Número no construible con regla y compás

Sea $P(X) = X^4 + 4X + 2 \in \mathbb{Q}[X]$, como es irreducible por Eisenstein, si llamamos $x_1, x_2, x_3, x_4 \in \mathbb{C}$ a sus raíces, resulta que $(\mathbb{Q}[x_i] : \mathbb{Q}) = 4 \ \forall i$. Veamos que el cuerpo de descomposición $\mathbb{Q}[x_1, x_2, x_3, x_4]$ contiene alguna subextensión de grado 3.

Recordemos cómo resolver la ecuación de grado cuatro:

$$X^4 + aX^2 + bX + c = 0$$

le sumamos y le restamos $2uX^2 + u^2$ y obtenemos

$$\begin{aligned}
0 &= X^4 + aX^2 + bX + c + 2uX^2 + u^2 - (2uX^2 + u^2) \\
0 &= X^4 + 2uX^2 + u^2 + aX^2 + bX + c - (2uX^2 + u^2) \\
0 &= (X^2 + u)^2 - ((2u - a)X^2 - bX + u^2 - c) \\
(X^2 + u)^2 &= (2u - a)X^2 - bX + u^2 - c
\end{aligned}$$

y queremos elegir u de manera tal que $(2u-a)X^2 - bX + u^2 - c$ sea el cuadrado de un binomio, es decir, debemos resolver $b^2 - 4(2u - a)(u^2 - c) = 0$ que es una ecuación de grado tres. Una vez resuelta nos queda:

$$\begin{aligned}
(X^2 + u)^2 &= (2u - a)X^2 - bX + u^2 - c \\
(X^2 + u)^2 &= ((\sqrt{2u - a})X + (\sqrt{u^2 - c}))^2 \\
X^2 + u &= \pm((\sqrt{2u - a})X + (\sqrt{u^2 - c}))
\end{aligned}$$

y de estas dos cuadráticas despejamos x_1, x_2, x_3, x_4

Supongamos que x_1 y x_2 son las raíces de

$$X^2 + u = (\sqrt{2u - a})X + (\sqrt{u^2 - c})$$

es decir

$$\begin{aligned}
x_1^2 + u &= (\sqrt{2u - a})x_1 + (\sqrt{u^2 - c}) \\
x_2^2 + u &= (\sqrt{2u - a})x_2 + (\sqrt{u^2 - c})
\end{aligned}$$

restando ambas ecuaciones obtenemos:

$$\begin{aligned}
x_1^2 - x_2^2 &= (\sqrt{2u - a})(x_1 - x_2) \\
x_1 + x_2 &= (\sqrt{2u - a}) \\
(x_1 + x_2)^2 &= 2u - a \\
\frac{(x_1 + x_2)^2 + a}{2} &= u
\end{aligned}$$

de donde queda claro que $u \in \mathbb{Q}[x_1, x_2] \subseteq \mathbb{Q}[x_1, x_2, x_3, x_4]$.

Volviendo al cuerpo de descomposición de $P(X) = X^4 + 4X + 2 \in \mathbb{Q}[X]$.

$$\begin{aligned}
0 &= X^4 + 4X + 3 + 2uX^2 + u^2 - (2uX^2 + u^2) \\
0 &= X^4 + 2uX^2 + u^2 + 4X + 2 - (2uX^2 + u^2) \\
0 &= (X^2 + u)^2 - (2uX^2 - 4X + u^2 - 2) \\
2uX^2 - 4X + u^2 - 2 &= (X^2 + u)^2
\end{aligned}$$

de donde u satisface:

$$\begin{aligned}
0 &= 4^2 - 4(2u)(u^2 - 2) \\
0 &= 4 - 2u(u^2 - 2) \\
0 &= 2 - u(u^2 - 2) \\
0 &= u^3 - 2u - 2
\end{aligned}$$

pero $X^3 - 2X - 2 \in \mathbb{Q}[X]$ es irreducible (por el criterio de Eisenstein). Entonces $(\mathbb{Q}[u] : \mathbb{Q}) = 3$ y ya sabíamos que $\mathbb{Q}[u] \subseteq \mathbb{Q}[x_1, x_2] \subseteq \mathbb{Q}[x_1, x_2, x_3, x_4]$.

Por otro lado, si tuviésemos una resolución $\mathbb{Q} \subsetneq E \subsetneq \mathbb{Q}[x_1]$, con $2 = (E : \mathbb{Q}) = (\mathbb{Q}[x_1] : E)$, tomando $Q = irr(x_1, E) \in E[X]$ tendría grado dos, y $\frac{P}{Q} = R \in E[X]$ también, suponiendo que x_2 sea la otra raíz de Q nos quedaría $\mathbb{Q}[x_1] = \mathbb{Q}[x_1, x_2]$ y $(\mathbb{Q}[x_1, x_2, x_3, x_4] : \mathbb{Q}[x_1, x_2]) = 2$ o 1.

Pero en este caso tendríamos

$$\begin{aligned}
(\mathbb{Q}[x_1, x_2, x_3, x_4] : \mathbb{Q}) &= (\mathbb{Q}[x_1, x_2, x_3, x_4] : \mathbb{Q}[x_1, x_2])(\mathbb{Q}[x_1, x_2] : \mathbb{Q}) \\
&= 4\,(\mathbb{Q}[x_1, x_2, x_3, x_4] : \mathbb{Q}[x_1, x_2]) \\
&= 8 \text{ o } 4
\end{aligned}$$

absurdo! pues ya sabemos que $\mathbb{Q}[u] \subseteq \mathbb{Q}[x_1, x_2, x_3, x_4]$.$\square$