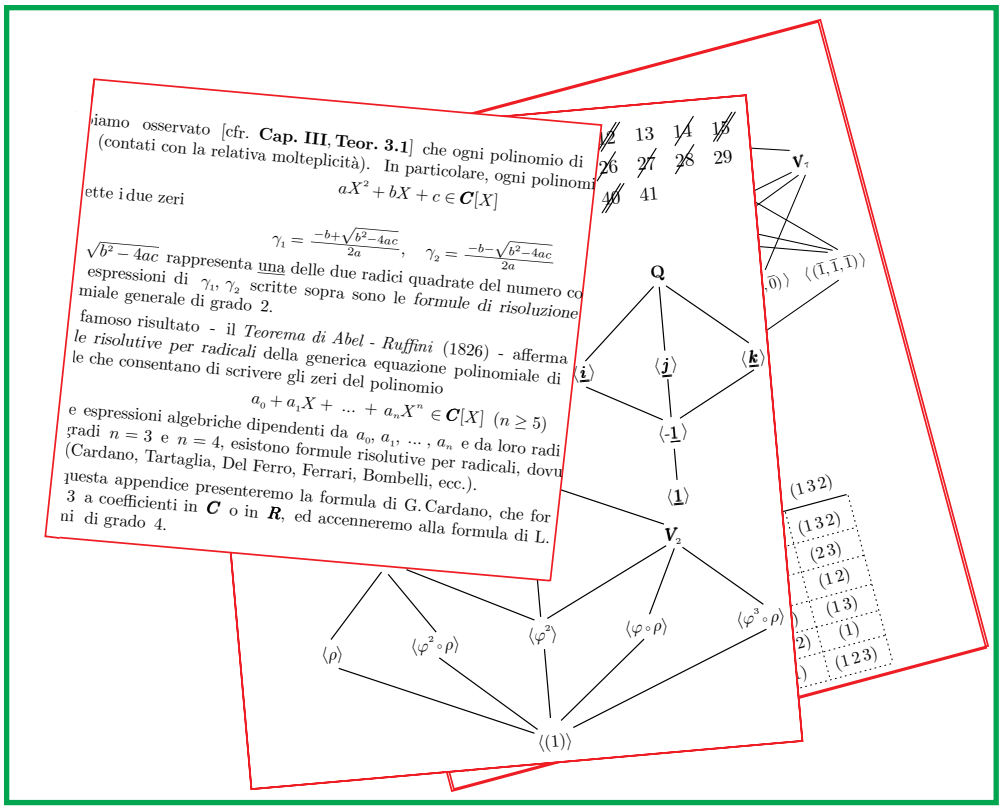
Università degli Studi di Roma "La Sapienza"
Dipartimento di Matematica "G.Castelnuovo"
A.A. 2004-2005

GIULIO CAMPANELLA

APPUNTI DI ALGEBRA 1

Duecento esercizi svolti



In questo volume sono raccolti quasi duecento esercizi di Algebra, relativi al corso 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.

Gli argomenti presentati e le notazioni usate fanno riferimento al testo ***Appunti di Algebra 1*** *(Edizioni Nuova Cultura, 2005), che raccoglie le lezioni del corso.*

Indice

Esercizi del Capitolo I 1
Esercizi del Capitolo II 23
Esercizi del Capitolo III 31
Esercizi del Capitolo IV 51
Altri esercizi 73

Soluzioni degli 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

$$\neg(\mathcal{P} \vee \mathcal{Q}) \quad \text{e} \quad (\neg\mathcal{P}) \wedge (\neg\mathcal{Q})$$

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

$$\mathcal{P} \wedge (\mathcal{Q} \vee \mathcal{R}) \quad \text{e} \quad (\mathcal{P} \wedge \mathcal{Q}) \vee (\mathcal{P} \wedge \mathcal{R}).$$

(*iii*) Assegnate due proposizioni $\mathcal{P}$, $\mathcal{Q}$, verificare che sono logicamente equivalenti le due proposizioni

$$\mathcal{P} \not\Longrightarrow \mathcal{Q} \quad \text{e} \quad \mathcal{P} \wedge \neg\mathcal{Q}.$$

Soluzione. Siano $\mathcal{P}$, $\mathcal{Q}$ due proposizioni. Le tavole di verità della negazione di $\mathcal{P}$, dell'intersezione $\mathcal{P} \wedge \mathcal{Q}$ e dell'unione $\mathcal{P} \vee \mathcal{Q}$ sono le seguenti:

$\mathcal{P}$	$\neg\mathcal{P}$
V	**F**
F	**V**

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

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

(*i*) Le due proposizioni $\mathcal{P}$, $\mathcal{Q}$ possono essere vere o false. Si hanno quindi quattro possibili combinazioni di vero-falso per le coppie $(\mathcal{P}, \mathcal{Q})$. Per ciascuna di esse scriviamo le corrispondenti tavole di verità di $\neg\mathcal{P}$, $\neg\mathcal{Q}$, $\mathcal{P} \vee \mathcal{Q}$, $\neg(\mathcal{P} \vee \mathcal{Q})$ e $(\neg\mathcal{P}) \wedge (\neg\mathcal{Q})$. Basta poi confrontare le ultime due colonne e vedere che coincidono.

$\mathcal{P}$	$\mathcal{Q}$	$\neg\mathcal{P}$	$\neg\mathcal{Q}$	$\mathcal{P} \vee \mathcal{Q}$	$\neg(\mathcal{P} \vee \mathcal{Q})$	$\neg(\mathcal{P}) \wedge \neg(\mathcal{Q})$
V	**V**	**F**	**F**	**V**	**F**	**F**
V	**F**	**F**	**V**	**V**	**F**	**F**
F	**V**	**V**	**F**	**V**	**F**	**F**
F	**F**	**V**	**V**	**F**	**V**	**V**

(*ii*) Le tre assegnate proposizioni $\mathcal{P}$, $\mathcal{Q}$, $\mathcal{R}$ possono essere vere o false. Si hanno quindi otto possibili combinazioni di vero-falso per le terne $(\mathcal{P}, \mathcal{Q}, \mathcal{R})$. Per ciascuna di esse scriviamo le corrispondenti tavole di $\mathcal{Q} \vee \mathcal{R}$, $\mathcal{P} \wedge \mathcal{Q}$, $\mathcal{P} \wedge \mathcal{R}$, $\mathcal{P} \wedge (\mathcal{Q} \vee \mathcal{R})$ e $(\mathcal{P} \wedge \mathcal{Q}) \vee (\mathcal{P} \wedge \mathcal{R})$. Basta poi confrontare le ultime due colonne e vedere che coincidono.

$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{R}$	$\mathcal{Q} \vee \mathcal{R}$	$\mathcal{P} \wedge \mathcal{Q}$	$\mathcal{P} \wedge \mathcal{R}$	$\mathcal{P} \wedge (\mathcal{Q} \vee \mathcal{R})$	$(\mathcal{P} \wedge \mathcal{Q}) \vee (\mathcal{P} \wedge \mathcal{R})$
V	**V**	**V**	**V**	**V**	**V**	**V**	**V**
V	**V**	**F**	**V**	**V**	**F**	**V**	**V**
V	**F**	**V**	**V**	**F**	**V**	**V**	**V**
V	**F**	**F**	**F**	**F**	**F**	**F**	**F**
F	**V**	**V**	**V**	**F**	**F**	**F**	**F**
F	**V**	**F**	**V**	**F**	**F**	**F**	**F**
F	**F**	**V**	**V**	**F**	**F**	**F**	**F**
F	**F**	**F**	**F**	**F**	**F**	**F**	**F**

Nota. È evidente che anche le proposizioni $\mathcal{P} \vee (\mathcal{Q} \wedge \mathcal{R})$ e $(\mathcal{P} \vee \mathcal{Q}) \wedge (\mathcal{P} \vee \mathcal{R})$ sono logicamente equivalenti. Tali equivalenze sono note come *formule di De Morgan*.

(*iii*) Procedendo come nei due casi precedenti, basterà confrontare le tavole di verità di $\neg(\mathcal{P} \Longrightarrow \mathcal{Q})$ e $\mathcal{P} \wedge \neg\mathcal{Q}$. Infatti

$\mathcal{P}$	$\mathcal{Q}$	$\neg\mathcal{Q}$	$\mathcal{P}\wedge\neg\mathcal{Q}$	$\mathcal{P}\Longrightarrow\mathcal{Q}$	$\neg(\mathcal{P}\Longrightarrow\mathcal{Q})$
V	**V**	**F**	**F**	**V**	**F**
V	**F**	**V**	**V**	**F**	**V**
F	**V**	**F**	**F**	**V**	**F**
F	**F**	**V**	**F**	**V**	**F**

* * *

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.

Soluzione. (*i*) Si ha: $x\in A-(B-C) \iff x\in A\wedge(x\notin B-C)$.

Si osservi che $x\in B-C \iff x\in B\wedge x\notin C$. Negando tale equivalenza, si ottiene

$$x\notin B-C \iff x\notin B\vee x\in C.$$

Ne segue:

$x\in A-(B-C) \iff x\in A\wedge[x\notin B\vee x\in C] \iff$

$[x\in A\wedge x\notin B]\vee[x\in A\wedge x\in C] \iff (x\in A-B)\vee(x\in A\cup C) \iff x\in(A-B)\cup(A\cap C)$.

(*ii*) Si ha:

$x\in(A-B)-C \iff (x\in A-B)\wedge(x\notin C) \iff [x\in A\wedge x\notin B]\wedge(x\notin C) \iff$

$x\in A\wedge[x\notin B\wedge x\notin C] \iff x\in A\wedge[x\notin B\cup C] \iff x\in A-(B\cup C)$.

(*iii*) Da (*ii*) e dall'ovvia inclusione $B-C\subseteq B\cup C$ segue:

$$A-(B-C)\supseteq A-(B\cup C)=(A-B)-C.$$

Un esempio in cui tale inclusione è stretta può essere ottenuto ponendo $A=B=C\neq\emptyset$. Infatti si ha:

$$(A-A)-A=\emptyset-A=\emptyset, \text{ mentre } A-(A-A)=A-\emptyset=A\neq\emptyset.$$

* * *

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

Soluzione. (*i*) Si ha:

$x\in(A\cup B)-C \iff (x\in A\cup B)\wedge x\notin C \iff [x\in A\vee x\in B]\wedge(x\notin C) \iff$

$[x\in A\wedge x\notin C]\vee[x\in B\wedge x\notin C] \iff (x\in A-C)\vee(x\in B-C) \iff x\in(A-C)\cup(B-C)$.

Si ha:

$x\in(A\cap B)-C \iff [x\in A\wedge x\in B]\wedge x\notin C \iff [x\in A\wedge x\notin C]\wedge[x\in B\wedge x\notin C] \iff$

$(x\in A-C)\wedge(x\in B-C) \iff x\in(A-C)\cap(B-C)$.

(*ii*) Si ha:

$x\in A\cap(B-C) \iff (x\in A)\wedge[x\in B\wedge x\notin C] \iff [x\in A\wedge x\in B]\wedge[x\in A\wedge x\notin C] \iff$

$x\in(A\cap B)\cap(A-C)$.

(*iii*) Si denoti con X un insieme contenente $A\cup B\cup C$. Risulta:

$x\in A\cup(B-C) \iff x\in A\vee[x\in B\wedge x\notin C] \iff [x\in A\vee x\in B]\wedge[x\in A\vee x\notin C] \iff$

$[x\in A\cup B]\wedge[x\in A\cup(X-C)] \iff x\in(A\cup B)\cap T$ con $T=A\cup(X-C)$.

Si può anche osservare che $T = X - (C - A)$. Infatti:

$$x \in X - (C - A) \iff x \in X \wedge x \notin C - A \iff x \notin C - A \iff$$
$$\iff (x \in A) \vee (x \notin C) \iff x \in A \cup (X - C)].$$

* * *

1.4. (*i*) 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 $f^{-1}(f(\boldsymbol{D}))$.

Soluzione. (*i*) Risulta: $f(x) = f(-x), \ \forall\, x \in \boldsymbol{Z}$. Dunque f non è iniettiva.

Risulta: $Im(f) = \{1, 2, 5, 10, 17, 26, 37, 50, 65, 82, \dots\}$. Ad esempio $0 \notin Im(f)$. Dunque f non è suriettiva.

(*ii*) Si ponga $A = \boldsymbol{N}$. Si ha, $\forall\, x, y \in A : \ x^2 + 1 = y^2 + 1 \Longrightarrow x^2 = y^2 \Longrightarrow x = y$. Dunque $f_{|\boldsymbol{N}}$ è iniettiva.

Sia ora B tale che $\boldsymbol{N} \subset B \subset \boldsymbol{Z}$. Se $y \in B - \boldsymbol{N}$, allora $f(y) = y^2 + 1 = f(-y)$. Essendo $y \neq -y$, $f_{|B}$ non è iniettiva. Pertanto $A = \boldsymbol{N}$ è massimale rispetto alla proprietà che $f_{|A}$ è iniettiva.

(*iii*) Si ha: $f^{-1}(\boldsymbol{P}) = \big\{x \in \boldsymbol{Z} \mid f(x) \in \boldsymbol{P}\big\} = \big\{x \in \boldsymbol{Z} \mid x^2 + 1 \text{ è pari}\big\} = \big\{x \in \boldsymbol{Z} \mid x^2 \text{ è dispari}\big\}\big\} = \boldsymbol{Z} - 2\boldsymbol{Z}$ (interi dispari).

Analogamente, $f^{-1}(\boldsymbol{D}) = \big\{x \in \boldsymbol{Z} \mid f(x) \in \boldsymbol{D}\big\} = \big\{x \in \boldsymbol{Z} \mid x^2 \text{ è pari}\big\} = 2\boldsymbol{Z}$ (interi pari).

(*iv*) Si ha: $f(\boldsymbol{N}) = Im(f)$ e dunque $f^{-1}(f(\boldsymbol{N})) = f^{-1}(Im(f)) = \boldsymbol{Z}$.

Si ha:

$$f^{-1}(f(\boldsymbol{P})) = \big\{x \in \boldsymbol{Z} \mid f(x) = f(y), \ \exists\, y \in \boldsymbol{P}\big\} = \big\{x \in \boldsymbol{Z} \mid x^2 + 1 = (2n)^2 + 1, \ \exists\, n \in \boldsymbol{N}\big\} =$$
$$\big\{x \in \boldsymbol{Z} \mid x^2 = (2n)^2, \ \exists\, n \in \boldsymbol{N}\big\} = \big\{x \in \boldsymbol{Z} \mid x = \pm 2n, \ \exists\, n \in \boldsymbol{N}\big\} = \big\{\pm 2n, \ \ \forall\, n \in \boldsymbol{N}\big\} = 2\boldsymbol{Z}.$$

Si ha infine:

$$f^{-1}(f(\boldsymbol{D})) = \big\{x \in \boldsymbol{Z} \mid x^2 + 1 = (2n + 1)^2 + 1, \ \exists\, n \in \boldsymbol{N}\big\} = \big\{x \in \boldsymbol{Z} \mid x = \pm(2n + 1), \ \exists\, n \in \boldsymbol{N}\big\} =$$
$$\big\{\pm(2n + 1), \ \ \forall\, n \in \boldsymbol{N}\big\} = \boldsymbol{Z} - 2\boldsymbol{Z}.$$

* * *

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}.

Soluzione. (*i*) Sia $f(n) = f(m)$. Se n, m sono pari: $n - 1 = m - 1 \Longrightarrow n = m$. Se n, m sono dispari: $n + 1 = m + 1 \Longrightarrow n = m$. Se $n = 2h$ è pari e $m = 2k + 1$ è dispari: $2h - 1 = (2k + 1) + 1 \Longrightarrow 2h - 2k = 3$: assurdo. Analogamente si ottiene un assurdo se n è dispari e m è pari. Si conclude che f è iniettiva.

(*ii*) Sia $a \in \boldsymbol{Z}$. Se $a = 2h$, $f(2h-1) = (2h-1)+1 = a$. Se $a = 2h+1$, $f(2h+2) = (2h+2)-1 = a$. Dunque f è suriettiva.

(*iii*) Da (*i*) e (*ii*) f è biiettiva. Per calcolarne l'inversa $g := f^{-1}$, si osservi da (*ii*) che

$$g(2h) = 2h - 1, \ g(2h + 1) = 2h + 2.$$

Dunque $f^{-1} = f$.

Nota Si può in effetti verificare che $f^2 = \mathbf{1}_{\boldsymbol{Z}}$. Infatti si ha:

$f^2(2h) = f\big(f(2h)\big) = f(2h-1) = 2h-1+1 = 2h = \mathbf{1}_{\boldsymbol{Z}}(2h)$,
$f^2(2h+1) = f\big(f(2h+1)\big) = f(2h+2) = 2h+2-1 = 2h+1 = \mathbf{1}_{\boldsymbol{Z}}(2h+1)$.

* * *

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.

Soluzione. (*i*) Sia $f(a_1) = f(a_2)$. Allora $g(f(a_1)) = g(f(a_2))$, cioè $(g \circ f)(a_1) = (g \circ f)(a_2)$. Essendo $g \circ f$ iniettiva, allora $a_1 = a_2$ e quindi f è iniettiva.

(*ii*) Sia $c \in C$. Esiste $a \in A$ tale che $(g \circ f)(a) = c$. Allora $g(f(a)) = c$, cioè $f(a) \in g^{-1}(c)$. Ne segue che g è suriettiva.

(*iii*) Siano $b_1, b_2 \in B$ tali che $g(b_1) = g(b_2)$. Poiché f è suriettiva, $\exists\, a_1, a_2 \in A$ tali che $f(a_1) = b_1$ e $f(a_2) = b_2$. Allora $(g \circ f)(a_1) = g(b_1) = g(b_2) = (g \circ f)(a_2)$. Essendo $g \circ f$ iniettiva, allora $a_1 = a_2$ e quindi $b_1 = f(a_1) = f(a_2) = b_2$. Dunque g è iniettiva.

(*iv*) Sia $b \in B$ e sia $c = g(b)$. Poiché $g \circ f$ è suriettiva, $\exists\, a \in A$ tale che $g(f(a)) = c$. Essendo g iniettiva, da $g(f(a)) = c = g(b)$ segue che $f(a) = b$, cioè $fa \in f^{-1}(b)$. Dunque f è suriettiva.

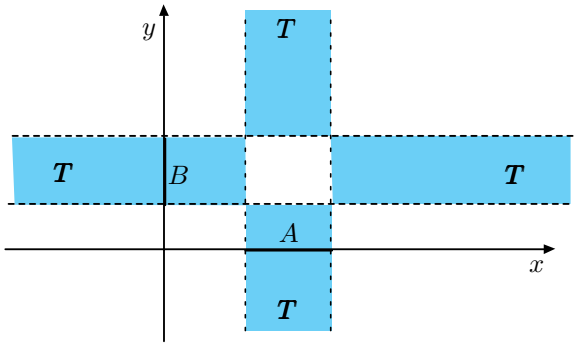
(*v*) Sia $A = \{a_1, a_2\}$, $B = \{b_1, b_2, b_3\}$, $C = \{c_1, c_2\}$. Siano $f : A \to B$, $g : B \to C$ tali che:

$$f(a_1) = b_1,\ f(a_2) = b_2; \quad g(b_1) = c_1,\ g(b_2) = g(b_3) = c_2.$$

Le due applicazioni f, g verificano le condizioni richieste.

* * *

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 $\boldsymbol{S}_1$, $\boldsymbol{S}_2$.

Soluzione. (*i*) $\boldsymbol{T}$ è unione delle sue due semistrisce orizzontali, che sono descritte dal prodotto cartesiano $(\boldsymbol{R} - A) \times B$, e delle sue due semistrisce verticali, che sono descritte dal prodotto cartesiano $A \times (\boldsymbol{R} - B)$. Dunque

$$\boldsymbol{T} = \big[(\boldsymbol{R} - A) \times B\big] \cup \big[A \times (\boldsymbol{R} - B)\big].$$

(*ii*) Si osserva subito che $\boldsymbol{S} = \mathbf{C}_{\boldsymbol{R}^2}(\boldsymbol{T})$. Tenuto conto della formula:

(*) $\mathbf{C}_X(A_1 \cup A_2) = \mathbf{C}_X A_1 \cap \mathbf{C}_X A_2$, $\forall\, A_1,\ A_2 \subseteq X$,

da (*i*) segue che

$$\boldsymbol{S} = \mathbf{C}_{\boldsymbol{R}^2}(\boldsymbol{T}) = \mathbf{C}_{\boldsymbol{R}^2}\big[(\mathbf{C}_{\boldsymbol{R}}A\times B)\cup(A\times\mathbf{C}_{\boldsymbol{R}}B)\big] = \mathbf{C}_{\boldsymbol{R}\times\boldsymbol{R}}\big(\mathbf{C}_{\boldsymbol{R}}A\times B\big)\cap\mathbf{C}_{\boldsymbol{R}\times\boldsymbol{R}}\big(A\times\mathbf{C}_{\boldsymbol{R}}B)\big) =: \boldsymbol{S}_1\cap\boldsymbol{S}_2.$$

Tenuto poi conto della formula:

$(**)\ \ \mathbf{C}_{X\times Y}(A_1\times A_2) = \big(\mathbf{C}_X A_1\times Y\big)\cup\big(X\times\mathbf{C}_Y A_2\big),\ \ \forall\, A_1\subseteq X,\ A_2\subseteq Y,$

si ha:

$$\boldsymbol{S}_1 = \mathbf{C}_{\boldsymbol{R}\times\boldsymbol{R}}\big((\mathbf{C}_{\boldsymbol{R}}A)\times B\big) = \big((\mathbf{C}_{\boldsymbol{R}}(\mathbf{C}_{\boldsymbol{R}}A)\times\boldsymbol{R}\big)\cup(\boldsymbol{R}\times\mathbf{C}_{\boldsymbol{R}}B) = (A\times\boldsymbol{R})\cup\big(\boldsymbol{R}\times(\boldsymbol{R}-B)\big)$$
$$\boldsymbol{S}_2 = \mathbf{C}_{\boldsymbol{R}\times\boldsymbol{R}}\big(A\times(\mathbf{C}_{\boldsymbol{R}}B)\big) = (\mathbf{C}_{\boldsymbol{R}}A\times\boldsymbol{R})\cup\big(\boldsymbol{R}\times(\mathbf{C}_{\boldsymbol{R}}(\mathbf{C}_{\boldsymbol{R}}B)\big) = \big((\boldsymbol{R}-A)\times\boldsymbol{R}\big)\cup\big(\boldsymbol{R}\times B\big).$$

* * *

1.8. Sia $f:\boldsymbol{R}\to\boldsymbol{R}$ l'applicazione così definita:

$$f(x) = [x],\ \forall\, x\in\boldsymbol{R}\quad [\text{dove } [x] \text{ denota la } \textit{parte intera di } x, \text{ cioè il massimo intero } \leq x].$$

Posto $A = 2\boldsymbol{N} = \{0,\,2,\,4,\,6,\,8,\,\ldots\}$, individuare gli insiemi $f^{-1}\big(f(A)\big)$ e $f\big(f^{-1}(A)\big)$.

Soluzione. Si noti che f induce l'identità su $\boldsymbol{Z}$. Ne segue in particolare che $f(2\boldsymbol{N}) = 2\boldsymbol{N}$. Allora:

$$f^{-1}\big(f(2\boldsymbol{N})\big) = f^{-1}(2\boldsymbol{N}) = \{x\in\boldsymbol{R}\ :\ [x]\in 2\boldsymbol{N}\} = [0,1)\cup[2,3)\cup[4,5)\cup\ \ldots = \bigcup_{k\geq 0}[2k,2k+1),$$

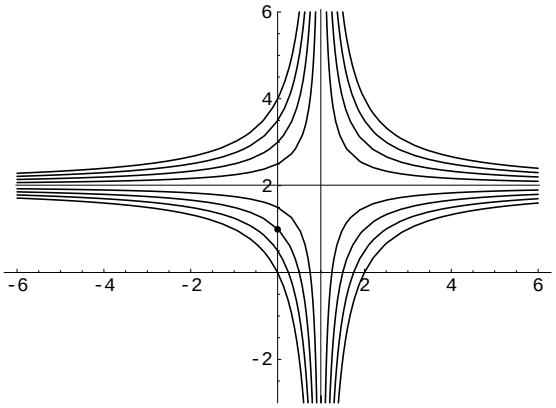
mentre

$$f\big(f^{-1}(2\boldsymbol{N})\big) = f\big([0,1)\cup[2,3)\cup[4,5)\cup\ \ldots\big) = \{0,\,2,\,4,\,6,\,8,\,\ldots\} = 2\boldsymbol{N}.$$

* * *

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 $\boldsymbol{R}^2$.

Soluzione. Nel piano $\boldsymbol{R}^2$ si consideri la famiglia delle iperboli aventi per asintoti le rette $x=1$ e $y=2$.



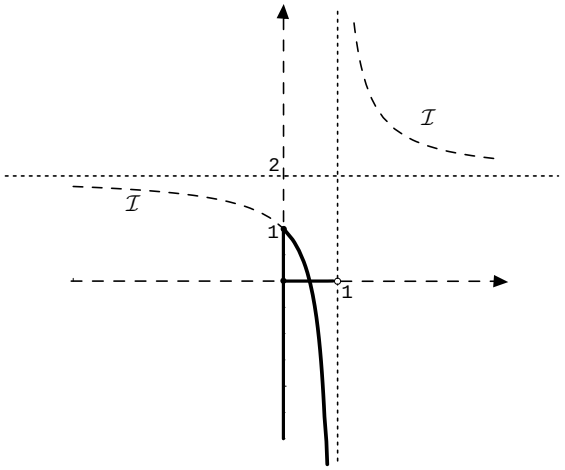
Tali iperboli hanno equazione del tipo $(x-1)(y-2) = c,\ \forall\, c\in\mathbf{R}$. Imponendo a tali iperboli il passaggio per il punto $(0,1)$, si ottiene $(0-1)(1-2) = c$, da cui $c=1$.

Si è quindi ottenuta l'iperbole $\mathcal{I}$ di equazione $(x-1)(y-2)=1$. Tale iperbole definisce la funzione

$$f(x) = y = \tfrac{1}{x-1} + 2,\ \forall\, x\neq 1.$$

La restrizione $f_{|_{[0,1)}}$ ha per immagine l'intervallo $(-\infty,1]$ ed è decrescente e quindi biiettiva. Quindi

$f_{|_{[0,1),su}}$: $[0,1) \to (-\infty, 1]$ è una biiezione cercata.



* * *

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 $g := f_{\big|X} : X \to X$ è una biiezione.

(*iii*) Verificare che $g^3 = \mathbf{1}_X$. Dedurne l'inversa di g.

Soluzione. (*i*) Si ha, $\forall\, x, y \in \boldsymbol{R}^{\cdot}$:

$$f(x) = f(y) \implies 1 - \tfrac{1}{x} = 1 - \tfrac{1}{y} \implies \tfrac{1}{x} = \tfrac{1}{y} \implies x = y.$$

Ne segue che f è iniettiva.

Sia $b \in \boldsymbol{R}$. Se $b = 1 - \frac{1}{x}$ (con $x \neq 0$), allora: $bx = x - 1 \implies (1-b)x = 1 \implies x = \frac{1}{1-b}$ (se $b \neq 1$). Ne segue che $\forall\, b \in \boldsymbol{R} - \{1\}$, $b = f(\frac{1}{1-b})$ e dunque $Im(f) \supseteq \boldsymbol{R} - \{1\}$. Infine $1 \notin Im(f)$ [altrimenti $1 - \frac{1}{x} = 1 \implies -\frac{1}{x} = 0 \implies 0 = 1$: assurdo]. Si conclude che $Im(f) = \boldsymbol{R} - \{1\}$.

(*ii*) g è ovviamente iniettiva. Inoltre $Im(g) \subseteq Im(f) = \boldsymbol{R} - \{1\}$. Risulta: $0 \notin Im(g)$ [altrimenti $1 - \frac{1}{x} = 1 \implies \frac{1}{x} = 1 \implies x = 1$, mentre $1 \notin X$]. Dunque $Im(g) \subseteq X$.

Viceversa, $\forall\, b \in X$, $\frac{1}{1-b} \in X$ e $g(\frac{1}{1-b}) = b$. Dunque $Im(g) = X$.

(*iii*) Risulta, $\forall\, x \in X$:

$$g^3(x) = g^2(g(x)) = g^2(\tfrac{x-1}{x}) = g(1 - \tfrac{x}{x-1}) = g(\tfrac{1}{1-x}) = 1 - \tfrac{1}{\frac{1}{1-x}} = x = \mathbf{1}_X(x).$$

Da $g^3 = \mathbf{1}_X$ segue che $g^2 \circ g = \mathbf{1}_X = g \circ g^2$. Dunque $g^{-1} = g^2$. Risulta quindi:

$$g^{-1}(x) = \tfrac{1}{1-x},\ \forall\, x \in X.$$

* * *

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.

Soluzione. (*i*) L'applicazione f è iniettiva ma non suriettiva; infatti, se $f(x) = f(y)$, allora $2x + 3 = 2y + 3$, da cui, con ovvi calcoli, $x = y$. Quindi f è iniettiva. Inoltre $Im(f)$ è l'insieme degli interi dispari e quindi f non è suriettiva.

Analogamente verifichiamo che g è suriettiva ma non iniettiva. Infatti, ad esempio, $g(2) = 2 = g(-1)$ e dunque g non è iniettiva. Per verificare la suriettività basta osservare che, $\forall\, x \in \boldsymbol{Z}$, risulta $x = g(2x - 5)$ [ovvero anche $x = g(2x - 2)$].

(*ii*) Consideriamo ora il prodotto operatorio $g \circ f$. Per ogni $x \in \boldsymbol{Z}$ risulta:

$$(g \circ f)(x) = g(f(x)) = g(2x+3) = \tfrac{(2x+3)+3}{2} + 1 = x + 4.$$

Tale aplicazione è ovviamente biunivoca.

Per quanto riguarda infine il prodotto operatorio $f \circ g$, osserviamo che, essendo g non iniettiva e f non suriettiva, tale prodotto non è né iniettivo né suriettivo. Risulta:

$$(f \circ g)(x) = f(g(x)) = \begin{cases} f(\frac{x}{2}+1), \text{ se } x \text{ è pari} \\ f(\frac{x+3}{2}+1), \text{ se } x \text{ è dispari} \end{cases} = \begin{cases} x+5, \text{ se } x \text{ è pari} \\ x+8, \text{ se } x \text{ è dispari.} \end{cases}$$

* * *

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 $f^{-1} = g_3^{-1} \circ g_2^{-1} \circ g_1^{-1}$.

Soluzione. (*i*) Posto $y = 2 - \frac{x-1}{2}$, risulta $x = 5 - 2y$. Si verifica subito che la funzione

$$g : \boldsymbol{Q} \to \boldsymbol{Q} \text{ tale che } g(y) = 5 - 2y$$

è inversa di f. Dunque f è biiettiva e $f^{-1} = g$.

(*ii*) Si ponga ad esempio:

$g_3 : \boldsymbol{Q} \to \boldsymbol{Q}$ tale che $x \to x - 1$, $\forall\, x \in \boldsymbol{Q}$, $\quad g_2 : \boldsymbol{Q} \to \boldsymbol{Q}$ tale che $x \to \frac{x}{2}$, $\forall\, x \in \boldsymbol{Q}$,

$g_1 : \boldsymbol{Q} \to \boldsymbol{Q}$ tale che $x \to 2 - x$, $\forall\, x \in \boldsymbol{Q}$.

Le tre applicazioni sono biiettive, con inverse rispettivamente:

$$g_3^{-1} : y \to y + 1; \quad g_2^{-1} : y \to 2y; \quad g_1^{-1} : y \to 2 - y \quad (\forall\, y \in \mathbf{Q}).$$

Risulta:

$(g_1 \circ g_2 \circ g_3)(x) = g_1(g_2(x-1)) = g_1(\frac{x-1}{2}) = 2 - \frac{x-1}{2} = f(x)$;

$(g_3^{-1} \circ g_2^{-1} \circ g_1^{-1})(y) = g_3^{-1}(g_2^{-1}(2-y)) = g_3^{-1}(4-2y) = 5 - 2y = f^{-1}(y)$.

* * *

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.

Soluzione. (*i*) Si ha: $f(t) = \frac{1}{2} \sin 2t$. La funzione $y = \sin 2x$ cresce (con continuità) da 0 ad 1 nell'intervallo $[0, \frac{\pi}{4}]$ e decresce (con continuità) da 1 a 0 nell'intervallo $[\frac{\pi}{4}, \frac{\pi}{2}]$. Ne segue che f è crescente da 0 ad $\frac{1}{2}$ nell'intervallo $[0, \frac{\pi}{4}]$ e decresce da $\frac{1}{2}$ a 0 nell'intervallo $[\frac{\pi}{4}, \frac{\pi}{2}]$. In particolare, $Im(f) = (0, \frac{1}{2}]$.

(*ii*) Risulta: $f(\frac{\pi}{2} - t) = \sin(\frac{\pi}{2} - t) \cos(\frac{\pi}{2} - t) = \cos t \sin t = f(t)$, $\forall\, t \in (0, \frac{\pi}{2})$. Dunque f non è iniettiva.

(*iii*) Risulta, $\forall\, t, s \in (0, \frac{\pi}{2})$:

$$t \rho_f s \iff f(t) = f(s) \iff \sin 2t = \sin 2s \iff 2s = \pi - 2t \iff s = \tfrac{\pi}{2} - t.$$

Pertanto $[t]_{\rho_f} = \{t, \frac{\pi}{2} - t\}$, $\forall\, t \in (0, \frac{\pi}{2})$.
Si noti che ogni classe di equivalenza $[t]_{\rho_f}$ è formata da due numeri (distinti, se $t \neq \frac{\pi}{4}$): di essi uno soltanto è contenuto nell'intervallo $(0, \frac{\pi}{4}]$. Risulta quindi:

$$A = (0, \tfrac{\pi}{2}) \big/ \rho_f = \left\{ [t]_{\rho_f}, \ \forall\, t \in (0, \tfrac{\pi}{4}] \right\}.$$

Posto $I = (0, \frac{\pi}{4}]$, l'applicazione $\varphi : I \to A$ tale che $\varphi(t) = [t]_{\rho_f}$ è suriettiva [per definizione di A] ed iniettiva [se infatti $[t]_{\rho_f} = [s]_{\rho_f}$ e $t, s \in I$, allora $t = s$]. Si conclude che φ è una biiezione cercata.

* * *

1.14. Sia ρ la seguente relazione su $\boldsymbol{R}$:

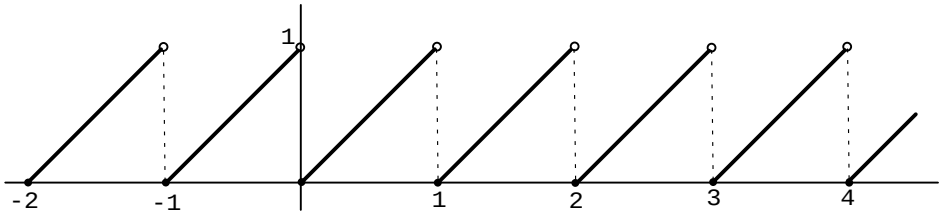
$$x \rho y \iff x - y \in \boldsymbol{Z}.$$

(*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 $[0, 1)$.

Soluzione. (*i*) Risulta:
$x \rho x$, $\forall\, x \in \boldsymbol{R}$ [infatti $x - x = 0 \in \boldsymbol{Z}$];
$x \rho y \implies y \rho x$ [infatti $x - y \in \boldsymbol{Z} \implies y - x \in \boldsymbol{Z}$];
$x \rho y$ e $y \rho z \implies x \rho z$ [infatti $x - y \in \boldsymbol{Z}$, $y - z \in \boldsymbol{Z} \implies x - z = x - y + y - z \in \boldsymbol{Z}$].
Si ha: $[x]_\rho = \{y \in \boldsymbol{R} \,|\, y - x \in \boldsymbol{Z}\} = \{y \in \boldsymbol{R} \,|\, y \in x + \boldsymbol{Z}\} = x + \boldsymbol{Z}$.
(*ii*) Sia $g : \boldsymbol{R} \to \boldsymbol{R}$ l'applicazione *parte decimale*, così definita:

$$g(x) = x - [x], \ \forall\, x \in \boldsymbol{R},$$

con $[x]$ *parte intera* di x [= massimo intero $\leq x$]. Si verifica che g ha il seguente grafico:



Ovviamente $Im(g) = [0, 1)$ e si ha: $x \rho_g y \iff x - [x] = y - [y]$.
Verifichiamo che $\rho_g = \rho$:
$x \rho_g y \implies x - y = [x] - [y] \implies x - y \in \boldsymbol{Z} \implies x \rho y$. Dunque $\rho_g \subseteq \rho$.
$x \rho y \implies y = x + n$, $\exists\, n \in \boldsymbol{Z} \implies [y] = [x+n] = [x] + n \implies y - [y] = x + n - (n + [x]) = x - [x] \implies$
$\implies x \rho_g y$. Dunque $\rho \subseteq \rho_g$.
Poiché $\rho = \rho_g$, l'applicazione

$$\boldsymbol{R}/_\rho \to [0, 1) \text{ tale che } [x]_\rho \to g(x) = x - [x], \ \forall\, [x] \in \boldsymbol{R}/_\rho,$$

è una biiezione, come richiesto.

* * *

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 $A/_\rho \times B/_\sigma$.

Soluzione. (*i*) Risulta:
$(a, b)\, \mathfrak{R}\, (a, b)$ [infatti $a \rho a$ e $b \sigma b$];
$(a, b)\, \mathfrak{R}\, (a_1, b_1) \implies (a_1, b_1)\, \mathfrak{R}\, (a, b)$ [infatti $a \rho a_1 \implies a_1 \rho a$ e $b \sigma b_1 \implies b_1 \sigma b$];
$(a, b)\, \mathfrak{R}\, (a_1, b_1)$, $(a_1, b_1)\, \mathfrak{R}\, (a_2, b_2) \implies (a, b)\, \mathfrak{R}\, (a_2, b_2)$ [infatti $a \rho a_1$, $a_1 \rho a_2 \implies a \rho a_2$ e $b \sigma b_1$, $b_1 \sigma b_2 \implies b \sigma b_2$].

(*ii*) Sia $f : A \times B \to A/_\rho \times B/_\sigma$ l'applicazione così definita:

$$f((a, b)) = \big([a]_\rho, [b]_\sigma\big), \ \forall\, (a, b) \in A \times B$$

[f è il prodotto delle due proiezioni canoniche].
f è ovviamente suriettiva. Infatti, $\forall\, \big([a]_\rho, [b]_\sigma\big) \in A/_\rho \times B/_\sigma$, risulta che $f((a, b)) = \big([a]_\rho, [b]_\sigma\big)$.
Verifichiamo ora che la relazione ρ_f associata ad f coincide con $\mathfrak{R}$. Si ha:

$$(a, b) \rho_f (a_1, b_1) \iff f((a, b)) = f((a_1, b_1)) \iff \big([a]_\rho, [b]_\sigma\big) = \big([a_1]_\rho, [b_1]_\sigma\big) \iff$$

$[a]_\rho = [a_1]_\rho$ e $[b]_\sigma = [b_1]_\sigma \iff a\rho a_1$ e $b\sigma b_1 \iff (a,b)\,\mathfrak{R}\,(a_1,b_1)$.

In base al teorema fondamentale delle applicazioni, l'applicazione

$$F : A\times B/_{\mathfrak{R}} \to A/_\rho \times B/_\sigma \text{ tale che } F([(a,b)]_{\mathfrak{R}}) = f((a,b)) = \big([a]_\rho, [b]_\sigma\big),$$

è una biiezione, come richiesto.

* * *

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 $\boldsymbol{R}^{2\,*}/_\rho$?

Soluzione. (*i*) Risulta: $(a,b)\rho(c,d) \iff ad - bc = 0$. È evidente che ρ è riflessiva e simmetrica. Verifichiamo che ρ è transitiva: $\begin{cases}(a,b)\rho(c,d)\\(c,d)\rho(e,f)\end{cases} \implies (a,b)\rho(e,f)$.

Per ipotesi, $\begin{cases} ad = bc\\ cf = de.\end{cases}$ Si hanno due possiblità: $d \neq 0$ oppure $d = 0$.

Se $d \neq 0$, $\begin{cases} adf = bcf\\ bcf = bde,\end{cases}$ da cui $adf = bde$. Quindi $d(af - be) = 0$, da cui $af - be = 0$ $(d \neq 0)$. Dunque $(a,b)\rho(e,f)$.

Se $d = 0$, $\begin{cases} ade = bce\\ acf = ade,\end{cases}$ da cui $bce = acf$. Quindi $c(af - be) = 0$, da cui $be - af = 0$ $(c \neq 0$, essendo $d = 0)$. Dunque ancora $(a,b)\rho(e,f)$.

Se estendessimo ρ a tutto $\boldsymbol{R}^2$, ρ non sarebbe più una relazione di equivalenza: risulta infatti $(0,0)\rho(x,y)$, $\forall\,(x,y \in \boldsymbol{R}^2$, e dunque, ad esempio, $(1,0)\rho(0,0)$, $(0,0)\rho(0,1)$, ma $(1,0)\not\rho(0,1)$.

(*ii*) La retta $\mathbf{r}$ ha equazioni parametriche $\begin{cases} x = at\\ y = bt,\end{cases}$ $\forall\, t \in \boldsymbol{R}$. Per ogni $(at,bt) \in \mathbf{r} - \{(0,0)\}$, si ha $(at,bt)\rho(a,b)$. Dunque $\mathbf{r} - \{(0,0)\} \subseteq [(a,b)]_\rho$.

Viceversa, sia $(c,d) \in [(a,b)]_\rho$ $(ad = bc)$. Se $b \neq 0$, allora $(c,d) = \big(a\frac{b}{d}, b\frac{b}{d}\big) \in \mathbf{r} - \{(0,0)\}$. Se $b = 0$, allora $a \neq 0$. Ne segue $d = 0$ e quindi $(c,d) = (c,0) = \big(a\frac{c}{a}, 0\frac{c}{a}\big) = \big(a\frac{c}{a}, b\frac{c}{a}\big) \in \mathbf{r} - \{(0,0)\}$.

(*iii*) L'insieme quoziente $\boldsymbol{R}^{2\,*}/_\rho$ è formato dalle rette passanti per l'origine $(0,0)$ (e private dell'origine). Dunque $\boldsymbol{R}^{2\,*}/_\rho$ corrisponde biunivocamente al fascio proprio di rette di $\boldsymbol{R}^2$ per l'origine.

* * *

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.

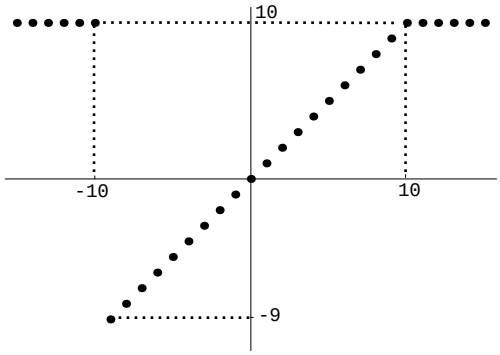
(*ii*) Determinare $f^{-1}(10)$.

(*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 $\{1, 2, \ldots, 20\}$.

Soluzione. (*i*) Si ha: $10 = f(10) = f(11)$. Ciò basta ad affermare che f non è iniettiva.
Risulta: $Im(f) = \boldsymbol{Z} \cap [-9, 10] = \{-9, -8, \ldots, 9, 10\}$. Dunque f non è suriettiva.

Si osservi che il grafico di f è il seguente:



(*ii*) Si ha: $f^{-1}(10) = \boldsymbol{Z} \cap \big((-\infty, -10] \cup [10, +\infty)\big) = \{..., -11, -10, 10, 11, ...\}$.

(*iii*) Si ha: $x \rho_f y \iff f(x) = f(y) \iff x = y$ oppure $|x|, |y| \geq 10$. Le classi di equivalenza modulo ρ_f sono quindi le seguenti:

$$[-9] = \{-9\},\ ...,\ [9] = \{9\},\ [10] = \{..., -11, -10, 10, 11, ...\}.$$

(*iv*) Si consideri l'applicazione suriettivizzata $f_{su} : \boldsymbol{Z} \to Im(f) = \boldsymbol{Z} \cap [-9, 10]$. Poiché f opera come f_{su}, allora $\rho_{f_{su}} = \rho_f$. Essendo f_{su} suriettiva, è 'canonicamente' definita la biiezione

$$\varphi : \boldsymbol{Z}/_{\rho_f} = \boldsymbol{Z}/_{\rho_{f_{su}}} \to Im(f),\ \text{ tale che }\ [x] \to f(x),\ \forall\, [x] \in \boldsymbol{Z}/_{\rho_f}.$$

Si consideri ora la 'traslazione' $g : Im(f) \to \{1, 2, ..., 20\}$ tale che

$$y \to y + 10,\ \forall\, y \in Im(f) = \{-9, -8, ..., 9, 10\}.$$

g è certamente una biiezione. Ne segue che

$$g \circ \varphi : \boldsymbol{Z}/_{\rho_f} \to \{1, 2, ..., 20\},\ \text{ tale che }\ [x] \to f(x) + 10,\ \forall\, [x] \in \boldsymbol{Z}/_{\rho_f}\ ,$$

è una biiezione, come richiesto.

* * *

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 $\Gamma = \{(t, |t|),\ \forall\, t \in \boldsymbol{R}\}$.

Soluzione. (*i*) Se $r \geq 0$, si ha: $f(r, r) = \sqrt{r^2} = r$. Se $r < 0$, si ha: $f(-r, r) = -\sqrt{-r^2} - -|r| = r$. Dunque f è suriettiva.

Per verificare che f non è iniettiva, basta osservare che tutti i punti (x, y) tali che $xy = 0$ hanno la stessa immagine 0 tramite f.

(*ii*) Sia $r \geq 0$. Si ha:

$$f^{-1}(r) = \{(x, y) \in \boldsymbol{R}^2 : xy \geq 0 \ \text{ e } \ \sqrt{xy} = r\} = \{(x, y) \in \boldsymbol{R}^2 : xy = r^2\}.$$

Se $r < 0$,

$$f^{-1}(r) = \{(x, y) \in \boldsymbol{R}^2 : xy < 0 \ \text{ e } \ -\sqrt{-xy} = r\} = \{(x, y) \in \boldsymbol{R}^2 : xy = -r^2\}.$$

Dunque

$$f^{-1}(r) = \begin{cases} asse\ x \cup\ asse\ y, & \text{se } r = 0, \\ \text{iperbole di equazione } xy = r^2, & \text{se } r > 0, \\ \text{iperbole di equazione } xy = -r^2, & \text{se } r < 0. \end{cases}$$

(*iii*) Si verifica facilmente che ρ è una relazione di equivalenza su $\boldsymbol{R}^2$. Tenuto conto della definizione di ρ_f, va provato che $(x,y)\rho(x_1,y_1) \iff f(x,y) = f(x_1,y_1)$.

($\Longrightarrow$). Se $xy = x_1y_1 \geq 0$, $f(x,y) = \sqrt{xy} = \sqrt{x_1y_1} = f(x_1,y_1)$. Se invece $xy = x_1y_1 < 0$, $f(x,y) = -\sqrt{-xy} = -\sqrt{-x_1y_1} = f(x_1,y_1)$.

($\Longleftarrow$). Sia $f(x,y) = f(x_1,y_1)$. Se $xy \geq 0$, allora $f(x_1,y_1) = f(x,y) = \sqrt{xy} \geq 0$ e quindi $f(x_1,y_1) = \sqrt{x_1y_1}$. Allora $\sqrt{xy} = \sqrt{x_1y_1}$ e quindi $xy = x_1y_1$. Se invece $xy < 0$, allora $f(x_1,y_1) = f(x,y) = -\sqrt{-xy} < 0$ e quindi $f(x_1,y_1) = -\sqrt{x_1y_1}$. Allora $-\sqrt{-xy} = -\sqrt{-x_1y_1}$ e quindi $-xy = -x_1y_1$, cioè $xy = x_1y_1$.

(*iv*) L'insieme quoziente $\boldsymbol{R}^2/_{\rho_f}$ ha per elementi (classi di equivalenza) le iperboli $xy = c$, $\forall\, c \in \mathbf{R}$. L'insieme Γ è unione delle due semirette

$$Y_1 = \{(x,x),\ \forall\, x \geq 0\}, \quad Y_2 = \{(x,-x),\ \forall\, x \leq 0\},$$

[rispettivamente bisettrice del I e del II quadrante].

All'iperbole $xy = c$, con $c \geq 0$ si può associare il punto $(\sqrt{c},\sqrt{c}) \in Y_1$; all'iperbole $xy = c$, con $c < 0$ si può associare il punto $(-\sqrt{-c},\sqrt{-c}) \in Y_2$.

L'applicazione $\varphi : \boldsymbol{R}^2/_{\rho_f} \to \Gamma$ così costruita è biiettiva. Formalmente φ ha la seguente definizione:

$$\varphi([x,y]_{\rho_f}) = \begin{cases} \left(\sqrt{xy},\sqrt{xy}\right), & \text{se } \ xy \geq 0 \\ \left(-\sqrt{-xy},\sqrt{-xy}\right), & \text{se } \ xy < 0, \end{cases} \qquad \forall\, [x,y]_{\rho_f} \in \boldsymbol{R}^2/_{\rho_f}.$$

* * *

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, $\forall\, (a,b,c)\,, (a_1,b_1,c_1) \in A$:

$$(a,b,c)\,\rho_1\,(a_1,b_1,c_1) \iff abc_1 = a_1b_1c; \ \ (a,b,c)\,\rho_2\,(a_1,b_1,c_1) \iff (a+b)c_1 = (a_1+b_1)c.$$

(*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 $F : A/_{\rho_1} \to A/_{\rho_2}$.

Soluzione. (*i*) La riflessività e la simmetria di ρ_1 e ρ_2 sono assolutamente ovvie. Verifichiamo la transitività di ρ_1.

$$\text{Se } \begin{cases} (a,b,c)\,\rho_1\,(a_1,b_1,c_1) \\ (a_1,b_1,c_1)\,\rho_1\,(a_2,b_2,c_2) \end{cases} \text{ allora } \begin{cases} abc_1 = a_1b_1c \\ a_1b_1c_2 = a_2b_2c_1, \end{cases} \text{ da cui } \begin{cases} abc_1c_2 = a_1b_1cc_2 \\ a_1b_1c_2c = a_2b_2c_1c. \end{cases}$$

Ne segue che $abc_1c_2 = a_2b_2c_1c$. Semplificando c_1 $(\neq 0)$ segue che

$$abc_2 = a_2b_2c, \text{ cioè che } (a,b,c)\,\rho_1\,(a_2,b_2,c_2).$$

Per la transitività di ρ_2 si procede in modo analogo.

(*ii*) Si ponga $f_1 : A \to \boldsymbol{Q}$ tale che $(a,b,c) \to \frac{ab}{c}$, $\forall\, (a,b,c) \in A$.

f_1 è suriettiva [infatti $\frac{a}{b} = f_1(a,1,b)$, $\forall\, \frac{a}{b} \in \boldsymbol{Q}$]; inoltre $\rho_{f_1} = \rho_1$ [infatti $(a,b,c)\,\rho_{f_1}\,(a_1,b_1,c_1) \iff \frac{ab}{c} = \frac{a_1b_1}{c_1} \iff abc_1 = a_1b_1c \iff (a,b,c)\,\rho_1\,(a_1,b_1,c_1)$]. Dunque f_1 induce una biiezione $F_1 : A/_{\rho_1} \to \boldsymbol{Q}$ tale che

$$F_1([a,b,c]_1) = \tfrac{ab}{c},\ \forall\, [a,b,c]_1 \in A/_{\rho_1}.$$

Analogamente, si definisce $f_2 : A \to \boldsymbol{Q}$ tale che $(a,b,c) \to \frac{a+b}{c}$, $\forall\, (a,b,c) \in A$. Anche f_2 è suriettiva e $\rho_{f_2} = \rho_2$. Allora f_2 induce la biiezione $F_2 : A/_{\rho_2} \to \mathbf{Q}$ tale che

$$F_2([a,b,c]_2) = \tfrac{a+b}{c},\ \forall\, [a,b,c]_2 \in A/_{\rho_2}.$$

(*iii*) Una biiezione richiesta è $F := F_2^{-1} \circ F_1$. Risulta:

$$F_2^{-1} \circ F_1 :\ [a,b,c]_1 \to \tfrac{ab}{c} \to [ab,0,c]_2.$$

Dunque $F([a,b,c]_1) = [ab,0,c]_2$.

* * *

1.20. Nell'insieme $\boldsymbol{Z}^{\cdot} = \boldsymbol{Z} - \{0\}$ si consideri la partizione $\mathfrak{F}$ formata dai seguenti quattro insiemi:

$\mathbf{P}_+ = \{2, 4, 6, 8, \dots\}$ [pari positivi], $\mathbf{P}_- = \{-2, -4, -6, -8, \dots\}$ [pari negativi],

$\mathbf{D}_+ = \{1, 3, 5, 7, \dots\}$ [dispari positivi], $\mathbf{D}_- = \{-1, -3, -5, -7, \dots\}$ [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 $\rho_f = \rho$.

Soluzione. Si ha, $\forall\, a, b \in \boldsymbol{Z}$:

$$a \rho b \iff a, b \in \mathbf{P}_+ \text{ oppure } a, b \in \mathbf{P}_- \text{ oppure oppure } a, b \in \mathbf{D}_+ \text{ oppure } a, b \in \mathbf{D}_-$$
$$\iff ab > 0 \text{ e } a, b \text{ sono entrambi pari o entrambi dispari.}$$

Definiamo $f : \boldsymbol{Z}^{\cdot} \to \{-2, -1, 1, 2\}$ tale che

$$f(t) = \begin{cases} (-1)^t, & \text{se } t \in \boldsymbol{Z}^+ \\ 2(-1)^{|t|}, & \text{se } t \in \boldsymbol{Z}^-. \end{cases}$$

Si osserva subito che :

$$f(\mathbf{P}_+) = \{1\},\ f(\mathbf{D}_+) = \{-1\},\ f(\mathbf{P}_-) = \{2\},\ f(\mathbf{D}_-) = \{-2\}.$$

Ne segue che f è suriettiva e che $\rho_f = \rho$. Infatti dalla precedente osservazione segue che

$$a \rho_f b \iff f(a) = f(b) \iff a, b \in \mathbf{P}_+ \text{ oppure } a, b \in \mathbf{P}_- \text{ oppure } \dots .$$

* * *

1.21. Come è noto, la relazione di divisibilità in $\boldsymbol{Z}$ è così definita:

$$\forall\, a, b \in \boldsymbol{Z},\ a \,|\, b \iff b = ah,\ \exists\, h \in \boldsymbol{Z}.$$

Indicheremo sempre con $|$ sia la relazione di divisibilità ristretta a $\boldsymbol{N}$ [cioè $a \,|\, b \iff b = ah,\ \exists\, h \in \boldsymbol{N}$], che quella ristretta a $\boldsymbol{N}^{\cdot} = \boldsymbol{N} - \{0\}$ [cioè $a \,|\, b \iff b = ah,\ \exists\, h \in \boldsymbol{N}^{\cdot}$].

(*i*) Verificare che $(\boldsymbol{Z}, |)$, è un insieme *pre-ordinato*, [cioè che la relazione $|$ è riflessiva e transitiva], ma non simmetrica né antisimmetrica.

(*ii*) Verificare che $(\boldsymbol{N}, |)$ è un insieme ordinato, non totalmente, e che ammette un primo ed un ultimo elemento.

(*iii*) Verificare che $(\boldsymbol{N}^{\cdot}, |)$ è un insieme ordinato (non totalmente) e calcolare eventuali massimo, minimo, estremo inferiore ed estremo superiore dei due suoi seguenti sottoinsiemi:

$$2^{\boldsymbol{N}} = \{2^h,\ \forall\, h \in \boldsymbol{N}\}, \quad \boldsymbol{T} = \{2, 3, 6\}.$$

Soluzione. (*i*) Per ogni $a, b, c \in \boldsymbol{Z}$: $a|a$ [infatti $a = a \cdot 1$]; se $a|b$ e $b|c$, allora $a|c$ [infatti, se $b = ah$, $c = bk$, allora $c = ahk$ e quindi $a|c$]. Dunque $|$ è riflessiva e transitiva. Invece $|$ non è simmetrica [ad esempio $2|4$ mentre $4 \not| 2$] e non è antisimmetrica [ad esempio $2|-2$, $-2|2$ ma $2 \neq -2$].

(*ii*) In $(\boldsymbol{N}, |)$ la relazione $|$ è (come in $\boldsymbol{Z}$) riflessiva e transitiva. Verifichiamo che è anche antisimmetrica. Sia infatti $a \,|\, b$ e $b \,|\, a$. Allora: se $b = 0$, anche $a = 0$; se $b \neq 0$ si ha: $b = ah$, $a = bk \Longrightarrow b = bkh \Longrightarrow b(1 - kh) = 0 \Longrightarrow 1 - kh = 0 \Longrightarrow kh = 1 \Longrightarrow k = h = 1 \Longrightarrow a = b$. Inoltre $(\boldsymbol{N}, |)$ non è totalmente ordianto [ad esempio $2 \not| 3$ e $3 \not| 2$].

Si ponga $a \leq b \iff a \,|\, b$. Risulta:

$1 \,|\, a,\ \forall\, a \in \boldsymbol{N}$ [infatti $a = a \cdot 1$] e dunque $1 \leq a,\ \forall\, a \in \boldsymbol{N}$.

$a|0,\ \forall\, a \in \boldsymbol{N}$ [infatti $0 = a \cdot 0$] e dunque $a \leq 0,\ \forall\, a \in \boldsymbol{N}$. Pertanto $1, 0$ sono rispettivamente il primo elemento (o minimo) e l'ultimo elemento (o massimo) di $(\boldsymbol{N}, |)$.

(*iii*) In $(\boldsymbol{N}^{\cdot}, |)$ la relazione $|$ è (come in $\boldsymbol{N}$) una relazione d'ordine non totale. Si ricorda che

$$inf(2^{\boldsymbol{N}}) = max(Minor(2^{\boldsymbol{N}})), \quad sup(2^{\boldsymbol{N}}) = min(Maggior(2^{\boldsymbol{N}})).$$

Si ha:

$$Minor(2^{\boldsymbol{N}}) = \{a \in \boldsymbol{N}^{\cdot} :\ a|2^h,\ \forall\, h \in \boldsymbol{N}\} = \{1\}, \quad Maggior(2^{\boldsymbol{N}}) = \{a \in \boldsymbol{N}^{\cdot} :\ 2^h|a,\ \forall\, h \in \boldsymbol{N}\} = \emptyset.$$

Ne segue: $2^{\boldsymbol{N}}$ non è limitato superiormente e quindi non esiste $sup(2^{\boldsymbol{N}})$ [e tantomeno $max(2^{\boldsymbol{N}})$]; invece $inf(2^{\boldsymbol{N}}) = 1$ e poiché $1 \in 2^{\boldsymbol{N}}$, anche $min(2^{\boldsymbol{N}}) = 1$.

Risulta infine che $6 = max(\boldsymbol{T})$ (perché $2 \,|\, 6,\ 3 \,|\, 6,\ 6 \,|\, 6$), mentre $\nexists\, min(\boldsymbol{T})$ (perché $2 \not| 3$ e $3 \not| 6$), ma $inf(\boldsymbol{T}) = 1$ (perché $Minor(T) = \{1\}$).

* * *

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.

Soluzione. (*i*) Siano $a, b \in A,\ a \neq b$. Per ipotesi $min(\{a, b\})$ esiste, ed è a oppure b. Allora $a \leq b$ oppure $b \leq a$. Ne segue che $(A, \leq)$ è totalmente ordinato.

(*ii*) Sia $A = \{a_1, a_2, \dots, a_n\}$. Essendo $(A, \leq)$ totalmente ordinato, si può assumere che risulti: $a_1 < a_2 < \dots < a_n$. Per ogni $S \subseteq A,\ S \neq \emptyset$, $min(S)$ esiste [è l'elemento di indice minimo in S]. Ne segue che $(A, \leq)$ è bene ordinato.

(*iii*) Si consideri ad esempio l'insieme ordinato $(\boldsymbol{Z}, \leq)$ [oppure $(\boldsymbol{Q}, \leq)$ o $(\boldsymbol{R}, \leq)$] È noto che $(\boldsymbol{Z}, \leq)$ è totalmente ordinato. Ma $(\boldsymbol{Z}, \leq)$ non è bene ordinato: ad esempio il sottoinsieme $S = \{-n,\ \forall\, n \geq 0\}$ è privo di minimo.

* * *

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 $sup(\{S\}) = S,\ \forall\, S \in \boldsymbol{\mathcal{P}}(A)$?

Soluzione. (*i*) $\boldsymbol{\mathcal{P}}(A)$ è un insieme di cardinalità $2^3 = 8$. È formato dai seguenti elementi:

$$\emptyset,\ \{a\},\ \{b\},\ \{c\},\ \{a, b\},\ \{a, c\},\ \{b, c\},\ \{a, b, c\} = A.$$

Si ha, $\forall\, S, T, R \in \boldsymbol{\mathcal{P}}(A)$:

$$S \subseteq S;\quad S \subseteq T,\ T \subseteq S \Longrightarrow S = T;\quad S \subseteq T,\ T \subseteq R \Longrightarrow S \subseteq R.$$

Ne segue che $(\boldsymbol{\mathcal{P}}(A), \subseteq)$ è un insieme ordinato. Poiché ad esempio $\{a\} \not\subseteq \{b\}$ e $\{b\} \not\subseteq \{a\}$, allora $(\boldsymbol{\mathcal{P}}(A), \subseteq)$ non è totalmente ordinato [e quindi neppure bene ordinato]. Il suo primo elemento (o minimo) è $\emptyset$; il suo ultimo elemento (o massimo) è A.

(*ii*) Risulta: $Minor(\{a\}) = \big\{\emptyset, \{a\}\big\}$, $\quad Maggior(\{a\}) = \big\{\{a\}, \{a, b\}, \{a, c\}, A\big\}$.

(*iii*) Per ogni $S \in \boldsymbol{\mathcal{P}}(A)$, $Maggior(\{S\}) \ni S$. Se poi $T \in Maggior(\{S\})$, allora $T \supseteq S$. Dunque $S = min\big(Maggior(\{S\})\big) = sup(\{S\})$. L'affermazione è quindi vera; è anzi vero che $S = max(\{S\})$. Inoltre il risultato vale in ogni insieme ordinato $(A, \leq)$: $sup(\{a\}) = max(\{a\}) = a,\ \forall\, a \in A$.

* * *

1.24. Verificare che in un anello unitario $(A, +, \cdot)$ l'unità 1_A è unica.

Soluzione. Siano 1_A e $1'_A$ due unità di A. Si ha:

$$\begin{cases} 1_A \cdot 1'_A = 1_A & \text{(pensando } 1'_A \text{ come unità);} \\ 1_A \cdot 1'_A = 1'_A & \text{(pensando } 1_A \text{ come unità).} \end{cases}$$

Allora $1_A = 1'_A$.

* * *

1.25. Sia A' un sottoinsieme non vuoto di un anello $(A, +, \cdot)$. Verificare che

$$A' \text{ è un sottoanello di } A \iff A' - A' \subseteq A' \text{ e } A' \cdot A' \subseteq A'.$$

Soluzione. Le due condizioni $A' - A' \subseteq A'$ e $A' \cdot A' \subseteq A'$ vanno rispettivamente interpretate nella forma:

$$a - b \in A',\ \forall\, a, b \in A' \quad \text{e} \quad ab \in A',\ \forall\, a, b \in A'.$$

($\Longrightarrow$). Essendo A' un sottoanello di A, allora A' è un anello rispetto alle operazioni $+, \cdot$ (ristrette ad $A' \times A'$).

Siano quindi $a, b \in A'$. Allora $-b \in A'$ e $a + (-b) = a - b \in A'$; inoltre $ab \in A'$. Dunque si ha: $A' - A' \subseteq A'$ e $A' \cdot A' \subseteq A'$.

($\Longleftarrow$). Sia A' un sottoinsieme non vuoto di A tale che $A' - A' \subseteq A'$ e $A' \cdot A' \subseteq A'$. Si ha:

$0 \in A'$ [infatti $0 = a - a \in A'$ (con $a \in A'$)];
$\forall\, a \in A',\ -a \in A'$ [infatti $-a = 0 - a \in A'$];
$\forall\, a, b \in A',\ a + b = a - (-b) \in A'$;
$\forall\, a, b, c \in A',\ (a + b) + c = a + (b + c)$ [infatti è vero in A];
$\forall\, a, b \in A',\ a + b = b + a$ [infatti è vero in A].

Abbiamo così verificato che $(A, +)$ è un gruppo commutativo. Si ha inoltre:

$\forall\, a, b \in A',\ ab \in A'$ [infatti $A' \cdot A' \subseteq A'$];
$\forall\, a, b, c \in A',\ (ab)c = a(bc)$ [infatti è vero in A];
$\forall\, a, b, c \in A',\ a(b + c) = ab + ac$ e $(a + b)c = ac + bc$ [infatti è vero in A].

Si conclude che A' è un anello.

* * *

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.

Soluzione. (*i*) Si ha: $f(0_A) = \begin{cases} f(0_A) + f(0_A) \\ f(0_A) + 0_B. \end{cases}$ Dunque $f(0_A) + 0_B = f(0_A) + f(0_A)$ e quindi, cancellando a sinistra, $f(0_A) = 0_B$.

(*ii*) Risulta: $f(-a) + f(a) = f((-a) + a) = f(0_A) = 0_B$ [da (*i*)]. Analogamente, si verifica che anche $f(a) + f(-a) = 0_B$. Dunque si conclude che $f(-a)$ è l'opposto di $f(a)$: $f(-a) = -f(a)$.

(*iii*) In base all'Esercizio **20**, bisogna verificare che $f(A) - f(A) \subseteq f(A)$ e $f(A) \cdot f(A) \subseteq f(A)$. Si ha infatti, $\forall\, a, a' \in A$:

$$\begin{cases} f(a) - f(a') = f(a) + (-f(a')) = f(a) + (f(-a')) = f(a - a') \in f(A); \\ f(a) \cdot f(a') = f(aa') \in f(A). \end{cases}$$

* * *

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*) $\mathbf{0} : A \to B$ tale che $\mathbf{0}(a) = 0_B,\ \forall\, a \in A$.

(*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 $f(1_A) = 1_B$.

Soluzione. (*i*)(*a*). L'applicazione *nulla* $\mathbf{0} : A \to B$ tale che $\mathbf{0}(a) = 0_B,\ \forall\, a \in A$ è un omomorfismo di anelli. Infatti, $\forall\, a, a' \in A$:

$$\mathbf{0}(a + a') = 0_B = 0_B + 0_B = \mathbf{0}(a) + \mathbf{0}(a'); \quad \mathbf{0}(a \cdot a') = 0_B = 0_B \cdot 0_B = \mathbf{0}(a) \cdot \mathbf{0}(a').$$

Si ha: $\mathbf{0}(1_A) = 0_B \neq 1_B$. [Si noti che in un anello unitario si assume che lo zero non coincida mai con l'unità].

(*i*)(*b*). L'applicazione $f : \boldsymbol{R} \to \mathfrak{M}_2(\boldsymbol{R})$ tale che $f(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix},\ \forall\, a \in \boldsymbol{R}$, è un omomorfismo di anelli. Infatti, $\forall\, a, a' \in A$:

$$f(a + a') = \begin{pmatrix} a + a' & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a' & 0 \\ 0 & 0 \end{pmatrix} = f(a) + f(a').$$

$$f(a\cdot a')=\begin{pmatrix} aa' & 0\\ 0 & 0\end{pmatrix}=\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix} a' & 0\\ 0 & 0\end{pmatrix}=f(a)\cdot f(a').$$

Si ha: $f(1_{\mathbf{R}})=\begin{pmatrix} 1 & 0\\ 0 & 0\end{pmatrix}\neq\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}=1_{\mathfrak{M}_2(\boldsymbol{R})}$.

(*ii*) Essendo f suriettiva, $\forall\, b\in B$, $\exists\, a\in A$ tale che $f(a)=b$. Allora:

$$b=f(a)=\begin{cases} f(a\cdot 1_A)=f(a)\cdot f(1_A)=b\cdot f(1_A);\\ f(1_A\cdot a)=f(1_A)\cdot f(a)=f(1_A)\cdot b.\end{cases}$$

Dunque $b\cdot f(1_A)=b=f(1_A)\cdot b$, $\forall\, b\in B$. Poiché l'unità è unica (cfr. Esercizio **24**) si conclude che $f(1_A)=1_B$.

(*iii*) In ogni anello integro B vale la *legge di cancellazione del prodotto*:

$$ab=ac,\ a\neq 0\implies b=c$$

[infatti $ab=ac\Longrightarrow ab-ac=0\Longrightarrow a(b-c)=0\Longrightarrow b-c=0\Longrightarrow b=c$].

Essendo $f\neq 0$, $\exists\, a\in A$ tale che $f(a)\neq 0$. Allora

$$1_B\cdot f(a)=f(a)=f(1_A\cdot a)=f(1_A)\cdot f(a).$$

Cancellando a destra $f(a)$, si ottiene $1_B=f(1_A)$.

* * *

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?

Soluzione. (*i*) Sia $a\in\mathcal{U}(A)$, con $aa'=1_A$. Allora $f(a)\cdot f(a')=f(aa')=f(1_A)=1_B$. Quindi $f(a)\in\mathcal{U}(B)$ e pertanto $f(\mathcal{U}(A))\subseteq\mathcal{U}(B)$.

(*ii*) Si consideri l'inclusione canonica $i:\boldsymbol{Z}\hookrightarrow\boldsymbol{Q}$ [che è un omomorfismo unitario di anelli]. Si ha: $\mathcal{U}(\boldsymbol{Z})=\{\pm 1\}$ e $\mathcal{U}(\boldsymbol{Q})=\boldsymbol{Q}^{\cdot}=\boldsymbol{Q}-\{0\}$. Dunque $i(\mathcal{U}(\boldsymbol{Z}))\subset\mathcal{U}(\boldsymbol{Q})$.

(*iii*) Sia f l'omomorfismo non unitario dell'Esercizio **4**(*i*)(*b*). Si ha:

$$f(\mathcal{U}(\boldsymbol{R}))=f(\boldsymbol{R}^{\cdot})=\Big\{\begin{pmatrix} r & 0\\ 0 & 0\end{pmatrix},\ \forall\, r\neq 0\Big\},\quad \mathcal{U}(\mathfrak{M}_2(\boldsymbol{R}))=\{A\in\mathfrak{M}_2(\boldsymbol{R})\,|\,det(A)\neq 0\}.$$

Risulta quindi $f(\mathcal{U}(\boldsymbol{R}))\not\subset\mathcal{U}(\mathfrak{M}_2(\boldsymbol{R}))$ [anzi si ha che $f(\mathcal{U}(\boldsymbol{R}))\cap\mathcal{U}(\mathfrak{M}_2(\boldsymbol{R}))=\emptyset$].

Nota. Più banalmente, siano A, B anelli unitari e $f=\mathbf{0}:A\to B$ l'omomorfismo nullo. Allora $f(\mathcal{U}(A))=\{0\}\not\subset\mathcal{U}(B)$.

* * *

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.

Soluzione. Assumiamo noto che $(\boldsymbol{\mathcal{P}}(X),\Delta)$ sia un gruppo abeliano [cfr. **Esempi 3.2**(*iii*)]. Ricordiamo che $\emptyset$ è l'elemento neutro [infatti $A\Delta\emptyset=A$, $\forall\, A\in\boldsymbol{\mathcal{P}}(X)$] e che il reciproco di ogni $A\in\boldsymbol{\mathcal{P}}(X)$ è A stesso [infatti $A\Delta A=\emptyset$].

Consideriamo in $\boldsymbol{\mathcal{P}}(X)$ l'operazione $\cap$. Bisogna verificare che, $\forall\, A,B,C\in\boldsymbol{\mathcal{P}}(X)$, risulta:

(*i*) $\cap$ è associativa: $A\cap(B\cap C)=(A\cap B)\cap C$;

(*ii*) valgono le proprietà distributive: $\begin{cases} A\cap(B\Delta C)=(A\cap B)\Delta(A\cap C),\\ (A\Delta B)\cap C=(A\cap C)\Delta(B\cap C);\end{cases}$

(*iii*) $\cap$ ha elemento neutro X: $A\cap X=X\cap A=A$;

(*iv*) $\cap$ è commutativa: $A\cap B=B\cap A$.

Di tali proprietà possiamo limitarci a verificare soltanto la prima delle due formule di (*ii*), essendo le altre proprietà del tutto ovvie. Si ha:

$$\begin{aligned} x \in A \cap (B \Delta C) &\iff \big[(x \in A) \wedge (x \in B - C)\big] \vee \big[(x \in A) \wedge (x \in C - B)\big] \iff \\ &\iff \big[x \in A \wedge x \in B \wedge x \notin C)\big] \vee \big[x \in A \wedge x \in C \wedge x \notin B)\big] \iff \\ &\iff x \in \big[(A \cap B) - C)\big] \cup \big[(A \cap C) - B)\big] \iff \\ &\iff x \in \big[(A \cap B) - (A \cap C)\big] \cup \big[(A \cap C) - (B \cap C)\big] \iff \\ &\iff x \in (A \cap B) \Delta (A \cap C). \end{aligned}$$

[Si verifica facilmente che $(A \cap B) - (A \cap C) = (A \cap B) - C$].

Infine per verificare che, se $|X| \geq 2$, l'anello $(\boldsymbol{\mathcal{P}}(X), \Delta, \cap)$ non è integro, basta osservare che, $\forall\, A \in \boldsymbol{\mathcal{P}}(X)$, con $A \neq \emptyset,\, X$, risulta

$$A \cap (X - A) = \emptyset,$$

e dunque A è un divisore dello zero [essendo $A,\, X - A \neq \emptyset$]

* * *

1.30. Utilizzando il seguente fatto: $\nexists\, k \in \boldsymbol{N}$ tale che $0 < k < 1$, dimostrare la validità della *proprietà archimedea* in $\boldsymbol{N}$:

$$\forall\, m,\, n \in \boldsymbol{N},\ n \neq 0,\ \exists\, p \in \boldsymbol{N} \text{ tale che } m < np.$$

Soluzione. Se $m = 0$, basta porre $p = 1$. Sia allora $m > 0$.

Se $\exists\, p \in \boldsymbol{N}$ tale che $m = n\,p$, allora $n(p+1) = n\,p + n = m + n > m$ e dunque $m < n(p+1)$. Assumiamo, per assurdo, che sia $m > n\,p,\ \forall\, p \in \boldsymbol{N}$. Allora in particolare $m > n\,m$, cioè $1m > n\,m$. Cancellando m, segue che $1 > n$. Poiché non esistono naturali compresi strettamente tra 0 ed 1, segue che $n = 0$: assurdo, per ipotesi.

* * *

1.31. [*Esonero 8/4/03*] Utilizzando il principio di induzione si dimostri che, per ogni numero naturale positivo n, risulta:

$$1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1) = \tfrac{(2n)!}{2^n \cdot n!}.$$

Soluzione. *Base induttiva:* il risultato è vero per $n = 1$. Infatti $1 = \frac{2!}{2 \cdot 1!}$.

Passo induttivo: sia $n \geq 1$ e supponiamo che valga la formula

$$1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1) = \tfrac{(2n)!}{2^n \cdot n!}.$$

Verifichiamo che un'analoga formula vale per $n+1$. Infatti si ha:

$$\begin{aligned} &1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1) \cdot (2(n+1)-1) = 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1) \cdot (2n+1) = \\ &= \tfrac{(2n)!}{2^n \cdot n!} \cdot (2n+1) = \tfrac{(2n+1)!}{2^n \cdot n!}\, \tfrac{2(n+1)}{2(n+1)} = \tfrac{(2(n+1))!}{2^{n+1} \cdot (n+1)!}. \end{aligned}$$

* * *

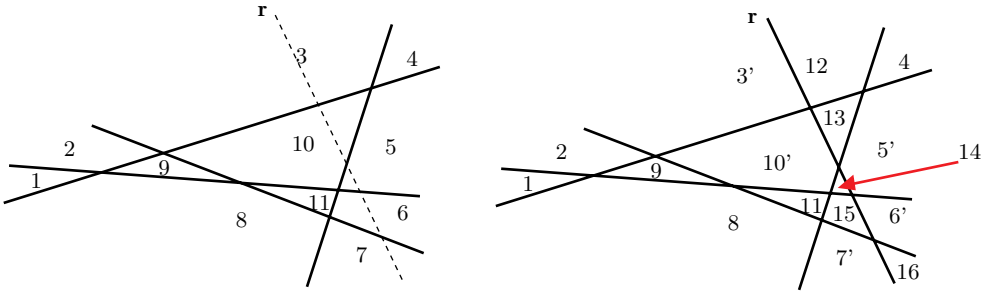
1.32. Per ogni intero $n \geq 1$, denotiamo con $\mathfrak{P}_n$ un insieme di n rette del piano in "posizione generica" [cioè non parallele tra loro e non incidenti a tre a tre]. Dimostrare per induzione su $n \geq 1$ che $\mathfrak{P}_n$ ripartisce il piano in $1 + \binom{n+1}{2}$ regioni disgiunte.

Soluzione. *Base induttiva:* il risultato è vero per $n = 1$. Infatti una retta $\mathfrak{P}_1$ ripartisce il piano in 2 parti e $1 + \binom{1+1}{2} = 2$.

Passo induttivo: sia $n \geq 1$. Si assume il risultato vero per ogni $\mathfrak{P}_n$ e lo si dimostra per $\mathfrak{P}_{n+1}$.

Si scelgano n rette in $\mathfrak{P}_{n+1}$: tali rette sono in posizione generica e quindi, per ipotesi induttiva, ripartiscono il piano in $1 + \binom{n+1}{2}$ regioni disgiunte. L'ultima retta $\boldsymbol{r}$ di $\mathfrak{P}_{n+1}$ [quella non scelta] interseca le altre n rette in n punti distinti. Dunque viene ripartita in $n+1$ segmenti disgiunti [di cui due illimitati]. Ciascuno di essi giace in un'unica regione [tra quelle sopra considerate] e la divide in due regioni disgiunte. Dunque $\mathfrak{P}_{n+1}$ ripartisce il piano in $1 + \binom{n+1}{2} + (n+1)$ regioni disgiunte. Risulta:

$$1+\tbinom{n+1}{2}+(n+1)=1+\tbinom{n+1}{2}+\tbinom{n+1}{1}=1+\tbinom{n+2}{2}.$$



[Nel disegno, relativo a $\mathfrak{P}_5$, quattro rette individuano undici regioni del piano; la quinta retta $\boldsymbol{r}$ suddivide ciascuna delle cinque regioni $3, 10, 5, 6, 7$ in due parti, creando le dieci regioni $3', 12, 10', 13, 5', 14, 6', 15, 7', 16$.]

* * *

1.33. Siano x, y numeri reali. Dimostrare che, $\forall\, n \geq 0$, vale la seguente formula:

$$\sum_{k=0}^{n}(x+ky)=\tfrac{1}{2}(n+1)(2x+ny).$$

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

Base induttiva. Per $n=0$ la formula vale, in quanto $\sum_{k=0}^{0}(x+ky)=x=\frac{1}{2}(0+1)(2x+0y)$.

Passo induttivo. Sia $n>0$ ed assumiamo che la formula valga per $n-1$:

$$\sum_{k=0}^{n-1}(x+ky)=\tfrac{1}{2}\,n(2x+(n-1)y).$$

Proviamo che è vera per n:

$$\sum_{k=0}^{n}(x+ky)=\sum_{k=0}^{n-1}(x+ky)+(x+ny)=\tfrac{1}{2}\,n(2x+(n-1)y)+x+ny=nx+\tfrac{1}{2}\,n(n-1)y+x+ny=$$
$$=(n+1)x+(\tfrac{1}{2}\,n(n-1)+n)y=\tfrac{1}{2}(n+1)2x+\tfrac{1}{2}(n^2+n)y=\tfrac{1}{2}(n+1)(2x+ny).$$

* * *

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

$$\boldsymbol{a}(n)=x^{F(n-1)}\,y^{F(n)},\ \forall\, n\geq 1.$$

Soluzione. *Base induttiva.* L'asserto è vero per $n=1$: infatti $\boldsymbol{a}(1)=y$ e $x^{F(0)}\,y^{F(1)}=x^0y^1=y$.
Passo induttivo. Sia $n\geq 2$; supposto che, $\forall\, k\leq n-1$ risulti $\boldsymbol{a}(k)=x^{F(k-1)}\,y^{F(k)}$, dimostriamo che $\boldsymbol{a}(n)=x^{F(n-1)}\,y^{F(n)}$. Infatti:

$$\boldsymbol{a}(n)=\boldsymbol{a}(n-2)\cdot\boldsymbol{a}(n-1)=x^{F(n-3)}\,y^{F(n-2)}\,x^{F(n-2)}\,y^{F(n-1)}=$$
$$=x^{F(n-3)+F(n-2)}\,y^{F(n-2)+F(n-1)}=x^{F(n-1)}\,y^{F(n)}.$$

Si noti però che per $n=2$, $F(n-3)$ non è definito. Dunque occorre far iniziare il passo induttivo da $n=3$ e verificare prima il caso $n=2$. Si inserisca quindi, prima del passo induttivo, questa verifica:

$$\boldsymbol{a}(2)=\boldsymbol{a}(0)\cdot\boldsymbol{a}(1)=xy\quad\text{e}\quad x^{F(1)}\,y^{F(2)}=x^1y^1=xy.$$

* * *

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].

Soluzione. Consideriamo la successione ricorsiva $\{a_n\}$. Osserviamo che, $\forall\, n \geq 2,\ a_n - a_{n-1} = n$. Si ha quindi:

$$a_n = a_n - \sum_{k=1}^{n-1} a_k + \sum_{k=1}^{n-1} a_k = (a_n - a_{n-1}) + (a_{n-1} - a_{n-2}) + \,.....\, + (a_2 - a_1) + a_1 =$$
$$= n + (n-1) + \,.....\, + 2 + 1 = \tbinom{n+1}{2}.$$

Dunque $a_n = \binom{n+1}{2},\ \forall\, n \geq 2$. Tale uguaglianza vale anche per $n = 1$ [infatti $1 = a_1 = \binom{1+1}{2}$]. Dunque la formula chiusa richiesta è la seguente:

$$a_n = \tbinom{n+1}{2},\ \ \forall\, n \geq 1.$$

Consideriamo ora la successione ricorsiva $\{b_n\}$. Osserviamo che, $\forall\, n \geq 2,\ b_n/b_{n-1} = n$. Si ha quindi:

$$b_n = b_n \cdot \tfrac{b_{n-1}}{b_{n-1}} \cdot \tfrac{b_{n-2}}{b_{n-2}} \cdot \,.....\, \cdot \tfrac{b_2}{b_2} \cdot \tfrac{b_1}{b_1} = \tfrac{b_n}{b_{n-1}} \cdot \tfrac{b_{n-1}}{b_{n-2}} \cdot \,.....\, \cdot \tfrac{b_2}{b_1} \cdot b_1 = n \cdot (n-1) \cdot \,.....\, \cdot 2 \cdot 1 = n!$$

Dunque $b_n = n!,\ \forall\, n \geq 2$. Tale uguaglianza vale anche per $n = 1$ [infatti $b_1 = 1 = 1!$]. Dunque la formula chiusa richiesta è la seguente:

$$b_n = n!,\ \ \forall\, n \geq 1.$$

* * *

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 ?

Soluzione. (*i*) Risulta: $\mathcal{N}(z) = z\,\overline{z} = \frac{1}{8}$ e quindi $\frac{1}{z} = \frac{\overline{z}}{z\,\overline{z}} = 8\overline{z} = 2 - 2i$.

Posto $\frac{1}{z} = r(\cos t_0 + i \sin t_0),\ 0 \leq t_0 < 2\pi$, si ha:

$$r = \left|\tfrac{1}{z}\right| = \sqrt{4+4} = \sqrt{8}, \quad t_0 = 2\pi - \arccos \tfrac{2}{\sqrt{8}} = 2\pi - \tfrac{\pi}{4} = \tfrac{7}{4}\pi$$

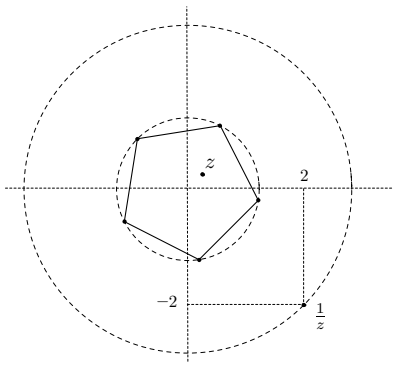
e quindi $\frac{1}{z} = \sqrt{8}\big(\cos \frac{7}{4}\pi + i \sin \frac{7}{4}\pi\big)$.

(*ii*) Risulta: $(\frac{1}{z})^{\frac{1}{5}} = (2-2i)^{\frac{1}{5}} = \big\{r^{\frac{1}{5}}\big(\cos \frac{t_0+2k\pi}{5} + i \sin \frac{t_0+2k\pi}{5}\big),\ \forall\, k = 0, .., 4\big\} =$

$$= \big\{2^{\frac{3}{10}}\big(\cos \tfrac{7\pi+8k\pi}{20} + i \sin \tfrac{7\pi+8k\pi}{20}\big),\ \forall\, k = 0, .., 4\big\}.$$

Le cinque radici quinte di $\frac{1}{z}$ sono i vertici di un pentagono regolare inscritto nella circonferenza di centro $2^{\frac{3}{10}}$ (centrata in O), con angoli $\frac{(7+8k)\pi}{20}$, per $k = 0 .., 4$.

Risulta: $\pi < \frac{(7+8k)\pi}{20} < \frac{3\pi}{2} \iff 20 < 7 + 8k < 30 \iff k = 2$. L'unica radice quinta avente parte reale e parte immaginaria negative è quindi $2^{\frac{3}{10}}\big(\cos \frac{23}{20}\pi + i \sin \frac{23}{20}\pi\big)$.



* * *

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 $\boldsymbol{R}^2$.

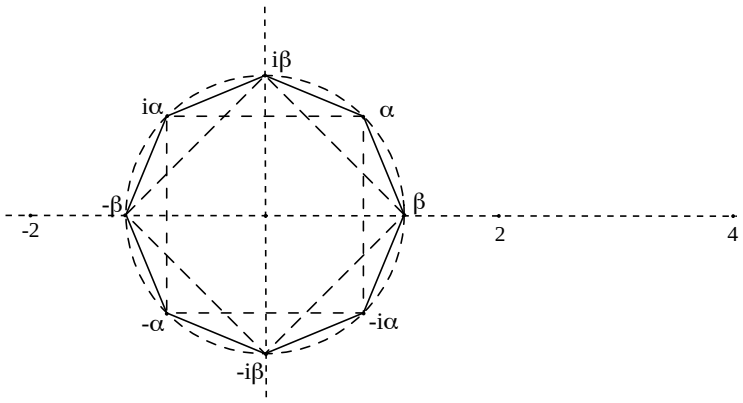
Soluzione. (*i*) Si ha: $-2 = 2(\cos\pi + i\sin\pi)$. Allora $(-2)^{1/4}$ contiene in particolare

$$\alpha = 2^{1/4}\big(\cos\tfrac{\pi}{4} + i\sin\tfrac{\pi}{4}\big) = 2^{1/4}\big(\tfrac{1}{\sqrt2} + i\,\tfrac{1}{\sqrt2}\big) = \tfrac{1}{2^{1/4}}(1+i).$$

Essendo $\{\pm1, \pm i\}$ le radici quarte dell'unità, allora

$$(-2)^{1/4} = \big\{\pm\alpha, \pm i\alpha\big\} = \big\{\pm\tfrac{1}{2^{1/4}}(1+i),\ \pm\tfrac{1}{2^{1/4}}(1+i)i = \big\{\pm\tfrac{1}{2^{1/4}}(1+i),\ \pm\tfrac{1}{2^{1/4}}(-1+i)\big\}.$$

(*ii*) Ogni radice quarta γ di -2 è anche radice ottava di 4 [infatti $\gamma^4 = -2 \implies \gamma^8 = (-2)^2 = 4$]. Dunque quattro delle otto radici ottave di 4 sono quelle sopra ottenute. Le quattro restanti sono ottenibili a partire da $\beta = 4^{1/8} = 2^{1/4}$ [è l'unica radice reale tra le otto], moltiplicando tale radice per $\pm1, \pm i$. Si ottengono le altre quattro radici ottave di 4: $\pm(2^{1/4}),\ \pm i(2^{1/4})$.



Le otto radici ottenute si dispongono nei vertici di un poligono regolare 8-latero di raggio $2^{1/4}$, di cui un vertice (cioè β) si trova sul semiasse x positivo.

* * *

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.

Soluzione. Risulta: $z = r\big(\cos t + i\sin t\big)$, con

$$\begin{cases} r = |z| = \sqrt{4+4} = 2^{3/2} \\ t = 2\pi - \arccos\frac{-2}{\sqrt8} = 2\pi - (\pi - \frac{\pi}{4}) = \frac{5\pi}{4}. \end{cases}$$

Calcoliamo $z^{3/4}$. Risulta:

$$z^3 = r^3\big(\cos 3t + i\sin 3t\big) = 2^{9/2}\big(\cos\tfrac{15\pi}{4} + i\sin\tfrac{15\pi}{4}\big)$$

e quindi, per $k = 0, 1, 2, 3$:

$$z^{3/4} = (z^3)^{1/4} = \big(2^{9/2}\big)^{1/4}\Big[\cos\big(\tfrac{\frac{15\pi}{4}+2k\pi}{4}\big) + i\sin\big(\tfrac{\frac{15\pi}{4}+2k\pi}{4}\big)\Big] =$$
$$= 2^{9/8}\big[\cos\big(\tfrac{15\pi}{16} + \tfrac{k\pi}{2}\big) + i\sin\big(\tfrac{15\pi}{16} + \tfrac{k\pi}{2}\big)\big].$$

I quattro numeri complessi $z^{3/4}$ sono vertici di un quadrato del piano di Argand-Gauss inscritto nella circonferenza di raggio $2^{9/8} \cong 2.18$ (centrata in O).

Calcoliamo ora $z^{4/3}$. Risulta:

$$z^4 = r^4\big(\cos 4t + i\sin 4t\big) = 2^6\big(\cos 5\pi + i\sin 5\pi\big) = 2^6\big(\cos\pi + i\sin\pi\big)$$

e quindi, per $k = 0, 1, 2$:

$$z^{4/3} = (z^4)^{1/3} = 2^{6/3}\big[\cos\big(\tfrac{\pi+2k\pi}{3}\big) + i\sin\big(\tfrac{\pi+2k\pi}{3}\big)\big] =$$
$$= 4\big[\cos\big(\tfrac{\pi}{3} + \tfrac{2k\pi}{3}\big) + i\sin\big(\tfrac{\pi}{3} + \tfrac{2k\pi}{3}\big)\big].$$

Si tratta di tre numeri complessi, vertici di un triangolo equilatero del piano di Argand-Gauss inscritto in una circonferenza di raggio 4 (centrata in O).

* * *

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*) $\{z = a + i\,b \in \boldsymbol{C} :\ a, b \in \boldsymbol{Z}\}$.

Soluzione. (*i*) Posto $A = \{z = a + i\,b \in \boldsymbol{C} :\ a = b\}$, verificheremo che $(A, +) \cong (\boldsymbol{R}, +)$ e che A non è chiuso rispetto al prodotto. Si consideri l'applicazione

$$f : \boldsymbol{R} \to A \text{ tale che } f(a) = a + ia,\ \forall\, a \in \boldsymbol{R}.$$

Ovviamente f è biiettiva; inoltre

$$f(a + b) = (a + b) + i(a + b) = a + ia + b + ib = f(a) + f(b).$$

Dunque f è un isomorfismo tra $(\boldsymbol{R}, +)$ e $(A, +)$.

Ad esempio $1 + i \in A$ e $(1 + i)(1 + i) = 2i \notin A$: dunque A non è chiuso rispetto al prodotto.

(*ii*) Posto $\boldsymbol{U} = \{z \in \boldsymbol{C} :\ \mathcal{N}(z) = 1\}$, verificheremo che $\boldsymbol{U}$ non è chiuso rispetto alla somma, ma che è un sottogruppo di $(\boldsymbol{C}^{\cdot}, \cdot)$ (rispetto al prodotto).

Ad esempio $1, i \in \boldsymbol{U}$, ma $1 + i \notin \boldsymbol{U}$. Se $z_1, z_2 \in \boldsymbol{U}$, allora $z_1 z_2 \in \boldsymbol{U}$ [infatti $\mathcal{N}(z_1 z_2) = z_1 z_2\, \overline{z_1 z_2} = z_1\, \overline{z_1}\, z_2\, \overline{z_2} = \mathcal{N}(z_1)\mathcal{N}(z_2) = 1 \cdot 1 = 1$]: dunque $\boldsymbol{U}$ è chiuso rispetto al prodotto. Si ha: $1 \in \boldsymbol{U}$ (ovvio); se $z \in \boldsymbol{U}$, anche $\frac{1}{z} \in \boldsymbol{U}$ [infatti $\frac{1}{z} = \frac{\overline{z}}{z\,\overline{z}} = \frac{\overline{z}}{1} = \overline{z}$ e $\mathcal{N}(\overline{z}) = \overline{z}\,\overline{\overline{z}} = \overline{z}\, z = 1$: dunque $\mathcal{N}(\frac{1}{z}) = 1$]; infine l'associatività vale in $\boldsymbol{U}$ perché vale in $\boldsymbol{C}^{\cdot}$.

(*iii*) Posto $\boldsymbol{Q}[i] := \{a + ib \in \boldsymbol{C} \ :\ a, b \in \boldsymbol{Q}\}$, si verifica che $\boldsymbol{Q}[i]$ è un campo (sottocampo di $\boldsymbol{C}$). Infatti si verifica che $\boldsymbol{Q}[i] - \boldsymbol{Q}[i] \subseteq \boldsymbol{Q}[i]$, $\boldsymbol{Q}[i] \cdot \boldsymbol{Q}[i] \subseteq \boldsymbol{Q}[i]$. Infine, $\forall\, z \in \boldsymbol{Q}[i]$, anche $\frac{1}{z} \in \boldsymbol{Q}[i]$.

(*iv*) Posto $\boldsymbol{Z}[i] := \{a + ib \in \boldsymbol{C} \ :\ a, b \in \boldsymbol{Z}\}$, si verifica che $\boldsymbol{Z}[i]$ è un sottoanello di $\boldsymbol{C}$ (e quindi un dominio d'integrità), ma non è un campo [infatti $\frac{1}{1+i} = \frac{1}{2} - i\frac{1}{2} \notin \boldsymbol{Z}[i]$. Tale anello è chiamato *anello degli interi di Gauss*.

* * *

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 $f(\boldsymbol{U}) \subseteq \boldsymbol{U}$).

Soluzione. (*i*) Poiché $\overline{\overline{z}} = z,\ \forall\, z \in \boldsymbol{C}$, allora $\varphi^2 = \mathbf{1}_{\boldsymbol{C}}$. Dunque φ è biiettiva, con $\varphi^{-1} = \varphi$. Si ha:

$$\varphi(z_1 + z_2) = \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} = \varphi(\overline{z_1}) + \varphi(\overline{z_2}),$$

$$\varphi(z_1 \cdot z_2) = \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2} = \varphi(\overline{z_1}) \cdot \varphi(\overline{z_2}).$$

Dunque φ è un isomorfismo di $\boldsymbol{C}$ su se stesso.

(*ii*) (*a*) Risulta: $f^2 = \mathbf{1}_{\boldsymbol{C}}$. Dunque $f : \boldsymbol{C}^{\cdot} \to \boldsymbol{C}^{\cdot}$ è biiettiva (con inversa se stessa). Si ha:

$$f(z_1 z_2) = \tfrac{1}{z_1 z_2} = \tfrac{1}{z_1}\tfrac{1}{z_2} = f(z_1) f(z_2).$$

Dunque f è isomorfismo del gruppo $(\boldsymbol{C}^{\cdot}, \cdot)$ in sé.

(*b*) Risulta:

$$f(z) = z \iff \tfrac{1}{z} = z \iff z^2 = 1 \iff z \in \sqrt{1} \iff z = \pm 1.$$

(*c*) Bisogna verificare che se $\mathcal{N}(z) = 1$, allora $\mathcal{N}(\frac{1}{z}) = 1$. Infatti

$$\tfrac{1}{z} = \tfrac{\overline{z}}{z\,\overline{z}} = \tfrac{\overline{z}}{1} = \overline{z} \quad \text{e} \quad \mathcal{N}(\overline{z}) = \overline{z}\,\overline{\overline{z}} = \overline{z}\, z = z\,\overline{z} = 1.$$

Si noti che risulta : $f(\boldsymbol{U}) = \boldsymbol{U}$. Infatti, $\forall\, z \in \boldsymbol{U},\ z = f\big(\frac{1}{\frac{1}{z}}\big)$ e $\frac{1}{\frac{1}{z}} \in \boldsymbol{U}$. f opera su $\boldsymbol{U}$ come il coniugio su $\boldsymbol{R}^2$ (simmetria rispetto all'*asse* x).

* * *

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.

Soluzione. (i) Si noti preliminarmente che

$$z^2 = (3-4\,i)^2 = 9-16-24\,i = -7-24\,i, \quad \tfrac{1}{z} = \tfrac{\bar z}{z\,\bar z} = \tfrac{3+4\,i}{25} = \tfrac{3}{25} + \tfrac{4}{25}\,i.$$

Per rispondere correttamente alla domanda bisogna però calcolare z^2 e $\frac{1}{z}$ tramite le formule

$$z^2 = \rho^2\big(\cos(2\vartheta_0) + i\sin(2\vartheta_0)\big), \quad \tfrac{1}{z} = \tfrac{1}{\rho}\big(\cos(-\vartheta_0) + i\sin(-\vartheta_0)\big),$$

con $z = \rho(\cos\vartheta_0 + i\sin\vartheta_0)$. Il modulo ρ e l'argomento principale ϑ_0 di z sono:

$$\rho = |z| = \sqrt{9+16} = 5, \quad \vartheta_0 = 2\pi - \arccos\tfrac{3}{\sqrt{25}} = 2\pi - \arccos\tfrac{3}{5} \approx 5.35589 \text{ (rad)}.$$

Risulta quindi:

$$\begin{cases} \cos\vartheta_0 = \cos(2\pi - \arccos\frac{3}{5}) = \cos(\arccos\frac{3}{5}) = \frac{3}{5}, \\ \sin\vartheta_0 = -\sqrt{1-\cos^2\vartheta_0} = -\sqrt{1-\frac{9}{25}} = -\frac{4}{5} \end{cases}$$

[si noti che il seno di un angolo del IV quadrante è negativo]. Allora:

$$\begin{cases} \cos(2\vartheta_0) = \cos^2\vartheta_0 - \sin^2\vartheta_0 = \frac{9}{25} - \frac{16}{25} = -\frac{7}{25}, \\ \sin(2\vartheta_0) = 2\sin\vartheta_0\cos\vartheta_0 = 2(-\frac{4}{5})(\frac{3}{5}) = -\frac{24}{25}. \end{cases}$$

Quindi $z^2 = 25(-\frac{7}{25} - i\,\frac{24}{25}) = -7-24\,i$ (come precedentemente ottenuto).

Calcoliamo ora $\frac{1}{z}$. Si ha: $\cos(-\vartheta_0) = \cos\vartheta_0 = \frac{3}{5}$, $\sin(-\vartheta_0) = -\sin\vartheta_0 = \frac{4}{5}$ e dunque $\frac{1}{z} = \frac{1}{5}(\frac{3}{5} + \frac{4}{5}\,i) = \frac{3}{25} + \frac{4}{25}\,i$ (come precedentemente ottenuto).

(ii) Risulta: $\sqrt{z} = \big\{\alpha, -\alpha\big\}$, con $\alpha = \sqrt{\rho}\,\big(\cos\frac{\vartheta_0}{2} + i\sin\frac{\vartheta_0}{2}\big)$.

Poiché $\frac{3\pi}{2} < \vartheta_0 < 2\pi$, allora $\frac{3\pi}{4} < \frac{\vartheta_0}{2} < \pi$ e quindi $\sin(\frac{\vartheta_0}{2}) > 0$ mentre $\cos(\frac{\vartheta_0}{2}) < 0$. Quindi

$$\begin{cases} \cos(\frac{\vartheta_0}{2}) = -\sqrt{\frac{1+\cos\vartheta_0}{2}} = -\sqrt{\frac{1+\frac{3}{5}}{2}} = -\frac{2}{\sqrt5}, \\ \sin(\frac{\vartheta_0}{2}) = \sqrt{\frac{1-\cos\vartheta_0}{2}} = \sqrt{\frac{1-\frac{3}{5}}{2}} = \frac{1}{\sqrt5}. \end{cases}$$

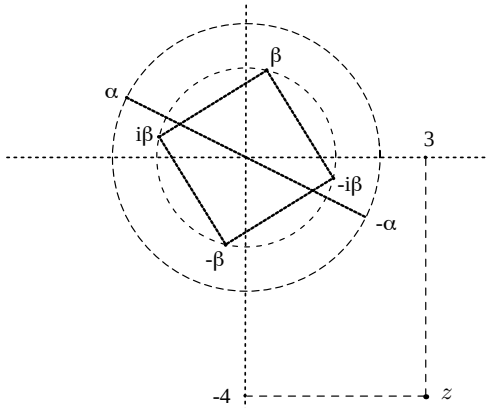
Dunque $\alpha = \sqrt5\,\big(-\frac{2}{\sqrt5} + i\,\frac{1}{\sqrt5}\big) = -2+i$ e pertanto $\sqrt{z} = \big\{-2+i,\, 2-i\big\}$.

Risulta: $z^{1/4} = \big\{\beta, i\,\beta, -\beta, -i\,\beta\big\}$, con $\beta = \rho^{1/4}\big(\cos(\frac{\vartheta_0}{4}) + i\sin(\frac{\vartheta_0}{4})\big)$.

Poiché $\frac{3\pi}{8} < \frac{\vartheta_0}{4} < \frac{\pi}{2}$, allora $\cos(\frac{\vartheta_0}{4})$, $\sin(\frac{\vartheta_0}{2}) > 0$ e quindi

$$\begin{cases} \cos(\frac{\vartheta_0}{4}) = \sqrt{\frac{1+\cos(\frac{\vartheta_0}{2})}{2}} = \sqrt{\frac{1-\frac{2}{\sqrt5}}{2}} = \frac{\sqrt{\sqrt5-2}}{\sqrt2\,5^{1/4}}, \\ \sin(\frac{\vartheta_0}{4}) = \sqrt{\frac{1-\cos(\frac{\vartheta_0}{2})}{2}} = \sqrt{\frac{1+\frac{2}{\sqrt5}}{2}} = \frac{\sqrt{\sqrt5+2}}{\sqrt2\,5^{1/4}}. \end{cases}$$

Dunque $\beta = 5^{1/4}\big(\cos(\frac{\vartheta_0}{4}) + i\sin(\frac{\vartheta_0}{4})\big) = \frac{1}{\sqrt2}\,\big(\sqrt{\sqrt5-2} + i\,\sqrt{\sqrt5+2}\big)$.



* * *

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: $i(a) = \frac{a}{1}, \ \ \forall\, a \in \boldsymbol{R}$. Verificare che i è un omomorfismo iniettivo di anelli. i è detto *immersione canonica* di R nel suo campo dei quozienti K.

Soluzione. (*i*) $\equiv$ è certamente riflessiva e simmetrica. Verifichiamo che è anche transitiva. Sia $(a, b) \equiv (c, d)$ e $(c, d) \equiv (e, f)$. Allora $ad = bc$, $cf = de$. Moltiplicando tali uguaglianze per f, b (risp.), si ottiene $adf = bcf$, $bcf = bde$ e dunque $(af - be)d = 0$. Poiché R è integro, d non è uno 0-divisore e dunque $af - be = 0$. Si conclude che $(a, b) \equiv (e, f)$.

(*ii*) Siano $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$. Allora $ab' = a'b$, $cd' = c'd$. Risulta:

$$(a'd' + b'c')bd = a'b\, dd' + c'd\, bb' = ab'\, dd' + cd'\, bb' = (ad + bc)b'd'$$

e dunque $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$. Pertanto $+$ è ben definita. Analogamente

$$ac\, b'd' = ab'\, cd' = a'b\, c'd = a'c'\, bd$$

e dunque $\frac{ac}{bd} = \frac{a'c'}{b'd'}$. Pertanto anche $\cdot$ è ben definita.

Si verificano facilmente tutti gli assiomi che rendono $(K, +, \cdot)$ un anello commutativo con unità [si osservi che lo zero e l'unità di K sono risp. $\frac{0}{1}$, $\frac{1}{1}$]. Inoltre, $\forall\, \frac{a}{b} \in K^{\star}$, anche $\frac{b}{a} \in K$ e $\frac{b}{a} \cdot \frac{a}{b} = \frac{1}{1}$. Dunque ogni elemento non nullo ammette inverso e quindi K è un campo.

(*iii*) Risulta, $\forall\, a, b \in R$: $i(a + b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1}$, $\quad i(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1}$.

Dunque i è un omomorfismo di anelli. Infine, se $i(a) = i(b)$, allora $\frac{a}{1} = \frac{b}{1}$ e dunque $a = b$. Pertanto i è iniettiva.

* * *

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.

Soluzione. L'insieme delle successioni a valori in $\boldsymbol{R}$ [risp. in $\boldsymbol{N}$] è $\boldsymbol{R}^{\boldsymbol{N}}$ [risp. $\boldsymbol{N}^{\boldsymbol{N}}$]. Poiché $\boldsymbol{R} \sim 2^{\boldsymbol{N}}$, allora $\boldsymbol{R}^{\boldsymbol{N}} \sim (2^{\boldsymbol{N}})^{\boldsymbol{N}} \sim 2^{\boldsymbol{N}\times\boldsymbol{N}} \sim 2^{\boldsymbol{N}} \sim \boldsymbol{R}$. Inoltre $|\boldsymbol{R}| = |2^{\boldsymbol{N}}| = |2|^{|\boldsymbol{N}|} \le |\boldsymbol{N}|^{|\boldsymbol{N}|} \le |\boldsymbol{R}|^{|\boldsymbol{N}|} = |\boldsymbol{R}^{\boldsymbol{N}}| = |\boldsymbol{R}|$. Per antisimmetria si conclude che $|\boldsymbol{N}|^{|\boldsymbol{N}|} = |\boldsymbol{R}|$.

* * *

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 $\boldsymbol{R}[X_1, X_2, \ldots, X_n] \sim \boldsymbol{R}$.

Soluzione. Poiché $\boldsymbol{R}[X_1, X_2, \ldots, X_n] = \boldsymbol{R}[X_1][X_2] \ldots [X_n]$, è sufficiente verificare che $\boldsymbol{R}[X] \sim \boldsymbol{R}$.

Ogni polinomio $P = \sum_{i=0}^{n} a_i X^i \in \boldsymbol{R}[X]$ è identificabile con la successione (definitivamente nulla) dei suoi coefficienti $\{a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots.\}$. Dunque $\boldsymbol{R} \subset \boldsymbol{R}[X] \subset \boldsymbol{R}^{\boldsymbol{N}}$. Ne segue che $|\boldsymbol{R}| \le \big|\boldsymbol{R}[X]\big| \le \big|\boldsymbol{R}^{\boldsymbol{N}}\big|$. Poiché $\boldsymbol{R}^{\boldsymbol{N}} \sim \boldsymbol{R}$ [cfr. l'esercizio precedente], allora $|\boldsymbol{R}| \le \big|\boldsymbol{R}[X]\big| \le |\boldsymbol{R}|$ e dunque, per antisimmetria, $\big|\boldsymbol{R}[X]\big| = |\boldsymbol{R}|$, cioè $\boldsymbol{R}[X] \sim \boldsymbol{R}$, come richiesto.

* * *

1.45. Verificare che l'insieme delle funzioni reali di variabile reale ha cardinalità superiore a quella del continuo.

Soluzione. Risulta: $\boldsymbol{R}^{\boldsymbol{R}} \sim \big(2^{\boldsymbol{N}}\big)^{\boldsymbol{R}} \sim 2^{\boldsymbol{N}\times\boldsymbol{R}}$. Se dimostriamo che $\boldsymbol{N}\times\boldsymbol{R} \sim \boldsymbol{R}$, allora $\boldsymbol{R}^{\boldsymbol{R}} \sim 2^{\boldsymbol{R}}$ e quindi $|\boldsymbol{R}|^{|\boldsymbol{R}|} = 2^{|\boldsymbol{R}|} > |\boldsymbol{R}|$. Osservato che $\{1\}\times\boldsymbol{R} \subset \boldsymbol{N}\times\boldsymbol{R} \sim \boldsymbol{R} \subset \boldsymbol{R}\times\boldsymbol{R}$, si ha

$$|\boldsymbol{R}| = 1\cdot|\boldsymbol{R}| = |\{1\}\times\boldsymbol{R}| \le |\boldsymbol{N}\times\boldsymbol{R}| \le |\boldsymbol{R}\times\boldsymbol{R}| = |\boldsymbol{R}|.$$

Dunque $\boldsymbol{N}\times\boldsymbol{R} \sim \boldsymbol{R}$, come richiesto

* * *

Soluzioni degli 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 $x, y, z \in \boldsymbol{Z}$.

Soluzione. (*i*) Siano $a_1, \dots, a_n$ interi non tutti nulli. Si chiama *massimo comun divisore* di $a_1, \dots, a_n$ ogni intero $d \geq 1$ tale che

$$(i)\ d \,|\, a_1,\ \dots, d \,|\, a_n; \quad (ii)\ \text{se}\ \ d' \,|\, a_1,\ \dots, d' \,|\, a_n,\ \text{allora}\ \ d' \,|\, d.$$

(*ii*) Posto $d = MCD(a,b,c)$, $d_1 = MCD(b,c)$, $d_2 = MCD(a, d_1)$, si tratta di verificare che

$$d \,|\, d_2 \ \text{e}\ \ d_2 \,|\, d.$$

- Si ha: $d_2 \,|\, \begin{matrix} a \\ d_1 \end{matrix}$, $d_1 \,|\, \begin{matrix} b \\ c \end{matrix}$ e dunque, per transitività, $d_2 \,|\, \begin{matrix} a \\ b \\ c \end{matrix}$. Ne segue che $d_2 \,|\, d$.

- Poiché $d \,|\, \begin{matrix} a \\ b \\ c \end{matrix}$, allora $d \,|\, \begin{matrix} a \\ MCD(b,c) = d_1 \end{matrix}$ e dunque $d \,|\, d_2$.

(*iii*) Si ponga $d = MCD(ab, ac, bc)$. Poiché $d \,|\, \begin{matrix} ab \\ ac \end{matrix}$, allora $d \,|\, MCD(ab, ac) = |a| \cdot 1$ e dunque $d \,|\, a$. Analogamente, da $d \,|\, \begin{matrix} ab \\ bc \end{matrix}$ segue che $d \,|\, b$. Poiché $d \,|\, \begin{matrix} a \\ b \end{matrix}$ e $MCD(a,b) = 1$, allora $d \,|\, 1$ cioè $d = 1$.

(*iv*) La risposta è negativa. Se ad esempio si pone $a = 2$, $b = 3$, $c = 4$, allora $MCD(2,3,4) = 1$, mentre $MCD(6,8,12) \neq 1$.

(*v*) Si ponga $d = MCD(b,c)$. Dall'identità di Bézout, $d = br + cs$, $\exists\, r, s \in \boldsymbol{Z}$. Da (*ii*) segue che $1 = MCD(a,d)$ e dunque $1 = au + dv$, $\exists\, u, v \in \boldsymbol{Z}$. Pertanto

$$1 = au + dv = au + (br + cs)v = au + b\,rv + c\,sv,$$

che è l'identità di Bézout cercata.

Nota. Con la stessa dimostrazione si può verificare che sussiste sempre un'identità di Bézout, cioè che se $MCD(a,b,c) = d$, allora $d = ax + by + cz$, $\exists\, x, y, z \in \boldsymbol{Z}$.

* * *

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 ?

Soluzione. (*i*) Risulta:

a ha inverso aritmetico $(mod\ p^2) \iff \exists\, b \in \boldsymbol{Z}$ tale che $ab - 1 \equiv 0\ (mod\ p^2) \iff$
$\exists\, b \in \boldsymbol{Z}$ tale che $p^2 \,|\, ab - 1 \iff \exists\, b, c \in \boldsymbol{Z}$ tali che $ab - 1 = cp^2 \iff$
$\exists\, b, c \in \boldsymbol{Z}$ tali che $1 = ab - cp^2 \iff (a, p^2) = 1$.

Si ha:

$$(a, p^2) \neq 1 \iff a \in p\boldsymbol{Z}\ [\text{e}\ 1 \leq a < p^2] \iff a \in \{p, 2p, 3p, \dots, (p-1)p\}.$$

Gli elementi cercati sono dunque $p, 2p, 3p, \dots, (p-1)p$.

(*ii*) Per ipotesi, $\exists\, b \in \boldsymbol{Z}$ tale che $ab \equiv 1\ (mod\ m)$. Allora $m \,|\, ab - 1$, $n \,|\, m$ e quindi $n \,|\, ab - 1$, cioè $ab \equiv 1\ (mod\ n)$. Allora a ammette lo stesso inverso aritmetico $b\ (mod\ n)$.

L'ultima affermazione è in generale falsa. Si ponga infatti $n = 5$, $m = 10$ ed $a = 4$. Risulta: 4 ha inverso aritmetico $(mod\ 5)$ $[4 \cdot 4 \equiv 1\ (mod\ 5)]$ ma 4 non ha inverso aritmetico $(mod\ 10)$ [infatti

$(4, 10) \neq 1$]. L'affermazione non è però sempre falsa. Si ponga infatti $n = 5$, $m = 10$ ed $a = 3$. 3 ha inverso aritmetico sia $(mod\ 5)$ che $(mod\ 10)$ [infatti $3 \cdot 2 \equiv 1\ (mod\ 5)$ e $3 \cdot 7 \equiv 1\ (mod\ 10)$].

* * *

2.3. Risolvere l'equazione congruenziale lineare $121\,X \equiv 22\ (mod\ 33)$, indicandone un sistema completo di soluzioni *mod* 33.

Soluzione. Risulta $11 = (121, 33) \,\big|\, 22$ e quindi l'equazione è compatibile. L'equazione è equivalente a $11\,X \equiv 2\ (mod\ 3)$, cioè $2\,X \equiv 2\ (mod\ 3)$. Moltiplicando per l'inverso aritmetico di 2 $(mod\ 3)$, l'equazione si semplifica nella forma $X \equiv 4\ (mod\ 3)$, cioè $X \equiv 1\ (mod\ 3)$. La totalità delle soluzioni è data da $1 + 3\boldsymbol{Z}$. Un sistema completo di soluzioni è dato da

$$\big\{1 + \tfrac{33}{11}\,h,\ \forall\, h = 0, 1,\ ..., 10\big\} = \{1,\ 4,\ 7,\ 10,\ 13,\ 16,\ 19,\ 22,\ 25,\ 28,\ 31\}.$$

[Si noti che $(1 + 33\boldsymbol{Z}) \cup (4 + 33\boldsymbol{Z}) \cup (7 + 33\boldsymbol{Z}) \cup\ ...\ \cup (31 + 33\boldsymbol{Z}) = 1 + 3\boldsymbol{Z}$].

* * *

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.

Soluzione. Per $n = 10,\ 12,\ 14,\ 16,\ 2 \,\big|\, (6, n)$ e quindi $(6, n)$ non divide 9. Ne segue che l'equazione $6\,X \equiv 9\ (mod\ n)$ è incompatibile.

Sia $n = 9$. L'equazione $6\,X \equiv 9\ (mod\ 9)$ è equivalente a $6\,X \equiv 0\ (mod\ 9)$ ed è ovviamente compatibile: una soluzione è $x = 0$. L'equazione equivale a $2\,X \equiv 0\ (mod\ 3)$. La totalità delle soluzioni è $3\boldsymbol{Z}$. Un sistema completo di soluzioni $(mod\ 9)$ è $\{0,\ 0 + \frac{9}{3},\ 0 + 2\frac{9}{3}\} = \{0,\ 3,\ 6\}$.
[Si noti che $(9\boldsymbol{Z}) \cup (3 + 9\boldsymbol{Z}) \cup (6 + 9\boldsymbol{Z}) = 3\boldsymbol{Z}$].

Sia $n = 11$. L'equazione $6\,X \equiv 9\ (mod\ 11)$ è compatibile [infatti $1 = (6, 11) \,\big|\, 9$]. Poiché 6 ha inverso aritmetico 2 $(mod\ 11)$, l'equazione equivale a $X \equiv 18\ (mod\ 11)$, cioè $X \equiv 7\ (mod\ 11)$. L'insieme delle soluzioni è $7 + 11\boldsymbol{Z}$. Un sistema completo di soluzioni $(mod\ 11)$ è $\{7\}$.

Sia $n = 13$. L'equazione $6\,X \equiv 9\ (mod\ 13)$ è compatibile [infatti $1 = (6, 13) \,\big|\, 9$]. 6 ha inverso aritmetico -2 $(mod\ 13)$, ovvero 11 $(mod\ 13)$. L'equazione è equivalente a $X \equiv -18\ (mod\ 13)$, cioè $X \equiv 8\ (mod\ 13)$. Le soluzioni sono $8 + 13\boldsymbol{Z}$. Un sistema completo di soluzioni $(mod\ 13)$ è $\{8\}$.
Sia $n = 15$. L'equazione $6\,X \equiv 9\ (mod\ 15)$ è compatibile [infatti $3 = (6, 15) \big| 9$]. L'equazione è equivalente a $2X \equiv 3\ (mod\ 5)$ e 2 ha inverso aritmetico 3 $(mod\ 5)$. Allora l'equazione è equivalente a $X \equiv 9\ (mod\ 5)$, cioè $X \equiv 4\ (mod\ 5)$. L'insieme delle soluzioni è $4 + 5\boldsymbol{Z}$. Un sistema completo di soluzioni $(mod\ 15)$ è $\{4,\ 4 + \frac{15}{3},\ 4 + 2\frac{15}{3}\} = \{4,\ 9,\ 14\}$.

* * *

2.5. Risolvere il seguente sistema 'cinese' di equazioni congruenziali lineari

$$\begin{cases} X \equiv 2\ (mod\ 5) \\ X \equiv 1\ (mod\ 3) \\ X \equiv 6\ (mod\ 14) \\ X \equiv 5\ (mod\ 11). \end{cases}$$

Soluzione. La generica soluzione della prima equazione è

$$X = 2 + 5t_1,\ \forall\, t_1 \in \boldsymbol{Z}.$$

Sostituendo nella seconda,

$$2 + 5t_1 \equiv 1\ (mod\ 3),\ \text{ cioè }\ t_1 \equiv 1\ (mod\ 3),\ \text{ da cui }\ t_1 = 1 + 3t_2,\ \exists\, t_2 \in \boldsymbol{Z}.$$

Sostituendo nella precedente espressione di X, si ottiene la generica soluzione delle prime due equazioni

$$X = 7 + 5t_2,\ \forall\, t_2 \in \boldsymbol{Z}.$$

Sostituendo nella terza,

$$7 + 5t_2 \equiv 6\ (mod\ 14),\ \text{ cioè }\ t_2 \equiv 13\ (mod\ 14),\ \text{ da cui }\ t_2 = 13 + 14t_3,\ \exists\, t_3 \in \boldsymbol{Z}.$$

Sostituendo nella precedente espressione di X, si ottiene la generica soluzione delle prime tre equazioni

$$X = 202 + 210t_3,\ \forall\, t_3 \in \boldsymbol{Z}.$$

Sostituendo nella quarta,

$$202 + 210t_3 \equiv 5\ (mod\ 11),\ \text{cioè}\ \ t_3 \equiv 1\ (mod\ 11),\ \text{da cui}\ \ t_3 = 1 + 11t_4,\ \exists\, t_4 \in \boldsymbol{Z}.$$

Sostituendo nella precedente espressione di X, si ottiene la generica soluzione del sistema:

$$X = 202 + 210 + 2310\, t_4 = 412 + 2310\, t_4.$$

* * *

2.6. Risolvere il seguente sistema di equazioni congruenziali lineari

$$\begin{cases} 18\,X \equiv 12\ (mod\ 30) \\ 7\,X \equiv 4\ (mod\ 9) \\ 28\,X \equiv 14\ (mod\ 98). \end{cases}$$

Soluzione. Semplificando la prima e la terza equazione, il sistema diventa

$$\begin{cases} 3\,X \equiv 2\ (mod\ 5) \\ 7\,X \equiv 4\ (mod\ 9) \\ 2\,X \equiv 1\ (mod\ 7). \end{cases}$$

Osserviamo che i moduli sono a due a due coprimi e che ciascuna equazione è compatibile. Dunque il sistema è compatibile ed ammette un'unica soluzione $mod\ 315$ [essendo $315 = 5 \cdot 7 \cdot 9$].

Trasformiamo il sistema in un sistema cinese. Osservato che $3 \cdot 2 \equiv 1\ (mod\ 5)$, $7 \cdot 4 \equiv 1\ (mod\ 9)$ e $2 \cdot 4 \equiv 1\ (mod\ 7)$, sistema precedente diventa

$$\begin{cases} 6\,X \equiv 4\ (mod\ 5) \\ 28\,X \equiv 16\ (mod\ 9) \\ 8\,X \equiv 4\ (mod\ 7), \end{cases} \quad \text{cioè} \quad \begin{cases} X \equiv 4\ (mod\ 5) \\ X \equiv 7\ (mod\ 9) \\ X \equiv 4\ (mod\ 7). \end{cases}$$

Risolviamo tale sistema. Dalla prima equazione

$$X = 4 + 5t_1.$$

Inserendo X nella seconda equazione si ottiene

$$4 + 5t_1 \equiv 7\ (mod\ 9),\ \text{cioè}\ \ t_1 \equiv 6\ (mod\ 9)\ \ \text{e quindi}\ \ t_1 = 6 + 9t_2.$$

Sostituendo tale valore nella precedente espressione di X, si ottiene

$$X = 34 + 45\, t_2.$$

Inserendo X nella terza equazione si ottiene

$$34 + 45t_2 \equiv 4\ (mod\ 7),\ \text{cioè}\ \ t_2 \equiv 4\ (mod\ 7)\ \ \text{e quindi}\ \ t_2 = 4 + 7t_3.$$

Sostituendo tale valore nella precedente espressione di X, si ottiene

$$X = 34 + 180 + 315\, t_3 = 214 + 315\, t_3.$$

L'unica soluzione del sistema $(mod\ 315)$ è quindi $X = 214$.

* * *

2.7. Verificare se il seguente sistema di equazioni congruenziali lineari è compatibile:

$$\begin{cases} 2\,X \equiv 8\ (mod\ 9) \\ 2\,X \equiv 6\ (mod\ 15). \end{cases}$$

Soluzione. Ciascuna delle due equazioni è compatibile [infatti $1 = (2,9)|8$ e $1 = (2,17)|6$] ma i moduli non sono coprimi.

Trasformiamo il sistema in un sistema di *tipo cinese*. Poiché $2 \cdot 5 \equiv 1\ (mod\ 9)$ e $2 \cdot 8 \equiv 1\ (mod\ 15)$, il sistema diventa

$$\begin{cases} X \equiv 40\ (mod\ 9) \\ X \equiv 48\ (mod\ 15), \end{cases} \quad \text{cioè} \quad \begin{cases} X \equiv 4\ (mod\ 9) \\ X \equiv 3\ (mod\ 15). \end{cases}$$

Posto $d = (9, 15) = 3$, un noto risultato afferma che tale sistema è compatibile $\iff d \,\big|\, 4 - 3$. Dunque il sistema è incompatibile.

Assumendo invece di non conoscere il precedente risultato, si può eseguire la seguente verifica diretta. Dalla prima equazione, $X = 4 + 9t$. Sostituendo nella seconda, $4 + 9t \equiv 3\ (mod\ 15)$, cioè

$9t \equiv 14\ (mod\ 15)$. Poiché $3 = (9, 15)$ non divide 14, tale equazione è incompatibile e dunque il sistema è incompatibile.

* * *

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.

Soluzione. Innanzitutto semplifichiamo i coefficienti delle singole equazioni; essendo $6425 \equiv 5\ mod\ 12$ e $8614 \equiv 4\ mod\ 7$, il sistema è equivalente al seguente

$$\begin{cases} 5\,X \equiv 7 \ \ mod\ 12 \\ 4\,X \equiv 3 \ \ mod\ 7 \\ 3\,X \equiv a \ \ mod\ 8. \end{cases}$$

Osserviamo poi che $5 \equiv -7\ mod\ 12$ e $4 \equiv -3\ mod\ 7$. Pertanto risulta:

$$\begin{cases} X \equiv -1 \ \ mod\ 12 \\ X \equiv -1 \ \ mod\ 7 \\ 3\,X \equiv a \ \ mod\ 8. \end{cases}$$

Le prime due equazioni hanno allora come soluzione $X = -1 + 84k,\ k \in \boldsymbol{Z}$; sostituendo tale valore nella terza equazione, otteniamo:

$$3(-1 + 84k) \equiv a \ \ mod\ 8 \ \text{ ovvero } \ 4k \equiv a + 3 \ \ mod\ 8.$$

Affinché tale equazione abbia soluzione, deve risultare che $4 = (4, 8) \,|\, a + 3$, cioè $a + 3 = 4t$, da cui

$$a = 4t - 3 \equiv 4t + 5 \begin{cases} \equiv 1\ mod\ 8, \text{ se } t \text{ è dispari} \\ \equiv 5\ mod\ 8, \text{ se } t \text{ è pari.} \end{cases}$$

Nel primo caso la terza equazione diventa $X \equiv 3\ mod\ 8$. Riprendendo la risoluzione del sistema si ottiene $t = 1 + 2h$ e quindi la soluzione generale del sistema è

$$X = -1 + 84(1 + 2h) = 83 + 168\,h.$$

Nel secondo caso la terza equazione diventa $X \equiv 7\ mod\ 8$. Riprendendo la risoluzione del sistema si ottiene $t = 0 + 2h$ e quindi la soluzione generale del sistema è

$$X = -1 + 84(0 + 2h) = -1 + 168\,h.$$

* * *

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.

Soluzione. Risolviamo il sistema formato dalle prime due equazioni

$$\begin{cases} 2X \equiv 5\ (mod\ 7) \\ X \equiv 4\ (mod\ 9), \end{cases} \quad \text{che equivale a} \quad \begin{cases} X \equiv 6\ (mod\ 7) \\ X \equiv 4\ (mod\ 9). \end{cases}$$

Posto $X = 6 + 7s\ (s \in \mathbf{Z})$, allora $6 + 7s \equiv 4\ (mod\ 9)$, cioè $s \equiv 1\ (mod\ 9)$. Dunque $s = 1 + 9t\ (t \in \boldsymbol{Z})$ e pertanto $X = 6 + 7 + 63t$. Il sistema delle prime due equazioni equivale a $X \equiv 13\ (mod\ 63)$.

Il sistema assegnato equivale quindi a

$$\begin{cases} X \equiv 13\ (mod\ 63) \\ 4X \equiv a\ (mod\ 15), \end{cases} \quad \text{che equivale a} \quad \begin{cases} X \equiv 13\ (mod\ 63) \\ X \equiv 4a\ (mod\ 15). \end{cases}$$

Tale sistema è risolubile $\iff$ l'equazione $13 + 63t \equiv 4a\ (mod\ 15)$ è risolubile $\iff$ l'equazione $3t \equiv 4a + 2\ (mod\ 15)$ è risolubile $\iff MCD(3, 15) \,|\, 4a + 2 \iff 3 \,|\, 4a + 2 \iff a \equiv 1\ (mod\ 3)$.

Dunque il sistema assegnato è risolubile $\iff a = 1, 4, 7, 10, 13$.

Sia $a = 1$. Da $3t \equiv 6\ (mod\ 15)$ segue $t \equiv 2\ (mod\ 5)$, cioè $t = 2 + 5s$ e quindi
$$X = 13 + 63(2 + 5s) = 139 + 315\,s,\ \forall\, s \in \boldsymbol{Z}.$$
Sia $a = 4$. Da $3t \equiv 18\ (mod\ 15)$ segue $t \equiv 1\ (mod\ 5)$, cioè $t = 1 + 5s$ e quindi
$$X = 13 + 63(1 + 5s) = 76 + 315\,s,\ \forall\, s \in \boldsymbol{Z}.$$
Sia $a = 7$. Da $3t \equiv 30\ (mod\ 15)$ segue $t \equiv 0\ (mod\ 5)$, cioè $t = 5s$ e quindi
$$X = 13 + 63(5s) = 13 + 315\,s,\ \forall\, s \in \boldsymbol{Z}.$$
Sia $a = 10$. Da $3t \equiv 42\ (mod\, 15)$ segue $t \equiv -1\ (mod\, 5)$, cioè $t = -1 + 5s$ e quindi
$$X = 13 + 63(-1 + 5s) = -50 + 315\,s,\ \forall\, s \in \boldsymbol{Z}.$$
Sia $a = 13$. Da $3t \equiv 54\ (mod\, 15)$ segue $t \equiv -2\ (mod\ 5)$, cioè $t = -2 + 5s$ e quindi
$$X = 13 + 63(-2 + 5s) = -113 + 315\,s,\ \forall\, s \in \boldsymbol{Z}.$$

* * *

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 $a',\, b'$.

Soluzione. (*i*) I moduli delle due equazioni sono coprimi. La seconda equazione è sempre compatibile [infatti $1 = (3, 8)\,\big|\, b,\ \forall\, b \in \boldsymbol{Z}$], mentre la prima equazione è compatibile $\iff (5, a)\,\big|\, 3 \iff a \not\equiv 0\ (mod\ 5)$. Si conclude che
$$\text{il sistema è compatibile} \iff a \not\equiv 0\ (mod\ 5).$$
(*ii*) La seconda equazione equivale a $X \equiv 3b\ (mod\ 8)$, ed ha quindi generica soluzione $X = 3b + 8s,\ \forall\, s \in \boldsymbol{Z}$. Sostituendo nella prima equazione, si ottiene
$$3ab + 8as \equiv\ 3\ (mod\ 5),\ \text{cioè}\ \ 3ab + 3as \equiv\ 3\ (mod\ 5),\ \text{ovvero}\ \ as \equiv\ 1 - ab\ (mod\ 5).$$
Denotato con a' un inverso aritmetico di $a\ \ (mod\ 5)$, tale equazione si trasforma in
$$s \equiv\ (1 - ab)a'\ (mod\ 5),\ \text{da cui}\ \ s = (1 - ab)a' + 5t,\ \ \forall\, t \in \boldsymbol{Z}.$$
Si conclude che $\forall\, a \not\equiv\ 0\ (mod\ 5)$, il sistema ha come generica soluzione
$$X = 3b + 8(1 - ab)a' + 40t,\ \ \forall\, t \in \boldsymbol{Z}.$$

* * *

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?

Soluzione. (*i*) Sia $\overline{x}_{18} = \overline{y}_{18}$. Per dimostrare che f è ben definita, bisogna verificare che $(\overline{x}_6,\, \overline{x}_3) = (\overline{y}_6,\, \overline{y}_3)$, cioè che $\overline{x}_6 = \overline{y}_6$ e $\overline{x}_3 = \overline{y}_3$.

Per ipotesi, $18\,|\, x - y$ e quindi $6\,|\, x - y$ e $3\,|\, x - y$; da ciò segue la tesi.

(*ii*) Si ha:

$f(\overline{0}_{18}) = (\overline{0}_6,\, \overline{0}_3),\ \ f(\overline{1}_{18}) = (\overline{1}_6,\, \overline{1}_3),\ \ f(\overline{2}_{18}) = (\overline{2}_6,\, \overline{2}_3),\ \ f(\overline{3}_{18}) = (\overline{3}_6,\, \overline{0}_3),$
$f(\overline{4}_{18}) = (\overline{4}_6,\, \overline{1}_3),\ \ f(\overline{5}_{18}) = (\overline{5}_6,\, \overline{2}_3),\ \ f(\overline{6}_{18}) = (\overline{0}_6,\, \overline{0}_3),\ \ f(\overline{7}_{18}) = (\overline{1}_6,\, \overline{1}_3),$
$f(\overline{8}_{18}) = (\overline{2}_6,\, \overline{2}_3),\ \ f(\overline{9}_{18}) = (\overline{3}_6,\, \overline{0}_3),\ \ f(\overline{10}_{18}) = (\overline{4}_6,\, \overline{1}_3),\ \ f(\overline{11}_{18}) = (\overline{5}_6,\, \overline{2}_3),$
$f(\overline{12}_{18}) = (\overline{0}_6,\, \overline{0}_3),\ \ f(\overline{13}_{18}) = (\overline{1}_6,\, \overline{1}_3),\ \ f(\overline{14}_{18}) = (\overline{2}_6,\, \overline{2}_3),\ \ f(\overline{15}_{18}) = (\overline{3}_6,\, \overline{0}_3),$
$f(\overline{16}_{18}) = (\overline{4}_6,\, \overline{1}_3),\ \ f(\overline{17}_{18}) = (\overline{5}_6,\, \overline{2}_3).$

Ne segue che

$$Im(f) = \{(\overline{0}_6, \overline{0}_3),\ (\overline{1}_6, \overline{1}_3),\ (\overline{2}_6, \overline{2}_3),\ (\overline{3}_6, \overline{0}_3),\ (\overline{4}_6, \overline{1}_3),\ (\overline{5}_6, \overline{2}_3)\}.$$

Inoltre: $f^{-1}((\overline{0}_6, \overline{0}_3)) = \{\overline{0}_{18}, \overline{6}_{18}, \overline{12}_{18}\}$, $f^{-1}((\overline{1}_6, \overline{2}_3)) = \emptyset$.

(*iii*) g non è ben definita [e quindi non ha senso chiedersi se sia iniettiva]. Infatti $\overline{0}_6 = \overline{6}_6$, ma $g(\overline{0}_6) = \overline{0}_{18} \neq \overline{6}_{18} = g(\overline{6}_6)$.

* * *

2.12. Utilizzando il teorema Cinese del Resto, verificare che le ultime tre cifre di $n = 46^{14}$ sono $6, 5, 6$.

Soluzione. Si tratta di determinare il resto della divisione euclidea di n per 10^3 [cioè di risolvere la congruenza $X \equiv n\ (mod\ 1000)$].

Il teorema Cinese del Resto asserisce che esiste l'isomorfismo

$$F : \boldsymbol{Z}_{1000} \to \boldsymbol{Z}_8 \times \boldsymbol{Z}_{125} \quad \text{tale che} \quad F(\overline{x}_{1000}) = \big(\overline{x}_8, \overline{x}_{125}\big),\ \forall\, \overline{x}_{1000} \in \boldsymbol{Z}_{1000}.$$

Risulta: $n = 46^{14} = (46^2)^7 = 2116^7$ e

$$F(\overline{2116}) = F(\overline{116}) = \big(\overline{116}_8, \overline{116}_{125}\big) = \big(\overline{4}_8, \overline{-9}_{125}\big),$$
$$F(\overline{n}) = F(\overline{2116^7}) = F(\overline{2116}^7) = \big(\overline{4}_8^{\,7}, \overline{-9}_{125}^{\,7}\big).$$

In $\boldsymbol{Z}_8$: $\overline{4}^7 = \overline{4}^2 \cdot \overline{4}^5 = \overline{0} \cdot \overline{4}^5 = \overline{0}$. In $\boldsymbol{Z}_{125}$: $\overline{-9}^7 = \overline{-9} \cdot \overline{81}^3 = \overline{-9} \cdot \overline{81} \cdot \overline{81}^2 = \overline{21} \cdot \overline{81}^2 = \overline{21} \cdot \overline{61} = \overline{31}$.

Dunque $F(\overline{n}) = \big(\overline{4}_8^{\,7}, \overline{-9}_{125}^{\,7}\big) = \big(\overline{0}_8, \overline{31}_{125}\big)$.

Consideriamo il sistema cinese

$$\begin{cases} X \equiv 0\ (mod\ 8) \\ X \equiv 31\ (mod\ 125). \end{cases}$$

Dalla seconda equazione: $X = 31 + 125\,t$. Ne segue:

$31 + 125 \equiv 0\ (mod\ 8)$, cioè $-1 + 5t \equiv 0\ (mod\ 8)$, ovvero $t \equiv 5\ (mod\ 8)$, da cui $t = 5 + 8s$.

Dunque $X = 31 + 125(5 + 8s) = 656 + 1000\,s$. Ne segue:

$$F(\overline{n}) = F(\overline{656}) = \quad \text{e quindi} \quad \overline{n} = \overline{656},$$

cioè $n \equiv 656\ (mod\ 1000)$. Le ultime tre cifre di n sono quindi 6, 5, 6.

* * *

2.13. Determinare, se esiste, il minimo intero $n > 0$ tale che 7123^n abbia come ultima cifra 1.

Soluzione. Basta risolvere l'equazione $7123^n \equiv X\ (mod\ 10)$. Si ha: $7123 \equiv 3\ (mod\ 10)$. Dunque $7123^n \equiv 3^n\ (mod\ 10)$. Risulta:

$$3^1 \equiv 3\ (mod\ 10),\ 3^2 \equiv 9\ (mod\ 10),\ 3^3 \equiv 7\ (mod\ 10),\ 3^4 \equiv 1\ (mod\ 10).$$

Pertanto $n = 4$ è l'esponente richiesto.

* * *

2.14. Considerati i numeri naturali 734^h, $\forall\, h \geq 2$, determinare le possibili ultime due cifre di tali numeri.

Soluzione. Poiché 734 è pari, per ogni $h \geq 2$, 734^h è multiplo di 4 e dunque le sue due ultime cifre vanno cercate tra le seguenti 25:

$$00,\ 04,\ 08,\ 12,\ \ldots\ ,\ 88,\ 92,\ 96.$$

Per ottenere tali cifre, basta risolvere le seguenti equazioni congruenziali:

$$X \equiv 734^h\ (mod\ 100), \quad \text{ovvero} \quad X \equiv 34^h\ (mod\ 100), \quad \forall\, h \geq 2.$$

Dal teorema Cinese del Resto, $F : \boldsymbol{Z}_{100} \to \boldsymbol{Z}_4 \times \boldsymbol{Z}_{25}$ è un isomorfismo. Allora

$$F\big(\overline{734^h}\big) = F\big(\overline{34^h}\big) = F(\overline{34}^{\,h}) = F(\overline{34})^h = \big(\overline{2}, \overline{9}\big)^h = \big(\overline{2}^h, \overline{9}^h\big) \in \boldsymbol{Z}_4 \times \boldsymbol{Z}_{25}.$$

Poiché, in $\boldsymbol{Z}_4$, $\overline{2}^h = \overline{0}$, $\forall\, h \geq 2$, allora $F\big(\overline{734^h}\big) = \big(\overline{0}, \overline{9}^h\big)$, $\forall\, h \geq 2$. Calcoliamo in $\boldsymbol{Z}_{25}$ le potenze $\overline{9}^h$. Si ha:

$\overline{9}^2 = \overline{81} = \overline{6}$, $\overline{9}^3 = \overline{54} = \overline{4}$, $\overline{9}^4 = \overline{36} = \overline{11}$, $\overline{9}^5 = \overline{99} = \overline{24}$, $\overline{9}^6 = \overline{-9} = \overline{16}$, $\overline{9}^7 = \overline{144} = \overline{19}$,
$\overline{9}^8 = \overline{171} = \overline{21}$, $\overline{9}^9 = \overline{189} = \overline{14}$, $\overline{9}^{10} = \overline{126} = \overline{1}$, $\overline{9}^{11} = \overline{9}$, $\overline{9}^{12} = \overline{6} = \overline{9}^2$, ecc.

Dunque

$$\big\{F\big(\overline{734^h}\big),\ \forall\, h \geq 2\big\} = \big\{(\overline{0},\overline{6}),\ (\overline{0},\overline{4}),\ (\overline{0},\overline{11}),\ (\overline{0},\overline{24}),\ (\overline{0},\overline{16}),\ (\overline{0},\overline{19}),\ (\overline{0},\overline{21}),\ (\overline{0},\overline{14}),\ (\overline{0},\overline{1}),\ (\overline{0},\overline{9})\big\}.$$

Si tratta ora di risolvere i dieci sistemi di equazioni congruenziali lineari

$$\begin{cases} X \equiv 0 \ (mod\ 4) \\ X \equiv h \ (mod\ 25), \end{cases}$$

con $h = 6,\ 4,\ 11,\ 24,\ 16,\ 19,\ 21,\ 14,\ 1,\ 9$.

Dalla prima equazione, $X = 4s$ e quindi, sostituendo nella seconda,

$$4s \equiv h \ (mod\ 25), \ \text{cioè} \ \ s \equiv 19\,h \ (mod\ 25).$$

Ne segue $X = 4{\cdot}19\,h = 76\,h$, con $h = 6,\ 4,\ 11,\ 24,\ 16,\ 19,\ 21,\ 14,\ 1,\ 9$. Riducendo *modulo* 100, si ottengono le dieci "ultime due cifre" dei numeri 734^h:

$$56,\ 04,\ 36,\ 24,\ 16,\ 44,\ 96,\ 64,\ 76,\ 84.$$

* * *

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.

Soluzione. (*i*) Risulta: $133^{42} \equiv 33^{42}\ (mod\ 100)$. Essendo $(33, 100) = 1$, il teorema di Eulero-Fermat asserisce che $33^{\varphi(100)} \equiv 1\ (mod\ 100)$. Essendo $\varphi(100) = (4-2)(25-5) = 40$, allora $33^{40} \equiv 1\ (mod\ 100)$. Pertanto

$$33^{42} \equiv 1{\cdot}33^2 = 1089 \equiv 89\ (mod\ 100).$$

Le ultime due cifre di n sono 8, 9.

(*ii*) Bisogna risolvere la congruenza $133^{42} \equiv X\ (mod\ 1000)$.

Si noti che in questo caso il teorema di Eulero-Fermat asserisce che $133^{\varphi(1000)} = 133^{400} \equiv 1\ (mod\ 1000)$, ma tale uguaglianza non ci è di aiuto, dovendo calcolare soltanto 133^{42}. Utilizzeremo invece il teorema Cinese del Resto, che afferma che $F : \boldsymbol{Z}_{1000} \to \boldsymbol{Z}_8 \times \boldsymbol{Z}_{125}$ è un isomorfismo.

Si ha: $F(\overline{133}) = (\overline{5},\ \overline{8}) \in \boldsymbol{Z}_8 \times \boldsymbol{Z}_{125}$ e dunque $F(\overline{133^{42}}) = (\overline{5}^{42},\ \overline{8}^{42})$.

Calcoliamo quindi $\overline{5}^{42}$ in $\boldsymbol{Z}_8$ e $\overline{8}^{42}$ in $\boldsymbol{Z}_{125}$. Si ha: $5^{42} = (5^2)^{21} \equiv 1^{21} \equiv 1\ (mod\ 8)$. Dunque $\overline{5}^{42} = \overline{1} \in \boldsymbol{Z}_8$. Relativamente a $\overline{8}^{42} \in \boldsymbol{Z}_{125}$, osserviamo che $8^{42} = 2^{126}$. Essendo $(2, 125) = 1$, dal teorema di Eulero-Fermat $2^{\varphi(125)} \equiv 1\ (mod\ 125)$, cioè $2^{100} \equiv 1\ (mod\ 125)$. Allora

$$2^{126} \equiv 2^{26} = (2^7)^3{\cdot}2^5 = 128^3{\cdot}32 \equiv 3^3{\cdot}32 = 864 \equiv 114\ (mod\ 125).$$

Dunque $\overline{8}^{42} = \overline{114} \in \boldsymbol{Z}_{125}$ e pertanto $F(\overline{133^{42}}) = (\overline{1},\ \overline{114}) \in \boldsymbol{Z}_8 \times \boldsymbol{Z}_{125}$.

Risolvendo ora il sistema *cinese*

$$\begin{cases} X \equiv 1 \ (mod\ 8) \\ X \equiv 114 \ (mod\ 125), \end{cases}$$

si ottiene come generica soluzione $x = 489 + 1000t,\ \forall\, t \in \boldsymbol{Z}$. Dunque le ultime tre cifre di n sono 4, 8, 9.

* * *

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 $\boldsymbol{Z}_n$.

Soluzione. Si ponga $\boldsymbol{D} = \boldsymbol{Z}_n^{\cdot} - \mathcal{U}(\boldsymbol{Z}_n)$. Poiché $\mathcal{U}(\boldsymbol{Z}_n) = \big\{\overline{k} \in \boldsymbol{Z}_n\ :\ 0 < k < n,\ (k, n) = 1\big\}$, allora

$$\boldsymbol{D} = \big\{\overline{k} \in \boldsymbol{Z}_n\ :\ 0 < k < n,\ (k, n) > 1\big\}.$$

Dobbiamo verificare che ogni $\overline{k} \in \boldsymbol{D}$ è uno zero-divisore di $\boldsymbol{Z}_n$. Essendo $d := (k, n) > 1$, allora

$$k = dk_1, \ \ n = dn_1, \ \text{con} \ \ 0 < n_1 < n.$$

Si ha:

$$kn_1 = (dk_1)n_1 = k_1(dn_1) = k_1 n \equiv 0 \ mod\, n, \ \text{cioè} \ \overline{k}\,\overline{n_1} = \overline{0} \ \text{in} \ \boldsymbol{Z}_n, \ \text{con} \ \overline{n_1} \neq \overline{0}.$$

Perciò $\overline{k}$ è uno zero-divisore in $\boldsymbol{Z}_n$.

* * *

2.17. Utilizzando opportunamente la relazione di congruenza *mod* 3, verificare che esiste un'unica terna di numeri primi della forma

$$(n,\, n-2,\, n-4), \ \text{con} \ n \in \boldsymbol{N}.$$

Soluzione. La terna $(7, 5, 3)$ è una terna di primi del tipo richiesto ed è evidente che per $n \leq 7$ non esistono altre terne di primi di questo tipo. Sia quindi $n \geq 8$. Allora:

- se $n \equiv 0 \ (mod\, 3)$, allora $n = 3t, \ \exists\, t \geq 3$, e quindi n non è primo.

- se $n \equiv 1 \ (mod\, 3)$, allora $n - 4 \equiv 1 - 4 \equiv 0 \ (mod\, 3)$ e quindi $n - 4 = 3t, \ \exists\, t \geq 2$, cioè $n - 4$ non è primo.

- se $n \equiv 2 \ (mod\, 3)$, allora $n - 2 \equiv 2 - 2 \equiv 0 \ (mod\, 3)$ e quindi $n - 2 = 3t, \ \exists\, t \geq 2$, cioè $n - 2$ non è primo.

* * *

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:

$$(a) \ \ Q \ \text{non è primo}; \quad (b) \ \ \exists\, p_k \in A \ \text{tale che} \ p_k \,|\, Q.$$

Soluzione. (a) Poiché $Q \equiv -1 \equiv 3 \ (mod\, 4)$, se per assurdo Q fosse primo, allora $Q = p_k, \ \exists\, k \in A$. Ma allora $p_k = 4P - 1 = 4p_1 \dots p_k \dots p_n - 1$ e dunque $1 = 4p_1 \dots p_k \dots p_n - p_k$, cioè $p_k \,|\, 1$: assurdo.

(b) Da (a) segue che $Q = q_1 \dots q_t$, con $q_1, \dots, q_t$ primi. Essendo Q dispari, i primi q_i sono dispari e dunque congruenti a 1 o 3 $(mod\, 4)$. Se per assurdo ogni $q_i \equiv 1 \ (mod\, 4)$, allora anche $\prod_{i=1}^{t} q_i \equiv 1 \ (mod\, 4)$, mentre $Q \equiv 3 \ (mod\, 4)$. Si conclude che Q ammette almeno un divisore $p_k \in A$.

Da (b), $p_k \,|\, Q$. Allora $4p_1 \dots p_k \dots p_n - 1 = p_k t$, da cui segue che $p_k \,|\, 1$: assurdo.

Nota. Si può anche dimostrare (ma la dimostrazione è meno elementare) che esistono infiniti primi congruenti a 1 *mod* 4.

Segnaliamo infine che vale il seguente risultato molto più forte, dovuto Dirichlet: assegnati due interi coprimi a, b, esistono infiniti primi congruenti a b *mod* a, ciè del tipo $ax + b$.

* * *

Soluzioni degli 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.

Soluzione. Dividiamo F per G. Si ha:

$$\begin{array}{l|l}
X^6+4X^5+2X^4-8X^3-7X^2+4X+4 & X^3+X^2+X+1 \\
\cancel{X^6+X^5+X^4+X^3} & \hline
\cancel{} & X^3+3X^2-2X-10 \\
\not/\ 3X^5+X^4-9X^3-7X^2+4X+4 & \\
\cancel{3X^5+3X^4+3X^3+3X^2} & \\
\not/\ -2X^4-12X^3-10X^2+4X+4 & \\
\cancel{-2X^4-2X^3-2X^2-2X} & \\
\not/\ -10X^3-8X^2+6X+4 & \\
\cancel{-10X^3-10X^2-10X-10} & \\
\not/\ 2X^2+16X+14 &
\end{array}$$

Dunque $F = GQ_1 + R_1$, con $\begin{cases} Q_1 = X^3 + 3X^2 - 2X - 10 \\ R_1 = 2X^2 + 16X + 14. \end{cases}$

Dividiamo G per R_1. Si ha:

$$\begin{array}{l|l}
X^3+X^2+X+1 & 2X^2+16X+14 \\
\cancel{X^3+8X^2+7X} & \hline
\cancel{} & \frac{1}{2}X-\frac{7}{2} \\
\not/\ -7X^2-6X+1 & \\
\cancel{-7X^2-56X-49} & \\
\not/\ 50X+50 &
\end{array}$$

Dunque $G = R_1Q_2 + R_2$, con $\begin{cases} Q_2 = \frac{1}{2}X - \frac{7}{2} \\ R_2 = 50X + 50. \end{cases}$

Dividiamo ora R_1 per R_2. Si ha:

$$\begin{array}{l|l}
2X^2+16X+14 & 50X+50 \\
\cancel{2X^2+2X} & \hline
\cancel{} & \frac{1}{25}X+\frac{7}{25} \\
\not/\ 14X+14 & \\
\cancel{14X+14} & \\
0 &
\end{array}$$

Dunque $R_1 = R_2Q_3 + 0$, con $Q_3 = \frac{1}{25}x + \frac{7}{25}$.

Si conclude che $D := MCD(F, G) \sim R_2 = 50x + 50$ e poiché D deve essere monico, $D = X + 1$.

Calcoliamo ora un'identità di Bézout per F, G. Si ha:

$$[R_2] = [G] - [R_1]Q_2, \quad [R_1] = [F] - [G]Q_1.$$

e quindi

$$[R_2] = [G] - ([F] - [G]Q_1)Q_2 = -[F]Q_2 + [G](1 + Q_1Q_2).$$

Risulta: $1 + Q_1Q_2 = \frac{1}{2}X^4 - 2X^3 - \frac{23}{2}X^2 + 2X + 36$. Ne segue:

$$50X + 50 = (-\tfrac{1}{2}X + \tfrac{7}{2})\,F + (\tfrac{1}{2}X^4 - 2X^3 - \tfrac{23}{2}X^2 + 2X + 36)\,G.$$

L'identità di Bézout richiesta è quindi:

$$X+1=\tfrac{1}{50}(-\tfrac{1}{2}X+\tfrac{7}{2})\,F+\tfrac{1}{50}(\tfrac{1}{2}X^4-2X^3-\tfrac{23}{2}X^2+2X+36)\,G.$$

* * *

3.2. Dei due polinomi F e G dell'esercizio precedente (pensati in $\boldsymbol{Z}[X]$), calcolare gli zeri razionali con le relative molteplicità.

Soluzione. Sia $\alpha=\frac{r}{s}\in\boldsymbol{Q}$, con $(r,s)=1$. Se α è uno zero di F, allora $r\big|4$ e $s\big|1$. Dunque

$$\begin{cases} r=\pm1,\,\pm2,\,\pm4 \\ s=\pm1 \end{cases} \quad \text{e quindi } \alpha=\pm1,\,\pm2,\,\pm4.$$

Si verifica subito che $F(1)=F(-1)=F(-2)=0$, mentre $F(2),\,F(4),\,F(-4)\neq0$. Dunque $X-1$, $X+1$, $X+2$ sono divisori di F. Pertanto

$$f=(X-1)(X+1)(X+2)F_1=(X^3+2X^2-X-2)F_1,$$

per un opportuno polinomio F_1 di grado 3.

Per valutare la molteplicità dei tre zeri, è necessario determinare F_1. Si ha:

$$\begin{array}{l|l}
X^6+4X^5+2X^4-8X^3-7X^2+4X+4 & X^3+2X^2-X-2 \\
\cline{2-2}
X^6+2X^5-X^4-2X^3 & X^3+2X^2-X-2 \\
\cline{1-1}
\quad 2X^5+3X^4-6X^3-7X^2+4X+4 & \\
\quad 2X^5+4X^4-2X^3-4X^2 & \\
\cline{1-1}
\quad -X^4-4X^3-3X^2+4X+4 & \\
\quad -X^4-2X^3+X^2+2X & \\
\cline{1-1}
\quad -2X^3-4X^2+2X+4 & \\
\quad -2X^3-4X^2+2X+4 & \\
\cline{1-1}
\quad 0 &
\end{array}$$

Dunque $F_1=X^3+2X^2-X-2$ e quindi

$$F=(X^3+2X^2-X-2)^2=(X-1)^2(X+1)^2(X+2)^2.$$

Si conclude che F ammette tre zeri razionali, tutti di molteplicità 2.

Veniamo ora al polinomio G. Se $\alpha=\frac{r}{s}$, è uno zero razionale di G, deve risultare che $r\big|1$ e $s\big|1$. Dunque $\alpha=\pm1$. Si ha: $G(1)\neq0$, mentre $G(-1)=0$. Dunque -1 è l'unico zero razionale di G. Valutiamone la moltiplicità. Si ha: $G=(X+1)(X^2+1)$. Poiché X^2+1 non ha zeri razionali (e neppure reali), allora G ha come unico zero razionale $\alpha=1$, con molteplicità 1.

* * *

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 $\boldsymbol{Z}_6[X]$?

Soluzione. (*i*) Risulta, in $\boldsymbol{Z}_7[X]$: $F=G\,(\overline{6}X^3+\overline{6}X)+\overline{5}X$. Infatti

$$\begin{array}{l|l}
\overline{2}X^5+X^3+\overline{4}X & \overline{5}X^2+\overline{1} \\
\cline{2-2}
\overline{30}X^5+\overline{6}X^3 & \overline{6}X^3+\overline{6}X \\
\cline{1-1}
\cancel{-\overline{28}X^5}+\overline{2}X^3+\overline{4}X & \\
\quad \overline{30}X^3+\overline{6}X & \\
\cline{1-1}
\quad \cancel{-\overline{28}X^3}+\overline{5}X &
\end{array}$$

[Si noti ad esempio che il primo addendo del quoziente è $\overline{2}\cdot\overline{5}^{-1}X^{5-2}=\overline{2}\cdot\overline{3}\,X^3=\overline{6}\,X^3$, ecc.].

(*ii*) $\boldsymbol{Z}_6$ non è un campo. Tuttavia il polinomio divisore G ha coefficiente direttore invertibile in $\boldsymbol{Z}_6$. In quest'ipotesi la divisione euclidea di F per G può essere ugualmente eseguita e si ottiene:

$$F = G\,(\overline{4}X^3 + \overline{3}X) + X.$$

Infatti:

$$\begin{array}{r|l} \overline{2}X^5 + X^3 + \overline{4}X & \overline{5}X^2 + \overline{1} \\ \cline{2-2} \overline{20}X^5 + \overline{4}X^3 & \overline{4}X^3 + \overline{3}X \\ \cline{1-1} -\cancel{\overline{18}X^5} + \overline{3}X^3 + \overline{4}X & \\ \overline{15}X^3 + \overline{3}X & \\ \cline{1-1} -\cancel{\overline{12}X^3} + X & \end{array}$$

* * *

3.4. (*i*) Determinare un'identità di Bézout per i due polinomi

$$F = X^4 + X^2 + \overline{1},\ \ G = X^3 + X + \overline{1} \in \boldsymbol{Z}_2[X].$$

(*ii*) Determinare un'identità di Bézout per gli stessi polinomi pensati in $\boldsymbol{Z}_3[X]$.

Soluzione. (*i*) Si procede con l'algoritmo euclideo delle divisioni successive. Utilizzando la divisione con resto, si ottiene:

$$F = G\,X + (X + \overline{1}),$$
$$G = (X + \overline{1})\,(X^2 + X) + \overline{1}.$$

Dunque $MCD(F, G) = \overline{1}$. Risulta [tenendo conto che $-\overline{1} = \overline{1}$]:

$$\overline{1} = G + (F + G\,X)(X^2 + X) = F(X^2 + X) + G(\overline{1} + X(X^2 + X)).$$

Un'identità di Bézout è quindi:

$$\overline{1} = (X^2 + X)\,F + (X^3 + X^2 + \overline{1})\,G.$$

(*ii*) Con l'algoritmo euclideo delle divisioni successive si ottiene:

$$F = G\,X + (\overline{1} + \overline{2}X),$$
$$G = (\overline{1} + \overline{2}X)\,(\overline{2}X^2 + \overline{2}X + \overline{1}) + \overline{0}.$$

Dunque $MCD(F, G) = \overline{1} + \overline{2}X$ e pertanto un'identità di Bézout è

$$\overline{1} + \overline{2}X = F + \overline{2}X\,G.$$

* * *

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 $\varphi_{|_{\boldsymbol{Z}}} = \mathbf{1}_{\boldsymbol{Z}}$.

(*ii*) Verificare che il polinomio $\varphi(X)$ ha grado 1.

(*iii*) Dedurre da (*ii*) che φ fissa il grado dei polinomi, cioè $\partial\big(\varphi(P)\big) = \partial P,\ \forall\, P \in \boldsymbol{Z}[X]$.

Soluzione. (*i*) Ovviamente $\varphi(0) = 0$. Poiché φ è unitario [cfr. **Eserc. I.27**], allora $\varphi(1) = 1$. Ne segue, $\forall\, n \geq 1,\ \varphi(n) = \varphi(1+1+\ ...\ +1) = n\,\varphi(1) = n$; inoltre, $\varphi(-n) = -\varphi(n) = -n$. Dunque $\varphi(n) = n,\ \forall\, n \in \boldsymbol{Z}$.

(*ii*) Poiché $\varphi(X) \notin \boldsymbol{Z}$, allora $s := \partial(\varphi(X)) \geq 1$ e bisogna verificare che $s = 1$. Per ogni $P = \sum_{i=0}^{n} a_i X^i \in \boldsymbol{Z}[X]$, con $n = \partial P \geq 1$, risulta:

$$\varphi(P) = \sum_{i=0}^{n} a_i\,\varphi(X)^i \ \text{ e } \ \partial\big(\varphi(P)\big) = \partial\big(a_n\varphi(X)^n\big) = ns \geq s.$$

Se per assurdo fosse $s > 1$, allora $\partial(\varphi(P)) \geq 2$. Dunque $Im(\varphi)$ non conterrebbe polinomi di grado 1. Invece $Im(\varphi) = \boldsymbol{Z}[X]$: assurdo.

(*iii*) Sia $P = \sum_{i=0}^{n} a_i X^i \in \boldsymbol{Z}[X]$, con $n = \partial P$. Allora $\partial\big(\varphi(P)\big) = \partial\big(a_n\varphi(X)^n\big) = n = \partial(P)$.

* * *

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.

Soluzione. Se $\partial F = 1$, F ammette un'unica radice reale con molteplicità 1.

Sia $n := \partial F \geq 3$. Il polinomio F, pensato in $\boldsymbol{C}[X]$ ammette n zeri, contati con la rispettiva molteplicità. Valutiamo il numero degli zeri non reali di F.

Se $\alpha \in \boldsymbol{C} - \boldsymbol{R}$ e $F(\alpha) = 0$, allora $\overline{\alpha} \neq \alpha$ e $F(\overline{\alpha}) = \overline{F(\alpha)} = \overline{0} = 0$. Dunque $\overline{\alpha}$ è un altro zero non reale di F. Se poi α ha una data molteplicità, $\overline{\alpha}$ ha la stessa molteplicità. Infatti:

$$(X-\alpha)^i \,\big|\, F \implies F = (X-\alpha)^i G,\ \exists\, G \in \boldsymbol{C}[X] \implies \overline{F} = F = (X-\overline{\alpha})^i\, \overline{G} \implies (X-\overline{\alpha})^i \,\big|\, F;$$

analogamente si verifica che $(X-\overline{\alpha})^i \,\big|\, F \implies (X-\alpha)^i \,\big|\, F$.

Si conclude che il numero degli zeri complessi non reali di F [contati con la rispettiva molteplicità] è pari. Essendo $n = \partial F$ dispari, si conclude che il numero degli zeri reali di F [contati con la rispettiva molteplicità] è dispari, in quanto differenza di un dispari meno un pari.

* * *

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 $\frac{dF}{dX}$.

Soluzione. (*i*) Le prime due verifiche sono semplicissime (e lasciate al lettore). Dimostriamo la terza proprietà (nota come "*regola di Leibnitz*"). Posto $F = \sum_{i=0}^{n} a_i X^i$, $G = \sum_{j=0}^{m} b_j X^j$, allora

$$\tfrac{dF}{dX} = \sum_{i=1}^{n} i a_i X^{i-1} = \sum_{j=0}^{n-1} (j+1) a_{j+1} X^j,\quad \tfrac{dG}{dX} = \sum_{h=0}^{m-1} (h+1) b_{h+1} X^h.$$

Dalla definizione di prodotto di polinomi,

$$\tfrac{d(FG)}{dX} = \tfrac{d}{dX}\Big(\sum_{k=0}^{n+m} c_k X^k\Big) = \sum_{k=0}^{n+m-1} (k+1) c_{k+1} X^k,\ \text{ con }\ c_{k+1} = \sum_{h=0}^{k+1} a_h\, b_{k-h+1}.$$

Inoltre:

$$G\cdot\tfrac{dF}{dX} = \sum_{k=0}^{n+m-1} c'_k X^k,\ \text{con }\ c'_k = \sum_{h=0}^{k} (h+1) a_{h+1} b_{k-h}$$

$$F\cdot\tfrac{dG}{dX} = \sum_{k=0}^{n+m-1} c''_k X^k,\ \text{con }\ c''_k = \sum_{h=0}^{k} (k-h+1) a_h b_{k-h+1}.$$

Bisogna verificare che $(k+1)c_{k+1} = c'_k + c''_k$, $\forall\, k = 0, \ldots, n+m-1$. Infatti:

$$\begin{aligned} c'_k + c''_k &= \big[(k+1)a_0 b_{k+1} + 1\cdot a_1 b_k\big] + \big[k\, a_1 b_k + 2\cdot a_2 b_{k-1}\big] + \big[(k-1)a_2 b_{k-1} + 3\cdot a_3 b_{k-2}\big] + \\ &\quad + \ \ldots\ + \big[1\cdot a_k\, b_1 + (k+1) a_{k+1}\, b_0\big] = \\ &= (k+1)\big(a_0 b_{k+1} + \ \ldots\ + a_{k+1}\, b_0\big) = (k+1)c_{k+1}. \end{aligned}$$

(*ii*) Dal teorema di Ruffini, $X - \alpha \,\big|\, F$ e quindi $F = (X-\alpha)G$, $\exists\, G \in \boldsymbol{C}[X]$.

($\implies$). Se α è uno zero multiplo di F, $F = (X-\alpha)^t H$, con $t \geq 2$ e $H \in \boldsymbol{C}[X]$. Allora, dalla regola di Leibnitz,

$$\tfrac{dF}{dX} = t(X-\alpha)^{t-1} H + (X-\alpha)^t\, \tfrac{dH}{dX}$$

e quindi $\frac{dF}{dX}(\alpha) = 0 + 0 = 0$.

($\impliedby$). Sia $\frac{dF}{dX}(\alpha) = 0$. Poiché, sempre per la regola di Leibnitz, $\frac{dF}{dX} = (X-\alpha)\frac{dG}{dX} + G$, allora

$$0 = \tfrac{dF}{dX}(\alpha) = 0 + G(\alpha),\ \text{cioè}\ \ G(\alpha) = 0,\ \text{ovvero}\ \ X - \alpha \,\big|\, G.$$

Ne segue che $F = (X-\alpha)G = (X-\alpha)^2 H,\ \exists\, H \in \boldsymbol{C}[X]$. Quindi α ha almeno molteplicità 2 per F.

Nota. Poiché il teorema di Ruffini e la regola di Leibnitz valgono se A è un dominio d'integrità, nell'equivalenza appena dimostrata si può assumere che $F \in A[X]$, con A dominio d'integrità, e che α sia uno zero di F in un opportuno dominio d'integrità B contenente A.

* * *

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 $0 \le \partial A < \partial G$ e $0 \le \partial B < \partial F$.

Soluzione. ($\Longrightarrow$). Per ipotesi $D = MCD(F,G)$ ha grado ≥ 1. Se $F = DF_1$ e $G = DG_1$, allora $0 \le \partial F_1 < \partial F$ e $0 \le \partial G_1 < \partial G$. Si ha:

$$F_1 G = F_1 D G_1 = F G_1.$$

Dunque $A = G_1$ e $B = F_1$ sono i polinomi cercati.

($\Longleftarrow$). Sia $D = MCD(F,G)$ e $H = mcm(F,G)$. Bisogna dimostrare che $\partial D \ge 1$.

È noto che $DH = FG$ e dunque $\partial D + \partial H = \partial F + \partial G$. Poniamo $M := AF = BG$. Poiché $\begin{matrix} F \\ G \end{matrix} \Big| M$, allora $H \,\big|\, M$ e dunque

$$\partial H = \partial F + \partial G - \partial D \le \partial M.$$

Poiché $\partial M = \partial A + \partial F < \partial F + \partial G$, allora

$$\partial F + \partial G - \partial D < \partial F + \partial G,$$

cioè $\partial D > 0$, come richiesto.

* * *

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 $n, m \ge 1$. Sia V il K-spazio vettoriale dei polinomi in $K[X]$ aventi grado $\le n+m-1$, 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:

$$F,\ XF,\ X^2F,\ \ldots,\ X^{m-1}F,\ G,\ XG,\ X^2G,\ \ldots,\ X^{n-1}G$$

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:

$$F, G \text{ hanno un fattore comune (non costante)} \iff Ris(F,G) = 0.$$

Soluzione. In base all'esercizio precedente, F, G hanno un fattore comune (non costante) $\iff$

$\exists\, A, B \in K[X]$ tali che $AF = BG$, con $0 \le \partial A < \partial G$ e $0 \le \partial B < \partial F \iff$

$\exists\, a_0, \ldots a_{m-1}, b_0, \ldots b_{n-1} \in K$ (non tutti nulli), tali che $\big(\sum_{i=0}^{m-1} a_i X^i\big)F = \big(\sum_{j=0}^{n-1} b_j X^j\big)G \iff$

$\exists\, a_0, \dots a_{m-1}, b_0, \dots b_{n-1} \in K$ (non tutti nulli), tali che $\sum_{i=0}^{m-1} a_i (X^i F) - \sum_{j=0}^{n-1} b_j (X^j G) = 0 \iff$
i vettori $F, XF, \dots, X^{m-1}F, G, XG, \dots, X^{n-1}G$ sono linearmente dipendenti $\iff$
$Ris(F,G) = 0$.

Nota. Si osservi che se $\sum_{i=0}^{m-1} a_i X^i F + \sum_{j=0}^{n-1} b_j X^j G = 0$ è una relazione di dipendenza linere tra i polinomi $F, \dots, X^{m-1}F, G, \dots, X^{n-1}G$, non può risultare $a_0 = \dots = a_{m-1} = 0$ [ovvero $b_0 = \dots = b_{n-1} = 0$]; altrimenti G [ovvero F] sarebbe uno zero-divisore in $K[X]$.

* * *

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.

Soluzione. Risulta:
$$T(F) = F(X-1) = (X-1)^3 + X(X-1)^2 + (X-1) + 1 = X^3 - 2X^2 + 2X = X(X^2 - 2X + 2).$$
Poiché $T(F)$ è riducibile, anche F lo è. Per ottenerne una fattorizzazione, applicheremo T^{-1} a $T(F)$. Poiché $T^{-1}(P(X)) = P(X+1),\ \forall\, P(X) \in K[X]$, si ha:
$$F = T^{-1}(T(F)) = T^{-1}(X(X^2 - 2X + 2)) = (X+1)\big((X+1)^2 - 2(X+1) + 2\big) = (X+1)(X^2+1).$$
La fattorizzazione richiesta è quindi [come del resto si poteva verificare direttamente]
$$F = (X+1)(X^2+1).$$

* * *

3.11. Verificare che il polinomio $X^4 + \overline{1} \in \boldsymbol{Z}_3[X]$ è riducibile e scriverne una fattorizzazione.

Soluzione. Risulta, posto $f = X^4 + \overline{1} \in \boldsymbol{Z}_3[X]$:
$$f(\overline{0}) \neq \overline{0},\ f(\overline{1}) \neq \overline{0},\ f(\overline{2}) \neq \overline{0}.$$
Dunque f non ha fattori di grado 1.

Essendo $\overline{1} = \overline{1} \cdot \overline{1} = \overline{2} \cdot \overline{2}$, f potrebbe ammettere una delle seguenti fattorizzazioni:
$$f = (X^2 + aX + \overline{1})(X^2 + bX + \overline{1}) \text{ oppure } f = (X^2 + aX + \overline{2})(X^2 + bX + \overline{2}).$$

Nel primo caso si ottiene il sistema
$$\begin{cases} a + b = \overline{0} \\ \overline{2} + ab = \overline{0} \\ a + b = \overline{0}, \end{cases} \quad \text{da cui} \quad \begin{cases} b = -a = \overline{2}a \\ \overline{2} + \overline{2}a = \overline{0} \end{cases}$$
e quindi $\overline{1} + a^2 = \overline{0}$, da cui $a^2 = \overline{2}$. Una tale equazione non ha soluzioni in $\boldsymbol{Z}_3$. Dunque il sistema è incompatibile.

Nel secondo caso si ottiene il sistema
$$\begin{cases} a + b = \overline{0} \\ \overline{1} + ab = \overline{0} \\ \overline{2}(a+b) = \overline{0}, \end{cases} \quad \text{da cui} \quad \begin{cases} b = \overline{2}a \\ ab = \overline{2} \end{cases}$$
e quindi $\overline{2}a^2 = \overline{2}$, da cui $a^2 = \overline{1}$. Pertanto $a = \overline{1}, \overline{2}$. Il sistema ha quindi soluzioni $(a,b) = (\overline{1}, \overline{2})$ oppure $(a,b) = (\overline{2}, \overline{1})$. Ne segue che
$$f = (X^2 + X + \overline{2})(X^2 + \overline{2}X + \overline{2}) \text{ in } \boldsymbol{Z}_3[X].$$

* * *

3.12. Verificare che il polinomio $X^4 + 1 \in \boldsymbol{Z}[X]$ è irriducibile.

Soluzione. $f = X^4 + 1 \in \boldsymbol{Z}[X]$ non ha zeri in $\boldsymbol{Q}$ [infatti $\alpha^4 + 1 > 0,\ \forall\, \alpha \in \boldsymbol{Q}$]. Un'eventuale fattorizzazione di f è del tipo

$$f = (X^2 + aX + 1)(X^2 + bX + 1) \quad \text{oppure} \quad f = (X^2 + aX - 1)(X^2 + bX - 1).$$

Nel primo caso si ottiene il sistema

$$\begin{cases} a + b = 0 \\ 2 + ab = 0 \\ a + b = 0, \end{cases} \quad \text{da cui} \quad \begin{cases} b = -a \\ 2 - a^2 = 0. \end{cases}$$

Dall'ultima equazione, $a^2 = 2$ e quindi non esistono soluzioni in $\boldsymbol{Z}$.

Nel secondo caso si ottiene il sistema

$$\begin{cases} a + b = 0 \\ -2 + ab = 0 \\ -(a + b) = 0, \end{cases} \quad \text{da cui} \quad \begin{cases} b = -a \\ -2 - a^2 = 0. \end{cases}$$

Dall'ultima equazione, $a^2 = -2$ e quindi non esistono soluzioni in $\boldsymbol{Z}$.

Si conclude che f è irriducibile in $\boldsymbol{Z}[X]$.

* * *

3.13. Fattorizzare il polinomio $X^6 - X^4 - X^2 + 1 \in \boldsymbol{Z}[X]$.

Soluzione. Risulta:

$$X^6 - X^4 - X^2 + 1 = X^6 - X^2 - (X^4 - 1) = X^2(X^4 - 1) - (X^4 - 1) = (X^2 - 1)(X^4 - 1) =$$
$$= (X^2 + 1)(X^2 - 1)^2 = (X^2 + 1)(X - 1)^2 (X + 1)^2.$$

* * *

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.

Soluzione. Sia $f = X^4 - X^3 + X^2 - X + 1 \in \boldsymbol{Z}[X]$. Si opera su f con la sostituzione lineare $\varphi : \boldsymbol{Z}[X] \to \boldsymbol{Z}[X]$ tale che $\varphi(X) = X - 1$. Si ottiene:

$$\varphi(f) = (X - 1)^4 - (X - 1)^3 + (X - 1)^2 - (X - 1) + 1 = \ldots = X^4 - 5X^3 + 10X^2 - 10X + 5.$$

Posto $p = 5$, sono verificate le condizioni di Eisenstein. Dunque f 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.

Soluzione. Posto $f = X^4 - 3X^3 + 3X^2 - 3X + 9 \in \boldsymbol{Z}[X]$, si osserva subito che non si può applicare il criterio di Eisenstein [l'unico primo possibile sarebbe $p = 3$, ma $p^2 \,|\, 9$]. Operiamo con verifica diretta modulo 2. Considerata la riduzione di f

$$\overline{f} = X^4 + X^3 + X^2 + X + \overline{1} \in \boldsymbol{Z}_2[X],$$

risulta $\overline{f}(\overline{0}), \overline{f}(\overline{1}) \neq \overline{0}$. Dunque $\overline{f}$ non ha fattori di grado 1. Poniamo

$$\overline{f} = (X^2 + aX + \overline{1})(X^2 + bX + \overline{1}).$$

Si ottiene il sistema

$$\begin{cases} a + b = \overline{1} \\ \overline{0} + ab = \overline{1} \\ b + a = \overline{1}, \end{cases} \quad \text{da cui} \quad \begin{cases} a + b = \overline{1} \\ ab = \overline{1}. \end{cases}$$

Da $ab = \overline{1}$ segue $a = b = \overline{1}$ e quindi $a + b = \overline{1} + \overline{1} = \overline{1}$: assurdo.

Il sistema è incompatibile e quindi $\overline{f}$ è irriducibile in $\boldsymbol{Z}_2[X]$. Allora f è irriducibile in $\boldsymbol{Z}[X]$.

* * *

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.

Soluzione. (*i*) Essendo f monico, f è irriducibile su $\boldsymbol{Q} \iff$ lo è su $\boldsymbol{Z}$. Verifichiamo quindi se f è irriducibile in $\boldsymbol{Z}[X]$.

Verifichiamo se f ha zeri razionali: sia $q = \frac{r}{s} \in \boldsymbol{Q}$, con $(r,s) = 1$. Se q è uno zero di f, $r \big| -1$ e $s \big| 1$. Dunque $q = \pm 1$. Ma $f(1), f(-1) \neq 0$. Dunque f non ha zeri razionali e pertanto non ha fattori di grado 1 (in $\boldsymbol{Q}[X]$).

f potrebbe ammettere una fattorizzazione con polinomi di grado 2 (irriducibili) in $\boldsymbol{Q}[X]$. Possiamo assumere tali polinomi monici. Dunque

$$f = (X^2 + aX + b)(X^2 + cX + d), \text{ con } a, b, c, d \in \boldsymbol{Z}.$$

Essendo $bd = -1$, si può assumere $b = 1$, $d = -1$. Dunque

$$f = (X^2 + aX + 1)(X^2 + cX - 1) = X^4 + (a + c)X^3 + ac\,X^2 + (c - a)X - 1.$$

Ne segue il sistema

$$\begin{cases} a + c = 3 \\ ac = 2 \\ c - a = 1. \end{cases}$$

Tale sistema ammette l'unica soluzione $a = 1$, $c = 2$. Dunque

$$f = (X^2 + X + 1)(X^2 + 2X - 1) \quad \text{[fattorizzazione in } \boldsymbol{Q}[X]\text{]}.$$

(*ii*) Risulta: $X^2 + X + 1$ è irriducibile in $\boldsymbol{R}[X]$ [infatti $\Delta = 1 - 4 < 0$]. Invece $X^2 + 2X - 1 = (X + 1 - \sqrt{2})(X + 1 + \sqrt{2}) \in \boldsymbol{R}[X]$. Pertanto

$$f = (X^2 + X + 1)(X + 1 - \sqrt{2})(X + 1 + \sqrt{2}) \quad \text{[fattorizzazione in } \boldsymbol{R}[X]\text{]}.$$

(*iii*) In $\boldsymbol{C}[X]$, $X^2 + X + 1 = (X + \frac{1}{2} - \frac{\sqrt{3}}{2}i)(X + \frac{1}{2} + \frac{\sqrt{3}}{2}i)$. Dunque

$$f = (X + \tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i)(X + \tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i)(X + 1 - \sqrt{2})(X + 1 + \sqrt{2}) \quad \text{[fattorizzazione in } \boldsymbol{C}[X]\text{]}.$$

(*iv*) Tramite l'omomorfismo $\boldsymbol{Z}[X] \to \boldsymbol{Z}_3[X]$, il polinomio f si trasforma in

$$\overline{f} = (X^2 + X + \overline{1})(X^2 + \overline{2}X + \overline{2}).$$

Si ha: $X^2 + X + \overline{1} = (X + \overline{2})^2$, mentre $X^2 + \overline{2}X + \overline{2}$ è irriducibile [in quanto non ha zeri in $\boldsymbol{Z}_3$]. Dunque

$$\overline{f} = (X + \overline{2})^2(X^2 + \overline{2}X + \overline{2}) \quad \text{[fattorizzazione in } \boldsymbol{Z}_3[X]\text{]}.$$

* * *

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 $\boldsymbol{Z}_3[X]/_{(f)}$.

Soluzione. (*i*) Risulta:

$$f(\overline{0}) = \overline{1} \neq \overline{0}, \quad f(\overline{1}) = \overline{1} \neq \overline{0}, \quad f(\overline{2}) = \overline{37} = \overline{1} \neq \overline{0}.$$

Dunque f non ammette in $\boldsymbol{Z}_3[X]$ fattori di grado 1.

Verifichiamo se f ammette una fattorizzazione con un polinomio di grado 3 ed uno di grado 2. Tali polinomi possono essere scelti monici (come f). Poiché il prodotto dei rispettivi termini noti è $\overline{1}$, e poiché in $\boldsymbol{Z}_3$ risulta: $\overline{1} = \overline{1} \cdot \overline{1} = \overline{2} \cdot \overline{2}$ (mentre $\overline{a} \cdot \overline{b} \neq \overline{1}$, se $\overline{a} \neq \overline{b}$), possono presentarsi a priori due diverse fattorizzazioni:

$$(a) \quad f = (X^3 + aX^2 + bX + \overline{1})(X^2 + cX + \overline{1}),$$
$$(b) \quad f = (X^3 + aX^2 + bX + \overline{2})(X^2 + cX + \overline{2}).$$

Caso (a). Risulta:

$$f = X^5 + (a + c)X^4 + (\overline{1} + b + ac)X^3 + (\overline{1} + a + bc)X^2 + (b + c)X + \overline{1}.$$

Ne segue il sistema

$$\begin{cases} a+c=\overline{0} \\ \overline{1}+b+ac=\overline{0} \\ \overline{1}+a+bc=\overline{0} \\ b+c=\overline{2}, \end{cases} \quad \text{e quindi} \quad \begin{cases} a=\overline{2}c \\ b=\overline{2}+\overline{2}c \\ \overline{1}+\overline{2}+\overline{2}c+\overline{2}c^2=\overline{0} \\ \overline{1}+\overline{2}c+\overline{2}c+\overline{2}c^2=\overline{0}. \end{cases}$$

Dalle ultime due equazioni, $\begin{cases} \overline{2}(c+c^2)=\overline{0} \\ \overline{1}+\overline{2}c+\overline{0}=\overline{0}, \end{cases}$ da cui $\begin{cases} c+c^2=\overline{0} \\ \overline{2}c=\overline{2} \end{cases}$ e quindi $\begin{cases} c=\overline{1} \\ \overline{1}+\overline{1}^2=\overline{0}. \end{cases}$

Ciò è assurdo. Dunque una fattorizzazione di tipo (a) non è possibile.

Caso (b). Risulta:

$$f=X^5+(a+c)X^4+(\overline{2}+b+ac)X^3+(\overline{2}+\overline{2}a+bc)X^2+\overline{2}(b+c)X+\overline{1}.$$

Quindi

$$\begin{cases} a+c=\overline{0} \\ \overline{2}+b+ac=\overline{0} \\ \overline{2}+\overline{2}a+bc=\overline{0} \\ \overline{2}(b+c)=\overline{2}, \end{cases} \quad \text{da cui} \quad \begin{cases} b=\overline{1}+\overline{2}c \\ a=\overline{2}c \\ \overline{2}+\overline{1}+\overline{2}c+\overline{2}c^2=\overline{0} \\ \overline{2}+c+c+\overline{2}c^2=\overline{0}, \end{cases}$$

Dalle ultime due equazioni, $\begin{cases} \overline{2}(c+c^2)=\overline{0} \\ \overline{2}+\overline{0}=\overline{0}, \end{cases}$ che è palesemente assurdo. Si conclude che f è irriducibile in $\boldsymbol{Z}_3[X]$.

(ii) Risulta:

$$\boldsymbol{Z}_3[X]/_{(f)}=\boldsymbol{Z}_3[\alpha \,|\, \alpha^5=2+\alpha]=\{a+b\alpha+c\alpha^2+d\alpha^3+e\alpha^4,\ \forall\, a,b,c,d\in\boldsymbol{Z}_3 \text{ (e con } \alpha^5=2+\alpha)\}.$$

Sia $(\alpha^3)^{-1}=a+b\alpha+c\alpha^2+c\alpha^3+d\alpha^4$. Allora:

$$\begin{aligned} \overline{1} &= (a+b\alpha+c\alpha^2+d\alpha^3+e\alpha^4)\alpha^3= \\ &= a\alpha^3+b\alpha^4+c(\overline{2}+\alpha)+d\alpha(\overline{2}+\alpha)+e\alpha^2(\overline{2}+\alpha)= \\ &= \overline{2}c+(c+\overline{2}d)\alpha+(d+\overline{2}e)\alpha^2+(a+e)\alpha^3+b\alpha^4. \end{aligned}$$

Quindi:

$$\overline{2}c=\overline{1},\ c+\overline{2}d=\overline{0},\ d+\overline{2}e=\overline{0},\ a+e=\overline{0},\ b=\overline{0},$$

da cui

$$c=\overline{2},\ d=\overline{2},\ e=\overline{2},\ a=\overline{1},\ b=\overline{0}.$$

Pertanto $(\alpha^3)^{-1}=\overline{1}+\overline{2}X^2+\overline{2}X^3+\overline{2}X^4$.

* * *

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).

Soluzione. (i) Verifichiamo se f ammette zeri razionali. Posto $q=\frac{r}{s}\in\boldsymbol{Q}$, con $MCD(r,s)=1$, se $f(q)=0$, allora $r\,|\,2$ e $s\,|\,1$, cioè $r=\pm1,\pm2$ e $s=\pm1$. Ne segue che $q=\pm1,\pm2$. Ma si osserva subito che $f(1)$, $f(-1)$, $f(2)$, $f(-2)\neq0$. Dunque f non ammette zeri e quindi non ammette fattori di grado 1.

Assumiamo ora che f sia prodotto di due polinomi di grado 2 (entrambi monici). Poiché il termine noto di tale prodotto è 2, possono sussistere due casi:

(a) $f=(X^2+aX-1)(X^2+bX-2)$, con $a,b\in\boldsymbol{Q}$,

(b) $f=(X^2+aX+1)(X^2+bX+2)$, con $a,b\in\boldsymbol{Q}$.

Caso (a). Risulta:

$$f=(X^2+aX-1)(X^2+bX-2)=X^4+(a+b)X^3+(ab-3)X^2+(-b-2a)X+2$$

e quindi

$$\{a+b=-1,\ ab-3=3,\ -b-2a=-1.$$

Dalla prima e terza equazione: $a = 2, b = -3$; ma tali valori non soddisfano la seconda equazione. Dunque il sistema è incompatibile e la supposta fattorizzazione non esiste.

Caso (b). Risulta:

$$f = (X^2 + aX + 1)(X^2 + bX + 2) = X^4 + (a+b)X^3 + (ab+3)X^2 + (b+2a)X + 2$$

e quindi

$$\{a + b = -1,\ ab + 3 = 3,\ b + 2a = -1.$$

Tale sistema ammette (un'unica) soluzione $\{a = 0,\ b = -1$. Dunque

$$f = (X^2 + 1)(X^2 - X + 2).$$

(ii) Denotata con $x\ [= \overline{X}]$ la classe di $X\ mod\, f$, risulta:

$$\boldsymbol{Q}[X]/_{(f)} = \{a + bx + cx^2 + dx^3,\ \forall\, a, b, c, d \in \boldsymbol{Q}\}.$$

[con $x^4 = x^3 - 3x^2 + x - 2$]. Posto $x^{-1} = a + bx + cx^2 + dx^3$, si ha:

$$1 = x(a + bx + cx^2 + dx^3) = -2d + (a+d)x + (b-3d)x^2 + (c+d)x^3.$$

Dunque

$$\{-2d = 1,\ a + d = 0,\ b - 3d = 0,\ c + d = 0,$$

da cui:

$$\{d = -\tfrac{1}{2},\ a = \tfrac{1}{2},\ b = -\tfrac{3}{2},\ c = \tfrac{1}{2}.,$$

Pertanto $x^{-1} = \frac{1}{2}(1 - 3x + x^2 - x^3)$.

(iii) Poiché $\overline{f} = \overline{0} = (x^2+1)(x^2 - x + 2)$, allora $x^2 + 1$ e $x^2 - x + 2$ sono due zero-divisori non nulli dell'anello $\boldsymbol{Q}[X]/_{(f)}$.

(iv) Per assurdo, sia $ax + b$ uno zero-divisore non nullo dell'anello $\boldsymbol{Q}[X]/_{(f)}$. Allora esiste $\overline{g} \neq \overline{0}$ tale che $\overline{g}(ax + b) = \overline{0}$. Dunque $f \,|\, (aX + b)g$, cioè $(aX + b)g = fh$ [con $h \in \boldsymbol{Q}[X]$] e quindi $(aX + b) \,|\, fh$.

Ora, poiché $MCD(aX + b, f) = 1$ [in quanto f non ha fattori di grado 1], dal lemma di Euclide segue che $aX + b \,|\, h$, cioè $h = (aX + b)l$ [con $l \in \boldsymbol{Q}[X]$]. Segue che $(aX + b)g = f(aX + b)l$ e quindi $g = fl$, cioè $\overline{g} = \overline{0}$: assurdo.

* * *

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 $\boldsymbol{Z}_5[X]/_{(f_a)}$.

Soluzione. (i) Sia $a = \overline{0}$. Allora $f_{\overline{0}} = X^3 + \overline{2}X = X(X^2 + \overline{2})$. Il polinomio $g = X^2 + \overline{2} \in \boldsymbol{Z}_5[X]$ è irriducibile [in quanto si verifica che $g(a) \neq \overline{0}$, $\forall\, a \in \mathbf{Z}_5$]. Dunque $f_{\overline{0}} = X(X^2 + \overline{2})$ è la fattorizzazione richiesta.

Sia $a = \overline{1}$. Allora $f_{\overline{1}} = X^3 + \overline{2}X + \overline{1}$. Se $f_{\overline{1}}$ fosse riducibile, ammetterebbe uno zero in $\boldsymbol{Z}_5$. Ma si ha:

$$f_{\overline{1}}(\overline{0}) = \overline{1},\ f_{\overline{1}}(\overline{1}) = \overline{4},\ f_{\overline{1}}(\overline{2}) = \overline{3},\ f_{\overline{1}}(\overline{3}) = \overline{4},\ f_{\overline{1}}(\overline{4}) = \overline{3},$$

e dunque $f_{\overline{1}}$ è irriducibile.

Sia $a = \overline{2}$. Allora $f_{\overline{2}} = X^3 + \overline{2}X + \overline{2}$. Risulta:

$$f_{\overline{2}}(\overline{1}) = \overline{5} = \overline{0},\ f_{\overline{2}}(\overline{3}) = \overline{35} = \overline{0}$$

e dunque $(X - \overline{1})(X - \overline{3}) = (X + \overline{4})(X + \overline{2}) = X^2 + X + \overline{3}$ è un divisore di $f_{\overline{2}}$. Dividendo $f_{\overline{2}}$ per $X^2 + X + \overline{3}$, si ottiene $f_{\overline{2}} = (X^2 + X + \overline{3})(X + \overline{4})$. Si conclude che $f_{\overline{2}} = (X + \overline{4})^2(X + \overline{2})$ è la fattorizzazione richiesta.

Sia $a = \overline{3}$. Allora $f_{\overline{3}} = X^3 + \overline{2}X + \overline{3}$. Risulta:

$$f_{\overline{3}}(\overline{2}) = \overline{15} = \overline{0},\ f_{\overline{3}}(\overline{4}) = \overline{75} = \overline{0}$$

e dunque $(X - \overline{2})(X - \overline{4}) = (X + \overline{3})(X + \overline{1}) = X^2 + \overline{4}X + \overline{3}$ è un divisore di $f_{\overline{3}}$. Dividendo $f_{\overline{3}}$ per $X^2 + \overline{4}X + \overline{3}$, si ottiene $f_{\overline{3}} = (X^2 + \overline{4}X + \overline{3})(X + \overline{1})$. Si conclude che $f_{\overline{3}} = (X + \overline{1})^2(X + \overline{3})$ è la fattorizzazione richiesta.

Sia infine $a = \overline{4}$. Allora $f_{\overline{4}} = X^3 + \overline{2}X + \overline{4}$. Si ha:

$$f_{\overline{4}}(\overline{0}) = \overline{4},\ f_{\overline{4}}(\overline{1}) = \overline{2},\ f_{\overline{4}}(\overline{2}) = \overline{1},\ f_{\overline{4}}(\overline{3}) = \overline{2},\ f_{\overline{4}}(\overline{4}) = \overline{1},$$

e dunque $f_{\overline{4}}$ è irriducibile.

(*ii*) Scegliamo il primo polinomio irriducibile precedentemente ottenuto: $f_{\overline{1}} = X^3+\overline{2}X+\overline{1}$. Denotata con x la classe di X $mod\, f_{\overline{1}}$, risulta:

$$\boldsymbol{Z}_5[X]/_{(f_{\overline{1}})} = \big\{a + bx + cx^2,\ \forall\, a, b, c \in \boldsymbol{Z}_5,\ \text{con } x^3 = -\overline{1} - \overline{2}x = \overline{4} + \overline{3}x\big\}.$$

Sia $x^{-1} = a + bx + cx^2$. Si ha:

$$\overline{1} = (a + bx + cx^2)x = ax + bx^2 + c(\overline{4} + \overline{3}x) = \overline{4}c + (a + \overline{3}c)x + bx^2.$$

Ne segue: $\big\{\overline{4}c = \overline{1},\ a + \overline{3}c = \overline{0},\ b = \overline{0},$ da cui $\big\{c = \overline{4},\ a = \overline{3},\ b = \overline{0}$. Pertanto $x^{-1} = \overline{3} + \overline{4}x^2$.

Si noti che anche $f_{\overline{4}} = X^3 + \overline{2}X + \overline{4}$ è irriducibile. Procedendo in modo analogo si ottiene $x^{-1} = \overline{2} + \overline{x}^2$.

* * *

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 $n \le x$].

(*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.

Soluzione. (*i*) Tenuto conto che il termine noto di un polinomio f è $f(0)$, risulta:

$f\,\rho\,f$. Infatti $[f(0)] = [f(0)]$.

$f\,\rho\,g \Longrightarrow g\,\rho\,f$. Infatti $[f(0)] = [g(0)] \Longrightarrow [g(0)] = [f(0)]$.

$f\,\rho\,g$ e $g\,\rho\,h \Longrightarrow f\,\rho\,h$. Infatti $[f(0)] = [g(0)] = [h(0)] \Longrightarrow [f(0)] = [h(0)]$.

(*ii*) Risulta: $\big[\frac{1}{2} + X\big]_{\rho} = \big[\frac{1}{2}\big]_{\rho} = \big[0\big]_{\rho} = \big[X + X^2\big]_{\rho} = \big\{f \in \mathbf{Q}[X] :\ 0 \le f(0) < 1\big\}$.

(*iii*) Sia $\varphi : \boldsymbol{Q}[X] \to \boldsymbol{Z}$ l'applicazione così definita:

$$\varphi(f) = [f(0)],\ \forall\, f \in \boldsymbol{Q}[X].$$

Ovviamente φ è suriettiva [infatti $\varphi(a) = a,\ \forall\, a \in \boldsymbol{Z}$].

Inoltre $\varphi(f) = \varphi(g) \iff [f(0)] = [g(0)] \iff f\,\rho\,g$. Dunque la relazione ρ_φ indotta da φ coincide con ρ. Ne segue che l'applicazione

$$\varphi^* : \boldsymbol{Q}[X]/_{\rho} \to \boldsymbol{Z},\ \text{tale che } [f]_\rho \to \varphi(f) = [f(0)],$$

è una biiezione.

* * *

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.

Soluzione. (*i*) Si verifica subito che, $\forall\, a \in \boldsymbol{Z}_3$, $f(a) \neq \overline{0}$, $g(a) \neq \overline{0}$. Dunque f, g sono irriducibili in $\boldsymbol{Z}_3[X]$.

(*ii*) Risulta, posto $t = X + (f)$:

$$\boldsymbol{Z}_3[X]/(f) = \big\{a + bt,\ \forall\, a, b \in \boldsymbol{Z}_3,\ \text{con } t^2 + \overline{1} = \overline{0}\big\} = \boldsymbol{Z}_3[t \,|\, t^2 = \overline{2}] =$$
$$= \big\{\overline{0},\ \overline{1},\ \overline{2},\ t,\ \overline{1} + t,\ \overline{2} + t,\ \overline{2}t,\ \overline{1} + \overline{2}t,\ \overline{2} + \overline{2}t,\ \text{con } t^2 = \overline{2}\big\}.$$

Analogamente, posto $s = X + (g)$:

$$\boldsymbol{Z}_3[X]/(g) = \{a+bs,\ \forall\, a,b\in\boldsymbol{Z}_3,\ \text{con } s^2+\overline{2}s+\overline{2}=\overline{0}\} = \boldsymbol{Z}_3[s\,|\,s^2=\overline{1}+s] =$$
$$= \{\overline{0},\ \overline{1},\ \overline{2},\ s,\ \overline{1}+s,\ \overline{2}+s,\ \overline{2}s,\ \overline{1}+\overline{2}s,\ \overline{2}+\overline{2}s,\ \text{con } s^2=s+\overline{1}\}.$$

La tavola moltiplicativa di quest'ultimo campo è la seguente:

$\cdot$	$\overline{1}$	$\overline{2}$	s	$\overline{1}+s$	$\overline{2}+s$	$\overline{2}s$	$\overline{1}+\overline{2}s$	$\overline{2}+\overline{2}s$
$\overline{1}$	$\overline{1}$	$\overline{2}$	s	$\overline{1}+s$	$\overline{2}+s$	$\overline{2}s$	$\overline{1}+\overline{2}s$	$\overline{2}+\overline{2}s$
$\overline{2}$	$\overline{2}$	$\overline{1}$	$\overline{2}s$	$\overline{2}+\overline{2}s$	$\overline{1}+\overline{2}s$	s	$\overline{2}+s$	$\overline{1}+s$
s	$\overline{s}$	$\overline{2}s$	$\overline{1}+s$	$\overline{1}+\overline{2}s$	$\overline{1}$	$\overline{2}+\overline{2}s$	$\overline{2}$	$\overline{2}+s$
$\overline{1}+s$	$\overline{1}+s$	$\overline{2}+\overline{2}s$	$\overline{1}+\overline{2}s$	$\overline{2}$	s	$\overline{2}+s$	$\overline{2}s$	$\overline{1}$
$\overline{2}+s$	$\overline{2}+s$	$\overline{1}+\overline{2}s$	$\overline{1}$	s	$\overline{2}+\overline{2}s$	$\overline{2}$	$\overline{1}+s$	$\overline{2}s$
$\overline{2}s$	$\overline{2}s$	s	$\overline{2}+\overline{2}s$	$\overline{2}+s$	$\overline{2}$	$\overline{1}+s$	$\overline{1}$	$\overline{1}+\overline{2}s$
$\overline{1}+\overline{2}s$	$\overline{1}+\overline{2}s$	$\overline{2}+s$	$\overline{2}$	$\overline{2}s$	$\overline{1}+s$	$\overline{1}$	$\overline{2}+\overline{2}s$	s
$\overline{2}+\overline{2}s$	$\overline{2}+\overline{2}s$	$\overline{1}+s$	$\overline{2}+s$	$\overline{1}$	$\overline{2}s$	$\overline{1}+\overline{2}s$	s	$\overline{2}$

Un eventuale isomorfismo

$$\varphi : \boldsymbol{Z}_3[t\,|\,t^2=\overline{2}] \to \boldsymbol{Z}_3[s\,|\,s^2=\overline{1}+s]$$

è completamente individuato se è assegnato $\varphi(t)$. Se $\varphi(t)=a+bs$, da $t^2=\overline{2}$ segue che $(a+bs)^2=\overline{2}$. Esaminando la tavola moltiplicativa scritta sopra, segue che gli elementi il cui quadrato è $\overline{2}$ sono $\overline{1}+s$ e $\overline{2}+\overline{2}s$. Poniamo ad esempio $\varphi(t)=\overline{1}+s$. Allora

$$\varphi(a+bt) = a+b(1+s) = (a+b)+bs$$

Tale applicazione è biiettiva [con inversa $\psi : c+ds \to c+d(\overline{2}+t)$] ed è un omomorfismo per definizione. Ne segue che φ è un isomorfismo tra i due campi.

* * *

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 $\boldsymbol{Z}_5[X]/(f)$.

Soluzione. (*i*) Si scriva f come prodotto di due polinomi di grado 3. Indicati con α,β i rispettivi termini noti, deve risultare $\alpha\cdot\beta=\overline{1}$. In $\boldsymbol{Z}_5$, $\overline{1}=\overline{1}\cdot\overline{1}=\overline{2}\cdot\overline{3}=\overline{4}\cdot\overline{4}$. Esistono quindi tre possibili coppie di termini noti: $(\alpha,\beta)=(\overline{1},\overline{1})$, $(\overline{2},\overline{3})$, $(\overline{4},\overline{4})$. Cominciamo con $(\alpha,\beta)=(\overline{1},\overline{1})$. Poniamo:

$$f = (X^3+aX^2+bX+\overline{1})(X^3+cX^2+dX+\overline{1}).$$

Risulta: $f = X^6+(a+c)X^5+(b+d+ac)X^4+(\overline{2}+bc+ad)X^3+(a+c+bd)X^2+(b+d)X+1$. Ne segue il sistema

$$\begin{cases} a+c=\overline{1} \\ b+d+ac=\overline{1} \\ \overline{2}+bc+ad=\overline{3} \\ a+c+bd=\overline{1} \\ b+d=\overline{1} \end{cases} \quad \text{e quindi} \quad \begin{cases} a+c=\overline{1} \\ b+d=\overline{1} \\ ac=\overline{0} \\ bd=\overline{0} \\ bc+ad=\overline{1}. \end{cases}$$

Se $a=\overline{0}$, segue: $d=\overline{0}$, $b=\overline{1}$, $c=\overline{1}$ e quindi

$$f = (X^3+X+\overline{1})(X^3+X^2+\overline{1}).$$

Per concludere che si tratta della fattorizzazione richiesta, basta osservare che i due polinomi $g=X^3+X+\overline{1}$ ed $h=X^3+X^2+\overline{1}$ sono irriducibili. Infatti $g(\overline{t})\neq\overline{0}$, $h(\overline{t})\neq\overline{0}$, $\forall\,\overline{t}\in\boldsymbol{Z}_5$.

(*ii*) Posto $x=X+(f)$, l'anello $\boldsymbol{Z}_5[X]/(f)$ è formato da tutti e soli i polinomi

$$a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+a_5x^5,\quad \forall\, a_0,\ldots,a_5\in\boldsymbol{Z}_5,$$

con la condizione: $x^6=-x^5-x^4-\overline{3}x^3-x^2-x-\overline{1}$.

Tale anello ha 5^6 elementi. Inoltre non è integro: infatti $\overline{g}\cdot\overline{h}=\overline{0}$, con $\overline{g},\overline{h}\neq\overline{0}$.

(*iii*) Risulta: $\big(\overline{f - X - \overline{1}}\big)^4 = \big(\overline{f} - x - \overline{1}\big)^4 = \big(\overline{0} - x - \overline{1}\big)^4 = (x + \overline{1})^4 = x^4 + \overline{4}x^3 + \overline{6}x^2 + \overline{4}x + \overline{1} = x^4 + \overline{4}x^3 + x^2 + \overline{4}x + \overline{1}$.

* * *

3.23. [*Esame 1/7/03*] (*i*) Stabilire, motivando la risposta, quali tra i seguenti anelli sono campi e quali non lo sono.

$$K_1 = \boldsymbol{Q}[X]\big/_{(X^4+X^3+X^2+X+1)}, \quad K_2 = \boldsymbol{Z}_2[X]\big/_{(X^3+X^2+X+\overline{1})},$$
$$K_3 = \boldsymbol{C}[X]\big/_{(X^4-2\pi X^2+\pi^2+4)}, \quad K_4 = \boldsymbol{Z}_7[X]\big/_{(X^3+\overline{4})}.$$

(*ii*) Stabilire inoltre quali tra tali anelli contengono divisori dello zero e, in questo caso, indicarne esplicitamente una coppia.

Soluzione. (*i*) K_1 è un campo in quanto $X^4 + X^3 + X^2 + X + 1 =$ è un polinomio irriducibile.

K_2 non è un campo in quanto $X^3 + X^2 + X + \overline{1} = (X + \overline{1})^3 \in \boldsymbol{Z}_2[X]$.

K_3 ovviamente non è un campo in quanto non esistono in $\boldsymbol{C}[X]$ polinomi irriducibili di grado > 1.

K_4 è un campo in quanto $X^3 + \overline{4}$ non ha zeri in $\boldsymbol{Z}_7$ [come facilmente si verifica] ed, essendo di grado 3, è quindi irriducibile.

(*ii*) Per ottenere un divisore dello zero di K_2 basta considerare una fattorizzazione non banale di $f = X^3 + X^2 + X + \overline{1} \in \boldsymbol{Z}_2[X]$, ad esempio $f = (X + \overline{1})(X + \overline{1})^2 = (X + \overline{1})(X^2 + \overline{1})$. Dunque $[X + \overline{1}]$ e $[X^2 + \overline{1}]$ sono divisori dello zero di K_2.

Per K_3 basta osservare che

$$X^4 - 2\pi X^2 + \pi^2 + 4 = \big(X^2 - (\pi + 2i)\big)\big(X^2 - (\pi - 2i)\big)$$

e quindi $[X^2 - (\pi + 2i)]$, $[X^2 - (\pi - 2i)]$ sono divisori dello zero di K_4.

* * *

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 $K = \boldsymbol{Z}_5[X]\big/_{(f)}$ e determinare gli eventuali elementi di K che non sono quadrati (in K).

(*iii*) Determinare una fattorizzazione non banale del polinomio $X^2 - \overline{2}\alpha \in K[X]$.

Soluzione. (*i*) Risulta: $f(a) \neq \overline{0}$, $\forall\, a \in \boldsymbol{Z}_5$. Ne segue che f è irriducibile in $\boldsymbol{Z}_5[X]$ (in quanto di grado 2).

(*ii*) K è formato dai seguenti 25 elementi:

$$\begin{array}{ccccc}
\overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\
\alpha & \overline{1}+\alpha & \overline{2}+\alpha & \overline{3}+\alpha & \overline{4}+\alpha \\
\overline{2}\alpha & \overline{1}+\overline{2}\alpha & \overline{2}+\overline{2}\alpha & \overline{3}+\overline{2}\alpha & \overline{4}+\overline{2}\alpha \\
\overline{3}\alpha & \overline{1}+\overline{3}\alpha & \overline{2}+\overline{3}\alpha & \overline{3}+\overline{3}\alpha & \overline{4}+\overline{3}\alpha \\
\overline{4}\alpha & \overline{1}+\overline{4}\alpha & \overline{2}+\overline{4}\alpha & \overline{3}+\overline{4}\alpha & \overline{4}+\overline{4}\alpha
\end{array}$$

[avendo posto $\alpha = X + (f)$]. Gli elementi di K soddisfano alla condizione: $\alpha^2 = -\alpha - \overline{1} = \overline{4}\alpha + \overline{4}$.

La tavola dei corrispondenti quadrati è la seguente:

$$\begin{array}{ccccc}
\overline{0} & \overline{1} & \overline{4} & \overline{4} & \overline{1} \\
\overline{4}+\overline{4}\alpha & \alpha & \overline{3}+\overline{3}\alpha & \overline{3} & \overline{2}\alpha \\
\overline{1}+\alpha & \overline{2} & \overline{4}\alpha & \overline{3}\alpha & \overline{2}+\overline{2}\alpha\,. \\
\overline{1}+\alpha & \overline{2}+\overline{2}\alpha & \overline{3}\alpha & \overline{4}\alpha & \overline{2} \\
\overline{4}+\overline{4}\alpha & \overline{2}\alpha & \overline{3} & \overline{3}+\overline{3}\alpha & \alpha
\end{array}$$

Da tale lista mancano 12 elementi di K, che sono i non quadrati cercati:

$$\overline{2}+\alpha,\ \overline{3}+\alpha,\ \overline{4}+\alpha,\ \overline{1}+\overline{2}\alpha,\ \overline{3}+\overline{2}\alpha,\ \overline{4}+\overline{2}\alpha,$$
$$\overline{1}+\overline{3}\alpha,\ \overline{2}+\overline{3}\alpha,\ \overline{4}+\overline{3}\alpha,\ \overline{1}+\overline{4}\alpha,\ \overline{2}+\overline{4}\alpha,\ \overline{3}+\overline{4}\alpha.$$

(*ii*) Dalla tavola dei quadrati si evince che $\overline{2}\alpha$ è un quadrato e, più precisamente che è il quadrato dei due elementi $\overline{4}+\alpha$ e $\overline{1}+\overline{4}\alpha$. Ne segue che il polinomio $X^2-\overline{2}\alpha \in K[X]$ ammette come fattori i due polinomi di grado 1:

$$X-(\overline{4}+\alpha) \quad \text{e} \quad X-(\overline{1}+\overline{4}\alpha).$$

* * *

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.

Soluzione. Si ponga $P=X^3-X^2-X+1$. Essendo $P=(X+1)(X-1)^2$, l'elemento $[X^3+X^2]$ è un divisore dello zero, in quanto

$$[X^3+X^2][(X-1)^2]=[X^2][X+1][(X-1)^2]=[X^2][P]=[X^2][0]=[0].$$

L'elemento $[X+2]$ è invece invertibile in quanto è relativamente primo con P. Eseguendo la divisione con resto, si ottiene

$$P=(X+2)(X^2-3X+5)-9,$$

da cui

$$[X+2]^{-1}=\left[\tfrac{1}{9}X^2-\tfrac{1}{3}X+\tfrac{5}{9}\right].$$

Verifica:

$(X+2)(\frac{1}{9}X^2-\frac{1}{3}X+\frac{5}{9})=\frac{1}{9}X^3-\frac{1}{9}X^2-\frac{1}{9}X+\frac{1}{9}+1=\frac{1}{9}\,P+1\equiv 1\ (mod\ P)$.

* * *

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.

Soluzione. Poiché risulta, in $\boldsymbol{Z}_5[X]$:

$$X^3+\overline{2}X+\overline{2}=(X^2+X+\overline{3})(X-\overline{1}),$$

si ha che A non è un campo e che $[X^2+X+\overline{3}]\cdot[X-\overline{1}]=[\overline{0}]$.

Relativamente all'anello B, si verifica subito che è un campo [infatti il polinomio $X^3+\overline{3}X+\overline{2}\in \boldsymbol{Z}_5[X]$ è irriducibile (in quanto non ha zeri in $\boldsymbol{Z}_5$)]. La classe $[X^2+X+\overline{3}]\in B$ è quindi invertibile.

Per calcolarne l'inverso, applichiamo l'algoritmo euclideo delle divisioni successive, alla ricerca del MCD tra $X^3+\overline{3}X+\overline{2}$ e $X^2+X+\overline{3}$ in $\boldsymbol{Z}_5[X]$. Si ha:

$$\begin{aligned} X^3+\overline{3}X+\overline{2}&=(X^2+X+\overline{3})(X-\overline{1})+X\\ X^2+X+\overline{3}&=X(X-\overline{1})+\overline{3}\end{aligned}$$

Ne segue: $\overline{3}=(X^2+X+\overline{3})(X^2)-(X+\overline{1})(X^3+\overline{3}X+\overline{2})$.
Allora, in B: $[\overline{3}]=[X^2+X+\overline{3}]\cdot[X^2]$ e dunque

$$[\overline{1}]=[\overline{3}\cdot\overline{2}]=[X^2+X+\overline{3}]\cdot[\overline{2}X^2],$$

cioè $[X^2+X+\overline{3}]^{-1}=[\overline{2}X^2]$.

* * *

3.27. Assegnato il polinomio $f=X^5+\overline{1}\in\boldsymbol{Z}_7[X]$, determinarne una fattorizzazione come prodotto di polinomi irriducibili (in $\boldsymbol{Z}_7[X]$).

Soluzione. Verifichiamo se esiste $\overline{a}\in\boldsymbol{Z}_7$ tale che $f(\overline{a})=\overline{0}$, cioè se il polinomio f ammette un fattore di grado 1.

Se un tale elemento $\overline{a}$ esiste, risulta $a^5+1\equiv 0\ (mod\ 7)$. Certamente $\overline{a}\neq\overline{0}$ e dunque $(a,7)=1$. Dal Piccolo Teorema di Fermat, $a^6\equiv 1\ (mod\ 7)$ e quindi

$$1\equiv a^6=a^5\cdot a\equiv -a\ (mod\ 7),\ \text{cioè}\ \ a\equiv 6\ (mod\ 7).$$

Verifichiamo allora che $f(\overline{6})=\overline{0}$. Infatti:

$$6^5=2^5 3^5=32\cdot 27\cdot 9\equiv 4\cdot 6\cdot 2\equiv 6\equiv -1\ (mod\ 7).$$

Abbiamo così ottenuto che $X-\overline{6}=X+\overline{1}\,|\,f$. Eseguendo la divisione con resto di f per $X+\overline{1}$, si ottiene

$$f=X^5+\overline{1}=(X+\overline{1})(X^4+\overline{6}X^3+X^2+\overline{6}X+\overline{1}).$$

Consideriamo il polinomio

$$g=X^4+\overline{6}X^3+X^2+\overline{6}X+\overline{1}\in \boldsymbol{Z}_7[X].$$

Dividendo g per $X+\overline{1}$, si ottiene resto $\overline{5}$ (in $\boldsymbol{Z}_7$). Dunque $X+\overline{1}$ non divide g e quindi g non ha fattori di grado 1. Tuttavia g potrebbe essere prodotto di due polinomi irriducibili di grado 2 in $\boldsymbol{Z}_7[X]$ (entrambi monici), cioè

$$(*)\qquad g=(X^2+aX+b)(X^2+cX+d).$$

Alla ricerca di eventuali fattorizzazioni di g, studiamo la compatibilità del sistema (a valori in $\boldsymbol{Z}_7$) ottenuto uguagliando i coefficienti di ugual grado in $(*)$.

Essendo $bd=\overline{1}$ (in $\boldsymbol{Z}_7$), si hanno per (b,d) le seguenti quattro possibilità:

$$(\overline{1},\overline{1}),\quad (\overline{2},\overline{4}),\quad (\overline{3},\overline{5}),\quad (\overline{6},\overline{6}).$$

(i) $b=d=\overline{1}$. In tal caso $(*)$ si trasforma nel sistema

$$\begin{cases} a+c=\overline{6}\\ \overline{1}+ac+\overline{1}=\overline{1}\\ a+c=\overline{6}, \end{cases}\quad\text{cioè}\quad \begin{cases} a+c=\overline{6}\\ ac=\overline{6}. \end{cases}$$

Ne segue $c=\overline{6}+\overline{6}a$ e quindi $\overline{6}a^2+\overline{6}a=\overline{6}$, cioè $a^2+a=\overline{1}$. Ma il polinomio $X^2+X-\overline{1}\in\boldsymbol{Z}_7[X]$ non ha zeri (come facilmente si verifica) e dunque il sistema è incompatibile.

(ii) $b=\overline{2}$, $d=\overline{4}$. In tal caso $(*)$ si trasforma nel sistema

$$\begin{cases} a+c=\overline{6}\\ \overline{2}+ac+\overline{4}=\overline{1}\\ \overline{4}a+\overline{2}c=\overline{6}. \end{cases}$$

Dalla terza e prima equazione, $\overline{2}a+\overline{12}=\overline{6}$, cioè $a=\overline{4}$ e quindi $c=\overline{2}$. Sostituendo nella seconda equazione si ottiene un assurdo. Anche in tal caso il sistema è incompatibile.

(iii) $b=\overline{3}$, $d=\overline{5}$. In tal caso $(*)$ si trasforma nel sistema

$$\begin{cases} a+c=\overline{6}\\ \overline{3}+ac+\overline{5}=\overline{1}\\ \overline{5}a+\overline{3}c=\overline{6}. \end{cases}$$

Dalla seconda equazione, $ac=\overline{0}$; dalla terza e prima equazione, $\overline{2}a+\overline{18}=\overline{6}$, cioè $a=\overline{2}$ e quindi $c=\overline{4}$. Ma allora $ac\neq\overline{0}$: assurdo.

(iv) $b=\overline{6}$, $d=\overline{6}$. In tal caso $(*)$ si trasforma nel sistema

$$\begin{cases} a+c=\overline{6}\\ \overline{6}+ac+\overline{6}=\overline{1}\\ \overline{6}a+\overline{6}c=\overline{6}. \end{cases}$$

Dalla prima e terza equazione, $\overline{6}=\overline{36}$: assurdo.

Si conclude che g è irriducibile (in $\boldsymbol{Z}_7[X]$) e dunque la fattorizzazione di f cercata è la seguente:

$$X^5+1=(X+\overline{1})(X^4+\overline{6}X^3+X^2+\overline{6}X+\overline{1})\in\boldsymbol{Z}_7[X].$$

* * *

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 $\boldsymbol{Z}[i]$.

Soluzione. (*i*) Sia $z = a + ib \in \boldsymbol{Z}[i]$. Si ha: $z \in \mathcal{U}(\boldsymbol{Z}[i]) \iff \frac{1}{z} \in \boldsymbol{Z}[i] \iff \frac{\overline{z}}{z\overline{z}} \in \boldsymbol{Z}[i] \iff a^2 + b^2 = 1 \iff a = \pm 1,\ b = 0$ oppure $a = 0,\ b = \pm 1 \iff z = \pm 1, \pm i$. Dunque

$$\mathcal{U}(\boldsymbol{Z}[i]) = \{\pm 1,\ \pm i\}.$$

Il gruppo delle radici complesse quarte dell'unità è $\langle \zeta_4 \rangle$, con

$$\zeta_4 = \cos\tfrac{2\pi}{4} + i\sin\tfrac{2\pi}{4} = \cos\tfrac{\pi}{2} + i\sin\tfrac{\pi}{2} = i.$$

Dunque $\langle \zeta_4 \rangle = \langle i \rangle = \{1,\ i,\ -1,\ -i\}$. Pertanto $\mathcal{U}(\boldsymbol{Z}[i]) = \langle \zeta_4 \rangle$.

(*ii*) Sia $\mathcal{N}(z) = p$ un numero primo. Se z non fosse irriducibile, allora $z = z_1 z_2$, con $z_1,\ z_2$ non invertibili [cioè con $\mathcal{N}(z_1), \mathcal{N}(z_2) \neq 1$]. Dunque $p = \mathcal{N}(z) = \mathcal{N}(z_1)\mathcal{N}(z_2)$. Pertanto p non sarebbe primo.

(*iii*) Per assurdo, sia $z = 3$ riducibile. Allora $3 = z_1 z_2$, con $\mathcal{N}(z_1), \mathcal{N}(z_2) \neq 1$. Ne segue che $9 = \mathcal{N}(z_1)\mathcal{N}(z_2)$ e quindi $\mathcal{N}(z_1) = \mathcal{N}(z_2) = 3$. Se ad esempio $z_1 = a + ib$, allora $3 = \mathcal{N}(z) = a^2 + b^2$. Ma $\nexists\, a, b \in \boldsymbol{Z}$ tali che $a^2 + b^2 = 3$.

(*iv*) Sia $z = 5$. Allora $\mathcal{N}(z) = 25$. Assumiamo che z ammetta fattorizzazione non banale $z = z_1 z_2$. Allora $\mathcal{N}(z_1) = \mathcal{N}(z_2) = 5$. Se $z_1 = a + ib$, allora $5 = a^2 + b^2$ e quindi $a = \pm 2,\ b = \pm 1$ oppure $a = \pm 1,\ b = \pm 2$. Si ponga ad esempio

$$z_1 = 1 + 2i, \quad z_2 = 1 - 2i.$$

Si ottiene $z_1 z_2 = 5$. $z_1,\ z_2$ sono irriducibili (perché hanno norma prima). Dunque $5 = (1+2i)(1-2i)$ è la fattorizzazione cercata.

Si noti che risulta anche $5 = (2 - i)(2 + i)$. Si tratta essenzialmente della stessa fattorizzazione. Infatti $1 + 2i \sim 2 - i$ e $1 - 2i \sim 2 + i$.

* * *

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.

Soluzione. (*i*) Si esegua la divisione con resto di z per w. Poiché

$$\tfrac{z}{w} = \tfrac{z\,\overline{w}}{\mathcal{N}(w)} = \tfrac{(4+2i)(3+i)}{10} = 1 + i,$$

allora $q = 1 + i,\ r = 0$ e quindi $z = wq = (3 - i)(1 + i)$. Si conclude che $MCD(z, w) = w = 3 - i$.

(*ii*) È noto che ogni intero di Gauss a norma prima è irriducibile e che gli elementi invertibili di $\boldsymbol{Z}[i]$ sono tutti e soli gli interi di Gauss a norma 1 [cioè $\pm 1, \pm i$].

Da (*i*), $z = (3 - i)(1 + i)$. Poiché $\mathcal{N}(1 + i) = 2,\ 1 + i$ è irriducibile.

Risulta: $\mathcal{N}(3 - i) = 10$. Posto $3 - i = z_1 z_2$, allora $\mathcal{N}(z_1)\mathcal{N}(z_2) = 10$. Sia ad esempio $\mathcal{N}(z_1) = 2$ (e $\mathcal{N}(z_2) = 5$). Si verifica subito che $z_1 = \pm 1 \pm i$ [infatti: $a^2 + b^2 = 2 \Longrightarrow a^2 = b^2 = 1 \Longrightarrow a = \pm 1,\ b = \pm 1$]. Posto ad esempio $z_1 = 1 + i$, si divida $3 - i$ per $1 + i$. Risulta:

$$\tfrac{3-i}{1+i} = \tfrac{(3-i)(1+i)}{2} = \tfrac{2-4i}{2} = 1 - 2i$$

e quindi $3 - i = (1 + i)(1 - 2i)$. I due fattori ottenuti sono irriducibili, in quanto hanno norma prima (rispettivamente 2, 5)

Si conclude che una fattorizzazione di z in fattori irriducibili è

$$z = 4 + 2i = (1 + i)^2(1 - 2i).$$

* * *

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.

Soluzione. (*i*) Cominciamo con la divisione di z_1 per z_2.

Poiché $\frac{z_1}{z_2} = \frac{(4+3i)(3+2i)}{9+4} = \frac{6}{13} + \frac{17}{13}i$, si pone

$$q_1 = 0 + i = i, \quad r_1 = z_1 - z_2 q_1 = 2.$$

Allora $z_1 = q_1 z_2 + r_1$, cioè $4 + 3i = i(3 - 2i) + 2$.

Dividiamo ora z_2 per r_1. Poiché $\frac{z_2}{r_1} = \frac{3-2i}{2} = \frac{3}{2} - i$, si pone

$$q_2 = 2 - i = i, \quad r_2 = z_2 - q_2 r_1 = -1.$$

Allora $z_2 = q_2 r_1 + r_2$, cioè $3 - 2i = (2 - i)2 - 1$.

Dividiamo r_1 per r_2. Si ha: $2 = (-1)(-1) + 0$.

Si conclude che $MCD(z_1, z_2) = -1 \sim 1$.

(*ii*) Si ha:

$$\begin{aligned} 1 &= -(\underline{3 - 2i}) + (2 - i)\underline{2} \\ \underline{2} &= (\underline{4 + 3i}) - i(\underline{3 - 2i}). \end{aligned}$$

Ne segue che:

$$1 = -(\underline{3 - 2i}) + (2 - i)\left[(\underline{4 + 3i}) - i(\underline{3 - 2i})\right] = (2 - i)(\underline{4 + 3i}) + (-2 - 2i)(\underline{3 - 2i}).$$

Si è ottenuta l'identità di Bézout

$$1 = (2 - i)z_1 - (2 + 2i)z_2.$$

(*iii*) Poiché risulta, in generale, che $mcm(z_1, z_2) = \frac{z_1 z_2}{MCD(z_1, z_2)}$, allora

$$mcm(z_1, z_2) = \tfrac{z_1 z_2}{1} = z_1 z_2 = 18 + i$$

(*iv*) Ovviamente $z_1 \big| z_1 \overline{z_1} = 25$. Dunque $z_1 \big| 5 \cdot 5$. Basta allora verificare che $z_1 \nmid 5$ e si conclude che z_1 non è primo.

Se per assurdo $z_1 \big| 5$, allora $5 = (4 + 3i)(a + ib)$, per un opportuno $a + ib \in \boldsymbol{Z}[i]$. Ne segue

$$5 = 4a - 3b + i(3a + 4b) \text{ ovvero } \begin{cases} 4a - 3b = 5 \\ 3a + 4b = 0. \end{cases}$$

Tale sistema ammette un'unica soluzione in $\boldsymbol{Q}$, calcolabile risolvendo il sistema. Si ottiene $a = \frac{4}{5}$, $b = \frac{3}{5}$. Poiché $a, b \notin \boldsymbol{Z}$ si ha l'assurdo e dunque $z_1 \nmid 5$.

(*v*) Da (*iv*) segue che z_1 è riducibile. Dunque $z_1 = z'\, z'', \text{con } z'\, z''$ non invertibili. Allora $25 = \mathcal{N}(z')\mathcal{N}(z'')$ e quindi $\mathcal{N}(z') = \mathcal{N}(z'') = 5$. Determiniamo gli elementi di $\boldsymbol{Z}[i]$ di norma 5. Se $z' = a + ib$ e $a^2 + b^2 = 5$, allora

$$a = \pm 1,\ b = \pm 2 \text{ oppure } a = \pm 2,\ b = \pm 1.$$

Si hanno quindi otto interi di Gauss:

$$1 + 2i,\ 1 - 2i,\ -1 + 2i,\ -1 - 2i,\ 2 + i,\ 2 - i,\ -2 + i,\ -2 - i.$$

Scegliamo ad esempio $z' = 1 + 2i$ e poniamo $z'' = a + ib$. Allora

$$z_1 = z' z'' = (1 + 2i)(a + ib) = a - 2b + i(b + 2a) \text{ e quindi } \begin{cases} a - 2b = 4 \\ b + 2a = 3. \end{cases}$$

Risolvendo tale sistema si ottiene $a = 2$, $b = -1$. Dunque $z'' = 2 - i$.

Poiché $z' = 1 + 2i$ e $z'' = 2 - i$ hanno norma 5, sono irriducibili. Quindi

$$4 + 3i = (1 + 2i)(2 - i)$$

è la fattorizzazione cercata.

* * *

3.31. Si consideri il dominio d'integrità $\boldsymbol{Z}[\sqrt{-2}] = \left\{a + b\sqrt{-2},\ \forall\, a, b \in \boldsymbol{Z}\right\}$.

(*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.

Soluzione. (*i*) Osservato che $\boldsymbol{Z}[\sqrt{-2}] \subset \boldsymbol{Q}[\sqrt{-2}]$ (sottocampo di $\boldsymbol{C}$), risulta, posto $z = a + b\sqrt{-2}$:

$$z \in \mathcal{U}(\boldsymbol{Z}[\sqrt{-2}]) \iff \tfrac{1}{z} \in \boldsymbol{Z}[\sqrt{-2}] \iff \tfrac{\bar{z}}{z\bar{z}} \in \boldsymbol{Z}[\sqrt{-2}] \iff \tfrac{a-b\sqrt{-2}}{a^2+2b^2} \in \boldsymbol{Z}[\sqrt{-2}] \iff$$
$$\iff a^2 + 2b^2 = 1 \iff a = \pm 1,\ b = 0 \iff z = \pm 1.$$

Dunque $\mathcal{U}(\boldsymbol{Z}[\sqrt{-2}]) = \{\pm 1\}$.

(*ii*) Se gli elementi $3,\ 1 + 2\sqrt{-2},\ 1 - 2\sqrt{-2}$ fossero irriducibili, allora l'elemento $9 \in \boldsymbol{Z}[\sqrt{-2}]$ ammetterebbe due fattorizzazioni diverse [in quanto 3 è associato soltanto a se stesso e a -3] e dunque $\boldsymbol{Z}[\sqrt{-2}]$ sarebbe un UFD. Va però verificato se i tre elementi in questione sono irriducibili.

Consideriamo l'elemento $3 \in \boldsymbol{Z}[\sqrt{-2}]$ e scriviamolo nella forma $3 = z_1 z_2$, con $z_1, z_2 \in \boldsymbol{Z}[\sqrt{-2}]$. Poiché $\mathcal{N}(3) = 9 = \mathcal{N}(z_1)\mathcal{N}(z_2)$, sono possibili i due casi

$$\mathcal{N}(z_1) = \mathcal{N}(z_2) = 3; \quad \mathcal{N}(z_1) = 9,\ \mathcal{N}(z_2) = 1 \ \text{(o viceversa)}$$

[si noti che $\mathcal{N}(z) \geq 0,\ \forall\, z \in \boldsymbol{Z}[\sqrt{-2}]$]. Nel secondo caso, la fattorizzazione è banale. Assumiamo che sia verificato il primo caso. Posto $z_1 = a + b\sqrt{-2}$, si ha

$$\mathcal{N}(z_1) = 3 \iff a^2 + 2b^2 = 3 \iff a^2 = b^2 = 1 \iff z = \pm 1 \pm \sqrt{-2}.$$

Ci sono quindi in $\boldsymbol{Z}[\sqrt{-2}]$ quattro elementi di norma 3. Eseguendone i prodotti a due a due si ottiene in particolare che

$$(1 + \sqrt{-2})(1 - \sqrt{-2}) = 3$$

e quindi 3 è riducibile.

Procedendo in modo analogo, si verifica che anche gli altri due elementi $1 + 2\sqrt{-2},\ 1 - 2\sqrt{-2}$ [anch'essi di norma 9] sono riducibili, risultando:

$$1 + 2\sqrt{-2} = (1 - \sqrt{-2})(-1 + \sqrt{-2}), \quad 1 - 2\sqrt{-2} = (1 + \sqrt{-2})(-1 - \sqrt{-2}).$$

Allora:

$$9 = \begin{cases} 3 \cdot 3 = (1 + \sqrt{-2})^2 (1 - \sqrt{-2})^2 \\ (1 + 2\sqrt{-2})(1 - 2\sqrt{-2}) = (1 - \sqrt{-2})(-1 + \sqrt{-2})(1 + \sqrt{-2})(-1 - \sqrt{-2}). \end{cases}$$

Le due fattorizzazioni in elementi irriducibili sono essenzialmente uguali, in quanto differiscono soltanto per l'ordine dei fattori e per il segno di due fattori (cioè a meno di elementi associati). Dunque non si può affatto concludere che $\boldsymbol{Z}[\sqrt{-2}]$ non sia un UFD.

Nota. Si potrebbe invece dimostrare che $\boldsymbol{Z}[\sqrt{-2}]$ è un UFD. Un suggerimento: determinare una divisione con resto in $\boldsymbol{Z}[\sqrt{-2}]$.

* * *

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 $3\ (mod\ 4)$.

Soluzione. Se $a \in \boldsymbol{Z}$ è pari, $a = 2h$, allora $a^2 = 4h^2 \equiv 0\ (mod\ 4)$. Se $a \in \boldsymbol{Z}$ è dispari, $a = 2h + 1$, allora $a^2 = 4h^2 + 4h + 1 \equiv 1\ (mod\ 4)$. Ne segue che, $\forall\, a, b \in \boldsymbol{Z}$, si hanno tre possibili casi:

$$a^2 + b^2 \equiv \begin{cases} 0 + 0 = 0\ (mod\ 4) \\ 0 + 1 = 1\ (mod\ 4) \\ 1 + 1 = 2\ (mod\ 4), \end{cases}$$

e quindi $a^2 + b^2 \not\equiv 3\ (mod\ 4)$.

Sia ora $p = 3 + 4k$ un primo in $\boldsymbol{N}$ e sia $p = zw$, con $z, w \in \boldsymbol{Z}[i],\ z = a + ib$. Allora

$$p^2 = \mathcal{N}(p) = \mathcal{N}(z)\mathcal{N}(w) = (a^2 + b^2)\mathcal{N}(w)$$

e quindi $a^2 + b^2$ assume uno dei tre valori: $1,\ p,\ p^2$. Ma per quanto sopra osservato non può risultare $a^2 + b^2 = p$ e dunque

$$a^2 + b^2 = 1 \implies z \in \mathcal{U}(\boldsymbol{Z}[i]); \quad a^2 + b^2 = p^2 \implies w \in \mathcal{U}(\boldsymbol{Z}[i]).$$

Si conclude che p è irriducibile in $\boldsymbol{Z}[i]$.

* * *

3.33. [Proposto dallo studente V.Capraro]. (*i*) Sia $\widetilde{\ }: K[X] \to K[X]$ 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.

Soluzione. (*i*) Nelle ipotesi considerate, $\partial P = \partial \widetilde{P}$. Poiché $\widetilde{\widetilde{P}} = P$, basterà dimostrare soltanto l'implicazione ($\Longrightarrow$).

Se $\partial P = 1$, allora $\partial \widetilde{P} = 1$ e dunque $\widetilde{P}$ è irriducibile. Assumiamo quindi P irriducibile in $K[X]$, con $\partial P = n \geq 2, \ a_0 \neq 0$. Per assurdo, sia $\widetilde{P}$ riducibile e sia H un fattore irriducibile di $\widetilde{P}$. Posto $h = \partial H$, allora $1 \leq h < n$. Inoltre $\partial \widetilde{H} = \partial H$ [infatti H è irriducibile e quindi ha termine noto $\neq 0$].

Denotiamo con A la matrice di Sylvester di $\widetilde{P}, H$ [cfr.**Esercizio 9**]. Si tratta di una matrice quadrata di ordine $n+h$, il cui determinante $Ris(\widetilde{P}, H)$ è nullo [in quanto $\widetilde{P}, H$ hanno in comune un fattore (cioè H)]. Si applica alle colonne di A la permutazione che porta la colonna j-sima di A nella colonna $(n+h-j+1)$-sima, $\forall j = 1, \ldots, n+k$ [cioè che scambia la prima colonna con l'ultima, ecc.]. Si ottiene così una matrice A_1, il cui determinante è ancora nullo.

Si applicano ora ad A_1 le due seguenti permutazioni sulle righe: la permutazione che trasforma la riga i-sima di A_1 nella riga $(h-i+1)$-sima, $\forall i = 1, \ldots, h$, e la permutazione che trasforma la riga $(h+s)$-sima di A_1 nella riga $(n+h-s+1)$-sima, $\forall s = 1, \ldots, n$. La matrice ottenuta (il cui determinante è ancora nullo) coincide con la matrice di Sylvester di $P, \widetilde{H}$. Ne segue che $Ris(P, \widetilde{H}) = 0$ e quindi $P, \widetilde{H}$ hanno un fattore non costante in comune. Poiché $\partial H = \partial \widetilde{H}$ e P è irriducibile, si ha un assurdo.

(*ii*) Vale il seguente risultato (*tipo Eisenstein*):

Sia $f \in \boldsymbol{Z}[X]$ un polinomio primitivo, con $\partial f = n \geq 1$. Sia $f = \sum_{k=0}^{n} a_k X^k$. Se $\exists p$ primo verificante le seguenti condizioni:

$$p \,|\, a_n, \ p \,|\, a_{n-1}, \ \ldots \ , \ p \,|\, a_1, \ p \nmid a_0 \ \ e \ \ p^2 \nmid a_n,$$

allora f è irriducibile in $\boldsymbol{Z}[X]$.

Nelle attuali ipotesi si può applicare ad $\widetilde{f}$ l'usuale criterio di Eisenstein. Da (*i*) segue che $\widetilde{\widetilde{f}} = f$ è irriducibile in $\boldsymbol{Q}[X]$ e dunque in $\boldsymbol{Z}[X]$.

* * *

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 $\boldsymbol{Z}[X]$.

Soluzione. A è un anello commutativo unitario finito. Se $\big(\prod_{\alpha \in A^\cdot} \alpha\big)^2 \neq 0$, allora A non ammette zero-divisori, cioè è integro. Ne segue che $\overline{f}$ è irriducibile in $Z_p[X]$ e dunque che f è irriducibile in $Z[X]$.

* * *

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) $MCD(F,P) \neq 1$.

Soluzione. (a) $\Longrightarrow$ (b) è ovvio.

(b) $\Longrightarrow$ (c). Per assurdo, sia $(P,F)=1$. Allora, per opportuni S, $R \in K[X]$, risulta $1 = PS + FR$ e dunque $1 = 0 + \overline{F}\,\overline{R}$. Dunque $\overline{F}$ è invertibile in A, contro l'ipotesi.

(c) $\Longrightarrow$ (a). Sia D un divisore irriducibile di (F,P). Poiché $D \left| \begin{matrix} P \\ F \end{matrix} \right.$, allora $P = DR$, $F = DT$, per opportuni R, $T \in K[X]$. Ne segue che

$$FR = DTR = PT \equiv 0 \ (mod\ P), \ \text{cioè} \ \overline{F}\,\overline{R} = 0.$$

Si osservi che $1 \leq \partial R < n$ e dunque $\overline{R} \neq 0$. Si conclude che $\overline{F}$ è uno zero-divisore in A.

* * *

Soluzioni degli 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 $n \in \boldsymbol{Z}$.

Soluzione. (*i*) L'insieme $H_0 := \{nt + ms,\ \forall\, t,s \in \boldsymbol{Z}\,\}$ è un sottogruppo di $(\boldsymbol{Z},+)$. Infatti risulta: $H_0 - H_0 \subseteq H_0$ [essendo $nt + ms - (nt' + ms') = n(t-t') + m(s-s') \in H_0$].

Se $H \leq \boldsymbol{Z}$ e $H \ni n,m$, allora $H \ni nt + ms$, $\forall\, t,d \in \boldsymbol{Z}$ e quindi $H \supseteq H_0$. Si conclude che $\langle n,\, m\rangle = H_0$.

(*ii*) Sia $d = an + bm$ [identità di Bézout]. Allora $dt = atn + btm \in \langle n,\, m\rangle$, $\forall\, t \in \boldsymbol{Z}$. Perciò $\langle d\rangle \subseteq \langle n,\, m\rangle$. Viceversa, posto $n := dn_1$, $m := dm_1$, allora $nt + ms = (n_1 t + m_1 s)d \in \langle d\rangle$ e quindi $\langle n,\, m\rangle \subseteq \langle d\rangle$.

(*iii*) Sia H un sottogruppo di $(\boldsymbol{Z},+)$. Se $H = \{0\}$, allora $H = \langle 0\rangle$. Sia $H \neq \{0\}$. Allora $H \cap \boldsymbol{N}^+ \neq \emptyset$ e sia $n := min(H \cap \boldsymbol{N}^+)$. Per ogni $t \in H$: $t = qn + r$, con $0 \leq r < n$. Allora $r = t - qn \in H$. Per la minimalità di n, $r = 0$. Ne segue che $t = hn$ e quindi $t \in \langle n\rangle$. Allora $H \subseteq \langle n\rangle$. L'inclusione opposta è ovvia.

* * *

4.2. Sia G un gruppo <u>finito</u> e sia H un sottoinsieme non vuoto di G. Verificare che

$$H \leq G \iff H \cdot H \subseteq H.$$

Soluzione. ($\Longrightarrow$). È ovvio.

($\Longleftarrow$). Basta verificare che $H \cdot H^{-1} \subseteq H$.

Poiché $|G| = n < \infty$, risulta che $\circ(h) \,\big|\, n$, $\forall\, h \in H$. Posto $t := \circ(h)$, ne segue che $t < \infty$.

Da $h^t = 1$, segue che $h\, h^{t-1} = 1$. Allora $h^{-1} = h^{t-1} \in H$. È quindi provato che $H^{-1} \subseteq H$. Ne segue che $H \cdot H^{-1} \subseteq H \cdot H \subseteq H$.

* * *

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 $\mathbf{Q}^+ = \{q \in \mathbf{Q} \,:\, q > 0\}$].

Soluzione. Il sottogruppo $\langle \boldsymbol{L}\rangle$ è formato dai numeri reali del tipo

$$\sum_{i=1}^{s} r_i\, lg(n_i),\ \forall\, s \geq 0,\ \forall\, r_i \in \boldsymbol{Z},\ \forall\, n_i \in \boldsymbol{N},\ n_i > 0.$$

L'applicazione lg stabilisce un isomorfismo tra i gruppi $(\boldsymbol{R}^+,\cdot)$ e $(\boldsymbol{R},+)$ [infatti $lg(ab) = lg(a)lg(b)$, $\forall\, a,b > 0$]. Poiché $(\mathbf{Q}^+,\cdot)$ è un sottogruppo di $(\boldsymbol{R}^+,\cdot)$, $lg(\mathbf{Q}^+)$ è un sottogruppo di $(\boldsymbol{R},+)$, isomorfo a $(\boldsymbol{Q}^+,\cdot)$. Basta allora verificare che $\langle \boldsymbol{L}\rangle = lg(\mathbf{Q}^+)$. Infatti:

- essendo $\boldsymbol{L} \subseteq lg(\mathbf{Q}^+)$ allora $\langle \boldsymbol{L}\rangle \leq lg(\mathbf{Q}^+)$;
- $\forall\, q = \frac{n}{m} \in \boldsymbol{Q}^+$ $(n,m > 0)$, si ha: $lg(q) = lg(n) - lg(m) \in \langle \boldsymbol{L}\rangle$. Dunque $lg(\mathbf{Q}^+) \leq \langle \boldsymbol{L}\rangle$.

* * *

4.4. Per ogni $n \geq 1$ sia $\boldsymbol{C}_n$ il gruppo delle radici $n-$esime dell'unità e sia $\boldsymbol{C}_\infty := \bigcup_{n\geq 1} \boldsymbol{C}_n$.

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 $\boldsymbol{C}_\infty \neq \boldsymbol{U}$?

Soluzione. (*i*) Siano $z_1, z_2 \in \boldsymbol{C}_\infty$. Esistono $n_1, n_2 \in \boldsymbol{N}^+$ tali che $z_1^{n_1} = z_2^{n_2} = 1$. Allora:

$$(z_1 z_2)^{n_1 n_2} = z_1^{n_1 n_2} \cdot z_2^{n_1 n_2} = (z_1^{n_1})^{n_2} \cdot (z_2^{n_2})^{n_1} = 1^{n_1} \cdot 1^{n_2} = 1.$$

Dunque $z_1 z_2 \in \boldsymbol{C}_\infty$.

Ovviamente $1 \in \boldsymbol{C}_1 \subset \boldsymbol{C}_\infty$. Se infine $z \in \boldsymbol{C}_\infty$ e $z \in \boldsymbol{C}_n$, allora $\frac{1}{z} \in \boldsymbol{C}_n$ e quindi $\frac{1}{z} \in \boldsymbol{C}_\infty$.

(*ii*) Sia $z \in \boldsymbol{C}_\infty$. Se $z \in \boldsymbol{C}_n$, allora $\circ(z) \big| n$ e dunque $\circ(z) < \infty$. Viceversa, se $\circ(z) < \infty$ e $\circ(z) = m$, allora $z \in \boldsymbol{C}_m$ e dunque $z \in \boldsymbol{C}_\infty$.

(*iii*) Siano $z_1, z_2 \in \boldsymbol{U}$. Dunque $\mathcal{N}(z_1)\mathcal{N}(z_2) = 1$. Allora $\mathcal{N}(z_1 z_2) = \mathcal{N}(z_1)\mathcal{N}(z_2) = 1$ e dunque $z_1 z_2 \in \boldsymbol{U}$. Ovviamente $1 \in \boldsymbol{U}$. Infine $\mathcal{N}(\frac{1}{z}) = \frac{1}{\mathcal{N}(z)} = 1$ e dunque $\frac{1}{z} \in \boldsymbol{U}$.

(*iv*) Per ogni $z \in \boldsymbol{C}_\infty$, $z^n = 1$ $(\exists\, n \geq 1)$. Dunque $1 = \mathcal{N}(z^n) = \mathcal{N}(z)^n$. Poiché $\mathcal{N}(z) \in \boldsymbol{R}^+$, da $\mathcal{N}(z)^n = 1$ segue $\mathcal{N}(z) = 1$ [l'unica radice reale e positiva di 1 è 1]: dunque $z \in \boldsymbol{U}$.

Si noti che $\boldsymbol{C}_\infty$ ha cardinalità $|\boldsymbol{N}|$ [infatti è unione di un'infinità numerabile di insiemi finiti], mentre $\boldsymbol{U}$ ha cardinalità $|\boldsymbol{R}|$. Dunque $\boldsymbol{C}_\infty < \boldsymbol{U}$.

* * *

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 $H_1 H_2$ è un sottogruppo di $\boldsymbol{S}_4$ ed è un gruppo di Klein.

(*ii*) Verificare che $H_1 H_3$ 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?

Soluzione. (*i*) Risulta:

$$H_1 H_2 = \{(1),\, (1,\,2),\, (3,\,4),\, (1,2)(3,\,4)\}, \quad H_2 H_1 = \{(1),\, (3,\,4),\, (1,\,2),\, (3,\,4)(1,2)\}.$$

Poiché $H_1 H_2 = H_2 H_1$, allora $H_1 H_2$ è un sottogruppo di $\boldsymbol{S}_4$. Tale sottogruppo ha tre elementi di periodo 2 e quindi è isomorfo ad un gruppo di Klein.

(*ii*) Risulta :

$$H_1 H_3 = \{(1),\, (1,\,2),\, (1,\,4),\, (1,\,2)(1,\,4) = (1,\,2,\,4)\}.$$

Non si tratta di un sottogruppo di $\boldsymbol{S}_4$. Infatti $\circ(1,\,2,\,4) = 3$ non divide l'ordine di $H_1 H_3$.
Ovviamente $\langle H_1 \cup H_3 \rangle = \langle (1),\, (1,\,2),\, (1,\,4) \rangle = \langle (1,\,2),\, (1,\,4) \rangle$. Tale sottogruppo contiene, oltre a (1), $(1,\,2)$ e $(1,\,4)$, anche le permutazioni

$$(1,\,2,\,4) = (1,\,2)(1,\,4),\ (1,\,4,\,2) = (1,\,2,\,4)^{-1},\ (2,\,4) = (1,\,2,\,4)(1,\,2).$$

Dunque $\langle H_1 \cup H_3 \rangle \supseteq \boldsymbol{S}(\{1,2,4\}) \supseteq H_1 \cup H_3$ e pertanto $\langle H_1 \cup H_3 \rangle = \boldsymbol{S}(\{1,2,4\}) \cong \boldsymbol{S}_3$.

(*iii*) Risulta:

$$H = \langle H_1 \cup H_2 \cup H_3 \rangle = \langle (1,\,2),\, (3,\,4),\, (1,\,4) \rangle.$$

Il sottogruppo H contiene i 3-cicli:

$$(1,\,2)(1,\,4) = (1,\,2,\,4) \text{ e quindi } (1,\,4,\,2) = (1,\,2,\,4)^{-1};$$
$$(1,\,4)(3,\,4) = (1,\,3,\,4) \text{ e quindi } (1,\,4,\,3) = (1,\,3,\,4)^{-1};$$
$$(1,\,2,\,4)(1,\,4,\,3) = (1,\,2,\,3) \text{ e quindi } (1,\,3,\,2) = (1,\,2,\,3)^{-1};$$
$$(1,\,2,\,3)(1,\,4,\,2) = (2,\,3,\,4) \text{ e quindi } (2,\,4,\,3) = (2,\,3,\,4)^{-1}.$$

Dunque H contiene tutti gli otto 3-cicli di $\boldsymbol{S}_4$. È noto che il gruppo alterno $\boldsymbol{A}_4$ è generato dai 3-cicli. Dunque $\boldsymbol{A}_4 \leq H$. Ma H contiene anche permutazioni dispari (ad esempio i suoi tre 2-cicli generatori). Dunque $\boldsymbol{A}_4 < H$. Si conclude che $H = \boldsymbol{S}_4$.

* * *

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 $\langle b,\, c \rangle \cong \boldsymbol{S}_3$.

Soluzione. (*i*) Poiché $\circ(a) = 2\cdot 3 = 6$, risulta:

$$\langle a\rangle = \{1,\, a,\, a^2,\, a^3,\, a^4,\, a^5\}.$$

Si ha:

$$a^2 = (1\,3\,2), \quad a^3 = (4\,5), \quad a^4 = (1\,2\,3), \quad a^5 = (1\,3\,2)(4\,5).$$

Poichè $b = (1\,2\,3) = a^4$, allora $\langle a,\, b\rangle = \langle a\rangle \cong \boldsymbol{C}_6$.

(*ii*) Risulta: $\circ(a) = 6$, $\circ(c) = 2$; inoltre $c \notin \langle a\rangle$ e $ca = a^5c$. Si conclude che

$$\langle a,\, c\rangle = \{1,\, a,\, a^2,\, a^3,\, a^4,\, a^5,\, c,\, ac,\, a^2c,\, a^3c,\, a^4c,\, a^5c\}$$

[con $a^6 = c^2 = 1$, $ca = a^5c$]. Tale gruppo è manifestamente isomorfo al gruppo diedrale $\boldsymbol{D}_6 = \big\langle \varphi,\, \rho \;\big|\; \varphi^6 = 1 = \rho^2,\, \rho\circ\varphi = \varphi^5\circ\rho\big\rangle$. Per ottenere un isomorfismo tra i due gruppi, basta definire

$$f : \langle a,\, c\rangle \to \boldsymbol{D}_6 \text{ tale che } f(a) = \varphi,\, f(c) = \rho$$

[e poi estendere f agli altri elementi, in modo che sia un omomorfismo].

(*iii*) Poiché $\circ(b) = 3$, $\circ(c) = 2$ e poiché $cb = b^2c = (1,\, 3)$, allora

$$\langle b,\, c\rangle = \{1,\, b,\, b^2,\, c,\, bc,\, b^2c\}.$$

Si tratta di un gruppo non abeliano di ordine 6. Dunque $\langle b,\, c\rangle \cong \boldsymbol{S}_3$. Un isomorfismo $f : \langle b,\, c\rangle \to \boldsymbol{S}_3$ è ottenuto ponendo

$$f(b) = (1,\, 2,\, 3), \quad f(c) = (1,\, 2)$$

[e poi estendendo f agli altri elementi, in modo che sia un omomorfismo].

* * *

4.7. Determinare le permutazioni di $\boldsymbol{S}_5$ aventi struttura ciclica $(\_\ \_\ \_)(\_\ \_)$ e quelle aventi struttura ciclica $(\_\ \_)(\_\ \_)$.

Soluzione. Le permutazioni di tipo $(\_\ \_\ \_)(\_\ \_)$ in $\boldsymbol{S}_5$ sono in corrispondenza biunivoca con i 3-cicli di $\boldsymbol{S}_5$. Infatti, posto $X = \{1,2,3,4,5\}$, ad ogni 3-ciclo $(a,\, b,\, c) \in \boldsymbol{S}_5$, resta univocamente associata la permutazione $(a,\, b,\, c)(d,\, e)$, con $\{d, e\} = X - \{a, b, c\}$.

I 3-cicli di $\boldsymbol{S}_5$ sono $\binom{5}{3}(3-1)! = 20$. Pertanto le permutazioni di $\boldsymbol{S}_5$ con struttura ciclica $(\_\ \_\ \_)(\_\ \_)$ sono 20, cioè:

$$\begin{array}{l}(1,\, 2,\, 3)(4,\, 5),\ (1,\, 2,\, 4)(3,\, 5),\ (1,\, 2,\, 5)(3,\, 4),\ (1,\, 3,\, 4)(2,\, 5),\ (1,\, 3,\, 5)(2,\, 4),\\ (1,\, 4,\, 5)(2,\, 3),\ (2,\, 3,\, 4)(1,\, 5),\ (2,\, 3,\, 5)(1,\, 4),\ (2,\, 4,\, 5)(1,\, 3),\ (3,\, 4,\, 5)(1,\, 2),\\ (1,\, 3,\, 2)(4,\, 5),\ (1,\, 4,\, 2)(3,\, 5),\ (1,\, 5,\, 2)(3,\, 4),\ (1,\, 4,\, 3)(2,\, 5),\ (1,\, 5,\, 3)(2,\, 4),\\ (1,\, 5,\, 4)(2,\, 3),\ (2,\, 4,\, 3)(1,\, 5),\ (2,\, 5,\, 3)(1,\, 4),\ (2,\, 5,\, 4)(1,\, 3),\ (3,\, 5,\, 4)(1,\, 2).\end{array}$$

In $\boldsymbol{S}_4$ le permutazioni aventi struttura ciclica $(\_\ \_)(\_\ \_)$ sono 3, cioè $(1,\, 2)(3,\, 4)$, $(1,\, 3)(2,\, 4)$ e $(1,\, 4)(2,\, 3)$. In $\boldsymbol{S}_5$ le permutazioni aventi struttura ciclica $(\_\ \_)(\_\ \_)$ sono ottenute eliminando di volta in volta da $X = \{1,2,3,4,5\}$ un elemento e scrivendo le tre permutazioni sui quattro elementi rimasti. Sono quindi $5\cdot 3 = 15$, cioè:

$$\begin{array}{l}(1,\, 2)(3,\, 4),\ (1,\, 3)(2,\, 4),\ (1,\, 4)(3,\, 2),\\ (1,\, 2)(3,\, 5),\ (1,\, 3)(2,\, 5),\ (1,\, 5)(2,\, 3),\\ (1,\, 2)(4,\, 5),\ (1,\, 4)(2,\, 5),\ (1,\, 5)(2,\, 4),\\ (1,\, 3)(4,\, 5),\ (1,\, 4)(3,\, 5),\ (1,\, 5)(3,\, 4),\\ (2,\, 3)(4,\, 5),\ (2,\, 4)(3,\, 5),\ (2,\, 5)(3,\, 4).\end{array}$$

* * *

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 $h + k \le n$).

Soluzione. (*i*) Si scelga in $\boldsymbol{S}_6$ un 3-ciclo $(a,\, b,\, c)$, con $a, b, c \in X := \{1,2,3,4,5,6\}$. Esso andrà poi moltiplicato per un 2-ciclo $(d,\, e)$, con $d, e \in X - \{a, b, c\}$; per la scelta di tale 2-ciclo si hanno ovviamente 3 possibilità.

Come noto, i 3-cicli di $\boldsymbol{S}_6$ possono essere scelti in $\binom{6}{3}(3-1)! = 40$ modi diversi. Moltiplicando ognuno di essi per uno dei 3 possibili 2-cicli, si ottengono complessivamente $40 \cdot 3 = 120$ permutazioni del tipo cercato.

(*ii*) I k-cicli di $\boldsymbol{S}_n$ sono $\binom{n}{k}(k-1)!$, mentre gli h-cicli scelti in un gruppo $\boldsymbol{S}_{n-k}$ (con $n-k \geq h$) sono $\binom{n-k}{h}(h-1)!$. Complessivamente si hanno $\binom{n}{k}\binom{n-k}{h}(k-1)!\,(h-1)!$ permutazioni che sono prodotto di un k-ciclo per un h-ciclo disgiunti. Tali permutazioni sono a due a due distinte in quanto $k > h$.

* * *

4.9. Determinare tutte le strutture cicliche in $\boldsymbol{S}_{16}$, le cui permutazioni abbiano periodo 28. Indicare di ciascuna la parità.

Soluzione. Si ricorda che, se la permutazione $\sigma \in \boldsymbol{S}_n$ è espressa come prodotto di cicli disgiunti $\gamma_1\gamma_2 \dots \gamma_t$, allora $\circ(\sigma) = mcm\big(\circ(\gamma_1), \circ(\gamma_2), \dots, \circ(\gamma_t)\big)$. Inoltre, perché i cicli γ_i siano disgiunti, è necessario che risulti $\sum_{i=1}^{t} \circ(\gamma_i) \leq n$. Si può infine assumere (visto che cicli disgiunti commutano) che risulti $\circ(\gamma_1) \geq \circ(\gamma_2) \dots \geq \circ(\gamma_t)$.

Ciò premesso, sia $\sigma \in \boldsymbol{S}_{16}$, $\sigma = \gamma_1\gamma_2 \dots \gamma_t$. Deve essere

$$\sum_{i=1}^{t} \circ(\gamma_i) \leq 16 \quad \text{e} \quad mcm\big(\circ(\gamma_1), \circ(\gamma_2), \dots, \circ(\gamma_t)\big) = 28.$$

Perché sia verificata quest'ultima condizione deve risultare: $\circ(\gamma_1) = 7$, $\circ(\gamma_2) = 4$ e σ può eventualmente possedere altri cicli il cui periodo sia divisore di 4 (ciò che non altera il mcm). Sono possibili i seguenti quattro casi (ciascuno dei quali rappresenta una distinta struttura ciclica):

$$\begin{aligned}
&\sigma_1 = \gamma_1\gamma_2,\\
&\sigma_2 = \gamma_1\gamma_2\gamma_3, \text{ con } \circ(\gamma_3) = 4,\\
&\sigma_3 = \gamma_1\gamma_2\gamma_4, \text{ con } \circ(\gamma_4) = 2,\\
&\sigma_4 = \gamma_1\gamma_2\gamma_5\gamma_6, \text{ con } \circ(\gamma_5) = \circ(\gamma_6) = 2.
\end{aligned}$$

Ricordato che ogni k-ciclo è prodotto di $k-1$ trasposizioni, si ha: le permutazioni σ_1 sono di classe dispari [esprimibili come un prodotto di 9 trasposizioni]; le permutazioni σ_2 sono di classe pari [esprimibili come un prodotto di 12 trasposizioni]; le permutazioni σ_3 sono di classe pari [prodotto di 10 trasposizioni]; infine, le permutazioni σ_4 sono di classe dispari [prodotto di 11 trasposizioni];

* * *

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** $\boldsymbol{A}_4 \iff \exists\, \tau \in \boldsymbol{A}_4 : \tau^{-1}\sigma\tau = \sigma'$].

Soluzione. (*i*) $\boldsymbol{A}_4$ è formata dalle dodici permutazioni di classe pari di $\boldsymbol{S}_4$. Le strutture cicliche di $\boldsymbol{S}_4$ di tipo pari sono $(\_)$, $(\_\ \_)(\_\ \_)$ e $(\_\ \_\ \_)$. Le dodici permutazioni pari sono

(1),
$(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)$,
$(1,2,3)$, $(1,2,4)$, $(1,3,4)$, $(2,3,4)$, $(1,3,2)$, $(1,4,2)$, $(1,4,3)$, $(2,4,3)$.

Per ottenere la classe di coniugio $[\sigma]_{\boldsymbol{A}_4}$ di $\sigma = (1,2,3)$, bisogna calcolare $\tau^{-1}\sigma\tau$, $\forall\, \tau \in \boldsymbol{A}_4$. Si ha:

$(1)(1,2,3)(1) = (1,2,3)$,
$(1,2)(3,4)(1,2,3)(1,2)(3,4) = (1,4,2)$,
$(1,3)(2,4)(1,2,3)(1,3)(2,4) = (1,3,4)$,
$(1,4)(2,3)(1,2,3)(1,4)(2,3) = (2,4,3)$,
$(1,3,2)(1,2,3)(1,2,3) = (1,2,3)$, $\quad (1,2,3)(1,2,3)(1,3,2) = (1,2,3)$,
$(1,4,2)(1,2,3)(1,2,4) = (2,4,3)$, $\quad (1,2,4)(1,2,3)(1,4,2) = (1,3,4)$,
$(1,4,3)(1,2,3)(1,3,4) = (2,4,3)$, $\quad (1,3,4)(1,2,3)(1,4,3) = (1,4,2)$,
$(2,4,3)(1,2,3)(2,3,4) = (1,3,4)$, $\quad (2,3,4)(1,2,3)(2,4,3) = (1,4,2)$.

Si conclude che $[\sigma]_{\boldsymbol{A}_4} = \{(1,2,3), (1,4,2), (1,3,4), (2,4,3)\}$.
[Si noti che la classe di coniugio di σ in $\boldsymbol{S}_4$ è formata da tutti gli otto 3-cicli].

* * *

4.11. Sia $\mathfrak{T}$ un triangolo isoscele non equilatero. Indicati con 2, 3 i due vertici della base di $\mathfrak{T}$, verificare che $\boldsymbol{Isom}(\mathfrak{T}) = \langle (2,3) \rangle$.

Soluzione. Essendo $\mathfrak{T}$ un triangolo, $\boldsymbol{Isom}(\mathfrak{T}) \leq \boldsymbol{S}_3$. Si osserva subito che $(2,3)$ è indotta dalla riflessione di asse la retta $\boldsymbol{r}$ bisettrice del vertice 1. Dunque $\langle (2,3) \rangle \leq \boldsymbol{Isom}(\mathfrak{T})$. Per concludere, basta verificare che $(1,2), (1,3), (1,2,3), (1,3,2), \notin \boldsymbol{Isom}(\mathfrak{T})$. Ci limitiamo a verificare che $(1,2), (1,2,3) \notin \boldsymbol{Isom}(\mathfrak{T})$.

Se per assurdo $(1,2) \in \boldsymbol{Isom}(\mathfrak{T})$, esisterebbe un'isometria $g \in \boldsymbol{Isom}(\mathfrak{T})$ tale che

$$g(1) = 2, \quad g(2) = 1, \quad g(3) = 3.$$

In particolare g trasforma il lato $\overline{13}$ nel lato $\overline{g(1)g(3)} = \overline{23}$. Ciò è assurdo in quanto un'isometria conserva le distanze ed i lati in questione hanno lunghezze diverse. [Analogamente si verifica che $(1,3) \notin \boldsymbol{Isom}(\mathfrak{T})$].

Se per assurdo $(1,2,3) \in \boldsymbol{Isom}(\mathfrak{T})$, esisterebbe un'isometria $h \in \boldsymbol{Isom}(\mathfrak{T})$ tale che

$$h(1) = 2, \quad h(2) = 3, \quad h(3) = 1.$$

In particolare h trasforma il lato $\overline{12}$ nel lato $\overline{h(1)h(2)} = \overline{23}$. Si conclude come nel caso precedente. [Analogamente si verifica che $(1,3,2) \notin \boldsymbol{Isom}(\mathfrak{T})$].

* * *

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.

Soluzione. Risulta: $|\mathcal{U}(\boldsymbol{Z}_{50})| = \varphi(50) = \varphi(2)\varphi(25) = 1 \cdot (5^2 - 5) = 20$. Si ha:

$$\mathcal{U}(\boldsymbol{Z}_{50}) = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{21}, \overline{23}, \overline{27}, \overline{29}, \overline{31}, \overline{33}, \overline{37}, \overline{39}, \overline{41}, \overline{43}, \overline{47}, \overline{49}\}.$$

Calcoliamo $\circ(\overline{3})$. Poiché $\circ(\overline{3}) \big| 20$, allora $\circ(\overline{3}) \in \{2, 4, 5, 10, 20\}$. Si ha:

$$\overline{3}^2 = \overline{9} \neq \overline{1}; \quad \overline{3}^4 = \overline{81} = \overline{31} \neq \overline{1}; \quad \overline{3}^5 = \overline{31} \cdot \overline{3} = \overline{93} = \overline{43} \neq \overline{1}; \quad \overline{3}^{10} = \overline{-7}^2 = \overline{49} \neq \overline{1}.$$

Dunque $\circ(\overline{3}) = 20$ e pertanto $\mathcal{U}(\boldsymbol{Z}_{50})$ è ciclico, di ordine 20, con generatore $\overline{3}$.

Osserviamo che $\mathcal{U}(\boldsymbol{Z}_{50})$ ha $\varphi(20)$ generatori. Essendo $\varphi(20) = \varphi(4) \cdot \varphi(5) = 8$, $\mathcal{U}(\boldsymbol{Z}_{50})$ ha quindi 8 generatori. Si tratta delle potenze $\overline{3}^k$, con $MCD(k, 20) = 1$. Dunque i generatori sono

$$\overline{3}, \ \overline{3}^3, \ \overline{3}^7, \ \overline{3}^9, \ \overline{3}^{11}, \ \overline{3}^{13}, \ \overline{3}^{17}, \ \overline{3}^{19}.$$

Si ha:

$$\begin{aligned}
&\overline{3}^3 = \overline{27},\\
&\overline{3}^7 = \overline{3}^5 \cdot \overline{3}^2 = \overline{-7} \cdot \overline{9} = \overline{-63} = \overline{-13} = \overline{37},\\
&\overline{3}^9 = \overline{3}^5 \cdot \overline{3}^4 = \overline{-7} \cdot \overline{31} = \overline{-217} = \overline{-17} = \overline{33},\\
&\overline{3}^{11} = \overline{3}^9 \cdot \overline{3}^2 = \overline{-17} \cdot \overline{9} = \overline{-15} = \overline{-3} = \overline{47},\\
&\overline{3}^{13} = \overline{3}^{11} \cdot \overline{3}^2 = \overline{-3} \cdot \overline{9} = \overline{-27} = \overline{23},\\
&\overline{3}^{17} = \overline{3}^{10} \cdot \overline{3}^7 = \overline{-1} \cdot \overline{-13} = \overline{13},\\
&\overline{3}^{19} = \overline{3}^{17} \cdot \overline{3}^2 = \overline{13} \cdot \overline{9} = \overline{117} = \overline{17}.
\end{aligned}$$

Gli elementi di periodo 4 sono $\varphi(4) = 2$. Vanno cercati tra i non generatori di $\mathcal{U}(\boldsymbol{Z}_{50})$. Il primo non generatore $(\neq \overline{1})$ è $\overline{7}$. Si ha: $\overline{7}^2 = \overline{49} = \overline{-1}$, $\overline{7}^4 = \overline{-1}^2 = \overline{1}$. Dunque $\circ(\overline{7}) = 4$. L'altro elemento di periodo 4 è $\overline{7}^3$. Si ha: $\overline{7}^3 = \overline{7}^2 \cdot \overline{7} = \overline{-1} \cdot \overline{7} = \overline{43}$.

* * *

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.

Soluzione. (*i*) Risulta:

$$\mathcal{U}(\boldsymbol{Z}_{15}) = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}.$$

I suoi sottogruppi ciclici propri sono:

$$\langle\overline{2}\rangle = \{\overline{1}, \overline{2}, \overline{4}, \overline{8}\} = \langle\overline{8}\rangle,\ \langle\overline{4}\rangle = \{\overline{1}, \overline{4}\},\ \langle\overline{7}\rangle = \{\overline{1}, \overline{7}, \overline{4}, \overline{13}\} = \langle\overline{13}\rangle,$$
$$\langle\overline{11}\rangle = \{\overline{1}, \overline{11}\} \quad \text{e} \quad \langle\overline{14}\rangle = \{\overline{1}, \overline{14}\}.$$

Inoltre, essendo $\overline{11}\cdot\overline{4} = \overline{14}$, il gruppo $\mathcal{U}(\boldsymbol{Z}_{15})$ ammette il sottogruppo (non ciclico e quindi) di Klein $\boldsymbol{K} = \{\overline{1}, \overline{4}, \overline{11}, \overline{14}\}$.

(*ii*) I tre quozienti sono

$$\mathcal{U}(\boldsymbol{Z}_{15})/_{\langle\overline{4}\rangle} = \{\langle\overline{4}\rangle = \{\overline{1}, \overline{4}\},\ \overline{2}\langle\overline{4}\rangle = \{\overline{2}, \overline{8}\},\ \overline{7}\langle\overline{4}\rangle = \{\overline{7}, \overline{13}\},\ \overline{11}\langle\overline{4}\rangle = \{\overline{11}, \overline{14}\}\};$$
$$\mathcal{U}(\boldsymbol{Z}_{15})/_{\langle\overline{11}\rangle} = \{\langle\overline{11}\rangle, \overline{2}\langle\overline{11}\rangle, \overline{4}\langle\overline{11}\rangle, \overline{8}\langle\overline{11}\rangle\};$$
$$\mathcal{U}(\boldsymbol{Z}_{15})/_{\langle\overline{14}\rangle} = \{\langle\overline{14}\rangle, \overline{2}\langle\overline{14}\rangle, \overline{4}\langle\overline{14}\rangle, \overline{8}\langle\overline{14}\rangle\}.$$

Il primo è un gruppo di Klein [in quanto ha tre elementi di periodo 2]; gli altri due sono ciclici, generati ad esempio dalla classe di $\overline{2}$.

Un isomorfismo $\varphi : \mathcal{U}(\boldsymbol{Z}_{15})/_{\langle\overline{11}\rangle} \to \mathcal{U}(\boldsymbol{Z}_{15})/_{\langle\overline{14}\rangle}$ è ad esempio il seguente:

$$\langle\overline{11}\rangle \to \langle\overline{14}\rangle, \quad \overline{2}\langle\overline{11}\rangle \to \overline{2}\langle\overline{14}\rangle, \quad \overline{4}\langle\overline{11}\rangle \to \overline{4}\langle\overline{14}\rangle, \quad \overline{8}\langle\overline{11}\rangle \to \overline{8}\langle\overline{14}\rangle.$$

* * *

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:

$$\sigma_1 = \tau\,\sigma_2\,\tau^{-1} \quad \text{dove } \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}.$$

Soluzione. (*i*) Per ogni 5-ciclo $(a\,b\,c\,d\,e) \in \boldsymbol{S}_5$, il sottogruppo $\langle(a\,b\,c\,d\,e)\rangle$ è ciclico di ordine 5 e quindi è isomorfo a $\boldsymbol{Z}_5$.

Scelte due permutazioni disgiunte $(a\,b),\ (c\,d) \in \boldsymbol{S}_5$, l'insieme

$$\{(1),\ (a\,b),\ (c\,d),\ (a\,b)(c\,d)\}$$

è un gruppo di Klein.

Scelti un 2-ciclo $(a\,b)$ e un 3-ciclo $(a\,b\,c)$, il sottogruppo

$$\langle(a\,b),\ (a\,b\,c)\rangle = \{(1),\ (a\,b),\ (a\,c),\ (b\,c),\ (a\,b\,c),\ (a\,c\,b)\}$$

è isomorfo a $\boldsymbol{S}_3$.

Non esiste in $\boldsymbol{S}_5$ un elemento di periodo 7 [in quanto 7 non divide $|\boldsymbol{S}_5| = 5!$]. Dunque $\boldsymbol{S}_5$ non ammette sottogruppi isomorfi a $\boldsymbol{Z}_7$.

Scelta infine la permutazione $(a\,b\,c)(d\,e) \in \boldsymbol{S}_5$ [prodotto di cicli disgiunti], tale permutazione ha periodo 6 e dunque genera il gruppo $\langle(a\,b\,c)(d\,e)\rangle$, isomorfo a $\boldsymbol{Z}_6$.

(*ii*) Le strutture cicliche di $\boldsymbol{S}_5$ sono le seguenti:

$$(\_\ \_\ \_\ \_\ \_),\ (\_\ \_\ \_\ \_),\ (\_\ \_\ \_),\ (\_\ \_\ \_)(\_\ \_),\ (\_\ \_),\ (\_\ \_)(\_\ \_),\ (\_)$$

e le corrispondenti permutazioni hanno rispettivamente periodo $5, 4, 3, 6, 2, 2, 1$.

(*iii*) Risulta:

$$\sigma_1 = (1\,4\,3)(2\,5), \quad \sigma_2 = (1\,5)(2\,4\,3).$$

Si può scegliere $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} = (1\,2)$ e risulta

$$\tau\,\sigma_2\,\tau^{-1} = (1\,2)(1\,5)(2\,4\,3)(1\,2) = (1\,4\,3)(2\,5) = \sigma_1.$$

* * *

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: $\boldsymbol{S}_7$, $\boldsymbol{Z}_{11}$, $\boldsymbol{D}_5$, $\boldsymbol{Z}_{15}$.

Soluzione. (*i*) Una volta scritte tutte le possibili strutture cicliche di $\boldsymbol{S}_9$, quelle di ordine 6 sono quelle in cui il *mcm* delle lunghezze dei cicli è 6. Si ottengono quindi le seguenti strutture cicliche:

$$(6,3),\ (6),\ (3,3,2),\ (3,2,2,2),\ (3,2),\ (3,2,2),\ (6,2)$$

[ad esempio, $(6,3)$ corrisponde alla struttura ciclica $(\_\,\_\,\_\,\_\,\_\,\_)(\_\,\_\,\_)$, ecc.]. Di tali strutture cicliche, soltanto le ultime due sono pari [la parità è ottenuta sommando le lunghezze di ogni ciclo, diminuito di 1]. Le strutture cicliche di classe dispari e di ordine 6 sono dunque le prime cinque della lista precedente.

(*ii*) Si scelga, ad esempio, $\tau = (1\,2\,8\,3\,9\,4)$, ovvero $\tau = (1\,2)(3\,9\,4\,7\,8)$.

(*iii*) Si ponga ad esempio $\boldsymbol{H}_1 = \{\sigma \in \boldsymbol{S}_9 : \sigma(8) = 8 \text{ e } \sigma(9) = 9\}$.

Non esiste alcun sottogruppo $\boldsymbol{H}_2 \cong \boldsymbol{Z}_{11}$, perché in $\boldsymbol{S}_9$ non ci sono elementi di periodo 11.

Per ottenere un sottogruppo $\boldsymbol{H}_3 \cong \boldsymbol{D}_5$, basta associare ai vertici di un pentagono regolare le cifre $1,2,3,4,5$ e rappresentare tramite permutazioni dei vertici i movimenti rigidi del pentagono. Risulta: $\boldsymbol{H}_3 = \langle (1\,2\,3\,4\,5), (2\,5)(3\,4) \rangle$.

Poiché $\boldsymbol{Z}_{15} \cong \boldsymbol{Z}_3 \times \boldsymbol{Z}_5$, un sottogruppo $\boldsymbol{H}_4 \cong \boldsymbol{Z}_{15}$ è ad esempio il gruppo ciclico $\langle (1\,2\,3)(4\,5\,6\,7\,8) \rangle$.

* * *

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 $hk = kh$, $\forall\, h \in H$, $\forall\, k \in K$.

Soluzione. (*i*) Sia $x \in G$ e sia γ_x l'automorfismo interno di G corrispondente ad x. L'immagine $\gamma_x(H) = xHx^{-1}$ è un sottogruppo di G, avente ordine m (come H). Dall'ipotesi, $\gamma_x(H) = H$, cioè $xHx^{-1} = H$, da cui $xH = Hx$. Si conclude che $H \trianglelefteq G$.

(*ii*) Si consideri l'elemento $h^{-1}k^{-1}h\,k \in G$ (detto *commutatore di* h, k). Basterà dimostrare che $h^{-1}k^{-1}h\,k = 1$ (e da ciò si deduce subito che $hk = kh$).

Si ha: $h^{-1}k^{-1}h\,k = \begin{cases} h^{-1}(k^{-1}h\,k) \\ (h^{-1}k^{-1}h)\,k. \end{cases}$ Inoltre $\begin{cases} k^{-1}h\,k \in k^{-1}H\,k = H \ \text{ (perché } H \trianglelefteq G), \\ h^{-1}k^{-1}h \in h^{-1}Kh = K \ \text{ (perché } K \trianglelefteq G). \end{cases}$

Si conclude che $h^{-1}k^{-1}h\,k \in \begin{cases} H \cdot H = H \\ K \cdot K = K \end{cases}$ e dunque $h^{-1}k^{-1}h\,k \in H \cap K = \{1\}$.

* * *

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 $HK \cong H \times K$.

Soluzione. (*i*) È ben noto che HK è un sottogruppo di G. È definita l'applicazione

$$\varphi : H \times K \to HK \ \text{ tale che } \varphi((h,k)) = hk, \ \forall\, h \in H, \ \forall\, k \in K.$$

Verifichiamo che φ è un omomorfismo di gruppi. Risulta, $\forall\, (h,k), (h_1,k_1) \in H \times K$:

$$\varphi\big((h,k)(h_1,k_1)\big) = \varphi\big((hh_1, kk_1)\big) = hh_1\,kk_1 = hk\,h_1k_1 = \varphi((h,k))\,\varphi((h_1,k_1)).$$

L'applicazione φ è ovviamente suriettiva. Verifichiamo che è anche iniettiva. Se infatti $hk = h_1k_1$, allora $h_1^{-1}h = k_1k^{-1} \in H \cap K = \{1\}$. Dunque $h_1^{-1}h = 1$, $k_1k^{-1} = 1$ e pertanto $h = h_1$, $k = k_1$.

Abbiamo così dimostrato che φ è un isomorfismo tra HK e $H \times K$.

(*ii*) Sia $|H| = r$, $|K| = s$, con $(r,s) = 1$. Ogni elemento $h \in H$, $h \neq 1$, ha per periodo un divisore di r e dunque $\circ(h) \nmid s$. Pertanto $h \notin K$. È così provato che $H \cap K = \{1\}$.

L'ultima affermazione segue da (*i*).

Nota. Si può facilmente verificare che, se H, K sono normali in G e $H \cap K = \{1\}$, allora H, K sono permutabili elemento per elemento. Se infatti $h \in H$, $k \in K$, posto $x := hkh^{-1}k^{-1}$ basta verificare che $x = 1$. Infatti, essendo H, K normali in G:

$$x = \begin{matrix} h(kh^{-1}k^{-1}) \in H\cdot(kHk^{-1}) \subseteq H\cdot H \subseteq H \\ (hkh^{-1})k^{-1} \in (hKh^{-1})\cdot K \subseteq K\cdot K \subseteq K. \end{matrix} \quad \text{Dunque } x \in H \cap K = \{1\}.$$

* * *

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 $G_1, G_2, \ldots G_t$ sono gruppi ciclici finiti, di ordini a due a due coprimi e se $g_1, g_2, \ldots g_t$ 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.

Soluzione. (*i*) Per semplificare le notazioni denotiamo con lo stesso simbolo $\cdot$ l'operazione di ogni gruppo G_i e con 1 l'elemento neutro di G_i; allora $(1, \ldots, 1)$ è elemento di neutro di $G_1 \times G_2 \times \ldots \times G_t$.

Si ponga: $n := \circ\big((g_1, g_2, \ldots, g_t)\big)$, $n_i := \circ(g_i)$, $m := mcm\big(n_1, \ldots, n_t\big)$. Bisogna verificare che

$$n \,\big|\, m \text{ e } m \,\big|\, n.$$

Poiché $n_i \,\big|\, m$, $g_i^m = 1$. Dunque $\big((g_1, g_2, \ldots, g_t)\big)^m = \big(g_1^m, \ldots, g_t^m\big) = (1, \ldots, 1)$. Ne segue che $n \,\big|\, m$. Viceversa, da $\circ\big((g_1, g_2 \ldots, g_t)\big) = n$, segue che $(1, \ldots, 1) = \big((g_1, g_2 \ldots, g_t)\big)^n = \big(g_1^n, \ldots, g_t^n\big)$. Allora $n_i \,\big|\, n$, $\forall\, i = 1, \ldots, t$, e dunque $m \,\big|\, n$ (per definizione di mcm).

(*ii*) Essendo $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$, il teorema cinese del resto induce l'isomorfismo di gruppi additivi

$$\varphi : \boldsymbol{Z}_{420} \to \boldsymbol{Z}_3 \times \boldsymbol{Z}_4 \times \boldsymbol{Z}_5 \times \boldsymbol{Z}_7 \text{ tale che } \varphi(\overline{x}) = \big(\overline{x}_3, \overline{x}_4, \overline{x}_5, \overline{x}_7\big).$$

In particolare, $\varphi(\overline{33}) = (\overline{0}, \overline{1}, \overline{3}, \overline{5}) \in \boldsymbol{Z}_3 \times \boldsymbol{Z}_4 \times \boldsymbol{Z}_5 \times \boldsymbol{Z}_7$. Risulta:

$$\circ(\overline{0}) = 1 \text{ (in } \boldsymbol{Z}_3); \ \circ(\overline{1}) = 4 \text{ (in } \boldsymbol{Z}_4); \ \circ(\overline{3}) = 5 \text{ (in } \boldsymbol{Z}_5); \ \circ(\overline{5}) = 7 \text{ (in } \boldsymbol{Z}_7).$$

Quindi

$$\circ(\overline{33}) = mcm(1, 4, 5, 7) = 140.$$

[*Nota.* Più rapidamente, $\circ(\overline{33}) = \frac{420}{MCD(33,420)} = \frac{420}{3} = 140$.]

(*iii*) $G_1 \times G_2 \times \ldots \times G_t$ ha ordine $\prod_{i=1}^{t} n_i$. Da (*i*), $\circ\big((g_1, g_2 \ldots, g_t)\big) = mcm\big(n_1, \ldots, n_t\big) = \prod_{i=1}^{t} n_i$ (essendo $n_1, \ldots n_t$ a due a due coprimi). Quindi $G_1 \times G_2 \times \ldots \times G_t$ è ciclico, con generatore $(g_1, g_2, \ldots g_t)$.

* * *

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.

Soluzione. Sia $x \in G$ un elemento di periodo massimo in G. Scelto arbitrariamente $y \in G$, sia $\circ(y) = m$. Sono possibili due casi:

$$m \,\big|\, \circ(x) \text{ oppure } m \nmid \circ(x).$$

Proveremo nel primo caso che $y \in \langle x \rangle$ e verificheremo che nel secondo caso si ottiene un assurdo. Ne consegue che $G = \langle x \rangle$.

(a) Sia $m \,|\, \circ(x)$. Esiste in $\langle x\rangle$ (perché è ciclico) un unico sottogruppo di ordine m. D'altra parte $|\langle y\rangle| = m$ e quindi (per l'ipotesi di unicità di sottogruppi di ordine m), $\langle y\rangle \leq \langle x\rangle$. Allora $y \in \langle x\rangle$.

(b) Per ottenere l'assurdo richiesto, faremo uso dei tre seguenti risultati:

(i) Un sottogruppo unico del suo ordine in un gruppo finito G è normale in G (cfr. **Eserc. 4.16***(i)*).

(ii) Se H, K sono due sottogruppi normali in G, con $H \cap K = \{1\}$, allora sono permutabili elemento per elemento e quindi $H \times K \cong HK$ (cfr. **Eserc. 4.17**).

(iii) Se G_1, G_2 sono gruppi ciclici finiti, con ordini coprimi, allora $G_1 \times G_2$ è ciclico, generato da una coppia di generatori dei due gruppi (cfr. **Eserc. 4.18**).

Si ponga: $m = p_1^{r_1} \dots p_s^{r_s}$ e $\circ(x) = p_1^{t_1} \dots p_s^{t_s}$, con $r_i, t_i \geq 0$. Poiché $m \nmid \circ(x)$, almeno un esponente r_i è maggiore del corrispondente esponente t_i; assumiamo quindi $r_1 > t_1$.

Si considerino i due elementi di G:

$$x_1 = x^{p_1^{t_1}}, \quad y_1 = 1/_{y^{p_1^{r_1}}} = y^{p_2^{r_2} \dots p_s^{r_s}}$$

e se ne calcoli il periodo:

$$\circ(x_1) = \frac{\circ(x)}{MCD\big(\circ(x), p_1^{t_1}\big)} = p_2^{t_2} \dots p_s^{t_s}, \quad \circ(y_1) = \frac{\circ(y)}{MCD\big(\circ(y), p_2^{r_2} \dots p_s^{r_s}\big)} = p_1^{r_1}.$$

Siccome $MCD\big(\circ(x_1), \circ(y_1)\big) = 1$, allora $\langle x_1\rangle \cap \langle y_1\rangle = \{1\}$. Da ($i$), i sottogruppi $\langle x_1\rangle$, $\langle y_1\rangle$ (unici del rispettivo ordine) sono normali in G. Dunque sono permutabili. Da (ii) segue che $\langle x_1\rangle \cdot \langle y_1\rangle \cong \langle x_1\rangle \times \langle y_1\rangle$. In particolare (x_1, y_1) corrisponde (in tale isomorfismo) a $x_1 y_1$. Infine, da (iii) $\langle x_1\rangle \times \langle y_1\rangle$ è ciclico con generatore (x_1, y_1). Ne segue che $\circ\big(x_1 y_1\big) = \circ\big((x_1, y_1)\big) = |\langle x_1\rangle \times \langle y_1\rangle| = \circ(x_1) \cdot \circ(y_1)$.
Ma $\circ(x_1) \cdot \circ(y_1) = p_1^{r_1} p_2^{t_2} \dots p_s^{t_s} > p_1^{t_1} \dots p_s^{t_s} = \circ(x)$. Dunque $x_1 y_1$ ha un periodo superiore a quello di x: ciò è assurdo per la scelta fatta inizialmente.

* * *

4.20. (i) Verificare che $\boldsymbol{D}_6/_{\langle \varphi^3\rangle} \cong \boldsymbol{S}_3$.

(ii) Esplicitare un isomorfismo tra tali gruppi.

Soluzione. (i) Osserviamo che $\langle \varphi^3\rangle \lhd \boldsymbol{D}_6$. Basta verificare che i sei laterali sinistri di $\langle \varphi^3\rangle$ coincidono con i rispettivi laterali destri. Infatti:

$$\varphi\langle\varphi^3\rangle = \{\varphi, \varphi^4\} = \langle\varphi^3\rangle\varphi; \qquad \varphi^2\langle\varphi^3\rangle = \{\varphi^2, \varphi^5\} = \langle\varphi^3\rangle\varphi^2;$$
$$\rho\langle\varphi^3\rangle = \{\rho, \varphi^3\circ\rho\} = \langle\varphi^3\rangle\rho; \qquad (\varphi\circ\rho)\langle\varphi^3\rangle = \{\varphi\circ\rho, \varphi^4\circ\rho\} = \langle\varphi^3\rangle(\varphi\circ\rho);$$
$$(\varphi^2\circ\rho)\langle\varphi^3\rangle = \{\varphi^2\circ\rho, \varphi^5\circ\rho\} = \langle\varphi^3\rangle(\varphi^2\circ\rho).$$

Il gruppo quoziente $\boldsymbol{D}_6/_{\langle\varphi^3\rangle}$ ha cardinalità 6. Si tratta quindi di un gruppo isomorfo a $\boldsymbol{C}_6$ o a $\boldsymbol{S}_3$. Esaminiamo i periodi dei suoi elementi. Si ha: $\circ(\varphi\langle\varphi^3\rangle) = 3$ [infatti $\varphi^2\langle\varphi^3\rangle \neq \varphi\langle\varphi^3\rangle$, $\varphi^3\langle\varphi^3\rangle = \langle\varphi^3\rangle$]. Ne segue che anche $\circ(\varphi^2\langle\varphi^3\rangle) = 3$. Inoltre si verifica che $2 = \circ(\rho\langle\varphi^3\rangle) = \circ((\varphi\circ\rho)\langle\varphi^3\rangle) = \circ((\varphi^2\circ\rho)\langle\varphi^3\rangle)$. Ne segue che $\boldsymbol{D}_6/_{\langle\varphi^3\rangle} \cong \boldsymbol{S}_3$.

(ii) Osservato che φ, ρ sono generatori di $\boldsymbol{D}_6$ e che $(1, 2)$, $(1, 2, 3)$ sono generatori di $\boldsymbol{S}_3$, si ponga:

$$f : \boldsymbol{D}_6 \to \boldsymbol{S}_3 \text{ tale che } f(\varphi) = (1, 2, 3), \quad f(\rho) = (1, 2),$$

e si estenda f agli altri elementi di $\boldsymbol{D}_6$, in modo che f sia un omomorfismo. Dunque:

$$f(\varphi^2) = (1, 3, 2), \quad f(\varphi^3) = (1), \quad f(\varphi^4) = (1, 2, 3),$$
$$f(\varphi^5) = (1, 3, 2), \quad f(\varphi\circ\rho) = (1, 2, 3)(1, 2) = (2, 3),$$
$$f(\varphi^2\circ\rho) = (1, 3, 2)(1, 2) = (1, 3), \quad f(\varphi^3\circ\rho) = (1)(1, 2) = (1, 2),$$
$$f(\varphi^4\circ\rho) = (1, 2, 3)(1, 2) = (2, 3), \quad f(\varphi^5\circ\rho) = (1, 3, 2)(1, 2) = (1, 3).$$

Allora $Im(f) = \boldsymbol{S}_3$ e $Ker(f) = \langle\varphi^3\rangle$. Quindi $\boldsymbol{D}_6/_{\langle\varphi^3\rangle} \cong \boldsymbol{S}_3$.

* * *

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.

Soluzione. Per definizione, $\boldsymbol{C}_4 = \langle i\rangle = \{1, i, -1, -i\}$. Poiché i due gruppi $\boldsymbol{V}, \boldsymbol{C}_4$ non sono isomorfi, nessuno degli omomorfismi da determinare potrà essere biiettivo.

Se $f : \boldsymbol{V} \to \boldsymbol{C}_4$ è un omomorfismo, allora $f(1) = 1$. Inoltre, poiché $\circ(f(x))|\circ(x)$, allora $f(x) \neq \pm i$ [in quanto 4 non divide 2]. Dunque $f(a),\ f(b),\ f(c) \in \{\pm 1\}$ ed a priori si hanno 8 possibili terne $\big(f(a),\ f(b),\ f(c)\big)$:

$$(1,1,1),\ (1,-1,-1),\ (-1,1,-1),\ (-1,-1,1),$$
$$(1,1,-1),\ (1,-1,1),\ (-1,1,1),\ (-1,-1,-1).$$

Verificheremo che solo le prime quattro terne corrispondono ad altrettanti omomorfismi da $\boldsymbol{V}$ a $\boldsymbol{C}_4$.

La terna $(1,1,1)$ corrisponde all'omomorfismo banale $\mathbf{0} : \boldsymbol{V} \to \boldsymbol{C}_4$.

La terna $(1,-1,-1)$ corrisponde all'applicazione

$$f : \boldsymbol{V} \to \boldsymbol{C}_4 \text{ tale che: } f(a) = 1,\ f(b) = -1,\ f(c) = -1.$$

f è un omomorfismo. Infatti:

$$\begin{cases} f(ab) = f(c) = -1 \\ f(a)f(b) = 1 \cdot (-1) = -1, \end{cases} \quad \begin{cases} f(ac) = f(b) = -1 \\ f(a)f(c) = 1 \cdot (-1) = -1, \end{cases} \quad \begin{cases} f(bc) = f(a) = 1 \\ f(b)f(c) = -1 \cdot (-1) = 1. \end{cases}$$

[Non occorrono altre verifiche perché i gruppi sono abeliani].

In modo analogo si verifica che anche le terne $(-1,1,-1)$, $(-1,-1,1)$ corrispondono ad altri due omomorfismi.

Ora verifichiamo che le rimanenti quattro terne definiscono applicazioni che non sono omomorfismi. Infatti:

se $(1,1,-1)$ corrisponde all'applicazione g, $g(ab) = g(c) = -1$, mentre $g(a)g(b) = 1 \cdot 1 = 1$;
se $(1,-1,1)$ corrisponde all'applicazione h, $h(ac) = h(b) = -1$, mentre $h(a)h(c) = 1$;
se $(-1,1,1)$ corrisponde all'applicazione m, $m(bc) = m(a) = -1$, mentre $m(b)m(c) = 1$;
se $(-1,-1,-1)$ corrisponde all'applicazione n, $n(ab) = n(c) = -1$, mentre $n(a)n(b) = 1$.

* * *

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].

Soluzione. (*i*) Si ha:

$$\mathbf{Q} = \langle \underline{\boldsymbol{i}},\ \underline{\boldsymbol{j}},\ \underline{\boldsymbol{k}} \mid \underline{\boldsymbol{i}}^2 = \underline{\boldsymbol{j}}^2 = \underline{\boldsymbol{k}}^2 = -\underline{\mathbf{1}},\ \underline{\boldsymbol{i}}\underline{\boldsymbol{j}} = -\underline{\boldsymbol{j}}\underline{\boldsymbol{i}} = \underline{\boldsymbol{k}},\ \underline{\boldsymbol{j}}\underline{\boldsymbol{k}} = -\underline{\boldsymbol{k}}\underline{\boldsymbol{j}} = \underline{\boldsymbol{i}},\ \underline{\boldsymbol{k}}\underline{\boldsymbol{i}} = -\underline{\boldsymbol{i}}\underline{\boldsymbol{k}} = \underline{\boldsymbol{j}} \rangle =$$
$$= \{\underline{\mathbf{1}},\ -\underline{\mathbf{1}}, \underline{\boldsymbol{i}},\ -\underline{\boldsymbol{i}},\ \underline{\boldsymbol{j}},\ -\underline{\boldsymbol{j}},\ \underline{\boldsymbol{k}},\ -\underline{\boldsymbol{k}}\}.$$

Verifichiamo che i quattro laterali sinistri di $\langle -1 \rangle = \{\pm 1\}$ coincidono con i corrispondenti laterali destri. Infatti:

$$\underline{\boldsymbol{i}}\langle -\underline{\mathbf{1}} \rangle = \{\pm \underline{\boldsymbol{i}}\} = \langle -\underline{\mathbf{1}} \rangle \underline{\boldsymbol{i}}, \quad \underline{\boldsymbol{j}}\langle -\underline{\mathbf{1}} \rangle = \{\pm \underline{\boldsymbol{j}}\} = \langle -\underline{\mathbf{1}} \rangle \underline{\boldsymbol{j}}, \quad \underline{\boldsymbol{k}}\langle -\underline{\mathbf{1}} \rangle = \{\pm \underline{\boldsymbol{k}}\} = \langle -\underline{\mathbf{1}} \rangle \underline{\boldsymbol{k}}.$$

Dunque $\langle -\underline{\mathbf{1}} \rangle \triangleleft \mathbf{Q}$.

(*ii*) $\mathbf{Q}/_{\langle -\underline{\mathbf{1}} \rangle}$ ha ordine 4. Risulta:

$$\mathbf{Q}/_{\langle -\underline{\mathbf{1}} \rangle} = \big\{ \langle -\underline{\mathbf{1}} \rangle,\ \underline{\boldsymbol{i}}\langle -\underline{\mathbf{1}} \rangle,\ \underline{\boldsymbol{j}}\langle -\underline{\mathbf{1}} \rangle,\ \underline{\boldsymbol{k}}\langle -\underline{\mathbf{1}} \rangle \big\}$$

e $\circ(\underline{\boldsymbol{i}}\langle -\underline{\mathbf{1}} \rangle) = 2$ [infatti $\underline{\boldsymbol{i}}\langle -\underline{\mathbf{1}} \rangle \cdot \underline{\boldsymbol{i}}\langle -\underline{\mathbf{1}} \rangle = \underline{\boldsymbol{i}}^2\langle -\underline{\mathbf{1}} \rangle = \langle -\underline{\mathbf{1}} \rangle$]. Analogamente, $\circ(\underline{\boldsymbol{j}}\langle -\underline{\mathbf{1}} \rangle) = \circ(\underline{\boldsymbol{k}}\langle -\underline{\mathbf{1}} \rangle) = 2$. Poiché $\mathbf{Q}/_{\langle -\underline{\mathbf{1}} \rangle}$ ha tre elementi di periodo 2, è un gruppo di Klein.

* * *

4.23. Determinare il quoziente del gruppo moltiplicativo dei razionali non nulli $(\boldsymbol{Q}^{\cdot}, \cdot)$ modulo il sottogruppo $(\boldsymbol{C}_2, \cdot)$.

Soluzione. Si consideri il sottogruppo $(\boldsymbol{Q}^{>0}, \cdot)$ di $(\boldsymbol{Q}^{\cdot}, \cdot)$ e l'applicazione

$$f : \boldsymbol{Q}^{\cdot} \to \boldsymbol{Q}^{>0} \text{ tale che } f(q) = |q|,\ \forall\, q \in \boldsymbol{Q}^{\cdot}.$$

Si ha, $\forall\, q_1, q_2 \in \boldsymbol{Q}^{\cdot}$:

$$f(q_1 q_2) = |q_1 q_2| = |q_1||q_2| = f(q_1)f(q_2),$$

e dunque f è un omomorfismo. f è ovviamente suriettiva. Infine

$$Ker(f) = \{q \in \boldsymbol{Q}^{\cdot} \ :\ |q| = 1\} = \{\pm 1\} = \boldsymbol{C}_2.$$

Dal teorema fondamentale di omomorfismo, $\boldsymbol{Q}^{\cdot}/_{\boldsymbol{C}_2} \cong (\boldsymbol{Q}^{>0}, \cdot)$.

* * *

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*.

Soluzione. Si ponga $\boldsymbol{H}_1 = \boldsymbol{A}_4$ (gruppo alterno). Poiché $(\boldsymbol{S}_4 : \boldsymbol{A}_4) = 2$, allora $\boldsymbol{A}_4 \lhd \boldsymbol{S}_4$. Inoltre $\boldsymbol{S}_4/\boldsymbol{A}_4 \cong \boldsymbol{C}_2$ è abeliano.

Il gruppo alterno $\boldsymbol{A}_4$ è formato [oltre che dall'unità (1)] dagli otto 3-cicli

$$(123),\ (132),\ (124),\ (142),\ (134),\ (143),\ (234),\ (243)$$

e dalle tre coppie di 2-cicli disgiunti

$$(12)(34),\ (13)(24),\ (14)(23).$$

Si verifica facilmente che queste ultime tre permutazioni formano, con l'unità (1), un gruppo di Klein $\boldsymbol{V}$. Verificheremo ora che $\boldsymbol{V} \lhd \boldsymbol{A}_4$. Infatti, i tre laterali sinistri modulo $\boldsymbol{V}$ sono

$$\begin{aligned} \boldsymbol{V} &= \{(1),\ (12)(34),\ (13)(24),\ (14)(23)\};\\ (123)\boldsymbol{V} &= \{(123),\ (134),\ (243),\ (142)\};\\ (132)\boldsymbol{V} &= \{(132),\ (143),\ (234),\ (124)\}. \end{aligned}$$

Si verifica subito che $\boldsymbol{V}(123) = (123)\boldsymbol{V}$. Ne segue che anche $\boldsymbol{V}(132) = (132)\boldsymbol{V}$. Dunque $\boldsymbol{V} \lhd \boldsymbol{A}_4$.

Per concludere che $\boldsymbol{H}_2 = \boldsymbol{V}$ è il secondo sottogruppo cercato, basta osservare che $\left|\boldsymbol{A}_4/\boldsymbol{V}\right| = 3$ e dunque $\boldsymbol{A}_4/\boldsymbol{V} \cong \boldsymbol{C}_3$ è abeliano.

* * *

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.

Soluzione. $(\boldsymbol{C}_4, \cdot)$ e $(\boldsymbol{Z}_4, +)$ sono gruppi isomorfi. Un isomorfismo $f : \boldsymbol{C}_4 \to \boldsymbol{Z}_4$ è il seguente:

$$f(1) = \overline{0},\ f(i) = \tilde{1},\ f(-1) = \tilde{2},\ f(-i) = \tilde{3}.$$

Risulta:

$$\boldsymbol{Hom}(\boldsymbol{Z}_4, \boldsymbol{Z}_6) = \{\overline{k}_- : \boldsymbol{Z}_4 \to \boldsymbol{Z}_6,\ \forall\, \overline{k} \in \boldsymbol{Z}_6 \text{ tale che } \circ(\overline{k}) \,\big|\, MCD(4,6) = 2\}.$$

In $\boldsymbol{Z}_6$ gli unici elementi il cui periodo divida 2 sono $\overline{0}$, $\overline{3}$. L'unico omomorfismo non banale da $(\boldsymbol{C}_4, \cdot)$ a $(\boldsymbol{Z}_6, +)$ è quindi $g = \overline{3}_- \circ f$. Risulta:

$$g(1) = \overline{0},\ g(i) = (\overline{3}_-)(\tilde{1}) = \overline{3},\ g(-1) = (\overline{3}_-)(\tilde{1}) = \overline{0},\ g(-i) = (\overline{3}_-)(\tilde{3}) = \overline{3}.$$

Pertanto $Im(g) = \langle\overline{3}\rangle$ e $Ker(g) = \langle\overline{-1}\rangle$.

* * *

4.26. Determinare l'insieme $\boldsymbol{Hom}(\boldsymbol{C}_6, \boldsymbol{C}_{12})$. Di ciascuno dei 6 omomorfismi ottenuti indicare l'immagine ed il nucleo.

Soluzione. Sia $\boldsymbol{C}_6 = \langle\zeta\rangle$, con $\zeta = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6}$ e sia $\boldsymbol{C}_{12} = \langle\eta\rangle$, con $\eta = \cos\frac{2\pi}{12} + i\sin\frac{2\pi}{12}$.

È noto che $\boldsymbol{C}_6 \cong \boldsymbol{Z}_6$, tramite (ad esempio) un isomorfismo $f : \boldsymbol{C}_6 \to \boldsymbol{Z}_6$ tale che $\zeta^k \to \tilde{k}$ (con $k = 0, ..., 5$) mentre $\boldsymbol{C}_{12} \cong \boldsymbol{Z}_{12}$, tramite (ad esempio) un isomorfismo $g : \boldsymbol{C}_{12} \to \boldsymbol{Z}_{12}$ tale che $\eta^h \to \overline{h}$ (con $h = 0, ..., 11$).

Si ha quindi

$$\boldsymbol{Hom}(\boldsymbol{C}_6, \boldsymbol{C}_{12}) \cong \boldsymbol{Hom}(\boldsymbol{Z}_6, \boldsymbol{Z}_{12}) = \{\overline{k}_- : \boldsymbol{Z}_6 \to \boldsymbol{Z}_{12},\ :\ \circ(\overline{k}) \,\big|\, MCD(6,12) = 6\}.$$

Calcolati i periodi degli elementi di $\boldsymbol{Z}_{12}$, si osserva che

$$\circ(\overline{k}) \,\big|\, 6 \iff \circ(\overline{k}) = 1, 2, 3, 6 \iff \overline{k} \in \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\} = \{\overline{2h}_-,\ \forall\, h = 0, ..., 5\}.$$

I sei omomorfismi di $\boldsymbol{Hom}(\boldsymbol{C}_6, \boldsymbol{C}_{12})$ sono quindi, $\forall\, h = 0, ..., 5$:

$$\varphi_h := g^{-1} \circ (\overline{2h}_-) \circ f : \boldsymbol{C}_6 \to \boldsymbol{Z}_6 \to \boldsymbol{Z}_{12} \to \boldsymbol{C}_{12}$$

tale che

$$\zeta^k \to \tilde{k} \to \overline{2hk} \to \eta^{2hk} \quad (\text{con } k = 0, ..., 5)$$

[in particolare $\varphi_h(\zeta) = \eta^{2h}$]. Esaminiamo in dettaglio i sei omomorfismi:

$\varphi_0 : \boldsymbol{C}_6 \to \boldsymbol{C}_{12}$ tale che $\zeta \to 1$ ha $Ker(\varphi_0) = \boldsymbol{C}_6,\ Im(\varphi_0) = \langle 1 \rangle$ (omomorfismo banale);
$\varphi_1 : \boldsymbol{C}_6 \to \boldsymbol{C}_{12}$ tale che $\zeta \to \eta^2$ ha $Ker(\varphi_1) = \langle 1 \rangle,\ Im(\varphi_1) = \langle \eta^2 \rangle \cong \boldsymbol{C}_6$;
$\varphi_2 : \boldsymbol{C}_6 \to \boldsymbol{C}_{12}$ tale che $\zeta \to \eta^4$ ha $Ker(\varphi_2) = \langle \zeta^3 \rangle \cong \boldsymbol{C}_2,\ Im(\varphi_2) = \langle \eta^4 \rangle \cong \boldsymbol{C}_3$;
$\varphi_3 : \boldsymbol{C}_6 \to \boldsymbol{C}_{12}$ tale che $\zeta \to \eta^6$ ha $Ker(\varphi_3) = \langle \zeta^2 \rangle \cong \boldsymbol{C}_3,\ Im(\varphi_3) = \langle \eta^6 \rangle \cong \boldsymbol{C}_2$;
$\varphi_4 : \boldsymbol{C}_6 \to \boldsymbol{C}_{12}$ tale che $\zeta \to \eta^8$ ha $Ker(\varphi_4) = \langle \zeta^3 \rangle \cong \boldsymbol{C}_2,\ Im(\varphi_4) = \langle \eta^4 \rangle \cong \boldsymbol{C}_3$;
$\varphi_5 : \boldsymbol{C}_6 \to \boldsymbol{C}_{12}$ tale che $\zeta \to \eta^{10}$ ha $Ker(\varphi_5) = \langle 1 \rangle,\ Im(\varphi_5) = \langle \eta^2 \rangle \cong \boldsymbol{C}_6$.

* * *

4.27. Determinare gli endomorfismi di $(\boldsymbol{C}_5, \cdot)$ [gruppo delle radici quinte dell'unità] che non sono automorfismi.

Soluzione. Si tratta di determinare $\boldsymbol{\mathcal{E}nd}(\boldsymbol{C}_5) - \boldsymbol{\mathcal{A}ut}(\boldsymbol{C}_5)$. Poiché $\boldsymbol{C}_5 \cong \boldsymbol{Z}_5$, allora

$$\boldsymbol{\mathcal{A}ut}(\boldsymbol{C}_5) \cong \boldsymbol{\mathcal{A}ut}(\boldsymbol{Z}_5) \cong \boldsymbol{\mathcal{U}}(\boldsymbol{Z}_5) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\},$$

$$\boldsymbol{\mathcal{E}nd}(\boldsymbol{C}_5) \cong \boldsymbol{\mathcal{E}nd}(\boldsymbol{Z}_5) = \{\overline{k}_- : \boldsymbol{Z}_5 \to \boldsymbol{Z}_5,\ \forall\, \overline{k} \in \boldsymbol{Z}_5\}.$$

L'unico endomorfismo di $\boldsymbol{Z}_5$ che non è un automorfismo è quindi l'omomorfismo banale $\overline{0}_-$. Ad esso corrisponde l'omorfismo banale di $\boldsymbol{C}_5$, cioè l'applicazione

$$\boldsymbol{1} : \boldsymbol{C}_5 \to \boldsymbol{C}_5 \text{ tale che } \boldsymbol{1}(\zeta^k) = 1,\ \forall\, k = 1, ..., 4,$$

[con $\zeta = \cos\frac{2\pi}{5} + i \sin\frac{2\pi}{5}$].

* * *

4.28. Determinare gli insiemi $\boldsymbol{\mathcal{H}om}(\boldsymbol{S}_3, \boldsymbol{Z}_3)$ e $\boldsymbol{\mathcal{H}om}(\boldsymbol{Z}_3, \boldsymbol{S}_3)$.

Soluzione. Sia $f \in \boldsymbol{\mathcal{H}om}(\boldsymbol{S}_3, \boldsymbol{Z}_3)$. Per ogni 2-ciclo $(a, b) \in \boldsymbol{S}_3$, risulta che $\circ(f((a, b)))\big|2$. Tenuto conto che in $\boldsymbol{Z}_3$, $\circ(\overline{1}) = \circ(\overline{2}) = 3$, allora $f((a, b)) = \overline{0}$. Ne segue (essendo f un omomorfismo) che

$$f((1, 2, 3)) = f((1, 2)(1, 3)) = f((1, 2)) + f((1, 3)) = \overline{0} + \overline{0} = \overline{0},$$
$$f((1, 3, 2)) = f((1, 3)(1, 2)) = f((1, 3)) + f((1, 2)) = \overline{0} + \overline{0} = \overline{0}.$$

Dunque $f = \boldsymbol{0}$ (omomorfismo banale). Ne segue che $\boldsymbol{\mathcal{H}om}(\boldsymbol{S}_3, \boldsymbol{Z}_3)$ è formato dal solo omomorfismo banale.

Sia ora $f \in \boldsymbol{\mathcal{H}om}(\boldsymbol{Z}_3, \boldsymbol{S}_3)$. Essendo $\boldsymbol{Z}_3 = \langle \overline{1} \rangle$, f è completamente individuata da $f(\overline{1})$. Inoltre $\circ(f(\overline{1}))\big| \circ (\overline{1}) = 3$. Dunque $f(\overline{1}) \in \langle (1, 2, 3) \rangle$. Ne segue che $\boldsymbol{\mathcal{H}om}(\boldsymbol{Z}_3, \boldsymbol{S}_3)$ è formato dai tre omomorfismi:

$f_0 : \boldsymbol{Z}_3 \to \boldsymbol{S}_3$, tale che $f_0(\overline{1}) = (1),\ f_0(\overline{2}) = (1),\ f_0(\overline{0}) = (1)$;
$f_1 : \boldsymbol{Z}_3 \to \boldsymbol{S}_3$, tale che $f_1(\overline{1}) = (1, 2, 3),\ f_1(\overline{2}) = (1, 3, 2),\ f_1(\overline{0}) = (1)$;
$f_2 : \boldsymbol{Z}_3 \to \boldsymbol{S}_3$, tale che $f_2(\overline{1}) = (1, 3, 2),\ f_2(\overline{2}) = (1, 2, 3),\ f_2(\overline{0}) = (1)$.

* * *

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 $\boldsymbol{Z}_2 \times \boldsymbol{Z}_4$.

Soluzione. (*i*) Si ha:

$$\mathcal{U}(\boldsymbol{Z}_{15}) = \{\overline{k} \in \boldsymbol{Z}_{15} \ :\ 1 \le k < 15,\ MCD(k, 15) = 1\} = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$$

[si noti che $\varphi(15) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$]. Valutiamo i periodi degli elementi di $\mathcal{U}(\boldsymbol{Z}_{15})$:

$\circ(\overline{1}) = 1$;
$\circ(\overline{2}) = 4$ $[\overline{2}^2 \neq \overline{1};\ \overline{2}^4 = \overline{16} = \overline{1}]$;
$\circ(\overline{4}) = 2$ $[\overline{4}^2 = \overline{1}]$;
$\circ(\overline{7}) = 4$ $[\overline{7}^2 = \overline{49} = \overline{4} \neq \overline{1};\ \overline{7}^4 = \overline{4}^2 = \overline{1}]$;

$\circ(\overline{8}) = 4 \;\; [\overline{8}^2 = \overline{64} = \overline{4} \neq \overline{1};\; \overline{8}^4 = \overline{4}^2 = \overline{1}];$
$\circ(\overline{11}) = 2 \;\; [\overline{11}^2 = \overline{-4}^2 = \overline{1}];$
$\circ(\overline{13}) = 4 \;\; [\overline{13}^2 = \overline{-2}^2 = \overline{4} \neq \overline{1};\; \overline{13}^4 = \overline{4}^2 = \overline{1}];$
$\circ(\overline{14}) = 2 \;\; [\overline{14}^2 = \overline{-1}^2 = \overline{1}].$

Si nota subito che $\mathcal{U}(\boldsymbol{Z}_{15})$ non è ciclico [non ha elementi di periodo 8]. Invece $\mathcal{U}(\boldsymbol{Z}_{15})$ è abeliano [in quanto $\boldsymbol{Z}_{15}$ è un anello commutativo].

(*ii*) Assumiamo nota la struttura del prodotto diretto $\boldsymbol{Z}_2 \times \boldsymbol{Z}_4$. Osserviamo che gli elementi di $\mathcal{U}(\boldsymbol{Z}_{15})$ e di $\boldsymbol{Z}_2 \times \boldsymbol{Z}_4$ hanno gli stessi periodi [tre elementi di periodo 2 e quattro di periodo 4]. Per ottenere un isomorfismo bisogna far corrispondere elementi di ugual periodo.

In $\boldsymbol{Z}_2 \times \boldsymbol{Z}_4$ si ha:

$$\begin{array}{llll} \circ((\overline{0},\tilde{0})) = 1, & \circ((\overline{0},\tilde{1})) = 4, & \circ((\overline{0},\tilde{2})) = 2, & \circ((\overline{0},\tilde{3})) = 4, \\ \circ((\overline{1},\tilde{0})) = 2, & \circ((\overline{1},\tilde{1})) = 4, & \circ((\overline{1},\tilde{2})) = 2, & \circ((\overline{1},\tilde{3})) = 4. \end{array}$$

Inoltre $\boldsymbol{Z}_2 \times \boldsymbol{Z}_4$ ha due sottogruppi ciclici di ordine 4: $\langle(\overline{0},\tilde{1})\rangle$ e $\langle(\overline{1},\tilde{1})\rangle$, che si intersecano in $\langle(\overline{0},\tilde{2})\rangle$. Invece $\mathcal{U}(\boldsymbol{Z}_{15})$ ha i due ciclici $\langle\overline{2}\rangle = \{\overline{1}, \overline{2}, \overline{4}, \overline{8}\}$ e $\langle\overline{7}\rangle = \{\overline{1}, \overline{7}, \overline{4}, \overline{13}\}$, che si intersecano in $\langle\overline{4}\rangle$.

Un isomorfismo cercato $f : \mathcal{U}(\boldsymbol{Z}_{15}) \to \boldsymbol{Z}_2 \times \boldsymbol{Z}_4$ trasforma quindi $\overline{4}$ in $(\overline{0},\tilde{2})$ $[f(\overline{4}) = (\overline{0},\tilde{2})]$. Poniamo: $f(\overline{2}) = (\overline{0},\tilde{1}), \quad f(\overline{7}) = (\overline{1},\tilde{1})$. Allora:

$$\begin{aligned} &f(\overline{8}) = f(\overline{2}^3) = 3(\overline{0},\tilde{1}) = (\overline{0},\tilde{3}), \\ &f(\overline{13}) = f(\overline{7}^3) = 3(\overline{1},\tilde{1}) = (\overline{1},\tilde{3}), \\ &f(\overline{14}) = f(\overline{2}\cdot\overline{7}) = f(\overline{2}) + f(\overline{7}) = (\overline{0},\tilde{1}) + (\overline{1},\tilde{1}) = (\overline{1},\tilde{2}). \end{aligned}$$

f è per costruzione un omomorfismo ed è biiettiva.

* * *

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 $\boldsymbol{Z}_{12}$.

Soluzione. Denoteremo con $\overline{k}$ la classe resto di un intero k modulo 18 e con $\tilde{k}$ la classe resto di un intero k modulo 12.

(*i*) Risulta:

$$\boldsymbol{Hom}(\boldsymbol{Z}_{12}, \boldsymbol{Z}_{18}) = \left\{ \overline{k}_- : \boldsymbol{Z}_{12} \to \boldsymbol{Z}_{18} \text{ tali che } \circ(\overline{k}) \,\middle|\, MCD(12,18) = 6 \right\}$$

[dove $\overline{k}_-$ denota la moltiplicazione per $\overline{k}$, così definita: $\overline{k}_-(\tilde{t}) = \overline{kt},\ \forall\, \tilde{t} \in \boldsymbol{Z}_{12}$].

Gli elementi di $\boldsymbol{Z}_{18}$ aventi per periodo un divisore di 6 sono $\overline{0}$, $\overline{3}$, $\overline{6}$, $\overline{9}$, $\overline{12}$, $\overline{15}$. In corrispondenza esistono i sei omomorfismi da $\boldsymbol{Z}_{12}$ a $\boldsymbol{Z}_{18}$

$$\overline{3h}_- : \boldsymbol{Z}_{12} \to \boldsymbol{Z}_{18},\ \forall\, h = 0,1,2,3,4,5.$$

(*ii*) Risulta:

$$\boldsymbol{Hom}(\boldsymbol{Z}_{18}, \boldsymbol{Z}_{12}) = \left\{ \tilde{h}_- : \boldsymbol{Z}_{18} \to \boldsymbol{Z}_{12} \text{ tali che } \circ(\tilde{h}) \,\middle|\, MCD(12,18) = 6 \right\}.$$

Gli elementi di $\boldsymbol{Z}_{12}$ aventi per periodo un divisore di 6 sono $\tilde{0}$, $\tilde{2}$, $\tilde{4}$, $\tilde{6}$, $\tilde{8}$, $\tilde{10}$. In corrispondenza esistono i sei omomorfismi da $\boldsymbol{Z}_{18}$ a $\boldsymbol{Z}_{12}$

$$\widetilde{2h}_- : \boldsymbol{Z}_{18} \to \boldsymbol{Z}_{12},\ \forall\, h = 0,1,2,3,4,5.$$

(*iii*) Gli endomorfismi di $\boldsymbol{Z}_{12}$ che si fattorizzano tramite $\boldsymbol{Z}_{18}$ sono, $\forall\, h,k = 0,1,2,3,4,5$:

$$\widetilde{2h}_- \circ \overline{3k}_- : \boldsymbol{Z}_{12} \to \boldsymbol{Z}_{18} \to \boldsymbol{Z}_{12} \quad \text{tale che } \tilde{t} \to \overline{3kt} \to (\widetilde{6hkt}) = (\widetilde{6hk})\tilde{t}.$$

Se hk è pari, $\widetilde{6hk} = \tilde{0}$ e dunque l'endomorfismo ottenuto è quello banale. Se invece hk è dispari, $\widetilde{6hk} = \tilde{6}$ e dunque l'unico endomorfismo non banale ottenuto è

$$\tilde{6}_- : \boldsymbol{Z}_{12} \to \boldsymbol{Z}_{12} \quad \text{tale che } \tilde{6}_-(\tilde{t}) = \widetilde{6t},\ \forall\, \tilde{t} \in \boldsymbol{Z}_{12}.$$

* * *

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*) $\mathbf{GL}_n(\boldsymbol{R})/_{\mathbf{SL}_n(\boldsymbol{R})} \cong (\boldsymbol{R}^{\cdot}, \cdot)$.

Soluzione. (*i*) Basta verificare che, $\forall\, A \in \mathbf{GL}_n(\boldsymbol{R})$, risulta: $A\,\mathbf{SL}_n(\boldsymbol{R}) \subseteq \mathbf{SL}_n(\boldsymbol{R})\,A$.

Sia $B \in \mathbf{SL}_n(\boldsymbol{R})$ $[det(B) = 1]$. Allora $AB = AB(A^{-1}A) = (ABA^{-1})A$. Si ha: $det(ABA^{-1}) = det(A) \cdot 1 \cdot \frac{1}{det(A)} = 1$ e dunque $B_1 := ABA^{-1} \in \mathbf{SL}_n(\boldsymbol{R})$. Allora $AB = B_1A \in \mathbf{SL}_n(\boldsymbol{R})\,A$.

(*ii*) Sia $det : \mathbf{GL}_n(\boldsymbol{R}) \to \boldsymbol{R}^{\cdot}$ tale che $A \to det(A)$. Si ha: $det(A_1A_2) = det(A_1)det(A_2)$ e dunque det è un omomorfismo. Ovviamente det è suriettivo [infatti $r = det(\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix})$, $\forall\, r \in \boldsymbol{R}^{\cdot}$]. Infine

$$Ker(det) = \{A \in \mathbf{GL}_n(\boldsymbol{R}) \ : \ det(A) = 1\} = \mathbf{SL}_n(\boldsymbol{R}).$$

Si conclude, dal teorema fondamentale di omomorfismo, che $\mathbf{GL}_n(\boldsymbol{R})/_{\mathbf{SL}_n(\boldsymbol{R})} \cong (\boldsymbol{R}^{\cdot}, \cdot)$.

* * *

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 $\boldsymbol{\mathcal{A}ut}(\boldsymbol{S}_3)/_{\boldsymbol{\mathcal{I}}(\boldsymbol{S}_3)}$.

Soluzione. (*i*) Il centro $\boldsymbol{\mathcal{Z}}(\boldsymbol{S}_3)$ è il sottogruppo delle permutazioni di $\boldsymbol{S}_3$ che commutano con ogni permutazione di $\boldsymbol{S}_3$. Ovviamente $(1) \in \boldsymbol{\mathcal{Z}}(\boldsymbol{S}_3)$. Poiché

$$(1,\,2)(1,\,2,\,3) \neq (1,\,2,\,3)(1,\,2), \quad (1,\,3)(2,\,3) \neq (2,\,3)(1,\,3),$$

allora $(1,\,2)$, $(1,\,3)$, $(2,\,3)$, $(1,\,2,\,3) \notin \boldsymbol{\mathcal{Z}}(\boldsymbol{S}_3)$. Ne segue che $\boldsymbol{\mathcal{Z}}(\boldsymbol{S}_3) = \{(1)\}$. Poiché $\boldsymbol{\mathcal{I}}(\boldsymbol{S}_3) \cong \boldsymbol{S}_3/_{\boldsymbol{\mathcal{Z}}(\boldsymbol{S}_3)}$, segue che $\boldsymbol{\mathcal{I}}(\boldsymbol{S}_3) \cong \boldsymbol{S}_3$.

(*ii*) $\forall\, f \in \boldsymbol{\mathcal{A}ut}(\boldsymbol{S}_3)$, si ha

$$f((1,\,2) \in \{(1,\,2),\,(1,\,3),\,(2,\,3)\} \ \text{ e } \ f((1,\,2,\,3) \in \{(1,\,2,\,3),\,(1,\,3,\,2)\}.$$

Poiché $\boldsymbol{S}_3 = \langle (1,\,2), (1,\,2,\,3) \rangle$, f è completamente individuato da $f((1,\,2))$, $f((1,\,2,\,3))$. Dunque $\boldsymbol{\mathcal{A}ut}(\boldsymbol{S}_3)$ ha al più sei elementi. D'altra parte $\boldsymbol{\mathcal{A}ut}(\boldsymbol{S}_3)$ possiede sei automorfismi interni. Dunque $\boldsymbol{\mathcal{A}ut}(\boldsymbol{S}_3) = \boldsymbol{\mathcal{I}}(\boldsymbol{S}_3) \cong \boldsymbol{S}_3$ e $\boldsymbol{\mathcal{A}ut}(\boldsymbol{S}_3)/_{\boldsymbol{\mathcal{I}}(\boldsymbol{S}_3)} \cong \{1\}$.

Nota. Ad esempio, l'automorfismo interno $\gamma = \gamma_{(123)}$ è il seguente:

$$\begin{aligned}
&\gamma((1,\,2)) = (1,\,2,\,3)(1,\,2)(1,\,3,\,2) = (1,\,3),\\
&\gamma((1,\,3)) = (1,\,2,\,3)(1,\,3)(1,\,3,\,2) = (2,\,3),\\
&\gamma((2,\,3)) = (1,\,2,\,3)(2,\,3)(1,\,3,\,2) = (1,\,2),\\
&\gamma((1,\,2,\,3)) = (1,\,2,\,3)(1,\,2,\,3)(1,\,3,\,2) = (1,\,2,\,3),\\
&\gamma((1,\,3,\,2)) = (1,\,2,\,3)(1,\,3,\,2)(1,\,3,\,2) = (1,\,3,\,2).
\end{aligned}$$

* * *

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.

Soluzione. (*i*) Risulta:

$$\boldsymbol{D}_4 = \langle \varphi, \rho \mid \varphi^4 = \rho^2 = 1;\ \rho \circ \varphi = \varphi^3 \circ \rho \rangle = \{1,\,\varphi,\,\varphi^2,\,\varphi^3,\,\rho,\,\varphi\circ\rho,\,\varphi^2\circ\rho,\,\varphi^3\circ\rho\}.$$

Si osservi che

$\rho,\,\varphi \notin \boldsymbol{\mathcal{Z}}(\boldsymbol{D}_4)$ [infatti $\varphi \circ \rho \neq \rho \circ \varphi$];
$\varphi^3 \notin \boldsymbol{\mathcal{Z}}(\boldsymbol{D}_4)$ [infatti $\varphi^3 \circ \rho \neq \rho \circ \varphi^3$];

$\varphi\circ\rho \notin \boldsymbol{\mathcal{Z}}(\boldsymbol{D}_4)$ [infatti $\varphi\circ(\varphi\circ\rho) \neq (\varphi\circ\rho)\circ\varphi$];
$\varphi^2\circ\rho \notin \boldsymbol{\mathcal{Z}}(\boldsymbol{D}_4)$ [infatti $\varphi\circ(\varphi^2\circ\rho) \neq (\varphi^2\circ\rho)\circ\varphi$];
$\varphi^3\circ\rho \notin \boldsymbol{\mathcal{Z}}(\boldsymbol{D}_4)$ [infatti $\varphi\circ(\varphi^3\circ\rho) \neq (\varphi^3\circ\rho)\circ\varphi$].

Invece $\varphi^2 \in \boldsymbol{\mathcal{Z}}(\boldsymbol{D}_4)$. Infatti:

$\varphi^2\circ\varphi = \varphi\circ\varphi^2$, $\varphi^2\circ\varphi^3 = \varphi^3\circ\varphi^2$, $\varphi^2\circ\rho = \rho\circ\varphi^2$,
$\varphi^2\circ(\varphi\circ\rho) = (\varphi\circ\rho)\circ\varphi^2$, $\varphi^2\circ(\varphi^2\circ\rho) = (\varphi^2\circ\rho)\circ\varphi^2$, $\varphi^2\circ(\varphi^3\circ\rho) = (\varphi^3\circ\rho)\circ\varphi^2$.

Si conclude che $\boldsymbol{\mathcal{Z}}(\boldsymbol{D}_4) = \langle\varphi^2\rangle$ (gruppo ciclico di ordine 2).

(*ii*) Risulta:

$$\boldsymbol{\mathcal{I}}(\boldsymbol{D}_4) \cong \boldsymbol{D}_4\big/_{\boldsymbol{\mathcal{Z}}(\boldsymbol{D}_4)} = \boldsymbol{D}_4\big/_{\langle\varphi^2\rangle} = \big\{\langle\varphi^2\rangle,\, \langle\varphi^2\rangle\varphi,\, \langle\varphi^2\rangle\rho,\, \langle\varphi^2\rangle(\varphi\circ\rho)\big\}$$

Risulta:

$\big(\langle\varphi^2\rangle\varphi\big)\big(\langle\varphi^2\rangle\varphi\big) = \langle\varphi^2\rangle\varphi^2 = \langle\varphi^2\rangle$;
$\big(\langle\varphi^2\rangle\rho\big)\big(\langle\varphi^2\rangle\rho\big) = \langle\varphi^2\rangle\rho^2 = \langle\varphi^2\rangle$;
$\big(\langle\varphi^2\rangle(\varphi\circ\rho)\big)\big(\langle\varphi^2\rangle(\varphi\circ\rho)\big) = \langle\varphi^2\rangle(\varphi\circ\rho)^2 = \langle\varphi^2\rangle$.

Dunque i tre elementi $\neq \langle\varphi^2\rangle$ di $\boldsymbol{\mathcal{I}}(\boldsymbol{D}_4)$ hanno periodo 2. Pertanto $\boldsymbol{\mathcal{I}}(\boldsymbol{D}_4)$ è un gruppo di Klein $\boldsymbol{V}$.

(*iii*) I quattro automorfismi interni di $\boldsymbol{D}_4$ sono:

$$\mathbf{1} = \gamma_1,\quad \gamma_\varphi,\quad \gamma_\rho,\quad \gamma_{\varphi\circ\rho}.$$

Calcoliamone le immagini su φ, ρ [generatori di $\boldsymbol{D}_4$]. Si ha:

$\mathbf{1}(\varphi) = \varphi$, $\mathbf{1}(\rho) = \rho$;
$\gamma_\varphi(\varphi) = \varphi\circ\varphi\circ\varphi^3 = \varphi$, $\gamma_\varphi(\rho) = \varphi\circ\rho\circ\varphi^3 = \varphi^2\circ\rho$;
$\gamma_\rho(\varphi) = \rho\circ\varphi\circ\rho = \varphi^3$, $\gamma_\rho(\rho) = \rho\circ\rho\circ\rho = \rho$;
$\gamma_{\varphi\circ\rho}(\varphi) = (\varphi\circ\rho)\circ\varphi\circ(\varphi\circ\rho) = \varphi^3$, $\gamma_{\varphi\circ\rho}(\rho) = (\varphi\circ\rho)\circ\rho\circ = \varphi^2\circ\rho$.

(*iv*) Sia $f \in \boldsymbol{Aut}(\boldsymbol{D}_4)$. Tenuto conto che $\circ(f(\varphi)) = 4$, allora $f(\varphi) \in \{\varphi, \varphi^3\}$. In ogni caso, $f(\varphi^2) = \varphi^2$. Tenuto poi conto che $\circ(f(\rho)) = 2$, allora $f(\rho) \in \{\rho, \varphi\circ\rho, \varphi^2\circ\rho, \varphi^3\circ\rho\}$. Si noti infine che gli automorfismi di $\boldsymbol{D}_4$ sono al più otto e di essi quattro sono interni.

Consideriamo l'applicazione

$$f : \boldsymbol{D}_4 \to \boldsymbol{D}_4 \quad \text{tale che} \quad f(\varphi) = \varphi,\ f(\rho) = \varphi\circ\rho,$$

ed estendiamola a $\boldsymbol{D}_4$ usando le regole di omomorfismo. Si ha:

$f(\varphi^2) = \varphi^2$, $f(\varphi^3) = \varphi^3$, $f(\varphi^4) = f(1) = 1$, $f(\rho^2) = f(1) = 1$,
$f(\varphi\circ\rho) = f(\varphi)\circ f(\rho) = \varphi^2\circ\rho$, $f(\varphi^2\circ\rho) = f(\varphi^2)\circ f(\rho) = \varphi^3\circ\rho$, $f(\varphi^3\circ\rho) = f(\varphi^3)\circ f(\rho) = \rho$.

Inoltre f è compatibile con la relazione $\rho\circ\varphi = \varphi^3\circ\rho$. Infatti: $f(\rho\circ\varphi) = f(\rho)\circ f(\varphi) = \rho = f(\varphi^3\circ\rho)$.

Si conclude che $f \in \boldsymbol{Aut}(\boldsymbol{D}_4) - \boldsymbol{\mathcal{I}}(\boldsymbol{D}_4)$.

Nota. Si può facilmente verificare che $\circ(f) = 4$ e, dal teorema di Lagrange, che $|\boldsymbol{Aut}(\boldsymbol{D}_4)| = 8$. I tre ulteriori automorfismi di $\boldsymbol{D}_4$ sono f^3, g, h, dove g, h sono definiti (sui generatori) in questo modo:

$$g(\varphi) = \varphi^3,\ g(\rho) = \varphi\circ\rho; \quad h(\varphi) = \varphi^3,\ h(\rho) = \rho.$$

Dall'esame dei periodi degli automorfismi ottenuti, si conclude che $\boldsymbol{Aut}(\boldsymbol{D}_4) \cong \boldsymbol{D}_4$.

* * *

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 $\boldsymbol{T}$.

Soluzione. (*i*) Per ogni $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $A' = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \in \boldsymbol{T}$, si ha:

$$A(A')^{-1} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} \frac{1}{a'} & \frac{-b'}{a'c'} \\ 0 & \frac{1}{c'} \end{pmatrix} = \begin{pmatrix} \frac{a}{a'} & \frac{-ab'+ba'}{a'c'} \\ 0 & \frac{c}{c'} \end{pmatrix} \in \boldsymbol{T}$$

e dunque $\boldsymbol{T}$ è un sottogruppo di $\boldsymbol{GL}_2(\boldsymbol{Q})$.

(*ii*) È sufficiente verificare che ad esempio $B\boldsymbol{T} \not\subset \boldsymbol{T}B$. Scelta in $\boldsymbol{T}$ proprio la matrice A_0, basta quindi verificare che $BA_0 \notin \boldsymbol{T}B$.

Per assurdo, esista $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in \boldsymbol{T}$ tale che $BA_0 = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} B$. Allora

$$BA_0 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} x+y & y \\ z & z \end{pmatrix}.$$

Ne segue che $1 = z = 2$: assurdo.

(*iii*) Risulta: $\boldsymbol{H} = \langle A_0 \rangle = \{A_0^t,\ \forall\, t \in \boldsymbol{Z}\}$. Poiché

$$A_0^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},\ A_0^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix},\ \text{allora}\ A_0^t = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix},\ \forall\, t \in \mathbf{Z}.$$

Si noti che $\boldsymbol{H} \cong (\boldsymbol{Z}, +)$ (gruppo ciclico infinito). Ovviamente $\boldsymbol{H}$ è un sottogruppo di $\boldsymbol{T}$ [essendo un sottogruppo di $\boldsymbol{GL}_2(\boldsymbol{Q})$ ed un sottoinsieme di $\boldsymbol{T}$].

(*iv*) Basta verificare se, $\forall \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \boldsymbol{T}$, risulta:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \boldsymbol{H} \subseteq \boldsymbol{H} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},$$

cioè se, $\forall\, t \in \boldsymbol{Z}$, esiste $x = x(t) \in \boldsymbol{Z}$ tale che

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},$$

ovvero tale che $\begin{pmatrix} a & at+b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & b+cx \\ 0 & c \end{pmatrix}$. Tali matrici coincidono $\iff at = cx$.

Scelti ad esempio $a = 1$, $c = 2$, $t = 3$, non esiste $x \in \boldsymbol{Z}$ tale che $1 \cdot 3 = 2x$. Dunque $\boldsymbol{H}$ non è normale in $\boldsymbol{T}$.

* * *

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 $\boldsymbol{T}$.

Soluzione. (*i*) [Cfr. **Esercizio 30**(*i*),(*ii*)].

(*ii*) Verifichiamo che $\boldsymbol{H}_1 \leq \mathbf{GL}_2(\boldsymbol{R})$ [e quindi $\boldsymbol{H}_1 \leq \boldsymbol{T}$, essendo $\boldsymbol{H}_1 \subseteq \boldsymbol{T}$].

Infatti, per ogni $A_1 = \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix},\ A_2 = \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} \in \boldsymbol{H}_1$, si ha:

$$A_1 A_2^{-1} = \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} \frac{1}{a_2} & 0 \\ 0 & \frac{1}{b_2} \end{pmatrix} = \begin{pmatrix} \frac{a_1}{a_2} & 0 \\ 0 & \frac{b_1}{b_2} \end{pmatrix} \in \boldsymbol{H}_1.$$

Scelta in $\boldsymbol{T}$ la matrice $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, basterà verificare che $A\boldsymbol{H}_1 \not\subseteq \boldsymbol{H}_1 A$ [per concludere che $\boldsymbol{H}_1$ non è normale in $\boldsymbol{T}$]. Scelta ad esempio in $\boldsymbol{T}$ la matrice $B = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, allora $AB = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$. Se per assurdo $AB \in \boldsymbol{H}_1 A$, $\exists \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \in \boldsymbol{H}_1$ tale che $AB = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & x \\ 0 & y \end{pmatrix}$. Dunque $\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} x & x \\ 0 & y \end{pmatrix}$ e quindi in particolare, $x = 1 = 2$: assurdo.

(*iii*) Verifichiamo che $\boldsymbol{H}_2 \leq \boldsymbol{T}$. Per ogni $B_1 = \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}$, $B_2 = \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} \in \boldsymbol{H}_2$, si ha $B_1B_2 = \begin{pmatrix} 1 & b_1+b_2 \\ 0 & 1 \end{pmatrix} \in \boldsymbol{H}_2$; inoltre $I_2 \in \boldsymbol{H}_2$ e $B_1^{-1} = \begin{pmatrix} 1 & -b_1 \\ 0 & 1 \end{pmatrix} \in \boldsymbol{H}_2$. Dunque $\boldsymbol{H}_2 \leq \mathbf{GL}_2(\boldsymbol{R})$ e quindi $\boldsymbol{H}_2 \leq \boldsymbol{T}$.

Per verificare che $\boldsymbol{H}_2 \lhd \boldsymbol{T}$, bisogna verificare che per ogni $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \boldsymbol{T}$ $(ac \neq 0)$, risulta $A\boldsymbol{H}_2 \subseteq \boldsymbol{H}_2 A$.

Per ogni $B = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \in \boldsymbol{H}_2$, risulta $AB = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & ak+b \\ 0 & c \end{pmatrix}$. Bisogna verificare che esiste $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in \boldsymbol{H}_2$ tale che $AB = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & b+cx \\ 0 & c \end{pmatrix}$. Confrontando le matrici ottenute, segue che $b + cx = ak + b$, da cui $x = \frac{ak}{c}$ [si noti che $c \neq 0$, perché $ac \neq 0$]. Segue che $AB \in \boldsymbol{H}_2 A$, cioè $A\boldsymbol{H}_2 \subseteq \boldsymbol{H}_2 A$.

* * *

4.36. [*Esame 10/6/03*] Sia $(\boldsymbol{G}, \cdot)$ un gruppo e sia $g_0 \in \boldsymbol{G}$. Si ponga:

$$\boldsymbol{C}(g_0) := \{g \in \boldsymbol{G} \ : \ g_0\, g = g\, g_0\}$$

[$\boldsymbol{C}(g_0)$ 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 $\boldsymbol{C}(\rho)$.

Soluzione. (*i*) Risulta:

$1 \in \boldsymbol{C}(g_0)$. Infatti $1 \cdot g_0 = g_0 \cdot 1$.

$g, g' \in \boldsymbol{C}(g_0) \Longrightarrow gg' \in \boldsymbol{C}(g_0)$. Infatti $(gg')g_0 = g(g'g_0) = g(g_0g') = (gg_0)g' = (g_0g)g' = g_0(gg')$.

$g \in \boldsymbol{C}(g_0) \Longrightarrow g^{-1} \in \boldsymbol{C}(g_0)$. Infatti, moltiplicando a destra e a sinistra l'uguaglianza $gg_0 = g_0g$ per g^{-1}, si ha: $g^{-1}(gg_0)g^{-1} = g^{-1}(g_0g)g^{-1}$, da cui $(g^{-1}g)(g_0g^{-1}) = (g^{-1}g_0)(gg^{-1})$, cioè $g_0g^{-1} = g^{-1}g_0$.

(*ii*) Per ogni $h \in \boldsymbol{Z}$, $g_0^h \in \boldsymbol{C}(g_0)$. Infatti

$$g_0^h g_0 = g_0^{h+1} = g_0 g_0^h.$$

Dunque $\langle g_0 \rangle \leq \boldsymbol{C}(g_0)$.

(*iii*) Ovviamente $\boldsymbol{C}(\varphi) \geq \langle \varphi \rangle = \{1, \varphi, \varphi^2, \varphi^3\}$. Inoltre $\rho \notin \boldsymbol{C}(\varphi)$ [infatti $\varphi \circ \rho \neq \rho \circ \varphi$]. Ne segue che $\boldsymbol{C}(\varphi) < \boldsymbol{D}_4$ e quindi, per ragioni di ordine, $\boldsymbol{C}(\varphi) = \langle \varphi \rangle$.

Si osservi che $\varphi^2 \in \boldsymbol{C}(\rho)$ [infatti $\varphi^2 \circ \rho = \rho \circ \varphi^2$]. Inoltre ovviamente $\rho \in \boldsymbol{C}(\rho)$ mentre $\varphi \notin \boldsymbol{C}(\rho)$. Ne segue che $\boldsymbol{C}(\rho) \supseteq \{1, \rho, \varphi^2, \varphi^2 \circ \rho\}$. Poiché $\boldsymbol{C}(\rho) < \boldsymbol{D}_4$, allora $\boldsymbol{C}(\rho) = \{1, \rho, \varphi^2, \varphi^2 \circ \rho\}$ (gruppo di Klein).

* * *

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 $\boldsymbol{Aut}(G)$ e $\boldsymbol{Aut}(G')$ sono isomorfi, esplicitando un isomorfismo tra essi.

(*ii*) Indicato con $\boldsymbol{Isom}(G, G')$ l'insieme degli isomorfismi da G a G', determinare una biiezione tra $\boldsymbol{Isom}(G, G')$ e $\boldsymbol{Aut}(G)$.

(*iii*) Verificare che $\boldsymbol{Aut}(\boldsymbol{Z}_9)$ e $\boldsymbol{Aut}(\boldsymbol{Z}_7)$ sono gruppi isomorfi. Quanti isomorfismi esistono tra tali gruppi?

Soluzione. (*i*) Sia $\varphi : \boldsymbol{Aut}(G) \to \boldsymbol{Aut}(G')$ l'applicazione così definita:

$$\varphi(f) = f_0 \circ f \circ f_0^{-1},\ \forall\, f \in \mathcal{A}ut(G).$$

Si noti che $f_0 \circ f \circ f_0^{-1}$ è un automorfismo in quanto composizione di isomorfismi; il suo inverso è l'applicazione $\psi : \boldsymbol{Aut}(G') \to \boldsymbol{Aut}(G)$ tale che $\psi(f') = f_0^{-1} \circ f' \circ f_0$, $\forall\, f' \in \boldsymbol{Aut}(G')$. Verifichiamo che φ è un omomorfismo di gruppi. Risulta, $\forall\, f, f' \in \boldsymbol{Aut}(G)$:

$$\varphi(f \circ f') = f_0 \circ (f \circ f') \circ f_0^{-1} = f_0 \circ (f \circ f_0^{-1} \circ f_0 \circ f') \circ f_0^{-1} =$$
$$= (f_0 \circ f \circ f_0^{-1}) \circ (f_0 \circ f' \circ f_0^{-1}) = \varphi(f) \circ \varphi(f').$$

(*ii*) Sia $\Phi : \boldsymbol{Aut}(G) \to \boldsymbol{Isom}(G, G')$ l'applicazione così definita:

$$\Phi(f) = f_0 \circ f,\ \forall\, f \in \boldsymbol{Aut}(G).$$

Φ è un'applicazione biiettiva, con inversa

$$\Psi : \boldsymbol{Isom}(G, G') \to \boldsymbol{Aut}(G) \text{ tale che } \Psi(h) = f_0^{-1} \circ h,\ \forall\, h \in \boldsymbol{Isom}(G, G').$$

(*iii*) Risulta:

$$\boldsymbol{Aut}(\boldsymbol{Z}_9) \cong \mathcal{U}_9 = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}, \quad \boldsymbol{Aut}(\boldsymbol{Z}_7) \cong \mathcal{U}_7 = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}.$$

In $\mathcal{U}_9$: $\overline{2}^2 = \overline{4} \neq \overline{1}$; $\overline{2}^3 = \overline{8} \neq \overline{1}$. Dunque $\circ(\overline{2}) = 6$ e quindi $\mathcal{U}_9 \cong \boldsymbol{C}_6$ (ciclico di ordine 6).
In $\mathcal{U}_7$: $\overline{3}^2 = \overline{2} \neq \overline{1}$; $\overline{3}^3 = \overline{6} \neq \overline{1}$. Dunque $\circ(\overline{3}) = 6$ e quindi anche $\mathcal{U}_7 \cong \boldsymbol{C}_6$.
È quindi dimostrato che $\boldsymbol{Aut}(\boldsymbol{Z}_9) \cong \boldsymbol{C}_6 \cong \boldsymbol{Aut}(\boldsymbol{Z}_7)$.

Da (*ii*), gli insiemi

$$\boldsymbol{Isom}(\boldsymbol{Aut}(\boldsymbol{Z}_9), \boldsymbol{Aut}(\boldsymbol{Z}_7)) \text{ e } \boldsymbol{Aut}(\boldsymbol{Aut}(\boldsymbol{Z}_9))$$

sono in corrspondenza biunivoca. Inoltre, da (*i*),

$$\boldsymbol{Aut}(\boldsymbol{Aut}(\boldsymbol{Z}_9)) \cong \boldsymbol{Aut}(\boldsymbol{C}_6) \cong \boldsymbol{Aut}(\boldsymbol{Z}_6) \cong \mathcal{U}_6 \cong \boldsymbol{C}_2.$$

Ne segue che gli isomorfismi tra $\boldsymbol{Aut}(\boldsymbol{Z}_9)$ e $\boldsymbol{Aut}(\boldsymbol{Z}_7)$ sono due.

* * *

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 $G/_H \cong H'$.

Soluzione. (*i*) Risulta:

$$G = \mathcal{U}(\boldsymbol{Z}_{21}) = \{\overline{a} \in \boldsymbol{Z}_{21} :\ (a, 21) = 1\} = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{8}, \overline{10}, \overline{11}, \overline{13}, \overline{16}, \overline{17}, \overline{19}, \overline{20}\},$$
$$G' = \boldsymbol{A}_4 = \left\{ \begin{array}{l} (1), (123), (132), (124), (142), (134), (143), \\ (234), (243), (12)(34), (13)(24), (14)(23) \end{array} \right\}.$$

I due gruppi hanno lo stesso ordine 12, ma $\mathcal{U}(\boldsymbol{Z}_{21})$ è commutativo, mentre $\boldsymbol{A}_4$ non lo è. Dunque non sono isomorfi.

(*ii*) I divisori positivi di 12 sono: $1, 2, 3, 4, 6, 12$.

Per $d = 1$, basta scegliere i due sottogruppi banali $\{\overline{1}\}$ e $\{(1)\}$. I divisori $d = 6$, 12 vanno esclusi perché $\boldsymbol{A}_4$ non ha sottogruppi di ordine 6 e $G \ncong G'$. Per ottenere gruppi isomorfi di ordini $d = 2$, 3, basta determinare nei due gruppi elementi di periodo 2 e 3. In $\mathcal{U}(\boldsymbol{Z}_{21})$ ad esempio $\overline{20}$ ha periodo 2 mentre $\overline{4}$ ha periodo 3; in $\boldsymbol{A}_4$ ad esempio $(12)(34)$ ha periodo 2 mentre (123) ha periodo 3. Dunque $\langle\overline{20}\rangle \cong \langle(12)(34)\rangle$ e $\langle\overline{4}\rangle \cong \langle(123)\rangle$.

Resta da esaminare il divisore $d = 4$. $\boldsymbol{A}_4$ ha un unico sottogruppo di ordine 4, isomorfo al gruppo di Klein: è il gruppo

$$K = \{(1),\ (12)(34), (13)(24), (14)(23)\}.$$

Si verifica subito che in $\mathcal{U}(\boldsymbol{Z}_{21})$ l'insieme

$$H = \{\overline{1}, \overline{20}, \overline{8}, \overline{13}\}$$

è anch'esso un gruppo di Klein. H e K sono dunque sottogruppi isomorfi.

(*iii*) Considerato in $\mathcal{U}(\boldsymbol{Z}_{21})$ il sottogruppo H sopra definito, si osserva subito che il gruppo quoziente $\mathcal{U}(\boldsymbol{Z}_{21})/_H$ ha ordine 3 e dunque è necessariamente isomorfo al sottogruppo $\langle(123)\rangle$ di $\boldsymbol{A}_4$.

* * *

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.

Soluzione. (*i*) I tre sottoinsiemi S_i contengono $\overline{0}$ e l'opposto di ogni loro elemento. Ne segue, $\forall\, i = 1, 2, 3$:

$\overline{a}\,\rho_i\,\overline{a},\ \forall\,\overline{a} \in \boldsymbol{Z}_{18}$ [infatti $\overline{a} - \overline{a} = \overline{0} \in S_i$];

$\overline{a}\,\rho_i\,\overline{b} \Longrightarrow \overline{b}\,\rho_i\,\overline{a},\ \forall\,\overline{a}, \overline{b} \in \boldsymbol{Z}_{18}$ [infatti $\overline{a} - \overline{b} \in S_i \Longrightarrow \overline{b} - \overline{a} \in S_i$];

Le tre relazioni sono riflessive e simmetriche.

Si osservi che S_2 è un sottogruppo di $(\boldsymbol{Z}_{18}, +)$ [mentre S_1 e S_3 non lo sono]. Ne segue che ρ_2 è anche transitiva. Infatti, se $\overline{a}\,\rho_2\,\overline{b}$ e $\overline{b}\,\rho_2\,\overline{c}$, allora $\overline{a}-\overline{b}$, $\overline{b}-\overline{c} \in S_2$ e dunque $\overline{a}-\overline{c} = (\overline{a}-\overline{b})+(\overline{b}-\overline{c}) \in S_2$, cioè $\overline{a}\,\rho_2\,\overline{c}$.

Invece ρ_1 e ρ_3 non sono transitive. Infatti

$$\overline{11}\,\rho_1\,\overline{6},\ \overline{6}\,\rho_1\,\overline{1} \ \text{ ma } \overline{11}\ \not\rho_1\,\overline{1}; \quad \overline{15}\,\rho_3\,\overline{8},\ \overline{8}\,\rho_3\,\overline{1} \ \text{ ma } \overline{15}\ \not\rho_3\,\overline{1}.$$

(*ii*) La relazione d'equivalenza ρ_2 è la relazione d'equivalenza associata al sottogruppo (normale) $\langle\overline{6}\rangle$ di $(\boldsymbol{Z}_{18}, +)$. Risulta quindi:

$$\boldsymbol{Z}_{18}/_{\rho_2} = \big\{\langle\overline{6}\rangle = S_2,\, \overline{1} + \langle\overline{6}\rangle,\, \overline{2} + \langle\overline{6}\rangle,\, \overline{3} + \langle\overline{6}\rangle,\, \overline{4} + \langle\overline{6}\rangle,\, \overline{5} + \langle\overline{6}\rangle\big\}.$$

Si consideri l'intervallo $\boldsymbol{I}_6 = \{0, 1, 2, 3, 4, 5\}$ e l'applicazione $\varphi : \boldsymbol{Z}_{18} \to \boldsymbol{I}_6$ tale che

$$\varphi(\overline{a}) = r, \ \text{ se } a = 6q + r,\ 0 \le r < 6,\ \forall\,\overline{a} \in \boldsymbol{Z}_{18}\,.$$

φ è ovviamente suriettiva ed è ben definita [se $\overline{a}' = \overline{a}$, $\varphi(\overline{a}') = \varphi(\overline{a}) = r$]. Risulta:

$$\overline{a}\,\rho_\varphi\,\overline{b} \iff \varphi(\overline{a}) = \varphi(\overline{b}) \iff a \equiv b\ (mod\,6) \iff \overline{a} - \overline{b} \in \langle\overline{6}\rangle \iff \overline{a}\,\rho_2\,\overline{b}.$$

Dunque $\rho_\varphi = \rho_2$ e φ è un'applicazione cercata.

La biiezione $\varphi^* : \boldsymbol{Z}_{18}/_{\rho_2} \to \boldsymbol{I}_6$ è così definita:

$$\varphi^*\big(\overline{t} + \langle\overline{6}\rangle\big) = \varphi(\overline{t}) = t,\ \forall\, t = 0, \dots, 5.$$

* * *

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.

Soluzione. Si considerino in $(\boldsymbol{Z}_{12}, +)$ i due seguenti sottogruppi:

$$H = \langle\overline{2}\rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}, \quad K = \langle\overline{3}\rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}.$$

Entrambi sono ovviamente normali. Il secondo teorema di isomorfismo afferma che:

$$(H + K)/_H \cong K/_{H\cap K}$$

[si noti che, in struttura additiva, il prodotto HK coincide con $H + K$]. Si ha:

$$H \cap K = \langle\overline{2}\rangle \cap \langle\overline{3}\rangle = \langle\overline{6}\rangle, \quad H + K = \langle\overline{2}\rangle + \langle\overline{3}\rangle = \langle\overline{1}\rangle = \boldsymbol{Z}_{12}\,.$$

Allora:

$$\langle\overline{3}\rangle/_{\langle\overline{6}\rangle} \cong \langle\overline{1}\rangle/_{\langle\overline{2}\rangle}.$$

Denotiamo con Φ tale isomorfismo. Esso è indotto dall'epimorfismo $\varphi : \langle\overline{3}\rangle \to \boldsymbol{Z}_{12}/_{\langle\overline{2}\rangle}$ tale che $\overline{3}t \to \overline{3}t + \langle\overline{2}\rangle$, [con $0 \le t \le 3$], cioè

$$\overline{0} \to \langle\overline{2}\rangle,\ \ \overline{3} \to \overline{3} + \langle\overline{2}\rangle = \overline{1} + \langle\overline{2}\rangle,\ \ \overline{6} \to \overline{6} + \langle\overline{2}\rangle = \langle\overline{2}\rangle,\ \ \overline{9} \to \overline{9} + \langle\overline{2}\rangle = \overline{1} + \langle\overline{2}\rangle.$$

Allora Φ opera in questo modo:

$$\overline{0} + \langle\overline{6}\rangle \to \langle\overline{2}\rangle,\ \ \overline{3} + \langle\overline{6}\rangle \to \overline{1} + \langle\overline{2}\rangle.$$

* * *

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.

Soluzione. (*i*) Essendo G non ciclico, dal teorema di Lagrange segue che $\circ(x) = 3,\ \forall\, x \in G,\ x \neq 1$. Siano a, b due elementi di G, di periodo 3 e non legati tra loro da alcuna relazione algebrica. Allora G contiene i seguenti elementi

$$1,\ a,\ a^2,\ b,\ b^2,\ ab,\ a^2b,\ ab^2,\ a^2b^2,\ ba,\ ba^2,\ b^2a,\ b^2a^2$$

Si verifica facilmente che i primi nove elementi sono a due a due distinti. Ad esempio a^2b^2 è diverso dagli otto elementi che lo precedono in quanto:

- $a^2b^2 = 1 \implies a^2a = 1 = a^2b^2 \implies a = b^2$;
- $a^2b^2 = a \implies ab^2 = 1 \implies a = b$;
- $a^2b^2 = a^2 \implies b^2 = 1$;
- $a^2b^2 = b \implies a^2b = 1 \implies b = a$;
- $a^2b^2 = b^2 \implies a^2 = 1$;
- $a^2b^2 = ab \implies ab = 1 \implies b = a^2$;
- $a^2b^2 = a^2b \implies b = 1$;
- $a^2b^2 = ab^2 \implies a = 1$.

Verifichiamo ora che $ba = ab$.

Certo $ba \neq 1,\ a,\ a^2,\ b,\ b^2$. Se per assurdo fosse $ba = a^2b$, allora, essendo $\circ(ab) = 3$:

$1 = (ab)^3 = a(ba)(ba)b = a\,a^2b\,bab = b^2ab$, da cui: $b = b^3ab \implies b = ab \implies a = 1$: assurdo.

Analogamente, se fosse $ba = ab^2$:

$$1 = (ab)^3 = a(ba)(ba)b = a\,ab^2\,bab = a^2\,ab = b\text{: assurdo.}$$

Infine, se fosse $ba = a^2b^2$:

$$1 = (ab)^3 = a(ba)(ba)b = a\,a^2b^2\,bab = ab\text{: assurdo.}$$

Si conclude che necessariamente $ba = ab$. Da tale uguaglianza segue:

$$ba^2 = ba\,a = ab\,a = a\,ba = a^2b;\ \ b^2a = b\,ba = b\,ab = ab\,b = ab^2;$$
$$b^2a^2 = b\,ba\,a = ba\,ba = ab\,ba = ab^2a = a\,ab^2 = a^2b^2.$$

(*ii*) Il prodotto diretto $\boldsymbol{Z}_3 \times \boldsymbol{Z}_3$ è formato dai nove elementi

$$(\overline{0},\overline{0}),\ (\overline{1},\overline{0}),\ (\overline{2},\overline{0}),\ (\overline{0},\overline{1}),\ (\overline{1},\overline{1}),\ (\overline{2},\overline{1}),\ (\overline{0},\overline{2}),\ (\overline{1},\overline{2}),\ (\overline{2},\overline{2}).$$

L'operazione è la somma (componennte per componente). Basta definire $f : G \to \boldsymbol{Z}_3 \times \boldsymbol{Z}_3$ tale che:

$$f(a) = (\overline{1},\overline{0}),\ f(b) = (\overline{0},\overline{1})$$

e quindi si ottiene:

$$f(1) = (\overline{0},\overline{0}),\ f(a^2) = (\overline{2},\overline{0}),\ f(b^2) = (\overline{0},\overline{2}),$$
$$f(ab) = (\overline{1},\overline{1}),\ f(a^2b) = (\overline{2},\overline{1}),\ f(ab^2) = (\overline{1},\overline{2}),\ f(a^2b^2) = (\overline{2},\overline{2}).$$

(*iii*) Da (*i*) e (*ii*) segue che un gruppo di ordine 9 o è ciclico (isomorfo a $\boldsymbol{Z}_9$) ovvero è isomorfo a $\boldsymbol{Z}_3 \times \boldsymbol{Z}_3$. In ogni caso è abeliano.

* * *

4.42. [Proposto dallo studente V.Capraro]. Sia $(G, \cdot)$ un gruppo abeliano finito.

(*i*) Se $G = \{1,\ a_1,\ \dots,\ a_n\}$ verificare che $(\prod_{i=1}^{n} a_i)^2 = 1$.

(*ii*) Dedurre da (*i*) che, se $(K, +, \cdot)$ è un campo finito e $K = \{0,\ 1,\ a_1,\ \dots,\ a_n\}$, 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

$$F \text{ è irriducibile in } K[X] \iff \big(\prod_{\alpha \in A^\cdot} \alpha\big)^2 = 1.$$

Soluzione. (*i*) Denotiamo con a_i' l'inverso di a_i. Essendo G abeliano, si possono permutare gli elementi del prodotto $(\prod_{i=1}^{n} a_i)^2$, in modo da accostare a ciascun elemento a_i il proprio inverso a_i'. Dunque

$$(\prod_{i=1}^{n} a_i)^2 = a_1 a_1' \dots a_n a_n' = 1 \dots 1 = 1.$$

(*ii*) $(K,+)$ è un gruppo finito commutativo. Da (*i*) segue che

$$(1+\sum_{i=1}^{n} a_i)^2 = 0 \text{ e dunque } 1+\sum_{i=1}^{n} a_i = 0.$$

Anche $(K^\cdot,\cdot)$ è un gruppo finito commutativo. Da (*i*) segue che

$$(\prod_{i=1}^{n} a_i)^2 = 1 \text{ e dunque } \prod_{i=1}^{n} a_i = \pm 1.$$

(*iii*) ($\Longrightarrow$) A è un campo finito. Da (*ii*) segue che $\big(\prod_{\alpha \in A^\cdot} \alpha\big)^2 = 1$.

($\Longleftarrow$) Sia $\big(\prod_{\alpha \in A^\cdot} \alpha\big)^2 = 1$. Essendo A un anello c.u. finito, dall'ipotesi segue che A è integro. Ne segue che A è un campo, cioè che F è irriducibile in $K[X]$.

* * *

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.

Soluzione. Le permutazioni cercate sono tutte e sole quelle che contengono uno dei seguenti quattro prodotti di cicli:

$$(12)(34),\ (12)(3)(4),\ (1)(2)(34),\ (1)(2)(3)(4).$$

Ognuna di esse fissa anche il sottoinsieme $\{5,6\}$. Dunque i quattro prodotti di cicli sopra considerati si completano con (56) o $(5)(6)$. Si ottengono quindi le seguenti otto permutazioni

$$(12)(34)(56),\ (12)(34)(5)(6),\ (12)(3)(4)(56),\ (12)(3)(4)(5)(6),$$
$$(1)(2)(34)(56),\ (1)(2)(34)(5)(6),\ (1)(2)(3)(4)(56),\ (1)(2)(3)(4)(5)(6).$$

Pertanto (eliminando gli 1-cicli):

$$\boldsymbol{H} = \big\{(12)(34)(56),\ (12)(34),\ (12)(56),\ (12),\ (34)(56),\ (34),\ (56),(1)\big\}.$$

Si tratta di un gruppo con otto elementi. Sette di essi hanno periodo 2 [in quanto prodotti di 2-cicli disgiunti]. Pertanto

$$\boldsymbol{H} \cong \boldsymbol{Z}_2 \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_2.$$

Si osserva subito che $\boldsymbol{H} = \langle (12),\ (34),\ (56)\rangle$.

* * *

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 $G'/_{H'}$.

Soluzione. Poiché $H' \trianglelefteq G'$, è definito il gruppo quoziente $G'/_{H'}$ e la proiezione $\pi : G' \to G'/_{H'}$ è un omomorfismo. Ne segue che l'applicazione

$$\varphi := \pi \circ f : G \to G'/_{H'}, \text{ tale che } \varphi(x) = f(x)H', \ \forall\, x \in G,$$

è un omomorfismo di gruppi , il cui nucleo è

$$Ker(\varphi) = \{x \in G \ : \ f(x)H' = H'\} = \{x \in G \ : \ f(x) \in H'\} = f^{-1}(H').$$

Ne segue che, in quanto nucleo di un omomorfismo, $f^{-1}(H') \trianglelefteq G$.

Dal teorema fondamentale di omomorfismo, applicato a φ, segue che l'omomorfismo

$$\overline{\varphi} : G/_{Ker(\varphi)} \to G'/_{H'}$$

è iniettivo. Dunque $G/_{f^{-1}(H')}$ è isomorfo ad un sottogruppo di $G'/_{H'}$.

* * *

ALTRI ESERCIZI

[Sono stati raccolti in questa sezione molti degli esercizi assegnati agli esami di Algebra 1 degli ultimi due anni accademici. Altri esercizi sono stati proposti agli studenti durante il corso.]

5.1. È assegnata l'applicazione $f : \boldsymbol{N}\times\boldsymbol{N} \to \boldsymbol{Z}$ tale che

$$f(a,b) = a^2 - b^2, \ \forall\,(a,b) \in \boldsymbol{N}\times\boldsymbol{N}.$$

(*i*) Determinare le due controimmagini $f^{-1}(0)$, $f^{-1}(2)$. Dire se f è iniettiva o suriettiva.

(*ii*) Verificare che gli insiemi $\boldsymbol{D} = 1 + 2\boldsymbol{Z}$ e $4\boldsymbol{Z}$ (risp. gli interi dispari ed i multipli interi di 4) sono contenuti in $Im(f)$.

(*iii*) Verificare che $Im(f) = \boldsymbol{D} \cup 4\boldsymbol{Z}$.

Soluzione. (*i*) Risulta: $(a,b) \in f^{-1}(0) \iff a^2 - b^2 = 0 \iff a - b$ (essendo $a, b \geq 0$). Dunque

$$f^{-1}(0) = \{(a,a), \ \forall\, a \in \boldsymbol{N}\}.$$

Risulta: $(a,b) \in f^{-1}(2) \iff a^2 - b^2 = 2 \iff (a-b)(a+b) = 2$. Poiché $a > b$ e $a + b \geq a - b$, allora necessariamente $a + b = 2$, $a - b = 1$. Ne segue che $a = b + 1$ e quindi $2b + 1 = 2$: assurdo. Si conclude che $f^{-1}(2) = \emptyset$.

Dalle considerazioni precedenti segue che f non è iniettiva né suriettiva.

(*ii*) Risulta, per ogni $n \geq 1$,

$$f(n, n-1) = 2n - 1 \ \text{ e } \ f(n-1, n) = -f(n, n-1) = 1 - 2n.$$

Ne segue che per ogni naturale dispari $n = 2k - 1$ $(k \geq 1)$ risulta $f(k, k-1) = n$. Analogamente, per ogni negativo dispari $n = 2k - 1$ $(k \leq 0)$ risulta $f(|k|, |k| + 1) = n$. Dunque $\boldsymbol{D} \subseteq Im(f)$.

Per ogni $n \geq 2$, risulta:

$$f(n, n-2) = 4(n-1) \ \text{ e } \ f(n-2, n) = -4(n-1).$$

Sia quindi $n = 4k$. Se $k \geq 1$, $n = f(k+1, k-1)$; se $k \leq -1$, $n = f(|k| - 1, |k| + 1)$; se infine $k = 0$, $n = 0 = f(0,0)$. Si conclude che $4\boldsymbol{Z} \subseteq Im(f)$.

(*iii*) Da (*ii*) segue che $Im(f) \supseteq \boldsymbol{D} \cup 4\boldsymbol{Z}$. Ovviamente $\boldsymbol{Z} - (\boldsymbol{D} \cup 4\boldsymbol{Z}) = 2\boldsymbol{D} = \{\pm 2, \pm 6, \pm 10, ...\}$. Se verifichiamo che $\forall\, n \in 2\boldsymbol{D}$ risulta $f^{-1}(n) = \emptyset$, allora possiamo concludere che $Im(f) = \boldsymbol{D} \cup 4\boldsymbol{Z}$.

Sia $n = 2d$, con d dispari e per assurdo sia $2d = f(a,b) = (a+b)(a-b)$. Assumiamo che sia

$$n = (2d_1)d_2, \ \text{ con } \ d_1, d_2 \ \text{ fattori dispari}$$

Osservato che $a + b \geq a - b$, distinguiamo due casi: $2d_1 \geq d_2$ e $2d_1 \leq d_2$.

Nel primo caso si ha: $\begin{cases} a + b = 2d_1 \\ a - b = d_2, \end{cases}$ da cui $a = b + d_2$ e quindi $d_2 = 2(d_1 - b)$, pari: assurdo. Nel secondo caso si ha: $\begin{cases} a - b = 2d_1 \\ a + b = d_2, \end{cases}$ da cui $a = b + 2d_1$ e quindi $d_2 = 2(d_1 + b)$, ancora pari: assurdo. Si conclude che $f^{-1}(2d) = \emptyset$, come richiesto.

* * *

5.2 [*Esame 15/6/04*] Sia $h : \boldsymbol{C} \to \boldsymbol{R}$ la seguente applicazione:

$$h(z) = max\big(\mathcal{R}e(z), \mathcal{I}m(z)\big), \ \forall\, z \in \boldsymbol{C}.$$

(*i*) Verificare se h è iniettiva o suriettiva.

(*ii*) Calcolare le controimmagini $h^{-1}(t)$, $\forall\, t \in \boldsymbol{R}$ e $h^{-1}\big([0, +\infty)\big)$. Identificato $\boldsymbol{C}$ con $\boldsymbol{R}^2$, descrivere tali controimmagini in $\boldsymbol{R}^2$.

(*iii*) Posto $W = \{ti, \ \forall\, t \in \boldsymbol{R}\}$, calcolare $h(W)$.

Soluzione. (*i*) h non è iniettiva. Infatti $h(x+iy) = h(y+ix)$, $\forall\, x+iy \in \boldsymbol{C}$. h è invece suriettiva. Infatti, $\forall\, t \in \boldsymbol{R}$, $h(t+it) = t$.

(*ii*) Risulta, $\forall\, t \in \boldsymbol{R}$:

$$h^{-1}(t) = \{x + iy \in \boldsymbol{C} \,\big|\, max\{x, y\} = t\} = \{t + iy,\ \forall\, y \le t\} \cup \{x + it,\ \forall\, x \le t\}.$$

Identificando $z = x + iy \in \boldsymbol{C}$ con $(x, y) \in \boldsymbol{R}^2$, $h^{-1}(t)$ è unione delle due semirette orizzontale e verticale di $\boldsymbol{R}^2$, aventi comune origine nel punto (t, t) e dirette rispettivamente verso sinistra e verso il basso.

Risulta:

$$h^{-1}\big([0, +\infty)\big) = \{x + iy \in \boldsymbol{C} \,\big|\, max\{x, y\} \ge 0\} \equiv \{(x, y) \in \boldsymbol{R}^2 \,\big|\, max\{x, y\} \ge 0\} =$$
$$= \{(x, y) \in \boldsymbol{R}^2 \,\big|\, x \ge 0 \ \text{ oppure } \ y \ge 0\} = \boldsymbol{R}^2 - [(-\infty, 0) \times (-\infty, 0)]$$

[si tratta dell'unione del I, II e IV quadrante di $\boldsymbol{R}^2$].

(*iii*) Risulta, $\forall\, t \in \boldsymbol{R},\ h(ti) = \begin{cases} 0, \text{ se } t \le 0 \\ t, \text{ se } t \ge 0. \end{cases}$ Pertanto

$$h(W) = \{h(ti),\ \forall\, t \in \boldsymbol{R}\} = [0, +\infty).$$

* * *

5.3. Sia ρ la relazione di equivalenza su $\boldsymbol{N} \times \boldsymbol{N}$ così definita:

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

(*i*) Determinare la partizione su $\boldsymbol{N} \times \boldsymbol{N}$ indotta da ρ e calcolare la cardinalità di ogni classe di equivalenza.

(*ii*) Determinare una biiezione tra l'insieme quoziente $\boldsymbol{N} \times \boldsymbol{N}\big/_{\rho}$ ed $\boldsymbol{N}$.

Soluzione. (*i*) Si denota con $[(a, b)]_{\rho}$ la classe di equivalenza di (a, b) *mod* ρ. Posto $t := max\{a, b\}$, si ha:

$$(a, b)\, \rho\, (t, k) \ \text{ e } \ (a, b)\, \rho\, (k, t),\ \ \forall\, k = 0, \ldots, t.$$

Viceversa, se $(a, b)\, \rho\, (c, d)$ allora $max\{c, d\} = t$ e dunque $\begin{cases} (c, d) = (t, k), \text{ se } c \ge d \\ (c, d) = (k, t), \text{ se } c \le d. \end{cases}$ Si conclude pertanto che

$$[(a, b)]_{\rho} = \{(t, 0),\, (t, 1),\, \ldots,\, (t, t),\, (t - 1, t),\, \ldots,\, (1, t),\, (0, t)\},\ \text{ se } \ t = max\{a, b\}.$$

Ne segue subito che

$$|[(a, b)]_{\rho}| = 2t + 1 = 1 + 2\, max\{a, b\}.$$

(*ii*) Si consideri l'applicazione $f : \boldsymbol{N} \times \boldsymbol{N} \to \boldsymbol{N}$ così definita: $f((a, b)) = max\{a, b\},\ \forall\, (a, b) \in \boldsymbol{N} \times \boldsymbol{N}$. Ovviamente $\rho_f = \rho$. Inoltre f è suriettiva [infatti $t = f((t, 0)),\ \forall\, t \in \boldsymbol{N}$]. Ne segue che l'applicazione

$$F : \boldsymbol{N} \times \boldsymbol{N}\big/_{\rho} \to \boldsymbol{N} \ \text{ tale che } \ F\big([(a, b)]_{\rho}\big) = max\{a, b\},\ \ \forall\, [(a, b)]_{\rho} \in \boldsymbol{N} \times \boldsymbol{N}\big/_{\rho},$$

è una biiezione richiesta.

* * *

5.4 [*Esame 15/6/04*] Sia p un numero primo e sia ρ la seguente relazione su $\boldsymbol{Z} \times \boldsymbol{Z}$:

$$(a, b) \rho (c, d) \iff p \,\big|\, ab - cd,\ \ \forall\, (a, b),\, (c, d) \in \boldsymbol{Z} \times \boldsymbol{Z}.$$

(*i*) Verificare che ρ è una relazione di equivalenza su $\boldsymbol{Z} \times \boldsymbol{Z}$.

(*ii*) Calcolare la classe di equivalenza di $(0, 0)$ modulo ρ.

(*iii*) Determinare un'applicazione suriettiva $f : \boldsymbol{Z} \times \boldsymbol{Z} \to \boldsymbol{Z}_p$ la cui relazione di equivalenza associata ρ_f coincida con ρ.

Soluzione. (*i*) Verifichiamo che ρ è una relazione di equivalenza. Risulta:

$(a, b) \rho (a, b)$ [infatti $p \,\big|\, ab - ab = 0$];

$(a, b) \rho (c, d) \implies (c, d) \rho (a, b)$ [infatti $p \,\big|\, ab - cd \implies p \,\big|\, cd - ab$];

$(a, b) \rho (c, d),\ (c, d) \rho (e, f) \implies (a, b) \rho (e, f)$ [infatti $p \,\big|\, ab - cd,\ p \,\big|\, cd - ef \implies p \,\big|\, ab - ef$].

(*ii*) Risulta:

$$[(0,0)] = \{(a,b) \in \boldsymbol{Z}\times\boldsymbol{Z} \ : \ (a,b)\rho(0,0)\} = \{(a,b) \in \boldsymbol{Z}\times\boldsymbol{Z} \ : \ p \,\big|\, ab\}.$$

Essendo p primo, $p \,\big|\, ab \implies p \,\big|\, a$ o $p \,\big|\, b$, cioè $a \in p\boldsymbol{Z}$ o $b \in p\boldsymbol{Z}$. Ne segue

$$[(0,0)] = (p\boldsymbol{Z}\times\boldsymbol{Z}) \cup (\boldsymbol{Z}\times p\boldsymbol{Z}).$$

(*iii*) Si ponga: $f : \boldsymbol{Z}\times\boldsymbol{Z} \to \boldsymbol{Z}_p$ tale che

$$f(a,b) = \overline{ab} \in \boldsymbol{Z}_p, \ \forall\, (a,b) \in \boldsymbol{Z}\times\boldsymbol{Z}.$$

f è suriettiva. Infatti $f(1,k) = \overline{k}, \ \forall\, k = 0, \ldots, p-1$. Inoltre

$$(a,b)\rho_f\,(c,d) \iff \overline{ab} = \overline{cd} \iff p \,\big|\, ab - cd \iff (a,b)\rho(c,d).$$

Dunque f è un'applicazione verificante le condizioni richieste.

* * *

5.5 [*Esame 6/7/04*] Sia $\boldsymbol{S}^1 = \{(x,y) \in \boldsymbol{R}^2 \,\big|\, x^2 + y^2 = 1\}$ la circonferenza unitaria di $\boldsymbol{R}^2$. Sono assegnate le due funzioni:

$f : \boldsymbol{C}^{\cdot} \to \boldsymbol{S}^1$ tale che $f(z) = \frac{z}{|z|} \equiv \big(\frac{x}{\sqrt{x^2+y^2}}, \frac{y}{\sqrt{x^2+y^2}}\big), \ \forall\, z = x + iy \in \boldsymbol{C}^{\cdot}$;

$g : \boldsymbol{S}^1 \to [0,\pi]$ tale che $g(P) = \arccos(x), \ \forall\, P = (x,y) \in \boldsymbol{S}^1$.

(*i*) Determinare le relazioni di equivalenza ρ_f, ρ_g associate ad f, g, descrivendone le classi di equivalenza.

(*ii*) Definire l'applicazione $h := g \circ f : \boldsymbol{C}^{\cdot} \to [0,\pi]$. Dire se h è iniettiva o/e suriettiva. Descrivere in $\boldsymbol{R}^2$ le classi di equivalenza della relazione associata ρ_h.

Soluzione. (*i*) Risulta, $\forall\, z, w \in \boldsymbol{C}^{\cdot}$:

$$z\rho_f\, w \iff \tfrac{z}{|z|} = \tfrac{w}{|w|}.$$

Dunque

$$[z]_{\rho_f} = \{w \in \boldsymbol{C}^{\cdot} \,\big|\, w = z\tfrac{|w|}{|z|}\} = \{cz, \ \forall\, c \in \boldsymbol{R}, \ c > 0\}.$$

[In effetti, $f(cz) = f(z), \ \forall\, c > 0$]. Nel piano di Gauss $\boldsymbol{R}^2$, $[z]_{\rho_f}$ coincide con la semiretta aperta di origine $(0,0)$ passante per il punto (x,y).

Risulta, $\forall\, P = (x,y), \ P' = (x',y') \in \boldsymbol{S}^1$:

$$P\rho_g\, P' \iff \arccos(x) = \arccos(x') \iff x = x'.$$

Tenuto conto che $x^2 + y^2 = 1 = x'^2 + y'^2$, da $x' = x$ segue che $y' = \pm y$. Pertanto

$$[P]_{\rho_g} = \{P = (x,y), \ P' = (x,-y)\}.$$

[Si tratta di due punti di $\boldsymbol{S}^1$ simmetrici rispetto all'*asse* x].

(*ii*) Risulta, $\forall\, z = x + iy \in \boldsymbol{C}^{\cdot}$:

$$h(z) = g(f(z)) = \arccos\big(\tfrac{x}{\sqrt{x^2+y^2}}\big).$$

Le due applicazioni f, g sono suriettive. Infatti:

- $\forall\, P = (x,y) \in \boldsymbol{S}^1$: $f(x+iy) = (\frac{x}{1}, \frac{y}{1}) = P$;
- $\forall\, t \in [0,\pi]$: $g(\cos t, \sin t) = \arccos(\cos t) = t$.

Ne segue che h, in quanto composizione di applicazioni suriettive, è suriettiva.

Invece h non è iniettiva. Infatti, $\forall\, z = x + iy \in \boldsymbol{C} - \boldsymbol{R}$, con $|z| = 1$, risulta $h(z) = h(\overline{z})$, mentre $z \neq \overline{z}$.

Si ha, $\forall\, z = x + iy, \ z' = x' + iy' \in \boldsymbol{C}^{\cdot}$:

$$z\rho_h z' \iff \arccos\big(\tfrac{x}{\sqrt{x^2+y^2}}\big) = \arccos\big(\tfrac{x'}{\sqrt{x'^2+y'^2}}\big) \iff \tfrac{x}{\sqrt{x^2+y^2}} = \tfrac{x'}{\sqrt{x'^2+y'^2}} \iff$$

$$\iff \mathcal{R}e(\tfrac{z}{|z|}) = \mathcal{R}e(\tfrac{z'}{|z'|}) \iff \text{i due punti } \tfrac{z}{|z|}, \ \tfrac{z'}{|z'|} \text{ coincidono o sono simmetrici rispetto all'}asse\ x.$$

Dunque $[z]_{\rho_h}$ è formata dall'unione di due semirette di comune origine $(0,0)$, simmetriche rispetto all'*asse* x.

* * *

5.6 Sia ρ la seguente relazione su $\boldsymbol{Z}$: $\forall\, x, y \in \boldsymbol{Z}$,

$$x \rho\, y \iff x = y \ \text{ oppure } \ x + y = -1$$

(*i*) Verificare che ρ è una relazione di equivalenza su $\boldsymbol{Z}$ e determinare la classe di equivalenza di ogni $x \in \boldsymbol{Z}$.

(*ii*) Sia $f : \boldsymbol{Z} \to \boldsymbol{Z}$ la seguente applicazione:

$$f(x) = -x, \ \text{se } \ x \text{ è pari}; \ \ f(x) = x + 1, \ \text{se } \ x \text{ è dispari}.$$

Determinare $Im(f)$. Verificare che $\rho = \rho_{_f}$. Descrivere una biiezione tra l'insieme quoziente $\boldsymbol{Z}\big/_{\rho}$ e l'insieme $\boldsymbol{P}$ degli interi pari.

Soluzione. (*i*) Per ogni $x, y \in \boldsymbol{Z}$, risulta ovvviamente:
$x \rho\, x$; $\ x \rho\, y \Longrightarrow y \rho\, x$ [infatti $\ x = y$ opp. $x + y = -1 \ \Longrightarrow y = x$ opp. $y + x = -1$].
Verifichiamo ora la proprietà transitiva: $\ x \rho\, y, \ y \rho\, z \Longrightarrow x \rho\, z$. Infatti
$x = y, \ y = z \Longrightarrow x = z \Longrightarrow x \rho\, z$;
$x = y, \ y + z = -1 \Longrightarrow x + z = -1 \Longrightarrow x \rho\, z$;
$x + y = -1, \ y = z \Longrightarrow x + z = -1 \Longrightarrow x \rho\, z$;
$x + y = -1, \ y + z = -1 \Longrightarrow x + y = y + z \Longrightarrow x = z \Longrightarrow x \rho\, z$.
Per ogni $x \in \boldsymbol{Z}$:

$$[x] = \{y \in \boldsymbol{Z} : \ x \rho\, y\} = \{x, \, -x - 1\}.$$

[Si noti che ogni classe di equivalenza è formata da due interi].

(*ii*) Per definizione $Im(f) \subseteq \boldsymbol{P}$ [infatti, se x è dispari, $x + 1$ è pari]. Viceversa, $\forall\, 2a \in \boldsymbol{P}$, risulta $f(-2a) = 2a = f(2a - 1)$. Dunque anche $\boldsymbol{P} \subseteq Im(f)$. Pertanto $Im(f) = \boldsymbol{P}$.
Verifichiamo che $\rho = \rho_{_f}$. Si ha

$$x \rho_{_f} y \iff \begin{cases} -x = -y \quad \text{se } \ x, y \text{ pari}, \\ x + 1 = y + 1 \quad \text{se } \ x, y \text{ dispari}, \\ x + 1 = -y \quad \text{se } \ x \text{ dispari e } y \text{ pari}, \\ -x = y + 1 \quad \text{se } \ x \text{ pari e } y \text{ dispari} \end{cases} \iff \begin{cases} x = y \quad \text{se } \ x \equiv y \ (mod\, 2), \\ x + y = -1 \quad \text{se } \ x \not\equiv y \ (mod\, 2) \end{cases} \iff$$

$\iff x = y$ oppure $\ x + y = -1 \iff x \rho\, y$.

Poiché $\rho = \rho_{_f}$ e $Im(f) = \boldsymbol{P}$, dal teorema fondamentale delle applicazioni segue che è biiettiva l'applicazione

$$F : \boldsymbol{Z}\big/_{\rho} \to \boldsymbol{P}$$

tale che $F([x]) = -x$, se x è pari; $\ F([x]) = x + 1$, se x è dispari. F agisce come segue:
$[0] = [-1] \to 0, \quad [1] = [-2] \to 2, \quad [2] = [-3] \to -2, \quad [3] = [-4] \to 4, \quad [4] = [-5] \to -4$, ecc..

* * *

5.7 [*Esonero 22/4/03*] Sia $f : \boldsymbol{R}^3 \to \boldsymbol{R}^2$ l'applicazione così definita:

$$f(x, y, z) = (xy, \, yz), \ \ \forall\, (x, y, z) \in \boldsymbol{R}^3.$$

(*i*) Verificare se f è iniettiva o suriettiva.

(*ii*) Determinare l'immagine tramite f del piano π di equazione $x = 0$ di $\boldsymbol{R}^3$.

(*iii*) Determinare la controimmagine tramite f della diagonale $x = y$ di $\boldsymbol{R}^2$.

(*iv*) Sia $g : \boldsymbol{R}^2 \to \boldsymbol{R}^3$ la seguente applicazione: $\ g(x, y) = (x, \, 0, \, y), \ \ \forall\, (x, y) \in \boldsymbol{R}^2$. Verificare se le applicazioni $f \circ g$ e $g \circ f$ sono iniettive o suriettive.

Soluzione. (*i*) Si ha, $\ \forall\, a, b \in \boldsymbol{R}$: $\ f(a, 0, b) = (0, 0) = f(0, 0, 0)$. Dunque f non è iniettiva. Per ogni $(a, b) \in \boldsymbol{R}^2$, risulta: $\ f(a, 1, b) = (a, b)$. Dunque f è suriettiva.

(*ii*) Il piano π è formato dai punti $(0, t, s), \ \ \forall\, t, s \in \boldsymbol{R}$. Risulta $\ f(0, t, s) = (0, \, ts)$. Viceversa, $\forall\, (0, b) \in \boldsymbol{R}^2$, si ha $\ (0, b) = f(0, 1, b)$. Dunque $\ f(\pi)$ è la retta $\ x = 0$ [cioè l'*asse* y] del piano $\boldsymbol{R}^2$.

(*iii*) Indichiamo con $\boldsymbol{d}$ la retta diagonale $\ x = y$ di $\boldsymbol{R}^2$. Risulta:

$$f^{-1}(\boldsymbol{d}) = \{(x, y, z) \in \boldsymbol{R}^3 \ : \ f(x, y, z) \in \boldsymbol{d}\} = \{(x, y, z) \in \boldsymbol{R}^3 \ : \ xy = yz\}.$$

Se $\ y \neq 0$, allora $\ x = z$; se $\ y = 0$, x, y sono arbitrari. Dunque

$$f^{-1}(\boldsymbol{d}) = \big[y = 0\big] \cup \big[y \neq 0, \ x = z\big].$$

(*iv*) Risulta: $(f\circ g)(x,y) = f(x,0,y) = (0,0,0)$. Dunque $f\circ g$ è l'applicazione costante di valore $(0,0)$. Non è iniettiva né suriettiva.

Risulta: $(g\circ f)(x,y,z) = g(xy,\, yz) = (xy,\, 0,\, yz)$. $g\circ f$ non è suriettiva [infatti ha immagine nel piano $y=0$] e neppure iniettiva [infatti, $\forall\, a,b\in\boldsymbol{R}$, $(g\circ f)(a,0,b) = (0,0,0) = (g\circ f)(0,0,0)$].

* * *

5.8 [*Esonero 22/4/03*] Per ogni $(h,k)\in\boldsymbol{Z}\times\boldsymbol{Z}$, si consideri il quadrato

$$\mathbf{Q}_{(h,k)} = [h,h+1)\times[k,k+1)\subset\boldsymbol{R}^2.$$

Sia $\mathfrak{F} = \{\mathbf{Q}_{(h,k)},\ \forall\,(h,k)\in\boldsymbol{Z}\times\boldsymbol{Z}\}$ la partizione di $\boldsymbol{R}^2$ formata da tali quadrati. Indicata con ρ la relazione su $\boldsymbol{R}^2$ associata ad $\mathfrak{F}$, si verifichi che $\boldsymbol{R}^2/_\rho$ è in corrispondenza biunivoca con $\boldsymbol{Z}\times\boldsymbol{Z}$.

Soluzione. Per ogni (a,b), $(c,d)\in\boldsymbol{R}^2$, risulta:

$$(a,b)\rho\,(c,d) \iff (a,b),\,(c,d)\in\mathbf{Q}_{(h,k)},\ \exists\,(h,k)\in\boldsymbol{Z}\times\boldsymbol{Z} \iff a,c\in[h,h+1);\ b,d\in[k,k+1) \iff$$
$$\iff a,c \text{ hanno la stessa parte intera e } b,d \text{ hanno la stessa parte intera.}$$

Indicata con $[x]$ la parte intera di un numero reale x, si definisce

$$F:\boldsymbol{R}^2\to\boldsymbol{Z}\times\boldsymbol{Z} \quad\text{tale che}\quad F(a,\,b) = ([a],[b]),\ \ \forall\,(a,b)\in\boldsymbol{R}^2.$$

Risulta: $(a,b)\rho_{_F}(c,d) \iff ([a],[b]) = ([c],[d]) \iff [a]=[c],\ [b]=[d] \iff a,c$ hanno la stessa parte intera e b,d hanno la stessa parte intera $\iff (a,b)\rho\,(c,d)$. Dunque $\rho_{_F} = \rho$. Inoltre F è suriettiva. Si conclude che $\boldsymbol{R}^2/_\rho$ è in corrispondenza biunivoca con $\boldsymbol{Z}\times\boldsymbol{Z}$, tramite l'applicazione che associa alla classe di (a,b) la coppia $([a],[b])$.

* * *

5.9 (*i*) Verificare che ogni dominio d'integrità finito è un campo.

(*ii*) Verificare che ogni anello commutativo, integro e finito è unitario.

Soluzione. (*i*) Sia A un dominio d'integrità finito e sia $A^\cdot = \{x_1,\, x_2,\, \dots, x_n\}$. Si fissi arbitrariamente un elemento $x_i\in A^\cdot$. Essendo A integro, gli n elementi

$$x_1x_i,\ x_2x_i,\ \dots\,, x_nx_i$$

sono non nulli e a due a due distinti [se infatti $x_h\,x_i = x_k\,x_i$, allora $(x_h - x_k)x_i = 0$ e quindi $x_h = x_k$]. Dunque

$$A^\cdot = \{x_1x_i,\ x_2x_i,\ \dots\,, x_nx_i\}.$$

Poiché $1\in A^\cdot$, allora $\exists\,k_i$ $(1\le k_i\le n)$ tale che $x_{k_i}\,x_i = 1$. Essendo A commutativo, vale anche $x_i\,x_{k_i} = 1$ e dunque $x_{k_i} = {x_i}^{-1}$. Si conclude che ogni elemento $x_i\in A^\cdot$ è invertibile, cioè che A è un campo.

(*ii*) Sia A un anello commutativo, integro e finito. Come in (*i*), se $A^\cdot = \{x_1,\, x_2,\, \dots, x_n\}$, fissato $x\in A^\cdot$, allora $A^\cdot = \{xx_1,\, x_2,\, \dots, xx_n\}$. In particolare, $x\in A^\cdot$ e dunque $x = xx_i$ $(\exists\, i,\ 1\le i\le n)$.

Verifichiamo che x_i è elemento neutro di A. Poiché A è commutativo, basta verificare che, $\forall\, y\in A^\cdot$, $y\,x_i = y$. Si ha infatti:

$$\text{se } y = xx_j,\ \text{allora } y\,x_i = (xx_j)x_i = xx_j\,x_i = xx_i\,x_j = (xx_i)x_j = xx_j = y.$$

Nota. Da (*i*) e (*ii*) segue subito che ogni anello commutativo, integro e finito è un campo.

* * *

5.10 [*Esonero 22/4/03*] È assegnato il numero complesso $z = 2^{3/4}(\cos\frac{\pi}{8} + i\sin\frac{\pi}{8})$.

(*i*) Determinare i numeri complessi $z^{4/3}$ e visualizzarli nel piano di Gauss.

(*ii*) Esistono altri numeri complessi w tali che $w^{4/3} = z^{4/3}$?

Soluzione. (*i*) Si tratta delle tre radici terze di z^4. Si ha:

$$z^4 = 2^3(\cos\tfrac{4\pi}{8} + i\sin\tfrac{4\pi}{8}) = 8i.$$

Poiché $8i$ ha modulo 8 e angolo $\vartheta = \frac{\pi}{2}$, allora

$$z^{4/3} = (8i)^{1/3} = \Big\{ 8^{1/3} \big[\cos\big(\tfrac{\frac{\pi}{2}+2k\pi}{3}\big) + i\sin\big(\tfrac{\frac{\pi}{2}+2k\pi}{3}\big)\big],\ \ \forall\, k = 0,\, 1,\, 2 \Big\}.$$

Per $k = 0$, si ottiene: $2(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}) = \sqrt{3} + i$;
per $k = 1$, si ottiene: $2(\cos\frac{5\pi}{6} + i\sin\frac{5\pi}{6}) = -\sqrt{3} + i$;
per $k = 2$, si ottiene: $2(\cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2}) = -2i$.

I tre numeri complessi ottenuti sono vertici di un triangolo equilatero inscritto nella circonferenza di centro $(0,0)$ e raggio 2 del piano di Gauss.

(*ii*) Da $w^{4/3} = z^{4/3}$ segue che $w^4 = (w^{4/3})^3 = (z^{4/3})^3 = z^4 = 8i$.
I numeri complessi cercati sono quindi le quattro radici quarte di $8i$. Si ha

$$\sqrt[4]{8i} = \Big\{ \sqrt[4]{8}\, \big[\cos\big(\tfrac{\frac{\pi}{2}+2k\pi}{4}\big) + i\sin\big(\tfrac{\frac{\pi}{2}+2k\pi}{4}\big)\big],\ \ \forall\, k = 0,\, 1,\, 2,\, 3 \Big\} =$$
$$= \Big\{ 2^{3/4} \big[\cos(\tfrac{\pi}{8} + \tfrac{k\pi}{2}) + i\sin(\tfrac{\pi}{8} + \tfrac{k\pi}{2})\big],\ \ \forall\, k = 0,\, 1,\, 2,\, 3 \Big\}.$$

* * *

5.11 [*Esame 24/2/05*] In $X = \boldsymbol{N}\times\boldsymbol{N} - \{(0,0)\}$ si consideri la seguente relazione di equivalenza ρ:

$$(a,b)\rho(c,d) \iff \tfrac{ab}{MCD(a,b)^2} = \tfrac{cd}{MCD(c,d)^2},\ \ \forall\,(a,b),\,(c,d) \in X.$$

(*i*) Verificare che ρ coincide con la relazione di equivalenza associata all'applicazione $f : X \to \boldsymbol{N}$ tale che

$$f(a,b) = \tfrac{mcm(a,b)}{MCD(a,b)},\ \ \forall\,(a,b) \in X.$$

(*ii*) Verificare che $f(a,b) = f(\frac{a}{d}, \frac{b}{d})$, con $d = MCD(a,b)$.
(*iii*) Determinare le classi di equivalenza *mod* ρ delle coppie $(0,1)$, $(1,1)$, $(3,10) \in X$. Dedurne una formula generale per il calcolo della classe di equivalenza di una generica coppia $(a,b) \in X$, *mod* ρ.

Soluzione. (*i*) Tenuto conto che $mcm(a,b)\cdot MCD(a,b) = ab$, si ha:

$$f(a,b) = \tfrac{mcm(a,b)\cdot MCD(a,b)}{MCD(a,b)\cdot MCD(a,b)} = \tfrac{ab}{MCD(a,b)^2}$$

e dunque

$$(a,b)\rho_f\,(c,d) \iff f(a,b) = f(c,d) \iff \tfrac{ab}{MCD(a,b)^2} = \tfrac{cd}{MCD(c,d)^2} \iff (a,b)\rho(c,d).$$

(*ii*) Poiché $MCD(\frac{a}{d}, \frac{b}{d}) = 1$, risulta:

$$f(\tfrac{a}{d}, \tfrac{b}{d}) = \tfrac{\frac{a}{d}\,\frac{b}{d}}{1^2} = \tfrac{ab}{d^2} = f(a,b).$$

(*iii*) Posto $\boldsymbol{N}^* = \boldsymbol{N} - \{0\}$ e $(a,b)\boldsymbol{N}^* = \{at, bt,\ \forall\, t > 0\}$, si ha:

$$[(0,1)]_\rho = f^{-1}(0) = \{(a,b) \in X \mid \tfrac{ab}{MCD(a,b)^2} = \tfrac{0}{1^2} = 0\} =$$
$$= \{(0,t),\ \forall\, t \in \boldsymbol{N}^*\} \cup \{(t,0),\ \forall\, t \in \boldsymbol{N}^*\} = (0,1)\boldsymbol{N}^* \cup (1,0)\boldsymbol{N}^*.$$

Analogamente:

$$[(1,1)]_\rho = f^{-1}(1) = \{(a,b) \in X \mid \tfrac{ab}{MCD(a,b)^2} = \tfrac{1}{1^2} = 1\} =$$
$$= \{(a,b) \in X \mid ab = MCD(a,b)^2\}.$$

Se $d = MCD(a,b)$ e $a = da_1$, $b = db_1$, si ha, per le coppie $(a,b) \in [(1,1)]_\rho$:
$d^2 = ab = a_1b_1d^2$ e dunque $a_1b_1 = 1$, cioè $a_1 = b_1 = 1$. Allora $a = b = d$. Pertanto

$$[(1,1)]_\rho = \{(t,t),\ \forall\, t \in \boldsymbol{N}^*\} = (1,1)\boldsymbol{N}^*.$$

Sia ora $(a,b) \in X$. Posto $n = \frac{ab}{MCD(a,b)^2}$, allora:

$$[(a,b)]_\rho = \{(c,d) \in X \mid cd = n\,MCD(c,d)^2\}$$
$$= \{(c_1\delta, d_1\delta) \in X \mid c_1d_1\delta^2 = n\delta^2 1\}\ \ [\text{con } \delta = MCD(c,d)]$$
$$= \{(c_1,d_1)\delta \in X \mid c_1d_1 = n\}.$$

Ne segue che

$$[(a,b)]_\rho = \bigcup\big\{(r,s)\boldsymbol{N}^* \cup (s,r)\boldsymbol{N}^*,\ \ \forall\,(r,s)\ \text{ tali che }\ n = rs,\ MCD(r,s) = 1,\ r \le s\big\}.$$

In particolare, essendo $30 = 1\cdot 30 = 2\cdot 15 = 3\cdot 10 = 5\cdot 6$, allora

$$[(3,10)]_\rho = (1,30)\boldsymbol{N}^* \cup (2,15)\boldsymbol{N}^* \cup (3,10)\boldsymbol{N}^* \cup (5,6)\boldsymbol{N}^* \cup$$
$$(30,1)\boldsymbol{N}^* \cup (15,2)\boldsymbol{N}^* \cup (10,3)\boldsymbol{N}^* \cup (6,5)\boldsymbol{N}^*.$$

* * *

5.12 [*Esame 20/9/04*] Sono assegnati in $\boldsymbol{Z}$ i tre sottoinsiemi

$$A = 25 + 30\,\boldsymbol{Z}, \quad B = 35 + 50\,\boldsymbol{Z}, \quad C = 15 + 70\,\boldsymbol{Z}$$

e l'intervallo $I = [0, 5000]$. Utilizzando opportunamente la teoria delle congruenze, determinare l'insieme $A \cap B \cap C \cap I$.

Soluzione. Sia $x = 25 + 30k \in A$. Risulta:

$x \in B \iff 25 + 30k \equiv 35\ (50) \iff 3k \equiv 1\ (5) \iff k = 2 + 5h,\ \exists\, h \in \boldsymbol{Z} \iff$
$\iff x = 85 + 150h,\ \exists\, h \in \boldsymbol{Z}.$

Dunque $A \cap B = 85 + 150\,\boldsymbol{Z}$.

Sia ora $x = 85 + 150h \in A \cap B$. Risulta:

$x \in C \iff 85 + 150h \equiv 15\ (70) \iff 10h \equiv 0\ (70) \iff h = 7t,\ \exists\, t \in \boldsymbol{Z}.$

Dunque $A \cap B \cap C = 85 + 1050\,\boldsymbol{Z}$.

Si conclude che

$$A \cap B \cap C \cap I = \{85,\ 1135,\ 2185,\ 3235,\ 4285\}.$$

* * *

5.13 [*Esonero 22/4/03*] È assegnata l'applicazione $f : \boldsymbol{Z}_{64} \to \boldsymbol{Z}_2 \times \boldsymbol{Z}_4 \times \boldsymbol{Z}_8$ tale che

$$f(\overline{x}_{64}) = (\overline{x}_2,\, \overline{x}_4,\, \overline{x}_8),\ \forall\, \overline{x} = \overline{x}_{64} \in \boldsymbol{Z}_{64}.$$

(*i*) Calcolare le controimmagini $f^{-1}(\overline{1}_2,\, \overline{3}_4,\, \overline{7}_8)$ e $f^{-1}(\overline{0}_2,\, \overline{0}_4,\, \overline{1}_8)$.

(*ii*) Determinare $Im(f)$.

(*iii*) Verificare che l'insieme quoziente $\boldsymbol{Z}_{64}/_{\rho_f}$ [modulo la relazione di equivalenza ρ_f associata ad f] è in corrispondenza biunivoca con $\boldsymbol{Z}_8$.

Soluzione. (*i*) Risulta:

$$\overline{x} \in f^{-1}(\overline{1}_2,\, \overline{3}_4,\, \overline{7}_8) \iff \begin{cases} x \equiv 1 \mod 2 \\ x \equiv 3 \mod 4 \\ x \equiv 7 \mod 8. \end{cases}$$

Cerchiamo di risolvere tale sistema di equazioni congruenziali. Dalla prima equazione, $x = 1 + 2t$. Sostituendo nella seconda: $1 + 2t \equiv 3 \mod 4$, cioè $t \equiv 1 \mod 2$, ovvero $t = 1 + 2s$. Allora $x = 3 + 4s$. Sostituendo nella terza: $3 + 4s \equiv 7 \mod 8$, cioè $s \equiv 1 \mod 2$, ovvero $s = 1 + 2v$. Allora $x = 7 + 8v$. Si conclude che

$$f^{-1}(\overline{1}_2,\, \overline{3}_4,\, \overline{7}_8) = \{\overline{7},\, \overline{15},\, \overline{23},\, \overline{31},\, \overline{39},\, \overline{47},\, \overline{55},\, \overline{63}\} \subset \boldsymbol{Z}_{64}.$$

Risulta

$$\overline{x} \in^{-1} (\overline{0}_2,\, \overline{0}_4,\, \overline{1}_8) \iff \begin{cases} x \equiv 0 \mod 2 \\ x \equiv 0 \mod 4 \\ x \equiv 1 \mod 8. \end{cases}$$

Tale sistema è incompatibile. Infatti dalla prima e dalla terza equazione, $x = 2t = 1 + 8s$ e dunque $2 \,|\, 1$: assurdo. Si conlude che $f^{-1}(\overline{0}_2,\, \overline{0}_4,\, \overline{1}_8) = \emptyset$.

(*ii*) Calcoliamo $Im(f)$. Si ha: $f(\overline{k+8}) = f(\overline{k}),\ \forall\, \overline{k} \in \boldsymbol{Z}_{64}$. Inoltre $f(\overline{h}) \neq f(\overline{k}),\ \forall\, \overline{h}, \overline{k} = \overline{0},\ \ldots\ , \overline{7},\ \overline{h} \neq \overline{k}$. Ne segue che

$$Im(f) = \{f(\overline{0}),\, f(\overline{1}),\, \ldots\ ,\, f(\overline{7})\}.$$

(*iii*) Poiché $\boldsymbol{Z}_{64}/_{\rho_f}$ è in corrispondenza biunivoca con $Im(f)$ e, in base a (*ii*), $|Im(f)| = 8$, allora $\boldsymbol{Z}_{64}/_{\rho_f} \sim \boldsymbol{Z}_8$.

* * *

5.14 [*Esame 6/7/04*] È assegnato il seguente sistema di equazioni congruenziali lineari, dipendenti da un parametro $a \in \boldsymbol{Z}$:

$$\begin{cases} 3X \equiv 4 \ (mod\ 10) \\ 5X \equiv \ a \ (mod\ 12) \\ 2X \equiv 7 \ (mod\ 9). \end{cases}$$

Determinare gli interi $a \in \boldsymbol{Z}$, con $0 \leq a \leq 11$, per cui il sistema è compatibile. Per siffatti interi calcolare la generica soluzione del sistema.

Soluzione. Il sistema formato dalla prima e terza equazione è sempre compatibile ed ha un'unica soluzione $mod\ 90$. Determineremo la generica soluzione di tale sistema e la inseriremo nella seconda equazione del sistema assegnato. I valori di a per cui tale equazione è compatibile sono i valori cercati.

Il sistema

$$\begin{cases} 3X \equiv 4 \ (mod\ 10) \\ 2X \equiv 7 \ (mod\ 9) \end{cases} \text{ equivale a } \begin{cases} X \equiv 4{\cdot}7 \equiv \ 8 \ (mod\ 10) \\ X \equiv 7{\cdot}5 \equiv \ 8 \ (mod\ 9), \end{cases}$$

la cui generica soluzione è $X = 8 + 90s, \ \forall\, s \in \boldsymbol{Z}$.

Sostituendo tale espressione nella seconda equazione del sistema si ottiene

$$5(8 + 90s) \equiv \ a \ (mod\ 12), \text{ cioè } \ 6s \equiv \ a - 4 \ (mod\ 12).$$

Tale equazione è compatibile $\iff MCD(6, 12) \,|\, a - 4 \iff 6 \,|\, a - 4 \iff a = 4, 10$. Il sistema è quindi compatibile $\iff a = 4$ oppure $a = 10$.

Sia $a = 4$. L'equazione $5X \equiv 4 \ (mod\ 12)$ è equivalente a $X \equiv 8 \ (mod\ 12)$. Ne segue $8 + 90s \equiv 8 \ (mod\ 12)$, cioè $6s \equiv 0 \ (mod\ 12)$, ovvero $s \equiv 0 \ (mod\ 2)$. Dunque $s = 2h$ e pertanto la generica soluzione del sistema è

$$X = 8 + 180\, h, \ \forall\, h \in \boldsymbol{Z}.$$

Sia $a = 10$. L'equazione $5X \equiv 10 \ (mod\ 12)$ è equivalente a $X \equiv 2 \ (mod\ 12)$. Ne segue $8 + 90s \equiv 2 \ (mod\ 12)$, cioè $6s \equiv -6 \ (mod\ 12)$, ovvero $s \equiv -1 \ (mod\ 2)$. Dunque $s = -1 + 2h$ e pertanto la generica soluzione del sistema è

$$X = 8 + 90(-1 + 2h) = -82 + 180h = 98 + 180k, \ \forall\, k \in \boldsymbol{Z}.$$

* * *

5.15 È assegnata l'equazione congruenziale lineare

$$12X \equiv 18 \ (mod\ n), \text{ con } \ 10 \leq n \leq 20.$$

Determinare gli eventuali n per cui tale equazione è compatibile ed un suo sistema completo di soluzioni è formato da tre interi. Per ogni n ottenuto, determinare determinare un sistema completo di soluzioni della corrispondente equazione.

Soluzione. L'equazione assegnata è compatibile $\iff d := (12, n) \,|\, 18$. Inoltre $d = 3$, in quanto un sistema completo di soluzioni è formato da 3 interi. Gli interi n cercati verificano quindi la condizione $3 = (12, n)$ [mentre la condizione $d \,|\, 18$ diventa superflua]. Risulta:

$$3 = (12, n) \iff n \text{ è dispari e multiplo di } 3.$$

Per $10 \leq n \leq 20$, l'unico intero dispari multiplo di 3 è $n = 15$.

Risolviamo l'equazione $12X \equiv 18 \ (mod\ 15)$. Tale equazione è equivalente a $12X \equiv 3 \ (mod\ 15)$, cioè a $4X \equiv 1 \ (mod\ 5)$. Essendo 4 un inverso aritmetico di 4 $(mod\ 15)$, l'quazione è equivalente a $X \equiv 4 \ (mod\ 5)$. Una sua soluzione è $x = 4$. Un sistema completo di soluzioni è quindi

$$\{4, \ 4 + \tfrac{15}{3}, \ 4 + \tfrac{30}{3}\} = \{4, \ 9, \ 14\}.$$

* * *

5.16 [*Esonero 22/4/03*] È assegnato il seguente sistema di equazioni congruenziali lineari:

$$\begin{cases} 4\, x \equiv 7a \ \ mod\ 3 \\ 2\, x \equiv a \ \ mod\ 7 \\ a\, x \equiv 4 \ \ mod\ 5, \end{cases}$$

dipendente da un parametro $a \in \boldsymbol{Z}$.

(*i*) Determinare per quali valori di a il sistema è compatibile.

(*ii*) Scrivere per siffatti valori la generica soluzione del sistema, in funzione di a e di un suo inverso aritmetico a' *mod* 5.

Soluzione. (*i*) La terza equazione del sistema è compatibile $\iff (a,5) \,|\, 4$. Posto $d := (a,5)$, allora $d = 1, 5$. Si ha: la terza equazione è compatibile $\iff d = 1 \iff 5 \nmid a$.

Assumiamo quindi che $5 \nmid a$. In tal caso il sistema è equivalente a

$$\begin{cases} x \equiv a \ \ mod\, 3 \\ x \equiv 4a \ \ mod\, 7 \\ x \equiv 4a' \ \ mod\, 5, \end{cases}$$

con a' inverso aritmetico di a *mod* 5. Poiché i tre moduli del sistema sono a due a due coprimi, si tratta di un sistema "cinese", che ammette un'unica soluzione *mod* 105.

(*ii*) Supponendo che $5 \nmid a$, risolviamo il sistema "cinese" sopra considerato.

Dalla prima equazione, $x = a+3t$; sostituendo nella seconda: $a+3t \equiv 4a \ mod\, 7$, cioè $t \equiv a \ mod\, 7$, ovvero $t = a + 7s$. Allora $x = 4a + 21s$. Sostituendo nella terza equazione: $4a + 21s \equiv 4a' \ mod\, 5$, cioè $s \equiv 4(a' - a) \ mod\, 5$, ovvero $s = 4(a' - a) + 5v$. Allora

$$x = 4a + 84(a' - a) + 105\, v = -80a + 84a' + 105\, v, \ \ \forall\, v \in \boldsymbol{Z},$$

è la generica soluzione richiesta.

* * *

5.17 [*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 $a',\, b'$.

Soluzione. (*i*) I moduli delle due equazioni sono coprimi. La seconda equazione è sempre compatibile [infatti $1 = (3,8) \,|\, b, \ \forall\, b \in \boldsymbol{Z}$], mentre la prima equazione è compatibile $\iff (5,a) \,|\, 3 \iff a \not\equiv 0\ (mod\, 5)$. Si conclude che

$$\text{il sistema è compatibile} \iff a \not\equiv 0\ (mod\, 5).$$

(*ii*) La seconda equazione equivale a $X \equiv 3b\ (mod\, 8)$, ed ha quindi generica soluzione $X = 3b + 8s, \ \forall\, s \in \boldsymbol{Z}$. Sostituendo nella prima equazione, si ottiene

$$3ab + 8as \equiv\ 3\ (mod\, 5), \ \text{cioè} \ \ 3ab + 3as \equiv\ 3\ (mod\, 5), \ \text{ovvero} \ \ as \equiv\ 1 - ab\ (mod\, 5).$$

Denotato con a' un inverso aritmetico di a $(mod\, 5)$, tale equazione si trasforma in

$$s \equiv\ (1 - ab)a'\ (mod\, 5), \ \text{da cui} \ \ s = (1 - ab)a' + 5t, \ \ \forall\, t \in \boldsymbol{Z}.$$

Si conclude che $\forall\, a \not\equiv\ 0\ (mod\, 5)$, il sistema ha come generica soluzione

$$X = 3b + 8(1 - ab)a' + 40t, \ \ \forall\, t \in \boldsymbol{Z}.$$

* * *

5.18 [*Esame 24/2/05*] Sono assegnate le tre equazioni congruenziali lineari

$$14X \equiv 2\ (mod\, 20), \quad 15X \equiv 3\ (mod\, 18), \quad X \equiv a\ (mod\, 12), \ \text{con} \ a \in \boldsymbol{Z}.$$

(*i*) Risolvere il sistema formato dalle prime due equazioni.

(*ii*) Determinare gli eventuali $a \in \boldsymbol{Z}$, con $0 \le a \le 11$, per cui il sistema formato dalle tre equazioni è compatibile. Per ciascuno di tali valori determinare la soluzione ed il modulo rispetto a cui è unica.

Soluzione. (*i*) L'equazione $14X \equiv 2\ (mod\ 20)$ è equivalente a $7X \equiv 1\ (mod\ 10)$ e quindi a $X \equiv 3\ (mod\ 10)$. L'equazione $15X \equiv 3\ (mod\ 18)$ è equivalente a $5X \equiv 1\ (mod\ 6)$ e quindi a $X \equiv 5\ (mod\ 6)$.

Il sistema formato dalle prime due equazioni assegnate è equivalente al sistema

$$\begin{cases} X \equiv 3 \ (mod\ 10) \\ X \equiv 5 \ (mod\ 6). \end{cases}$$

Tale sistema è compatibile, in quanto $MCD(10,6) \,|\, 3-5$. Il sistema ammette un'unica soluzione modulo $mcm(10,6) = 30$, che passiamo a determinare. Dalla prima equazione, $X = 3 + 10s$. Sostituendo nella seconda, $3 + 10s \equiv 5 \ (mod\ 6)$, cioè $4s \equiv 2 \ (mod\ 6)$, ovvero $s \equiv 2 \ (mod\ 3)$. Posto $s = 2 + 3t$, allora $X = 23 + 30t$.

Il sistema è dunque equivalente all'unica equazione

$$X \equiv 23 \ (mod\ 30).$$

(*ii*) Da (*i*) segue che il sistema formato dalle tre equazioni è equivalente al sistema

$$\begin{cases} X \equiv 23 \ (mod\ 30) \\ X \equiv a \ (mod\ 12). \end{cases}$$

Tale sistema è compatibile $\iff$ $MCD(30,12) \,|\, 23-a$ $\iff$ $6 \,|\, 23-a$ $\iff$ $a = 5, 11$ (se $0 \le a \le 11$).

Sia $a = 5$. Da $X = 23+30s$, segue $23+30s \equiv 5 \ (mod\ 12)$, cioè $s \equiv 1 \ (mod\ 2)$. Allora $s = 1+2t$ e quindi $X = 53 + 60t$. La soluzione del sistema è 53, unica $mod\ 60$.

Sia $a = 11$. Da $X = 23+30s$, segue $23+30s \equiv 11 \ (mod\ 12)$, cioè $s \equiv 0 \ (mod\ 2)$. Allora $s = 2t$ e quindi $X = 23 + 60t$. La soluzione del sistema è 23, unica $mod\ 60$.

* * *

5.19 Assegnati $a = 71$, $n = 143 = 11 \cdot 13$, calcolare, utilizzando il teorema Cinese del Resto, un inverso aritmetico di $a \ mod\ n$ [senza far uso dell'identità di Bézout relativa ad a, n].

Soluzione. Osservato che $n = 143 = 11 \cdot 13$ e $(11,13) = 1$, dal teorema Cinese del Resto segue che sussiste un isomorfismo

$$F : \boldsymbol{Z}_{143} \to \boldsymbol{Z}_{11} \times \boldsymbol{Z}_{13}.$$

In particolare, $F(\overline{a}) = \left(\overline{71}_{11}, \overline{71}_{13}\right) = \left(\overline{5}_{11}, \overline{6}_{13}\right)$. Ne segue che $F(\overline{a}^{-1}) = F(\overline{a})^{-1} = \left(\overline{5}_{11}^{\ -1}, \overline{6}_{13}^{\ -1}\right)$. Calcoliamo gli inversi aritmetici di $5 \ (mod\ 11)$ e di $6 \ (mod\ 13)$. Da $1 = (5,11) = 5(-2) + 11 \cdot 1$, segue che $\overline{5}_{11}^{\ -1} = \overline{-2}_{11} = \overline{9}_{11}$. Da $1 = (6,13) = 6(-2) + 13 \cdot 1$, segue che $\overline{6}_{13}^{\ -1} = \overline{-2}_{13} = \overline{11}_{13}$. Pertanto

$$F(\overline{a}^{-1}) = \left(\overline{9}_{11}, \overline{11}_{13}\right).$$

Risolviamo il sistema

$$\begin{cases} X \equiv 9 \ (mod\ 11) \\ X \equiv 11 \ (mod\ 13). \end{cases}$$

Si ottiene la soluzione $x = 141$ [unica $mod\ 143$)]. Si conclude che $a = 71$ ha inverso aritmetico $141 \ (mod\ 143)$.

* * *

5.20 Sia $n = 221$.

(*i*) Utilizzando il Piccolo Teorema di Fermat, verificare che n non è un numero primo.

(*ii*) Utilizzando il "criterio standard" di fattorizzazione in primi, determinare una fattorizzazione di n come prodotto di primi.

Soluzione. (*i*) Scriviamo $n - 1$ come somma di potenze decrescenti di 2. Risulta:

$$\begin{aligned} 220 &= 2 \cdot 110 + 0, \\ 110 &= 2 \cdot 55 + 0, \\ 55 &= 2 \cdot 27 + 1, \\ 27 &= 2 \cdot 13 + 1, \\ 13 &= 2 \cdot 6 + 1, \\ 6 &= 2 \cdot 3 + 0, \\ 3 &= 2 \cdot 1 + 1, \\ 1 &= 2 \cdot 0 + 1. \end{aligned}$$

Dunque

$$n - 1 = 220 = (1,1,0,1,1,1,0,0)_2 = 2^7 + 2^6 + 2^4 + 2^3 + 2^2.$$

Dobbiamo verificare se $\exists\, a \geq 2$ tale che $(a, 221) = 1$ e $a^{220} \not\equiv 1\ (mod\ 221)$. Poniamo $a = 2$. Allora

$$2^{220} = (2^{2^7})\,(2^{2^6})\,(2^{2^4})\,(2^{2^3})\,(2^{2^3}).$$

Calcoliamo $mod\ 221$ le potenze 2^{2^k}, per $k = 2, \ldots, 7$. Si ha:

$$\begin{aligned}
&2^{2^2} = 16 \equiv 16\ (mod\ 221),\\
&2^{2^3} \equiv 16^2 = 256 \equiv 35\ (mod\ 221),\\
&2^{2^4} \equiv 35^2 = 1225 \equiv 120\ (mod\ 221),\\
&2^{2^5} \equiv 120^2 = 14400 \equiv 35\ (mod\ 221),\\
&2^{2^6} \equiv 35^2 \equiv 120\ (mod\ 221),\\
&2^{2^7} \equiv 120^2 \equiv 35\ (mod\ 221).
\end{aligned}$$

Pertanto

$$2^{220} \equiv 35{\cdot}120{\cdot}120{\cdot}35{\cdot}16 \equiv 16 \not\equiv 1\ (mod\ 221).$$

Si conclude che $n = 221$ non è primo.

(*ii*) Si ponga $I_1 = \big[2, [\sqrt{221}]\big] \cap \boldsymbol{N} = [2, 14] \cap \boldsymbol{N}$. Si ha:

$$2, 3, 5, 7, 11 \not| n, \ \text{mentre}\ \ 13 \,|\, n.$$

Allora si pone $k_1 = 13$ e $n_1 = \frac{n}{k_1} = 17$. Poiché $I_2 = \big[13, [\sqrt{17}]\big] \cap \boldsymbol{N} = \emptyset$, il procedimento è concluso e si ha: $n = 13{\cdot}17$ (fattorizzazione in primi richiesta).

* * *

5.21 [*Esonero 22/4/03*] Determinare le ultime tre cifre di 37^{412}.

Soluzione. Bisogna risolvere l'equazione $37^{412} \equiv X\ mod\ 1000$.

Poiché $(37, 1000) = 1$, dal teorema di Eulero-Fermat, $37^{\varphi(1000)} \equiv 1\ mod\ 1000$. Essendo $\varphi(1000) = 400$, allora $37^{400} \equiv 1\ mod\ 1000$. Allora

$$37^{412} \equiv 37^{12}\ \ mod\ 1000.$$

Dal teorema Cinese del Resto, $F : \boldsymbol{Z}_{1000} \to \boldsymbol{Z}_8 \times \boldsymbol{Z}_{125}$ è un isomorfismo e si ha:

$$F(\overline{37}) = \big(\overline{5}, \overline{37}\big), \quad F(\overline{37^{12}}) = F(\overline{37}^{12}) = \big(\overline{5}^{12}, \overline{37}^{12}\big) \in \boldsymbol{Z}_8 \times \boldsymbol{Z}_{125}.$$

Si ha: $5^{12} = (5^3)^4 = (125)^4 \equiv 1^4 = 1\ mod\ 8$;

$$37^{12} = (37^2)^6 = (1369)^6 \equiv (-6)^6 = 6^6 = (216)^2 \equiv (-34)^2 = 34^2 = 1156 \equiv 31\ mod\ 125.$$

Dunque $F(\overline{37^{12}}) = (\overline{1}, \overline{76})$. Si risolva quindi il sistema

$$\begin{cases} X \equiv 1\ mod\ 8 \\ X \equiv 31\ mod\ 125. \end{cases}$$

Si ottiene la soluzione $x = 281 + 1000t, \ \forall\, t \in \boldsymbol{Z}$. Dunque le ultime tre cifre di 37^{412} sono 2, 8, 1.

* * *

5.22 [*Esonero 7/6/04*] È assegnato in $\boldsymbol{Z}_3[X]$ il polinomio $P = X^5 + X^2 + \overline{2}$.

(*i*) Verificare se P è irriducibile in $\boldsymbol{Z}_3[X]$.

(*ii*) Calcolare (se esiste) l'inverso nell'anello $\boldsymbol{Z}_3[X]/_{(P)}$ di ciascuno dei seguenti tre polinomi

$$X^2, \ \ \overline{2}X + \overline{2}, \ \ X^2 + \overline{2}X + \overline{2} \in \boldsymbol{Z}_3[X].$$

Soluzione. (*i*) Osservato che $P(\overline{0})$, $P(\overline{1})$, $P(\overline{2}) \neq \overline{0}$ e che $\overline{2} = \overline{1}{\cdot}\overline{2} = \overline{2}{\cdot}\overline{1}$, P potrebbe ammettere in $\boldsymbol{Z}_3[X]$ una delle due seguenti fattorizzazioni:

$$P = (X^3 + aX^2 + bX + \overline{2})(X^2 + cX + \overline{1}); \quad P = (X^3 + aX^2 + bX + \overline{1})(X^2 + cX + \overline{2}).$$

Confrontando i coefficienti di ugual grado, si ottengono rispettivamente i sistemi (a coefficienti in $\boldsymbol{Z}_3$)

$$\begin{cases} a + c = \overline{0} \\ b + ac + \overline{1} = \overline{0} \\ \overline{2} + bc + a = \overline{1} \\ \overline{2}c + b = \overline{0}, \end{cases} \qquad \begin{cases} a + c = \overline{0} \\ b + ac + \overline{2} = \overline{0} \\ \overline{1} + bc + \overline{2}a = \overline{1} \\ c + \overline{2}b = \overline{0}. \end{cases}$$

Si verifica che il primo è incompatibile, mentre il secondo ammette soluzione $a = \overline{1}$, $b = c = \overline{2}$. Pertanto P è riducibile e si fattorizza nella forma

$$P = (X^3 + X^2 + \overline{2}X + \overline{1})(X^2 + \overline{2}X + \overline{2}).$$

(*ii*) Risulta:

$$\boldsymbol{Z}_3[X]\big/_{(P)} = \boldsymbol{Z}_3[x \,|\, P(x) = \overline{0}] = \left\{a + bx + cx^2 + dx^3 + ex^4,\ \forall\, a, b, c, d, e \in \boldsymbol{Z}_3,\ \text{ con } x^5 = \overline{1} + \overline{2}x^2\right\}.$$

Tale anello non è integro. Ad esempio $(x^3 + x^2 + \overline{2}x + \overline{1})(x^2 + \overline{2}x + \overline{2}) = \overline{0}$ ed i due fattori sono zero-divisori.

Ovviamente $x^2 + \overline{2}x + \overline{2}$ non ammette inverso (essendo uno zero-divisore).

Per ottenere (se esiste) un inverso di x^2, basta osservare, da $x^5 = \overline{1} + \overline{2}x^2$, che $\overline{1} = x^5 + x^2 = x^2(x^3 + \overline{1})$ e dunque $(x^2)^{-1} = x^3 + \overline{1}$.

Infine, per ottenere (se esiste) un inverso di $\overline{2}x + \overline{2}$, basta risolvere il sistema di equazioni lineari (a coefficienti in $\boldsymbol{Z}_3$) ottenuto da

$$(\overline{2}x + \overline{2})(a + bx + cx^2 + dx^3 + ex^4) = \overline{1},$$

ovvero da

$$(x + \overline{1})(a + bx + cx^2 + dx^3 + ex^4) = \overline{2}.$$

Si ottiene l'unica soluzione $a = b = \overline{0}$, $d = \overline{1}$, $c = e = \overline{2}$ e dunque

$$(\overline{2}x + \overline{2})^{-1} = \overline{2}x^2 + x^3 + \overline{2}x^4.$$

* * *

5.23 [*Esonero 7/6/04*] Sono assegnati in $\boldsymbol{Z}_2[X]$ i due polinomi $P = X^2 + X + \overline{1}$ e $Q = X^5 + X + \overline{1}$.

(*i*) Verificare che $K = \boldsymbol{Z}_2[X]\big/_{(P)}$ è un campo. Scriverne gli elementi e la tavola moltiplicativa.

(*ii*) Fattorizzare Q in $K[X]$.

[*Suggerimento.* Verificare per prima cosa se Q ammette zeri in K].

Soluzione. (*i*) Risulta $P(\overline{0}) = \overline{1} = P(\overline{1})$. Dunque P non ha zeri in $\boldsymbol{Z}_2$ e pertanto è irriducibile in $\boldsymbol{Z}_2[X]$. Ne segue che $K = \boldsymbol{Z}_2[X]\big/_{(P)}$ è un campo.

Risulta: $K = \boldsymbol{Z}_2[x \,|\, x^2 = x + \overline{1}] = \{a + bx,\ \forall\, a, b \in \boldsymbol{Z}_2,\ \text{con } x^2 = x + \overline{1}\} =$

$$= \{\overline{0},\, \overline{1},\, x,\, \overline{1} + x,\ \text{con } x^2 = x + \overline{1}\}.$$

La tavola moltiplicativa di K è la seguente

$\cdot$	$\overline{1}$	x	$\overline{1}+x$
$\overline{1}$	$\overline{1}$	x	$\overline{1}+x$
x	x	$\overline{1}+x$	$\overline{1}$
$\overline{1}+x$	$\overline{1}+x$	$\overline{1}$	x

(*ii*) Verifichiamo se Q ammette zeri in K. Si ha:

$Q(\overline{0}) = \overline{1} = Q(\overline{1})$; $Q(x) = x^4 x + x + \overline{1} = (x+\overline{1})^2 x + x + \overline{1} = (x^2+\overline{1})x + x + \overline{1} = x^3 + \overline{1} = x^2 + x + \overline{1} = \overline{0}$;

$Q(\overline{1} + x) = (\overline{1} + x)^4 (\overline{1} + x) + (\overline{1} + x) + \overline{1} = x^2(\overline{1} + x) + x = x + x = \overline{0}$.

Ne segue che in $K[X]$ il polinomio Q ammette i fattori $X + x$ e $X + (x + 1)$. Risulta

$$F := (X + x)(X + (x + 1)) = X^2 + X + \overline{1} \text{ e } G := Q/F = X^3 + X^2 + \overline{1}.$$

Essendo G un polinomio di grado 3 [in $K[X]$], per decidere se è irriducibile, basta verificare se ammette zeri in K. Si ha:

$G(\overline{0}) = G(\overline{1}) = \overline{1}$; $G(x) = x^3 + x^2 + \overline{1} = x^3 + x = x(x^2 + \overline{1}) = x\, x = \overline{1} + x \neq \overline{0}$;

$G(\overline{1} + x) = (\overline{1} + x)^3 + (\overline{1} + x)^2 + \overline{1} = (\overline{1} + x)^2 x + \overline{1} = \overline{1} + x^2 = x \neq \overline{0}$.

Si conclude che G è irriducibile in $K[X]$ e dunque Q si fattorizza in $K[X]$ nella forma

$$Q = (X + x)(X + (x + 1))(X^3 + X^2 + \overline{1}).$$

* * *

5.24 Utilizzando la riduzione modulo un primo, verificare che il polinomio $f = X^6 + 4X^2 + 2 \in \boldsymbol{Z}[X]$ non ammette fattori irriducibili di grado 3.

Soluzione. Si osservi che gli eventuali zeri razionali di f sono ± 1, ± 2, ma che $f(\pm 1)$, $f(\pm 2) \neq 0$. Ciò significa che f non ha fattori lineari e che quindi un suo eventuale fattore g di grado 3 è necessariamente irriducibile.

Essendo 2 il termine noto di f, la riduzione di f *mod* 2 è un polinomioriducibile e dunque è inutile prenderlo in considerazione. Consideriamo invece la riduzione di f *mod* 3:

$$\overline{f} = X^6 + X^2 + \overline{2} \in \boldsymbol{Z}_3[X].$$

Se verifichiamo che $\overline{f}$ non ammette alcuna fattorizzazione $\overline{g}\,\overline{h}$, con $\partial\,\overline{g} = 3$, $\partial\,\overline{h} = 3$, allora lo stesso è vero per f. Dunque f non ha fattori di grado 3 (tantomeno irriducibili).

Procedendo per assurdo, poniamo

$$\overline{f} = \big(X^3 + aX^2 + bX + \overline{2}\big)\big(X^3 + cX^2 + dX + \overline{1}\big) \in \boldsymbol{Z}_3[X]$$

[si noti che in $\boldsymbol{Z}_3$, $\overline{2}$ si fattorizza solo nella forma $\overline{1}\cdot\overline{2}$ o $\overline{2}\cdot\overline{1}$]. Confrontando i coefficienti di ugual grado si ottiene il sistema

$$\begin{cases} a + c = \overline{0} \\ b + d + ac = \overline{0} \\ bc + ad = \overline{0} \\ a + bd + \overline{2}c = \overline{1} \\ b + \overline{2}d = \overline{0}. \end{cases}$$

Risolvendolo, si ottiene: $c = \overline{2}a$, $b = d$, $a^2 + d = \overline{0}$, $d^2 + \overline{2}a = \overline{1}$ e dunque $a^4 + \overline{2}a = \overline{1}$. Ma $\nexists\, a \in \boldsymbol{Z}_3$ verificante l'ultima equazione e pertanto il sistema è incompatibile, come richiesto.

* * *

5.25 (*i*) Sia $K := \boldsymbol{Q}[X]/_{(X^3-2)}$. Verificare che in $K[X]$ il polinomio $F = X^3 - 2$ ammette un fattore irriducibile G di grado 2.

(*ii*) Esprimere il generico elemento del campo $L := K[X]/_{(G)}$.

(*iii*) Come si fattorizza $F = X^3 - 2$ in $L[X]$?

Soluzione. (*i*) Il polinomio $F = X^3 - 2$ è irriducibile su $\boldsymbol{Q}$ e dunque K è un campo. Risulta

$$K = \boldsymbol{Q}[x \,|\, x^3 = 2] = \{a + bx + cx^2,\ \forall\, a, b, c \in \boldsymbol{Q};\ x^3 = 2\}.$$

Poiché F ammette in $\boldsymbol{R}$ lo zero $\sqrt[3]{2}$, allora K si identifica al sottocampo di $\boldsymbol{R}$:

$$\boldsymbol{Q}[\sqrt[3]{2}\,] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4},\ \forall\, a, b, c \in \boldsymbol{Q}\}$$

(ed in particolare x si identifica con $\sqrt[3]{2}$).

Ovviamente $X - x \,\big|\, F$ in $K[X]$ (in quanto $F(x) = 0$). Eseguendo la divisione con resto, si ottiene:

$$F = (X - x)(X^2 + xX + x^2) \in K[X].$$

Poniamo $G = X^2 + xX + x^2$ e verifichiamo che G è irriducibile in $K[X]$. Per assurdo, assumiamo G riducibile e scriviamolo come prodotto di due fattori lineari: $G = (X - \alpha)(X - \beta)$, con $\alpha, \beta \in K$. Ne segue che

$$(*) \qquad F = (X - \sqrt[3]{2})(X - \alpha)(X - \beta) \in K[X] \subset \boldsymbol{R}[X] \subset \boldsymbol{C}[X].$$

Ma in $\boldsymbol{C}[X]$ il polinomio F ammette i tre zeri $\sqrt[3]{2}$, $\sqrt[3]{2}\,\zeta_3$, $\sqrt[3]{2}\,\zeta_3^2$ [dove ζ_3 è radice primitiva terza dell'unità] e dunque

$$(**) \qquad F = (X - \sqrt[3]{2})(X - \sqrt[3]{2}\,\zeta_3)(X - \sqrt[3]{2}\,\zeta_3^2) \in \boldsymbol{C}[X].$$

Poiché $\boldsymbol{C}[X]$ è un *UFD*, le due fattorizzazioni $(*), (**)$ coincidono (a meno dell'ordine dei fattori). Ne segue che $\sqrt[3]{2}\,\zeta_3, \sqrt[3]{2}\,\zeta_3^2 \in \boldsymbol{R}$: assurdo.

(*ii*) $L = K[X]/_{(G)}$ è un campo (essendo G irriducibile in $K[X]$). Posto $[X]_G = \xi$, allora

$$\begin{aligned} K[X]/_{(G)} &= K[\xi \,|\, \xi^2 + x\xi + x^2 = 0] = \big\{a + b\xi,\ \forall\, a, b \in K;\ \xi^2 + x\xi + x^2 = 0\big\} = \\ &= \big\{a + bx + cx^2 + d\xi + ex\xi + fx^2\xi,\ \forall\, a, b, c, d, e, f \in \boldsymbol{Q};\ x^3 = 2,\ \xi^2 + x\xi + x^2 = 0\big\}. \end{aligned}$$

(*iii*) In $L[X]$ il polinomio G ammette zero ξ e dunque $X - \xi \,\big|\, G$. Eseguendo la divisione con resto di G per $X - \xi$, si ottiene

$$G = (X - \xi)(X + (x + \xi)) + 0$$

e pertanto in $L[X]$:

$$F = (X - x)(X - \xi)(X + (x + \xi)).$$

* * *

5.26 È assegnato l'anello $\boldsymbol{Z}_8[X]$.

(*i*) Verificare che il polinomio $f = \overline{1} + \overline{2}X$ è invertibile in $\boldsymbol{Z}_8[X]$, calcolandone un inverso. Verificare la stessa cosa per il polinomio $g = \overline{1} + \overline{4}X \in \boldsymbol{Z}_8[X]$.

(*ii*) Dire perché invece $m = \overline{1} + \overline{3}X$ non è invertibile in $\boldsymbol{Z}_8[X]$.

Soluzione. (*i*) Si ponga $\overline{1} = fh$, con $h \in \boldsymbol{Z}_8[X]$, polinomio incognito.

Se fosse $\partial h = 0$, allora $h = a \in \boldsymbol{Z}_8$. In tal caso: $a \cdot (\overline{1} + \overline{2}X) = \overline{1}$, da cui $a = \overline{1}$, $\overline{2}a = \overline{0}$, cioè $\overline{2} = \overline{0}$: assurdo.

Assumiamo $\partial h = 1$. Quindi $h = a + bX \in \boldsymbol{Z}_8[X]$, $b \neq \overline{0}$. Allora

$$\overline{1} = (\overline{1} + \overline{2}X)(a + bX) = a + (\overline{2}a + b)X + \overline{2}bX^2$$

e quindi

$$\{\ a = \overline{1},\ \overline{2}a + b = \overline{0},\ \overline{2}b = \overline{0}, \quad \text{cioè} \quad \{\ a = \overline{1},\ b = \overline{-2} = \overline{6},\ \overline{2}b = \overline{0}.$$

Tale sistema è incompatibile, in quanto $\overline{2} \cdot \overline{6} \neq \overline{0}$.

Assumiamo ora $\partial h = 2$ e quindi $h = a + bX + cX^2 \in \boldsymbol{Z}_8[X]$, $c \neq \overline{0}$. Allora

$$\overline{1} = (\overline{1} + \overline{2}X)(a + bX + cX^2) = a + (\overline{2}a + b)X + (\overline{2}b + c)X^2 + \overline{2}cX^3$$

e quindi

$$\{\ a = \overline{1},\ \overline{2}a + b = \overline{0},\ \overline{2}b + c = \overline{0},\ \overline{2}c = \overline{0}.$$

Ne segue: $a = \overline{1}$, $b = \overline{6}$, $c = \overline{4}$. Si conclude che, in $\boldsymbol{Z}_8[X]$,

$$f^{-1} = h = \overline{1} + \overline{6}X + \overline{4}X^2.$$

Per il polinomio $g = \overline{1} + \overline{4}X \in \boldsymbol{Z}_8[X]$ si può procedere nello stesso modo. Si ottiene subito che

$$g^2 = (\overline{1} + \overline{4}X)^2 = \overline{1} + \overline{8}X + \overline{16}X^2 = \overline{1} + \overline{0} + \overline{0} = \overline{1}$$

e dunque $g^{-1} = g$.

(*ii*) Assumiamo che il polinomio $m = \overline{1} + \overline{3}X \in \boldsymbol{Z}_8[X]$ sia invertibile e denotiamo con h il suo inverso. Sia $\partial h = n \geq 0$ e sia a il coefficente direttore di h. Da $\overline{1} = mh$ segue che $\overline{1} = \overline{3}aX^{n+1} + ...$ e dunque $\overline{3}a = \overline{0}$, da cui $a = \overline{0}$ (essendo $\overline{3}$ invertibile in $\boldsymbol{Z}_8$). Ciò è ovvviamente assurdo.

* * *

5.27 [*Esame 6/7/04*] È assegnato in $\boldsymbol{Z}_3[X]$ il polinomio $P = X^2 + X + \overline{2}$.

(*i*) Verificare che l'anello $A = \boldsymbol{Z}_3[X]\Big/_{(P)}$ è un campo e scriverne gli elementi.

(*ii*) Considerati in $A[X]$ tutti i polinomi $X^2 - a$, $\forall\, a \in A$, determinare tra essi gli eventuali polinomi irriducibili.

Soluzione. (*i*) Poiché $P(\overline{0}), P(\overline{1}), P(\overline{2}) \neq \overline{0}$, P non ha zeri in $\boldsymbol{Z}_3$ e dunque è irriducibile in $\boldsymbol{Z}_3[X]$. Ne segue che l'anello A è un campo. Risulta:

$$A = \boldsymbol{Z}_3\big[x \,\big|\, P(x) = \overline{0}\big] = \big\{a + bx,\ \forall\, a, b \in \boldsymbol{Z}_3;\ x^2 = \overline{1} + \overline{2}x\big\} =$$
$$= \big\{\overline{0},\ \overline{1},\ \overline{2},\ x,\ \overline{1} + x,\ \overline{2} + x,\ \overline{2}x,\ \overline{1} + \overline{2}x,\ \overline{2} + \overline{2}x\big\}.$$

(*ii*) I polinomi cercati sono quelli per cui a è un *non quadrato* in A [cioè per cui $\nexists\, b \in A\ :\ b^2 = a$]. Scriviamo la *tavola dei quadrati* in A, ponendo sotto ad ogni $a \in A$ il suo quadrato:

a	:	$\overline{0}$	$\overline{1}$	$\overline{2}$	x	$\overline{1} + x$	$\overline{2} + x$	$\overline{2}x$	$\overline{1} + \overline{2}x$	$\overline{2} + \overline{2}x$
a^2	:	$\overline{0}$	$\overline{1}$	$\overline{1}$	$\overline{1} + \overline{2}x$	$\overline{2} + x$	$\overline{2}$	$\overline{1} + \overline{2}x$	$\overline{2}$	$\overline{2} + x$

Come si vede, i *non quadrati* in A sono i seguenti quattro elementi:

$$x,\ \overline{1} + x,\ \overline{2}x,\ \overline{2} + \overline{2}x.$$

Conseguentemente, i polinomi irriducibili richiesti sono

$$X^2 - x,\ X^2 - (\overline{1} + x),\ X^2 - \overline{2}x,\ X^2 - (\overline{2} + \overline{2}x).$$

* * *

5.28 [*Esame 15/6/04*] È assegnato in $\boldsymbol{Z}[X]$ il polinomio $f = X^6 - 4$. Scrivere una fattorizzazione di f come prodotto di fattori irriducibili nei seguenti anelli:

$$\boldsymbol{Q}[X], \quad \boldsymbol{R}[X], \quad \boldsymbol{C}[X], \quad \boldsymbol{Z}_5[X].$$

Soluzione. Risulta: $f = (X^3 - 2)(X^3 + 2) \in \boldsymbol{Z}[X]$. I due polinomi

$$g_1 = X^3 - 2, \quad g_2 = X^3 + 2$$

sono irriducibili in $\boldsymbol{Z}[X]$ [si applichi ad esempio il criterio di Eisenstein, con $p = 2$]. Poiché sono primitivi, sono anche irriducibili in $\boldsymbol{Q}[X]$. Quindi $f = g_1 g_2$ è la fattorizzazione cercata in $\boldsymbol{Q}[X]$.

$\alpha_1 = \sqrt[3]{2}$ è uno zero reale di g_1, mentre $\alpha_2 = \sqrt[3]{-2} = -\sqrt[3]{2} = -\alpha_1$ è uno zero reale di g_2. Risulta, dalla divisione euclidea:

$$g_1 = (X - \alpha_1)(X^2 + \alpha_1 X + \alpha_1^2), \quad g_2 = (X + \alpha_1)(X^2 - \alpha_1 X + \alpha_1^2).$$

I due polinomi di grado 2 sopra cosiderati sono irriducibili in $\boldsymbol{R}[X]$ [infatti hanno entrambi discriminante $\Delta = -3\alpha_1^2 < 0$]. Si conclude che la fattorizzazione irriducibile di f in $\boldsymbol{R}[X]$ è

$$f = (X - \alpha_1)(X + \alpha_1)(X^2 + \alpha_1 X + \alpha_1^2)(X^2 - \alpha_1 X + \alpha_1^2).$$

In $\boldsymbol{C}[X]$, il polinomio f ha ovviamente sei zeri, ottenibili calcolando le radici (complesse) dei due polinomi di grado 2 della precedente fattorizzazione. Possiamo però meglio osservare che i sei zeri di f sono le sei radici seste di 4, ovvero le tre radici terze di 2 e le tre radici terze di -2. Dunque sono

$$\alpha_1,\ \alpha_1\zeta_3,\ \alpha_1\zeta_3^2,\ -\alpha_1,\ -\alpha_1\zeta_3,\ -\alpha_1\zeta_3^2,$$

e quindi la fattorizzazione irriducibile di f in $\boldsymbol{C}[X]$ è

$$f = (X - \alpha_1)(X + \alpha_1)(X - \alpha_1\zeta_3)(X + \alpha_1\zeta_3)(X - \alpha_1\zeta_3^2)(X + \alpha_1\zeta_3^2).$$

In $\boldsymbol{Z}_5[X]$, risulta $f = X^6 - \overline{4} = (X^3 - \overline{2})(X^3 + \overline{2}) = (X^3 + \overline{3})(X^3 + \overline{2})$.

Il polinomio $X^3 + \overline{3} \in \boldsymbol{Z}_5[X]$ ammette $\overline{3}$ come zero. Dalla divisione euclidea segue che

$$X^3 + \overline{3} = (X - \overline{3})(X^2 + \overline{3}X + \overline{4}) = (X + \overline{2})(X^2 + \overline{3}X + \overline{4}).$$

Il polinomio $X^2 + \overline{3}X + \overline{4}$ non ha zeri in $\boldsymbol{Z}_5$ e dunque è irriducibile in $\boldsymbol{Z}_5[X]$.

Analogamente, il polinomio $X^3 + \overline{2} \in \boldsymbol{Z}_5[X]$ ammette $\overline{2}$ come zero. Dalla divisione euclidea segue che

$$X^3 + \overline{2} = (X - \overline{2})(X^2 + \overline{2}X + \overline{4}) = (X + \overline{3})(X^2 + \overline{2}X + \overline{4}).$$

Anche $X^2 + \overline{2}X + \overline{4}$ è privo di zeri e dunque irriducibile in $\boldsymbol{Z}_5[X]$. Si conclude così che la fattorizzazione irriducibile di f in $\boldsymbol{Z}_5[X]$ è

$$f = (X + \overline{2})(X + \overline{3})(X^2 + \overline{2}X + \overline{4})(X^2 + \overline{3}X + \overline{4}).$$

* * *

5.29. [*Esonero 6/6/05*] È assegnato il polinomio $f = X^5 + 2X^3 - X + 2 \in \boldsymbol{Z}[X]$.

(*i*) Scrivere una fattorizzazione di f in $\boldsymbol{Q}[X]$ come prodotto di polinomi irriducibili.

(*ii*) Indicata con $\overline{f}$ la riduzione di f in $\boldsymbol{Z}_2[X]$, scrivere il generico elemento dell'anello $A = \boldsymbol{Z}_2[X]/_{(\overline{f})}$ e indicarne la cardinalità.

(*iii*) Esaminare le classi in A dei polinomi X, $X + \overline{1}$, $X^2 + X + \overline{1} \in \boldsymbol{Z}_2[X]$ e dire se si tratta di 0-divisori o di elementi invertibili in A.

Soluzione. (*i*) Gli eventuali zeri razionali di f sono numeri razionali $\frac{r}{s}$, con $r \,|\, 2$, $s \,|\, 1$. Dunque i possibili zeri di f sono ± 1, ± 2. Si verifica subito che $f(-1) = 0$. Dunque $X + 1 \,|\, f$. Procedendo con la divisione euclidea, si ottiene

$$f = (X + 1)(X^4 - X^3 + 3X^2 - 3X + 2).$$

Verifichiamo ora se il polinomio $g = X^4 - X^3 + 3X^2 - 3X + 2$ è ulteriormente riducibile. Applicando la riduzione in $\boldsymbol{Z}_3$, si ottiene il polinomio $\overline{g} = X^4 + \overline{2}X^3 + \overline{2} \in \boldsymbol{Z}_3[X]$. Tale polinomio non ha zeri in $\boldsymbol{Z}_3$ (come subito si verifica) e quindi, se si fattorizza, ammette solo una fattorizzazione con due polinomi di grado 2, del tipo

$$g = X^4 + \overline{2}X^3 + \overline{2} = (X^2 + aX + \overline{2})(X^2 + bX + \overline{1})$$

[si noti che, in $\boldsymbol{Z}_3$, $\overline{2}$ è ottenibile solo come prodotto di $\overline{1}$ per $\overline{2}$ o viceversa]. Sviluppando il prodotto e confrontando i coefficienti di ugual grado, si ottiene il sistema

$$\left\{a + b = \overline{2},\ \overline{1} + ab + \overline{2} = \overline{0},\ b + \overline{2}a = \overline{0}\right.$$

da cui segue: $a = b = \overline{1}$, mentre $ab = \overline{0}$: assurdo. Si conclude che $\overline{g}$ è irriducibile in $\boldsymbol{Z}_3[X]$ e quindi che g lo è in $\boldsymbol{Z}[X]$. Dal teorema di Gauss, g è irriducibile in $\boldsymbol{Q}[X]$. La fattorizzazione di f richiesta è quindi $f = (X + 1)(X^4 - X^3 + 3X^2 - 3X + 2)$.

(*ii*) In $\boldsymbol{Z}_2[X]$, risulta: $\overline{f} = X^5 + X = X(X^4 + \overline{1}) = X(X + \overline{1})^4$. Il polinomio $\overline{f}$ è ovviamente riducibile e quindi A non è integro. Risulta, posto $x = X + (\overline{f})$:

$$A = \boldsymbol{Z}_2[x \,|\, x^5 = x] = \left\{a + bx + cx^2 + dx^3 + ex^4,\ \forall\, a, b, c, d, e \in \boldsymbol{Z}_2;\ x^5 = x\right\}.$$

L'anello A ha $2^5 = 32$ elementi.

(*iii*) Gli elementi x, $\overline{1} + x \in A$ sono ovviamente 0-divisori. Infatti

$$x(x^4 + \overline{1}) = \overline{0}, \quad (x + \overline{1})\,[x(x + \overline{1})^3] = \overline{0}.$$

Verifichiamo invece che l'elemento $\overline{1} + x + x^2$ è invertibile in A. Posto

$$\overline{1} = (\overline{1} + x + x^2)(a + bx + cx^2 + dx^3 + ex^4),$$

si ottiene il sistema in $\boldsymbol{Z}_2$:

$$\begin{cases} a = \overline{1} \\ a + b + d + e = \overline{0} \\ a + b + c + e = \overline{0} \\ b + c + d = \overline{0} \\ c + d + e = \overline{0}. \end{cases}$$

Dalla seconda e terza equazione, $c = d$; dalle ultime due allora $b = e = \overline{0}$. Il sistema ammette soluzione $a = c = d = \overline{1}$, $b = e = \overline{0}$. Dunque $(\overline{1} + x + x^2)(\overline{1} + x^2 + x^3) = \overline{1}$.

* * *

5.30 [*Esame 20/9/04*] È assegnato l'anello

$$A = \boldsymbol{Z}_2[X]\big/_{(P)}, \ \text{ con } \ P = X^5 + X^4 + X^3 + X^2 + X + \overline{1} \in \boldsymbol{Z}_2[X].$$

(*i*) Scrivere la fattorizzazione di P in $\boldsymbol{Z}_2[X]$.

(*ii*) Indicare l'espressione di un generico elemento di A, la cardinalità di A ed un suo zero-divisore.

(*iii*) Verificare se l'elemento $X + (P)$ è uno zero-divisore di A.

Soluzione. (*i*) Il polinomio P ammette $\overline{1}$ come zero. Dunque è fattorizzato da $X + \overline{1}$. Risulta subito:

$$P = (X + \overline{1})(X^4 + X^2 + \overline{1}) = (X + \overline{1})(X^2 + X + \overline{1})^2.$$

(*ii*) Risulta:

$$A = \boldsymbol{Z}_2[x \,|\, x^5 = x^4 + x^3 + x^2 + x + \overline{1}] = \left\{a + bx + cx^2 + dx^3 + ex^4,\ \ \forall\, a, b, c, d, e \in \boldsymbol{Z}_2\right\}.$$

L'anello A ha $2^5 = 32$ elementi.

Per ottenere uno zero-divisore di A basta considerare un fattore proprio di $P(x)$; ad esempio $x + \overline{1}$, $x^2 + x + \overline{1}$, $(x^2 + x + \overline{1})^2$, $(x + \overline{1})(x^2 + x + \overline{1})$.

(*iii*) Per verificare che $x = X + (P)$ non è uno zero-divisore in A basta verificare che

$$x(a + bx + cx^2 + dx^3 + ex^4) = \overline{0} \Longrightarrow\ a = b = c = d = e = \overline{0}.$$

Infatti da

$$x(a + bx + cx^2 + dx^3 + ex^4) = ax + bx^2 + cx^3 + dx^4 + e(x^4 + x^3 + x^2 + x + \overline{1}) = \overline{0},$$

segue subito che $d + e = c + e = b + e = a + e = e = \overline{0}$ e quindi $a = b = c = d = e = \overline{0}$.

* * *

5.31 [*Esonero 7/6/04*] Sono assegnati in $\boldsymbol{Z}[i]$ gli interi di Gauss

$$z_a = 2 + 3a\,i, \ \ \forall\, a \in \boldsymbol{Z}.$$

(*i*) Determinare gli z_a che sono multipli di $w = 1 - 2i$.

(*ii*) Per $a = 0, \pm 1, \pm 2,$ scrivere una fattorizzazione di z_a come prodotto di interi di Gauss irriducibili.

Soluzione. (*i*) I multipli di w sono tutti e soli gli interi di Gauss z_a tali che $\frac{z_a}{w} \in \boldsymbol{Z}[i]$. Si ha:

$$\frac{z_a}{w} = \frac{z_a\,\overline{w}}{w\,\overline{w}} = \tfrac{1}{5}(2 + 3a\,i)(1 + 2i) = \tfrac{2-6a}{5} + \tfrac{4+3a}{5}\,i.$$

Pertanto: $\frac{z_a}{w} \in \boldsymbol{Z}[i] \iff \frac{2-6a}{5},\ \frac{4+3a}{5} \in \boldsymbol{Z} \iff 5 \,\Big|\, \begin{matrix} 2-6a \\ 4+3a \end{matrix} \iff \begin{cases} 2 - 6a \equiv 0\ (mod\ 5) \\ 4 + 3a \equiv 0\ (mod\ 5) \end{cases} \iff$

$$\iff \begin{cases} 2 \equiv a\ (mod\ 5) \\ 4 \equiv 2a\ (mod\ 5) \end{cases} \iff a \equiv 2\ (mod\ 5) \iff a = 2 + 5t,\ \ \forall\, t \in \boldsymbol{Z}.$$

Gli interi di Gauss richiesti sono quindi i seguenti:

$$2 + 3(2 + 5t)i,\ \ \forall\, t \in \boldsymbol{Z}.$$

(*ii*) È noto che $\boldsymbol{Z}[i]$ è un UFD e dunque ogni intero ammette una fattorizzazione unica (a meno di elementi invertibili) come prodotto di fattori irriducibili. Risulta:

- $z_0 = 2$. Si ha: $2 = (1 - i)(1 + i)$ e poiché $1 + i,\ 1 - i$ hanno norma prima, sono irriducibili. Dunque la fattorizzazione di 2 appena scritta è quella cercata.

- $z_{\pm 1} = 2 \pm 3i$. Tali interi di Gauss hanno norma prima $(= 13)$ e dunque sono irriducibili.

- $z_2 = 2 + 6i$. Da (*i*) è noto che z_2 ha come fattore $1 - 2i$ [che è irriducibile, in quanto ha norma prima]. Risulta:

$$\tfrac{z_2}{1-2i} = -2 + 2i = 2(-1 + i) = (1 - i)(1 + i)(-1 + i)$$

e quindi la fattorizzazione di z_2 come prodotto di interi di Gauss irriducibili è

$$z_2 = 2 + 6i = -(1 - 2i)(1 + i)(1 - i)^2.$$

- $z_{-2} = 2 - 6i$. Poiché $z_{-2} = \overline{z_2}$, allora z_{-2} ha fattorizzazione "coniugata" a quella di z_2, cioè:

$$z_{-2} = 2 - 6i = -(\overline{1 - 2i})(\overline{1 + i})(\overline{1 - i})^2 = -(1 + 2i)(1 - i)(1 + i)^2.$$

* * *

5.32. [*Esonero 6/6/05*] In $\boldsymbol{Z}[i]$ sono assegnati gli interi di Gauss $z = 5 + 4i,\ w = 3i$.

(*i*) Eseguire la divisione con resto di z per w, determinandone quoziente e resto.

(*ii*) Verificare che w è un elemento primo in $\boldsymbol{Z}[i]$.

(*iii*) Descrivere in $\boldsymbol{Z}[i]$ la relazione $\equiv_w$ (relazione di congruenza *modulo* w) e indicare gli elementi dell'anello $A = \boldsymbol{Z}[i]/_{\equiv_w}$.

Soluzione. (*i*) In $\boldsymbol{Q}[i]$ si ha

$$\tfrac{z}{w} = \tfrac{z\,(-i)}{w(-i)} = \tfrac{4-5i}{3} = \tfrac{4}{3} - i\,\tfrac{5}{3}.$$

Si pone $q := 1-2i$ [1, -2 sono gli interi rispettivamente più prossimi a $\frac{4}{3}$, $-\frac{5}{3}$] e $r := z - wq = -1 + i$. Ovviamente $\mathcal{N}(r) = 2 < \mathcal{N}(w) = 9$. Si conclude che w, r sono rispettivamente quoziente e resto della divisione di z per w.

(*ii*) In $\boldsymbol{Z}[i]$ elementi primi ed irriducibili coincidono [vale infatti il Lemma di Euclide]. Per verificare che w è irriducibile basta dimostrare che non ammette fattorizzazioni non banali. Per assurdo, sia $w = z_1 z_2$, con $\mathcal{N}(z_1), \mathcal{N}(z_2) > 1$. Allora $9 = \mathcal{N}(w) = \mathcal{N}(z_1)\mathcal{N}(z_2)$ e dunque necessariamente $\mathcal{N}(z_1) = \mathcal{N}(z_2) = 3$. Ma in $\boldsymbol{Z}[i]$ nessun intero di Gauss ha norma 3 [infatti l'equazione $a^2 + b^2 = 3$ non ha soluzioni intere]. Si conclude che w è primo.

(*iii*) Risulta, $\forall\, a_1 + ib_1,\ a_2 + ib_2 \in \boldsymbol{Z}[i]$:

$$a_1 + ib_1 \equiv_w a_2 + ib_2 \iff w \,\big|\, (a_2 + ib_2) - (a_1 + ib_1).$$

Si noti che la classe di congruenza $[z]$ di $z = a + ib$ è rappresentata dal resto della divisione con resto di z per w. Dunque

$$A = \boldsymbol{Z}[i]/_{\equiv_w} = \big\{[a + ib],\ \forall\, a + ib \in \boldsymbol{Z}[i] \ \text{ tale che } \ \mathcal{N}(a + ib) < 9\big\}.$$

Ne segue che

$$A = \boldsymbol{Z}[i]/_{\equiv_w} = \big\{[a + ib],\ \forall\, a, b \in \boldsymbol{Z} \ \text{ tali che } \ -2 \le a, b \le 2\big\}.$$

A priori si contano 25 elementi in A. Ma gli interi a, b possono essere scelti ≥ 0 [infatti $a+ib \equiv_w a+ib+3i \equiv_w a+ib+3$ e quindi, se ad esempio $-2 \leq a \leq -1$, allora $[a+ib] = [a+3+ib]$ e $1 \leq a+3 \leq 2$].

Siano allora $z = a+ib$, $z_1 = a_1+ib_1$, con $0 \leq a, a_1 \leq 2$, $0 \leq b, b_1 \leq 2$; se $z \equiv_w z_1$, allora $3i \,\big|\, z-z_1$ e quindi $z - z_1 = 3i\,y$, $\exists\, y \in \boldsymbol{Z}[i]$. Dunque $9\mathcal{N}(y) = \mathcal{N}(z-z_1) \leq 4+4 = 8$. Ne segue che $y = 0$, cioè $z = z_1$. Si conclude quindi che A è formato da nove elementi:

$$A = \boldsymbol{Z}[i]\big/_{\equiv_w} = \big\{[0],\,[1],\,[2],\,[i],\,[1+i],\,[2+i],\,[2i],\,[1+2i],\,[2+2i]\big\}.$$

Nota. Si potrebbe verificare che A è un campo, isomorfo a $\boldsymbol{Z}_3[X]\big/_{(X^2+\overline{1})}$.

* * *

5.33. [*Esame 20/9/04*] Sono assegnati nel gruppo additivo $(\boldsymbol{Q}, +)$ dei numeri razionali i due sottoinsiemi

$$S = \{\tfrac{2}{3},\, \tfrac{3}{2}\}, \quad T = \{\tfrac{1}{p},\ \forall\, p \in \boldsymbol{P}\},$$

dove $\boldsymbol{P}$ denota l'insieme dei naturali primi.

(*i*) Descrivere gli elementi dei sottogruppi $\langle\, S\,\rangle$ e $\langle\, T\,\rangle$ di $(\boldsymbol{Q}, +)$ generati da tali sottoinsiemi.

(*ii*) Verificare che $\langle\, S\,\rangle$ è ciclico e indicarne un generatore.

(*iii*) Verificare che $\frac{1}{4} \notin \langle\, T\,\rangle$.

(*iv*) Verificare che $\langle\, T\,\rangle$ non è ciclico.

Soluzione. (*i*) Per definizione, il sottogruppo generato da un sottoinsieme Σ di un gruppo additivo (ed abeliano) G è l'insieme di tutte le somme del tipo

$$\sum_{i=1}^{t} n_i\, q_i\,, \quad \forall\, n_i \in \boldsymbol{Z}, \quad \forall\, q_i \in \Sigma, \quad \forall\, t \geq 1.$$

Ne segue:

$\langle\, S\,\rangle = \{\frac{2}{3}n + \frac{3}{2}m, \ \ \forall\, n, m \in \boldsymbol{Z}\}$;

$\langle\, T\,\rangle = \{\sum_{i=1}^{t} n_i \frac{1}{p_i}, \ \ \forall\, n_i \in \boldsymbol{Z}, \ \ \forall\, p_1, \ldots, p_t \ \text{ primi distinti}\}$.

(*ii*) Poiché $\langle\, S\,\rangle = \{\frac{4n+9m}{6}, \ \ \forall\, n, m \in \boldsymbol{Z}\}$ e poiché $(4, 9) = 1$, segue dall'identità di Bézout che $\frac{1}{6} \in \langle\, S\,\rangle$ e dunque $\langle\, \frac{1}{6}\,\rangle \subseteq \langle\, S\,\rangle$.

Viceversa, $\forall\, \frac{4n+9m}{6} \in \langle\, S\,\rangle$, risulta ovviamente che $\frac{4n+9m}{6} = (4n+9m)\frac{1}{6} \in \langle\, \frac{1}{6}\,\rangle$. Si conclude quindi che $\langle\, S\,\rangle$ è ciclico, con generatore $\frac{1}{6}$.

(*iii*) Per assurdo, $\frac{1}{4} \in \langle\, T\,\rangle$. Allora $\frac{1}{4} = \frac{n_1}{p_1} + \ldots + \frac{n_t}{p_t}$, con $p_1, \ldots, p_t$ primi a due a due distinti. Posto allora $N = p_1 p_2 \ldots p_t$ e $q_i = \frac{N}{p_i}$, $\forall\, i = 1, \ldots, t$, ne segue

$$\tfrac{1}{4} = \tfrac{1}{N}\big(n_1 q_1 + \ldots + n_t q_t\big),$$

da cui $4 \,\big|\, N$. Ciò è assurdo in quanto N è prodotto di fattori primi a due a due distinti.

(*iv*) Per assurdo, sia $\langle\, T\,\rangle = \langle\, \frac{a}{b}\,\rangle$, con $b \neq 0$. Allora, $\forall\, p \in \boldsymbol{P}$, risulta:

$$\tfrac{1}{p} = \tfrac{a}{b}\, n_p\,, \ \exists\, n_p \in \boldsymbol{Z}.$$

Dunque $b = a\, p\, n_p$ e pertanto $p \,\big|\, b$, $\forall\, p \in \boldsymbol{P}$. Dunque b ha infiniti divisori primi e ciò contraddice il teorema fondamentale dell'aritmetica: assurdo.

* * *

5.34 Verificato che $K = \boldsymbol{Z}_5[X]\big/_{(X^2+X+\overline{1})}$ è un campo [e che quindi il gruppo moltiplicativo $(K^{\cdot}, \cdot)$ è un gruppo ciclico],

(*i*) determinare i generatori del gruppo ciclico $(K^{\cdot}, \cdot)$.

(*ii*) per ogni divisore positivo d dell'ordine di $K^{\cdot}$, determinare un elemento di $K^{\cdot}$ di periodo d.

Soluzione. Il polinomio $P = X^2 + X + \overline{1} \in \boldsymbol{Z}_5[X]$ è irriducibile [infatti non ha zeri in Z_5, come subito si verifica]. Dunque P è irriducibile e pertanto K è un campo. Risulta:

$$K = \boldsymbol{Z}_5[x \mid x^2 + x + \overline{1} = 0] = \{a + bx,\ \forall\, a, b \in \boldsymbol{Z}_5;\ x^2 = -x - \overline{1} = \overline{4}x + \overline{4}\}$$

Tale campo ha 25 elementi e dunque $|K^\cdot| = 24$.

(*i*) I generatori di $K^\cdot$ sono $\varphi(24) = 8$. Una volta trovatone uno, che denoteremo ζ, gli altri sette sono dati da ζ^t con $1 < t < 24$, $(t, 24) = 1$. Per ottenere un generatore ζ si può procedere seguendo due strade:

(*a*) *per tentativi.*

(*b*) *cercando un elemento* α *di periodo* 3 *ed uno* β *di periodo* 8. Poichè i periodi di tali elementi sono coprimi e $K^\cdot$ è abeliano, allora $\langle\alpha\rangle \times \langle\beta\rangle \cong \langle\alpha\rangle\langle\beta\rangle$ e $\circ(\alpha\beta) = \circ((\alpha, \beta)) = mcm(3, 8) = 24$. Dunque $\alpha\beta$ è un generatore di $K^\cdot$.

Procediamo secondo il metodo (*a*), per tentativi: fissato un elemento ζ, calcoliamo successivamente le potenze ζ^2, ζ^3, ζ^4, ζ^6, ζ^8, ζ^{12} [arrestandoci però alla prima potenza che risultasse $= \overline{1}$].

Se poniamo $\zeta = \overline{1} + \overline{3}x$, risulta:

$$\zeta^2 = \overline{2} + \overline{2}x,\ \zeta^3 = \overline{1} + \overline{2}x,\ \zeta^4 = -x,\ \zeta^6 = \overline{2},\ \zeta^8 = \overline{4} + \overline{4}x,\ \zeta^{12} = \overline{4}.$$

Ne segue che $\circ(\zeta) = 24$. Gli altri sette generatori di $K^\cdot$ sono:

$$\zeta^5 = \overline{3} + \overline{2}x,\ \zeta^7 = \overline{2} + x,\ \zeta^{11} = \overline{1} + \overline{4}x,\ \zeta^{13} = \overline{4} + \overline{2}x,\ \zeta^{17} = \overline{2} + \overline{3}x,\ \zeta^{19} = \overline{3} + \overline{4}x,\ \zeta^{23} = \overline{4} + x.$$

(*ii*) I divisori positivi di 24 sono $d = 1, 2, 3, 4, 6, 8, 12, 24$. Per ottenere un elemento di periodo d basta calcolare $\zeta^{24/d}$. Si ottiene (con i calcoli già svolti):

$\zeta^{24/1} = \overline{1}$, di periodo 1; $\zeta^{24/2} = \zeta^{12} = \overline{4}$, di periodo 2; $\zeta^{24/3} = \zeta^8 = \overline{4} + \overline{4}x$, di periodo 3;

$\zeta^{24/4} = \zeta^6 = \overline{2}$, di periodo 4; $\zeta^{24/6} = \zeta^4 = \overline{4}x$, di periodo 6; $\zeta^{24/8} = \zeta^3 = \overline{1} + \overline{2}x$, di periodo 8;

$\zeta^{24/12} = \zeta^2 = \overline{2} + \overline{2}x$, di periodo 12; $\zeta^{24/24} = \zeta = \overline{1} + \overline{3}x$, di periodo 24.

Nota. Procedendo con il metodo (*b*), avremmo ad esempio potuto determinare $\alpha = x$ (di periodo 3) e $\beta = \overline{1} + \overline{2}x$ (di periodo 8), il cui prodotto $\alpha\beta = \overline{3} + \overline{4}x$ ha periodo 24.

* * *

5.35. [*Esame 24/2/05*] (*i*) Scrivere tutti i polinomi monici di grado tre in $\boldsymbol{Z}_2[X]$.

(*ii*) Di ciascuno di essi scrivere la fattorizzazione in fattori irriducibili.

(*iii*) Per ognuno dei polinomi irriducibili f trovati, scrivere tutti gli elementi del campo $K = \boldsymbol{Z}_2[X]/_{(f)}$. Verificare poi che il gruppo moltiplicativo $(K^\cdot, \cdot)$ è ciclico e indicarne un generatore, calcolandone le successive potenze.

Soluzione. I polinomi richiesti sono del tipo $X^3 + aX^2 + bX + c$, con $a, b, c \in \boldsymbol{Z}_2$. Sono quindi i seguenti otto polinomi:

X^3, $X^3 + 1$, $X^3 + X$, $X^3 + X + 1$,
$X^3 + X^2$, $X^3 + X^2 + 1$, $X^3 + X^2 + X$, $X^3 + X^2 + X + 1$.

(*ii*) Degli otto polinomi sopra considerati, sei sono riducibili, mentre due sono irriducibili (in quanto non hanno zeri in $\boldsymbol{Z}_2$). I sei riducibili e le rispettive fattorizzazioni sono:

X^3,
$X^3 + 1 = (X + 1)(X^2 + X + 1)$,
$X^3 + X = X(X + 1)^2$,
$X^3 + X^2 = X^2(X + 1)$,
$X^3 + X^2 + X = X(X^2 + X + 1)$,
$X^3 + X^2 + X + 1 = (X + 1)^3$.

I due polinomi irriducibili sono $f_1 = X^3 + X + 1$, $f_2 = X^3 + X^2 + 1$.

(*iii*) L'anello quoziente $K_1 = \boldsymbol{Z}_2[X]/_{(f_1)}$ è un campo, costituito dagli otto elementi $a + b\alpha + c\alpha^2$, $\forall\, a, b, c \in \boldsymbol{Z}_2$, con α simbolo tale che $f_1(\alpha) = 0$. Dunque

$$K_1 = \{0,\ 1,\ \alpha,\ 1 + \alpha,\ \alpha^2,\ 1 + \alpha^2,\ \alpha + \alpha^2,\ 1 + \alpha + \alpha^2\},\ \text{con } \alpha^3 = 1 + \alpha.$$

$(K_1^\cdot, \cdot)$ è un gruppo con sette elementi e dunque è ciclico, isomorfo a $\mathbf{C}_7$. Ogni suo elemento $\neq 1$ è un generatore. Ad esempio lo è α. Le sue potenze sono:

$$\alpha^0 = 1,\ \alpha,\ \alpha^2,\ \alpha^3 = 1 + \alpha,\ \alpha^4 = \alpha + \alpha^2,\ \alpha^5 = 1 + \alpha + \alpha^2,\ \alpha^6 = 1 + \alpha^2.$$

Analogamente, $K_2 = \boldsymbol{Z}_2[X]/_{(f_2)} = \{0,\ 1,\ \beta,\ 1 + \beta,\ \beta^2,\ 1 + \beta^2,\ \beta + \beta^2,\ 1 + \beta + \beta^2\}$, con β simbolo tale che $f_2(\beta) = 0$, ovvero $\beta^3 = 1 + \beta^2$.

Anche $(K_2^{\cdot}, \cdot) \approx \mathbf{C}_7$ ed un generatore di tale gruppo è ad esempio β. Risulta:

$$\beta^0 = 1,\ \beta,\ \beta^2,\ \beta^3 = 1 + \beta^2,\ \beta^4 = 1 + \beta + \beta^2,\ \beta^5 = 1 + \beta,\ \beta^6 = \beta + \beta^2.$$

* * *

5.36. [*Esonero 7/6/04*] Nell'insieme $\mathfrak{M}_2(\boldsymbol{Z}_2)$ delle matrici quadrate di ordine 2 a valori in $\boldsymbol{Z}_2$, si consideri il gruppo $\mathbf{GL}_2(\boldsymbol{Z}_2)$ [rispetto al prodotto righe per colonne].

Scriverne gli elementi e dimostrare che è isomorfo ad un gruppo diedrale.

Soluzione. $\mathbf{GL}_2(\boldsymbol{Z}_2)$ è contenuto nell'insieme $\mathfrak{M}_2(\boldsymbol{Z}_2)$ delle matrici quadrate di ordine 2, a valori in $\boldsymbol{Z}_2$. Tale insieme è costituito dalle seguenti sedici matrici:

$$\begin{pmatrix} \overline{0} & \overline{0} \\ \overline{0} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{1} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix},$$

$$\begin{pmatrix} \overline{0} & \overline{1} \\ \overline{0} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}.$$

Tra queste sedici matrici, scegliamo quelle con determinante $\neq \overline{0}$. Si ottiene

$$\mathbf{GL}_2(\boldsymbol{Z}_2) = \left\{ \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \right\}.$$

Denotiamo rispettivamente tali matrici con 1, a, b, c, d, e. Risulta subito:

$$\circ(1) = 1,\ \circ(a) = \circ(b) = \circ(e) = 2,\ \circ(c) = \circ(d) = 3.$$

Allora $a^2 = c^3 = 1$, mentre $ac = c^2a$. Si conclude che $\mathbf{GL}_2(\boldsymbol{Z}_2)$ è isomorfo al gruppo diedrale del triangolo equilatero. Infatti

$$\mathbf{GL}_2(\boldsymbol{Z}_2) = \left\langle c,\ a \,\middle|\, c^3 = a^2 = 1,\ ac = c^2a \right\rangle \cong \boldsymbol{D}_3 = \boldsymbol{S}_3.$$

* * *

5.37. Sia $n = 2k$, con $k \geq 2$. Calcolare il numero delle permutazioni in $\boldsymbol{S}_n$ che sono prodotto di due k-cicli disgiunti.

Soluzione. Sia $\sigma = \gamma_1\gamma_2 \in \boldsymbol{S}_n$, con $n = 2k$ e con γ_1, γ_2 k-cicli disgiunti (e quindi complementari) di $\boldsymbol{S}_n$. Poiché i due cicli commutano, non è restrittivo assumere che γ_1 contenga 1 (e quindi che γ_2 non lo contenga). I cicli γ_1 sono tanti quante le permutazioni di $k-1$ elementi scelti in un insieme di $n-1$ elementi. Dunque sono $\binom{n-1}{k-1}(k-1)!$.

Fissato γ_1, il k-ciclo complementare γ_2 può essere scelto in $\binom{n-k}{k}(k-1)! = \binom{k}{k}(k-1)! = (k-1)!$ modi. Si conclude che le permutazioni cercate sono

$$\tbinom{n-1}{k-1}\left[(k-1)!\right]^2.$$

Ad esempio, in $\boldsymbol{S}_4$ la struttura ciclica $(\_\ \_)(\_\ \_)$ è formata da $\binom{3}{1}[1!]^2 = 3$ permutazioni, mentre in $\boldsymbol{S}_6$ la struttura ciclica $(\_\ \_\ \_)(\_\ \_\ \_)$ è formata da $\binom{5}{2}[2!]^2 = 40$ permutazioni.

* * *

5.38. [*Esame 15/6/04*] Sia $n \geq 4$. Nel gruppo simmetrico $\boldsymbol{S}_n$, si consideri il sottogruppo $H = \langle(123)\rangle$.

(*i*) Verificare che H non è normale in $\boldsymbol{S}_n$, determinando opportunamente una permutazione $\sigma \in \boldsymbol{S}_n$ tale che $\sigma H \neq H\sigma$.

(*ii*) È vero che ogni sottogruppo generato da un 3-ciclo di $\boldsymbol{S}_n$ è non normale?

(*ii*) Sia $n \geq 6$ e siano $\sigma, \tau \in \boldsymbol{S}_n$ due 3-cicli disgiunti. Descrivere il sottogruppo $\langle\sigma, \tau\rangle$ di $\boldsymbol{S}_n$ generato da questi due 3-cicli.

Soluzione. (*i*) Risulta: $H = \{(1), (123), (132)\}$. Si consideri il 2-ciclo $\sigma = (14)$. Risulta:

$H\sigma = \{(1)(14), (123)(14), (132)(14)\} = \{(14), (1234), (1324)\}$,

$\sigma H = \{(14)(1), (14)(123), (14)(132)\} = \{(14), (1423), (1432)\}$

e pertanto $H\sigma \neq \sigma H$, cioè H non è normale in $\boldsymbol{S}_n$.

(*ii*) Sia H un sottogruppo generato da un 3-ciclo (abc), con $1 \leq a,b,c \leq n$. Quindi $H = \{(1), (abc), (acb)\}$. Si scelga ora un naturale $d \neq a,b,c,\ 1 \leq d \leq n$. Risulta subito che $H(ad) \neq (ad)H$. Infatti

$$H(ad) = \{(ad),\ (abcd),\ (acbd)\},\ \text{mentre}\ \ (ad)H = \{(ad),\ (adbc),\ (adcb)\}.$$

(*iii*) Per ipotesi, $\sigma^3 = \tau^3 = 1$; inoltre, essendo σ, τ disgiunti, $\tau\sigma = \sigma\tau$. Ne segue che

$$\langle \sigma, \tau \rangle = \{1,\ \sigma,\ \sigma^2,\ \tau,\ \tau^2,\ \sigma\tau,\ \sigma^2\tau,\ \sigma\tau^2,\ \sigma^2\tau^2\}.$$

Tutti gli elementi (escluso 1) hanno periodo 3. Si conclude che il gruppo in questione è isomorfo a $\boldsymbol{Z}_3 \times \boldsymbol{Z}_3$.

* * *

5.39. [*Esonero 7/6/04*] Sia $\boldsymbol{S}_5$ il gruppo delle permutazioni sull'insieme $X = \{1,2,3,4,5\}$. Posto $V = \{1,2,3\}$, si indichi con $\boldsymbol{\Sigma}_V$ il sottogruppo di $\boldsymbol{S}_5$ formato dalle permutazioni che fissano (globalmente) V. Sia poi $\boldsymbol{H} = \boldsymbol{A}_5 \cap \boldsymbol{\Sigma}_V$ il sottogruppo delle permutazioni di classe pari che fissano V.

(*i*) Si descrivano le strutture cicliche del gruppo alterno $\boldsymbol{A}_5$, indicando il numero di permutazioni di ciascuna struttura ciclica.

(*ii*) Si determinino gli elementi di $\boldsymbol{H}$ e si dica di che tipo di sottogruppo di $\boldsymbol{S}_5$ si tratta.

Soluzione. (*i*) Risulta: $|\boldsymbol{A}_5| = \frac{5!}{2} = 60$. Le strutture cicliche di classe pari di $\boldsymbol{S}_5$ sono le seguenti:

$$(\_\ \_\ \_\ \_\ \_), \quad (\_\ \_\ \_), \quad (\_\ \_)(\_\ \_), \quad (\_).$$

I 5-cicli di $\boldsymbol{S}_5$ sono $\binom{5}{5}(5-1)! = 24$; i 3-cicli di $\boldsymbol{S}_5$ sono $\binom{5}{3}(3-1)! = 20$. Le coppie di 2-cicli disgiunti sono quindi $60 - (1 + 24 + 20) = 15$.

(*ii*) Nessuno dei 5-cicli di $\boldsymbol{S}_5$ può fissare V. Dei 3-cicli di $\boldsymbol{S}_5$, quelli che fissano V sono soltanto (123) e (132). Delle coppie di 2-cicli disgiunti di $\boldsymbol{S}_5$, quelle che fissano V [e quindi anche $X - V = \{4,5\}$] sono le seguenti tre: $(12)(45),\ (13)(45),\ (23)(45)$.

Si conclude che $\boldsymbol{H}$ è il seguente sottogruppo di $\boldsymbol{S}_5$:

$$\boldsymbol{H} = \{(1),\ (12)(45),\ (13)(45),\ (23)(45),\ (123),\ (132)\}.$$

Si tratta di un gruppo con sei elementi, di cui due di periodo 3 e tre di periodo 2. Pertanto $\boldsymbol{H} \cong \boldsymbol{S}_3$.

* * *

5.40. [*Esame 20/9/04*] (*i*) Verificare che nel gruppo simmetrico $\boldsymbol{S}_4$ un 3-ciclo σ ed un prodotto di due 2-cicli disgiunti γ non commutano tra loro.

(*ii*) Indicare gli elementi del gruppo alterno $\boldsymbol{A}_4$ e determinare il centro $\boldsymbol{\mathcal{Z}}(\boldsymbol{A}_4)$ di $\boldsymbol{A}_4$.

(*iii*) Dedurre da (*ii*) la struttura del gruppo $\boldsymbol{\mathcal{I}}(\boldsymbol{A}_4)$ degli automorfismi interni di $\boldsymbol{A}_4$ e descrivere esplicitamente almeno uno di tali automorfismi interni.

Soluzione. (*i*) $\boldsymbol{S}_4$ possiede otto 3-cicli e tre prodotti di 2-cicli disgiunti. Indicati con a,b,c,d i quattro elementi dell'insieme $\{1,2,3,4\}$, basterà verificare che, posto

$$\sigma = (abc),\ \gamma_1 = (ab)(cd),\ \gamma_2 = (ac)(bd),\ \gamma_3 = (ad)(bc),$$

risulta:

$$\sigma\,\gamma_1 \neq \gamma_1\,\sigma, \quad \sigma\,\gamma_2 \neq \gamma_2\,\sigma, \quad \sigma\,\gamma_3 \neq \gamma_3\,\sigma.$$

Infatti:

- $\sigma\,\gamma_1 = (abc)(ab)(cd) = (bcd), \quad \gamma_1\,\sigma = (ab)(cd)(abc) = (acd)$;
- $\sigma\,\gamma_2 = (abc)(ac)(bd) = (adb), \quad \gamma_2\,\sigma = (ac)(bd)(abc) = (bdc)$;
- $\sigma\,\gamma_3 = (abc)(ad)(bc) = (acd), \quad \gamma_3\,\sigma = (ad)(bc)(abc) = (adb)$.

(*ii*) Il gruppo alterno $\boldsymbol{A}_4$ è formato dalle dodici permutazioni pari di $\boldsymbol{S}_4$: si tratta della permutazione identica (1), degli otto 3-cicli e dei tre prodotti di 2-cicli disgiunti. Da (*i*) segue che nessun 3-ciclo commuta con un prodotto di 2-cicli disgiunti (e viceversa). Dunque $\boldsymbol{\mathcal{Z}}(\boldsymbol{A}_4) = \{(1)\}$.

(*ii*) È noto che, per ogni gruppo G risulta: $\boldsymbol{\mathcal{I}}(G) \cong G/\boldsymbol{\mathcal{Z}}(G)$. Dunque

$$\boldsymbol{\mathcal{I}}(\boldsymbol{A}_4) \cong \boldsymbol{A}_4/\{(1)\} \cong \boldsymbol{A}_4.$$

Dei dodici automorfismi interni di $\boldsymbol{A}_4$ descriviamo quello associato al 3-ciclo (123), cioè $\gamma = \gamma_{(123)}$. Si ha:

$\gamma((1)) = (123)(1)(132) = (1)$,
$\gamma((123)) = (123)(123)(132) = (123)$, $\gamma((132)) = (123)(132)(132) = (132)$,
$\gamma((124)) = (123)(124)(132) = (143)$, $\gamma((142)) = (123)(142)(132) = (134)$,
$\gamma((143)) = (123)(143)(132) = (234)$, $\gamma((134)) = (123)(134)(132) = (243)$,
$\gamma((234)) = (123)(234)(132) = (124)$, $\gamma((243)) = (123)(243)(132) = (142)$,
$\gamma((12)(34)) = (123)(12)(34)(132) = (13)(24)$,
$\gamma((13)(24)) = (123)(13)(24)(132) = (14)(23)$,
$\gamma((14)(23)) = (123)(14)(23)(132) = (12)(34)$.

* * *

5.41. Tenuto conto della struttura dei gruppi di ordine 8, verificare che in $\boldsymbol{S}_4$ esistono tre sottogruppi isomorfi a $\boldsymbol{D}_4$ e nessun altro tipo di sottogruppi di ordine 8.

Soluzione. $\boldsymbol{S}_4$ non ha elementi di periodo 8 e dunque non possiede sottogruppi isomorfi al gruppo ciclico di ordine 8.

Verifichiamo che $\boldsymbol{S}_4$ non possiede sottogruppi H isomorfi al gruppo $\mathbf{Q}$ delle unità dei quaternioni. È noto che $\mathbf{Q}$ possiede sei elementi di periodo 4. Allora H deve possedere tutti i sei 4-cicli di $\boldsymbol{S}_4$. Ma, ad esempio $(1234)(1243) = (142)$, mentre H non può possedere alcun 3-ciclo (perché $\mathbf{Q}$ non ha elementi di periodo 3).

Verifichiamo che $\boldsymbol{S}_4$ non possiede sottogruppi H isomorfi al gruppo $\boldsymbol{Z}_2\times\boldsymbol{Z}_4$. È noto che $\boldsymbol{Z}_2\times\boldsymbol{Z}_4$ possiede quattro elementi di periodo 4. Sia $\sigma = (1\,a\,b\,c) \in H$; escludendo $\sigma^{-1} = (1\,c\,b\,a)$, i restanti 4-cicli di $\boldsymbol{S}_4$ sono:

$$(1\,a\,c\,b),\ (1\,b\,a\,c),\ (1\,b\,c\,a),\ (1\,c\,a\,b).$$

Si verifica con semplici calcoli che il prodotto di σ per ciascuno di tali 4-cicli è un 3-ciclo e dunque non appartiene ad H. Ne segue che H possiede soltanto due elementi di periodo 4 (e non quattro, come richiesto).

Verifichiamo che $\boldsymbol{S}_4$ non possiede sottogruppi H isomorfi al gruppo $\boldsymbol{Z}_2\times\boldsymbol{Z}_2\times\boldsymbol{Z}_2$. È noto che $\boldsymbol{Z}_2\times\boldsymbol{Z}_2\times\boldsymbol{Z}_2$ possiede sette sottogruppi di Klein. Basterà allora verificare che in $\boldsymbol{S}_4$ esistono soltanto tre sottogruppi di Klein.

Un sottogruppo di Klein $V < \boldsymbol{S}_4$ contiene tre 2-cicli che commutano tra loro. Siano $(a\,b)$, $(c\,d) \in V$, diversi tra loro. Poiché commutano, sono necessariamente disgiunti [infatti due 2-cicli diversi e non disgiunti $(a\,b)$, $(a\,c)$ non commutano, come facilmente si verifica]. Ma di coppie di 2-cicli disgiunti $\boldsymbol{S}_4$ ne ha solo tre. Dunque $\boldsymbol{S}_4$ ha soltanto tre sottogruppi di Klein:

$$V_1 = \langle (12),\,(34)\rangle,\quad V_2 = \langle (13),\,(24)\rangle,\quad V_3 = \langle (14),\,(23)\rangle.$$

Verifichiamo infine che $\boldsymbol{S}_4$ possiede tre sottogruppi H isomorfi al gruppo diedrale $\boldsymbol{D}_4$.

Sia H un sottogruppo di $\boldsymbol{S}_4$, isomorfo a $\boldsymbol{D}_4$. H è generato da un 2-ciclo ρ e da un 4-ciclo φ, legati dalla relazione "diedrale" $\varphi\rho = \rho\varphi^3$.

Scelto ad esempio $\varphi = (1234)$ e $\rho = (13)$ [ovvero $\rho = (24)$], si verifica che

$$H_1 = \langle (1234),\,(13)\rangle = \{(1),\,(1234),\,(13)(24),\,(1432),\,(13),\,(12)(34),\,(23),\,(14)(23)\}$$

è diedrale. Si può poi verificare che, scegliendo come ρ un altro 2-ciclo (diverso da (24)) non è invece verificata la relazione diedrale.

I 4-cicli di $\boldsymbol{S}_4$ sono sei e due di essi sono già elementi di H_1. Restano quindi in $\boldsymbol{S}_4$ quattro 4-cicli. Partendo dai 4-cicli (1243) e (1324), si ottengono gli unici altri due sottogruppi diedrali di $\boldsymbol{S}_4$:

$$H_2 = \langle (1243),\,(14)\rangle,\quad H_3 = \langle (1324),\,(12)\rangle.$$

* * *

5.42. [*Esonero 6/6/05*] Nell'insieme $\mathfrak{M}_2(\boldsymbol{Z}_3)$ delle matrici quadrate di ordine 2 a valori in $\boldsymbol{Z}_3$, si consideri il sottoinsieme $\boldsymbol{H}$ formato dalle matrici triangolari superiori e a determinante $= \overline{1}$.

(*i*) Verificare che $\boldsymbol{H}$ è un sottogruppo del gruppo $G = \mathbf{SL}_2(\boldsymbol{Z}_3)$ [delle matrici a determinante $= \overline{1}$ in $\mathfrak{M}_2(\boldsymbol{Z}_3)$].

(*ii*) Elencare gli elementi di $\boldsymbol{H}$ e verificare se tale gruppo è ciclico.

(*iii*) Verificare se $\boldsymbol{H}$ è normale in G.

Soluzione. (*i*) Risulta: $\boldsymbol{H} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},\ \forall\, a,b,c \in \boldsymbol{Z}_3,\ ac = \overline{1} \right\}$. Poiché il prodotto di due matrici triangolari superiori [rispett. a determinante $= \overline{1}$] è ancora triangolare superiore [rispett. a determinante $= \overline{1}$], allora $\boldsymbol{H}\cdot\boldsymbol{H} \subseteq \boldsymbol{H}$. Essendo G finito, ciò è sufficiente per concludere che $\boldsymbol{H}$ è un sottogruppo di G.

(*ii*) Poiché, in $\boldsymbol{Z}_3$, $ac = \overline{1} \iff a = c = \overline{1}$ oppure $a = c = \overline{2}$, allora

$$\boldsymbol{H} = \left\{ \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{2} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{0} & \overline{2} \end{pmatrix}, \begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{2} \end{pmatrix}, \begin{pmatrix} \overline{2} & \overline{2} \\ \overline{0} & \overline{2} \end{pmatrix} \right\}.$$

$\boldsymbol{H}$ è un gruppo di 6 elementi: può essere isomorfo al ciclico $\boldsymbol{C}_6$ o a $\boldsymbol{S}_3$. Calcoliamone i periodi. Posto ad esempio $A = \begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{2} \end{pmatrix}$, si ha:

$$A^2 = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix},\ A^3 = \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{0} & \overline{2} \end{pmatrix},\ A^4 = \begin{pmatrix} \overline{1} & \overline{2} \\ \overline{0} & \overline{1} \end{pmatrix},\ A^5 = \begin{pmatrix} \overline{2} & \overline{2} \\ \overline{0} & \overline{2} \end{pmatrix},\ A^6 = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}.$$

Si conclude che $\circ(A) = 6$ e quindi $\boldsymbol{H} = \langle A \rangle \cong \boldsymbol{C}_6$.

(*iii*) Verifichiamo che $\boldsymbol{H}$ non è normale in G. Scelto $B = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix} \in G - \boldsymbol{H}$, basta verificare che $B\boldsymbol{H}B^{-1} \not\subseteq \boldsymbol{H}$. Scelta ad esempio in $\boldsymbol{H}$ la matrice A sopra definita, si ha infatti:

$$BAB^{-1} = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix} \begin{pmatrix} \overline{2} & \overline{1} \\ \overline{0} & \overline{2} \end{pmatrix} \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{2} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{2} & \overline{0} \end{pmatrix} \notin \boldsymbol{H}.$$

* * *

5.43. [*Esonero 7/6/04*] (*i*) Determinare il reticolo dei sottogruppi del gruppo $(\boldsymbol{Z}_3 \times \boldsymbol{Z}_3, +)$ [prodotto diretto di $\boldsymbol{Z}_3$ per se stesso].

(*ii*) Quanti sono gli omomorfismi da $\boldsymbol{Z}_9$ a $\boldsymbol{Z}_3 \times \boldsymbol{Z}_3$? Descriverne uno e calcolarne nucleo ed immagine.

Soluzione. (*i*) $\boldsymbol{Z}_3 \times \boldsymbol{Z}_3$ è formato dai nove elementi

$$(\overline{0},\overline{0}),\ (\overline{0},\overline{1}),\ (\overline{0},\overline{2}),\ (\overline{1},\overline{0}),\ (\overline{1},\overline{1}),\ (\overline{1},\overline{2}),\ (\overline{2},\overline{0}),\ (\overline{2},\overline{1}),\ (\overline{2},\overline{2}).$$

Tranne $(\overline{0},\overline{0})$ [che è elemento neutro e ha quindi periodo 1], tutti gli altri otto elementi hanno periodo 3. Ciascuno di essi, col proprio inverso, forma un sottogruppo ciclico di ordine 3. Per il teorema di Lagrange, non possono esistere in $\boldsymbol{Z}_3 \times \boldsymbol{Z}_3$ sottogruppi propri di altro ordine.

Dunque $\boldsymbol{Z}_3 \times \boldsymbol{Z}_3$ ammette i seguenti quattro sottogruppi propri

$$\langle (\overline{0},\overline{1}) \rangle = \{(\overline{0},\overline{0}),\ (\overline{0},\overline{1}),\ (\overline{0},\overline{2})\}, \qquad \langle (\overline{1},\overline{0}) \rangle = \{(\overline{0},\overline{0}),\ (\overline{1},\overline{0}),\ (\overline{2},\overline{0})\},$$
$$\langle (\overline{1},\overline{1}) \rangle = \{(\overline{0},\overline{0}),\ (\overline{1},\overline{1}),\ (\overline{2},\overline{2})\}, \qquad \langle (\overline{1},\overline{2}) \rangle = \{(\overline{0},\overline{0}),\ (\overline{1},\overline{2}),\ (\overline{2},\overline{1})\}.$$

(*ii*) Gli omomorfismi di $\boldsymbol{Z}_9$ in $\boldsymbol{Z}_3 \times \boldsymbol{Z}_3$ sono in corrispondenza con gli elementi di $\boldsymbol{Z}_3 \times \boldsymbol{Z}_3$ il cui periodo sia un divisore di 9. Per quanto sopra osservato, il periodo di ogni elemento di $\boldsymbol{Z}_3 \times \boldsymbol{Z}_3$ divide 9. Dunque gli omomorfismi richiesti sono nove. Ciascuno di essi è completamente individuato assegnando l'immagine del generatore $\tilde{1}$ di $\boldsymbol{Z}_9$.

Sia ad esempio $f : \boldsymbol{Z}_9 \to \boldsymbol{Z}_3 \times \boldsymbol{Z}_3$ tale che $f(\tilde{1}) = (\overline{1},\overline{2})$. Allora:

$$f(\tilde{0}) = (\overline{0},\overline{0}),\ f(\tilde{1}) = (\overline{1},\overline{2}),\ f(\tilde{2}) = (\overline{2},\overline{1}),$$
$$f(\tilde{3}) = (\overline{0},\overline{0}),\ f(\tilde{4}) = (\overline{1},\overline{2}),\ f(\tilde{5}) = (\overline{2},\overline{1}),$$
$$f(\tilde{6}) = (\overline{0},\overline{0}),\ f(\tilde{7}) = (\overline{1},\overline{2}),\ f(\tilde{8}) = (\overline{2},\overline{1}).$$

Risulta: $Ker(f) = \langle \tilde{3} \rangle$ e $Im(f) = \langle (\overline{1},\overline{2}) \rangle$.

* * *

5.44. [*Esonero 6/6/05*] (*i*) Determinare il reticolo dei sottogruppi del gruppo prodotto diretto $\boldsymbol{Z}_2 \times \boldsymbol{Z}_6$.

(*ii*) Determinare gli omomorfismi $f : \boldsymbol{Z}_{12} \to \boldsymbol{Z}_2 \times \boldsymbol{Z}_6$ tali che $|Im(f)| = 6$.

Soluzione. (*i*) Il gruppo $G = \boldsymbol{Z}_2 \times \boldsymbol{Z}_6$ è costituito dai seguenti 12 elementi

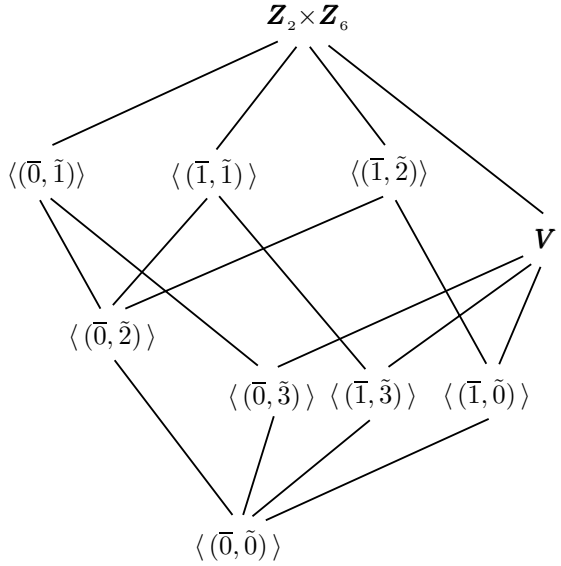
$$(\overline{0},\tilde{0}),\ (\overline{0},\tilde{1}),\ (\overline{0},\tilde{2}),\ (\overline{0},\tilde{3}),\ (\overline{0},\tilde{4}),\ (\overline{0},\tilde{5});\ (\overline{1},\tilde{0}),\ (\overline{1},\tilde{1}),\ (\overline{1},\tilde{2}),\ (\overline{1},\tilde{3}),\ (\overline{1},\tilde{4}),\ (\overline{1},\tilde{5}),$$

i cui periodi sono rispettivamente: 1, 6, 3, 2, 3, 6; 2, 6, 6, 2, 6, 6.

Essendo abeliano, G ha soltanto sottogruppi abeliani. Poiché ha sei elementi di periodo 6, ha tre sottogruppi ciclici di ordine 6, cioè

$$\langle(\overline{0},\tilde{1})\rangle = \langle(\overline{0},\tilde{5})\rangle,\ \ \langle(\overline{1},\tilde{1})\rangle = \langle(\overline{1},\tilde{5})\rangle,\ \ \langle(\overline{1},\tilde{2})\rangle = \langle(\overline{1},\tilde{4})\rangle.$$

Poiché G ha due soli elementi di periodo 3, allora G ha un solo sottogruppo ciclico di ordine 3: $\langle(\overline{0},\tilde{2})\rangle = \langle(\overline{0},\tilde{4})\rangle$. Infine, avendo G tre elementi di periodo 2, allora ha tre sottogruppi ciclici di ordine 2 ed un solo sottogruppo $\boldsymbol{V}$ di Klein da essi generato. Pertanto il reticolo dei sottogruppi è il seguente:



(*ii*) Denotiamo con $\underline{k}$ gli elementi di $\boldsymbol{Z}_{12}$. Ogni omomorfismo $f:\boldsymbol{Z}_{12}\to\boldsymbol{Z}_2\times\boldsymbol{Z}_6$ è individuato assegnando l'immagine di $\underline{1}\in\boldsymbol{Z}_{12}$. Inoltre $Im(f)=\langle f(\underline{1})\rangle$ e quindi $|Im(f)| = |\langle f(\underline{1})\rangle| = \circ(f(\underline{1}))$. Poiché deve essere verificata la condizione $|Im(f)|=6$, allora gli omomorfismi richiesti sono sei (uno per ciascun elemento di $\boldsymbol{Z}_2\times\boldsymbol{Z}_6$ di periodo 6):

$$f_1:\underline{k}\to k(\overline{0},\tilde{1}) = (\overline{0},\tilde{k}),\ \ \forall\,\underline{k}\in\boldsymbol{Z}_{12},\quad f_2:\underline{k}\to k(\overline{0},\tilde{5}) = (\overline{0},\tilde{5k}),\ \ \forall\,\underline{k}\in\boldsymbol{Z}_{12},$$
$$f_3:\underline{k}\to k(\overline{1},\tilde{1}) = (\overline{k},\tilde{k}),\ \ \forall\,\underline{k}\in\boldsymbol{Z}_{12},\quad f_4:\underline{k}\to k(\overline{1},\tilde{5}) = (\overline{k},\tilde{5k}),\ \ \forall\,\underline{k}\in\boldsymbol{Z}_{12},$$
$$f_5:\underline{k}\to k(\overline{1},\tilde{2}) = (\overline{k},\tilde{2k}),\ \ \forall\,\underline{k}\in\boldsymbol{Z}_{12},\quad f_6:\underline{k}\to k(\overline{1},\tilde{4}) = (\overline{k},\tilde{4k}),\ \ \forall\,\underline{k}\in\boldsymbol{Z}_{12}.$$

* * *

5.45. [*Esame 6/7/04*] Verificare che esistono quattro omomorfismi dal gruppo $(\boldsymbol{Z}_{10},+)$ al gruppo $(\boldsymbol{Z}_2\times\boldsymbol{Z}_4,+)$. Di ciascuno determinare nucleo ed immagine.

Soluzione. Sia $\Psi:\boldsymbol{\mathcal{H}om}(\boldsymbol{Z}_{10},\boldsymbol{Z}_2\times\boldsymbol{Z}_4)\to\boldsymbol{Z}_2\times\boldsymbol{Z}_4$ tale che

$$\Psi(f) = f(\overline{1}),\ \ \forall\, f\in\boldsymbol{\mathcal{H}om}(\boldsymbol{Z}_{10},\boldsymbol{Z}_2\times\boldsymbol{Z}_4).$$

È noto che Ψ è iniettiva e che $Im(\Psi)=\{x\in\boldsymbol{Z}_2\times\boldsymbol{Z}_4\ :\ \circ(x)\,\big|\,10\}$. Gli elementi di $\boldsymbol{Z}_2\times\boldsymbol{Z}_4$ ed i loro periodi sono rispettivamente:

$$\begin{array}{cccccccc}(\overline{0},\tilde{0}) & (\overline{0},\tilde{1}) & (\overline{0},\tilde{2}) & (\overline{0},\tilde{3}) & (\overline{1},\tilde{0}) & (\overline{1},\tilde{1}) & (\overline{1},\tilde{2}) & (\overline{1},\tilde{3})\\ 1 & 4 & 2 & 4 & 2 & 4 & 2 & 4\end{array}$$

e quindi gli elementi di $\boldsymbol{Z}_2\times\boldsymbol{Z}_4$ il cui periodo è un divisore di 10 sono $(\overline{0},\tilde{0})$, $(\overline{0},\tilde{2})$, $(\overline{1},\tilde{0})$, $(\overline{1},\tilde{2})$.

Ad essi corrispondono i quattro omomorfismi cercati:

$$\mathbf{0} = f_0:\boldsymbol{Z}_{10}\to\boldsymbol{Z}_2\times\boldsymbol{Z}_4 \text{ tale che } f_0(\tilde{t}) = (\overline{0},\tilde{0}),\ \ \forall\,\tilde{t}\in\boldsymbol{Z}_{10};$$
$$f_1:\boldsymbol{Z}_{10}\to\boldsymbol{Z}_2\times\boldsymbol{Z}_4 \text{ tale che } f_1(\tilde{t}) = (\overline{0},\tilde{2t}),\ \ \forall\,\tilde{t}\in\boldsymbol{Z}_{10};$$
$$f_2:\boldsymbol{Z}_{10}\to\boldsymbol{Z}_2\times\boldsymbol{Z}_4 \text{ tale che } f_2(\tilde{t}) = (\overline{1}t,\tilde{0}),\ \ \forall\,\tilde{t}\in\boldsymbol{Z}_{10};$$
$$f_3:\boldsymbol{Z}_{10}\to\boldsymbol{Z}_2\times\boldsymbol{Z}_4 \text{ tale che } f_3(\tilde{t}) = (\overline{1}t,\tilde{2}t),\ \ \forall\,\tilde{t}\in\boldsymbol{Z}_{10};$$

Si ha:

$$\begin{aligned}
&Ker(f_0) = \boldsymbol{Z}_{10}; && Im(f_0) = \{(\overline{0}, \tilde{0})\};\\
&Ker(f_1) = \langle\overline{2}\rangle \cong \boldsymbol{Z}_5; && Im(f_1) = \langle(\overline{0}, \tilde{2})\rangle \cong \boldsymbol{Z}_2;\\
&Ker(f_2) = \langle\overline{2}\rangle \cong \boldsymbol{Z}_5; && Im(f_2) = \langle(\overline{1}, \tilde{0})\rangle \cong \boldsymbol{Z}_2;\\
&Ker(f_3) = \langle\overline{2}\rangle \cong \boldsymbol{Z}_5; && Im(f_3) = \langle(\overline{1}, \tilde{2})\rangle \cong \boldsymbol{Z}_2.
\end{aligned}$$

* * *

5.46. Siano $G = \boldsymbol{Z}_6 \times \boldsymbol{Z}_4$, $G' = \boldsymbol{Z}_{12}$.

(*i*) Verificare che gli omomorfismi da G a G' sono 24.

(*ii*) Indicarne uno che sia suriettivo e calcolarne il nucleo.

(*iii*) Indicarne uno che non sia suriettivo (e non banale) e calcolarne nucleo ed immagine.

Soluzione. (*i*) Denotiamo con $\tilde{t}$ un elemento di $\boldsymbol{Z}_6$, con $\breve{t}$ un elemento di $\boldsymbol{Z}_4$ e con $\overline{t}$ un elemento di $\boldsymbol{Z}_{12}$. Il prodotto diretto $G = \boldsymbol{Z}_6 \times \boldsymbol{Z}_4$ è generato da $(\tilde{0}, \breve{1})$, $(\tilde{1}, \breve{0})$. Infatti

$$(\tilde{s}, \breve{t}) = s(\tilde{0}, \breve{1}) + t(\tilde{1}, \breve{0}), \ \forall\, (\tilde{s}, \breve{t}) \in \boldsymbol{Z}_6 \times \boldsymbol{Z}_4.$$

Se $f : \boldsymbol{Z}_6 \times \boldsymbol{Z}_4 \to \boldsymbol{Z}_{12}$ è un omomorfismo, allora, posto

$$\overline{a} = f\big((\tilde{0}, \breve{1})\big), \ \overline{b} = f\big((\tilde{1}, \breve{0})\big),$$

risulta: $\circ(\overline{a}) \,\big|\, \circ((\tilde{1}, \breve{0})) = 6$, $\circ(\overline{b}) \,\big|\, \circ((\tilde{0}, \breve{1})) = 4$. In $\boldsymbol{Z}_{12}$ si ha:

$$\circ(\overline{a}) \,\big|\, 6 \iff \overline{a} \in \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}; \ \circ(\overline{b}) \,\big|\, 4 \iff \overline{b}s \in \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}.$$

La coppia $(\overline{a}, \overline{b})$ può essere scelta in 24 modi. Per ognuna di tali scelte è definita l'applicazione

$$f : \boldsymbol{Z}_6 \times \boldsymbol{Z}_4 \to \boldsymbol{Z}_{12} \ \text{ tale che } \ f((\tilde{s}, \breve{t})) = \overline{sa + tb}.$$

Verifichiamo che tale applicazione è ben definita: se $\tilde{s} = \tilde{s}_1$ e $\breve{t} = \breve{t}_1$, allora $6 \,\big|\, s - s_1$, $4 \,\big|\, t - t_1$; inoltre $2 \,\big|\, a$, $3 \,\big|\, b$ e quindi $12 \,\big|\, a(s - s_1) + b(t - t_1) = (as + bt) - (as_1 + bt_1)$.

Verifichiamo infine che f è un omomorfismo. Infatti

$$f\big((\tilde{s}, \breve{t}) + (\tilde{s}_1, \breve{t}_1)\big) = f\big((\tilde{s} + \tilde{s}_1, \breve{t} + \breve{t}_1)\big) = \overline{(s + s_1)a + (t + t_1)b} = f((\tilde{s}, \breve{t})) + f((\tilde{s}_1, \breve{t}_1)).$$

(*ii*) Sia $f : G \to G'$ un omomorfismo. Risulta:

$$f \text{ è suriettiva} \iff \overline{1} \in Im(f) \iff \exists\, s, t \in \boldsymbol{Z} : \overline{1} = \overline{sa + tb}.$$

Scelti a, b coprimi, vale l'identità di Bézout $1 = sa + tb$, da cui $\overline{1} = \overline{sa + tb}$ (in $\boldsymbol{Z}_{12}$). Allora $f((\tilde{s}, \breve{t})) = \overline{sa + tb} = \overline{1}$ ed f è suriettiva.

Ad esempio, scegliamo $\overline{a} = \overline{4}$, $\overline{b} = \overline{3}$. Risulta:

$$f((\tilde{s}, \breve{t})) = \overline{4s + 3t}, \ \forall\, (\tilde{s}, \breve{t}) \in \boldsymbol{Z}_6 \times \boldsymbol{Z}_4.$$

Dal teorema fondamentale di omomorfismo, $\boldsymbol{Z}_{12} \cong (\boldsymbol{Z}_6 \times \boldsymbol{Z}_4)\big/_{Ker(f)}$ e quindi $|Ker(f)| = 2$. Poiché $f((\tilde{3}, \breve{0})) = \overline{4 \cdot 3 + 3 \cdot 0} = \overline{0}$, allora $Ker(f) = \langle(\tilde{3}, \breve{0})\rangle$.

(*iii*) Sia f definito come in (*i*) tramite la coppia $(\overline{a}, \overline{b})$. Si scelgano $\overline{a}, \overline{b} \in \boldsymbol{Z}_{12}$ tali che a, b non siano coprimi. Se ad esempio $2 \,\big|\, a$, $2 \,\big|\, b$, allora $Im(f) \leq \langle\overline{2}\rangle$ e quindi f non è suriettivo.

Scegliamo ad esempio $a = 2, b = 6$. Allora $Im(f) = \langle\overline{2}\rangle$ [infatti $g((\tilde{4}, \breve{3})) = \overline{8 + 18} = \overline{2}$]. Dal teorema fondamentale di omomorfismo, $\frac{24}{|Ker(f)|} = |\langle\overline{2}\rangle| = 6$, cioè $|Ker(f)| = 4$. Ovviamente $(\tilde{3}, \breve{1})) \in Ker(f)$ e $\circ((\tilde{3}, \breve{1}))) = 4$. Si conclude che $Ker(f)$ è ciclico e risulta

$$Ker(f) = \{(\tilde{0}, \breve{0})), (\tilde{3}, \breve{1})), (\tilde{0}, \breve{2})), (\tilde{3}, \breve{3}))\}.$$

* * *

5.47. Determinare l'insieme $\boldsymbol{\mathcal{H}om}(\boldsymbol{Z}_4, \boldsymbol{V})$ degli omomorfismi da $\boldsymbol{Z}_4$ al gruppo di Klein $\boldsymbol{V}$. Di ciascun omomorfismo ottenuto specificare nucleo ed immagine.

Soluzione. Si ponga $\boldsymbol{V} = \{1, a, b, c\}$ [con $a^2 = b^2 = c^2 = 1$, $ba = ab$]. Per ogni $f \in \boldsymbol{\mathcal{H}om}(\boldsymbol{Z}_4, \boldsymbol{V})$, f è completamente individuato conoscendo $f(\overline{1}) \in V$. Deve risultare: $\circ(f(\overline{1})) \,\big|\, \circ(\overline{1}) = 4$. Ma tale condizione non porta ad alcuna restrizione per f [infatti in $\boldsymbol{V}$ il periodo di ogni elemento è un divisore di 4]. Pertanto esistono quattro omomorfismi $f_i \in \boldsymbol{\mathcal{H}om}(\boldsymbol{Z}_4, \boldsymbol{V})$ $(0 \leq i \leq 3)$, così definiti:

$$f_0(\overline{1}) = 1, \ f_1(\overline{1}) = a, \ f_2(\overline{1}) = b, \ f_3(\overline{1}) = c.$$

Risulta:
$f_0(\overline{2}) = 1^2 = 1, f_0(\overline{3}) = 1^3 = 1$; $Ker(f_0) = \boldsymbol{Z}_4$, $Im(f_0) = \{1\}$ (f è l'omomorfismo banale);
$f_1(\overline{2}) = a^2 = 1, f_1(\overline{3}) = a^3 = a$; $Ker(f_1) = \langle\overline{2}\rangle$, $Im(f_1) = \langle a\rangle$;
$f_2(\overline{2}) = b^2 = 1, f_2(\overline{3}) = b^3 = b$; $Ker(f_2) = \langle\overline{2}\rangle$, $Im(f_2) = \langle b\rangle$;
$f_3(\overline{2}) = c^2 = 1, f_3(\overline{3}) = c^3 = c$; $Ker(f_3) = \langle\overline{2}\rangle$, $Im(f_3) = \langle c\rangle$.

* * *

5.48. Sono assegnati i gruppi $\boldsymbol{S}_3$ e $\boldsymbol{V}$ (gruppo di Klein).
(*i*) Determinare gli omomorfismi da $\boldsymbol{S}_3$ a $\boldsymbol{V}$.
(*ii*) Determinare gli omomorfismi da $\boldsymbol{V}$ a $\boldsymbol{S}_3$.

Soluzione. È noto che $\boldsymbol{V} = \langle a, b \,|\, a^2 = b^2 = 1, ba = ab\rangle$ e che $\boldsymbol{S}_3$ può essere generato da un 2-ciclo e da un 3-ciclo, ovvero da due 2-cicli distinti.

(*i*) Poiché $\boldsymbol{S}_3 = \langle(12), (123)\rangle$, un omomorfismo $f : \boldsymbol{S}_3 \to \boldsymbol{V}$ è individuato assegnando gli elementi $f((12)), f((123)) \in \boldsymbol{V}$. Poiché inoltre $\circ\big(f((123))\big) \,\big|\, \circ((123)) = 3$, necessariamente $f((123)) = 1$; di conseguenza, anche $f((132)) = 1$. La condizione $\circ\big(f((12))\big) \,\big|\, \circ((12)) = 2$ non pone invece alcuna limitazione a $f((12))$: dunque esistono quattro possibili immagini di (12) in $\boldsymbol{V}$. Infine, poiché $(13) = (12)(123)$ e $(23) = (12)(132)$, allora $f((13)) = f((12)) = f((23))$, cioè f si mantiene costante sui 2-cicli.

In conclusione, $\mathcal{H}om(\boldsymbol{S}_3, \boldsymbol{V})$ è formato da quattro omomorfismi f_0, f_1, f_2, f_3 tali che

$$f_0((12)) = 1, \quad f_1((12)) = a, \quad f_2((12)) = b, \quad f_3((12)) = c.$$

In particolare f_0 è l'omomorfismo banale, $Ker(f_i) = \langle(123)\rangle$, $\forall\, i = 1, 2, 3$, ed infine $Im(f_1) = \langle a\rangle$, $Im(f_2) = \langle b\rangle$, $Im(f_3) = \langle c\rangle$.

(*ii*) Sia $g : \boldsymbol{V} \to \boldsymbol{S}_3$ un omomorfismo. g è completamente individuato assegnando gli elementi $f(a), f(b) \in \boldsymbol{S}_3$. Poiché $\circ(g(a)) \,\big|\, 2$ e $\circ(g(b)) \,\big|\, 2$, allora $g(a)$ e $g(b)$ non possono essere 3-cicli. Inoltre $g(a), g(b)$ non possono essere due 2-cicli distinti tra loro [altrimenti, ricordato che due 2-cicli diversi generano $\boldsymbol{S}_3$, sarebbe $Im(g) = \boldsymbol{S}_3$ e ciò è assurdo per ovvie ragioni di cardinalità]. Oltre all'omomorfismo banale g_0, tale che $g_0(a) = g_0(b) = (1)$, esistono nove omomorfismi, cioè

$$g_1 : \begin{matrix} a \to (1) \\ b \to (12), \end{matrix} \quad g_2 : \begin{matrix} a \to (1) \\ b \to (13), \end{matrix} \quad g_3 : \begin{matrix} a \to (1) \\ b \to (23), \end{matrix}$$

$$g_4 : \begin{matrix} a \to (12) \\ b \to (1), \end{matrix} \quad g_5 : \begin{matrix} a \to (13) \\ b \to (1), \end{matrix} \quad g_6 : \begin{matrix} a \to (23) \\ b \to (1), \end{matrix}$$

$$g_7 : \begin{matrix} a \to (12) \\ b \to (12), \end{matrix} \quad g_8 : \begin{matrix} a \to (13) \\ b \to (13), \end{matrix} \quad g_9 : \begin{matrix} a \to (23) \\ b \to (23). \end{matrix}$$

Si noti che i primi tre omomorfismi hanno nucleo $\langle a\rangle$, i tre successivi hanno nucleo $\langle b\rangle$ e gli ultimi tre hanno nucleo $\langle ab\rangle$. Le immagini sono i tre sottoguppi ciclici di ordine 2 di $\boldsymbol{S}_3$.

* * *

5.49. [*Esame 23/9/03*] Sia $\varphi : \boldsymbol{Z}[X] \to \boldsymbol{Z}[X]$ l'applicazione così definita:

$$\varphi(a_0 + a_1X + \,...\, + a_nX^n) = a_0 + a_2X^2 + \,...\, + a_{2k}X^{2k} \quad (\text{con } k \text{ massimo tale che } 2k \le n)$$

[cioè φ annulla tutti i monomi di grado dispari e fissa quelli di grado pari].
(*i*) Verificare che φ non è iniettiva e determinare $Im(\varphi)$.
(*ii*) Verificare che l'applicazione $\Phi : \boldsymbol{Z}[X] \to \boldsymbol{Z}[X]$ tale che

$$\Phi(f(X)) = f(X^2), \ \forall\, f = f(X) \in \boldsymbol{Z}[X],$$

induce un isomorfismo Ψ tra $\boldsymbol{Z}[X]$ e $Im(\varphi)$.
(*iii*) Verificare che φ è un endomorfismo del gruppo $(\boldsymbol{Z}[X], +)$ e determinare $Ker(\varphi)$.
(*iv*) Dedurre dal teorema fondamentale di omomorfismo che il gruppo quoziente $\boldsymbol{Z}[X]/_{Ker(\varphi)}$ è isomorfo al gruppo $(\boldsymbol{Z}[X], +)$. Esplicitare un siffatto isomorfismo.

Soluzione. (*i*) Risulta: $\varphi(0) = \varphi(X) = 0$: dunque φ non è iniettiva. Posto

$$\boldsymbol{Z}[X^2] = \big\{ \sum_{i=0}^{n} a_i X^{2i},\ \forall\, a_i \in \boldsymbol{Z},\ \forall\, n \geq 0 \big\},$$

è evidente che $Im(\varphi) \subseteq \boldsymbol{Z}[X^2]$. Viceversa, ogni polinomio in $\boldsymbol{Z}[X^2]$ è immagine di se stesso tramite φ. Dunque $Im(\varphi) = \boldsymbol{Z}[X^2]$.

(*ii*) Φ ha ovviamente per immagine $Im(\varphi) = \boldsymbol{Z}[X^2]$. Φ è un omomorfismo: infatti

$$\Phi(f+g) = (f+g)(X^2) = f(X^2) + g(X^2) = \Phi(f) + \Phi(g).$$

Inoltre $Ker(\Phi) = \{0\}$. Infatti se $f = \sum_{i=0}^{n} a_i X^i \in Ker(\Phi)$, allora

$$0 = f(X^2) = \sum_{i=0}^{n} a_i X^{2i} \text{ e dunque } a_0 = ... = a_n = 0, \text{ cioè } f = 0.$$

Dal teorema fondamentale di omomorfismo segue che Φ induce l'isomorfismo

$$\Psi : \boldsymbol{Z}[X] \to \boldsymbol{Z}[X^2] \text{ tale che } \Psi(f(X)) = f(X^2).$$

(*iii*) $\forall\, f = \sum_{i=0}^{n} a_i X^i,\ g = \sum_{j=0}^{m} b_j X^j \in \mathbf{Z}[X]$, risulta [supposto $n \geq m$ e posto $b_{m+1} = ... = b_n = 0$]:

$$\varphi(f+g) = \varphi\big(\sum_{i=0}^{n}(a_i + b_i)X^i\big) = \sum_{2k \leq n} (a_{2k} + b_{2k})X^{2k} =$$

$$= \sum_{2k \leq n} a_{2k} X^{2k} + \sum_{2k \leq n} b_{2k} X^{2k} = \varphi(f) + \varphi(g).$$

Dunque φ è un omomorfismo di $(\boldsymbol{Z}[X], +)$ in sé. Risulta:

$$Ker(\varphi) = \big\{ f \in \boldsymbol{Z}[X] :\ \varphi(f) = 0 \big\} = \left\{ \begin{array}{c} \text{polinomi in } \boldsymbol{Z}[X] \text{ aventi solo} \\ \text{monomi di grado dispari} \end{array} \right\} = X\,\boldsymbol{Z}[X^2].$$

(*iv*) Dal teorema fondamentale di omomorfismo, l'applicazione

$$\varphi^* : \boldsymbol{Z}[X]\big/_{Ker(\varphi)} \to Im(\varphi) \text{ tale che } \varphi^*(f + Ker(\varphi)) = \varphi(f)$$

è un isomorfismo di gruppi. Ne segue che

$$\Psi^{-1} \circ \varphi^* : \boldsymbol{Z}[X]\big/_{Ker(\varphi)} \to \boldsymbol{Z}[X^2] \to \boldsymbol{Z}[X]$$

è un isomorfismo. Risulta, per ogni $f = \sum_{i=0}^{n} a_i X^i$,

$$\big(\Psi^{-1} \circ \varphi^*\big)(f + Ker(\varphi)) = \Psi^{-1}\big(\sum_{k \leq n/2} a_{2k} X^{2k}\big) = \sum_{k \leq n/2} a_{2k} X^k.$$

* * *

5.50. Sia $(Q, \cdot)$ il gruppo definito "per generatori e relazioni" in questo modo:

$$Q = \big\langle -1,\ a,\ b,\ c \ \big|\ a^2 = b^2 = c^2 = -1,\ (-1)^2 = 1,\ ab = (-1)ba = c \big\rangle.$$

(*i*) Verificare che Q coincide (a meno di isomorfismi) con il gruppo $\mathbf{Q}$ delle unità dei quaternioni.

(*ii*) Determinare il gruppo degli automorfismi interni $\boldsymbol{\mathcal{I}}(Q)$.

(*iii*) Verificare che ogni automorfismo $f \in \boldsymbol{Aut}(Q)$ è completamente individuato assegnando (opportunamente) una coppia di elementi $(f(a), f(b)) \in Q \times Q$. Dedurne che $|\boldsymbol{Aut}(Q)| = 24$.

Soluzione. (*i*) Risulta: $(-1)a = a(-1)$ [infatti $(-1)a = a^2 a = a\,a^2 = a(-1)$]. Analogamente, $(-1)b = b(-1)$ e $(-1)c = c(-1)$. Ne segue che -1 commuta con ogni elemento di Q. Si porrà:

$$-a := (-1)a,\ -b := (-1)b,\ -c := (-1)c.$$

Ne segue che $(-1)ba = (-b)a = b(-a)$ e tale elemento viene indicato brevemente come $-ba$.

Verifichiamo ora che $bc = a = -cb$, $ca = b = -ac$. Si ha:

$$bc = b(-ba) = (b(-b))a = 1\,a = a, \quad cb = (ab)b = a\,b^2 = a(-1) = -a,$$

$$ca = (-ba)a = -b(a^2) = -b(-1) = b, \quad ac = a(ab) = a^2\,b = (-1)a = -a.$$

Si ottiene quindi che $Q = \{1, -1, a, -a, b, -b, c, -c\}$ e che le relazioni che legano i generatori di Q sono esattamente quelle del gruppo $\mathbf{Q}$ delle unità dei quaternioni. Si conclude che $Q \cong \mathbf{Q}$.

(*ii*) Utilizzeremo l'isomorfismo $\boldsymbol{\mathcal{I}}(Q) \cong Q/_{\boldsymbol{\mathcal{Z}}(Q)}$, dove $\boldsymbol{\mathcal{Z}}(Q) = \{x \in Q \,\big|\, xy = yx,\ \forall\, y \in Q\}$ è il centro di Q. Dalle precedenti considerazioni si osserva subito che $\boldsymbol{\mathcal{I}}(Q) = \langle -1\rangle = \{1, -1\}$. Ne segue che $|\boldsymbol{\mathcal{I}}(Q)| = \frac{8}{2} = 4$.

Per ottenere i quattro automorfismi interni di Q basta scegliere quattro elementi di Q che appartengano a laterali (destri) differenti *mod* $\langle -1\rangle$, ad esempio 1, a, b, c. Dunque

$$\begin{array}{l}\gamma_1 = \mathbf{1}_Q : Q \to Q \ \text{ tale che } \ \gamma_1(y) = y,\ \forall\, y \in Q;\\ \gamma_a : Q \to Q \ \text{ tale che } \ \gamma_a(y) = a\,y\,a^{-1} = a\,y\,a^3,\ \forall\, y \in Q\\ \gamma_b : Q \to Q \ \text{ tale che } \ \gamma_b(y) = b\,y\,b^{-1} = b\,y\,b^3,\ \forall\, y \in Q\\ \gamma_c : Q \to Q \ \text{ tale che } \ \gamma_c(y) = c\,y\,c^{-1} = c\,y\,c^3,\ \forall\, y \in Q\end{array}$$

Risulta in particolare: $\gamma_a(a) = a$, $\gamma_a(b) = -b$; $\gamma_b(a) = -a$, $\gamma_b(b) = b$; $\gamma_c(a) = -a$, $\gamma_c(b) = -b$.

Si verifica facilmente che $\gamma_a^2 = \gamma_b^2 = \gamma_c^2 = \mathbf{1}_Q$. Pertanto $\boldsymbol{\mathcal{I}}(Q) \cong \boldsymbol{V}$ (gruppo di Klein).

(*iii*) Sia $f \in \boldsymbol{\mathcal{A}ut}(Q)$. Poiché -1 è l'unico elemento di Q di periodo 2, allora necessariamente $f(-1) = -1$. Ne segue che

$$f(-a) = -f(a),\ f(-b) = -f(b),\ f(-c) = -f(c).$$

Inoltre $f(c) = f(ab) = f(a)f(b)$. Ne segue che f è completamente assegnato conoscendo la coppia $(f(a), f(b))$.

Infine, si osservi che $f(a)$, $f(b)$ non possono assumere valori opposti [cioè, ad esempio c, $-c$]. Infatti si avrebbe $f(c) = f(ab) = f(a)f(b) = c(-c) = 1 = f(1)$: assurdo (in quanto f è iniettivo).

Gli elementi di $\boldsymbol{\mathcal{A}ut}(Q)$ corrispondono biunivocamente alle seguenti 24 coppie di elementi di Q:

$$\begin{array}{l}(a,b),\ (a,-b),\ (-a,b),\ (-a,-b),\\ (b,a),\ (b,-a),\ (-b,a),\ (-b,-a),\\ (a,c),\ (a,-c),\ (-a,c),\ (-a,-c),\\ (c,a),\ (c,-a),\ (-c,a),\ (-c,-a),\\ (b,c),\ (b,-c),\ (-b,c),\ (-b,-c),\\ (c,b),\ (c,-b),\ (-c,b),\ (-c,-b).\end{array}$$

In particolare, γ_1, γ_a, γ_b, γ_c corrispondono ordinatamente alle prime quattro coppie.

Nota. Calcolando (con pazienza) i periodi dei 24 omomorfismi, si scopre che $\boldsymbol{\mathcal{A}ut}(Q)$ "ha gli stessi periodi" di $\boldsymbol{S}_4$. Tale fatto suggerisce che $\boldsymbol{\mathcal{A}ut}(Q) \cong \boldsymbol{S}_4$.

* * *

5.51. Sia $(G, \cdot)$ un gruppo, g un suo elemento e $[g]_\sim$ la relativa classe di coniugio.

(*i*) Verificare che l'insieme

$$\boldsymbol{C}(g) := \{x \in G \,\big|\, gx = xg\} \ \text{ (detto } \textit{centralizzante di } g \textit{ in } G)$$

è un sottogruppo di G. Inoltre $\boldsymbol{C}(g) \geq \langle g\rangle$.

(*ii*) Verificare che $(G : \boldsymbol{C}(g)) = \big|[g]_\sim\big|$ (cioè l'indice del centralizzante di un elemento è la cardinalità dell'insieme dei suoi coniugati).

(*iii*) Se G è un gruppo finito e se $\{g_i\}_{i\in I}$ è una famiglia di rappresentanti di tutte le classi di coniugio (uno per ciacuna classe), verificare che vale la seguente formula

$$|G| = \sum_{i\in I} \frac{|G|}{\big|\boldsymbol{C}(g_i))\big|}$$

(detta *equazione delle classi in* G).

(*iv*) Determinare in $\boldsymbol{S}_4$ un rappresentante per ogni classe di coniugio e calcolarne il centralizzante.

Soluzione. (*i*) Ovviamente $1 \in \boldsymbol{C}(g)$ [infatti $g1 = 1g$]. Se $x, y \in \boldsymbol{C}(g)$, allora $xy \in \boldsymbol{C}(g)$ [infatti $(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$]. Infine, se $x \in \boldsymbol{C}(g)$, allora $x^{-1} \in \boldsymbol{C}(g)$ [infatti $gx = xg \implies (gx)^{-1} = (xg)^{-1} \implies x^{-1}g^{-1} = g^{-1}x^{-1} \implies x^{-1} = g^{-1}x^{-1}g \implies gx^{-1} = x^{-1}g$].

L'ultima affermazione è ovvia: infatti ogni potenza di g commuta con g.

(*ii*) Si ponga

$$\Phi : [g]_\sim \to \mathfrak{L}_s(\boldsymbol{C}(g)) \ \text{ tale che } \ \Phi(xgx^{-1}) = x\boldsymbol{C}(g),\ \forall\, xgx^{-1} \in [g]_\sim.$$

Si tratta di verificare che l'applicazione è ben definita: $xgx^{-1} = ygy^{-1} \implies x\boldsymbol{C}(g) = y\boldsymbol{C}(g)$. Infatti:

$$xgx^{-1} = ygy^{-1} \implies y^{-1}xgx^{-1} = gy^{-1} \implies y^{-1}xg = gy^{-1}x \implies$$

$$\Longrightarrow\ y^{-1}x\in \boldsymbol{C}(g)\ \Longrightarrow\ y^{-1}x\boldsymbol{C}(g)=\boldsymbol{C}(g)\ \Longrightarrow\ x\boldsymbol{C}(g)=y\boldsymbol{C}(g).$$

La stessa catena di implicazioni, percorse a ritroso, dimostra che Φ è iniettiva: $x\boldsymbol{C}(g)=y\boldsymbol{C}(g)\ \Longrightarrow\ xgx^{-1}=ygy^{-1}$. Infine, che Φ sia suriettiva è ovvio $[x\boldsymbol{C}(g)=\Phi(xgx^{-1})]$. Si conclude che Φ è biiettiva e quindi

$$\big|[g]_{\sim}\big|=\big|\mathfrak{L}_s(\boldsymbol{C}(g))\big|=(G:\boldsymbol{C}(g)).$$

(*iii*) Si ha: $G=\bigsqcup_{i\in I}[g_i]_{\sim}$ [infatti $\{[g_i]_{\sim}\}_{i\in I}$ è una partizione di G]. Dunque, da (*ii*):

$$|G|=\sum_{i\in I}\big|[g_i]_{\sim}\big|=\sum_{i\in I}(G:\boldsymbol{C}(g_i)).$$

Dal teorema di Lagrange, $(G:\boldsymbol{C}(g_i))=\frac{|G|}{\big|\boldsymbol{C}(g_i)\big|}$. Ne segue la formula cercata.

(*iv*) In ogni $\boldsymbol{S}_n$ le classi di coniugio sono formate dalle permutazioni con la stessa struttura ciclica. In $\boldsymbol{S}_4$ le strutture cicliche sono le seguenti:

$$(\_),\ (\_\ \_),\ (\_\ \_)(\ \_\ \_),\ (\_\ \_\ \_),\ (\_\ \_\ \_\ \_)$$

ed il numero di permutazioni di ciascuna di esse è dato rispettivamente da 1, 6, 3, 8, 6. Una famiglia di rappresentanti delle classi di coniugio è ad esempio

$$\{(1),\ (12),\ (12)(34),\ (123),\ (1234)\}.$$

Quindi: $(\boldsymbol{S}_4:\boldsymbol{C}((1)))=1$, $(\boldsymbol{S}_4:\boldsymbol{C}((12)))=6$, $(\boldsymbol{S}_4:\boldsymbol{C}((12)(34))))=3$, $(\boldsymbol{S}_4:\boldsymbol{C}((123)))=8$, e $(\boldsymbol{S}_4:\boldsymbol{C}((1234)))=6$.

In base al teorema di Lagrange, in ogni gruppo finito G risulta: $|\boldsymbol{C}(g)|=\frac{|G|}{(G:\boldsymbol{C}(g))}$. Quindi: $|\boldsymbol{C}((1))|=24/1=24$, $|\boldsymbol{C}((12))|=24/6=4$, $|\boldsymbol{C}((12)(34)))|=24/3=8$, $|\boldsymbol{C}((123))|=24/8=3$ e $|\boldsymbol{C}((1234))|=24/6=4$.

Ovviamente $\boldsymbol{C}((1))=\boldsymbol{S}_4$. Tenuto conto che $\boldsymbol{C}(g)\geq\langle g\rangle$, si conclude subito che

$$\boldsymbol{C}((123))=\langle(123)\rangle,\ \boldsymbol{C}((1234))=\langle(1234)\rangle\ \ \text{(ciclici)}.$$

Si osservi che (12) commuta con (34). Dunque $\boldsymbol{C}((12))\ni(12),(34)$. Poiché $\boldsymbol{C}((12))$ possiede quattro elementi, allora

$$\boldsymbol{C}((12))=\langle(12),\ (34)\rangle=\{(1),\ (12),\ (34),\ (12)(34)\}\ \ \text{(di Klein)}.$$

Il gruppo $\boldsymbol{C}((12)(34))$ ha otto elementi. Si noti che (12), (34), (13)(24) e (14)(23) permutano con (12)(34). Dunque appartengono a $\boldsymbol{C}((12)(34))$. Pertanto $\boldsymbol{C}((12)(34))$ contiene i sei elementi: (1), (12)(34), (12), (34), (13)(24), (14)(23). Ma allora contiene anche

$$(12)\cdot(13)(24)=(1423)\ \ \text{e}\ \ (12)\cdot(14)(23)=(1324).$$

Poiché tale gruppo (di ordine 8) ha cinque elementi di periodo 2, si conclude che è isomordo a $\boldsymbol{D}_4$ (gruppo diedrale).

* * *

5.52. [*Esonero 6/6/05*] Sia H un sottogruppo di un gruppo $(G,\cdot)$. Si chiama *normalizzante di H in G* l'insieme

$$\boldsymbol{N}_G(H)=\{x\in G\ \big|\ \gamma_x(H)=H\}=\{x\in G\ \big|\ xHx^{-1}=H\}$$

[dove γ_x è l'automorfismo interno di G associato ad x, cioè $\gamma_x(y)=xyx^{-1},\ \forall\, y\in G$].

(*i*) Verificare che $\boldsymbol{N}_G(H)$ è un sottogruppo di G.

(*ii*) Verificare che $H\trianglelefteq\boldsymbol{N}_G(H)$.

(*iii*) Verificare che, se $K\leq G$ e $H\trianglelefteq K$, allora $K\leq\boldsymbol{N}_G(H)$ [dunque il normalizzante di H è il più grande sottogruppo di G in cui H è normale].

(*iv*) Tenuto conto di (*iii*) e del reticolo dei sottogruppi di $\boldsymbol{D}_6$, calcolare il normalizzante del sottogruppo $\langle\rho\rangle$ di $\boldsymbol{D}_6$ [dove $\boldsymbol{D}_6$ è il gruppo di isometrie dell'esagono regolare e ρ ne è una riflessione dei vertici].

Soluzione. (*i*) Ovviamente $\gamma_1(H)=H$ e quindi $1\in\boldsymbol{N}_G(H)$. Siano $x,y\in\boldsymbol{N}_G(H)$; allora $\gamma_x(H)=H$, $\gamma_y(H)=H$ e quindi $\gamma_{xy}(H)=\gamma_x\circ\gamma_y(H)=\gamma_x(\gamma_y(H))=\gamma_x(H)=H$. Infine, se $x\in\boldsymbol{N}_G(H)$, da $xHx^{-1}=H$ segue che $x^{-1}Hx=H$ e dunque $\gamma_{x^{-1}}(H)=H$, cioè $x^{-1}\in\boldsymbol{N}_G(H)$.

(*ii*) Ovviamente $H \leq \boldsymbol{N}_G(H)$ [infatti $hHh^{-1} = H,\ \forall\, h \in H$]. Per ogni $x \in \boldsymbol{N}_G(H)$ si ha: $xH = Hx$ e dunque $H \trianglelefteq \boldsymbol{N}_G(H)$.

(*iii*) Sia $K \leq G$, con $H \trianglelefteq K$. Per ogni $k \in K$, si ha $kH = Hk$ e dunque $kHk^{-1} = H$, cioè $k \in \boldsymbol{N}_G(H)$. Allora $K \leq \boldsymbol{N}_G(H)$.

(*iv*) È noto che $\boldsymbol{D}_6 = \langle \varphi, \rho \rangle$, con $\varphi = (123456)$, $\rho = (26)(35) \in \boldsymbol{S}_6$. Il sottogruppo $\langle \rho \rangle$ non è normale in $\boldsymbol{D}_6$ [infatti $\varphi\langle\rho\rangle \neq \langle\rho\rangle\varphi$]. Inoltre $\langle \rho \rangle$ è contenuto (oltre che in $\boldsymbol{D}_6$) soltanto nei due sottogruppi

$$\boldsymbol{V}_1 = \langle \rho,\, \varphi^3 \circ \rho \rangle \ \text{(gruppo di Klein)},\ \boldsymbol{\Sigma}_1 = \langle \varphi^2, \rho \rangle \ \ (\cong \boldsymbol{S}_3).$$

Si noti che $\langle \rho \rangle$ è normale in $\boldsymbol{V}_1$ [in quanto ha indice 2] e che $\boldsymbol{V}_1$ non è contenuto in sottogruppi propri di $\boldsymbol{D}_6$ [per ragioni di cardinalità]. In base al fatto che il normalizzante di un sottogruppo H è il più grande sottogruppo in cui H è normale, si conclude che $\boldsymbol{V}_1$ è il normalizzante di $\langle \rho \rangle$.

Nota. Si osservi (anche se non strettamente necessario) che $\langle \rho \rangle$ non è normale in $\boldsymbol{\Sigma}_1$ [essendo $\varphi^2\langle\rho\rangle \neq \langle\rho\rangle\varphi^2$].

* * *

5.53. [*Esame 15/6/04*] Sia $(G, \cdot)$ un gruppo. Per ogni $a, b \in G$, si definisce *commutatore di* a, b il seguente elemento di G:

$$[a, b] := a\, b\, a^{-1} b^{-1}.$$

(*i*) Calcolare $[a, a]$, $[a, 1]$, $[a, a^{-1}]$, $[a, b][b, a]$, $\forall\, a, b \in G$.

(*ii*) Se G è abeliano, determinare il sottogruppo generato dai commutatori.

(*iii*) Scrivere la tavola dei commutatori del gruppo $\boldsymbol{S}_3$. Determinare il sottogruppo generato dai commutatori.

Soluzione. (*i*) Risulta, $\forall\, a, b \in G$:

$[a, a] = a\, a\, a^{-1} a^{-1} = a(a\, a^{-1}) a^{-1} = 1$;
$[a, 1] = a\, 1\, a^{-1} 1^{-1} = a\, a^{-1} = 1$;
$[a, a^{-1}] = a\, a^{-1} a^{-1} a = (aa^{-1})(a^{-1}a) = 1$;
$[a, b][b, a] = (a\, b\, a^{-1} b^{-1})(b\, a\, b^{-1} a^{-1}) = a\, b\, a^{-1}(b^{-1}b)\, a\, b^{-1} a^{-1} = \ \ldots\ = 1.$

(*ii*) Se G è abeliano, $[a, b] = a\, b\, a^{-1} b^{-1} = a\, a^{-1} b\, b^{-1} = 1$. Dunque l'insieme dei commutatori è $\{1\}$ e quindi il sottogruppo generato dai commutatori è $\{1\}$.

(*iii*) Il gruppo $\boldsymbol{S}_3$ è il seguente

$$\boldsymbol{S}_3 = \{(1),\ (12),\ (13),\ (23),\ (123),\ (132)\}$$

Per scrivere la tavola dei commutatori, si tenga conto dei risultati di (*i*). Si ottiene.

[,]	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(1)	(1)	(1)	(1)	(1)
(12)	(1)	(1)				
(13)	(1)		(1)			
(23)	(1)			(1)		
(123)	(1)				(1)	(1)
(132)	(1)				(1)	(1)

Ora si eseguano i calcoli richiesti. Ad esempio

$[(12), (13)] = (12)(13)(12)(13) = (132)$,
$[(12), (23)] = (12)(23)(12)(23) = (123)$, ecc.

La tavola completa dei commutatori è la seguente:

$[\ ,\ ]$	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(1)	(1)	(1)	(1)	(1)
(12)	(1)	(1)	(132)	(123)	(123)	(132)
(13)	(1)	(123)	(1)	(132)	(123)	(132)
(23)	(1)	(132)	(123)	(1)	(123)	(132)
(123)	(1)	(132)	(132)	(132)	(1)	(1)
(132)	(1)	(123)	(123)	(123)	(1)	(1)

I commutatori di $\boldsymbol{S}_3$ sono (1), (123), (132) ed il gruppo da essi generato è $\boldsymbol{A}_3$.

* * *