Appello del 14/7/2005

1) Dimostrare tramite il principio di induzione che $\sum_{k=0}^{n} (2k)^3 = 2n^2(n+1)^2 \quad \forall n \in \mathbb{N}$

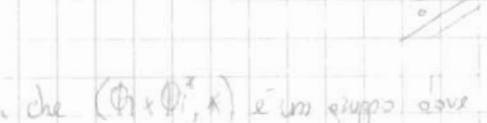
$P(0)$: $\sum_{k=0}^{0} (2k)^3 = 0 \quad 2\cdot 0^2(0+1)^2 = 0$ $\quad P(0)$ vera

$n > 0$: Ipotesi: $\sum_{k=0}^{n} (2k)^3 = 2n^2(n+1)^2$ $\quad$ Tesi: $\sum_{k=0}^{n+1} (2k)^3 = 2(n+1)^2(n+2)^2$

$\sum_{k=0}^{n+1} (2k)^3 = \sum_{k=0}^{n} (2k)^3 + (2(n+1))^3 = 2n^2(n+1)^2 + 2^3(n+1)^3 = 2(n+1)^2\left(n^2+4(n+1)\right) = 2(n+1)^2(n+2)^2$

$P(n)$ vera $\to$ $P(n+1)$ vera. Dunque $P(n)$ è vera $\forall n \in \mathbb{N}$

2) Si consideri l'insieme di permutazioni S_5 e si individui il sottogruppo H generato dalla permutazione $\alpha = (135)(24)$.
Si disegni il reticolo dei sottogruppi di H e si dica se è un reticolo di Boole



3) Si dimostri che $(\mathbb{R}\times\mathbb{R}^*, *)$ è un gruppo dove $*$ è l'operazione definita su $\mathbb{R}\times\mathbb{R}^*$ e $\forall (a,b),(a',b') \in \mathbb{R}\times\mathbb{R}^*$ si ha $(a,b)*(a',b') = (a'b+a, bb')$. Si dica se $\mathbb{R}\times\{1\}$ è sottogruppo di $(\mathbb{R}\times\mathbb{R}^*, *)$

$(\mathbb{R}\times\mathbb{R}^*, *)$ gruppo $\iff$ $*$ associativa, $*$ ha el. neutro, $\forall (a,b)\in\mathbb{R}\times\mathbb{R}^*$ $\exists$ inverso di $(a,b)\in\mathbb{R}\times\mathbb{R}^*$

$(a,b),(c,d),(e,f) \in \mathbb{R}\times\mathbb{R}^*$

$(a,b)*((c,d)*(e,f)) = (a,b)*(ed+e, df) = \left((ed+e)b+a, b(df)\right) = (edb+cb+a, bdf)$

$((a,b)*(c,d))*(e,f) = (cb+a, bd)*(e,f) = (e(bd)+b+a, bd(f)) = (ebd+cb+a, bdf) = (edb+cb+a, bdf)$

$*$ commutativa

$*$ è associativa

$(u,u') \in \mathbb{R}\times\mathbb{R}^*$ el. neutro $\iff \forall (a,b)\in\mathbb{R}\times\mathbb{R}^*$ $(a,b)*(u,u') = (a,b) = (u,u')*(a,b)$

$(a,b)*(u,u') = (ub+a, bu')$ $\quad (u,u')*(a,b) = (au'+u, u'b)$

$\begin{cases} (ub+a, bu') = (a,b) \\ (au'+u, u'b) = (a,b) \end{cases} \iff \begin{cases} ub+a = a \\ bu' = b \end{cases} \wedge \begin{cases} au'+u = a \\ u'b = b \end{cases}$

Dal 1° sistema si ottiene $(u,u') = \left(\frac{1}{b}, 1\right)$ Dal secondo $(u,u') = (0,1)$

Verifica: $(0,1)*(a,b) = (a\cdot 1+0, 1\cdot b) = (a,b)$ $\quad (a,b)*(0,1) = (0\cdot b+a, b\cdot 1) = (a,b)$

$\exists (0,1)\in\mathbb{R}\times\mathbb{R}^*$ t.c. $(a,b)*(0,1) = (a,b) = (0,1)*(a,b)$ $\quad (0,1)$ el. neutro

$(a',b') \in \mathbb{R}\times\mathbb{R}^*$ inverso di $(a,b)\in\mathbb{R}\times\mathbb{R}^* \iff (a,b)*(a',b') = (0,1) = (a',b')*(a,b)$

$(a,b)*(a',b') = (a'b+a, bb')$, $(a',b')*(a,b) = (ab'+a', b'b)$

$\begin{cases} (a'b+a, bb') = (0,1) \\ (ab'+a', b'b) = (0,1) \end{cases} \iff \begin{cases} a'b+a = 0 \\ bb' = 1 \end{cases} \wedge \begin{cases} ab'+a' = 0 \\ b'b = 1 \end{cases}$

Da entrambi i sistemi risulta $(a',b') = \left(-\frac{a}{b}, \frac{1}{b}\right)$

Verifica: $\left(-\frac{a}{b}, \frac{1}{b}\right)*(a,b) = \left(a\cdot\frac{1}{b}+\left(-\frac{a}{b}\right), \frac{1}{b}, b\right) = (0,1)$, $(a,b)*\left(-\frac{a}{b}, \frac{1}{b}\right) = \left(-\frac{a}{b}\cdot b+a, b\cdot\frac{1}{b}\right) = (0,1)$

$\forall (a,b) \in \mathbb{Q} \times \mathbb{Q}^* \quad \exists \left(-\frac{a}{b}, \frac{1}{b}\right) \in \mathbb{Q} \times \mathbb{Q}^* : \quad (a,b) * \left(-\frac{a}{b}, \frac{1}{b}\right) = (0,1) = \left(-\frac{a}{b}, \frac{1}{b}\right) * (a,b) \qquad \left(-\frac{a}{b}, \frac{1}{b}\right)$ inverso di (a,b)

$(\mathbb{Q} \times \mathbb{Q}^*, *)$ gruppo

$\mathbb{Q} \times \{1\}$ sottogruppo $\Leftrightarrow \mathbb{Q} \times \{1\} \neq \emptyset$ e $\forall (a,b), (c,d) \in \mathbb{Q} \times \{1\} \quad (a,b) * (c,d)^{-1} \in \mathbb{Q} \times \{1\}$

$(0,1) \in \mathbb{Q} \times \{1\} \Rightarrow \mathbb{Q} \times \{1\}$ non vuoto

$(a,b), (c,d) \in \mathbb{Q} \times \{1\} \Rightarrow (a,b) = (a,1), \ (c,d) = (c,1) \Rightarrow (c,d)^{-1} = \left(-\frac{c}{1}, \frac{1}{1}\right) = (-c, 1)$

$(a,1) * (-c,1) = (-c \cdot 1 + a, 1 \cdot 1) = (-c+a, 1) \in \mathbb{Q} \times \{1\}$

$\mathbb{Q} \times \{1\}$ sottogruppo di $(\mathbb{Q} \times \mathbb{Q}^*, *)$

4) Si fattorizzi: $p(x) = x^5 + x^4 + 1$ in $\mathbb{Z}_2$ e $\mathbb{Z}_3$

$p(x) \in \mathbb{Z}_2 \qquad \mathbb{Z}_2 = \{[0]_2, [1]_2\} = \{\bar{0}, \bar{1}\}$ Le radici si cercano in $\mathbb{Z}_2$

$p(\bar{0}) = \bar{0}^5 + \bar{0}^4 + \bar{1} = \bar{1} \neq \bar{0} \qquad p(\bar{1}) = \bar{1}^5 + \bar{1}^4 + \bar{1} = \bar{3} = \bar{1}$

$p(x)$ non ha radici, ma potrebbe spezzarsi in un polinomio di grado 2 e uno di grado 3.

I polinomi di grado 2 a coefficienti in $\mathbb{Z}_2$ sono: x^2+x, x^2+1, x^2. Dividiamo $p(x)$ per questi polinomi

$x^5+x^4+1 \ \big| \ x^2+x$

$-(x^5+x^4)$

$\quad // \quad 1$

$\frac{x^5}{x^2} = x^3 ; \ x^3(x^2+x) = x^5+x^4 ; \ x^5+x^4+1 - x^5-x^4 = 1$

Il resto è $\neq 0$, dunque (x^2+x) non è fattore di $p(x)$

$x^5+x^4+1 \ \big| \ x^2+1$

$-(x^5+x^3)$

x^4+x^3+1

$-(x^4+x^2)$

x^3+x^2+1

$-(x^3+x)$

x^2+x+1

$-(x^2+1)$

x

$\frac{x^5}{x^2} = x^3 ; \ x^3(x^2+1) = x^5+x^3 ; \ x^5+x^4+1 - x^5-x^3 = x^4-x^3+1 \equiv x^4+x^3+1$

$\frac{x^4}{x^2} = x^2 ; \ x^2(x^2+1) = x^4+x^2 ; \ x^4+x^3+1 - x^4-x^2 = x^3-x^2+1 \equiv x^3+x^2+1$

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

$\frac{x^2}{x^2} = 1 ; \ 1(x^2+1) = x^2+1 , \ x^2+x+1-x^2-1 = x$

Il resto è $\neq 0$, dunque (x^2+1) non è fattore di $p(x)$

$x^5+x^4+1 \ \big| \ x^2$

$-(x^5)$

$\quad // \quad x^4+1$

$-(x^4)$

$\quad // \quad 1$

$\frac{x^5}{x^2} = x^3 ; \ x^3(x^2) = x^5$

$\frac{x^4}{x^2} = x^2 ; \ x^2(x^2) = x^4$

Il resto è $\neq 0$, dunque x^2 non è fattore di $p(x)$

$p(x)$ irriducibile in $\mathbb{Z}_2$

$p(x) \in \mathbb{Z}_3 \qquad \mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\} = \{\bar{0}, \bar{1}, \bar{2}\}$ Le radici si cercano in $\mathbb{Z}_3$

$p(\bar{0}) = \bar{0}^5 + \bar{0}^4 + \bar{1} = \bar{1} \neq \bar{0} \qquad p(\bar{1}) = \bar{1}^5 + \bar{1}^4 + \bar{1} = \bar{3} = \bar{0}$

$\bar{1}$ radice di $p(x)$, dunque $x - \bar{1} = x + \bar{2}$ compare nella fattorizzazione

x^5+x^4+1 | $x+2$

$-(x^5+2x^4)$ | $x^4+2x^3+2x^2+2x+2$

$2x^4+1$

$-(2x^4+x^3)$

$2x^3+1$

$-(2x^3+x^2)$

$2x^2+1$

$-(2x^2+4x)$

$2x+1$

$-(2x+1)$

$//\ //$

$\frac{x^5}{x}=x^4$; $x^4(x+2)=x^5+2x^4$; $x^5+x^4+1-x^5-2x^4=-x^4+1\equiv 2x^4+1$

$\frac{2x^4}{x}=2x^3$; $2x^3(x+2)=2x^4+4x^3\equiv 2x^4+x^3$; $2x^4+1-2x^4-x^3=-x^3+1\equiv 2x^3+1$

$\frac{2x^3}{x}=2x^2$; $2x^2(x+2)=2x^3+4x^2\equiv 2x^3+x^2$; $2x^3+1-2x^3-x^2=-x^2+1\equiv 2x^2+1$

$\frac{2x^2}{x}=2x$; $2x(x+2)=2x^2+4x\equiv 2x^2+x$; $2x^2+1-2x^2-x=-x+1\equiv 2x+1$

$\frac{2x}{x}=2$; $2(x+2)=2x+4\equiv 2x+1$

$p(x)=(x+2)(x^4+2x^3+2x^2+2x+2)$. Cerchiamo in $\mathbb{Z}_3$ le radici di $x^4+2x^3+2x^2+2x+2$ escludendo $\bar{0}$

$p_1(\bar{1})=\bar{1}^4+\bar{2}\cdot\bar{1}^3+\bar{2}\cdot\bar{1}^2+\bar{2}\cdot\bar{1}+\bar{2}=\bar{1}+\bar{2}+\bar{2}+\bar{2}+\bar{2}=\bar{9}=\bar{0}$

$\bar{1}$ radice $\quad x-1\equiv x+2$ compare nella fattorizzazione

$x^4+2x^3+2x^2+2x+2$ | $x+2$

$-(x^4+2x^3)$ | x^3+2x+1

$//\ //\quad 2x^2+2x+2$

$-(2x^2+x)$

$//\quad x+2$

$-(x+2)$

$//\ //$

$\frac{x^4}{x}=x^3$; $x^3(x+2)=x^4+2x^3$;

$\frac{2x^2}{x}=2x$; $2x(x+2)=2x^2+4x\equiv 2x^2+x$; $2x^2+2x+2-2x^2+x=x+2$

$\frac{x}{x}=1$; $1(x+2)=x+2$

$p(x)=(x+2)^2(x^3+2x+1)$. Cerchiamo in $\mathbb{Z}_3$ le radici di x^3+2x+1 escludendo $\bar{0}$

$p_2(\bar{1})=\bar{1}^3+\bar{2}\cdot\bar{1}+\bar{1}=\bar{1}+\bar{2}+\bar{1}=\bar{4}=\bar{1}\neq 0$

$p_2(\bar{2})=\bar{2}^3+\bar{2}\cdot\bar{2}+\bar{1}=\bar{2}+\bar{1}+\bar{1}=\bar{4}=\bar{1}\neq 0$

x^3+2x+1 non ha radici in $\mathbb{Z}_3$ ed essendo di 3° grado è irriducibile

$p(x)=(x+2)^2(x^3+2x+1)$ fattorizzazione in $\mathbb{Z}_3$

Verifica: $(x+2)^2(x^3+2x+1)=(x^2+x+1)(x^3+2x+1)=x^5+2x^3+x^2+x^4+2x^2+x+x^3+2x+1=x^5+x^4+1$

5) Si consideri $A=\{7^r\cdot s\ ;\ r,s\in\mathbb{Z}\}$ e si dimostri che è sottoanello unitario di $(\mathbb{R},+,\cdot)$. Si trovi un elemento di A che non ha inverso. Si dica se $f:A\to A\ \ni\ \forall x\in A\ f(x)=7x$ è omomorfismo di anelli

A sottoanello unitario $\Leftrightarrow A$ sottogruppo di $(\mathbb{R},+)$, A chiuso per $\cdot$, $1\in A$

$1\in A$ poiché per $r=0$, $s=1$ $\quad 7^0\cdot 1=1$

$1\in A\Rightarrow A\neq\emptyset$

$x,y\in A\quad x=7^r\cdot s\quad y=7^q\cdot t$ con $r,s,q,t\in\mathbb{Z}$

per $r=q\quad x-y=7^r\cdot s-7^q\cdot t=7^r(s-t)\in A$ poiché $r\in\mathbb{Z}$ e $(s-t)\in\mathbb{Z}$

per $r>q\quad x-y=7^r\cdot s-7^q\cdot t=7^r\left(s-7^{q-r}\cdot t\right)\in A$ poiché $r\in\mathbb{Z}$, $q-r\in\mathbb{Z}\Rightarrow 7^{q-r}\in\mathbb{Z}\Rightarrow 7^{q-r}\cdot t\in\mathbb{Z}\Rightarrow s-7^{q-r}\cdot t\in\mathbb{Z}$

per $q>r\quad x-y=7^r\cdot s-7^q\cdot t=7^q\left(7^{r-q}\cdot s-t\right)\in A$ poiché $q\in\mathbb{Z}$, $r-q\in\mathbb{Z}\Rightarrow 7^{r-q}\in\mathbb{Z}\Rightarrow 7^{r-q}\cdot s\in\mathbb{Z}\Rightarrow 7^{r-q}\cdot s-t\in\mathbb{Z}$

Dunque $A \neq \emptyset$ e $\forall x,y \in A \; x-y \in A \iff A$ sottogruppo di $(\mathbb{R},+)$

$x,y \in A \quad x = 7^r \cdot s \quad y = 7^q \cdot t \quad r,s,q,t \in \mathbb{Z}$

$x \cdot y = 7^r \cdot s \cdot 7^q \cdot t = 7^{r+q}(s \cdot t) \in A$ poiché $r+q \in \mathbb{Z}$ e $s \cdot t \in \mathbb{Z}$

A chiuso per $\cdot$

A sottoanello di $(\mathbb{R},+,\cdot)$

Consideriamo $7^2 \cdot 2 \in A$, a' inverso di $7^2 \cdot 2 \iff 7^2 \cdot 2 \cdot a' = 1$

$7^2 \cdot 2 \cdot a' = 1 \iff a' = \frac{1}{7^2 \cdot 2} = \frac{1}{7^2} \cdot \frac{1}{2} = 7^{-2} \cdot \frac{1}{2}$ $\quad -2 \in \mathbb{Z}$ ma $\frac{1}{2} \notin \mathbb{Z}$ dunque $a' \notin A$

$7^2 \cdot 2$ non ha inverso in A

$f: A \to A$ è $\forall x \in A \; f(x) = 7x$ omomorfismo $\iff \forall x,y \in A \; f(x+y) = f(x) + f(y)$, $\forall x,y \in A \; f(x \cdot y) = f(x) \cdot f(y)$, $f(1) = 1$

$f(x+y) = 7(x+y) = 7x + 7y = f(x) + f(y)$

$f(x \cdot y) = 7(x \cdot y) = 7xy \qquad f(x) \cdot f(y) = 7x \cdot 7y = 49xy \qquad f(x \cdot y) \neq f(x) \cdot f(y)$

f non è omomorfismo di anelli