Algebra — 12 Luglio 2010

1. Siano $\mathbb{R}^*$ il gruppo **moltiplicativo** dei reali $\neq 0$, $\mathbb{R}$ il gruppo **additivo** dei reali e $\mathbb{R}^+$ il gruppo **moltiplicativo** dei reali positivi. Si considerino le funzioni $f : \mathbb{R}^* \to \mathbb{R}$ e $g : \mathbb{R}^* \to \mathbb{R}^+$ così definite:

$$\begin{aligned} f(x) &= \log(x^2) \\ g(x) &= \sqrt{x^2} \end{aligned}$$

   - Dimostrare che f e g sono omomorfismi di gruppi.
   - Trovare nucleo e immagine di f e di g.
   - Descrivere il gruppo quoziente $\mathbb{R}^*/\ker f$.
   - Descrivere il gruppo quoziente $\mathbb{R}^*/\ker g$.
   - Descrivere il gruppo quoziente $\mathbb{R}^*/\mathbb{R}^+$

2. Considerato il campo $\mathbb{F} = \mathbb{Z}_2[\alpha]$ con $\alpha^4 + \alpha + 1 = 0$

   - Verificare che il polinomio $x^4 + x + 1$ è irriducibile in $\mathbb{Z}_2[x]$.
   - Scrivere un polinomio riducibile di quarto grado in $\mathbb{Z}_2[x]$.
   - Scrivere gli elementi del campo $\mathbb{F}$.
   - Calcolare $(1 + \alpha + \alpha^2)(1 + \alpha^3)$ e $(1 + \alpha + \alpha^2) + (1 + \alpha + \alpha^3)$
   - Trovare $(1 + \alpha)^{-1}$.
   - Mostrare che α è un elemento primitivo.
   - Trovare un isomorfismo esplicito tra $\mathbb{F}^*$ e $\mathbb{Z}_{15}$.
   - Trovare un elemento di $\mathbb{F}^*$ di ordine 3.
   - Trovare l'ordine degli elementi di $\mathbb{F}^*$.

TRACCIA DELLE SOLUZIONI

Esercizio n.1:

$$\begin{aligned} f(xy) &= \log\left(x^2y^2\right) = \log(x^2) + \log(y^2) = f(x) + f(y) \\ g(xy) &= \sqrt{x^2y^2} = \sqrt{x^2}\sqrt{y^2} = g(x)g(y) \end{aligned}$$

$$\begin{aligned} \ker f &= \{\pm 1\}, \operatorname{Im} f = \mathbb{R} \\ \ker g &= \{\pm 1\}, \operatorname{Im} f = \mathbb{R}^+ \end{aligned}$$

$\mathbb{R}^*/\ker f = \{\overline{x} = \{\pm x\}, x \in \mathbb{R}^*\}$. Ogni classe può essere rappresentata dal suo elemento positivo e quindi il gruppo quoziente può essere identificato col gruppo moltiplicativo dei reali positivi. Lo stesso è vero per g. Si consideri ora l'omomorfismo suriettivo $h : \mathbb{R}^* \to \{\pm 1\}$ dato da $h(x) = 1$ se x è positivo e $h(x) = -1$ se x è negativo. Il suo nucleo è $\mathbb{R}^+$ e il teorema di isomorfismo assicura quindi che: $\mathbb{R}^*/\mathbb{R}^+ = \{\pm 1\}$.

Esercizio n.2: I 16 elementi sono:

$$\begin{aligned} &1, 1+\alpha, 1+\alpha^2, 1+\alpha^3, 1+\alpha+\alpha^2, 1+\alpha+\alpha^3, 1+\alpha^2+\alpha^3, 1+\alpha+\alpha^2+\alpha^3 \\ &0, \alpha, \alpha^2, \alpha^3, \alpha+\alpha^2, \alpha+\alpha^3, \alpha^2+\alpha^3, \alpha+\alpha^2+\alpha^3 \end{aligned}$$

Posto $(1+\alpha)^{-1} = a + b\alpha + c\alpha^2 + d\alpha^3$ con $a, b, c, d \in \mathbb{Z}_2$, si ha:

$$\begin{aligned} (1+\alpha)\left(a + b\alpha + c\alpha^2 + d\alpha^3\right) &= \\ a + b\alpha + c\alpha^2 + d\alpha^3 + a\alpha + b\alpha^2 + c\alpha^3 + d\alpha^4 &= \\ (a+d) + (a+b+d)\,\alpha + (b+d)\,\alpha^2 + (c+d)\,\alpha^3 &= 1 \end{aligned}$$

da cui si ricava subito: $a = 0, b, c, d = 1$. Un elemento primitivo è un generatore del gruppo $\mathbb{F}^*$ degli elementi invertibili del campo, ovvero un elemento di ordine moltiplicativo $15 = 3 \times 5$; siccome l'ordine di un elemento deve dividere l'ordine del gruppo, basta verificare che l'ordine di α non è né 3, né 5, e questo è immediato.
Un isomorfismo esplicito tra $\mathbb{F}^*$ e $\mathbb{Z}_{15}$ è, ovviamente, $1 \to 0$ e $\alpha \to 1$. E quindi $\alpha^n \to n$. Siccome gli isomorfismi preservano gli ordini, un elemento di ordine 3 è $\alpha^5 = \alpha\alpha^4 = \alpha\,(1+\alpha)$, infatti 5 ha ordine 3 in $\mathbb{Z}_{15}$. Nello stesso modo si trovano facilmente gli ordini di tutti gli elementi di $\mathbb{F}^*$