \textbf{Osserv. 1.1}(i)\text{]}.$$

Si ha: $\gamma_0 \boldsymbol{A}_n = \boldsymbol{B}_n$ e $\gamma_0 \boldsymbol{B}_n = \boldsymbol{A}_n$. Essendo $|\gamma_0 \boldsymbol{A}_n| = |\boldsymbol{A}_n|$, allora $|\boldsymbol{A}_n| = |\boldsymbol{B}_n|$. Ne segue:

$$n! = |\boldsymbol{S}_n| = |\boldsymbol{A}_n| + |\boldsymbol{B}_n| = 2|\boldsymbol{A}_n| \quad \text{e quindi} \quad |\boldsymbol{A}_n| = \tfrac{n!}{2}.$$

Nota. $\boldsymbol{B}_n$ non è mai un sottogruppo: infatti non è chiuso rispetto all'operazione di $\boldsymbol{S}_n$ [in quanto il prodotto di due permutazioni dispari è pari].

Esempi 1. Vogliamo scrivere gli elementi di $\boldsymbol{S}_1, \boldsymbol{S}_2, \boldsymbol{S}_3$ ed $\boldsymbol{S}_4$ ed indicarne le prime proprietà relative alla struttura gruppale.

(*i*) $\boldsymbol{S}_1 = \{(1)\}$ è il gruppo unità.

(*ii*) $\boldsymbol{S}_2 = \{(1), (1\,2)\}$ è il gruppo ciclico di ordine 2.

(*iii*) $\boldsymbol{S}_3 = \{(1), (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$. Risulta ad esempio $(1\,2)(1\,3) \neq (1\,3)(1\,2)$. Inoltre

$$\circ((1)) = 1;\ \circ((1\,2)) = \circ((1\,3)) = \circ((2\,3)) = 2;\ \circ((1\,2\,3)) = \circ((1\,3\,2)) = 3.$$

Si noti che si tratta del primo gruppo finito non abeliano che incontriamo. La tavola moltiplicativa di $\boldsymbol{S}_3$ è la seguente:

$\cdot$	(1)	$(1\,2)$	$(1\,3)$	$(2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
(1)	(1)	$(1\,2)$	$(1\,3)$	$(2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
$(1\,2)$	$(1\,2)$	(1)	$(1\,2\,3)$	$(1\,3\,2)$	$(1\,3)$	$(2\,3)$
$(1\,3)$	$(1\,3)$	$(1\,3\,2)$	(1)	$(1\,2\,3)$	$(2\,3)$	$(1\,2)$
$(2\,3)$	$(2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$	(1)	$(1\,2)$	$(1\,3)$
$(1\,2\,3)$	$(1\,2\,3)$	$(2\,3)$	$(1\,2)$	$(1\,3)$	$(1\,3\,2)$	(1)
$(1\,3\,2)$	$(1\,3\,2)$	$(1\,3)$	$(2\,3)$	$(1\,2)$	(1)	$(1\,2\,3)$

Si noti ancora che $\boldsymbol{S}_3$ è generato da due suoi 2-cicli. Scelti infatti ad esempio $(1\,2), (1\,3) \in \boldsymbol{S}_3$, risulta

$$\langle (1\,2), (1\,3) \rangle = \boldsymbol{S}_3$$

Infatti: $(1) = (1\,2)(1\,2)$, $(1\,2\,3) = (1\,2)(1\,3)$, $(1\,3\,2) = (1\,3)(1\,2)$ e $(2\,3) = (1\,2\,3)(1\,2) = (1\,2)(1\,3)(1\,2)$.

Quali sono i sottogruppi di $\boldsymbol{S}_3$?

Ovviamente abbiamo i due sottogruppi banali $\{(1)\}$ ed $\boldsymbol{S}_3$. Poiché $\boldsymbol{S}_3$ ha tre elementi di periodo 2, ci sono tre sottogruppi ciclici di ordine 2: $\langle (1\,2) \rangle$, $\langle (1\,3) \rangle$, $\langle (2\,3) \rangle$. C'è poi il sottogruppo alterno $\boldsymbol{A}_3 = \{(1), (1\,2\,3), (1\,3\,2)\}$, che è ciclico di ordine 3: $\boldsymbol{A}_3 = \langle (1\,2\,3) \rangle$.

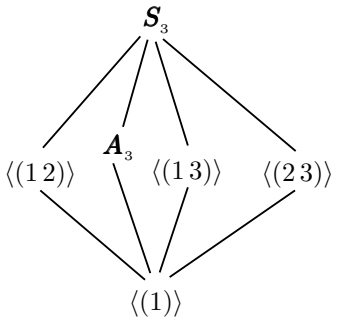
Verifichiamo ora che $\boldsymbol{S}_3$ non possiede altri sottogruppi.

Sia $\boldsymbol{H} \leq \boldsymbol{S}_3$ con $\boldsymbol{H} \neq \{(1)\}, \langle (1\,2)\rangle, \langle (1\,3)\rangle, \langle (2\,3)\rangle, \boldsymbol{A}_3$. Basterà verificare che $\boldsymbol{H} = \boldsymbol{S}_3$. Si noti che $\boldsymbol{H}$ contiene almeno un 2-ciclo [altrimenti $\boldsymbol{H} = \boldsymbol{A}_3$]. Ci sono due eventualità:

(**1**) $\boldsymbol{H}$ contiene un 2-ciclo γ ed un 3-ciclo σ. Allora $\boldsymbol{H}$ contiene anche l'altro 3-ciclo $\sigma^2 [= \sigma^{-1}]$ e quindi $\boldsymbol{H} \ni \gamma\sigma,\ \gamma\sigma^2$. Tali elementi sono distinti tra loro e distinti da (1), γ, σ, σ^2; dunque sono necessariamente i rimanenti 2-cicli di $\boldsymbol{S}_3$. Pertanto $\boldsymbol{H} = \boldsymbol{S}_3$.

(**2**) $\boldsymbol{H}$ contiene almeno due 2-cicli distinti di $\boldsymbol{S}_3$. Si verifica con semplici calcoli che il loro prodotto è un 3-ciclo. Dunque $\boldsymbol{H}$ rientra nel caso precedente e pertanto $\boldsymbol{H} = \boldsymbol{S}_3$.

Il reticolo dei sottogruppi di $\boldsymbol{S}_3$ è il seguente:



(*iv*) $\boldsymbol{S}_4$ è formato dai seguenti $4! = 24$ elementi:

(1)	periodo 1	[pari]
$(1\,2), (1\,3), (1\,4), (2\,3), (2\,4), (3\,4)$	periodo 2	[dispari]
$(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)$		[pari]
$(1\,2\,3), (1\,2\,4), (1\,3\,4), (2\,3\,4)$	periodo 3	[pari]
$(1\,3\,2), (1\,4\,2), (1\,4\,3), (2\,4\,3)$		
$(1\,2\,3\,4), (1\,2\,4\,3), (1\,3\,2\,4)$	periodo 4	[dispari]
$(1\,4\,3\,2), (1\,3\,4\,2), (1\,4\,2\,3)$		

Si noti che $\boldsymbol{S}_4$ non è ciclico (non ha elementi di periodo 24) e neppure abeliano. Ad esempio infatti

$$(1\,2\,3)(1\,2\,4) = (1\,4)(2\,3), \quad (1\,2\,4)(1\,2\,3) = (1\,3)(2\,4).$$

Il sottogruppo alterno $\boldsymbol{A}_4$ (formato dalle 12 permutazioni pari) è

$$\boldsymbol{A}_4 = \big\{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1\,2\,3), (1\,2\,4), (1\,3\,4), (2\,3\,4), (1\,3\,2), (1\,4\,2), (1\,4\,3), (2\,4\,3)\big\}.$$

Anch'esso è non ciclico e neppure abeliano.

Tra i sottogruppi di $\boldsymbol{S}_4$ segnaliamo inoltre: nove sottogruppi ciclici di ordine 2 (corrispondenti ai nove elementi di periodo 2), quattro sottogruppi ciclici di ordine 3 (corrispondenti agli otto elementi di periodo 3) e quattro sottogruppi isomorfi a $\boldsymbol{S}_3$ (sono $\boldsymbol{S}(\{1,2,3\})$, $\boldsymbol{S}(\{1,2,4\})$, $\boldsymbol{S}(\{1,3,4\})$ e $\boldsymbol{S}(\{2,3,4\})$. Non esiste invece alcun sottogruppo ciclico di ordine 6 (mancando in $\boldsymbol{S}_4$ elementi di periodo 6)

Osservazione 4. A proposito del gruppo alterno $\boldsymbol{A}_n$, è interessante osservare che, $\forall\, n \geq 3$, ogni $\sigma \in \boldsymbol{A}_n$ è prodotto di 3-cicli: dunque $\boldsymbol{A}_n$ *è generato dai* 3*-cicli di* $\boldsymbol{S}_n$. Sia infatti $\sigma \in \boldsymbol{A}_n$. Risulta:

$$\sigma = \gamma_1\gamma_2 \ldots \gamma_{2t} = (\gamma_1\gamma_2)(\gamma_3\gamma_4) \ldots (\gamma_{2t-1}\gamma_{2t}),$$

cioè σ è prodotto di coppie di trasposizioni. Basta allora verificare che ogni prodotto di due trasposizioni $(a\,b)(c\,d)$ è prodotto di 3-cicli. Sono possibili tre casi:

(**1**) le due trasposizioni coincidono;
(**2**) le due trasposizioni hanno un elemento comune;
(**3**) le due trasposizioni sono disgiunte.

Nel caso (**1**): $(a\,b)(a\,b) = (1) = (1\,2\,3)(1\,3\,2)$.
Nel caso (**2**): $(a\,b)(a\,c) = (a\,b\,c)$; $\quad (a\,b)(b\,c) = (a\,c\,b)$.

Nel caso (**3**): $(a\,b)(c\,d) = (a\,c\,b)(c\,b\,d)$ [verificare].

Concludiamo il paragrafo con il concetto di *struttura ciclica*. Se consideriamo, ad esempio, le due permutazioni $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 4 & 3 & 6 & 7 & 5 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 7 & 6 & 1 & 4 & 2 \end{pmatrix} \in \boldsymbol{S}_7$, e le scriviamo come prodotto di cicli disgiunti:

$$\sigma_1 = (1\,2)(3\,4)(5\,6\,7), \quad \sigma_2 = (1\,5)(2\,3\,7)(4\,6),$$

osserviamo che entrambe sono costituite da due 2-cicli e da un 3-ciclo. Diremo in tal caso che *hanno la stessa struttura ciclica*. Infatti:

Definizione 3. *Siano $\sigma_1, \sigma_2 \in \boldsymbol{S}_n$. Si dice che σ_1, σ_2 hanno la stessa struttura ciclica se, scritte come prodotto di cicli disgiunti, sono formate da cicli delle stesse lunghezze.*

Possiamo quindi ripartire $\boldsymbol{S}_n$ in sottoinsiemi formati da permutazioni con la stessa struttura ciclica. Verificheremo che tale partizione è realizzata tramite la relazione di equivalenza di *coniugio su* $\boldsymbol{S}_n$ (relazione che può essere definita in ogni gruppo G).

Definizione 4. *Sia G un gruppo. In G è definita la seguente relazione, detta relazione di coniugio:*

$$g_1 \sim g_2 \iff \exists\, x \in G \;\big|\; g_2 = x\, g_1\, x^{-1} \quad \textit{[ovvero } g_2 = \gamma_x(g_1) \textit{ (cfr. } \textbf{Osserv. 1.1}\textit{(ii)]}.$$

Si verifica facilmente che $\sim$ è una relazione di equivalenza su G. Se poi G è abeliano, $\sim$ è la relazione identica. In particolare, $\forall\, \sigma_1, \sigma_2 \in \boldsymbol{S}_n$:

$$\sigma_1 \sim \sigma_2 \iff \exists\, \tau \in \boldsymbol{S}_n \;\big|\; \sigma_2 = \tau^{-1}\sigma_1\tau \quad [= \tau \circ \sigma_1 \circ \tau^{-1}]$$

[e si dirà che σ_2 è coniugato di σ_1 tramite τ].

Proposizione 5. *Siano $\sigma_1, \sigma_2 \in \boldsymbol{S}_n$. Risulta:*

$$\sigma_1, \sigma_2 \textit{ hanno la stessa struttura ciclica} \iff \sigma_1 \sim \sigma_2.$$

Dim. Premettiamo la seguente affermazione:

(∗) Siano $\sigma_1, \sigma_2 \in \boldsymbol{S}_n$ tali che $\sigma_1 \sim \sigma_2$, con $\sigma_2 = \tau^{-1}\sigma_1\tau$. Se $\sigma_1(x) = y$, allora: $\sigma_2(\tau(x)) = \tau(y)$.

Giustifichiamo (∗). Risulta infatti:

$$\tau^{-1}\sigma_1\tau = \begin{pmatrix} \dots & \tau(x) & \dots & \tau(y) & \dots \\ \dots & x & \dots & y & \dots \end{pmatrix}\begin{pmatrix} \dots & x & \dots \\ \dots & y & \dots \end{pmatrix}\begin{pmatrix} \dots & x & \dots & y & \dots \\ \dots & \tau(x) & \dots & \tau(y) & \dots \end{pmatrix} = \begin{pmatrix} \dots & \tau(x) & \dots \\ \dots & \tau(y) & \dots \end{pmatrix} = \sigma_2.$$

($\Longleftarrow$). Sia $\sigma_1 = (\dots)\dots(a_1 \dots a_k)\dots(\dots)$ [prodotto di cicli disgiunti]. In particolare $\sigma_1(a_i) = a_{i+1}$ e dunque, per (∗), $\sigma_2(\tau(a_i)) = \tau(a_{i+1})$. Ne segue che σ_2 ammette tra i suoi cicli il ciclo $(\tau(a_1) \dots \tau(a_k))$ [corrispondente ad $(a_1 \dots a_k)$]. Si conclude che σ_1, σ_2 hanno la stessa struttura ciclica.

($\Longrightarrow$). Siano

$$\sigma_1 = (\dots)\dots(c_1 \dots c_k)\dots(\dots), \quad \sigma_2 = (\dots)\dots(d_1 \dots d_k)\dots(\dots)$$

due permutazioni di $\boldsymbol{S}_n$ con la stessa struttura ciclica. Assumiamo che in tali scritture compaiano anche gli eventuali 1-cicli di σ_1, σ_2. Se il ciclo $(c_1 \dots c_k)$ di σ_1 corrisponde al ciclo $(d_1 \dots d_k)$ di σ_2, si definisce $\tau \in \boldsymbol{S}_n$ tale che $\tau(c_i) = d_i$. [Si noti che τ è completamente individuato da tali condizioni]. Verifichiamo che $\sigma_2 = \tau^{-1}\sigma_1\tau$. Infatti si ha:

$$(\tau^{-1}\sigma_1\tau)(d_i) = (\tau \circ \sigma_1 \circ \tau^{-1})(d_i) = (\tau \circ \sigma_1)(c_i) = \tau(c_{i+1}) = d_{i+1} = \sigma_2(d_i).$$

Esempi 2. (*i*) Assegnati $\sigma, \tau \in \boldsymbol{S}_n$, per calcolare il coniugato $\tau^{-1}\sigma\tau$ di σ (tramite τ) conviene, invece di eseguire il calcolo diretto del prodotto, operare utilizzando la precedente affermazione (∗), come nel seguente esempio.

Siano $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 8 & 5 & 6 & 2 & 7 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 1 & 3 & 5 & 7 & 2 & 8 \end{pmatrix} \in \boldsymbol{S}_8$. Risulta:

$$\sigma = (1\,3)(2\,4\,8\,7), \quad \tau = (1\,4\,3)(2\,6\,7).$$

Quindi

$$\tau^{-1}\sigma\tau = \big((\tau(1)\,\tau(3)\big)\big((\tau(2)\,\tau(4)\,\tau(8)\,\tau(7)\big) = (4\,1)(6\,3\,8\,2).$$

Procedendo con il calcolo diretto si ha infatti:

$$\tau^{-1}\sigma\tau = (1\,3\,4)(2\,7\,6)(1\,3)(2\,4\,8\,7)(1\,4\,3)(2\,6\,7) = (1\,4)(2\,6\,3\,8) \quad [= (4\,1)(6\,3\,8\,2)].$$

(*ii*) Assegnate due permutazioni $\sigma_1, \sigma_2 \in \boldsymbol{S}_n$ con la stessa struttura ciclica, vogliamo determinare $\tau \in \boldsymbol{S}_n$ tale che $\sigma_2 = \tau^{-1}\sigma_1\tau$.

Siano $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 1 & 4 & 8 & 6 & 7 & 2 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 6 & 7 & 5 & 3 & 1 & 8 \end{pmatrix} \in \boldsymbol{S}_8$. Risulta:

$$\sigma_1 = (1\,3)(2\,5\,8), \quad \sigma_2 = (1\,4\,7)(3\,6).$$

Allora

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 6 & & 4 & & & 7 \end{pmatrix}.$$

Come si vede, τ non è completamente individuata. Riscriviamo allora σ_1 e σ_2 aggiungendo (ad esempio in ordine crescente) i rispettivi 1-cicli. Si ha:

$$\sigma_1 = (1\,3)(2\,5\,8)(2)(6)(7), \quad \sigma_2 = (1\,4\,7)(3\,6)(2)(5)(8).$$

Dunque

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 6 & 2 & 4 & 5 & 8 & 7 \end{pmatrix} = (1\,3\,6\,5\,4\,2)(7\,8).$$

Si noti che, variando l'ordine di scrittura dei cicli di σ_1 e σ_2, si ottengono altre permutazioni τ.

Completiamo il paragrafo formulando due ultime domande:

(***a***) *Quante sono le strutture cicliche di* $\boldsymbol{S}_n$ *?*

(***b***) *Quante permutazioni contiene una struttura ciclica di* $\boldsymbol{S}_n$ *?*

Relativamente alla domanda (***a***), si osservi che, poiché cicli disgiunti commutano, ogni struttura ciclica può essere ordinata (ad esempio) secondo la lunghezza decrescente dei suoi cicli. Ne segue che le strutture cicliche di $\boldsymbol{S}_n$ corrispondono biunivocamente all'insieme

$$\big\{(n_1, \ldots\ldots, n_t) \,\big|\, t \geq 1,\ \sum_{i=1}^{t} n_i = n \quad \text{e} \quad n_1 \geq n_2 \geq \ \ldots\ldots\ \geq n_t \geq 1\big\}.$$

Ad esempio, relativamente ad $\boldsymbol{S}_3$, l'insieme in questione è $\big\{(3),\ (2,\ 1),\ (1,\ 1,\ 1)\big\}$, corrispondente alle tre strutture cicliche:

$$\begin{cases} (\_\ \_\ \_) & \text{(3-ciclo)}, \\ (\_\ \_)(\_) = (\_\ \_) & \text{(2-ciclo)}, \\ (\_)(\_)(\_) = (\_) & \text{(1-ciclo)}. \end{cases}$$

Relativamente ad $\boldsymbol{S}_4$, l'insieme in questione è $\big\{(4),\ (3,\ 1),\ (2,\ 2),\ (2,\ 1,\ 1),\ (1,\ 1,\ 1,\ 1)\big\}$, a cui corrispondono le seguenti cinque strutture cicliche:

$$\begin{cases} (\_\ \_\ \_\ \_) & \text{(4-ciclo)}, \\ (\_\ \_\ \_)(\_) = (\_\ \_\ \_) & \text{(3-ciclo)}, \\ (\_\ \_)(\_\ \_) & \text{(coppia di 2-cicli)}, \\ (\_\ \_)(\_)(\_) = (\_\ \_) & \text{(2-ciclo)}, \\ (\_)(\_)(\_)(\_) = (\_) & \text{(1-ciclo)}. \end{cases}$$

Relativamente alla domanda (***b***), ci limitiamo ad affrontare il seguente problema: *quanti sono i k-cicli di* $\boldsymbol{S}_n$ *?*

Proposizione 6. *Sia* $2 \leq k \leq n$. *I k-cicli di* $\boldsymbol{S}_n$ *sono* $\binom{n}{k}(k-1)!$

Dim. Si fissino k elementi dell'insieme $X = \{1, 2, \ldots, n\}$: ci sono $\binom{n}{k}$ possibili scelte. Siano $\{a_1, \ldots, a_k\}$ gli elementi scelti in X. I k-cicli formati da $\{a_1, \ldots, a_k\}$ possono essere tutti indicati

con primo elemento a_1. Allora sono in corrispondenza biunivoca con tutte le possibili permutazioni dell'insieme $\{a_2, \dots, a_k\}$ e quindi sono $(k-1)!$. Si hanno quindi complessivamente $\binom{n}{k}(k-1)!$ possibili k-cicli.

Esercizio 1. Sia $X = \{1, 2, 3, 4, 5\}$ e sia $V = \{1, 3\} \subset X$.

(*i*) Verificare che l'insieme $\boldsymbol{H} = \{\sigma \in \boldsymbol{S}_5 \,|\, \sigma(V) = V\}$ è un sottogruppo di $\boldsymbol{S}_5$.

(*ii*) Determinare i 12 elementi di $\boldsymbol{H}$ e indicarne i periodi.

(*iii*) Verificare che $\boldsymbol{H}$ possiede: sette sottogruppi ciclici di ordine 2; un sottogruppo ciclico di ordine 3; tre sottogruppi di ordine 4, tre sottogruppi di ordine 6, di cui uno ciclico e due isomorfi a $\boldsymbol{S}_3$.

Soluzione. (*i*) Ovviamente $\mathbf{1} = (1) \in \boldsymbol{H}$. Se $\sigma, \tau \in \boldsymbol{H}$, risulta: $\sigma\tau(V) = \tau(\sigma(V)) = \tau(V) = V$. Dunque $\sigma\tau \in \boldsymbol{H}$. Se infine $\sigma \in \boldsymbol{H}$, allora $\sigma^{-1}(V) = \sigma^{-1}(\sigma(V)) = V$. Dunque $\sigma^{-1} \in \boldsymbol{H}$. Si conclude che $\boldsymbol{H} < \boldsymbol{S}_5$.

(*ii*) Gli elementi di $\boldsymbol{H}$ si ripartiscono in due sottoinsiemi disgiunti:

$$\boldsymbol{H}_0 = \{\sigma \in \boldsymbol{H} \,|\, \sigma(1) = 1 \text{ e } \sigma(3) = 3\}, \quad \boldsymbol{H}_1 = \{\sigma \in \boldsymbol{H} \,|\, \sigma(1) = 3 \text{ e } \sigma(3) = 1\}.$$

Si noti che, $\forall\, \sigma \in \boldsymbol{H}$, risulta $\sigma(X-V) = X-V$, cioè σ è permutazione sull'insieme $X-V = \{2, 4, 5\}$. Risulta:

$$\boldsymbol{S}(X-V) = \big\{(2) = (1), (2\,4), (2\,5), (4\,5), (2\,4\,5), (2\,5\,4)\big\} \cong \boldsymbol{S}_3.$$

Allora:

$$\boldsymbol{H}_0 = (1)(3)\boldsymbol{S}(X-V) = \big\{(1), (2\,4), (2\,5), (4\,5), (2\,4\,5), (2\,5\,4)\big\} \cong \boldsymbol{S}_3,$$

$$\boldsymbol{H}_1 = (1\,3)\boldsymbol{S}(X-V) = \big\{(1\,3), (1\,3)(2\,4), (1\,3)(2\,5), (1\,3)(4\,5), (1\,3)(2\,4\,5), (1\,3)(2\,5\,4)\big\}.$$

[Ovviamente $\boldsymbol{H}_0$ è un sottogruppo di $\boldsymbol{H}$ mentre $\boldsymbol{H}_1$ non lo è].

Oltre all'unità (1), $\boldsymbol{H}$ possiede:

sette elementi di periodo 2: $(2\,4)$, $(2\,5)$, $(4\,5)$, $(1\,3)$, $(1\,3)(2\,4)$, $(1\,3)(2\,5)$, $(1\,3)(4\,5)$;
due elementi di periodo 3: $(2\,4\,5)$, $(2\,5\,4)$;
due elementi di periodo 6: $(1\,3)(2\,4\,5)$, $(1\,3)(2\,5\,4)$.

(*iii*) I sette elementi di periodo 2 generano rispettivamente sette sottogruppi ciclici di ordine 2, mentre i due elementi di periodo 3 generano un sottogruppo ciclico di ordine 3:

$$\langle(2\,4\,5)\rangle = \{(1), (2\,4\,5), (2\,5\,4)\}$$

(sottogruppo alterno di $\boldsymbol{H}_0$).

I due elementi di periodo 6 generano il sottogruppo ciclico di ordine 6:

$$\boldsymbol{C}_6 = \langle(1\,3)(2\,4\,5)\rangle = \langle(1\,3)(2\,5\,4)\rangle = \{(1), (1\,3)(2\,4\,5), (2\,5\,4), (1\,3), (2\,4\,5), (1\,3)(2\,5\,4)\}.$$

Come già osservato, il gruppo $\boldsymbol{H}_0$ è un sottogruppo isomorfo a $\boldsymbol{S}_3$: è generato dai suoi tre 2-cicli. Esiste inoltre un altro sottogruppo di ordine 6, anch'esso isomorfo ad $\boldsymbol{S}_3$: è il gruppo $\tilde{\boldsymbol{H}}$ generato dalle tre permutazioni $(1\,3)(2\,4)$, $(1\,3)(2\,5)$, $(1\,3)(4\,5)$ [in effetti da due di esse]. Risulta:

$$\tilde{\boldsymbol{H}} = \big\{(1), (1\,3)(2\,4), (1\,3)(2\,5), (1\,3)(4\,5), (2\,4\,5), (2\,5\,4)\big\}.$$

Infine si osservi che $\boldsymbol{H}$ è prodotto [cfr. **Prop. 1.4**] dei suoi due sottogruppi $\langle(1\,3)\rangle$, $\boldsymbol{H}_0$ e che tali sottogruppi commutano "elemento per elemento" [in quanto formati da permutazioni disgiunte]. Allora, per ogni sottogruppo di $\langle(1\,3)\rangle$ ed ogni sottogruppo di $\boldsymbol{H}_0$, il prodotto di tali sottogruppi commuta ed è quindi un sottogruppo di $\boldsymbol{H}$. In particolare sono sottogruppi di $\boldsymbol{H}$:

$$\boldsymbol{V}_1 = \langle(1\,3)\rangle\langle(2\,4)\rangle = \big\{(1), (1\,3), (2\,4), (1\,3)(2\,4)\big\};$$
$$\boldsymbol{V}_2 = \langle(1\,3)\rangle\langle(2\,5)\rangle = \big\{(1), (1\,3), (2\,5), (1\,3)(2\,5)\big\};$$
$$\boldsymbol{V}_3 = \langle(1\,3)\rangle\langle(4\,5)\rangle = \big\{(1), (1\,3), (4\,5), (1\,3)(4\,5)\big\}.$$

Si tratta di tre *sottogruppi di Klein*: di essi ci occuperemo nel prossimo paragrafo.

Nota. Per il diagramma dei sottogruppi di $\boldsymbol{H}$ rinviamo al paragrafo **5**, applicazione *(B)*.

4. Isometrie del piano euclideo e gruppi diedrali

Premettiamo allo studio dei gruppi diedrali alcune nozioni di Geometria Euclidea, probabilmente non ancora note al lettore.

Sia $\boldsymbol{E}^2$ il piano euclideo: si tratta dell'ordinario *"piano fisico"*, in cui possibile misurare distanze ed angoli. In particolare, fissato un *riferimento cartesiano* di $\boldsymbol{E}^2$, la *distanza (o metrica) euclidea* tra due punti $P,\, P' \in \boldsymbol{E}^2$ è definita in questo modo:

$$d(P,P') := \sqrt{(x-x')^2+(y-y')^2}, \quad \forall\, P=(x,y),\, P'=(x',y') \in \boldsymbol{E}^2.$$

Definizione 1. *Un'isometria f di $\boldsymbol{E}^2$ è un'applicazione biiettiva $f : \boldsymbol{E}^2 \to \boldsymbol{E}^2$ che "conserva la distanza euclidea", cioè tale che:*

$$d\big(f(P), f(P')\big) = d(P,P'), \quad \forall\, P,\, P' \in \boldsymbol{E}^2.$$

(**1**) Si può verificare che l'insieme delle isometrie di $\boldsymbol{E}^2$, denotato $\boldsymbol{\mathcal{I}som}(\boldsymbol{E}^2)$, è un sottogruppo del gruppo $\boldsymbol{S}(\boldsymbol{E}^2)$ delle biiezioni di $\boldsymbol{E}^2$ in sé.

(**2**) Sia $\boldsymbol{H}$ un sottoinsieme non vuoto di $\boldsymbol{E}^2$. Si può facilmente verificare che l'insieme

$$\boldsymbol{\mathcal{I}som}(\boldsymbol{H}) = \big\{ f \in \boldsymbol{\mathcal{I}som}(\boldsymbol{E}^2) \,\big|\, f(\boldsymbol{H}) = \boldsymbol{H} \big\}$$

è un sottogruppo di $\boldsymbol{\mathcal{I}som}(\boldsymbol{E}^2)$.

(**3**) Ogni isometria f di $\boldsymbol{E}^2$ individua un operatore lineare (biiettivo) $\varphi_f : \boldsymbol{R}^2 \to \boldsymbol{R}^2$, così definito

$$\varphi_f\,(\overrightarrow{PQ}) = \overrightarrow{f(P)f(Q)}, \quad \forall\, \overrightarrow{PQ} \in \boldsymbol{R}^2.$$

Si può verificare che φ_f è un *operatore unitario*, cioè che, rispetto alla base canonica di $\boldsymbol{R}^2$, ha matrice del tipo

$$A = \begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix} \text{ oppure } B = \begin{pmatrix} \cos\vartheta & \sin\vartheta \\ \sin\vartheta & -\cos\vartheta \end{pmatrix}, \ \exists\, \vartheta \in \boldsymbol{R}.$$

Nel primo caso, $det(A) = 1$ e l'isometria è detta *diretta*; nel secondo caso, $det(B) = -1$ e l'isometria è detta *inversa*.

(**4**) Si può facilmente verificare che un'isometria trasforma rette in rette [se ad esempio P, Q, R sono tre punti allineati e $\overrightarrow{PR} = c\,\overrightarrow{PQ}$, allora $\overrightarrow{f(P)f(R)} = \varphi_f(\overrightarrow{PR}) = c\,\varphi_f(\overrightarrow{PQ}) = c\,\overrightarrow{f(P)f(Q)}$ e quindi $f(P), f(Q), f(R)$ sono allineati] e conserva il parallelismo tra rette. In particolare quindi trasforma *poligoni n-lateri* in poligoni n-lateri, inducendo una permutazione tra i vertici. [Intendiamo per *poligono n-latero* una linea spezzata, chiusa e semplice (cioè senza intersezioni), in cui tre vertici consecutivi non possono essere allineati].

Si può inoltre dimostrare che un'isometria conserva anche gli angoli tra rette. In particolare quindi trasforma *poligoni regolari* in *poligoni regolari*.

(**5**) Esistono quattro tipi di isometrie di $\boldsymbol{E}^2$:

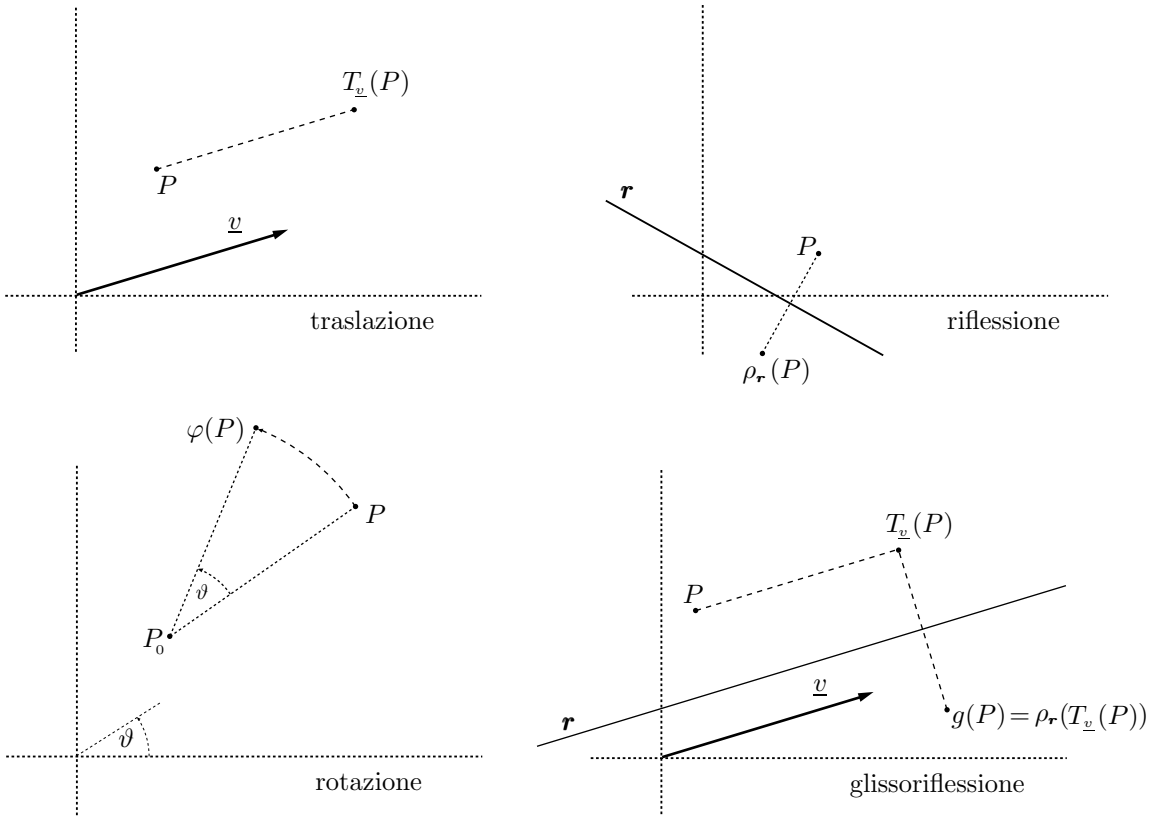
(*i*) le *traslazioni* $T = T_{\underline{v}}$ (con $\underline{v}$ vettore di $\boldsymbol{R}^2$);

(*ii*) le *riflessioni* $\rho = \rho_{\boldsymbol{r}}$ (di *asse* una retta $\boldsymbol{r}$ di $\boldsymbol{R}^2$);

(*iii*) le *rotazioni* $\varphi = \varphi_{P_0,\vartheta}$ (di *centro* una punto P_0 ed *angolo* ϑ);

(*iv*) le *glissoriflessioni* $g = \rho_{\boldsymbol{r}} \circ T_{\underline{v}}$ (con $\underline{v} \,\big|\big|\, \boldsymbol{r}$, $\underline{v} \neq \underline{0}$), ottenute componendo una traslazione (non identica) con una riflessione.

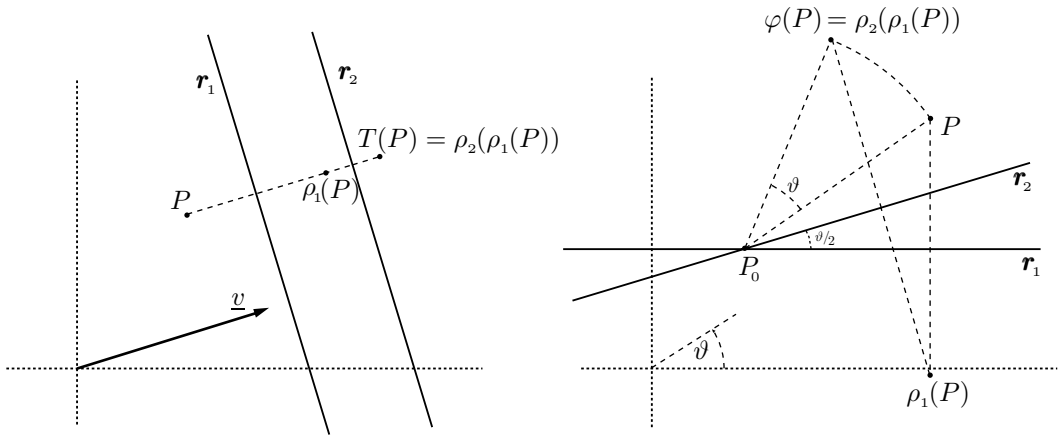
Le definizioni di tali isometrie dovrebbero essere chiarite dai disegni che seguono.



Si può dimostrare (*Teorema di Chasles*, 1831) che non esistono altri tipi di isometrie di $\boldsymbol{E}^2$. In particolare quindi componendo due isometrie di questi quattro tipi si ottiene ancora un'isometria di uno di questi quattro tipi.

Inoltre le traslazioni e le rotazioni sono isometrie dirette [in quanto si può verificare che la matrice del corrispondente operatore ha determinante $= 1$], mentre le riflessioni e le glissoriflessioni sono isometrie inverse [in quanto la matrice ha determinante $= -1$]. Infine, le rotazioni e le riflessioni hanno ovviamente punti fissi [risp. un punto ed una retta], mentre le traslazioni [diverse dall'identità $\mathbf{1} = T_{\underline{0}}$] e le glissoriflessioni non ne hanno.

(**6**) Si può infine dimostrare che ogni isometria è ottenibile componendo opportunamente delle riflessioni (e quindi che il gruppo $\boldsymbol{\mathcal{I}som}(\boldsymbol{E}^2)$ è generato dalle riflessioni). Si ha infatti, come dovrebbe essere chiaro dai disegni seguenti:



(*i*) $T_{\underline{v}} = \rho_{\boldsymbol{r}_2} \circ \rho_{\boldsymbol{r}_1}$, con $\boldsymbol{r}_1, \boldsymbol{r}_2$ rette ortogonali a $\underline{v}$ ed aventi distanza tra loro pari a $\frac{1}{2} \| \underline{v} \|$ [dove $\| \underline{v} \|$ denota la lunghezza del vettore $\underline{v}$].

(*ii*) $\varphi = \varphi_{P_0,\vartheta} = \rho_{\boldsymbol{r}_2} \circ \rho_{\boldsymbol{r}_1}$, con $\boldsymbol{r}_1, \boldsymbol{r}_2$ rette intersecantisi in P_0 e formanti tra loro angolo $\frac{\vartheta}{2}$.

Sia $\boldsymbol{\mathcal{P}_n}$ un poligono n-latero (non necessariamente regolare), con vertici $P_1, P_2, \dots, P_n$. Per ogni $f \in \boldsymbol{Isom}(\boldsymbol{\mathcal{P}_n})$, f induce la permutazione dei vertici di $\boldsymbol{\mathcal{P}_n}$:

$$\sigma_f = \begin{pmatrix} P_1 & P_2 & \dots & P_n \\ f(P_1) & f(P_2) & \dots & f(P_n) \end{pmatrix},$$

identificabile ad un elemento di $\boldsymbol{S}_n$. È quindi definita l'applicazione

$$\Phi : \boldsymbol{Isom}(\boldsymbol{\mathcal{P}_n}) \longrightarrow \boldsymbol{S}_n \text{ tale che } \Phi(f) = \sigma_f, \quad \forall\, f \in \boldsymbol{Isom}(\boldsymbol{\mathcal{P}_n}).$$

Φ è ovviamente un omomorfismo di gruppi [infatti $\Phi(g \circ f) = \sigma_{g \circ f} = \sigma_g \circ \sigma_f = \Phi(g) \circ \Phi(f)$].

Vogliamo ora verificare che Φ è iniettiva, cioè che, se $\sigma_f = \sigma_g$, allora $f = g$. Da $\sigma_f = \sigma_g$ segue in particolare che $f(P_1) = g(P_1)$, $f(P_2) = g(P_2)$, $f(P_3) = g(P_3)$; osserviamo poi che P_1, P_2, P_3 sono punti non allineati [in quanto vertici consecutivi di un poligono].

Per dimostrare che $f = g$ basta osservare che un'isometria f di $\boldsymbol{E}^2$ è completamente individuata se si conosce l'immagine (tramite f) di tre punti non allineati P_1, P_2, P_3. Se infatti $P \in \boldsymbol{E}^2$ e se $\overrightarrow{P_1P} = a\overrightarrow{P_1P_2} + b\overrightarrow{P_1P_3}$, allora

$$\overrightarrow{f(P_1)f(P)} = \varphi_f(\overrightarrow{P_1P}) = a\,\varphi_f(\overrightarrow{P_1P_2}) + b\,\varphi_f(\overrightarrow{P_1P_3}) = a\,\overrightarrow{f(P_1)f(P_2)} + b\,\overrightarrow{f(P_1)f(P_3)}$$

e dunque $f(P)$ è funzione di $f(P_1)$, $f(P_2)$, $f(P_3)$ e delle coordinate (a, b) di P nel riferimento affine definito da P_1, P_2, P_3.

Poiché f, g coincidono nei tre punti P_1, P_2, P_3, allora $f = g$.

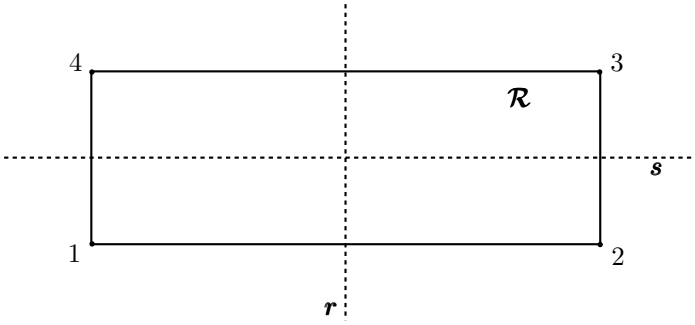
La conclusione di quanto precede è la seguente: *il fatto che* $\Phi : \boldsymbol{Isom}(\boldsymbol{\mathcal{P}_n}) \to \boldsymbol{S}_n$ *è un omomorfismo iniettivo ci consente di interpretare* $\boldsymbol{Isom}(\boldsymbol{\mathcal{P}_n})$ *come un sottogruppo di* $\boldsymbol{S}_n$.

In questo paragrafo studieremo:

- il gruppo $\boldsymbol{Isom}(\boldsymbol{\mathcal{R}})$, dove $\boldsymbol{\mathcal{R}}$ è un rettangolo (non quadrato), detto *gruppo di Klein*.
- i gruppi $\boldsymbol{Isom}(\boldsymbol{\mathcal{P}}_n)$, $n \geq 3$, dove $\boldsymbol{\mathcal{P}}_n$ è un poligono n-latero regolare, detti *gruppi diedrali*, ed usualmente denotati $\boldsymbol{D}_n$.

(*A*) Il gruppo di Klein

Sia $\boldsymbol{\mathcal{R}}$ un rettangolo non quadrato, di vertici 1, 2, 3, 4.



$\boldsymbol{Isom}(\boldsymbol{\mathcal{R}})$ è formato da quattro isometrie (identificabili a permutazioni di $\boldsymbol{S}_4$):

- l'isometria identica $\mathbf{1} = (1)$;
- la riflessione intorno all'asse $\boldsymbol{r}$, che si identifica a $(1\,2)(3\,4)$;
- la riflessione intorno all'asse $\boldsymbol{s}$, che si identifica a $(1\,4)(2\,3)$;
- la rotazione di angolo π e centro in $\boldsymbol{r} \cap \boldsymbol{s}$, che si identifica a $(1\,3)(2\,4)$.

Osservazione 1. Come possiamo assicurarci che non esistano altre isometrie che fissano $\boldsymbol{\mathcal{R}}$? Basterà verificare che le altre $24 - 4$ permutazioni di $\boldsymbol{S}_4$ non sono indotte da isometrie.

Ad esempio, consideriamo $(1\,2\,3) \in \boldsymbol{S}_4$. Se esistesse $f \in \boldsymbol{Isom}(\boldsymbol{\mathcal{R}})$ tale che $\sigma_f = (1\,2\,3)$, allora il lato $\overline{1\,2}$ di $\boldsymbol{\mathcal{R}}$ verrebbe trasformato da f nel lato $\overline{f(1)\,f(2)} = \overline{2\,3}$. Ma i due lati $\overline{1\,2}$, $\overline{2\,3}$ hanno lunghezze diverse (perché $\boldsymbol{\mathcal{R}}$ non è quadrato) mentre un'isometria conserva le distanze e quindi le lunghezze dei segmenti.

Il gruppo $\boldsymbol{Isom}(\boldsymbol{\mathcal{R}})$, detto *gruppo di Klein*, è dunque formato da quattro elementi. Si denota usualmente con $\boldsymbol{V}$ [dal tedesco "vier", cioè "quattro"]. Se poniamo:

$$1 := (1), \quad a := (1\,2)(3\,4), \quad b := (1\,4)(2\,3), \quad c := (1\,3)(2\,4),$$

allora $\boldsymbol{V} = \{1, a, b, c\}$ ha la seguente tavola moltiplicativa:

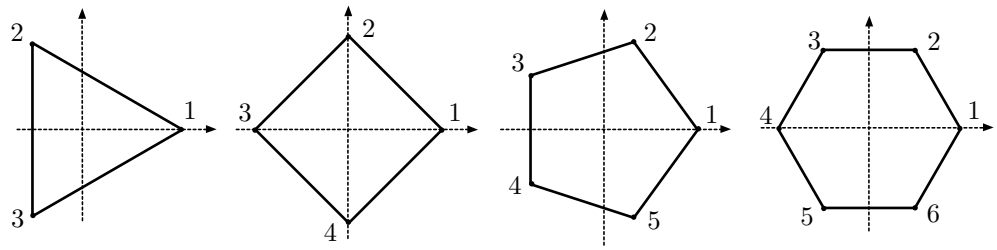
$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Si tratta, come si osserva, di un gruppo commutativo non ciclico [perché $\circ(a) = \circ(b) = \circ(c) = 2$]. Dunque $\boldsymbol{V} \ncong \boldsymbol{C}_4$. Proveremo nel seguito che $\boldsymbol{C}_4$ e $\boldsymbol{V}$ sono, a meno di isomorfismi, gli unici gruppi di ordine 4. Astrattamente parlando, $\boldsymbol{V}$ è un gruppo generato da due simboli a, b verificanti le relazioni: $a^2 = b^2 = 1$, $ba = ab$. Dunque

$$\boldsymbol{V} = \langle a, b \mid a^2 = b^2 = 1,\ ba = ab \rangle.$$

($\boldsymbol{B}$) Il gruppo diedrale

Per ogni $n \geq 3$, sia $\boldsymbol{D}_n = \boldsymbol{Isom}(\boldsymbol{\mathcal{P}}_n)$, dove $\boldsymbol{\mathcal{P}}_n$ è il poligono regolare n-latero. Assumeremo che $\boldsymbol{\mathcal{P}}_n$ sia centrato in O ed abbia vertici $1, 2, \ldots, n$, in senso antiorario e con vertice 1 situato sul semiasse x positivo.



$(n = 3)$ $(n = 4)$ $(n = 5)$ $(n = 6)$

Quali sono le isometrie f di $\boldsymbol{E}^2$ che fissano $\boldsymbol{\mathcal{P}}_n$? Si osserva facilmente che risulta $f(O) = O$ [infatti $f(O)$ ed O hanno la stessa distanza dai vertici di $\boldsymbol{\mathcal{P}}_n$; inoltre esiste un unico punto equidistante da tre punti non allineati (come lo sono tre vertici di $\boldsymbol{\mathcal{P}}_n$)]. Ne segue che le isometrie cercate non possono essere né traslazioni né glissoriflessioni; si tratta quindi di rotazioni di centro O oppure riflessioni di asse una retta passante per O.

($\boldsymbol{a}$) Indichiamo con $\varphi = \varphi_{O,\frac{2\pi}{n}}$ la rotazione (antioraria) di centro O e angolo $\frac{2\pi}{n}$. Tale rotazione fissa $\boldsymbol{\mathcal{P}}_n$ (e dunque $\varphi \in \boldsymbol{D}_n$) e trasforma il vertice i in $i+1$ [ed n in 1]. Dunque φ corrisponde all'n-ciclo $(1\,2\,3\,\ldots\,n) \in \boldsymbol{S}_n$. Tutte le potenze $\varphi, \varphi^2, \varphi^3, \ldots, \varphi^{n-1}, \varphi^n = \boldsymbol{1}$ sono elementi distinti di $\boldsymbol{D}_n$: si tratta delle uniche rotazioni di $\boldsymbol{E}^2$ che fissano il poligono $\boldsymbol{\mathcal{P}}_n$. Se infatti la rotazione $\varphi_{O,\vartheta}$ fissa $\boldsymbol{D}_n$, allora ne ruota i vertici e dunque $\vartheta = \frac{2k\pi}{n}$, $\exists\, k \in \boldsymbol{Z}$; allora $\vartheta = \frac{2h\pi}{n}$, con $0 \leq h < n$ [in quanto $\circ(\varphi) = n$].

($\boldsymbol{b}$) $\boldsymbol{\mathcal{P}}_n$ è simmetrico rispetto alle sue *diagonali* ed ai suoi *assi*. [Intendiamo per *diagonale* di $\boldsymbol{\mathcal{P}}_n$ ogni retta che unisce un vertice al centro di $\boldsymbol{\mathcal{P}}_n$; per *asse* di $\boldsymbol{\mathcal{P}}_n$ l'asse di ogni lato di $\boldsymbol{\mathcal{P}}_n$]. Se n è dispari, le diagonali coincidono con gli assi e sono n rette. Se n è pari, esistono $\frac{n}{2}$ diagonali ed $\frac{n}{2}$ assi: in tutto n rette. Tali n rette definiscono n riflessioni (distinte): si tratta delle uniche riflessioni di $\boldsymbol{E}^2$ che fissano $\boldsymbol{\mathcal{P}}_n$. Infatti, se $\rho_{\boldsymbol{r}} \in \boldsymbol{Isom}(\boldsymbol{\mathcal{P}}_n)$, per ragioni di simmetria $\boldsymbol{r}$ interseca $\boldsymbol{\mathcal{P}}_n$ in un vertice

o è asse di un lato di $\boldsymbol{\mathcal{P}}_n$. Dunque $\boldsymbol{r}$ è una diagonale o un asse di $\boldsymbol{\mathcal{P}}_n$.

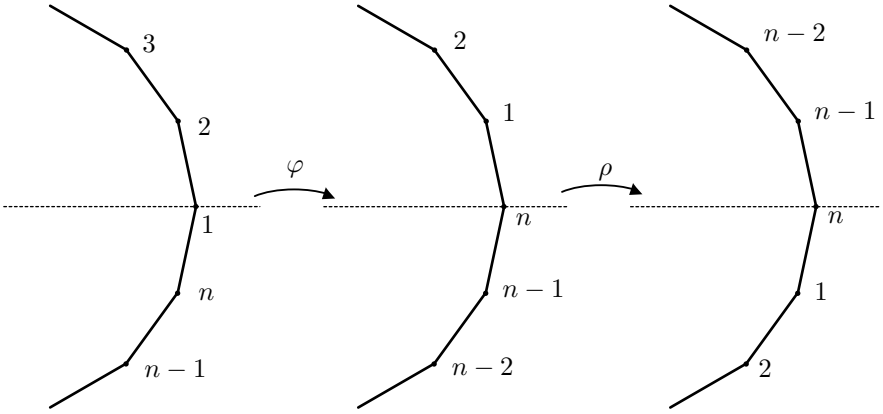
Denotiamo con ρ la riflessione rispetto all'asse x (che è certamente una di tali rette). Poché ρ fissa il vertice 1 e scambia 2 con n, 3 con $n-1$, ecc., allora ρ è identificabile ad un prodotto di 2-cicli disgiunti di $\boldsymbol{S}_n$. Precisamente,

- se n è dispari: $\rho = (2,\, n)(3,\, n-1)\ \ldots\ (\frac{n+1}{2}\,,\, \frac{n+3}{2})$;
- se n è pari: $\rho = (2,\, n)(3,\, n-1)\ \ldots\ (\frac{n}{2}\,,\, \frac{n+4}{2})$.

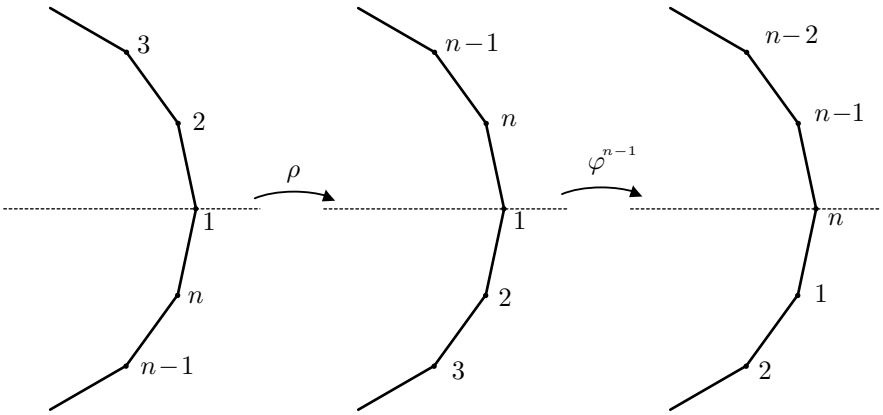
Le altre $n-1$ riflessioni di $\boldsymbol{D}_n$ coincidono con le seguenti isometrie: $\rho,\ \varphi\circ\rho,\ \varphi^2\circ\rho,\ \ldots.\,,\ \varphi^{n-1}\circ\rho$. Infatti si osserva facilmente che tali isometrie sono a due a due distinte e che sono riflessioni [in quanto, componendo una riflessione $\rho_{\boldsymbol{r}}$ con una rotazione $\varphi = \varphi_{P_0,\vartheta}$ (con $P_0 \in \boldsymbol{r}$) si ottiene un'isometria inversa con almeno un punto fisso (P_0), cioè una riflessione].

(***c***) Si noti che anche $\rho\circ\varphi$ è una riflessione. Vogliamo verificare che $\rho\circ\varphi = \varphi^{n-1}\circ\rho$.

Calcoliamo $\rho\circ\varphi$. Applicando a $\boldsymbol{\mathcal{P}}_n$ prima φ e poi ρ, risulta:



e quindi $\rho\circ\varphi = (1,\, n)(2,\, n-1)(3,\, n-2)\ \ldots.$. Calcoliamo ora $\varphi^{n-1}\circ\rho$. Risulta:



e quindi $\varphi^{n-1}\circ\rho = (1,\, n)(2,\, n-1)(3,\, n-2)\ \ldots.$. Abbiamo così verificato che $\rho\circ\varphi = \varphi^{n-1}\circ\rho$ (detta *relazione diedrale* di $\boldsymbol{D}_n$. Potevamo verificare tale relazione facendo ricorso alle corrispondenti permutazioni di $\boldsymbol{S}_n$. Infatti, osservato che $\varphi^{n-1} = \varphi^{-1} = (1,\, n,\, n-1,\, \ldots, 3,\, 2)$, si ha:

$$\rho\circ\varphi = \varphi\,\rho = (1,\, 2,\, \ldots, n)(2,\, n)(3,\, n-1)\ \ldots\ = (1,\, n)(2,\, n-1)\ldots\,;$$
$$\varphi^{n-1}\circ\rho = \rho\,\varphi^{n-1} = (2,\, n)(3,\, n-1)\ \ldots\ (1,\, n,\, n-1,\, \ldots 3,\, 2) = (1,\, n)(2,\, n-1)\ldots\,.$$

Dalla relazione diedrale ne seguono altre: ad esempio $\rho\circ\varphi^2 = \varphi^{n-2}\circ\rho$. Infatti

$$\rho\circ\varphi^2 = (\rho\circ\varphi)\circ\varphi = (\varphi^{n-1}\circ\rho)\circ\varphi = \varphi^{n-1}\circ(\rho\circ\varphi) = \varphi^{n-1}\circ\varphi^{n-1}\circ\rho = \varphi^{n-2}\circ\rho.$$

Più in generale: $\rho\circ\varphi^k = \varphi^{n-k}\circ\rho\ (1 \le k \le n)$.

Riassumendo i tre punti precedenti, possiamo concludere che $\boldsymbol{D}_n$ è formato da $2n$ elementi:

- n sono rotazioni: $\boldsymbol{1},\ \varphi,\ \varphi^2,\ \ldots.\,,\ \varphi^{n-1}$ [e $\varphi^n = \boldsymbol{1}$];
- n sono riflessioni: $\rho,\ \varphi\circ\rho,\ \varphi^2\circ\rho,\ \ldots.\,,\ \varphi^{n-1}\circ\rho$ [e $\rho^2 = \boldsymbol{1},\ \rho\circ\varphi = \varphi^{n-1}\circ\rho$].

Scriveremo quindi

$$\boldsymbol{D}_n = \langle\, \rho,\, \varphi \;\big|\; \varphi^n = \mathbf{1},\ \rho^2 = \mathbf{1},\ \rho\circ\varphi = \varphi^{n-1}\circ\rho \rangle.$$

Astrattamente parlando, $\boldsymbol{D}_n$ è un gruppo generato da due simboli ρ, φ, verificanti le tre relazioni sopra indicate. $\boldsymbol{D}_n$ non è ovviamente abeliano.

Concludiamo il paragrafo esaminando la struttura dei tre gruppi diedrali $\boldsymbol{D}_3$, $\boldsymbol{D}_4$, $\boldsymbol{D}_5$ [mentre per $\boldsymbol{D}_6$ si rinvia al paragrafo successivo].

(**1**) $|\boldsymbol{D}_3| = 6 = |\boldsymbol{S}_3|$. Dunque $\boldsymbol{D}_3 = \boldsymbol{S}_3$.

(**2**) $|\boldsymbol{D}_4| = 8 < |\boldsymbol{S}_4| = 24$. Dunque $\boldsymbol{D}_4 < \boldsymbol{S}_4$. Gli otto elementi di $\boldsymbol{D}_4$ sono:

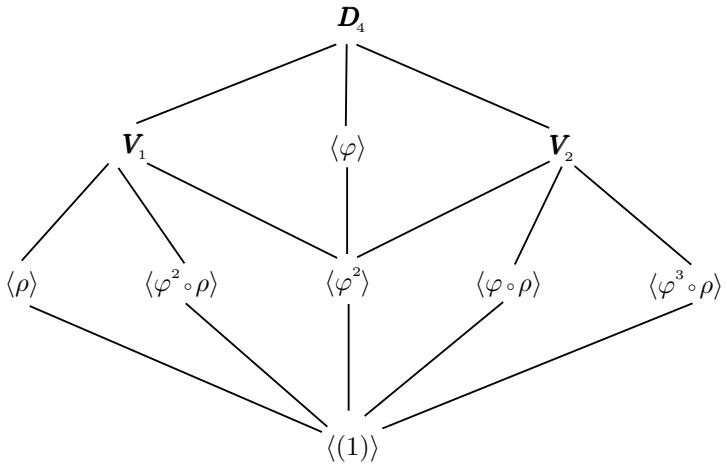
$\mathbf{1} = (1)$, $\rho = (2\,4)$
$\varphi = (1\,2\,3\,4)$, $\varphi\circ\rho = \rho\varphi = (2\,4)(1\,2\,3\,4) = (1\,2)(3\,4)$,
$\varphi^2 = (1\,3)(2\,4)$, $\varphi^2\circ\rho = \rho\varphi^2 = (2\,4)(1\,3)(2\,4) = (1\,3)$,
$\varphi^3 = (1\,4\,3\,2)$, $\varphi^3\circ\rho = \rho\varphi^3 = (2\,4)(1\,4\,3\,2) = (1\,4)(2\,3)$.

Con semplici calcoli (che si basano sulle tre relazioni di $\boldsymbol{D}_4$, cioè $\varphi^4 = \mathbf{1}$, $\rho^2 = \mathbf{1}$, $\rho\circ\varphi = \varphi^3\circ\rho$), si ottiene la tavola moltiplicativa di $\boldsymbol{D}_4$:

$\cdot$	$\mathbf{1}$	φ	φ^2	φ^3	ρ	$\varphi\circ\rho$	$\varphi^2\circ\rho$	$\varphi^3\circ\rho$
$\mathbf{1}$	$\mathbf{1}$	φ	φ^2	φ^3	ρ	$\varphi\circ\rho$	$\varphi^2\circ\rho$	$\varphi^3\circ\rho$
φ	φ	φ^2	φ^3	$\mathbf{1}$	$\varphi\circ\rho$	$\varphi^2\circ\rho$	$\varphi^3\circ\rho$	ρ
φ^2	φ^2	φ^3	$\mathbf{1}$	φ	$\varphi^2\circ\rho$	$\varphi^3\circ\rho$	ρ	$\varphi\circ\rho$
φ^3	φ^3	$\mathbf{1}$	φ	φ^2	$\varphi^3\circ\rho$	ρ	$\varphi\circ\rho$	$\varphi^2\circ\rho$
ρ	ρ	$\varphi^3\circ\rho$	$\varphi^2\circ\rho$	$\varphi\circ\rho$	$\mathbf{1}$	φ^3	φ^2	φ
$\varphi\circ\rho$	$\varphi\circ\rho$	ρ	$\varphi^3\circ\rho$	$\varphi^2\circ\rho$	φ	$\mathbf{1}$	φ^3	φ^2
$\varphi^2\circ\rho$	$\varphi^2\circ\rho$	$\varphi\circ\rho$	ρ	$\varphi^3\circ\rho$	φ^2	φ	$\mathbf{1}$	φ^3
$\varphi^3\circ\rho$	$\varphi^3\circ\rho$	$\varphi^2\circ\rho$	$\varphi\circ\rho$	ρ	φ^3	φ^2	φ	$\mathbf{1}$

Si noti che in $\boldsymbol{D}_4$ ci sono cinque elementi di periodo 2 [cioè φ^2, ρ, $\varphi\circ\rho$, $\varphi^2\circ\rho$, $\varphi^3\circ\rho$] e due elementi di periodo 4 [cioè φ, φ^3]. Osserviamo quindi che:

- $\langle\,\varphi\,\rangle$ è un sottogruppo ciclico di ordine 4.
- $\langle\,\rho\,\rangle$, $\langle\,\varphi^2\,\rangle$, $\langle\,\varphi\circ\rho\,\rangle$, $\langle\,\varphi^2\circ\rho\,\rangle$, $\varphi^3\circ\rho\,\rangle$ sono sottogruppi ciclici di ordine 2.
- $\boldsymbol{V}_1 = \{\mathbf{1}, \varphi^2, \rho, \varphi^2\circ\rho\}$ e $\boldsymbol{V}_2 = \{\mathbf{1}, \varphi^2, \varphi\circ\rho, \varphi^3\circ\rho\}$ sono due sottogruppi di Klein [per ottenerli basta determinare tutte le coppie di riflessioni che commutano tra loro e considerarne il sttogruppo generato]. Si ottiene il seguente reticolo di sottogruppi di $\boldsymbol{D}_4$:



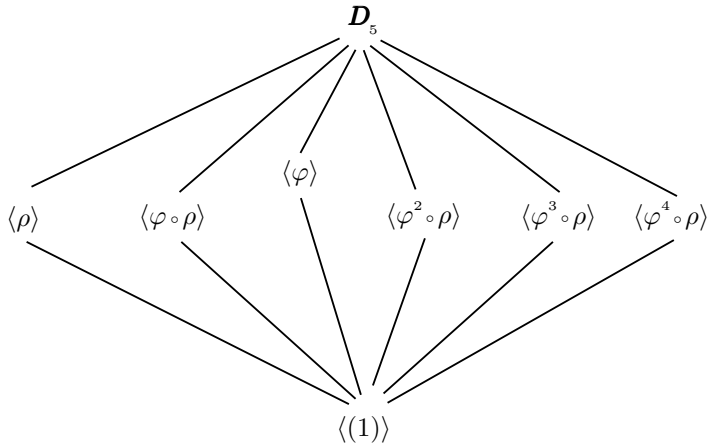
Si noti che le nostre attuali conoscenze non ci consentono di escludere a priori l'esistenza di altri sottogruppi di $\boldsymbol{D}_4$. Per poterlo fare occorrono i risultati del prossimo paragrafo (cfr. **Teor. 5.1**).

(**3**) $|\boldsymbol{D}_5| = 10 < |\boldsymbol{S}_5| = 120$. I dieci elementi di $\boldsymbol{D}_5$ sono:

$$\begin{array}{ll} \mathbf{1} = (1), & \rho = (2\,5)(3\,4), \\ \varphi = (1\,2\,3\,4\,5), & \varphi\circ\rho = \rho\varphi = (1\,2)(3\,5), \\ \varphi^2 = (1\,3\,5\,2\,4), & \varphi^2\circ\rho = \rho\varphi^2 = (1\,3)(4\,5), \\ \varphi^3 = (1\,4\,2\,5\,3), & \varphi^3\circ\rho = \rho\varphi^3 = (1\,4)(2\,3), \\ \varphi^4 = (1\,5\,4\,3\,2), & \varphi^4\circ\rho = \rho\varphi^4 = (1\,5)(2\,4). \end{array}$$

$\boldsymbol{D}_5$ ha quattro elementi di periodo 5 [cioè le rotazioni φ, φ^2, φ^3, φ^4] e cinque elementi di periodo 2 [cioè le riflessioni ρ, $\varphi\circ\rho$, $\varphi^2\circ\rho$, $\varphi^3\circ\rho$, $\varphi^4\circ\rho$]. Quindi $\boldsymbol{D}_5$ ha un sottogruppo ciclico di ordine 5 [cioè $\langle\,\varphi\,\rangle$] e cinque sottogruppi ciclici di ordine 2 [uno per ciascun elemento di periodo 2].

Perché $\boldsymbol{D}_5$ non ha altri sottogruppi? Anche per rispondere a questa domanda occorrono i risultati del prossimo paragrafo. Il reticolo dei sottogruppi di $\boldsymbol{D}_5$ è il seguente:



5. Classi laterali e teorema di Lagrange

Definizione 1. *Sia $(G,\cdot)$ un gruppo e sia H un sottogruppo di G. Per ogni $a \in G$, l'insieme*

$$Ha := \{ha,\ \forall\, h \in H\}$$

è detto laterale destro di a modulo H o (classe laterale destra di a modulo H). Se G ha struttura additiva, il laterale destro di a modulo H è l'insieme $H + a = \{h + a,\ \forall\, h \in H\}$.

Osservazione 1. (i) Si noti che

$$Ha = H \iff a \in H.$$

Se infatti $Ha = H$, allora $a = 1 \cdot a \in H$. Viceversa, se $a \in H$, allora: $Ha \subseteq H$ [in quanto $ha \in H,\ \forall\, h \in H$] e $H \subseteq Ha$ [in quanto $h = (ha^{-1})\, a \in Ha,\ \forall\, h \in H$].

(ii) Se $a \notin H$, Ha non è mai un sottogruppo di G. Infatti si ha: $1 \notin Ha$ [se per assurdo $1 \in Ha$, allora $1 = ha$, $\exists\, h \in H$, e dunque $a = h^{-1} \in H$: assurdo].

Lemma 1. $Ha = Hb \iff ab^{-1} \in H$.

Dim. ($\Longrightarrow$). Risulta: $a = 1 \cdot a = hb$, $\exists\, h \in H$. Dunque $ab^{-1} = h \in H$.

($\Longleftarrow$). Posto $h_1 := ab^{-1} \in H$, risulta: $a = a(b^{-1}b) = (ab^{-1})b = h_1 b$, cioè $a = h_1 b$ e quindi $b = h_1^{-1} a$. Per ogni $h \in H$, si ha $\begin{cases} ha = hh_1 b \in Hb \text{ e quindi } Ha \subseteq Hb, \\ hb = h(h_1^{-1} a) = (hh_1^{-1})\, a \in Ha \text{ e quindi } Hb \subseteq Ha. \end{cases}$

Nota. Si verifica immediatamente che $ab^{-1} \in H \iff a \in Hb \iff b \in Ha$.

Lemma 2. $Ha \neq Hb \implies Ha \cap Hb = \emptyset$.

Dim. Per assurdo, $\exists\, g \in G$ tale che $g = h_1 a = h_2 b$, con $h_1, h_2 \in H$. Da $h_1 a = h_2 b$ segue $h_2 = h_1 ab^{-1}$ e quindi $h_1^{-1} h_2 = ab^{-1}$. Pertanto $ab^{-1} \in H$. Dal **Lemma 1** segue allora che $Ha = Hb$, contro l'ipotesi.

Proposizione 1. *La famiglia $\mathfrak{L}_d(H)$ di tutti i laterali destri di G modulo H (a due a due distinti) è una partizione di G.*

Dim. Sia $\mathfrak{L}_d(H) = \{Ha_t,\ t \in I\}$ la famiglia di tutti i laterali destri modulo H, a due a due distinti. Ovviamente $\mathfrak{L}_d(H)$ è un ricoprimento di G [infatti, $\forall\, g \in G$, $g = 1 \cdot g \in Hg = Ha_t$, $\exists\, t \in I$]. Dal **Lemma 2** segue che $\mathfrak{L}_d(H)$ è una partizione di G.

Teorema 1. (*Teorema di Lagrange*). *Sia G un gruppo finito. Per ogni sottogruppo H di G, risulta: $|H| \,\big|\, |G|$ [cioè "l'ordine di un sottogruppo è un divisore dell'ordine del gruppo"].*

Dim. Se G è un gruppo finito, ogni suo sottogruppo H è finito ed è finito anche il numero dei suoi laterali destri. Inoltre tutti i laterali destri hanno la stessa cardinalità: infatti, $\forall\, a \in G$, l'applicazione

$$\varphi : H \to Ha \text{ tale che } \varphi(h) = ha,\ \forall\, h \in H,$$

è biiettiva (cfr. **Osserv. 1.1**(i)). Posto Allora $|G| = n$, $|H| = m$, $\mathfrak{L}_d(H) = \{Ha_1,\ \ldots\ , Ha_i\}$ (con $i = |\mathfrak{L}_d(H)|$), risulta:

$$n = \sum_{t=1}^{i} |Ha_t| = \sum_{t=1}^{i} |H| = mi,$$

cioè $n = mi$. Dunque $m \,|\, n$, cioè $|H| \,|\, |G|$.

Definizione 2. *Assegnati un gruppo G (anche infinito) ed un suo sottogruppo H, la cardinalità $i = |\mathfrak{L}_d(H)|$ è detta indice di H in G ed è usualmente denotata $(G : H)$.*

Dal teorema precedente segue che, se G è finito, $(G : H)$ è finito ed è un divisore di $|G|$.

Esaminiamo alcune importanti conseguenze del teorema di Lagrange.

Corollario 1. *Se G è finito, $\circ(a) \,|\, |G|$, $\forall\, a \in G$.*
Se in particolare $|G| = p$ è un numero primo, allora $G \cong \boldsymbol{C}_p$ (gruppo ciclico di ordine p) ed è privo di sottogruppi propri.

Dim. Risulta: $\circ(a) = |\langle a \rangle| \,|\, |G|$.

Se $|G| = p$ e $a \neq 1$, allora $\circ(a) = p$. Dunque G è ciclico. Dal teorema di Lagrange segue subito che G non ha sottogruppi $\neq \{1\}, G$.

Corollario 2. *Se $(G, \cdot)$ è finito, $a^{|G|} = 1$, $\forall\, a \in G$. [In struttura additiva, $|G|\, a = 0$, $\forall\, a \in G$].*

Dim. Dal **Cor. 1**, $\circ(a) \,|\, |G|$. Poiché $a^{\circ(a)} = 1$, allora $a^{|G|} = 1$.

Corollario 3. [*Ri-dimostrazione del Teorema di Eulero-Fermat*, cfr. **Cap. II**,**Teor. 6.2**]. *Sia $n \geq 2$. Per ogni $a \in \boldsymbol{Z}$, con $(a, n) = 1$, risulta:*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dim. È noto (cfr. **Cap. II**, **Osserv. 6.3**) che $\mathcal{U}(\boldsymbol{Z}_n)$ è un gruppo di ordine $\varphi(n)$. Essendo $(a, n) = 1$, allora $\overline{a} \in \mathcal{U}(\boldsymbol{Z}_n)$. Dal precedente **Cor. 2**,

$$\overline{a}^{\varphi(n)} = \overline{1}, \text{ cioè } \overline{a^{\varphi(n)}} = \overline{1} \text{ e quindi } a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Corollario 4. *A meno di isomorfismi, esistono soltanto due gruppi di ordine 4: il gruppo ciclico $\boldsymbol{C}_4$ ed il gruppo di Klein $\boldsymbol{V}$.*

Dim. Sia $(G, \cdot)$ un gruppo di ordine 4. Poniamo $G = \{1, a, b, c\}$. In base al **Cor. 1**, i tre elementi a, b, c possono avere periodo 2 oppure 4. Se almeno uno dei tre elementi ha periodo 4, $G \cong \boldsymbol{C}_4$.

Assumiamo quindi che $\circ(a) = \circ(b) = \circ(c) = 2$ e valutiamo il prodotto ab. Risulta:

- $ab \neq 1$ [altrimenti $ab = 1 = a^2$ e quindi, semplificando, $b = a$: assurdo];
- $ab \neq a$ [altrimenti, semplificando, $b = 1$: assurdo];
- $ab \neq b$ [altrimenti, semplificando, $a = 1$: assurdo].

Si conclude che $ab = c$. In modo analogo si verifica che anche $ba = c$ ed inoltre che $ac = ca = b$, $bc = cb = a$.

G ha esattamente la stessa tavola moltiplicativa del gruppo di Klein $\boldsymbol{V}$ (cfr. **4.(A)**): dunque $G \cong \boldsymbol{V}$.

Nota. Si osservi che il prodotto diretto $\boldsymbol{Z}_2 \times \boldsymbol{Z}_2$ è isomorfo a $\boldsymbol{V}$ [infatti non ha elementi di periodo 4 e quindi non è ciclico].

Corollario 5. *Se K è un campo finito, il suo gruppo moltiplicativo $(K^{\cdot}, \cdot)$ è ciclico.*

Dim. Tenuto conto della Nota al termine della dimostrazione di **Prop. 2.3**, basta dimostrare che, se $t \geq 1$ e $t \,|\, |K^{\cdot}|$, esiste al più un solo sottogruppo di $K^{\cdot}$ di ordine t.

Sia infatti $H \leq K^{\cdot}$, $|H| = t$. Per ogni $x \in H$, $\circ(x) \,|\, t$ e dunque (dal **Cor. 1**) $x^t = 1$. Allora x è uno zero del polinomio $P = X^t - 1 \in K[X]$. In base al teorema di Ruffini, in K esistono al più

t zeri di P e tali elementi sono tutti in H. Se ora H_1 è un altro sottogruppo di $K^\cdot$ di ordine t, poiché i suoi elementi sono zeri di P, appartengono a H. Ne segue che $H_1 \subseteq H$ e dunque $H_1 = H$.

Alla partizione $\mathfrak{L}_d(H)$ di G resta associata la relazione di equivalenza ρ_d così definita: $\forall\, a,\, b \in G$,

$$a\,\rho_d\,b \iff a,\, b \in Hg,\ \exists\, g \in G.$$

Lemma 3. *Siano $a, b \in G$. Risulta:*

$$a\,\rho_d\,b \iff a\,b^{-1} \in H \ \ [\iff Ha = Hb\,].$$

Ne segue che $[a]_{\rho_d} = Ha,\ \forall\, a \in G$.

Dim. Dalla Nota di **Lemma 1** segue che

$$a\,\rho_d\,b \iff a, b \in Hg,\, \exists\, g \in G \iff Ha = Hg = Hb \iff Ha = Hb.$$

Quindi, dal **Lemma 2** $a\,\rho_d\,b \iff ab^{-1} \in H$.

La classe di equivalenza $[a]_{\rho_d}$ è la classe laterale destra contenente a, cioè Ha. Dunque $[a]_{\rho_d} = Ha$. Tale uguaglianza può comunque essere verificata direttamente. Infatti:

$$[a]_{\rho_d} = \{b \in G : a\,\rho_d\,b\} = \{b \in G : ab^{-1} \in H\} = \{b \in G : b \in Ha\} = Ha$$

Segue dal lemma precedente che l'insieme quoziente $G/_{\rho_d}$ coincide con la famiglia $\mathfrak{L}_d(H)$ dei laterali destri di G. Da ciò segue che $(G : H) = \left|G/_{\rho_d}\right|$.

Definizione 3. *Per ogni $a \in G$, l'insieme*

$$aH := \{ah,\ \forall\, h \in H\}$$

è detto laterale sinistro di a modulo H (o classe laterale sinistra di a modulo H).

Si dimostra, in modo del tutto analogo a quanto fatto sopra, che:

- $aH = bH \iff a^{-1}b \in H$.
- $\mathfrak{L}_s(H) = \left\{aH,\ \forall\, a \in G\right\}$ è una partizione di G.
- se ρ_s è la relazione di equivalenza associata a tale partizione, risulta: $a\,\rho_s\,b \iff a^{-1}b \in H$.
- $G/_{\rho_s} = \mathfrak{L}_s(H)$.

Osservazione 2. (*i*) Verifichiamo su un esempio che in generale $\rho_s \neq \rho_d$.

Si scelga $G = \boldsymbol{S}_3$, $H = \langle\,(1\,2)\,\rangle = \{(1),\,(1\,2)\}$. I tre laterali destri mod H sono

$$H = \{(1),\,(1\,2)\},\quad H(1\,3) = \{(1\,3),\,(1\,2\,3)\},\quad H(2\,3) = \{(2\,3),\,(1\,3\,2)\},$$

mentre i tre laterali sinistri mod H sono

$$H = \{(1),\,(1\,2)\},\quad (1\,3)H = \{(1\,3),\,(1\,3\,2)\},\quad (2\,3)H = \{(2\,3),\,(1\,2\,3)\}.$$

Come si vede, $H(1\,3) \neq (1\,3)H$ (e analogamente $H(2\,3) \neq (2\,3)H$). Ne segue che $\rho_s \neq \rho_d$: infatti $(1\,3)\rho_d(1\,2\,3)$ mentre $(1\,3)\not\rho_s(1\,2\,3)$.

(*ii*) Anche se $\rho_s \neq \rho_d$, è comunque vero che $\left|G/_{\rho_d}\right| = \left|G/_{\rho_s}\right|$, cioè che il numero dei laterali destri [che è l'indice $(G : H)$] coincide con il numero dei laterali sinistri. Si consideri infatti l'applicazione

$$\varphi : G/_{\rho_d} \to G/_{\rho_s} \quad \text{tale che } \varphi(Ha) = a^{-1}H,\ \ \forall\, Ha \in G/_{\rho_d}.$$

Tale applicazione è ben definita. Infatti

$$Ha = Ha_1 \implies Ha\,a_1^{-1} = H \implies aa_1^{-1} \in H \implies aa_1^{-1}H = H \implies a_1^{-1}H = a^{-1}H.$$

Inoltre è biiettiva, in quanto ha per inversa l'applicazione (anch'essa ben definita)

$$\psi : G/_{\rho_s} \to G/_{\rho_d} \quad \text{tale che } \psi(bH) = H\,b^{-1},\ \ \forall\, bH \in G/_{\rho_s}.$$

(*iii*) Se G è abeliano ed H è un suo sottogruppo, risulta sempre $\rho_s = \rho_d$. Infatti, essendo G abeliano:

$$a\,\rho_s\,b \iff a^{-1}b \in H \iff b\,a^{-1} \in H \iff (b\,a^{-1})^{-1} \in H \iff a\,b^{-1} \in H \iff a\,\rho_d\,b.$$

Ci chiediamo in quali circostanze valga la condizione $\rho_s = \rho_d$. Vale il seguente risultato.

Proposizione 2. *Sia $H \leq G$. Si ha:*

$$\rho_s = \rho_d \iff Ha = aH,\ \forall\, a \in G.$$

Dim. ($\Longrightarrow$). Bisogna verificare che $Ha \subseteq aH \subseteq Ha,\ \forall\, a \in G$.

Si ha, $\forall\, h \in H$: $ha\,\rho_d\,a$ [infatti $ha\,a^{-1} = h \in H$] e quindi $ha\,\rho_s\,a$, cioè $haH = aH$. In particolare, $ha1 = ha \in aH$. Dunque è provato che $Ha \subseteq aH$.

Viceversa, $\forall\, h \in H$: $ah\,\rho_s\,a$ [infatti $(ah)^{-1}a = h^{-1}a^{-1}a = h^{-1} \in H$] e quindi $ah\,\rho_d\,a$, cioè $Hah = Ha$. In particolare, $1ah = ah \in Ha$. Dunque è provato che $aH \subseteq Ha$.

($\Longleftarrow$). Bisogna verificare che, $\forall\, a, b \in G$: $a\,\rho_s\,b \iff a\,\rho_d\,b$, ovvero che $aH = bH \iff Ha = Hb$. Ciò segue immediatamente dall'ipotesi ($Ha = aH$ e $Hb = bH$).

Definizione 4. *Sia $H \leq G$. H è detto sottogruppo normale di G se $\rho_s = \rho_d$ (cioè $Ha = aH,\ \forall\, a \in G$). Si scrive $H \trianglelefteq G$.*

Osservazione 3. (*i*) Abbiamo già dimostrato (cfr. **Osserv. 2**(*iii*)) che in un gruppo abeliano ogni sottogruppo è normale. Un esempio di sottogruppo non normale è invece il sottogruppo $H = \langle\,(1\,2)\,\rangle$ di $\boldsymbol{S}_3$. Infatti $H \not\trianglelefteq \boldsymbol{S}_3$ (cfr. **Osserv. 2**(*i*)).

(*ii*) Ogni sottogruppo di indice 2 è normale. Sia infatti $H \leq G$, con $(G : H) = 2$. Si ha:

$$G\big/_{\rho_d} = \big\{H,\, Ha\big\}, \quad G\big/_{\rho_s} = \big\{H,\, aH\big\},\ \text{con}\ a \in G - H.$$

Allora $G = H \sqcup Ha = H \sqcup aH$ e quindi $Ha = G - H = aH$. Quindi $Ha = aH,\ \forall\, a \in G - H$.

Se infine $a \in H$, ovviamente $Ha = H = aH$. Dalla **Prop. 2** segue che $\rho_s = \rho_d$.

Nota. Per ogni $n \geq 2$, $\boldsymbol{A}_n \trianglelefteq \boldsymbol{S}_n$ [infatti si verifica subito che $(\boldsymbol{S}_n : \boldsymbol{A}_n) = 2$)].

(*iii*) Per verificare se un sottogruppo è normale, conviene utilizzare il seguente risultato:

($*$) *se $Ha \subseteq aH,\ \forall\, a \in G$, allora $Ha = aH,\ \forall\, a \in G$.*

Per dimostrare ($*$) basta verificare che anche $aH \subseteq Ha,\ \forall\, a \in G$.

Sia $h \in H$. Per ipotesi, $Ha^{-1} \subseteq a^{-1}H$. In particolare quindi $h^{-1}a^{-1} = a^{-1}h_1,\ \exists\, h_1 \in H$. Dunque si ha: $ah = ((ah)^{-1})^{-1} = (h^{-1}a^{-1})^{-1} = (a^{-1}h_1)^{-1} = h_1^{-1}a \in Ha$.

Nota. La condizione $Ha \subseteq aH$ di ($*$) può essere ovviamente sostituita da $aH \subseteq Ha$.

(*iv*) Sia $H \leq G$. Si verifica facilmente che

$$H \trianglelefteq G \iff \forall\, h \in H,\, [h]_{\sim} \subseteq H$$

(cioè tutta la classe di coniugio di ogni elemento di H è contenuta in H). Infatti
($\Longrightarrow$) $\forall\, xhx^{-1} \in [h]_{\sim}$, da $xH = Hx$ segue $xh = h_1x$ ($\exists\, h_1 \in H$). Pertanto $xhx^{-1} \in H$.
($\Longleftarrow$) Bisogna verificare che $Hx \subseteq xH,\ \forall\, x \in G$. Sia $h \in H$. Poiché $x^{-1}hx \in [h]_{\sim} \subseteq H$, allora $x^{-1}hx = h_1,\ \exists\, h_1 \in H$. Dunque $hx = xh_1 \in xH$ e pertanto $Hx \subseteq xH$.

(*v*) Risulta infine: $H \trianglelefteq G \iff xHx^{-1} = H,\ \forall\, x \in G$.
Infatti si verifica subito che $xHx^{-1} = H \iff xH = Hx$.

Osservazione 4. Sia G un gruppo finito di ordine n. Se $m > 1$ ed $m \,\big|\, n$, non è detto che G ammetta un sottogruppo H di ordine m. Ad esempio verificheremo, nell'**Esercizio 1** in conclusione di questo paragrafo, che il gruppo alterno $\boldsymbol{A}_4$ (che è di ordine 12) non ammette alcun sottogruppo di ordine 6. Il teorema di Lagrange non dà quindi indicazioni sull'esistenza di sottogruppi di un gruppo finito; dà invece indicazioni sulla non esistenza di sottogruppi. Ad esempio, se torniamo alla conclusione del paragrafo precedente, ci permette di affermare che in $\boldsymbol{D}_5$ (di ordine 10) non esistono sottogruppi propri di ordini $\neq 2, 5$.

Altri più raffinati risultati (ad esempio teoremi dovuti a Cauchy ed a Sylow) danno invece indicazioni sull'esistenza di sottogruppi di un gruppo finito.

Come applicazione del teorema di Lagrange, determineremo:

(***A***) tutti i gruppi di ordine 6.
(***B***) il reticolo dei sottogruppi di $\boldsymbol{D}_6$.
(***C***) tutti i gruppi di ordine 8.

(***A***) Gruppi di ordine 6

Sia $(G,\cdot)$ un gruppo di ordine 6. Dal teorema di Lagrange segue che, $\forall\, g \in G,\ g \neq 1$, risulta $\circ(g) = 2, 3, 6$.

Se $\exists\, g \in G$ tale che $\circ(g) = 6$, allora $G \cong \boldsymbol{C}_6$ (gruppo ciclico di ordine 6). Assumiamo quindi che $G \ncong \boldsymbol{C}_6$. In tal caso $\circ(g) = 2, 3$. Esistono due possibilità:

$$(*)\ \exists\, a \in G \text{ tale che } \circ(a) = 3; \qquad (**)\ \nexists\, a \in G \text{ tale che } \circ(a) = 3.$$

Nel caso $(*)$, $G \ni 1,\ a,\ a^2\ (a^3 = 1)$, con $\circ(a^2) = 3$. Sia allora b un ulteriore elemento di G ed assumiamo, per assurdo, che $\circ(b) = 3$. Allora

$$G \ni 1,\ a,\ a^2,\ b,\ b^2,\ ab,\ a^2b.$$

I primi quattro elementi, come sappiamo, sono a due a due distinti. Cosa possiamo dire per gli altri tre? Si ha:

$b^2 \neq 1,\ a,\ a^2,\ b$ [se fosse $b^2 = a$, allora $b = b^4 = a^2$; se fosse $b^2 = a^2$, allora $b = b^4 = a^4 = a$];

$ab \neq 1,\ a,\ a^2,\ b,\ b^2$ [in base alla legge di cancellazione];

$a^2b \neq 1,\ a,\ a^2,\ b,\ b^2,\ ab$ [sempre in base alla legge di cancellazione].

Ma allora $|G| \geq 7$: assurdo.

Necessariamente allora $\circ(b) = 2$. In tal caso:

$$G \ni 1,\ a,\ a^2,\ b,\ ab,\ a^2b.$$

Per la legge di cancellazione, $ab \neq 1,\ a,\ a^2,\ b$ e $a^2b \neq 1,\ a,\ a^2,\ b,\ ab$. I sei elementi di G sopra considerati sono quindi a due a due distinti e "riempiono" tutto G.

Consideriamo in G il prodotto ba. Si ha $ba \neq 1,\ a,\ a^2,\ b$ [per la legge di cancellazione]. Inoltre $ba \neq ab$ [se no si avrebbe $\circ(ab) > 3$, in quanto

$$(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = a^2b^2 = a^2 \neq 1; \quad (ab)^3 = (ab)^2(ab) = a^2ab = b \neq 1].$$

Quindi necessariamente $ba = a^2b$. Da ciò segue poi che $ba^2 = ab$ [infatti $ba^2 = (ba)a = (a^2b)a = a^2(ba) = a^2(a^2b) = a^4b = ab$].

Si conclude che

$$G = \langle a,\ b \mid a^3 = b^2 = 1,\ ba = a^2b \rangle.$$

Dunque G è un gruppo generato dai due simboli a, b verificanti le tre relazioni scritte sopra. Ricordata la definizione di gruppo diedrale (data nel precedente paragrafo) si conclude che $G \cong \boldsymbol{D}_3 = \boldsymbol{S}_3$. Un isomorfismo tra G ed $\boldsymbol{S}_3$ è ottenuto ponendo, ad esempio,

$$\varphi : G \to \boldsymbol{S}_3 \text{ tale che } \varphi(1) = (1),\ \varphi(a) = (1\,2\,3),\ \varphi(b) = (2\,3),$$

ed estendendo poi φ a tutti i restanti elementi di G, in modo che sia un omomorfismo.

Nel caso $(**)$, $\nexists\, a \in G$ tale che $\circ(a) = 3$ e dunque $\circ(a) = 2,\ \forall\, a \in G,\ a \neq 1$.

Se $G \ni 1,\ a,\ b$ [elementi a due a due distinti, con $a^2 = b^2 = 1$], allora $ab \neq 1,\ a,\ b$ [in base alla legge di cancellazione] e dunque $G \ni 1,\ a,\ b,\ ab$.

Si noti che $ab = ba$ [infatti $(ab)(ba) = ab^2a = a^2 = 1$ e dunque $ba = (ab)^{-1}$; poiché $\circ(ab) = 2$, allora $(ab)^{-1} = ab$ e dunque $ba = ab$].

Ne segue che G contiene un ulteriore elemento c (con $c^2 = 1$). Si noti che $ac \neq 1,\ a,\ c,\ ab$. Inoltre $ac \neq b$ [altrimenti $ac = b = a^2b = a(ab)$ e quindi $c = ab$: assurdo]. Dunque

$$G = \{1,\ a,\ b,\ c,\ ab,\ ac\}.$$

Consideriamo ora in G il prodotto bc. Si ha:

$bc \neq 1,\ b,\ ab,\ c,\ ac$ [in base alla legge di cancellazione];
$bc \neq a$ [altrimenti $bc = a = b^2a = b(ab) \implies c = ab$: assurdo].

Dunque bc è un ulteriore elemento di G e pertanto $|G| \geq 7$: assurdo. Il caso (**) non può quindi verificarsi.

Possiamo concludere che, se $|G| = 6$, allora $G \cong \boldsymbol{C}_6$ oppure $G \cong \boldsymbol{S}_3$.

(*B*) Il reticolo dei sottogruppi di $\boldsymbol{D}_6$

Si ha:

$$\boldsymbol{D}_6 = \langle \varphi, \rho \mid \varphi^6 = \mathbf{1},\ \rho^2 = \mathbf{1},\ \rho\circ\varphi = \varphi^5\circ\rho \rangle = \{\mathbf{1}, \varphi, \varphi^2, \varphi^3, \varphi^4, \varphi^5, \rho, \varphi\circ\rho, \varphi^2\circ\rho, \varphi^3\circ\rho, \varphi^4\circ\rho, \varphi^5\circ\rho\}$$

La relazione diedrale $\rho\circ\varphi = \varphi^5\circ\rho$ implica $\rho\circ\varphi^k = \varphi^{6-k}\circ\rho$ $(1 \leq k \leq 6)$. Gli undici elementi $\neq \mathbf{1}$ hanno i seguenti periodi:

i sette elementi $\varphi^3,\ \rho,\ \varphi\circ\rho,\ \varphi^2\circ\rho,\ \varphi^3\circ\rho,\ \varphi^4\circ\rho,\ \varphi^5\circ\rho$ hanno periodo 2;

i due elementi $\varphi^2,\ \varphi^4$ hanno periodo 3;

i due elementi $\varphi,\ \varphi^5$ hanno periodo 6.

[Ad esempio, $\circ(\varphi^2\circ\rho) = 2$ perché $(\varphi^2\circ\rho)\circ(\varphi^2\circ\rho) = \varphi^2\circ(\rho\circ\varphi^2)\circ\rho = \varphi^2\circ(\varphi^4\circ\rho)\circ\rho = \varphi^6\circ\rho^2 = \mathbf{1}$, ecc.].

Poiché $|\boldsymbol{D}_6| = 12$, dal teorema di Lagrange segue che $\boldsymbol{D}_6$ *può* ammettere sottogruppi di ordine 2, 3, 4, 6.

- Relativamente ai sottogruppi di ordine 2 (che sono ciclici), basta osservare che essi sono in corrispondenza biunivoca con gli elementi di periodo 2. Si hanno quindi sette sottogruppi:

$$\langle \varphi^3 \rangle,\ \langle \rho \rangle,\ \langle \varphi\circ\rho \rangle,\ \langle \varphi^2\circ\rho \rangle,\ \langle \varphi^3\circ\rho \rangle,\ \langle \varphi^4\circ\rho \rangle,\ \langle \varphi^5\circ\rho \rangle.$$

- Relativamente ai sottogruppi di ordine 3 (che sono ciclici), basta osservare che ciascuno di essi deve contenere due elementi di periodo 3. Esaminando i periodi, si conclude che

$$\langle \varphi^2 \rangle = \{\mathbf{1}, \varphi^2, \varphi^4\}$$

è l'unico sottogruppo di ordine 3.

- Relativamente ai sottogruppi di ordine 4 (che sono ciclici o di Klein), osserviamo subito che non possono esistere sottogruppi ciclici [perché non esistono elementi di periodo 4]. Invece esistono esattamente tre sottogruppi di Klein:

$$\boldsymbol{V}_1 = \langle \rho, \varphi^3\circ\rho \rangle = \{\mathbf{1}, \varphi^3, \rho, \varphi^3\circ\rho\},$$
$$\boldsymbol{V}_2 = \langle \varphi\circ\rho, \varphi^4\circ\rho \rangle = \{\mathbf{1}, \varphi^3, \varphi\circ\rho, \varphi^4\circ\rho\},$$
$$\boldsymbol{V}_3 = \langle \varphi^2\circ\rho, \varphi^5\circ\rho \rangle = \{\mathbf{1}, \varphi^3, \varphi^2\circ\rho, \varphi^5\circ\rho\}.$$

[Non ne esistono altri: infatti ρ commuta soltanto con $\varphi^3\circ\rho$ (e con φ^3), $\varphi\circ\rho$ commuta soltanto con $\varphi^4\circ\rho$ (e con φ^3), ecc.].

- Relativamente ai sottogruppi di ordine 6 (che sono il gruppo ciclico $\boldsymbol{C}_6$ o $\boldsymbol{S}_3$), si osservi che esiste esattamente un ciclico $\boldsymbol{C}_6$:

$$\langle \varphi \rangle = \langle \varphi^5 \rangle = \{\mathbf{1}, \varphi, \varphi^2, \varphi^3, \varphi^4, \varphi^5\}$$

[perché esistono due soli elementi di periodo 6]. Esistono inoltre due sottogruppi $\cong \boldsymbol{S}_3$. Si tratta di

$$\boldsymbol{\Sigma}_1 = \langle \varphi^2, \rho \rangle = \{\mathbf{1}, \varphi^2, \varphi^4, \rho, \varphi^2\circ\rho, \varphi^4\circ\rho\},$$
$$\boldsymbol{\Sigma}_2 = \langle \varphi^2, \varphi\circ\rho \rangle = \{\mathbf{1}, \varphi^2, \varphi^4, \varphi\circ\rho, \varphi^3\circ\rho, \varphi^5\circ\rho\}.$$

Perché in $\boldsymbol{D}_6$ non esistono altri sottogruppi $\boldsymbol{\Sigma} \cong \boldsymbol{S}_3$? Osserviamo che $\varphi,\ \varphi^5 \notin \boldsymbol{\Sigma}$ [per ragioni di periodo] e che anche $\varphi^3 \notin \boldsymbol{\Sigma}$ [infatti si osserva che φ^3 commuta con ogni elemento di $\boldsymbol{D}_6$, mentre in $\boldsymbol{S}_3$ gli elementi di periodo 2 non commutano tra loro]. Un eventuale nuovo sottogruppo $\boldsymbol{\Sigma}$ dovrebbe contenere almeno una riflessione tra $\{\rho, \varphi^2\circ\rho, \varphi^4\circ\rho\}$ ed una tra $\{\varphi\circ\rho, \varphi^3\circ\rho, \varphi^5\circ\rho\}$. Moltiplicando tra loro tali riflessioni si ottiene una contraddizione (del tipo $\varphi,\ \varphi^3,\ \varphi^5 \in \boldsymbol{\Sigma}$).

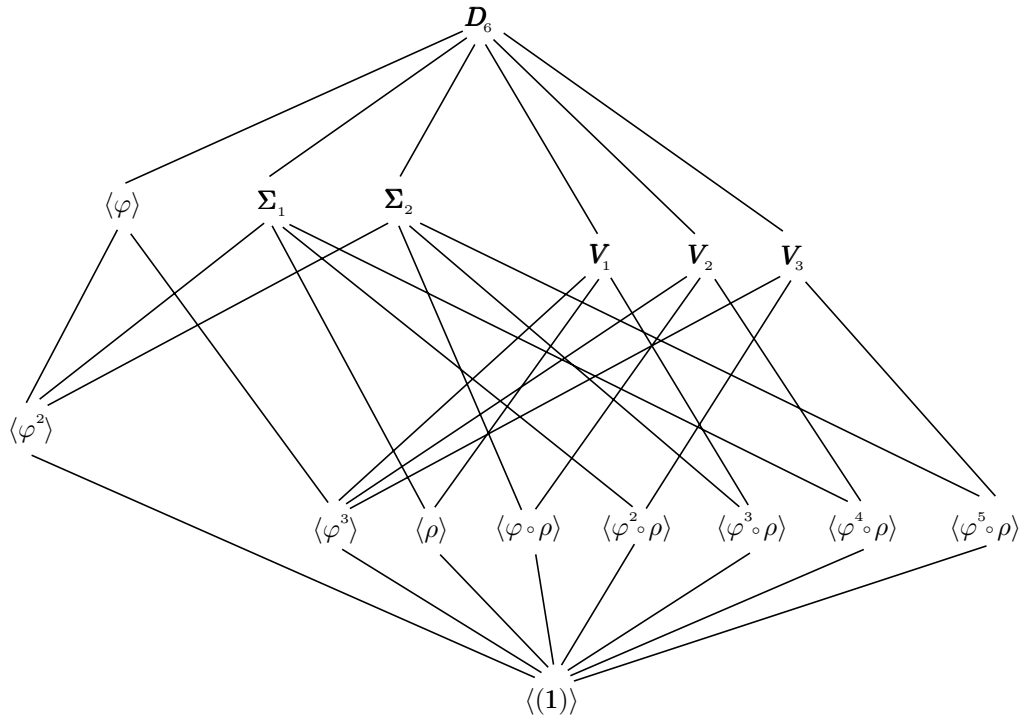
Nota. Si noti che i periodi degli elementi di $\boldsymbol{D}_6$ coincidono con quelli del gruppo

$$\boldsymbol{H} = \{\sigma \in \boldsymbol{S}_5 \mid \sigma(\{1,3\}) = \{1,3\}\}$$

introdotto in **Esercizio 3.1**. Anche il reticolo dei sottogruppi di $\boldsymbol{H}$ coincide con quello di $\boldsymbol{D}_6$. Tale fatto suggerisce che $\boldsymbol{D}_6$ ed $\boldsymbol{H}$ siano isomorfi. Si può infatti verificare che l'applicazione

$$\Psi : \boldsymbol{D}_6 \to \boldsymbol{H} \text{ tale che } \Psi(\varphi) = (1\,3)(2\,4\,5),\ \Psi(\rho) = (2\,4)$$

[ed estesa poi agli altri elementi di $\boldsymbol{D}_6$, in modo da risultare un omomorfismo] è un isomorfismo tra $\boldsymbol{D}_6$ ed $\boldsymbol{H}$.



Ci chiediamo infine quali dei sottogruppi di $\boldsymbol{D}_6$ sono normali.

- Certo sono normali i tre sottogruppi di ordine 6: $\boldsymbol{C}_6, \boldsymbol{\Sigma_1}, \boldsymbol{\Sigma_2}$ [in quanto hanno indice 2].

- Esaminiamo il sottogruppo ciclico $\boldsymbol{C}_3 := \langle\,\varphi^2\,\rangle = \{\mathbf{1}, \varphi^2, \varphi^4\}$. $\boldsymbol{C}_3$ ha quattro laterali destri:

$$\boldsymbol{C}_3, \quad \boldsymbol{C}_3\varphi = \{\varphi, \varphi^3, \varphi^5\}, \quad \boldsymbol{C}_3\rho = \{\rho, \varphi^2\circ\rho, \varphi^4\circ\rho\}, \quad \boldsymbol{C}_3(\varphi\circ\rho) = \{\varphi\circ\rho, \varphi^3\circ\rho, \varphi^5\circ\rho\},$$

e quattro laterali sinistri:

$$\boldsymbol{C}_3, \quad \varphi\boldsymbol{C}_3 = \boldsymbol{C}_3\varphi, \quad \rho\boldsymbol{C}_3 = \{\rho, \rho\circ\varphi^2, \rho\circ\varphi^4\} = \boldsymbol{C}_3\rho, \quad (\varphi\circ\rho)C_3 = \ \ldots\ = C_3(\varphi\circ\rho).$$

Ne segue che $\boldsymbol{C}_3 \triangleleft \boldsymbol{D}_6$.

- Esaminiamo i tre sottogruppi di Klein. Si ha:

$$\varphi\boldsymbol{V}_1 = \{\varphi, \varphi^4, \varphi\circ\rho, \varphi^4\circ\rho\} \neq \boldsymbol{V}_1\varphi = \{\varphi, \varphi^4, \varphi^5\circ\rho, \varphi^2\circ\rho\}$$

e dunque $\boldsymbol{V}_1 \not\triangleleft \boldsymbol{D}_6$. Analogamente si verifica che $\varphi\boldsymbol{V}_2 \neq \boldsymbol{V}_2\varphi$ e $\varphi\boldsymbol{V}_3 \neq \boldsymbol{V}_3\varphi$. Dunque $\boldsymbol{V}_2 \not\triangleleft \boldsymbol{D}_6$ e $\boldsymbol{V}_3 \not\triangleleft \boldsymbol{D}_6$.

- Esaminiamo infine i sette sottogruppi di ordine 2. Si ha:

$$\varphi\,\langle\,\rho\,\rangle = \{\varphi, \varphi\circ\rho\} \neq \langle\,\rho\,\rangle\,\varphi = \{\varphi, \varphi^5\circ\rho\}$$

e quindi $\langle\,\rho\,\rangle \not\triangleleft \boldsymbol{D}_6$. Analogamente si verifica che

$$\varphi\,\langle\,\varphi\circ\rho\,\rangle \neq \langle\,\varphi\circ\rho\,\rangle\,\varphi, \quad \varphi\,\langle\,\varphi^2\circ\rho\,\rangle \neq \langle\,\varphi^2\circ\rho\,\rangle\,\varphi, \qquad \varphi\,\langle\,\varphi^3\circ\rho\,\rangle \neq \langle\,\varphi^3\circ\rho\,\rangle\,\varphi,$$
$$\varphi\,\langle\,\varphi^4\circ\rho\,\rangle \neq \langle\,\varphi^4\circ\rho\,\rangle\,\varphi, \quad \varphi\,\langle\,\varphi^5\circ\rho\,\rangle \neq \langle\,\varphi^5\circ\rho\,\rangle\,\varphi,$$

e quindi $\langle\,\varphi\circ\rho\,\rangle, \langle\,\varphi^2\circ\rho\,\rangle, \langle\,\varphi^3\circ\rho\,\rangle, \langle\,\varphi^4\circ\rho\,\rangle, \langle\,\varphi^5\circ\rho\,\rangle \not\triangleleft \boldsymbol{D}_6$. Invece $\langle\,\varphi^3\,\rangle \triangleleft \boldsymbol{D}_6$. Infatti:

$$\rho\,\langle\,\varphi^3\,\rangle = \langle\,\varphi^3\,\rangle\,\rho, \quad \varphi\,\langle\,\varphi^3\,\rangle = \langle\,\varphi^3\,\rangle\,\varphi, \quad \varphi^2\,\langle\,\varphi^3\,\rangle = \langle\,\varphi^3\,\rangle\,\varphi^2,$$
$$(\varphi\circ\rho)\,\langle\,\varphi^3\,\rangle = \langle\,\varphi^3\,\rangle\,(\varphi\circ\rho), \quad (\varphi^2\circ\rho)\,\langle\,\varphi^3\,\rangle = \langle\,\varphi^3\,\rangle\,(\varphi^2\circ\rho).\ \text{r}$$

($\boldsymbol{C}$) Gruppi di ordine 8

Esistono cinque gruppi di ordine 8, a due a due non isomorfi [si può anzi dimostrare che non ne

esistono altri, a meno di isomorfismi (cfr. la successiva **Osserv. 6**(*ii*))]:

$\boldsymbol{C}_8$ (gruppo ciclico di ordine 8) [abeliano] (cfr. **Esempi 2.1**(*i*)).

$\boldsymbol{D}_4$ (gruppo diedrale) [non abeliano] (cfr. **4.(B)(2)**).

$\mathbf{Q}$ (gruppo delle unità dei quaternioni) [non abeliano] (cfr. **Cap. I, Prop. 5.22**).

$\boldsymbol{Z}_2\times\boldsymbol{Z}_4 = \{(\overline{0},\tilde{0}), (\overline{0},\tilde{1}), (\overline{0},\tilde{2}), (\overline{0},\tilde{3}), (\overline{1},\tilde{0}), (\overline{1},\tilde{1}), (\overline{1},\tilde{2}), (\overline{1},\tilde{3})\}$ [abeliano].

$\boldsymbol{Z}_2\times\boldsymbol{Z}_2\times\boldsymbol{Z}_2 = \{(\overline{0},\overline{0},\overline{0}), (\overline{0},\overline{0},\overline{1}), (\overline{0},\overline{1},\overline{0}), (\overline{0},\overline{1},\overline{1}), (\overline{1},\overline{0},\overline{0}), (\overline{1},\overline{0},\overline{1}), (\overline{1},\overline{1},\overline{0}), (\overline{1},\overline{1},\overline{1})\}$ [abeliano].

Sui primi due gruppi non abbiamo altro da aggiungere a quanto già detto in precedenza. Relativamente a $\mathbf{Q}$, osserviamo che

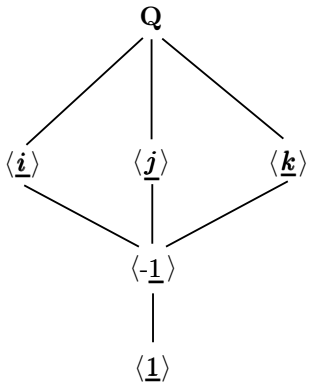
$$\mathbf{Q} = \langle \underline{\boldsymbol{i}}, \underline{\boldsymbol{j}}, \underline{\boldsymbol{k}} \,\big|\, \underline{\boldsymbol{i}}^2 = \underline{\boldsymbol{j}}^2 = \underline{\boldsymbol{k}}^2 = -\underline{\mathbf{1}},\ -\underline{\mathbf{1}}^2 = \underline{\mathbf{1}},\ \underline{\boldsymbol{i}}\underline{\boldsymbol{j}} = -\underline{\boldsymbol{j}}\underline{\boldsymbol{i}} = \underline{\boldsymbol{k}},\ \underline{\boldsymbol{j}}\underline{\boldsymbol{k}} = -\underline{\boldsymbol{k}}\underline{\boldsymbol{j}} = \underline{\boldsymbol{i}},\ \underline{\boldsymbol{k}}\underline{\boldsymbol{i}} = -\underline{\boldsymbol{i}}\underline{\boldsymbol{k}} = \underline{\boldsymbol{j}}\rangle.$$

In $\mathbf{Q}$ soltanto l'elemento $-\underline{\mathbf{1}}$ ha periodo 2; quindi $\mathbf{Q}$ ha un unico sottogruppo ciclico di ordine 2, cioè $\langle -\underline{\mathbf{1}}\rangle$. $\mathbf{Q}$ ha sei elementi di periodo 4, formanti tre sottogruppi ciclici:

$$\langle \underline{\boldsymbol{i}}\rangle = \{\underline{\mathbf{1}}, \underline{\boldsymbol{i}}, -\underline{\mathbf{1}}, -\underline{\boldsymbol{i}}\},\quad \langle \underline{\boldsymbol{j}}\rangle = \{\underline{\mathbf{1}}, \underline{\boldsymbol{j}}, -\underline{\mathbf{1}}, -\underline{\boldsymbol{j}}\},\quad \langle \underline{\boldsymbol{k}}\rangle = \{\underline{\mathbf{1}}, \underline{\boldsymbol{k}}, -\underline{\mathbf{1}}, -\underline{\boldsymbol{k}}\}.$$

Infine, $\mathbf{Q}$ non ha sottogruppi di Klein [in quanto ha un solo elemento di periodo 2].

Il reticolo dei sottogruppi di $\mathbf{Q}$ è il seguente:



Relativamente a $\boldsymbol{Z}_2\times\boldsymbol{Z}_4$, osserviamo che si tratta del prodotto diretto di $(\boldsymbol{Z}_2,+)$ per $(\boldsymbol{Z}_4,+)$. Tale gruppo ha, oltre all'unità $(\overline{0},\tilde{0})$:

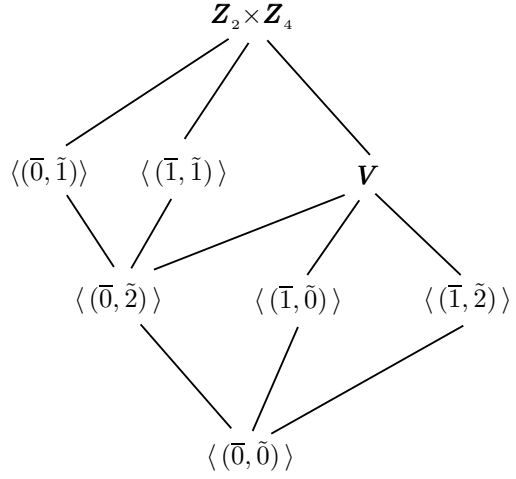
quattro elementi di periodo 4: $(\overline{0},\tilde{1})$, $(\overline{0},\tilde{3})$, $(\overline{1},\tilde{1})$, $(\overline{1},\tilde{3})$;

tre elementi di periodo 2: $(\overline{0},\tilde{2})$, $(\overline{1},\tilde{0})$, $(\overline{1},\tilde{2})$.

Ne segue che $\boldsymbol{Z}_2\times\boldsymbol{Z}_4$ ha tre sottogruppi ciclici di ordine 2: $\langle(\overline{0},\tilde{2})\rangle$, $\langle(\overline{1},\tilde{0})\rangle$, $\langle(\overline{1},\tilde{2})\rangle$.

Ha inoltre due sottogruppi ciclici di ordine 4: $\langle(\overline{0},\tilde{1})\rangle$, $\langle(\overline{1},\tilde{1})\rangle$.

Ha infine un sottogruppo di Klein $\boldsymbol{V} = \boldsymbol{Z}_2\times\langle\tilde{2}\rangle = \{(\overline{0},\tilde{0}), (\overline{0},\tilde{2}), (\overline{1},\tilde{0}), (\overline{1},\tilde{2})\}$. Il reticolo dei suoi sottogruppi è il seguente:



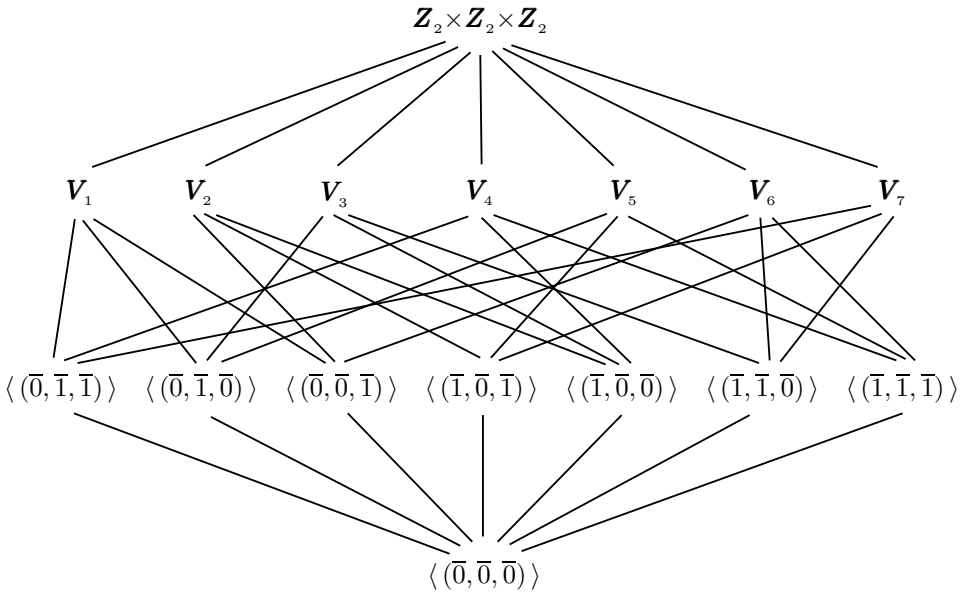
Relativamente a $\boldsymbol{Z}_2\times\boldsymbol{Z}_2\times\boldsymbol{Z}_2$, osserviamo che si tratta del prodotto diretto di $(\boldsymbol{Z}_2,+)$ per se stesso, tre volte.

Ha sette elementi di periodo 2 e quindi sette sottogruppi ciclici di ordine 2. Non ha sottogruppi ciclici di ordine 4, ma ha sette sottogruppi di Klein:

$$\boldsymbol{V}_1=\{\overline{0}\}\times\boldsymbol{Z}_2\times\boldsymbol{Z}_2,\quad \boldsymbol{V}_2=\boldsymbol{Z}_2\times\{\overline{0}\}\times\boldsymbol{Z}_2,\quad \boldsymbol{V}_3=\boldsymbol{Z}_2\times\boldsymbol{Z}_2\times\{\overline{0}\},$$
$$\boldsymbol{V}_4=\{(\overline{0},\overline{0},\overline{0}),\ (\overline{1},\overline{1},\overline{1}),\ (\overline{0},\overline{1},\overline{1}),\ (\overline{1},\overline{0},\overline{0})\},\quad \boldsymbol{V}_5=\{(\overline{0},\overline{0},\overline{0}),\ (\overline{1},\overline{1},\overline{1}),\ (\overline{0},\overline{1},\overline{0}),\ (\overline{1},\overline{0},\overline{1})\},$$
$$\boldsymbol{V}_6=\{(\overline{0},\overline{0},\overline{0}),\ (\overline{1},\overline{1},\overline{1}),\ (\overline{1},\overline{1},\overline{0}),\ (\overline{0},\overline{0},\overline{1})\},\quad \boldsymbol{V}_7=\{(\overline{0},\overline{0},\overline{0}),\ (\overline{1},\overline{1},\overline{0}),\ (\overline{1},\overline{0},\overline{1}),\ (\overline{0},\overline{1},\overline{1})\}.$$

[Tali sottogruppi sono stati ottenuti scegliendo due elementi distinti tra i sette di periodo 2 e considerandone il sottogruppo (di Klein) generato].

Il reticolo dei sottogruppi di $\boldsymbol{Z}_2\times\boldsymbol{Z}_2\times\boldsymbol{Z}_2$ è il seguente:



Osservazione 6. (*i*) Esaminando i periodi degli elementi dei diversi gruppi di ordine 8 sopra studiati, si può osservare che in ciascuno di essi gli elementi di periodo 2 sono in numero dispari. In effetti risulta:

Un gruppo $(G,\cdot)$ *di ordine* 8 *ammette un numero dispari di elementi di periodo* 2.

Se G è ciclico, ammette $\varphi(2)=1$ elementi di periodo 2. Supponiamo quindi G non ciclico: in tal caso i suoi sette elementi $\neq 1$ hanno periodo 2 o 4. Se quindi, per assurdo, G avesse un numero pari di elementi di periodo 2, ne avrebbe un numero dispari di periodo 4. Ognuno di tali elementi genera un sottogruppo ciclico di ordine 4, che ammette però $\varphi(4)=2$ generatori. Ne segue che G deve possedere un numero pari di elementi di periodo 4: assurdo.

(*ii*) Illustriamo schematicamente i passi che dimostrano che non esistono altri gruppi di ordine 8, oltre a quelli sopra considerati. Per i dettagli della dimostrazione rinviamo ad [**Armstrong** Th. 13.3].

Sia $|G|=8$ e G non ciclico. I suoi elementi $\neq 1$ hanno periodo 2 oppure 4. Si può verificare che se tutti tali elementi hanno periodo 2, allora $G\cong\boldsymbol{Z}_2\times\boldsymbol{Z}_2\times\boldsymbol{Z}_2$. Altrimenti, sia $\circ(x)=4$ e $y\notin\langle x\rangle$. Allora

$$G=\{1,\ x,\ x^2,\ x^3,\ y,\ xy,\ x^2y,\ x^3y\}$$

e risultano possibili due sole eventualità:

$$yx=xy\quad\text{ovvero}\quad yx=x^3y.$$

Nel primo caso si dimostra che $G\cong\boldsymbol{Z}_2\times\boldsymbol{Z}_4$; nel secondo caso si distinguono due ulteriori eventualità:

$$\circ(y)=2\quad\text{ovvero}\quad\circ(y)=4.$$

Nel primo caso si dimostra che $G \cong \boldsymbol{D}_4$ e nel secondo che $G \cong \mathbf{Q}$.

Concludiamo con il seguente risultato, preannunciato in **Osserv. 4**.

Esercizio 1. Verificare che il gruppo alterno $\boldsymbol{A}_4$ (sottogruppo di $\boldsymbol{S}_4$) non ammette sottogruppi di ordine 6.

Soluzione. Per assurdo, esista un sottogruppo $\boldsymbol{H}$ di $\boldsymbol{A}_4$, con $|\boldsymbol{H}| = 6$.

È noto che $\boldsymbol{H} \cong \boldsymbol{C}_6$ oppure $\boldsymbol{H} \cong \boldsymbol{S}_3$ e, poiché $\boldsymbol{S}_4$ (e quindi $\boldsymbol{A}_4$) non ha elementi di periodo 6, allora necessariamente $\boldsymbol{H} \cong \boldsymbol{S}_3$. Dunque $\boldsymbol{H}$ contiene tre elementi di periodo 2.

Si noti poi che $\boldsymbol{A}_4$ è formato dagli otto 3-cicli di $\boldsymbol{S}_4$ (elementi di periodo 3), dall'unità $\mathbf{1} = (1)$ e dai tre prodotti di 2-cicli

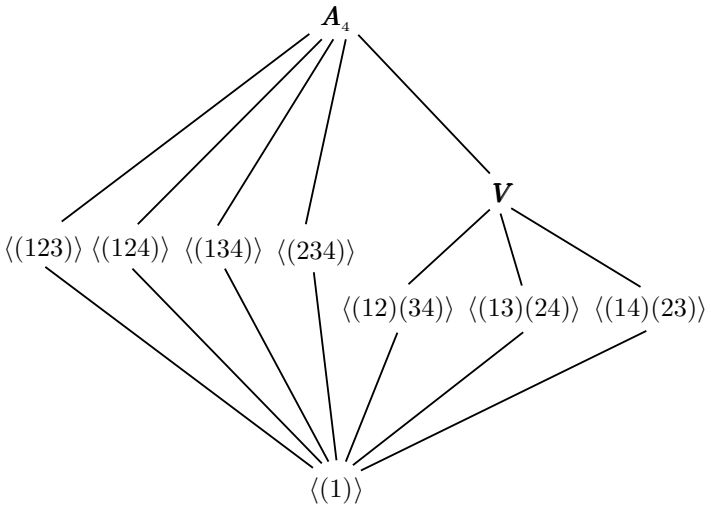
$$x = (1\,2)(3\,4),\ y = (1\,3)(2\,4),\ z = (1\,4)(2\,3)$$

(elementi di periodo 2). Si noti infine che

$$xy = yx = z,\ xz = zx = y,\ yz = zy = x.$$

Dunque $\boldsymbol{V} = \{\mathbf{1}, x, y, z\}$ (gruppo di Klein) è un sottogruppo di $\boldsymbol{A}_4$. Ma $x, y, z \in \boldsymbol{H}$ [sono i tre elementi di periodo 2 in $\boldsymbol{H}$] e dunque $\boldsymbol{V} \subseteq \boldsymbol{H}$: ciò è ovviamente assurdo [in quanto un gruppo di ordine 6 non ha sottogruppi di ordine 4, in base al teorema di Lagrange].

Nota. Gli otto 3-cicli di $\boldsymbol{A}_4$ generano quattro sottogruppi ciclici di ordine 3, cioè $\langle(123)\rangle$, $\langle(124)\rangle$, $\langle(134)\rangle$ e $\langle(234)\rangle$. Ognuno dei tre elementi di periodo 2 genera un sottogruppo ciclico di ordine 2. Oltre al gruppo di Klein $\boldsymbol{V}$ non ci sono quindi altri sottogruppi propri di $\boldsymbol{A}_4$, che ha perciò il seguente reticolo di sottogruppi.



6. Omomorfismi tra gruppi

La definizione di omomorfismo tra due gruppi, la terminologia e le prime proprietà degli omomorfismi sono state esposte nel paragrafo **1** di questo capitolo. Vogliamo comunque rimarcare il seguente semplice fatto.

Proposizione 1. *Se* $f : G \to G'$ *è un isomorfismo, anche* $f^{-1} : G' \to G$ *è un isomorfismo.*

Dim. Per definizione di applicazione inversa, si ha, $\forall\, x', y' \in G'$:

$$f^{-1}(x') = x \iff f(x) = x', \quad f^{-1}(y') = y \iff f(y) = y'.$$

Sia $f^{-1}(x'y') = z$ [cioè $f(z) = x'y'$]. Allora $f(z) = x'y' = f(x)f(y) = f(xy)$. Essendo f biiettiva, $z = xy$, cioè $f^{-1}(x'y') = f^{-1}(x')f^{-1}(y')$.

Nota. Con la stessa dimostrazione si prova che se $f : A \to A'$ è un isomorfismo di anelli, anche $f^{-1} : A' \to A$ è un isomorfismo di anelli.

Definizione 1. *Indicheremo rispettivamente con*

$$\boldsymbol{\mathcal{H}om}(G, G'), \quad \boldsymbol{\mathcal{E}nd}(G), \quad \boldsymbol{\mathcal{A}ut}(G), \quad \boldsymbol{\mathcal{I}}(G),$$

- *l'insieme degli omomorfismi tra i gruppi* G *e* G',
- *l'insieme* $\boldsymbol{\mathcal{H}om}(G, G)$ *degli endomorfismi di* G,
- *l'insieme degli automorfismi di* G,
- *l'insieme degli automorfismi interni di* G *(cfr.* **Osserv. 1.1***(ii)).*

Osservazione 1. (*i*) $\boldsymbol{\mathcal{H}om}(G, G')$ è un insieme non vuoto. Infatti l'applicazione costante

$$G \to G' \text{ tale che } g \to 1_{G'}, \quad \forall\, g \in G,$$

è un omomorfismo (detto *omomorfismo banale*).

(*ii*) $\boldsymbol{\mathcal{E}nd}(G) = \boldsymbol{\mathcal{H}om}(G, G)$ è chiuso rispetto al prodotto operatorio, verifica la proprietà associativa ed è dotato di elemento neutro $\mathbf{1}_G$, ma non è un gruppo [se $G \neq \{1_G\}$], in quanto non esiste l'inverso di un omomorfismo non biiettivo.

(*iii*) $\boldsymbol{\mathcal{A}ut}(G)$ è un gruppo [segue dalla **Prop. 1**].

(*iv*) $\boldsymbol{\mathcal{I}}(G)$ è un sottogruppo di $\boldsymbol{\mathcal{A}ut}(G)$.

Siano infatti $\gamma_x, \gamma_y \in \boldsymbol{\mathcal{I}}(G)$. Si ha, $\forall\, g \in G$:

$$(\gamma_y \circ \gamma_x)(g) = \gamma_y(xgx^{-1}) = y(xgx^{-1})y^{-1} = (yx)g(yx)^{-1} = \gamma_{yx}(g)$$

e dunque $\gamma_y \circ \gamma_x = \gamma_{yx}$. Inoltre si verifica subito che $\gamma_1 = \mathbf{1}_G$. Ne segue che $\gamma_x \circ \gamma_{x^{-1}} = \mathbf{1}_G = \gamma_{x^{-1}} \circ \gamma_x$, cioè $\gamma_x^{-1} = \gamma_{x^{-1}}$. Si conclude che $\boldsymbol{\mathcal{I}}(G)$ è un gruppo.

Nota. Risulta inoltre: $\boldsymbol{\mathcal{I}}(G) = \{\mathbf{1}_G\} \iff G$ è commutativo.

Infatti, se $\boldsymbol{\mathcal{I}}(G) = \{\mathbf{1}_G\}$, $\forall\, x, y \in G$: $y = \gamma_x(y) = xyx^{-1}$ e dunque $xy = yx$. Viceversa, se G è commutativo, $\gamma_x(y) = xyx^{-1} = xx^{-1}y = y = \mathbf{1}_G(y)$.

Proposizione 2. *Sia* $f : G \to G'$ *un omomorfismo. Sia* $a \in G$ *tale che* $\circ(a) < \infty$. *Risulta:*

(i) $\circ(f(a)) \,\big|\, \circ(a)$.

(ii) Se f *è un isomorfismo,* $\circ(f(a)) = \circ(a)$. *[Dunque un isomorfismo "conserva" il periodo di ogni elemento].*

Dim. (*i*) Se $\circ(a) = n$ [e dunque $a^n = 1_G$], allora $1_{G'} = f(1_G) = f(a^n) = f(a)^n$. Ne segue quindi $\circ(f(a)) \,\big|\, n$.

(*ii*) Sia $f : G \to G'$ un isomorfismo. Poiché $f^{-1} : G' \to G$ è un omomorfismo e $\circ(f(a)) < \infty$, allora $\circ(f^{-1}(f(a))) \,\big|\, \circ(f(a))$, cioè $\circ(a) \,\big|\, \circ(f(a))$. Ne segue che $\circ(f(a)) = \circ(a)$.

Proposizione 3. *Sia $f : G \to G'$ un omomorfismo di gruppi. Si ha:*
(i) $\forall\, H \leq G,\ f(H) \leq G'$.
(ii) $\forall\, H' \leq G',\ f^{-1}(H') \leq G$.

Dim. (*i*) Per ogni $f(a), f(b) \in f(H)$, con $a, b \in H$, risulta:

$$ab^{-1} \in H \ \text{ e } \ f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) \in f(H).$$

Dunque $f(H) \leq G'$.

(*ii*) Per ogni $a, b \in f^{-1}(H')$ [e dunque $f(a), f(b) \in H'$], risulta:

$$H' \ni f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}).$$

Allora $ab^{-1} \in f^{-1}(H')$. Dunque $f^{-1}(H') \leq G$.

Definizione 2. *Sia $f : G \to G'$ un omomorfismo di gruppi. L'insieme $f(G)$ è un sottogruppo di G', detto (sottogruppo) immagine di f e denotato $Im(f)$ (o $Im\, f$). L'insieme $f^{-1}(1_{G'})$ è un sottogruppo di G, detto nucleo di f e denotato $Ker(f)$ (o $Ker\, f$) [da "kernel" = nucleo].*

Proposizione 4. *Sia $f : G \to G'$ un omomorfismo di gruppi. Risulta:*

$$f \text{ è iniettivo } \iff Ker(f) = \{1_G\}.$$

Dim. ($\Longrightarrow$). Sia $a \in Ker(f)$: $f(a) = 1_{G'} = f(1_G) \implies a = 1_G$ [essendo f iniettiva].

($\Longleftarrow$). Se $f(a) = f(b)$, si ha: $1_{G'} = f(a)f(b)^{-1} = f(ab^{-1}) \implies ab^{-1} \in Ker(f) \implies ab^{-1} = 1_G \implies a = b$. Dunque f è iniettiva.

Proposizione 5. *Sia $f : G \to G'$ un omomorfismo di gruppi. Risulta:*

$$a\, Ker(f) = Ker(f)\, a,\ \forall\, a \in G.$$

Dunque $Ker(f) \trianglelefteq G$.

Dim. Basta verificare che $Ker(f)\, a \subseteq a\, Ker(f),\ \forall\, a \in G$. Infatti, $\forall\, x \in Ker(f)$, si ha:

$$f(a^{-1}xa) = f(a^{-1})1_{G'}\, f(a) = 1_{G'}$$

e quindi $y := a^{-1}xa \in Ker(f)$. Allora $xa = ay \in a\, Ker(f)$ e quindi $Ker(f)\, a \subseteq a\, Ker(f)$.

Osservazione 2. Indicate con ρ_s e ρ_d le due relazioni associate al sottogruppo $Ker(f)$, dalla precedente poposizione segue che $\rho_s = \rho_d$. Si ha:

$$a\rho_d b \iff ab^{-1} \in Ker(f) \iff f(ab^{-1}) = 1_{G'} \iff f(a)f(b^{-1}) = 1_{G'} \iff f(a) = f(b)$$

e nello stesso modo si verifica che anche $a\rho_s b \iff f(a) = f(b)$.

Ricordiamo che l'omomorfismo $f : G \to G'$, in quanto applicazione, induce su G la relazione di equivalenza ρ_f: $a\rho_f b \iff f(a) = f(b),\ \forall\, a, b \in G$. Ne segue che, relativamente a $Ker(f)$, risulta: $\rho_d = \rho_s = \rho_f$. Ricordato poi che $G/_{\rho_f}$ è in corrispondenza biunivoca con $Im(f)$ [cfr. **Cap. I, Prop.3.3**], si conclude che l'insieme $G/_{\rho_d} = G/_{\rho_s}$ è in corrispondenza biunivoca con $Im(f)$. Verificheremo nel prossimo paragrafo che tale biiezione è un isomorfismo di gruppi.

Ci occuperemo ora dello studio degli insiemi $\mathcal{Hom}(G, G')$, $\mathcal{End}(G)$ ed $\mathcal{Aut}(G)$, nell'ipotesi che G sia un gruppo ciclico (finito o infinito). Premettiamo un'osservazione relativa ai gruppi di automorfismi di gruppi isomorfi.

Osservazione 3. Siano G, G' due gruppi isomorfi e sia $f_0 : G \to G'$ un isomorfismo.

(*i*) Verifichiamo che $\boldsymbol{Aut}(G) \cong \boldsymbol{Aut}(G')$.

Si definisca l'applicazione

$$\Phi : \boldsymbol{Aut}(G) \to \boldsymbol{Aut}(G') \text{ tale che } \Phi(f) = f_0 \circ f \circ f_0^{-1}, \ \forall f \in \boldsymbol{Aut}(G),$$

cioè che renda commutativo il diagramma

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G \\ {\scriptstyle f_0^{-1}}\uparrow & & \downarrow{\scriptstyle f_0} \\ G' & \xrightarrow[\ \Phi(f)\ ]{} & G' \end{array}$$

Si vede con facilità che Φ è un isomorfismo di gruppi. Infatti

$$\Phi(f_1 \circ f_2) = f_0 \circ (f_1 \circ f_2) \circ f_0^{-1} = f_0 \circ f_1 \circ (f_0^{-1} \circ f_0) \circ f_2 \circ f_0^{-1} = \Phi(f_1) \circ \Phi(f_2).$$

Inoltre Φ ha per inversa l'applicazione

$$\Psi : \boldsymbol{Aut}(G') \to \boldsymbol{Aut}(G) \text{ tale che } \Psi(f') = {f_0}^{-1} \circ f' \circ f_0, \ \forall f' \in \boldsymbol{Aut}(G'),$$

che rende commutativo il diagramma

$$\begin{array}{ccc} G' & \xrightarrow{\ f'\ } & G' \\ {\scriptstyle f_0}\uparrow & & \downarrow{\scriptstyle f_0^{-1}} \\ G & \xrightarrow[\ \Psi(f')\ ]{} & G \end{array}$$

(*ii*) Indicato con $\boldsymbol{Isom}(G, G')$ l'insieme non vuoto degli isomorfismi da G a G' $[f_0 \in \boldsymbol{Isom}(G, G')]$, esiste una biiezione tra $\boldsymbol{Isom}(G, G')$ e $\boldsymbol{Aut}(G)$ [o $\boldsymbol{Aut}(G')$]. Infatti l'applicazione

$$F : \boldsymbol{Aut}(G) \to \boldsymbol{Isom}(G, G') \quad \text{tale che} \quad F(f) = f_0 \circ f, \ \forall f \in \boldsymbol{Aut}(G),$$

cioè

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G \\ & {\scriptstyle F(f)}\searrow & \downarrow{\scriptstyle f_0} \\ & & G' \end{array}$$

è una biiezione. Verifichiamolo:

- se $f_0 \circ f' = f_0 \circ f''$ [con $f', f'' \in \boldsymbol{Aut}(G)$], allora $f_0^{-1} \circ f_0 \circ f' = f_0^{-1} \circ f_0 \circ f''$ e quindi $f' = f''$.
- $\forall f_1 \in \boldsymbol{Isom}(G, G')$, $f_0^{-1} \circ f_1 \in \boldsymbol{Aut}(G)$ e $F(f_0^{-1} \circ f_1) = f_0 \circ f_0^{-1} \circ f_1 = f_1$.

Assumiamo che G sia un gruppo ciclico (finito o infinito) e poniamo $G = \langle a \rangle$. Risulta, per ogni $\varphi \in \boldsymbol{Hom}(\langle a \rangle, G')$:

$$\text{se } \varphi(a) = x, \text{ allora } \varphi(a^n) = \varphi(a)^n = x^n, \ \forall n \in \boldsymbol{Z}.$$

[Se G, G' hanno notazione additiva, $\varphi(na) = nx$, $\forall n \in \boldsymbol{Z}$]. Ne segue che φ è completamente individuato se è assegnato l'elemento $x = \varphi(a) \in G'$. Resta pertanto definita l'applicazione

$$\Psi : \boldsymbol{Hom}(\langle a \rangle, G') \to G' \quad \text{tale che} \quad \Psi(\varphi) = \varphi(a), \ \forall \varphi \in \boldsymbol{Hom}(\langle a \rangle, G').$$

Tale applicazione (che dipende dalla scelta del generatore a di $\langle a \rangle$) è ovviamente iniettiva: se infatti $\Psi(\varphi_1) = \Psi(\varphi_2)$, allora

$$\varphi_1(a^n) = \varphi_1(a)^n = \varphi_2(a)^n = \varphi_2(a^n), \ \forall n \in \boldsymbol{Z}.$$

Dunque $\varphi_1 = \varphi_2$.

Proposizione 6. *(i) Se* $\langle a \rangle \cong (\boldsymbol{Z}, +)$, Ψ *è una biiezione.*
(ii) Se $\langle a \rangle$ *è ciclico di ordine* n*, risulta:* $Im(\Psi) = \{x \in G' \ : \ \circ(x) \,|\, n\}$.

Dim. (*i*) Basta verificare che Ψ è suriettiva. Per ogni $x \in G'$, si definisce

$$f_x : (\boldsymbol{Z}, +) \to (G', \cdot) \text{ tale che } f_x(t) = x^t, \ \forall t \in \boldsymbol{Z}.$$

[Se G' ha notazione additiva, si ponga invece $f_x(t) = tx$, $\forall t \in \boldsymbol{Z}$]. Osserviamo che f_x è un omomorfismo. Infatti

$$f_x(t + s) = f_x(t) f_x(s), \ \forall t, s \in \boldsymbol{Z}.$$

Dunque $f_x \in \boldsymbol{Hom}(\boldsymbol{Z}, G')$. Si ha: $\Psi(f_x) = f_x(1) = x$. Dunque Ψ è suriettiva, come richiesto.

(*ii*) Supposto $G = \langle a \mid a^n = 1 \rangle$, bisogna verificare che $Im(\Psi) = \{x \in G' \text{ tali che } \circ(x) \mid n\}$.

($\subseteq$). Sia $x \in Im(\Psi)$: dunque $\exists f \in \boldsymbol{Hom}(\langle a \rangle, G')$ tale che $f(a) = x$.

Si ha: $\circ(f(a)) \mid \circ(a) = n$ [in base a **Prop. 2**(*i*)]. Dunque $x = f(a) \in \{x \in G' \text{ tali che } \circ(x) \mid n\}$.

($\supseteq$). Sia $x \in G'$ tale che $\circ(x) \mid n$. Si definisce l'applicazione

$$f_x : \langle a \mid a^n = 1 \rangle \to (G', \cdot) \text{ tale che } f_x(a^t) = x^t, \ \forall\, t = 0, \dots, n-1.$$

[Se G' ha notazione additiva, si ponga invece $f_x(a^t) = tx$, $\forall\, t = 0, \dots, n-1$]. Ovviamente $\Psi(f_x) = f_x(a) = x^1 = x$. Basta quindi verificare che $f_x \in \boldsymbol{Hom}(\langle a \rangle, G')$, cioè che risulta

$$f_x(a^t a^s) = f_x(a^t) f_x(a^s), \ \forall\, t, s : \ 0 \le t, s < n.$$

Infatti:

$f_x(a^t a^s) = f_x(a^{t+s}) = f_x(a^h) = x^h$, se $t + s \equiv h \ (mod\ n)$ e $0 \le h < n$.

$f_x(a^t) f_x(a^s) = x^t x^s = x^{t+s}$.

Poiché $\circ(x) \mid n$ e $n \mid t + s - h$, allora $x^{t+s-h} = 1_{G'}$, cioè $x^{t+s} = x^h$.

Utilizzando la proposizione precedente si ottengono i due seguenti corollari, che si riferiscono al caso in cui anche il gruppo G' è ciclico (finito o infinito).

Corollario 1. (*i*) $\boldsymbol{End}(\boldsymbol{Z}) = \{k\_ : \boldsymbol{Z} \to \boldsymbol{Z}, \ \forall\, k \in \boldsymbol{Z}\}$ *[con* $k\_(n) := kn$, $\forall\, n \in \boldsymbol{Z}$*]*.

(*ii*) $\boldsymbol{Aut}(\boldsymbol{Z}) = \{\mathbf{1}_{\boldsymbol{Z}}, -\mathbf{1}_{\boldsymbol{Z}}\}$.

(*iii*) *Per ogni* $n \ge 2$, $\boldsymbol{Hom}(\boldsymbol{Z}, \boldsymbol{Z}_n) = \{\overline{k}\_ : \boldsymbol{Z} \to \boldsymbol{Z}_n, \ \forall\, \overline{k} \in \boldsymbol{Z}_n\}$ *[con* $\overline{k}\_(n) := \overline{kn}$, $\forall\, n \in \boldsymbol{Z}$*]*.

Dim. (*i*) Sia $f \in \boldsymbol{End}(\boldsymbol{Z})$. Se $\Psi(f) = f(1) = k$, si ha, $\forall\, n \ge 0$:

$$f(n) = f(1 + \dots + 1) = nk \text{ e } f(-n) = -f(n) = -nk = (-n)k.$$

Dunque $f = k\_$. Viceversa, ogni applicazione $k\_ : \boldsymbol{Z} \to \boldsymbol{Z}$ è un omomorfismo.

(*ii*) Poiché $Im(k\_) = k\boldsymbol{Z}$, le uniche biiezioni di $\boldsymbol{End}(\boldsymbol{Z})$ sono $\mathbf{1}_{\boldsymbol{Z}} = 1\_$ e $-\mathbf{1}_{\boldsymbol{Z}} = -1\_$.

(*iii*) Per ogni $f \in \boldsymbol{Hom}(\boldsymbol{Z}, \boldsymbol{Z}_n)$, se $\Psi(f) = f(1) = \overline{k}$ [$\in \boldsymbol{Z}_n$], allora $f(t) = t\, f(1) = t\overline{k} = \overline{kt}$. Dunque $f = \overline{k}\_$. Viceversa, ogni applicazione $\overline{k}\_ : \boldsymbol{Z} \to \boldsymbol{Z}_n$ è un omomorfismo (da $\boldsymbol{Z}$ a $\boldsymbol{Z}_n$). Infatti $(\overline{k}\_)(t + s) = \overline{k(t+s)} = \overline{kt} + \overline{ks} = (\overline{k}\_)(t) + (\overline{k}\_)(s)$, $\forall\, t, s \in \boldsymbol{Z}$.

Corollario 2. *Per ogni* $n, m \ge 2$, *risulta:*

(*i*) $\boldsymbol{Hom}(\boldsymbol{Z}_n, \boldsymbol{Z}) = \{\mathbf{0}\}$ *[con* $\mathbf{0} : \boldsymbol{Z}_n \to \boldsymbol{Z}$ *omomorfismo banale]*.

(*ii*) $\boldsymbol{Hom}(\boldsymbol{Z}_n, \boldsymbol{Z}_m) = \{\overline{k}\_ : \boldsymbol{Z}_n \to \boldsymbol{Z}_m, \ \forall\, \overline{k} \in \boldsymbol{Z}_m \ : \ \circ(\overline{k}) \mid MCD(n, m)\}$ *[con* $\overline{k}\_(\tilde{t}) = \overline{kt}$, $\forall\, \tilde{t} \in \boldsymbol{Z}_n$*]*.

(*iii*) $\boldsymbol{End}(\boldsymbol{Z}_n) = \{\overline{k}\_ : \boldsymbol{Z}_n \to \boldsymbol{Z}_n, \ \forall\, \overline{k} \in \boldsymbol{Z}_n\}$.

(*iv*) $\boldsymbol{Aut}(\boldsymbol{Z}_n) = \{\overline{k}\_ : \boldsymbol{Z}_n \to \boldsymbol{Z}_n, \ : \overline{k} \in \mathcal{U}(\boldsymbol{Z}_n)\} \cong (\mathcal{U}(\boldsymbol{Z}_n), \cdot)$.

Dim. (*i*) Sia $f \in \boldsymbol{Hom}(\boldsymbol{Z}_n, \boldsymbol{Z})$. Dalla **Prop. 2**, $\circ(f(\overline{1})) \mid \circ(\overline{1}) = n$ e quindi $\circ(f(\overline{1}))$ è finito. Ma in $\boldsymbol{Z}$ soltanto 0 ha periodo finito. Dunque $f(\overline{1}) = 0$ e pertanto $f = \mathbf{0}$.

(*ii*) Cominciamo col verificare che, se $\circ(\overline{k}) \mid MCD(n, m)$, l'applicazione $\overline{k}\_ : \boldsymbol{Z}_n \to \boldsymbol{Z}_m$ è ben definita, cioè che:

$$\tilde{t} = \tilde{t}_1 \text{ (in } \boldsymbol{Z}_n) \implies \overline{kt} = \overline{kt_1} \text{ (in } \boldsymbol{Z}_m).$$

Assumiamo $\circ(\overline{k}) := s$. Dunque $s \mid n$ [e sia $n = sn_1$]. Per definizione di periodo, $s\overline{k} = \overline{0}$ (in $\boldsymbol{Z}_m$): dunque $m \mid sk$ [e sia $sk = mr$]. Da $\tilde{t} = \tilde{t}_1$ (in $\boldsymbol{Z}_n$), $n \mid t_1 - t$ [e sia $t_1 - t = n\ell$]. Allora:

$$kt_1 - kt = k(t_1 - t) = kn\ell = ksn_1\ell = mrn_1\ell.$$

Dunque $m \mid kt_1 - kt$, cioè $\overline{kt_1} = \overline{kt}$.

Infine, che $\overline{k}\_ : \boldsymbol{Z}_n \to \boldsymbol{Z}_m$ sia un omomorfismo è del tutto ovvio [infatti $\overline{k}\_(\tilde{t} + \tilde{s}) = \overline{k(t+s)} = \overline{kt} + \overline{ks} = \overline{k}\_(\tilde{t}) + \overline{k}\_(\tilde{s})$].

Viceversa, dimostriamo che ogni $f \in \boldsymbol{Hom}(\boldsymbol{Z}_n, \boldsymbol{Z}_m)$ è della forma $\overline{k}\,\_$ [con $\circ(\overline{k}) \,\big|\, MCD(n,m)$]. Dalla **Prop. 6**, $\Psi : \boldsymbol{Hom}(\boldsymbol{Z}_n, \boldsymbol{Z}_m) \to \boldsymbol{Z}_m$ ha per immagine $Im\Psi = \big\{\overline{k} \in \boldsymbol{Z}_m \,:\, \circ(\overline{k}) \,\big|\, n\big\}$. Poiché, $\forall\, \overline{k} \in \boldsymbol{Z}_m$, $\circ(\overline{k}) \,\big|\, m$, allora

$$Im\Psi = \big\{\overline{k} \in \boldsymbol{Z}_m \,:\, \circ(\overline{k}) \,\big|\, \begin{matrix} n \\ m \end{matrix}\big\} = \big\{\overline{k} \in \boldsymbol{Z}_m \,:\, \circ(\overline{k}) \,\big|\, MCD(n,m)\big\}.$$

Sia quindi $f \in \boldsymbol{Hom}(\boldsymbol{Z}_n, \boldsymbol{Z}_m)$. Se $\Psi(f) = f(\tilde{1}) = \overline{k}$, allora $\circ(\overline{k}) \,\big|\, MCD(n,m)$ e $f(\tilde{t}) = f(\tilde{1} + \,...\, + \tilde{1}) = \overline{k} + \,...\, + \overline{k} = \overline{tk}$, $\forall\, \tilde{t} \in \boldsymbol{Z}_n$. Dunque $f = \overline{k}\,\_$.

(*iii*) Segue subito da (*ii*). Se infatti $n = m$, $\forall\, \overline{k} \in \boldsymbol{Z}_n$ si ha che $\circ(\overline{k}) \,\big|\, n = MCD(n,n)$. Dunque $\boldsymbol{End}(\boldsymbol{Z}_n) = \boldsymbol{Hom}(\boldsymbol{Z}_n, \boldsymbol{Z}_n) = \big\{\overline{k}\,\_ : \boldsymbol{Z}_n \to \boldsymbol{Z}_n,\ \forall\, \overline{k} \in \boldsymbol{Z}_n\big\}$.

(*iv*) In base a (*iii*), $\boldsymbol{Aut}(\boldsymbol{Z}_n) = \big\{\overline{k}\,\_ : \boldsymbol{Z}_n \to \boldsymbol{Z}_n \,:\, \overline{k}\,\_ \text{ è biiettiva}\big\}$. Verifichiamo che

$$\overline{k}\,\_ \text{ è biiettiva} \iff \overline{k} \in \mathcal{U}(\boldsymbol{Z}_n).$$

($\Longrightarrow$). Se $\overline{k}\,\_$ è biiettiva, denotiamo con $\overline{h}\,\_$ la sua inversa. Allora $\overline{k}\,\_ \circ \overline{h}\,\_ = \mathbf{1}_{\boldsymbol{Z}_n}$ e quindi in particolare $\overline{1} = (\overline{k}\,\_ \circ \overline{h}\,\_)(\overline{1}) = \overline{k}\,\_(\overline{h}\,1) = \overline{k}\,\overline{h}$. Pertanto $\overline{k} \in \mathcal{U}(\boldsymbol{Z}_n)$.

($\Longleftarrow$). Se $\overline{k}\,\overline{h} = \overline{1}$, allora $(\overline{k}\,\_ \circ \overline{h}\,\_)(\overline{t}) = \overline{k}\,(\overline{ht}) = \overline{kht} = \overline{t}$. Pertanto $\overline{k}\,\_ \circ \overline{h}\,\_ = \mathbf{1}_{\boldsymbol{Z}_n}$. Allora $\overline{k}\,\_$ ammette inversa $\overline{h}\,\_$.

Per ottenere un isomorfismo tra $\boldsymbol{Aut}(\boldsymbol{Z}_n)$ e $\mathcal{U}(\boldsymbol{Z}_n)$, basta considerare l'applicazione biiettiva

$$\Phi : \mathcal{U}(\boldsymbol{Z}_n) \to \boldsymbol{Aut}(\boldsymbol{Z}_n) \text{ tale che } \Phi(\overline{k}) = \overline{k}\,\_,\ \forall\, \overline{k} \in \mathcal{U}(\boldsymbol{Z}_n),$$

e verificare che si tratta di un omomorfismo. Infatti $\Phi(\overline{k_1}\,\overline{k_2}) = \overline{k_1 k_2}\,\_ = \overline{k_1}\,\_ \circ \overline{k_2}\,\_ = \Phi(\overline{k_1}) \circ \Phi(\overline{k_2})$.

Esempio 1. Determiniamo $\boldsymbol{Hom}(\boldsymbol{Z}_8, \boldsymbol{Z}_{12})$, $\boldsymbol{Hom}(\boldsymbol{Z}_{12}, \boldsymbol{Z}_8)$, $\boldsymbol{Aut}(\boldsymbol{Z}_8)$ e $\boldsymbol{Aut}(\boldsymbol{Z}_{12})$.

Per ogni $k \in \boldsymbol{Z}$, denoteremo con $\overline{k}$ la classe resto di k in $\boldsymbol{Z}_{12}$ e con $\tilde{k}$ la classe resto di k in $\boldsymbol{Z}_8$. Risulta:

$$\boldsymbol{Hom}(\boldsymbol{Z}_8, \boldsymbol{Z}_{12}) = \big\{\overline{k}\,\_ : \boldsymbol{Z}_8 \to \boldsymbol{Z}_{12},\ \text{con } \circ(\overline{k}) \,\big|\, MCD(8,12) = 4\big\}.$$

In $\boldsymbol{Z}_{12}$ gli elementi il cui periodo divide 4 sono: $\overline{0}$, $\overline{3}$, $\overline{6}$, $\overline{9}$. Allora

$$\boldsymbol{Hom}(\boldsymbol{Z}_8, \boldsymbol{Z}_{12}) = \big\{\overline{0}\,\_,\, \overline{3}\,\_,\, \overline{6}\,\_,\, \overline{9}\,\_\big\}$$

[dove, ad esempio, $\overline{3}\,\_(\tilde{k}) = \overline{3k},\ \forall\, \tilde{k} \in \boldsymbol{Z}_8$].

Risulta poi:

$$\boldsymbol{Hom}(\boldsymbol{Z}_{12}, \boldsymbol{Z}_8) = \big\{\tilde{k}\,\_ : \boldsymbol{Z}_{12} \to \boldsymbol{Z}_8,\ \text{con } \circ(\tilde{k}) \,\big|\, MCD(8,12) = 4\big\}.$$

In $\boldsymbol{Z}_8$ gli elementi il cui periodo divide 4 sono: $\tilde{0}$, $\tilde{2}$, $\tilde{4}$, $\tilde{6}$. Allora

$$\boldsymbol{Hom}(\boldsymbol{Z}_{12}, \boldsymbol{Z}_8) = \big\{\tilde{0}\,\_,\, \tilde{2}\,\_,\, \tilde{4}\,\_,\, \tilde{6}\,\_\big\}.$$

Risulta infine:

$$\boldsymbol{Aut}(\boldsymbol{Z}_8) = \big\{\tilde{1}\,\_,\, \tilde{3}\,\_,\, \tilde{5}\,\_,\, \tilde{7}\,\_\big\} \text{ e } \boldsymbol{Aut}(\boldsymbol{Z}_{12}) = \big\{\overline{1}\,\_,\, \overline{5}\,\_,\, \overline{7}\,\_,\, \overline{11}\,\_\big\}.$$

Si tratta di due gruppi di Klein.

Osservazione 4. Sia G un gruppo generato da t elementi $a_1, \,...\, , a_t$. Un omomorfismo $f \in \boldsymbol{Hom}(G, G')$ è completamente individuato dagli elementi $f(a_1), \,...\, , f(a_t) \in G'$. In base alla **Prop. 2**, tali elementi verificano inoltre le condizioni $\circ(f(a_i)) \,\big|\, \circ(a_i)$ (se a_i ha periodo finito). Infine, le eventuali relazioni tra i generatori devono valere anche per le rispettive immagini [ad esempio, se $a_1 a_2 = a_2 a_1$, allora anche $f(a_1)f(a_2) = f(a_2)f(a_1)$].

Tali restrizioni spesso consentono di determinare gli omomorfismi tra due gruppi. Ad esempio si consideri il gruppo $\boldsymbol{S}_3$, che, come noto, è generato ad esempio dal 3-ciclo $a = (123)$ e dal 2-ciclo $b = (12)$. Se $f \in \boldsymbol{End}(\boldsymbol{S}_3)$, risulta: $\circ\big(f(a)\big) \,\big|\, 3$, $\circ\big(f(b)\big) \,\big|\, 2$ e dunque

$$f(a) \in \{(1),\, (123),\, (132)\}, \quad f(b) \in \{(1),\, (12),\, (13),\, (23)\}.$$

Si hanno pertanto al più 12 possibili scelte di coppie di elementi immagini dei due generatori. Ma in $\boldsymbol{S}_3$ vale la relazione $ba = a^2 b$ e quindi $f(b)f(a) = f(a)^2 f(b)$. Esaminando tale relazione per tutte le possibili coppie $\big(f(a), f(b)\big)$, dovremo scartarne due, cioè: $\big(f(a) = (123), f(b) = (1)\big)$ e $\big(f(a) = (132),\, f(b) = (1)\big)$. Si conclude che $\boldsymbol{End}(\boldsymbol{S}_3)$ è costituito da 10 omomorfismi.

Si può infine facilmente provare (cfr. **Eserc. 4.28**) che $\boldsymbol{Aut}(\boldsymbol{S}_3) \cong \boldsymbol{S}_3$.

Concludiamo con due semplici risultati, che proponiamo come esercizi.

Esercizio 1. Sia $\boldsymbol{V}$ il gruppo di Klein. Verificare che $\boldsymbol{Aut}(\boldsymbol{V}) \cong \boldsymbol{S}_3$.

Soluzione. Posto $\boldsymbol{V} = \{1, a, b, c\}$ (cfr. **4.(A)**), gli automorfismi di $\boldsymbol{V}$ vanno cercati tra le biiezioni di $\boldsymbol{V}$ che fissano l'elemento 1, cioè tra le permutazioni di $\{a, b, c\}$.
Tali permutazioni formano un gruppo $[\cong \boldsymbol{S}_3]$. Consideriamo ad esempio la biiezione $f \leftrightarrow (a\,b)$ [cioè la biiezione così definita: $f(1) = 1,\ f(a) = b,\ f(b) = a,\ f(c) = c$]. Per verificare che f è un isomorfismo, si osservi:

$$\begin{cases} f(ab) = f(c) = c \\ f(a)f(b) = ba = c, \end{cases} \quad \begin{cases} f(ac) = f(b) = a \\ f(a)f(c) = bc = a, \end{cases} \quad \begin{cases} f(bc) = f(a) = b \\ f(b)f(c) = ac = b. \end{cases}$$

Essendo poi $\boldsymbol{V}$ abeliano, non è necessaria altra verifica. Si conclude che $f \in \boldsymbol{Aut}(\boldsymbol{V})$.

In modo analogo si verifica che anche le biiezioni associate a $(a\,c)$, $(b\,c)$, $(a\,b\,c)$, $(a\,c\,b)$ appartengono a $\boldsymbol{Aut}(\boldsymbol{V})$. Dunque $\boldsymbol{Aut}(\boldsymbol{V}) \cong \boldsymbol{S}_3$.

Esercizio 2. Verificare che, per ogni gruppo G, risulta: $\boldsymbol{\mathcal{I}}(G) \trianglelefteq \boldsymbol{Aut}(G)$.

Soluzione. In base ad **Osserv. 5.3**(*iii*), basta verificare che

$$f \circ \boldsymbol{\mathcal{I}}(G) \subseteq \boldsymbol{\mathcal{I}}(G) \circ f, \quad \forall\, f \in \boldsymbol{Aut}(G),$$

cioè che, $\forall\, f \in \boldsymbol{Aut}(G)$, $\forall\, g \in G$:

$$f \circ \gamma_g \in \boldsymbol{\mathcal{I}}(G) \circ f, \text{ ovvero } \quad f \circ \gamma_g \circ f^{-1} \in \boldsymbol{\mathcal{I}}(G).$$

Infatti, $\forall\, x \in G$: $\big(f \circ \gamma_g \circ f^{-1}\big)(x) = f\big(\gamma_g(f^{-1}(x)\big) = f\big(g\, f^{-1}(x)\, g^{-1}\big) = f(g)\, f\big(f^{-1}(x)\big)\, f(g^{-1}) = f(g)\, x\, f(g^{-1}) = f(g)\, x\, f(g)^{-1} = \gamma_{f(g)}(x)$. Dunque $f \circ \gamma_g \circ f^{-1} = \gamma_{f(g)} \in \boldsymbol{\mathcal{I}}(G)$.

7. Gruppi quoziente e teorema fondamentale di omomorfismo

Sia H un sottogruppo di $(G,\cdot)$. Cercheremo di introdurre una struttura algebrica sull'insieme dei laterali destri $G/_{\rho_d} = \mathfrak{L}_d(H)$. Poniamo, $\forall\, Ha,\, Hb \in \mathfrak{L}_d(H)$:

$$Ha\cdot Hb = Hab.$$

Bisogna verificare se tale operazione è ben definita, cioè se:

$$Ha = Ha_1,\ Hb = Hb_1 \implies Hab = Ha_1b_1,$$

ovvero:

$$aa_1^{-1} \in H,\ bb_1^{-1} \in H \implies a\,b\,b_1^{-1}a_1^{-1} \in H.$$

Proposizione 1. *Se $H \trianglelefteq G$, l'operazione sopra introdotta è ben definita.*

Dim. Sia $h_1 := aa_1^{-1} \in H$ e $h_2 := bb_1^{-1} \in H$. Allora

$$a\,b\,b_1^{-1}a_1^{-1} = a\,(b\,b_1^{-1})\,a_1^{-1} = a\,h_2\,a_1^{-1}.$$

Essendo $H \trianglelefteq G$, $a\,h_2 \in aH = Ha$. Dunque $ah_2 = h_3\,a$, $\exists\, h_3 \in H$. Allora

$$a\,b\,b_1^{-1}a_1^{-1} = a\,h_2\,a_1^{-1} = h_3\,a\,a_1^{-1} = h_3h_1 \in H.$$

Osservazione 1. La proposizione precedente si inverte:

se l'operazione $Ha\cdot Hb = Hab$ è ben definita $(\forall\, Ha,\, Hb \in \mathfrak{L}_d(H))$, allora $H \trianglelefteq G$.

Infatti, in base ad **Osserv. 5.3**(*iii*), basta verificare che $aH \subseteq Ha$, $\forall\, a \in G$. Scelto comunque $h \in H$, si ha ovviamente che $Hh = H1$, $Ha = Ha$ e dunque (essendo l'operazione ben definita)

$$Ha\cdot Hh = Ha\cdot H1, \text{ cioè } Hah = Ha1 = Ha \text{ e quindi } aha^{-1} \in H.$$

Ne segue che $ah \in Ha$, cioè $aH \subseteq Ha$.

Ad esempio, ricordato che $H = \langle\,(1\,2)\,\rangle$ è un sottogruppo non normale di $\boldsymbol{S}_3$, possiamo verificare che l'operazione in questione non è ben definita. Si ha infatti:

$$\begin{cases} H(1\,3) = H(1\,2\,3) \\ H(2\,3) = H(1\,3\,2), \end{cases} \quad \text{ma} \quad \begin{cases} H(1\,3)\cdot H(2\,3) = H(1\,2\,3) \\ H(1\,2\,3)\cdot H(1\,3\,2) = H \end{cases} \quad \text{e } H \neq H(1\,2\,3).$$

Proposizione 2. *Se $H \trianglelefteq G$, $(G/_{\rho_d},\cdot)$ è un gruppo (rispetto all'operazione sopra definita), detto gruppo quoziente di G modulo H e denotato $G/_H$.*

Dim. L'operazione è ben definita (in base alla **Prop. 1**). Si ha:

(*i*) L'operazione è associativa. Infatti: $\big(Ha\cdot Hb\big)\cdot Hc = \big(Hab\big)\cdot Hc = H(ab)\,c = H(abc)$, mentre $Ha\cdot\big(Hb\cdot Hc\big) = Ha\cdot\big(Hbc\big) = Ha(bc) = H(abc)$.

(*ii*) L'operazione ha elemento neutro H. Infatti: $Ha\cdot H = Ha = H\cdot Ha$.

(*iii*) Esiste l'inverso di ogni elemento Ha, e risulta $(Ha)^{-1} = Ha^{-1}$. Infatti $Ha\cdot Ha^{-1} = Haa^{-1} = H = Ha^{-1}\cdot Ha$.

Osservazione 2. Se $H \trianglelefteq G$, allora $\rho_d = \rho_s$ e quindi anche $G/_{\rho_s} = G/_H$. Gli elementi di $G/_H$ possono essere indicati anche come laterali sinistri.

Si osservi inoltre che, se $(G,+)$ è un gruppo abeliano, ogni suo sottogruppo H (essendo normale) determina il gruppo quoziente $(G/_H,+)$, rispetto alla seguente operazione (commutativa)

$$(H+a)+(H+b) = H+(a+b),\quad \forall\, a,\, b \in G.$$

Osservazione 3. L'applicazione $\pi : G \to G/_H$ tale che $\pi(x) = Hx$, $\forall\, x \in G$, è un omomorfismo. Infatti

$$\pi(xy) = H\,xy = Hx \cdot Hy = \pi(x)\pi(y), \quad \forall\, x,\, y \in G.$$

Inoltre, $\forall\, Hx \in G/_H$, risulta $Hx = \pi(x)$ e dunque tale omomorfismo è suriettivo. È detto *proiezione canonica di G sul quoziente $G/_H$*.

Teorema 1. (*Teorema fondamentale di omomorfismo tra gruppi*). *Sia $f : G \to G'$ un omomorfismo di gruppi. f induce un unico isomorfismo $F : G/_{ker\, f} \to Im\, f$, tale che $f = i \circ F \circ \pi$, cioè tale che rende commutativo il seguente diagramma di gruppi*

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ G/_{Ker f} & \xrightarrow{\ F\ } & Im\, f \end{array}$$

Dim. Sono già stati osservati due fatti:

- $Ker\, f \trianglelefteq G$ [cfr. **Prop. 6.5**];
- $\rho_f = \rho_s\ [= \rho_d]$ [cfr. **Osserv. 6.2**].

Ne segue:

- $G/_{ker\, f} = G/_{\rho_f}$ è un gruppo [cfr. **Prop. 2**];
- dal teorema di decomposizione delle applicazioni (cfr. **Cap. I, Prop. 3.3**), esiste un'unica biiezione $F : G/_{\rho_f} \to Im\, f$ che rende commutativo il seguente diagramma di applicazioni:

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ G/_{\rho_f} & \xrightarrow{\ F\ } & Im\, f \end{array}$$

e risulta $F\big(aKer\, f\big) = f(a), \quad \forall\, a \in G$.

Le applicazioni π ed i [proiezione ed inclusione canonica] sono omomorfismi. Resta soltanto da verificare che anche F è un omomorfismo. Si ha infatti:

$$F\big(aKer\, f \cdot bKer\, f\big) = F\big(abKer\, f\big) = f(ab) = f(a)f(b),$$
$$F\big(aKer\, f\big) \cdot F\big(bKer\, f\big) = f(a)f(b).$$

Dunque F è un omomorfismo.

Dimostriamo ora alcune semplici conseguenze del teorema fondamentale di omomorfismo.

Corollario 1. *Per ogni gruppo G, risulta:*

$$\boldsymbol{\mathcal{I}}(G) \cong G/_{\boldsymbol{\mathcal{Z}}(G)}$$

[dove $\boldsymbol{\mathcal{Z}}(G) = \{g \in G\ :\ gx = xg,\ \forall\, x \in G\}$ è l'insieme degli elementi di G che commutano con ogni elemento di G; $\boldsymbol{\mathcal{Z}}(G)$ è detto centro di G. Se G è abeliano, $\boldsymbol{\mathcal{Z}}(G) = G$, mentre $\boldsymbol{\mathcal{I}}(G) = \{\mathbf{1}_G\}$].

Dim. Sia $\varphi : G \to \boldsymbol{\mathcal{I}}(G)$ tale che $\varphi(g) = \gamma_g, \quad \forall\, g \in G$. Verifichiamo che φ è un omomorfismo. Si ha: $\varphi(g_1g_2) = \gamma_{g_1\, g_2},\ \varphi(g_1) \circ \varphi(g_2) = \gamma_{g_1} \circ \gamma_{g_2}$ e, $\forall\, x \in G$:

$$(\gamma_{g_1} \circ \gamma_{g_2})(x) = \gamma_{g_1}(g_2\, x g_2^{-1}) = g_1(g_2\, x g_2^{-1})g_1^{-1} = (g_1\, g_2)x(g_1\, g_2)^{-1} = \gamma_{g_1\, g_2}(x).$$

Dunque $\varphi(g_1\, g_2) = \varphi(g_1)\varphi(g_2)$. L'omomorfismo φ è ovviamente suriettivo. Si ha infine: $Ker\, \varphi = \{g \in G\ :\ \gamma_g = \mathbf{1}_G\}$. Risulta:

$$\gamma_g = \mathbf{1}_G \iff gxg^{-1} = x,\ \forall\, x \in G \iff gx = xg,\ \forall\, x \in G \iff g \in \boldsymbol{\mathcal{Z}}(G).$$

Dunque $Ker\, \varphi = \boldsymbol{\mathcal{Z}}(G)$ e, dal teorema fondamentale di omomorfismo, segue che $\boldsymbol{\mathcal{I}}(G) \cong G/_{\boldsymbol{\mathcal{Z}}(G)}$.

Corollario 2. *Ogni quoziente di un gruppo ciclico è un gruppo ciclico.*

Dim. Se G è ciclico infinito, possiamo porre $G = (\boldsymbol{Z}, +)$. Sia $H = \langle\, n\,\rangle$ un sottogruppo di $(\boldsymbol{Z}, +)$. Risulta:

$$\boldsymbol{Z}/_{\langle n\rangle} \cong \boldsymbol{Z}_n \quad \text{(ciclico di ordine } n\text{)}.$$

Infatti la proiezione canonica

$$\pi : \boldsymbol{Z} \to \boldsymbol{Z}_n \text{ tale che } \pi(t) = \overline{t} \in \boldsymbol{Z}_n, \ \forall\, t \in \boldsymbol{Z},$$

è un omomorfismo suriettivo e $Ker\,\pi = \langle n\rangle$. Dal teorema fondamentale di omomorfismo, segue che $\boldsymbol{Z}/_{\langle n\rangle} \cong \boldsymbol{Z}_n$.

Sia ora G ciclico di ordine n ed assumiamo $G = (\boldsymbol{Z}_n, +)$. Sia H un sottogruppo di $\boldsymbol{Z}_n$, di ordine $d \le n$. Dalla **Prop. 2.2** (o dal teorema di Lagrange), $d \,|\, n$ e sia quindi $n = dk$. È noto, in base alla dimostrazione di **Prop. 2.3**(ii), che $H = \langle \overline{k}\rangle$.

Consideriamo l'endomorfismo $\overline{d}\_ : \boldsymbol{Z}_n \to \boldsymbol{Z}_n$ [moltiplicazione per $\overline{d}$]. Tale omomorfismo ha nucleo $Ker(\overline{d}\_) = \langle \overline{k}\rangle = H$ ed immagine $Im(\overline{d}\_) = \overline{d}\,\boldsymbol{Z}_n = \langle \overline{d}\rangle$. Dal teorema fondamentale di omomorfismo, risulta

$$\boldsymbol{Z}_n/_H \cong \langle \overline{d}\rangle,$$

cioè il quoziente $\boldsymbol{Z}_n/_H$ è ciclico, come richiesto.

Nota. Si verifica facilmente che $\langle \overline{d}\rangle \cong \boldsymbol{Z}_k$. Infatti, poiché $\circ(\overline{d}) = k$, in base al **Cor. 6.2**(ii) la moltiplicazione $\overline{d}\_ : \boldsymbol{Z}_k \to \boldsymbol{Z}_n$ è un omomorfismo [in quanto $\circ(\overline{d}) \,|\, k$]. Risulta subito che tale omomorfismo è iniettivo [infatti, se $\overline{dt} = \overline{0}$ in $\boldsymbol{Z}_n$, con $0 \le t < k$, allora $n = dk \,|\, dt$ e dunque $t = 0$] ed ha immagine $\overline{d}\,\boldsymbol{Z}_n = \langle \overline{d}\rangle$. Applicando ad esso il teorema fondamentale di omomorfismo, si ottiene che $\boldsymbol{Z}_k \cong \boldsymbol{Z}_k/_{\langle\overline{0}\rangle} \cong \langle \overline{d}\rangle$, come richiesto.

Il teorema fondamentale di omomorfismo è talvolta chiamato anche *primo teorema di isomorfismo*. Esistono in effetti altri due "teoremi di isomorfismo", entrambi conseguenza del teorema fondamentale di omomorfismo.

Corollario 3. (*Secondo teorema di isomorfismo*). *Sia H un sottogruppo normale di G. Per ogni sottogruppo K di G, risulta:*

$$HK/_H \cong K/_{H\cap K}\,.$$

Dim. Osserviamo per prima cosa che da $H \trianglelefteq G$ segue che $HK = KH$. Infatti:

- $\forall\, hk \in HK$: $\quad hk \in Hk = kH \subseteq KH$: dunque $HK \subseteq KH$,
- $\forall\, kh \in KH$: $\quad kh \in kH = Hk \subseteq HK$: dunque $KH \subseteq HK$.

In base a **Prop. 1.4**(ii), HK è un sottogruppo di G. Poiché $H \subseteq HK$ e $H \trianglelefteq G$, allora $H \trianglelefteq HK$. Dunque è definito il gruppo quoziente $HK/_H$.

Si definisce ora l'applicazione

$$\varphi : K \to HK/_H \quad \text{tale che } \varphi(c) = cH, \ \forall\, c \in K,$$

[si noti che $c = 1\cdot c \in HK$]. Si ha:

- φ è un omomorfismo $[\,\varphi(c_1c_2) = c_1c_2H = (c_1H)(c_2H) = \varphi(c_1)\,\varphi(c_2)\,]$;
- φ è suriettiva $[\,\forall\, hk \in HK,\ hk = k_1h_1 \in KH$ e quindi $hkH = k_1h_1H = k_1H = \varphi(k_1)\,]$;
- $Ker\,\varphi = H \cap K$ [infatti $Ker\,\varphi = \{c \in K \,:\, cH = H\} = \{c \in K \,:\, c \in H\} = H \cap K\,]$.

Dal teorema fondamentale di omomorfismo (applicato a φ), segue che

$$K/_{H\cap K} = K/_{Ker\,\varphi} \cong Im\,\varphi = HK/_H.$$

Corollario 4. (*Terzo teorema di isomorfismo*). *Siano H_1, H_2 due sottogruppi normali di G, con $H_1 \le H_2$. Risulta:*

$$G/_{H_2} \cong \frac{G/_{H_1}}{H_2/_{H_1}}\,.$$

Dim. Si osserva subito che $H_1 \trianglelefteq H_2$ [infatti $H_1 \trianglelefteq G$]. Sono quindi ben definiti i tre gruppi quoziente

$$G/_{H_1}, \quad G/_{H_2}, \quad H_2/_{H_1}.$$

Si ponga

$$\varphi : G/_{H_1} \to G/_{H_2} \quad \text{tale che} \quad \varphi(aH_1) = aH_2, \quad \forall\, aH_1 \in G/_{H_1}.$$

Risulta:

- φ è ben definita [se $aH_1 = a'H_1$, allora $a^{-1}a' \in H_1 \leq H_2$ e dunque $aH_2 = a'H_2$];
- φ è un omomorfismo [$\varphi(aH_1 \cdot bH_1) = \varphi(abH_1) = abH_2 = aH_2\, bH_2 = \varphi(aH_1)\cdot\varphi(bH_1)$];
- φ è suriettiva [$aH_2 = \varphi(aH_1)$, $\forall\, aH_2 \in G/_{H_2}$];
- $Ker\,\varphi = H_2/_{H_1}$ [infatti $Ker\,\varphi = \{aH_1 \,:\, aH_2 = H_2\} = \{aH_1 \,:\, a \in H_2\} = H_2/_{H_1}$].

Dal teorema fondamentale di omomorfismo (applicato a φ), segue che

$$\frac{G/_{H_1}}{H_2/_{H_1}} = \frac{G/_{H_1}}{Ker\,\varphi} \cong Im\,\varphi = G/_{H_2}.$$

Corollario 5. (*Teorema di corrispondenza*). *Sia $H \trianglelefteq G$. Si denoti con $\mathbf{\Sigma}_H$ l'insieme dei sottogruppi di G contenenti H e con $\mathbf{\Sigma}(G/_H)$ l'insieme dei sottogruppi di $G/_H$.*

La proiezione canonica $\pi : G \to G/_H$ induce una biiezione tra $\mathbf{\Sigma}_H$ e $\mathbf{\Sigma}(G/_H)$, così definita:

$$T \to \pi(T) = T/_H, \quad \forall\, T \in \mathbf{\Sigma}_H.$$

Inoltre risulta, $\forall\, T \in \mathbf{\Sigma}_H$: $T \trianglelefteq G \iff \pi(T) \trianglelefteq G/_H$.

Dim. Verifichiamo che l'applicazione sopra definita è suriettiva. Per ogni $\boldsymbol{\mathcal{L}} \in \mathbf{\Sigma}(G/_H)$, la controimmagine $\pi^{-1}(\boldsymbol{\mathcal{L}})$ è un sottogruppo di G [infatti, $\forall\, x, y \in \pi^{-1}(\boldsymbol{\mathcal{L}})$ risulta $Hx, Hy \in \boldsymbol{\mathcal{L}}$ e quindi $Hx\cdot Hy^{-1} = Hxy^{-1} \in \boldsymbol{\mathcal{L}}$, cioè $xy^{-1} \in \pi^{-1}(\boldsymbol{\mathcal{L}})$]; inoltre $\pi^{-1}(\boldsymbol{\mathcal{L}}) \supseteq H$ [infatti, $\forall\, h \in H$, $Hh = H \in \boldsymbol{\mathcal{L}}$]. Dunque $\pi^{-1}(\boldsymbol{\mathcal{L}}) \in \mathbf{\Sigma}_H$. Ovviamente risulta: $\pi\big(\pi^{-1}(\boldsymbol{\mathcal{L}})\big) = \boldsymbol{\mathcal{L}}$ e quindi l'applicazione è suriettiva.

Verifichiamo ora che è iniettiva: siano $T_1, T_2 \in \mathbf{\Sigma}_H$ tali che $\pi(T_1) = \pi(T_2)$, cioè $T_1/_H = T_2/_H$, e dimostriamo che $T_1 = T_2$. Sia $x \in T_1$. Allora $Hx \in T_1/_H = T_2/_H$ e quindi $\exists\, y \in T_2$ tale che $Hx = Hy$. Quindi $xy^{-1} \in H \leq T_2$, da cui $x = xy^{-1}y \in T_2$. È così provato che $T_1 \subseteq T_2$ e in modo analogo si verifica l'inclusione opposta.

Veniamo ora all'ultima affermazione. Sia $T \trianglelefteq G$. Dal terzo teorema di isomorfismo, $G/_T \cong \frac{G/_H}{T/_H}$ e dunque $T/_H \trianglelefteq G/_H$, cioè $\pi(T) \trianglelefteq G/_H$. Viceversa, posto $T/_H \trianglelefteq G/_H$, vogliamo verificare che $T \trianglelefteq G$. Si consideri la composizione φ delle due proiezioni canoniche:

$$G \to G/_H, \quad G/_H \to \frac{G/_H}{T/_H}.$$

Risulta, $\forall\, x \in G$, $\varphi(x) = (Hx)T/_H$. In particolare si ha:

$$x \in Ker(\varphi) \iff Hx \in T/_H \iff Hx = Ht, \exists\, t \in T \iff xt^{-1} \in H, \exists\, t \in T.$$

Ovviamente $T \leq Ker(\varphi)$. Viceversa, se $x \in Ker(\varphi)$ e $xt^{-1} \in H$, allora (essendo $H \leq T$) $x = xt^{-1}t \in T$ e dunque $Ker(\varphi) \leq T$. È così dimostrato che $Ker(\varphi) = T$ e quindi $T \trianglelefteq G$.

Esercizio 1. Utilizzando opportunamente il teorema fondamentale di omomorfismo, verificare che esistono esattamente due omomorfismi non banali da $\boldsymbol{A}_4$ a $\boldsymbol{D}_6$.

Come ben noto, risulta:

$\boldsymbol{A}_4 = \{(1),\ (12)(34),\ (13)(24),\ (14)(23),\ (123),\ (132),\ (124),\ (142),\ (134),\ (143),\ (234),\ (243)\}$,

$\boldsymbol{D}_6 = \langle\, \varphi, \rho \mid \varphi^6 = \rho^2 = 1,\ \rho\circ\varphi = \varphi^5\circ\rho \,\rangle = \{1,\ \varphi,\ \varphi^2,\ \varphi^3,\ \varphi^4,\ \varphi^5,\ \rho,\ \varphi\circ\rho,\ \varphi^2\circ\rho,\ \varphi^3\circ\rho,\ \varphi^4\circ\rho,\ \varphi^5\circ\rho\}$.

I due gruppi hanno entrambi ordine 12, ma non sono isomorfi. Assumiamo nota la struttura del reticolo dei sottogruppi di $\boldsymbol{D}_6$ [cfr. **5 (B)**]. Relativamente ad $\boldsymbol{A}_4$, è noto (cfr. **Eserc. 5.1**) che tale gruppo possiede i seguenti sottogruppi propri:

- tre gruppi ciclici di ordine 2: $\langle(12)(34)\rangle$, $\langle(13)(24)\rangle$, $\langle(14)(23)\rangle$;
- quattro gruppi ciclici di ordine 3: $\langle(123)\rangle$, $\langle(124)\rangle$, $\langle(134)\rangle$, $\langle(234)\rangle$;
- un gruppo di Klein: $\boldsymbol{V} = \{(1),\ (12)(34),\ (13)(24),\ (14)(23)\}$.

Lasciamo per esercizio la verifica che di tali sottogruppi soltanto $\boldsymbol{V}$ è normale in $\boldsymbol{A}_4$. [Ad esempio si può verificare che $(12)(34)\langle(123)\rangle \neq \langle(123)\rangle(12)(34)$, ecc.].

Sia ora $f : \boldsymbol{A}_4 \to \boldsymbol{D}_6$ un omomorfismo non banale. Allora $Ker(f)$ è un sottogruppo normale di $\boldsymbol{A}_4$ e quindi a priori $Ker(f)$ è uno dei seguenti sottogruppi: $\boldsymbol{A}_4, \boldsymbol{V}, \{1\}$. Certamente $Ker(f) \neq \boldsymbol{A}_4$ [perché f è non banale]; inoltre $Ker(f) \neq \{1\}$ [perché altrimenti f sarebbe iniettiva e quindi biiettiva (avendo i due gruppi la stessa cardinalità); dunque $\boldsymbol{A}_4 \cong \boldsymbol{D}_6$: assurdo]. Allora necessariamente $Ker(f) = \boldsymbol{V}$. Inoltre

$$\boldsymbol{A}_4/_{\boldsymbol{V}} = \{\boldsymbol{V},\ (123)\boldsymbol{V},\ (132)\boldsymbol{V}\},$$

con $(123)\boldsymbol{V} = \{(123),\ (243),\ (142),\ (134)\}$, $(132)\boldsymbol{V} = \{(132),\ (234),\ (143),\ (124)\}$.

Dal teorema fondamentale di omomorfismo,

$$\overline{f} : \boldsymbol{A}_4/_{\boldsymbol{V}} \to Im(f),\ \text{ tale che }\ \overline{f}(x\boldsymbol{V}) = f(x),\ \ \forall\, x \in \boldsymbol{A}_4,$$

è un isomorfismo (tra gruppi di ordine 3). Poiché esiste un unico sottogruppo di ordine 3 di $\boldsymbol{D}_6$ [e cioè il ciclico $\langle\varphi^2\rangle \cong \boldsymbol{C}_3$], necessariamente $Im(f) = \langle\varphi^2\rangle$. Gli omomorfismi non banali richiesti sono quindi in corrispondenza biunivoca con gli isomorfismi da $\boldsymbol{A}_4/_{\boldsymbol{V}}$ a $\langle\varphi^2\rangle$ [ovvero con gli automorfismi di $\boldsymbol{C}_3$]. Si ottengono quindi i due isomorfismi

$$\overline{f}_1 : \begin{cases} \boldsymbol{V} \to 1 \\ (123)\boldsymbol{V} \to \varphi^2 \\ (132)\boldsymbol{V} \to \varphi^4 \end{cases} \qquad \overline{f}_2 : \begin{cases} \boldsymbol{V} \to 1 \\ (123)\boldsymbol{V} \to \varphi^4 \\ (132)\boldsymbol{V} \to \varphi^2. \end{cases}$$

Ad essi corrispondono i due unici omomorfismi non banali cercati:

$f_1 : \boldsymbol{A}_4 \to \boldsymbol{D}_6$, che trasforma $\boldsymbol{V}$ in 1, $(123)\boldsymbol{V}$ in φ^2, $(132)\boldsymbol{V}$ in φ^4;

$f_2 : \boldsymbol{A}_4 \to \boldsymbol{D}_6$, che trasforma $\boldsymbol{V}$ in 1, $(123)\boldsymbol{V}$ in φ^4, $(132)\boldsymbol{V}$ in φ^2.

Concludiamo il paragrafo estendendo il concetto di quoziente dai gruppi alle strutture algebriche più ricche che conosciamo: anelli e spazi vettoriali.

Cerchiamo quindi di dare una definizione di "*anello quoziente modulo un sottoanello*".

Sia $(A, +, \cdot)$ un anello e sia $(B, +, \cdot)$ un suo sottoanello [dunque $B - B \subseteq B$ e $B\,B \subseteq B$]. Poiché $(A, +)$ è un gruppo abeliano, $(B, +)$ ne è un sottogruppo normale. Dunque l'insieme dei suoi laterali (destri o sinistri) $A/_B = \{a + B,\ \forall\, a \in A\}$ è dotato di struttura di gruppo (abeliano) rispetto all'operazione $+$ così definita:

$$(a_1 + B) + (a_2 + B) = (a_1 + a_2) + B,\ \ \forall\, a_1 + B,\, a_2 + B \in A/_B.$$

Ci chiediamo se è possibile definire "in modo naturale" su $A/_B$ un'operazione di prodotto in modo da rendere $A/_B$ un anello. Poniamo:

$$(*) \qquad (a_1 + B)\cdot(a_2 + B) = a_1 \cdot a_2 + B,\ \ \forall\, a_1 + B,\, a_2 + B \in A/_B.$$

Se tale operazione è ben posta, $(A/_B, +, \cdot)$ è un anello [infatti si verifica subito che che il prodotto è associativo e valgono le leggi di distributività]. Inoltre, se A è commutativo ed unitario, anche $A/_B$ lo è [con unità $1_A + B$].

Tuttavia, il prodotto $(*)$ non è in generale ben definito. Consideriamo ad esempio l'anello $(\boldsymbol{Q}, +, \cdot)$ ed il suo sottoanello $(\boldsymbol{Z}, +, \cdot)$. Osserviamo che

$$\tfrac{4}{3} + \boldsymbol{Z} = \tfrac{1}{3} + \boldsymbol{Z},\ \tfrac{1}{2} + \boldsymbol{Z} = -\tfrac{1}{2} + \boldsymbol{Z},\ \text{ma }\ (\tfrac{4}{3} + \boldsymbol{Z})\cdot(\tfrac{1}{2} + \boldsymbol{Z}) \neq (\tfrac{1}{3} + \boldsymbol{Z})\cdot(-\tfrac{1}{2} + \boldsymbol{Z})$$

[infatti $\tfrac{4}{3}\cdot\tfrac{1}{2} - \tfrac{1}{3}\cdot(-\tfrac{1}{2}) = \tfrac{5}{6} \notin \boldsymbol{Z}$].

Verifichiamo ora che

il prodotto $(*)$ *è ben definito* $\iff$ B *verifica le due condizioni:* $A\,B \subseteq B$ *e* $B\,A \subseteq B$

[che sono condizioni più forti di $B\,B \subseteq B$].

($\Longrightarrow$). Siano $a \in A$ e $b \in B$. Si tratta di verificare che $ab, ba \in B$. Poiché $b + B = 0 + B$ [infatti $b - 0 \in B$], allora $(a+B)(b+B) = (a+B)(0+B)$ e dunque $ab + B = 0 + B$, da cui $ab - 0 = ab \in B$. In modo analogo si verifica che $ba \in B$.

($\Longleftarrow$). Siano $a_1 + B = a'_1 + B$ e $a_2 + B = a'_2 + B$ [cioè $a'_1 - a_1,\ a'_2 - a_2 \in B$]. Bisogna verificare che

$$a_1 a_2 + B = a'_1 a'_2 + B, \text{ cioè } a'_1 a'_2 - a_1 a_2 \in B.$$

Infatti: $a'_1 a'_2 - a_1 a_2 = a'_1 a'_2 - a'_1 a_2 + a'_1 a_2 - a_1 a_2 =$

$= a'_1(a'_2 - a_2) + (a'_1 - a_1) a_2 \in a'_1 B + B a_2 \subseteq AB + BA \subseteq B + B \subseteq B.$

Un sottoanello B di A verificante le due condizioni sopra indicate [cioè $A\,B \subseteq B$ e $B\,A \subseteq B$] è detto *ideale* (o *ideale bilatero*) di A. Viene preferibilmente denotato con lettera I.

Abbiamo così provato che, assegnato un ideale I di un anello A [cioè un sottoinsieme non vuoto $I \subseteq A$ tale che $I - I \subseteq I$ e $A\,I \subseteq I$ e $I\,A \subseteq I$], è definito l'*anello quoziente* $A/_I = \{a + I,\ \forall\, a \in A\}$.

Si può facilmente verificare che (in perfetta analogia con quanto avviene per i gruppi) vale il *teorema fondamentale di omomorfismo tra anelli*:

Se $f : A \to B$ è un omomorfismo di anelli, allora $Ker(f)$ è un ideale di A ed esiste un unico isomorfismo di anelli

$$F : A/_{Ker(f)} \to Im(f), \text{ tale che } F(a + Ker(f)) = f(a),\ \forall\, a + Ker(f) \in A/_{Ker(f)}.$$

Si noti che un sottoanello <u>unitario</u> B di A che sia un ideale coincide con tutto A [infatti risulta: $A = 1_A\, A \subseteq BA \subseteq B \subseteq A$ e quindi $B = A$].

Si può facilmente verificare che gli ideali di $(\boldsymbol{Z}, +, \cdot)$ sono tutti e soli i sottoanelli $k\boldsymbol{Z}$, $\forall\, k \in \boldsymbol{N}$, e che $\boldsymbol{Z}/_{k\boldsymbol{Z}} \cong \boldsymbol{Z}/_{\equiv_k} = \boldsymbol{Z}_k$, $\forall\, k \geq 2$. Analogamente gli ideali di $(K[X], +, \cdot)$ sono tutti e soli i sottoanelli $PK[X]$, $\forall\, P \in K[X]$, ed i rispettivi quozienti $K[X]/_{PK[X]}$ coincidono con gli anelli $K[X]/_{\equiv_P}$, studiati nel paragrafo **4** del precedente capitolo. Infatti, $\forall\, F \in K[X]$, $[F]_P = F + PK[X]$.

Si noti che $\boldsymbol{Z}$ e $K[X]$ condividono la seguente importante proprietà: entrambi sono *domini ad ideali principali*, cioè domini di integrità, in cui tutti gli ideali sono formati dai multipli di un solo elemento (*generatore* dell'ideale). Naturalmente tale proprietà discende dal teorema della divisione con resto, valido in entrambe le strutture.

Osservazione 4. Vogliamo estendere ai K-spazi vettoriali le considerazioni svolte sopra.

Sia V un K-spazio vettoriale e sia W un suo sottospazio vettoriale. Il gruppo quoziente $(V/_W, +)$ è un gruppo commutativo unitario [come lo è $(V, +)$]. Ci chiediamo se $V/_W$ è dotato di struttura di K-spazio vettoriale. In tal caso $V/_W$ è detto *spazio vettoriale quoziente di V modulo W*. Poniamo:

$$K \times V/_W \to V/_W \text{ tale che } (c, v + W) \to cv + W,\ \forall\, c \in K,\ \forall\, v + W \in V/_W.$$

Tale applicazione è ben definita: se infatti $v + W = v_1 + W$ [cioè $v_1 - v \in W$], allora $cv + W = cv_1 + W$ [infatti $cv_1 - cv = c(v_1 - v) \in W$].

Basta quindi verificare che l'operazione di moltiplicazione per uno scalare sopra definita soddisfa agli assiomi previsti dalla definizione di K-spazio vettoriale:

- $c\big((v_1 + W) + (v_2 + W)\big) = c(v_1 + W) + c(v_2 + W)$;
- $(c + d)(v + W) = c(v + W) + d(v + W)$;
- $(c \cdot d)(v + W) = c\big(d(v + W)\big)$;
- $1(v + W) = v + W$.

Si conclude che per ogni sottospazio vettoriale W di V è definito lo spazio vettoriale quoziente $V/_W$.

8. Esercizi del Capitolo IV

4.1. Siano $n,\, m \in \boldsymbol{Z}$ e sia $d = MCD(n,m)$.

(*i*) Verificare che $\langle n,\, m\rangle = \{nt + ms,\ \forall\, t, s \in \boldsymbol{Z}\}$.

(*ii*) Verificare che $\langle n,\, m\rangle = \langle d\rangle$.

(*iii*) Sia H un sottogruppo di $(\boldsymbol{Z}, +)$. Verificare che $H = \langle n\rangle$, con $n \in \boldsymbol{Z}$.

* * * * * * * * *

4.2. Sia G un gruppo <u>finito</u> e sia H un sottoinsieme non vuoto di G. Verificare che

$$H \leq G \iff H \cdot H \subseteq H.$$

* * * * * * * * *

4.3. Sia $\boldsymbol{L} = \{lg(n),\ \forall\, n \in \mathbf{N},\ n \geq 1\}$. Si denoti con $\langle \boldsymbol{L}\rangle$ il sottogruppo di $(\mathbf{R}, +)$ generato da $\boldsymbol{L}$. Verificare che $\langle \boldsymbol{L}\rangle \cong (\mathbf{Q}^+, \cdot)$ [con $\mathbf{Q}^+ = \{q \in \mathbf{Q} \,:\, q > 0\}$].

* * * * * * * * *

4.4. Per ogni $n \geq 1$ sia $\boldsymbol{C}_n$ il gruppo delle radici $n-$esime dell'unità e sia $\boldsymbol{C}_\infty := \bigcup\limits_{n\geq 1} \boldsymbol{C}_n$.

Sia inoltre $\boldsymbol{U} = \{z \in \boldsymbol{C} \,:\, \mathcal{N}(z) = 1\}$ (numeri complessi di norma 1).

(*i*) Verificare che $\boldsymbol{C}_\infty$ è un sottogruppo del gruppo moltiplicativo dei complessi $(\boldsymbol{C}^{\cdot}, \cdot)$.

(*ii*) Verificare che $\boldsymbol{C}_\infty = \{z \in \boldsymbol{C} \,:\, \circ(z) < \infty\}$.

(*iii*) Verificare che $\boldsymbol{U}$ è un sottogruppo di $(\boldsymbol{C}^{\cdot}, \cdot)$

(*iv*) Verificare che $\boldsymbol{C}_\infty$ è un sottogruppo di $\boldsymbol{U}$. Perché $\boldsymbol{C}_\infty \neq \boldsymbol{U}$?

* * * * * * * * *

4.5. Nel gruppo $\boldsymbol{S}_4$ sono assegnati i tre sottogruppi

$$H_1 = \langle (1,\, 2)\rangle, \quad H_2 = \langle (3,\, 4)\rangle, \quad H_3 = \langle (1,\, 4)\rangle.$$

(*i*) Verificare che H_1H_2 è un sottogruppo di $\boldsymbol{S}_4$ ed è un gruppo di Klein.

(*ii*) Verificare che H_1H_3 non è un sottogruppo di $\boldsymbol{S}_4$ e che $\langle H_1 \cup H_3\rangle \cong \boldsymbol{S}_3$.

(*iii*) Posto $H = \langle H_1 \cup H_2 \cup H_3\rangle$, verificare che H contiene tutti i 3-cicli di $\boldsymbol{S}_4$. Cosa se ne deduce ?

* * * * * * * * *

4.6. In $\boldsymbol{S}_5$ sono assegnate le tre permutazioni $a = (1\,2\,3)(4\,5)$, $b = (1\,2\,3)$, $c = (1\,2)$.

(*i*) Verificare che $\langle a,\, b\rangle \cong \boldsymbol{C}_6$.

(*ii*) Verificare che $\langle a,\, c\rangle \cong \boldsymbol{D}_6$.

(*iii*) Verificare che $\langle b,\, c\rangle \cong \boldsymbol{S}_3$.

* * * * * * * * *

4.7. Determinare le permutazioni di $\boldsymbol{S}_5$ aventi struttura ciclica $(\_\ \_\ \_)(\_\ \_)$ e quelle aventi struttura ciclica $(\_\ \_)(\_\ \_)$.

* * * * * * * * *

4.8. (*i*) Calcolare il numero delle permutazioni in $\boldsymbol{S}_6$ che sono prodotto di un 3-ciclo e di un 2-ciclo disgiunti.

(*ii*) Dedurre da (*i*) una formula che permetta di calcolare il numero delle permutazioni in $\boldsymbol{S}_n$ che sono prodotto di un k-ciclo e di un h-ciclo disgiunti, con $k > h$ (e ovviamente $h + k \leq n$).

* * * * * * * * *

4.9. Determinare tutte le strutture cicliche in $\boldsymbol{S}_{16}$, le cui permutazioni abbiano periodo 28. Indicare di ciascuna la parità.

* * * * * * * * *

4.10. Sia $\boldsymbol{A}_4$ il sottogruppo alterno di $\boldsymbol{S}_4$.

(*i*) Indicare gli elementi di $\boldsymbol{A}_4$.

(*ii*) Scelto in $\boldsymbol{A}_4$ il 3-ciclo $\sigma = (1\,2\,3)$, determinare tutti i coniugati di σ **in** $\boldsymbol{A}_4$. [Ovviamente $\sigma \sim \sigma'$ **in** $\boldsymbol{A}_4 \iff \exists\, \tau \in \boldsymbol{A}_4 \,:\, \tau^{-1}\sigma\tau = \sigma'$].

* * * * * * * * *

4.11. Sia $\mathfrak{T}$ un triangolo isoscele non equilatero. Indicati con 2, 3 i due vertici della base di $\mathfrak{T}$, verificare che $\boldsymbol{\mathcal{I}som}(\mathfrak{T}) = \langle (2,\,3) \rangle$.

* * * * * * * * *

4.12. Verificare che il gruppo $\big(\mathcal{U}(\boldsymbol{Z}_{50}), \cdot\big)$ è ciclico e determinarne tutti i generatori. Determinarne poi gli eventuali elementi di periodo 4.

* * * * * * * * *

4.13. [*Esame 10/6/03*] (*i*) Costruire il reticolo dei sottogruppi del gruppo $(\mathcal{U}(\boldsymbol{Z}_{15}), \cdot)$ degli elementi invertibili di $\boldsymbol{Z}_{15}$.

(*ii*) Verificato che tale gruppo possiede tre sottogruppi di ordine 2, costruire i tre quozienti relativi a tali sottogruppi e verificare se sono tra loro o meno isomorfi. In caso affermativo descrivere esplicitamente un isomorfismo.

* * * * * * * * *

4.14. [*Esame 1/7/03*] (*i*) Nel gruppo $\boldsymbol{S}_5$ determinare, se possibile, un sottogruppo isomorfo a ciascuno dei seguenti gruppi:

$$\boldsymbol{Z}_5, \quad \boldsymbol{K} \cong \boldsymbol{Z}_2 \times \boldsymbol{Z}_2 \text{ (gruppo di Klein)}, \quad \boldsymbol{S}_3, \quad \boldsymbol{Z}_7, \quad \boldsymbol{Z}_6.$$

(*ii*) Elencare le possibili strutture cicliche ed i relativi ordini degli elementi di $\boldsymbol{S}_5$.

(*iii*) Determinare una permutazione $\tau \in \boldsymbol{S}_5$ tale che risulti:

$$\sigma_1 = \tau\,\sigma_2\,\tau^{-1} \quad \text{dove } \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}.$$

* * * * * * * * *

4.15. [*Esame 2/2/04*] Si consideri il gruppo di permutazioni $\boldsymbol{S}_9$.

(*i*) Determinare la struttura ciclica delle permutazioni $\sigma \in \boldsymbol{S}_9$ di ordine 6 e classe dispari.

(*ii*) Determinare una permutazione $\tau \in \boldsymbol{S}_9$ tale che $\sigma_1 = \tau \circ \sigma_2 \circ \tau^{-1}$, con

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 9 & 3 & 6 & 4 & 8 & 1 & 2 \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 4 & 1 & 7 & 6 & 9 & 2 & 3 & 8 \end{pmatrix}.$$

(*iii*) Verificare se esistono quattro sottogruppi $\boldsymbol{H}_1, \boldsymbol{H}_2, \boldsymbol{H}_3, \boldsymbol{H}_4$ di $\boldsymbol{S}_9$, che siano isomorfi rispettivamente ai seguenti gruppi: $\boldsymbol{S}_7$, $\boldsymbol{Z}_{11}$, $\boldsymbol{D}_5$, $\boldsymbol{Z}_{15}$.

* * * * * * * * *

4.16. (*i*) Sia G un gruppo finito e sia m un divisore positivo dell'ordine di G. Se esiste un <u>unico</u> sottogruppo H di G di ordine m, verificare che $H \trianglelefteq G$.

(*ii*) Sia $(G, \cdot)$ un gruppo e siano H, K due suoi sottogruppi normali. Verificare che se $H \cap K = \{1\}$, i sottogruppi H, K commutano "elemento per elemento", cioè risulta $hk = kh$, $\forall\, h \in H$, $\forall\, k \in K$.

* * * * * * * * *

4.17. Sia $(G, \cdot)$ un gruppo e siano H, K due suoi sottogruppi permutabili elemento per elemento.

(*i*) Verificare che se $H \cap K = \{1\}$, allora $HK \cong H \times K$.

(*ii*) Verificare che se H, K sono finiti ed hanno ordini relativamente primi, allora $H \cap K = \{1\}$ e quindi $HK \cong H \times K$.

* * * * * * * * *

4.18. (*i*) Sia $G_1 \times G_2 \times \ldots \times G_t$ il prodotto diretto di t gruppi $(t \geq 2)$. Per ogni $i = 1, \ldots, t$, sia $g_i \in G_i$ un elemento di periodo finito. Verificare che

$$\circ\big((g_1,\, g_2,\, \ldots, g_t)\big) = mcm\big(\circ(g_1),\, \ldots, \circ(g_t)\big).$$

(*ii*) Facendo ricorso alla formula precedente, calcolare il periodo di $\overline{33} \in \boldsymbol{Z}_{420}$.

(*iii*) Se G_1, G_2, ... G_t sono gruppi ciclici finiti, di ordini a due a due coprimi e se g_1, g_2, ... g_t ne sono rispettivi generatori, verificare che $G_1 \times G_2 \times \ldots \times G_t$ è ciclico e $(g_1, g_2, \ldots g_t)$ ne è un generatore.

* * * * * * * * *

4.19. Verificare che se $(G, \cdot)$ è un gruppo finito tale che, per ogni divisore positivo d di $|G|$, ammette al più un solo sottogruppo di ordine d, allora G è ciclico.

* * * * * * * * *

4.20. (*i*) Verificare che $\boldsymbol{D}_6/_{\langle \varphi^3 \rangle} \cong \boldsymbol{S}_3$.

(*ii*) Esplicitare un isomorfismo tra tali gruppi.

* * * * * * * * *

4.21. Sia $\boldsymbol{V} = \{1, a, b, c\}$ il gruppo di Klein e sia $\boldsymbol{C}_4$ il gruppo delle radici complesse quarte dell'unità. Determinare l'insieme $\boldsymbol{\mathcal{H}om}(\boldsymbol{V}, \boldsymbol{C}_4)$ ed indicarne gli eventuali isomorfismi.

* * * * * * * * *

4.22. Sia $\mathbf{Q}$ il gruppo (delle unità) dei quaternioni.

(*i*) Verificare che $\langle -\underline{\mathbf{1}} \rangle$ è un sottogruppo normale di $\mathbf{Q}$.

(*ii*) Verificare che $\mathbf{Q}/_{\langle -\underline{\mathbf{1}} \rangle} \cong \boldsymbol{V}$ [gruppo di Klein].

* * * * * * * * *

4.23. Determinare il quoziente del gruppo moltiplicativo dei razionali non nulli $(\boldsymbol{Q}^{\cdot}, \cdot)$ modulo il sottogruppo $(\boldsymbol{C}_2, \cdot)$.

* * * * * * * * *

4.24. Determinare in $\boldsymbol{S}_4$ due sottogruppi propri $\boldsymbol{H}_1$, $\boldsymbol{H}_2$ tali che:

- $\{(1)\} \lhd \boldsymbol{H}_2 \lhd \boldsymbol{H}_1 \lhd \boldsymbol{S}_4$.
- i tre gruppi quoziente $\boldsymbol{S}_4/_{\boldsymbol{H}_1}$, $\boldsymbol{H}_1/_{\boldsymbol{H}_2}$, $\boldsymbol{H}_2$ sono abeliani.

Nota. Si dice che tale proprietà rende $\boldsymbol{S}_4$ un *gruppo risolubile*.

* * * * * * * * *

4.25. Determinare l'unico omomorfismo non banale dal gruppo $(\boldsymbol{C}_4, \cdot)$ [delle radici quarte dell'unità] al gruppo $(\mathbf{Z}_6, +)$. Indicare nucleo ed immagine di tale omomorfismo.

* * * * * * * * *

4.26. Determinare l'insieme $\boldsymbol{\mathcal{H}om}(\boldsymbol{C}_6, \boldsymbol{C}_{12})$. Di ciascuno dei 6 omomorfismi ottenuti indicare l'immagine ed il nucleo.

* * * * * * * * *

4.27. Determinare gli endomorfismi di $(\boldsymbol{C}_5, \cdot)$ [gruppo delle radici quinte dell'unità] che non sono automorfismi.

* * * * * * * * *

4.28. Determinare gli insiemi $\boldsymbol{\mathcal{H}om}(\boldsymbol{S}_3, \boldsymbol{Z}_3)$ e $\boldsymbol{\mathcal{H}om}(\boldsymbol{Z}_3, \boldsymbol{S}_3)$.

* * * * * * * * *

4.29. (*i*) Verificare che il gruppo moltiplicativo $\mathcal{U}(\boldsymbol{Z}_{15})$ [degli elementi invertibili di $\boldsymbol{Z}_{15}$] è un gruppo abeliano non ciclico di ordine 8.

(*ii*) Determinare un isomorfismo tra $\mathcal{U}(\boldsymbol{Z}_{15})$ ed il prodotto diretto $\boldsymbol{Z}_2 \times \boldsymbol{Z}_4$.

* * * * * * * * *

4.30. Considerati i gruppi $(\boldsymbol{Z}_{12}, +)$ e $(\boldsymbol{Z}_{18}, +)$:

(*i*) Determinare tutti gli omomorfismi da $\boldsymbol{Z}_{18}$ a $\boldsymbol{Z}_{12}$.

(*ii*) Determinare tutti gli omomorfismi da $\boldsymbol{Z}_{12}$ a $\boldsymbol{Z}_{18}$.

(*iii*) Verificare che esiste un unico endomorfismo non banale di $\boldsymbol{Z}_{12}$ ottenuto componendo un omomorfismo da $\boldsymbol{Z}_{12}$ a $\boldsymbol{Z}_{18}$ con uno da $\boldsymbol{Z}_{18}$ a $\boldsymbol{Z}_{12}$.

* * * * * * * * *

4.31. Indicato con $\mathbf{SL}_n(\boldsymbol{R})$ il gruppo delle matrici quadrate di ordine n aventi determinante $= 1$, verificare che:

(*i*) $\mathbf{SL}_n(\boldsymbol{R}) \lhd \mathbf{GL}_n(\boldsymbol{R})$.

(*ii*) $\mathbf{GL}_n(\boldsymbol{R})\big/_{\mathbf{SL}_n(\boldsymbol{R})} \cong (\boldsymbol{R}^{\cdot}, \cdot)$.

* * * * * * * * *

4.32. (*i*) Calcolare il centro $\boldsymbol{\mathcal{Z}}(\boldsymbol{S}_3)$ di $\boldsymbol{S}_3$ e dedurne il gruppo degli automorfismi interni di $\boldsymbol{S}_3$.

(*ii*) Determinare i gruppi $\boldsymbol{\mathcal{A}ut}(\boldsymbol{S}_3)$ e $\boldsymbol{\mathcal{A}ut}(\boldsymbol{S}_3)\big/_{\boldsymbol{\mathcal{I}}(\boldsymbol{S}_3)}$.

* * * * * * * * *

4.33. Sia $\boldsymbol{D}_4$ il gruppo diedrale del quadrato.

(*i*) Determinare il centro $\boldsymbol{\mathcal{Z}}(\boldsymbol{D}_4)$.

(*ii*) Verificare che il gruppo $\boldsymbol{\mathcal{I}}(\boldsymbol{D}_4)$ degli automorfismi interni di $\boldsymbol{D}_4$ è isomorfo al gruppo di Klein.

(*iii*) Determinare i quattro automorfismi interni di $\boldsymbol{D}_4$, esplicitandone le immagini di un sistema di generatori di $\boldsymbol{D}_4$.

(*iv*) Verificare che $\boldsymbol{D}_4$ ammette automorfismi non interni.

* * * * * * * * *

4.34. [*Esonero 3/6/03*] Indichiamo con $\boldsymbol{T}$ l'insieme delle matrici triangolari superiori in $\boldsymbol{GL}_2(\boldsymbol{Q})$. Sia $A_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \boldsymbol{T}$ e sia $\boldsymbol{H}$ il sottogruppo di $\boldsymbol{GL}_2(\boldsymbol{Q})$ generato da A_0.

(*i*) Verificare che $\boldsymbol{T}$ è un sottogruppo di $\boldsymbol{GL}_2(\boldsymbol{Q})$.

(*ii*) Verificare che $\boldsymbol{T}$ non è normale in $\boldsymbol{GL}_2(\boldsymbol{Q})$. [*Suggerimento*: indicata con B la matrice trasposta di A_0, verificare che $BA_0 \notin \boldsymbol{T}\, B$].

(*iii*) Descrivere gli elementi di $\boldsymbol{H}$.

(*iv*) Verificare se $\boldsymbol{H}$ è un sottogruppo normale di $\boldsymbol{T}$.

* * * * * * * * *

4.35. Sia $\boldsymbol{T} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},\ \forall\, a, b, c \in \mathbf{R},\, ac \neq 0 \right\}$ l'insieme delle matrici triangolari superiori in $\mathbf{GL}_2(\mathbf{R})$. In $\boldsymbol{T}$ si considerino i due sottoinsiemi

$$\boldsymbol{H}_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix},\ \forall\, a, b \in \mathbf{R} \right\}, \quad \boldsymbol{H}_2 = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},\ \forall\, b \in \mathbf{R},\, b \neq 0 \right\}.$$

(*i*) Verificare che $\boldsymbol{T}$ è un sottogruppo non normale di $\mathbf{GL}_2(\mathbf{R})$.

(*ii*) Verificare che $\boldsymbol{H}_1$ è un sottogruppo non normale di $\boldsymbol{T}$.

(*iii*) Verificare che $\boldsymbol{H}_2$ è un sottogruppo normale di $\boldsymbol{T}$.

* * * * * * * * *

4.36. [*Esame 10/6/03*] Sia $(\boldsymbol{G}, \cdot)$ un gruppo e sia $g_0 \in \boldsymbol{G}$. Si ponga:

$$\boldsymbol{C}(g_0) := \left\{ g \in \boldsymbol{G} \ :\ g_0\, g = g\, g_0 \right\}$$

[$\boldsymbol{C}(g_0)$ è detto *centralizzante* di g_0].

(*i*) Verificare che $\boldsymbol{C}(g_0)$ è un sottogruppo di $\boldsymbol{G}$.

(*ii*) Verificare che $\boldsymbol{C}(g_0)$ contiene il sottogruppo $\langle g_0 \rangle$ generato da g_0.

(*iii*) Considerato il gruppo diedrale del quadrato

$$\boldsymbol{D}_4 = \left\langle \varphi, \rho \colon\ \varphi^4 = \rho^2 = 1,\ \rho \circ \varphi = \varphi^3 \circ \rho \right\rangle,$$

determinare i sottogruppi $\boldsymbol{C}(\varphi)$ e $\boldsymbol{C}(\rho)$.

* * * * * * * * *

4.37. [*Esame 1/7/03*] Siano G e G' due gruppi isomorfi e sia $f_0 : G \to G'$ un isomorfismo.

(*i*) Verificare che i gruppi di automorfismi $\boldsymbol{\mathcal{A}ut}(G)$ e $\boldsymbol{\mathcal{A}ut}(G')$ sono isomorfi, esplicitando un isomorfismo tra essi.

(*ii*) Indicato con $\boldsymbol{\mathcal{I}som}(G, G')$ l'insieme degli isomorfismi da G a G', determinare una biiezione tra $\boldsymbol{\mathcal{I}som}(G, G')$ e $\boldsymbol{\mathcal{A}ut}(G)$.

(*iii*) Verificare che $\boldsymbol{\mathcal{A}ut}(\boldsymbol{Z}_9)$ e $\boldsymbol{\mathcal{A}ut}(\boldsymbol{Z}_7)$ sono gruppi isomorfi. Quanti isomorfismi esistono tra tali gruppi?

* * * * * * * * *

4.38. [*Esame 23/9/03*] Sono assegnati i gruppi $G = \mathcal{U}(\boldsymbol{Z}_{21})$ [gruppo degli elementi invertibili dell'anello $\boldsymbol{Z}_{21}$] e $G' = \boldsymbol{A}_4$ [sottogruppo alterno del gruppo delle permutazioni $\boldsymbol{S}_4$].

(*i*) Indicare gli elementi dei due gruppi e dire perché G non è isomorfo a G'.

(*ii*) Determinare i divisori d di $|G|$ per i quali esistono sottogruppi S di G e S' di G' tali che $|S| = |S'| = d$ e $S \cong S'$.

(*iii*) Verificare se esistono sottogruppi H di G e H' di G' tali che $G/_H \cong H'$.

* * * * * * * * *

4.39. [*Esame 23/9/03*] Nell'insieme $\boldsymbol{Z}_{18}$ si considerino i tre sottoinsiemi

$$S_1 = \{\overline{0}, \overline{5}, \overline{13}\}, \quad S_2 = \{\overline{0}, \overline{6}, \overline{12}\}, \quad S_3 = \{\overline{0}, \overline{7}, \overline{11}\}$$

e le tre corrispondenti relazioni ρ_i $(i = 1, 2, 3)$ così definite:

$$\overline{a}\,\rho_i\,\overline{b} \iff \overline{a} - \overline{b} \in S_i\,,\ \forall\,\overline{a}, \overline{b} \in \boldsymbol{Z}_{18}\,.$$

(*i*) Dire se tali relazioni sono riflessive, simmetriche e transitive.

(*ii*) Se ρ_i è una relazione di equivalenza, si determinino un intervallo di naturali $\boldsymbol{I}_k = \{0, 1, ..., k-1\}$ ed un'applicazione suriettiva $\varphi : \boldsymbol{Z}_{18} \to \boldsymbol{I}_k$ tale che ρ_i sia la relazione di equivalenza associata alla funzione φ. Si costruisca infine la biiezione φ^* tra $\boldsymbol{Z}_{18}/_{\rho_i}$ e $\boldsymbol{I}_k$ indotta da φ.

* * * * * * * * *

4.40. Utilizzando il secondo teorema di isomorfismo, verificare che in $(\boldsymbol{Z}_{12}, +)$ risulta

$$\langle\overline{3}\rangle/_{\langle\overline{6}\rangle} \cong \langle\overline{1}\rangle/_{\langle\overline{2}\rangle} \quad [\cong \boldsymbol{Z}_2].$$

Esplicitare un siffatto isomorfismo.

* * * * * * * * *

4.41. Sia $(G, \cdot)$ un gruppo non ciclico e di ordine 9.

(*i*) Indicati con a, b due elementi di G di periodo 3 e non legati tra loro da alcuna relazione algebrica, verificare che $G = \langle a, b\rangle$; scrivere tutti gli elementi di G e verificare che G è commutativo.

(*ii*) Determinare un isomorfismo tra G ed il prodotto diretto $\boldsymbol{Z}_3 \times \boldsymbol{Z}_3$.

(*iii*) Classificare (a meno di isomorfismi) tutti i gruppi di ordine 9.

* * * * * * * * *

4.42. [Proposto dallo studente V.Capraro]. Sia $(G, \cdot)$ un gruppo abeliano finito.

(*i*) Se $G = \{1, a_1, \ldots, a_n\}$ verificare che $(\prod_{i=1}^{n} a_i)^2 = 1$.

(*ii*) Dedurre da (*i*) che, se $(K, +, \cdot)$ è un campo finito e $K = \{0, 1, a_1, \ldots, a_n\}$, risulta

$$1 + \sum_{i=1}^{n} a_i = 0, \quad \prod_{i=1}^{n} a_i = \pm 1.$$

(*iii*) Sia K un campo finito. Sia $F \in K[X]$, con $\partial F \geq 1$. Sia $A = K[X]/_{(F)}$. Verificare che

$$F \text{ è irriducibile in } K[X] \iff \Big(\prod_{\alpha \in A^\cdot} \alpha\Big)^2 = 1.$$

* * * * * * * * *

4.43. Posto $X = \{1, 2, 3, 4, 5, 6\}$, determinare nel gruppo $\boldsymbol{S}_6 = \boldsymbol{S}(X)$ il sottogruppo $\boldsymbol{H}$ delle permutazioni che fissano i due sottoinsiemi $\{1, 2\}$ e $\{3, 4\}$ di X. Scrivere esplicitamente gli elementi di $\boldsymbol{H}$ e descrivere tale gruppo.

* * * * * * * * *

4.44. Siano $(G, \cdot)$, $(G', \cdot)$ due gruppi e sia $f : G \to G'$ un omomorfismo di gruppi.

Verificare che se $H' \trianglelefteq G'$, allora $f^{-1}(H') \trianglelefteq G$ ed il gruppo quoziente $G/_{f^{-1}(H')}$ è isomorfo ad un sottogruppo di $G'/_{H'}$.

* * * * * * * * *

Appendice 4

Polinomi ciclotomici

È noto dal **Cap.IV.2** che, $\forall\, n \geq 1$, il gruppo $\boldsymbol{C}_n$ delle radici complesse n-sime dell'unità ammette $\varphi(n)$ generatori: le radici primitive n-sime. Posto $\zeta_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, tali radici primitive n-sime sono esattamente le seguenti:

$$\zeta_n^{\,k}, \ \text{ con } \ MCD(k,n) = 1 \ \text{ e } \ 1 \leq k \leq n.$$

Definizione 1. *Il polinomio*

$$\Phi_n(X) = \prod_{1\leq k\leq n,\,(k,n)=1} (X - \zeta_n^{\,k})$$

è detto n-simo polinomio ciclotomico. È evidente che $\Phi_n(X)$ è monico ed ha grado $\varphi(n)$. A priori, $\Phi_n(X) \in \boldsymbol{C}[X]$ (ma dimostreremo tra poco che $\Phi_n(X) \in \boldsymbol{Z}[X]$).

Proposizione 1. *Risulta, per ogni $n \geq 1$:*

$$X^n - 1 = \prod_{d|n,\,1\leq d\leq n} \Phi_d(X).$$

Dim. È noto, per definizione di radice n-sima dell'unità, che

$$X^n - 1 = \prod_{k=1}^{n} (X - \zeta_n^{\,k}).$$

È inoltre noto che ogni $\zeta_n^{\,k}$ è una radice primitiva d-sima dell'unità, per un unico divisore positivo d di n [se infatti $\circ(\zeta_n^{\,k}) = \frac{n}{(k,n)} = d$, allora $\langle\, \zeta_n^{\,k} \,\rangle = \boldsymbol{C}_d$, cioè $\zeta_n^{\,k}$ è una radice primitiva d-sima dell'unità]. Pertanto il polinomio $X - \zeta_n^{\,k}$ è un fattore di $\Phi_d(X)$. Suddividendo opportunamente le radici n-sime dell'unità, si ottiene l'uguaglianza polinomiale cercata.

Nota. Segue da tale uguaglianza che $n = \sum_{d|n,\,1\leq d\leq n} \varphi(d)$

Tale risultato viene applicato per determinare ricorsivamente i polinomi ciclotomici. Si ha ad esempio:

$\Phi_1(X) = X - 1,$

$\Phi_2(X) = (X^2 - 1)\big/_{\Phi_1(X)} = X + 1,$

$\Phi_3(X) = (X^3 - 1)\big/_{\Phi_1(X)} = X^2 + X + 1,$

$\Phi_4(X) = (X^4 - 1)\big/_{\Phi_1(X)\,\Phi_2(X)} = (X^4 - 1)\big/_{(X-1)(X+1)} = X^2 + 1,$

...

$\Phi_6(X) = (X^6 - 1)\big/_{\Phi_1(X)\,\Phi_2(X)\,\Phi_3(X)} = (X^6 - 1)\big/_{(X-1)(X+1)(X^2+X+1)} = X^2 - X + 1,$

...

$\Phi_p(X) = (X^p - 1)\big/_{\Phi_1(X)} = (X^p - 1)\big/_{(X-1)} = X^{p-1} + X^{p-2} + \,...\, + X + 1 \ \ (\forall\, p \ \text{ primo}).$

Corollario 1. *Per ogni $n \geq 1$, $\Phi_n(X) \in \boldsymbol{Z}[X]$.*

Dim. Per induzione forte su $n \geq 1$. Per $n = 1$ risulta $\Phi_1(X) = X - 1 \in \boldsymbol{Z}[X]$. Sia $n \geq 2$ e si assuma che, $\forall\, h = 1, \,..., n-1$, $\Phi_h(X) \in \boldsymbol{Z}[X]$. Si vuole dimostrare che $\Phi_n(X) \in \boldsymbol{Z}[X]$.

Si ponga $G := \prod_{d|n,\, 1\le d<n} \Phi_d(X)$. Per ipotesi induttiva, G è prodotto di polinomi in $\boldsymbol{Z}[X]$ e dunque $G \in \boldsymbol{Z}[X]$. Inoltre G è monico. È noto che in $\boldsymbol{Z}[X]$ è possibile eseguire la divisione euclidea, *a patto che il divisore sia monico*: dunque in $\boldsymbol{Z}[X]$ è possibile dividere $X^n - 1$ per G. Il quoziente di tale divisione è lo stesso che si otterrebbe se si eseguisse la divisione euclidea in $\boldsymbol{C}[X]$ e dunque coincide con $(X^n - 1)/_G = \Phi_n(X)$. Pertanto $\Phi_n(X) \in \boldsymbol{Z}[X]$.

Enunciamo il seguente risultato (la cui dimostrazione è semplice se n è la potenza di un primo), per il quale rinviamo a [**Stillwell**], pag. 71-72.

Teorema 1. *Per ogni $n \ge 1$, $\Phi_n(X)$ è un polinomio irriducibile (in $\boldsymbol{Z}[X]$).*

Osservazione 1. Il teorema precedente consente di fattorizzare facilmente (con fattori irriducibili) i polinomi del tipo $X^n - 1 \in \boldsymbol{Z}[X]$. Ad esempio, posto $n = 35$, si ha:

$$X^{35} - 1 = \Phi_1(X)\cdot\Phi_5(X)\cdot\Phi_7(X)\cdot\Phi_{35}(X)\,.$$

I quattro fattori irriducibili di $X^{35} - 1$ sono:

$\Phi_1(X) = X - 1, \quad \Phi_5(X) = X^4 + X^3 + X^2 + X + 1, \quad \Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1,$

$\Phi_{35}(X) = (X^{35} - 1)/_{\Phi_1(X)\,\Phi_5(X)\,\Phi_7(X)} = (X^{35} - 1)/_{(X^{11}+X^{10}+X^9+X^8+X^7-X^5-X^4-X^3-X^2-X-1)}.$

Eseguendo la divisione euclidea, si ottiene

$$\Phi_{35}(X) = X^{24} - X^{23} + X^{19} - X^{18} + X^{17} - X^{16} + X^{14} - X^{13} + X^{12} - X^{11} + X^{10} - X^8 + X^7 - X^6 + X^5 + X - 1.$$

Bibliografia

M.Fontana, S.Gabelli. *Insiemi, numeri, polinomi.* CISU, 1989
G.M. Piacentini Cattaneo. *Algebra.* Decibel - Zanichelli, 1996
R.Procesi Ciampi. *Lezioni di Algebra* - un primo modulo. Accademica, 2003.
B.Scimemi. *Algebretta. Un'introduzione al corso di algebra ...* Decibel - Zanichelli, 1972.
B.Scimemi. *Gruppi.* Decibel - Zanichelli, 1972, ... ,1993.

Testi per approfondimenti:
R.B.Allenby. *Rings,Fields and Groups. An introduction to Abstract Algebra.* Arnold, 1983.
M.A.Armstrong. *Groups and Symmetry.* UTM Springer V., 1988.
M.Artin. *Algebra.* Prentice Hall, 1991.
L.Childs. *A Concrete Introduction to Higher Algebra.* Springer V., 1983.
I.N.Herstein. *Algebra.* Editori Riuniti, 1982.
A.Machì. *Introduzione alla teoria dei gruppi.* Feltrinelli, 1974.
J.Stillwell. *Elements of Algebra: geometry, numbers, equations.* Springer V., 1994.

Testi per esercizi:
M.Fontana, S.Gabelli. *Esercizi di Algebra.* Aracne, 1993
R.Procesi Ciampi, R.Rota. *Algebra moderna. Esercizi.* Masson Ed. Veschi, 1996