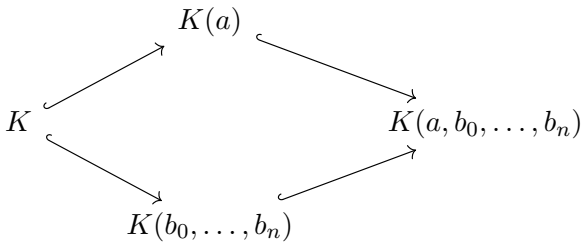
Exercice 1.
Soient $K \subset L \subset F$ comme dans l'énoncé. Pour montrer que F est algébrique sur K, il suffit de montrer que chaque $a \in F$ est algébrique sur K. Puisque a est algébrique sur L, il existe $b_0, \dots, b_n \in L$ tels que $m_{a,L}(t) = \sum_{i=0}^{n} b_i t^i$. En particulier, a est algébrique sur le sous-corps $K(b_0, \dots, b_n)$.

Nous allons comparer les deux chaînes d'extensions suivantes :



On prétend que les degrés

$$[K(a, b_0, \dots, b_n) : K(b_0, \dots, b_n)] \quad \text{et} \quad [K(b_0, \dots, b_n) : K]$$

sont finis. C'est le cas du premier par construction (cf la Proposition 4.2.7 et le Corollaire 4.2.13). Pour le second, par la formule de multiplication des degrés on se réduit à montrer que chaque

$$[K(b_0, \dots, b_{i+1}) : K(b_0, \dots, b_i)]$$

est fini. C'est le cas par le Corollaire 4.2.13, puisque b_{i+1} est algébrique sur K, donc a fortiori sur $K(b_0, \dots, b_i)$. On peut ainsi appliquer la Proposition 4.2.15 pour obtenir

$$[K(a, b_0, \dots, b_n) : K] = [K(a, b_0, \dots, b_n) : K(b_0, \dots, b_n)] \cdot [K(b_0, \dots, b_n) : K] < \infty.$$

On en déduit que l'extension intermédiaire $K \subset K(a) \subset K(a, b_0, \dots, b_n)$ est de degré fini sur K (il s'agit simplement d'algèbre linéaire : un sous-espace vectoriel d'un espace de dimension finie, est également de dimension finie). Donc a est algébrique sur K par le Corollaire 4.2.13.

Exercice 2.
Comme

$$\cos(2\pi/n) = \frac{e^{2\pi i/n} + e^{-2\pi i/n}}{2} \quad \sin(2\pi/n) = \frac{e^{2\pi i/n} - e^{-2\pi i/n}}{2i}$$

on voit que $\cos(2\pi/n), \sin(2\pi/n) \in \mathbb{Q}(\xi_n, i)$ si ξ_n désigne une racine primitive n-ième de l'unité, ce qui conclut.

On peut aussi tirer partie des polynômes de Chebyshev $\{T_n(x)\}_n$, qui ont la propriété que

$$\cos(n\theta) = T_n(\cos(\theta)) \quad \forall \theta \in \mathbb{R}\ n \geq 0.$$

Les polynômes $T_n(x)$ sont définis par la relation de récurrence

$$T_0(x) = 1, \quad T_1(x) = x, \quad T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x).$$

et il s'ensuit que les coefficients de $T_n(x)$ sont rationnels (et même entiers) pour tous les n.

On voit ainsi que $\cos(\theta)$ est algébrique sur $\mathbb{Q}(\cos(n\theta))$ pour tout $n \geq 1$. En prenant $\theta = 2\pi/m$ et $n = m$, on obtient ainsi que $\cos(2\pi/n)$ est algébrique sur $\mathbb{Q}(\cos(2\pi)) = \mathbb{Q}$.

Pour finir, la relation bien connue $\cos^2(\theta) + \sin^2(\theta) = 1$ entraîne que $\sin(2\pi/n)$ est algébrique sur $\mathbb{Q}(\cos(2\pi/n))$, et donc sur $\mathbb{Q}$ par l'Exercice 1.

Exercice 3.
Dans $\mathbb{Q}(x)$ on a la relation $x^3 - sx + 2 = 0$, ce qui montre que x est une racine du polynôme $t^3 - st + 2 \in \mathbb{Q}(s)[t]$. Ainsi $\mathbb{Q}(x) = \mathbb{Q}(s, x)$ est une extension algébrique de $\mathbb{Q}(s)$. On prétend que $\mathbb{Q}(s)$ est une extension transcendante de $\mathbb{Q}$. Si ce n'était pas le cas, alors par l'Exercice 1 l'extension $\mathbb{Q} \subset \mathbb{Q}(x)$ serait également algébrique, ce qui est absurde. Donc $[\mathbb{Q}(s) : \mathbb{Q}] = \infty$.

Calculons ensuite le degré de $\mathbb{Q}(x)$ sur $\mathbb{Q}(s)$. On prétend que $t^3 - st + 2$ est irréductible dans $\mathbb{Q}(s)[t]$, et il s'ensuivra que $[\mathbb{Q}(x) : \mathbb{Q}(s)] = 3$. Si ce polynôme n'est pas irréductible, puisqu'il est de degré 3 il doit admettre une racine dans $\mathbb{Q}(s)$. Puisque s est transcendant sur $\mathbb{Q}$, on peut traiter s comme une variable indépendante et oublier qu'elle a été définie en fonction de x. Supposons donc qu'il existe $p(s), q(s) \in \mathbb{Q}[s]$ tels que

$$\frac{p^3}{q^3} - s\frac{p}{q} + 2 = 0.$$

On obtient donc

$$p\left[p^2 - sq^2\right] = -2q^3 \quad \text{dans } \mathbb{Q}[s].$$

Distinguons deux cas :

1. p est un polynôme constant, qu'on peut sans perte de généralité prendre égal à 1. Dans ce cas $1 - sq^2 = -2q^3$. Le terme constant de $1 - sq^2$ vaut 1, tandis que celui de $-2q^3$ vaut $-2b^3$ où b est le coefficient constant de q. Donc $b \in \mathbb{Q}$ est une racine cubique de $-1/2$, ce qui est impossible. Donc p ne peut être constant.

2. p n'est pas constant. Puisque p divise le membre de gauche, il doit aussi diviser $-2q^3$, et donc q^3. En particulier p et q ne sont pas premiers entre eux. Or on peut sans perte de généralité les supposer premiers entre eux, on a donc une contradiction.

On obtient ainsi que $t^3 - st + 2$ est irréductible dans $\mathbb{Q}(s)$, ce qui conclut.

Voici une autre méthode pour montrer que $t^3 - st + 2 \in \mathbb{Q}(s)[t]$ est irréductible. Par le lemme de Gauss III, il suffit de montrer que ce polynôme est irréductible dans $\mathbb{Q}[s][t]$. Par la Proposition 3.9.1, il suffit de montrer que la réduction modulo s, à savoir $t^3 + 2 \in \mathbb{Q}[t]$, est irréducible. Par Gauss III encore, il suffit de montrer que $t^3+2 \in \mathbb{Z}[t]$ est irréductible, et cela se vérifie en appliquant le critère d'Eisenstein.

Exercice 4.
Note that the complex roots of $x^2 - 2$ are of the form $e^{\frac{2\pi ik}{n}}\sqrt{2}$ for $0 \leq k < n$. Moreover, note that $x^{2n} - 3x^n + 2$ can be factorized as $x^{2n} - 3x^n + 2 = (x^n - 2)(x^n - 1)$. One can conclude for Lemma 4.3.3 point (1) that the splitting fields are the same and they are given by $\mathbb{Q}(\xi, \sqrt[n]{2})$.

Exercice 5. 1. : These two polynomials are $x^3 + x + 1$ and $x^3 + x^2 + 1$, because we know that a degree 3 polynomial is irreducible if and only if it does not have a root. If we plug in 0, this means that we have to have a constant term, and if we plug in 1, this means that there has to be an odd number of terms. These two conditions together leave only the above two polynomials.

2. In both cases if α denotes the class of x in the quotient, then α^2 and α^4 are also roots of f.* This follows from $f(\alpha^2) = f(\alpha)^2 = 0$ and $f(\alpha^4) = f(\alpha)^4 = 0$. Note that they are indeed diffferent elements because they are represented by the classes of the polynominals x, x^2 and $x^2 + x$ and $x^3 + x$ respectively in the cases $f = x^3 + x + 1$ and $f = x^3 + x^2 + 1$.

   Remarque. C'est un fait général qui suit du fait que tous les corps finis sont des corps de décomposition que si $f(x) \in \mathbb{F}_q[x]$ est irréductible, alors il scinde sur $\mathbb{F}_q[x]/f(x)$ et les racines dans le quotient sont données par les classes x^{q^i} pour $i = 0, \deg(f) - 1$.

*This is also well understood using Galois theory.

3. Note that f and g are irreducible and that K is a field such that $L = \mathbb{F}_2[x]/f \cong \mathbb{F}_2(\alpha)$, where α is a roots of f. Since L is a extension of degree 3 of $K = \mathbb{F}_2[x]$, it is a finite field. Then by theorem 4.4.17, L is a splitting field of $x^8 - x$ over K. To see that it is also the splitting field of g, we know from the previous point that K contains all the roots of g and is an extension of degree 3. Using this one can conclude that K satisfies the definition of being the splitting field of g.

Exercice 6. 1. Use the following isomorphisms to define $\eta : K(\alpha) \to K'(\alpha')$

$$K(\alpha) \cong K[x]/(m_{\alpha,K}) \cong K'[x]/(\xi(m_{\alpha,K})) \cong K'[x]/(m_{\alpha',K'}) \cong K'(\alpha')$$

This shows that $L \cong L'$, and moreover by the universal property of polynomial rings and of fraction fields we have that η is the unique extension of ϕ such that $\eta(\alpha) = \alpha'$.

2. Use point (1) with the automorphism $K(x) \to K(x)$ given by $x \mapsto x + 1$. This isomorphism is induced by the universal property of polynomial rings and of fraction fields, and also that it is an isomorphism because it has an inverse given by $x \mapsto x - 1$

3. Use point (1) with the automorphism $K(x, y) \to K(x, y)$ given by $x \mapsto x$ and $y \mapsto x + y$, here the inverse is $x \mapsto x$ and $y \mapsto y - x$.