CORPS DES NOMBRES ALGEBRIQUES.

Théorème: Soit $K \subseteq L$ une extension de corps et L algébriquement clos.

1) Les éléments de L algébriques sur K forment un corps, $alg(K) \subseteq L$.

2) $alg(K)$ est algébriquement clos, donc $alg(K) = L$.

3) Si $\lambda, \mu \in alg(K)$, alors un polynôme annulateur de $\lambda+\mu$ est donné par
$$R(X) = \mathrm{Res}_{K(X)}(P(X-Y), Q(Y)).$$

Preuve:

1) Supposons $x, y \in alg(K)$, alors $[K(x):K] < +\infty$.
Si $y \in alg(K)$, alors $y \in alg(K(x))$, donc $K(x)[y] = K(x)(y)$ est un $K(x)$-ev de dimension finie.
Donc $[K(x,y) : K(x)] < +\infty$ d'où, $[K(x,y):K] = [K(x,y):K(x)]\cdot[K(x):K] < +\infty$.
Or, $K(x-y) \subseteq K(x,y)$ et $K(xy^{-1}) \subseteq K(x,y)$ si $y \neq 0$. Donc, on a
$$+\infty > [K(x,y):K] = [K(x,y):K(x-y)]\cdot[K(x-y):K]$$ Donc $[K(x-y):K] < +\infty$. idem pour $K(xy^{-1})$

2) On considère un polynôme non nul de $alg(K)[X]$, $P = \sum_{k=0}^{n} a_k X^k$ de racine z dans L alg. clos.
On va montrer que $z \in alg(K)$.
Par définition, $[K(a_0):K] < +\infty$ et de même qu'en (1), $[K(a_1,a_0):K(a_0)] < +\infty$, donc par multiplicativité des degrés, $[K(a_1,a_0):K] < +\infty$ et $[K(a_n,..,a_0):K(a_{n-1},\dots,a_0)] < +\infty$ et par une récurrence, $[K(a_n,..,a_0):K] < +\infty$. Or, comme $P(z) = 0$, alors
$$+\infty > [K(a_n,..,a_0,z):K] = [K(a_n,..,a_0,z):K(a_n,..,a_0)]\cdot[K(a_n,..,a_0):K]$$
Comme $z \in K(a_n,..,a_0,z)$, on en déduit que $K(z) \subseteq K(a_n,..,a_0,z)$ et que $[K(z):K] < +\infty$, donc $z \in alg(K)$.

3) **Lemme:** Soient $A \in \mathbb{K}_n[X]$ et $B \in \mathbb{K}_m[X]$. On définit le résultant $\mathrm{Res}(A,B)$ comme le déterminant de l'application linéaire:
$$\varphi : (U,V) \in \mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X] \longmapsto AU+BV \in \mathbb{K}_{n+m-1}[X].$$
Alors $\mathrm{Res}(A,B) \neq 0 \Leftrightarrow A \wedge B = 1$.

Preuve: Si $\mathrm{Res}(A,B) \neq 0$, alors φ est un isomorphisme, donc est surjectif, et $\exists (U,V) \in \mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X]$ tq. $AU+BV = 1$, donc $A \wedge B = 1$ par le thm de Bézout.
Si $A \wedge B = 1$, montrons que $\ker \varphi = \{(0,0)\}$. Soit $(U,V) \in \ker\varphi$. Alors,
$$AU + BV = 0 \Leftrightarrow AU = -BV.$$
Par le lemme de Gauss, comme $A \wedge B = 1$, alors, $A | V$ or, $\deg V = n-1 < \deg A = n$.
Donc $V = 0$. Donc $AU = 0$, et par intégrité de $\mathbb{K}[X]$, si $A \neq 0$, alors, $U = 0$. Donc $\ker\varphi = \{(0,0)\}$ et $\mathrm{Res}(A,B) = 0$

Sachant cela, si λ est annulé par $P \in K[Y]$ et μ par $Q \in K[Y]$, alors
... Dans ce cas $P(\lambda+\mu-Y)$ et $Q(Y)$ s'annulent en μ. Donc le résultant de ces deux polynômes en Y s'annule.

Ainsi, en regardant $P(X-Y)$ et $Q(Y)$ comme des polynômes à coefficients dans $K(X)$, on trouve que le résultant sera un élément de $K(X)$,

$$R(X) = \mathrm{Res}\,(P(X-Y), Q(Y))$$

En fait, $R(X) \in K[X]$ car c'est une sommes et produits de polynômes en X, et $R(\lambda+\mu)=0$.

Remarques :

▷ Développement que j'ai adoré préparé : thème classique, mais la troisième partie rend le développement de très bon niveau, avec l'apport du résultant (hors programme).

▷ De la même façon qu'on le fait pour la somme, le résultant permet de construire un polynôme annulateur pour le produit de nombres algébriques.
J'aimais bien présenter ce développement en disant que l'on peut montrer que l'espace des nombres algébriques est un corps de deux façons : une théorique et efficace, l'autre constructive mais plus calculatoire.

▷ Calculer un résultant, c'est calculer un déterminant, donc peu efficace en pratique. Par ailleurs, le résultant donne un polynôme annulateur, qui n'a aucune raison d'être minimal.
Mais je suppose qu'en présentant ce développement, il faut être capable, par le résultant, de trouver un polynôme annulateur de nombres du type $\sqrt{2} + \sqrt[3]{5}$.