$$
\begin{tikzcd}
 & \mathbb{C} \arrow[d, dash] & \\
 & \mathbb{A} & \\
 & \mathbb{Q}(i)[\sqrt[3]{2}] \arrow[u] \arrow[dl, dash] \arrow[dd, dash, "6"] \arrow[dr, dash, "3"] & \\
 \mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash, "3"'] & & \mathbb{Q}(i) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

$x^3-2=\min_{\mathbb{Q}}(\sqrt[3]{2})$

$x^2+1=\min_{\mathbb{Q}}(i)$

$x^3-2=\min_{\mathbb{Q}(i)}(\sqrt[3]{2})$

Cor. Let $F \subseteq E \subseteq L$ extensiones de campos y supongamos que E es algebraica sobre F. Si $\alpha \in L$ es algebraico sobre E, entonces α es algebraico sobre F.

Dem:

Sea $f(x) = e_0 + e_1 x + \cdots + e_n x^n \in E[x]$ tal que $f(\alpha) = 0$. Como cada e_i es algebraico sobre F, la extension $F \subseteq F[e_1, \ldots, e_n]$ es de grado finito, y por lo tanto algebraica. Notemos que $f(x) \in F[e_1, \ldots, e_n][x]$. Entonces α es algebraico, sobre $F[e_1, \ldots, e_n]$ y por lo tanto $[F[e_1, \ldots, e_n][\alpha] : F[e_1, \ldots, e_n]]$ es finita.

Por un resultado anterior

$$[F[e_1,\dots,e_n][\alpha]:F]$$

$$\begin{array}{cl} F[e_1,\dots,e_n][\alpha] & \\ | & \big\} <\infty = [F[e_1,\dots,e_n][\alpha]:F[e_1,\dots,e_n]][F[e_1,\dots,e_n]:F] < \infty \\ F[e_1,\dots,e_n] & \\ | & \big\} <\infty \\ F & \end{array}$$

Esto implica que α es algebraico sobre F.

Teorema: Sea $F \subseteq E$ una extension de campos y sea $\alpha \in E$ algebraico sobre F. Sea $I = \{f \in F[x] \mid f(\alpha) = 0\}$. Entonces I es un ideal de $F[x]$ y se tiene que:

a) I contiene un único polinomio mónico irreducible.

b) Si $f(x) \in I$ es irreducible, entonces $[F[\alpha] : F] = gr(f)$.

c) Si $f(x) \in I$ es irreducible, entonces $I = \langle f(x) \rangle$.

d) $F[\alpha] \cong F[x]/I$.

Dem:

d) Por definicion $I = \operatorname{Ker} ev_\alpha|_{F[x]}$, por lo tanto es un ideal. Además $F[\alpha] = \operatorname{Im} ev_\alpha|_{F[x]} \cong F[x]/I$

Como $F[x]$ es un DIP, $I = \langle g(x) \rangle$ para algún $g(x) \in F[x]$. Notemos que $g \neq 0$ y g no es constante. Ya que α es algebraico y $g(\alpha) = 0$.

Multiplicando por una constante podemos

asumir que $g(x)$ es mónico.

Si $f(x) \in I$ es irreducible, ent $f(x) = g(x)h(x)$. Esto implica que $h(x)$ es una unidad en particular, $\underbrace{gr(h)=0}$. Por lo tanto $g(x) = f(x)(h(x))^{-1}$. Por lo tanto $\langle g(x) \rangle = \underline{I} = \langle f(x) \rangle$. Esto tambien nos dice que $gr(f) = gr(g)$ y si $f(x)$ es mónico entonces $f(x) = g(x)$. Esto prueba (c)

Ahora supongamos que $g(x) = g_1(x)g_2(x)$. Entonces $g(\alpha) = g_1(\alpha)g_2(\alpha) = 0$

Entonces $g_1(\alpha)=0$ ó $g_2(\alpha)$. Es decir, $g_1(x)\in I$ ó $g_2(x)\in I$. En cualquiera de los casos $g|g_1$ ó $g|g_2$ pero $g_1|g$ y $g_2|g$. Esto implica que $g=u_1g_1$ ó $g=u_2g_2$ u_i unidad. Esto implica que $g_1(x)$ ó $g_2(x)$ es unidad. $\therefore$ (a).

Nos falta probar (b). Por un lema anterior $[F[\alpha]:F]\leq gr(g)=n$. Afirmamos que es conjunto $\{1,\alpha,\dots,\alpha^{n-1}\}\subseteq F[\alpha]$ es lin. ind. Supongamos que

$$\sum_{i=0}^{n-1} a_i\alpha^i=0.$$

Sea $f(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$

Entonces $f(\alpha)=0$. Por lo tanto

$f(x) \in I$. Así $g(x) \mid f(x)$ pero $gr(g) = n$
y $gr(f(x)) \leq n-1$. Esto no puede pasar
a menos que $f(x) = 0$ y por lo tanto
$a_i = 0$ $\forall 0 \leq i \leq n-1$. Esto prueba que $\{1, \alpha, \ldots, \alpha^{n-1}\}$
es lin. ind. $\therefore [F[\alpha] : F] = n = gr(g)$.

El único polinomio mónico irreducible $m \in F[x]$ tal que $m(\alpha) = 0$ es llamado
el polinomio mínimo de α sobre F y escribimos $m = \min_F(\alpha)$.

Notemos que $\min_F(\alpha)$ divide a cualquier polinomio $f(x) \in F[x]$ tal que $f(\alpha) = 0$.

Ejemplo: Sea $p \in \mathbb{Z}$ un primo y consideremos el polinomio $x^n - p \in \mathbb{Q}[x]$. $\sqrt[n]{p}$ es una raiz del polinomio monico $x^n - p$. Por lo tanto $\min_{\mathbb{Q}}(\sqrt[n]{p}) = x^n - p$. Entonces se tiene que $[\mathbb{Q}[\sqrt[n]{p}] : \mathbb{Q}] = n$.

Al conjunto de todos los $\alpha \in \mathbb{C}$ que son algebraicos sobre $\mathbb{Q}$ se le denota $\mathbb{A}$. Es decir, $\mathbb{A} = \{\alpha \in \mathbb{C} \mid \alpha \text{ es algebraico sobre } \mathbb{Q}\}$. A los elementos de $\mathbb{A}$ se les llama numeros algebraicos.

Por un resultado anterior tenemos que $\mathbb{A}$ es un campo intermedio entre $\mathbb{Q}$ y $\mathbb{C}$. Ademas, por definición la extensión $\mathbb{Q} \subseteq \mathbb{A}$ es algebraica sobre $\mathbb{Q}$. Notemos que por el ejemplo anterior $[\mathbb{A} : \mathbb{Q}] > n$ para toda n

ya que $\underbrace{\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[n]{p})}_{n} \subsetneq \mathbb{A}$

Cor. La extension $\mathbb{Q} \subseteq \mathbb{A}$ es de grado infinito.

Volvamos a considerar el polinomio $\underbrace{x^n - p}$ con p primo. Supongamos que tenemos $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$ tal que $[F:\mathbb{Q}]=\underline{m}$ con $\underline{\mathrm{mcd}(n,m)=1}$. Afirmamos que $\underline{x^n - p \text{ es}}$ $\underline{\text{irreducible sobre } F}$. Primero notemos que $\sqrt[n]{p} \notin F$. De lo contrario,

$$[F:\mathbb{Q}]=[F:\mathbb{Q}(\sqrt[n]{p})][\mathbb{Q}(\sqrt[n]{p}):\mathbb{Q}]$$ así que

$$\begin{tikzcd} F \arrow[d, dash] \arrow[dd, dash, bend right, "m"'] \\ \mathbb{Q}[\sqrt[n]{p}] \arrow[d, dash, "n"] \\ \mathbb{Q} \end{tikzcd}$$

$n \mid m$. ¡

$$\begin{tikzcd} & F[\sqrt[n]{p}] \arrow[dl, dash] \arrow[dr, dash, "\leftarrow n"] \arrow[dd, dash, "nm"] & \\ \mathbb{Q}(\sqrt[n]{p}) \arrow[dr, dash, "n"'] & & F \arrow[dl, dash, "m \leftarrow"] \\ & \mathbb{Q} & \end{tikzcd}$$

Consideremos el campo $F[\sqrt[n]{p}]$ y $f=\min_F(\sqrt[n]{p})$ así $[F[\sqrt[n]{p}]:F]=gr(f)$

Tenemos que $[F[\sqrt[n]{p}]:\mathbb{Q}]=[F[\sqrt[n]{p}]:F][F:\mathbb{Q}]$

Por otro lado $[F[\sqrt[n]{p}]:\mathbb{Q}]$ es divisible entre n. Por lo tantanto

$n \mid [F[\sqrt[n]{p}]:\mathbb{Q}]=gr(f)m$. Como $mcd(m,n)=1$

se tiene que $n \mid gr(f)$.

Si denotamos $g(x)=x^n-p\in F[x]$, como

$g(\sqrt[n]{p})=0$, entonces $f \mid g$. Esto implica

que $gr(f) \leq n$. Pero como $n \mid gr(f)$

$gr(f)=n$. Al ser $g(x)$ y $f(x)$ monicos

$g(x)=f(x)$ $\therefore$ $\min_F(\sqrt[n]{p})=x^n-p$.