SOLUZIONI DEGLI ESERCIZI SU ANELLI E CORPI

Esercizio 1.

È semplice verificare le proprietà degli anelli.
Associatività: $(na+nb)+nc = na+nb+nc = na+(nb+nc)$.
Commutatività: $na+nb = n(a+b) = n(b+a) = nb+na$.
Esistenza identità della somma: $na+0 = n(a+0) = na$.
Ecc........

Esercizio 2.

Verifichiamo le proprietà degli anelli. Dalle tabelle si vede facilmente che per l'operazione $\oplus$ si ha:

$$\begin{array}{lrcl}
\text{Associativa :} & (a\oplus b)\oplus c & = & a\oplus(b\oplus c)\\
\text{Identità :} & a\oplus a & = & a\\
 & b\oplus a & = & b\\
\text{Inverso :} & b\oplus b & = & a\\
 & a\oplus a & = & a
\end{array}$$

Inoltre (vedi tabelle):

$$\begin{array}{lrcccccccc}
\text{Associativa :} & (a\otimes b)\otimes b & = & a\otimes b & = & a & & & & \\
 & a\otimes(b\otimes b) & = & a\otimes b & = & a & & & & \\
 & & & & & & & & & \\
 & (a\otimes b)\otimes a & = & a\otimes a & = & a & & & & \\
 & a\otimes(b\otimes a) & = & a\otimes a & = & a & & & & \\
\dots & \dots & \dots & \dots & \dots & \dots & & & & \\
\text{Distributiva} & a\otimes(a\oplus b) & = & a\otimes b & = & a & & & & \\
 & a\otimes(a\oplus b) & = & (a\otimes a)\oplus(a\otimes b) & = & a\oplus a & = & a. & & \\
\dots & \dots & \dots & \dots & \dots & \dots & & & &
\end{array}$$

Esercizio 3.

Basta osservare che la somma di due numeri dispari è un numero pari: $2n+1+2m+1 = 2(m+n)+2$.

Esercizio 4.

Dimostriamo per prima cosa che S è chiuso rispetto alle operazioni indicate, infatti, per ogni $a, b, c, d \in \mathbb{Q}$ si ha

$$(a+b\sqrt{2})+(c+d\sqrt{2}) = (a+c)+(b+d)\sqrt{2} \in S;$$
$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+cb)\sqrt{2} \in S.$$

Vale poi la proprietà associativa della somma.

$$[(a+b\sqrt{2})+(a_1+b_1\sqrt{2})](a_2+b_2\sqrt{2}) = (a+b\sqrt{2})[(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2})]$$

Identità della somma: $0 = 0+0\sqrt{2}$.
Inverso: $(a+b\sqrt{2})+(-a-b\sqrt{2}) = 0$
Associatività del prodotto:

$$[(a+b\sqrt{2})(a_1+b_1\sqrt{2})](a_2+b_2\sqrt{2}) = (a+b\sqrt{2})[(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})].$$

La distributività segue da quella in $\mathbb{R}$:

$$(a+b\sqrt{2})[(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2})] = (a+b\sqrt{2})(a_1+b_1\sqrt{2})+(a+b\sqrt{2})(a_2+b_2\sqrt{2})$$

Esercizio 5.

Dimostriamo che S è chiuso rispetto alle operazioni indicate. Infatti per ogni $a, b, c, a_1, b_1, c_1 \in Q$ si ha

$$(a+b\sqrt[3]{5}+c\sqrt[3]{5^2})+(a_1+b_1\sqrt[3]{5}+c_1\sqrt[3]{5^2}) = (a+a_1)+(b+b_1)\sqrt[3]{5}+(c+c_1)\sqrt[3]{5^2} \in S.$$

$(a+b\sqrt[3]{5}+c\sqrt[3]{5^2})(a_1+b_1\sqrt[3]{5}+c_1\sqrt[3]{5^2}) = (aa_1+5bc_1+5cb_1)+(ab_1+ba_1+5cc_1)\sqrt[3]{5}+(ac_1+bb_1+ca_1)\sqrt[3]{5^2}.$

Associatività della somma: per ogni $a, b, c, a_1, b_1, c_1, a_2, b_2, c_2 \in S$:

$$[(a+b\sqrt[3]{5}+c\sqrt[3]{5^2})+(a_1+b_1\sqrt[3]{5}+c_1\sqrt[3]{5^2})]+(a_2+b_2\sqrt[3]{5}+c_2\sqrt[3]{5^2}) =$$
$$= (a+b\sqrt[3]{5}+c\sqrt[3]{5^2})+[(a_1+b_1\sqrt[3]{5}+c_1\sqrt[3]{5^2})+(a_2+b_2\sqrt[3]{5}+c_2\sqrt[3]{5^2})]$$

Identità: $0 = 0+0\sqrt[3]{5}+0\sqrt[3]{5^2}$.
Ineverso: per ogni $a, b, c \in S$

$$(a+b\sqrt[3]{5}+c\sqrt[3]{5^2})+(-a-b\sqrt[3]{5}-c\sqrt[3]{5^2}) = 0$$

Associatività del prodotto: per ogni $a, b, c, a_1, b_1, c_1, a_2, b_2, c_2 \in S$:

$$[(a+b\sqrt[3]{5}+c\sqrt[3]{5^2})(a_1+b_1\sqrt[3]{5}+c_1\sqrt[3]{5^2})](a_2+b_2\sqrt[3]{5}+c_2\sqrt[3]{5^2}) =$$
$$= (a+b\sqrt[3]{5}+c\sqrt[3]{5^2})[(a_1+b_1\sqrt[3]{5}+c_1\sqrt[3]{5^2})(a_2+b_2\sqrt[3]{5}+c_2\sqrt[3]{5^2})]$$

Proprietà distributiva: per ogni $a, b, c, a_1, b_1, c_1, a_2, b_2, c_2 \in S$:

$$(a+b\sqrt[3]{5}+c\sqrt[3]{5^2})[(a_1+b_1\sqrt[3]{5}+c_1\sqrt[3]{5^2})+(a_2+b_2\sqrt[3]{5}+c_2\sqrt[3]{5^2})] =$$
$$= (a+b\sqrt[3]{5}+c\sqrt[3]{5^2})(a_1+b_1\sqrt[3]{5}+c_1\sqrt[3]{5^2})+(a+b\sqrt[3]{5}+c\sqrt[3]{5^2})(a_2+b_2\sqrt[3]{5}+c_2\sqrt[3]{5^2})$$

Esercizio 6.

Proprietà associativa: per ogni $a, b, a_1, b_1 \in \mathbb{Z}$ si ha

$$[(a,b)+(a_1,b_1)]+(a_2,b_2) = (a+a_1+a_2, b+b_1+b_2)$$
$$(a,b)+[(a_1,b_1)+(a_2,b_2)] = (a+a_1+a_2, b+b_1+b_2)$$

Da cui

$$[(a,b)+(a_1,b_1)]+(a_2,b_2) = (a,b)+[(a_1,b_1)+(a_2,b_2)]$$

Identità: per ogni $a, b \in \mathbb{Z}$ si ha $(a,b)+(0,0) = (a+0, b+0) = (a,b)$.
Inverso: per ogni $a, b \in \mathbb{Z}$ si ha $(a,b)+(-a,-b) = (0,0)$.
Associatività del prodotto: per ogni a, b, a_1, b_1, a_2, b_2 si ha

$$[(a,b)(a_1,b_1)](a_2,b_2) = (aa_1, bb_1)(a_2,b_2) = (aa_1a_2, bb_1b_2)$$
$$(a,b)[(a_1,b_1)(a_2,b_2)] = (a,b)(a_1a_2, b_1b_2) = (aa_1a_2, bb_1b_2)$$

quindi

$$[(a,b)(a_1,b_1)](a_2,b_2) = (a,b)[(a_1,b_1)(a_2,b_2)].$$

Distributività: per ogni a, b, a_1, b_1, a_2, b_2

$$(a,b)[(a_1,b_1)+(a_2,b_2)] = (a,b)(a_1+a_2, b_1+b_2) = (a(a_1+a_2), b(b_1+b_2)) = (aa_1+aa_2, bb_1+bb_2)$$
$$(a,b)(a_1,b_1)+(a,b)(a_2,b_2) = (aa_1, bb_1)+(aa_2, bb_2) = (aa_1+aa_2, bb_1+bb_2)$$
$$\text{quindi}$$
$$(a,b)[(a_1,b_1)+(a_2,b_2)] = (a,b)(a_1,b_1)+(a,b)(a_2,b_2)$$

Si vede facilmente che le operazioni definite in M sono commutative. Inoltre l'anello $(M,+,\cdot)$ è dotato di identità per il $(\cdot)$. Infatti

$$(a,b)(1,1) = (a,b)$$

Ogni elemento $(a,b) \in M \setminus \{(0,0)\}$ ammette inverso. Infatti

$$(a,b)(a^{-1}, b^{-1}) = (1,1)$$

Esistono inoltre divisori dello zero: siano infatti $(x,y),(a,b) \in M \setminus \{(0,0)\}$ e supponiamo $(a,b)(x,y) = (0,0)$ ovvero $(ax,by) = (0,0)$, questo equivale a dire che $ax = 0 \wedge by = 0$. Da cui $(a = 0 \vee x = 0) \wedge (b = 0 \vee y = 0)$ ovvero

$$[a = 0 \wedge (b = 0 \vee y = 0)] \vee [x = 0 \wedge (b = 0 \vee y = 0)] \iff$$
$$\iff (a = 0 \wedge b = 0) \vee (a = 0 \wedge y = 0) \vee (x = 0 \wedge b = 0) \vee (x = 0 \wedge y = 0) \iff$$
$$(\text{essendo } (x,y),(a,b) \in M \setminus \{(0,0)\})$$
$$(a = 0 \wedge y = 0) \vee (x = 0 \wedge b = 0)$$

Le soluzioni sono quindi $(0,b) \wedge (x,0)$ oppure $(a,0) \wedge (0,y)$. Possiamo riassumere dicendo che i divisori di zero di $(M,+,\cdot)$ sono tutti gli elementi del tipo $(a,0),(0,b)$.

Esercizio 7.

L'identità del prodotto è data da $1 + 0\sqrt{2} = 1$.
Dimostriamo che esiste il reciproco, ovvero per ogni $a + b\sqrt{2} \in S \setminus \{0\}$ possiamo determinare $(a + b\sqrt{2})^{-1} \in S \setminus \{0\}$ tale che

$$(a + b\sqrt{2})(a + b\sqrt{2})^{-1} = 1$$

Onde, posto $(a + b\sqrt{2})^{-1} = x + y\sqrt{2}$, segue

$$(a + b\sqrt{2})(x + y\sqrt{2}) = (ax + 2by) + (ay + bx)\sqrt{2} = 1 \iff \begin{cases} ax + 2by &= 1 \\ bx + ay &= 0. \end{cases} \iff$$
$$\iff x = \frac{a}{a^2 - 2b^2}, \quad y = -\frac{b}{a^2 - 2b^2}.$$

Si noti che poiché $a, b \in \mathbb{Q}$ si ha $a^2 - 2b^2 \neq 0$. In definitiva abbiamo ottenuto

$$(a + b\sqrt{2})^{-1} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in S \setminus \{0\}$$

La commutatività è ovvia.

Esercizio 8.

Dimostriamo l'esistenza del reciproco, ovvero per ogni $a + b\sqrt[3]{5} + c\sqrt[3]{5^2} \in S \setminus \{0\}$ esiste $(a + b\sqrt[3]{5} + c\sqrt[3]{5^2})^{-1}$
Poniamo $(a + b\sqrt[3]{5} + c\sqrt[3]{5^2})^{-1} = x + y\sqrt[3]{5} + z\sqrt[3]{5^2}$. Si deve verificare che

$$(a + b\sqrt[3]{5} + c\sqrt[3]{5^2})(x + y\sqrt[3]{5} + z\sqrt[3]{5^2}) = 1$$

ovvero

$$(a+b\sqrt[3]{5}+c\sqrt[3]{5^2})(x+y\sqrt[3]{5}+z\sqrt[3]{5^2}) =$$
$$= (ax+5bz+5cy)+(ay+by+5cz)\sqrt[3]{5}+(az+by+cx)\sqrt[3]{5^2} = 1+0\sqrt[3]{5}+0\sqrt[3]{5^2}.$$

Da questo otteniamo l'inversa risolvendo il sistema lineare (che è risolubile per ogni $((a,b,c)\in\mathbb{Q}^3\setminus(0,0,0))$ in nell'incognita (x,y,z)

$$\begin{cases} ax+5cy+5bz &= 1 \\ bx+ay+5cz &= 0 \\ cx+by+az &= 0 \end{cases}$$

Esercizio 9.

Osserviamo che la somma di due matrici di $\mathcal{M}$ è ancora una matrice di $\mathcal{M}$:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} = \begin{pmatrix} a+a_1 & -b-b_1 \\ b+b_1 & a+a_1 \end{pmatrix}$$

La somma è anche commutativa. Anche il prodotto di due matrici di $\mathcal{M}$ fornisce una matrice di $\mathcal{M}$ ed è commutativo. Infatti

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} = \begin{pmatrix} aa_1-bb_1 & -(ab_1+ba_1) \\ ab_1+ba_1 & aa_1-bb_1 \end{pmatrix}$$

$$\begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} aa_1-bb_1 & -(ab_1+ba_1) \\ ab_1+ba_1 & aa_1-bb_1 \end{pmatrix}$$

L'identità della somma è

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Per quanto riguarda l'inverso si osserva che

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} -a & -(-b) \\ (-b) & -a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

L'identità del prodotto è la *matrice identità*

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{1}$$

$\mathcal{M}$ risulta un anello commutativo con identità. Verifichiamo che non ammette divisori di 0. Ovvero non esiste un elemento di $\mathcal{M}$

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

tale che

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = \begin{pmatrix} ax - by & -(ay + bx) \\ ay + bx & ax - by \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Esiste una soluzione $(x, y) \in \mathbb{R}^2 \setminus \{(0, 0)\}$ se e solo se $a^2 + b^2 = 0$. Infine si dimostra che ogni matrice non nulla ammette inversa risolvendo:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = \begin{pmatrix} ax - by & -(ay + bx) \\ ay + bx & ax - by \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Ovvero il sistema

$$\begin{cases} ax - by & = & 1 \\ ax + by & = & 0 \end{cases}$$

Quindi

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} \frac{a}{a^2+b^2} & \frac{b}{a^2+b^2} \\ -\frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Esercizio 10.

Poniamo

$$J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{2}$$

da cui, tenuto conto della definizione della matrice I (vedi (1) dell'esercizio precedente)

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a\,I + b\,J.$$

Definiamo l'applicazione $f : \mathbb{C} \longrightarrow \mathcal{M}$ nel modo seguente

$$f(a + ib) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

Si verifica facilmente che è un isomorfismo. È infatti biunivoca ed inoltre è un omomorfismo, in quanto

$$\begin{aligned} f((a + ib) + (a_1 + ib_1)) = f((a + a_1) + i(b + b_1)) = (a + a_1)I + (b + b_1)J = \\ = aI + bJ + a_1I + b_1J = f(a + ib) + f(a_1 + ib_1). \end{aligned}$$

$$\begin{aligned} f((a + ib)(a_1 + ib_1)) = f((aa_1 - bb_1) + i(ab_1 + a_1b)) = (aa_1 - bb_1)I + (ab_1 + a_1b)J = \\ = f(a + ib)f(a_1 + ib_1). \end{aligned}$$

Esercizio 11.

L'iniettività è ovvia. Verifichiamo che si tratta di un omomorfismo.

$$\begin{aligned} f((a+ib)+(a_1+ib_1)) = f((a+a_1)+i(b+b_1)) = (a+a_1)-i(b+b_1) = \\ = (a-ib)+(a_1-ib_1) = f(a+ib)+f(a_1+ib_1). \end{aligned}$$

$$\begin{aligned} f((a+ib)(a_1+ib_1)) = f((aa_1-bb_1)+i(ab_1+ba_1)) = aa_1-bb_1-i(ab_1+ba_1) \\ = (a-ib)(a_1-ib_1) = f(a+ib)f(a_1+ib_1). \end{aligned}$$

Esercizio 12.

L'iniettività è ovvia. Verifichiamo che si tratta di un omomorfismo.

$$\begin{aligned} f((a+b\sqrt{2})+(a_1+b_1\sqrt{2})) = f((a+a_1)+(b+b_1)\sqrt{2}) = (a+a_1)-(b+b_1)\sqrt{2} = \\ = (a-b\sqrt{2})+(a_1-b_1\sqrt{2}) = f(a+b\sqrt{2})+f(a_1+b_1\sqrt{2}). \end{aligned}$$

$$\begin{aligned} f((a+b\sqrt{2})(a_1+b_1\sqrt{2})) = f((aa_1+2bb_1)+(ab_1+ba_1)\sqrt{2}) = aa_1+2bb_1-(ab_1+ba_1)\sqrt{2} = \\ = (a-b\sqrt{2})(a_1-b_1\sqrt{2}) = f(a+b\sqrt{2})f(a_1+b_1\sqrt{2}). \end{aligned}$$

Esercizio 13.

(i) Osserviamo che dalla definizione di f

$$\begin{aligned} f((0,0)) = f((0,b)) = 0 \\ f((a,0)) = f((a,b)) = a, \end{aligned}$$

da questo

$$f((a,b)+(a_1,b_1)) = f((a+a_1,b+b_1)) = a+a_1 = f((a,b))+f((a_1,b_1)).$$

$$f((a,b)(a_1,b_1)) = f((aa_1,bb_1)) = aa_1 = f((a,b))f((a_1,b_1)).$$

(ii) $\ker f = \{(0,b) : \ b \in \mathbb{Z}\}$.

(iii) Osserviamo che due elementi $(a,b),(a_1,b_1) \in \mathbb{Z}\times\mathbb{Z}$ sono congrui mod $\ker f$ se e solo se

$$(a,b)-(a_1,b_1) \in \ker f \iff (a-a_1,b-b_1) \in \ker f \iff a = a_1.$$

Quindi ad ogni elemento di $(\mathbb{Z}\times\mathbb{Z})/\ker f$ corrisponde uno ed un solo elemento di $\mathbb{Z}$.

Esercizio 14.

Osserviamo che S è chiuso rispetto alla operazione di somma e di prodotto. Infatti per ogni $a,\ b,\ a_1,\ b_1 \in \mathbb{Q}$ risulta:

$$(a+b\sqrt{5}\,i)+(a_1+b_1\sqrt{5}\,i) = (a+a_1)+(b+b_1)\sqrt{5}i \in S.$$

$$(a+b\sqrt{5}\,i)(a_1+b_1\sqrt{5}\,i) = (aa_1-5bb_1)+(ab_1+a_1b)\sqrt{5}i \in S.$$

L'operazione $(+)$ è associativa: per ogni $a,b,a_1,b_1,a_2,b_2 \in \mathbb{Q}$ risulta

$$[(a+b\sqrt{5}\,i)+(a_1+b_1\sqrt{5}\,i)]+(a_2+b_2\sqrt{5}\,i) = (a+b\sqrt{5}\,i)+[(a_1+b_1\sqrt{5}\,i)+(a_2+b_2\sqrt{5}\,i)]$$

Inoltre $0+0\sqrt{5}\,i$ è l'identità della somma.

Per quanto riguarda l'inverso risulta $(a+b\sqrt{5}\,i)+(-a-b\sqrt{5}\,i) = 0+0\sqrt{5}\,i$

L'operazione di $(\cdot)$ è associativa. Infatti per ogni $a,b,a_1,b_1,a_2,b_2 \in \mathbb{Q}$:

$$[(a+b\sqrt{5}\,i)\cdot(a_1+b_1\sqrt{5}\,i)](a_2+b_2\sqrt{5}\,i) = (a+b\sqrt{5}\,i)[(a_1+b_1\sqrt{5}\,i)(a_2+b_2\sqrt{5}\,i)].$$

Vale la proprietà distributiva. Infatti per ogni $a, b, a_1, b_1 \in Q$ si ha:

$$\begin{aligned}(a+b\sqrt{5}\,i)[(a_1+b_1\sqrt{5}\,i)+(a_2+b_2\sqrt{5}\,i)] &= (a+b\sqrt{5}\,i)[(a_1+a_2)+(b_1+b_2)\sqrt{5}\,i] = \\ &= [a(a_1+a_2)-5b(b_1+b_2)]+[a(b_1+b_2)+b(a_1+a_2)]\sqrt{5}i.\end{aligned}$$

Mentre

$$\begin{gathered}(a+b\sqrt{5}\,i)(a_1+b_1\sqrt{5}\,i)+(a+b\sqrt{5}i)(a_2+b_2\sqrt{5}\,i) = \\ = (aa_1-5bb_1)+(ab_1+a_1b)\sqrt{5}i+(aa_2-5bb_2)+(ab_2+a_2b)\sqrt{5}i = \\ = [(aa_1-5bb_1)+(aa_2-5bb_2)]+[(ab_1+a_1b)+(ab_2+a_2b)\sqrt{5}\,i] = \\ = [a(a_1+a_2)-5b(b_1+b_2)]+[a(b_1+b_2)+b(a_1+a_2)]\sqrt{5}i.\end{gathered}$$

L'identità di $(\cdot)$ è $1+0\sqrt{5}i$

Per ogni $a+b\sqrt{5}i \in S \setminus \{0\}$ esiste il reciproco dato da

$$(a+b\sqrt{5}i)^{-1} = \frac{a}{a^2+5b^2} - \frac{b}{a^2+5b^2}\ \sqrt{5}\,i.$$

Questo si ottiene determinando $x, y \in Q$ tali che

$$(a+b\sqrt{5}i)(x+y\sqrt{5}i) = 1.$$

Infine è banale verificare che le operazioni di $(+)$ e $(\cdot)$ sono commutative, quindi $(S, +, \cdot)$ è un corpo.

Esercizio 15.

L'equazione data in $\mathbb{Z}_6$ può essere trasformata nel modo seguente

$$[3]x^2+[4]x-[4]x-[2]x+[5]-[5]-[1]=0 \iff [3]x^2+[4]x-[0]x+[5]-[0]=0 \iff [3]x^2+[4]x+[5]=0$$

Sostituendo nel primo membro di essa gli elementi di $\mathbb{Z}_6$ si ha

$$\begin{array}{lllllll} x &=& [0]: & [3][0]^2+[4][0]+[5] &=& [5] & \\ x &=& [1]: & [3][1]^2+[4][1]+[5] &=& [0] & \\ x &=& [2]: & [3][2]^2+[4][2]+[5] &=& [0]+[2]+[5] &=& [1] \\ x &=& [3]: & [3][3]^2+[4][3]+[5] &=& [3]+[0]+[5] &=& [2] \\ x &=& [4]: & [3][4]^2+[4][4]+[5] &=& [0]+[4]+[5] &=& [3] \\ x &=& [5]: & [3][5]^2+[4][5]+[5] &=& [3]+[2]+[5] &=& [4] \end{array}$$

Dunque l'equazione assegnata possiede una sola radice in $\mathbb{Z}_6$ data da $x=[1]$.

Esercizio 16.

L'equazione data in $\mathbb{Z}_6$ può essere trasformata nel modo seguente

$$x^2-5x=0 \iff x^2+x=6x \iff x^2+x=0 \tag{3}$$

Sostituendo nel primo membro di essa gli elementi di $\mathbb{Z}_6$ si ha

$$\begin{array}{lllllll} x & = & 0: & 0^2+0 & = & 0 & \\ x & = & 1: & 1^2+1 & = & 2 & \\ x & = & 2: & 2^2+2 & = & 4+2 & = & 0 \\ x & = & 3: & 3^2+3 & = & 3+3 & = & 0 \\ x & = & 4: & 4^2+4 & = & 4+4 & = & 2 \\ x & = & 5: & 5^2+5 & = & 1+5 & = & 0 \end{array}$$

Dunque l'equazione assegnata possiede quattro radici in $\mathbb{Z}_6$.
Osserviamo che l'equazione (3) può essere scritta anche nel modo seguente

$$x\,(x+1)=0$$

Le cui soluzioni sono $x=0$ oppure $x=-1$. Ma $x=-1$ in $\mathbb{Z}_6$ equivale a $x=5$. Inoltre ricordiamo che, poiché Z_6 non è un corpo ammette divisori di 0, altre soluzioni si ottengono dai sistemi

$$(a)\ \begin{cases} x=2 \\ x+1=3 \end{cases} \qquad (b)\ \begin{cases} x=3 \\ x+1=2 \end{cases} \qquad (c)\ \begin{cases} x=3 \\ x+1=4 \end{cases} \qquad (d)\ \begin{cases} x=4 \\ x+1=3 \end{cases}$$

Le soluzioni dei sistemi (a), (c), sono evidenti, mentre i sistemi (b) e (d) non hanno soluzione.

Esercizio 17.

Costruiamo le tabelle relative alle operazioni in $\mathbb{Z}_{10}$.
Tabella di $(\mathbb{Z}_{10},+)$:

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Tabella di $(\mathbb{Z}_{10},\cdot)$:

·	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Consideriamo il sottoanello $S_1 = (\{[0],[5]\},+,\cdot)$ di $(\mathbb{Z}_{10},+,\cdot)$. Le seguenti tabelle provano che si tratta effettivamente di un sottoanello.

+	0	5
0	0	5
5	5	0

$\cdot$	0	5
0	0	0
5	0	5

Possiamo stabilire il seguente isomorfismo di S_1 in $\mathbb{Z}_2$:

$$\varphi([0]) = [0]_2, \quad \varphi([5]) = [1]_2$$

Poiché $\mathbb{Z}_2$ è un corpo anche S_1 lo è.([1])

La struttura $S_2 = (\{[0],[2],[4],[6],[8]\},+,\cdot)$ è un sottoanello di $(\mathbb{Z}_{10},+,\cdot)$, come si prova facilmente con l'aiuto delle seguenti tabelle:

+	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	0
4	4	6	8	0	2
6	6	8	0	2	4
8	8	0	2	4	6

$\cdot$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	2	8	4

Definiamo un'applicazione ψ di $(\mathbb{Z}_5,+,\cdot)$ in S_2 :

$$\begin{aligned} \psi([0]_5) &= [0]_{10} \\ \psi([1]_5) &= [6]_{10} \\ \psi([2]_5) &= [2]_{10} \\ \psi([3]_5) &= [8]_{10} \\ \psi([4]_5) &= [4]_{10} \end{aligned}$$

ψ un isomorfismo, quindi, per quanto detto in precedenza, S_2 è un corpo perché $(\mathbb{Z}_5,+,\cdot)$ è un corpo.
Si noti che l'identità per il prodotto in S_2 è $[6]_{10}$.

[1]Dimostrare che se un anello è un isomorfo ad un corpo allora è un corpo.