Esercizio 14.13

Sia dato il polinomio $f(X) = X^4 + 2X^2 + 2 \in \mathbb{Q}[X]$. Ad esso si applicano le seguenti osservazioni:

- Risulta privo di radici razionali. Infatti le uniche possibili radici razionali sono $1,\ -1,\ 2,\ -2$, ma nessuno di questi numeri annulla il polinomio. Si può anche notare che la valutazione di $f(X)$ in un qualsiasi numero reale è sempre positiva.
  Ciò basta per concludere, in base al Primo Corollario al Teorema di Ruffini, che $f(X)$ non possiede, in $\mathbb{Q}[X]$, fattori di grado uno.
- La sua riduzione modulo 2 è X^4, certamente riducibile in $\mathbb{Z}_2[X]$. La sua riduzione modulo 3 è $\overline{f}(X) = X^4 + \overline{2}X^2 + \overline{2}$. Questo polinomio è privo di radici in $\mathbb{Z}_3$, in quanto $\overline{f}(\overline{0}) = \overline{2}$, $\overline{f}(\overline{1}) = \overline{f}(\overline{-1}) = \overline{2}$. Dunque esso non possiede, in $\mathbb{Z}_3[X]$, fattori di grado uno. Pertanto, esso sarà riducibile solo se si decomporrà nel prodotto di due fattori di grado due, ossia ammetterà una decomposizione del tipo

$$\overline{f}(X) = \left(X^2 + aX + b\right)\left(X^2 + cX + d\right),$$

per opportuni coefficienti $a, b, c, d \in \mathbb{Z}_3$. Si osservi come non sia restrittivo supporre che i due fattori siano, come $\overline{f}(X)$, monici. Il prodotto a secondo membro è il polinomio

$$X^4 + (a+c)X^3 + (b+d+ac)X^2 + (ad+bc)X + bd\ .$$

Uguagliando i suoi coefficienti a quelli di $\overline{f}(X)$, si ottiene il seguente sistema di equazioni:

$$\begin{cases} a + c & = & \overline{0} & (3) \\ b + d + ac & = & \overline{2} & (2) \\ ad + bc & = & \overline{0} & (1) \\ bd & = & \overline{2} & (0) \end{cases}$$

La decomposizione precedente esiste se e solo se questo sistema di equazioni ammette soluzione in $\mathbb{Z}_3$. Dalla (0) ricaviamo, a meno di scambiare b e d,

$$b = \overline{1},\ d = \overline{2}.$$

Sostituendo nella (1), si ottiene

$$\overline{2}a + c = \overline{0}, \quad \text{da cui} \quad c = a.$$

Sostituendo nella (3), avremo

$$\overline{2}a = \overline{0}, \quad \text{da cui} \quad a = \overline{0}.$$

Ne consegue che $c = \overline{0}$. Dalla (2) si deduce, infine, che

$$b + d = \overline{2},$$

ma ciò è incompatibile con il fatto che i due addendi a primo membro siano l'uno uguale a $\overline{1}$, l'altro

uguale a $\overline{2}$. Quindi il sistema non è risolubile.

Si conclude che $\overline{f}(X)$ è irriducibile in $\mathbb{Z}_3[X]$. Per il criterio di irriducibilità basato sulla riduzione modulo p, se ne deduce che $f(X)$ è irriducibile in $\mathbb{Q}[X]$.

- Il polinomio $f(X)$ è comunque irriducibile anche in virtù del criterio di Eisenstein, applicabile per $p = 2$.

Osservazione aggiuntiva

Sia $a \in \mathbb{Z}$. Allora, in $\mathbb{Z}_3$,

$$\overline{a} + \overline{a} = \overline{a + a} = \overline{2a} = \overline{2} \cdot \overline{a} \ \ (= 2\overline{a}),$$

ove si sono applicate, nell'ordine,

- la definizione di somma in $\mathbb{Z}_3$,
- la definizione di multiplo in $\mathbb{Z}$,
- la definizione di prodotto in $\mathbb{Z}_3$,
- (la definizione di multiplo in $\mathbb{Z}_3$)

Infine, se $\overline{2} \cdot \overline{a} = \overline{0}$, allora $\overline{a} = \overline{0}$ segue dalla cancellabilità di $\overline{2}$ in $\mathbb{Z}_3$, dovuta al fatto che 2 e 3 sono coprimi.