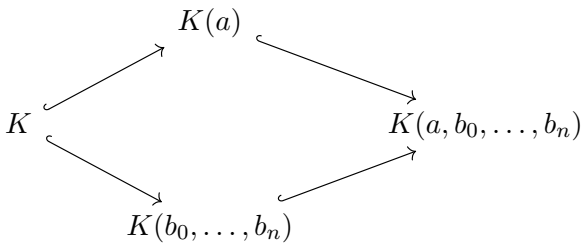
Exercice 1.
Soient $K \subset L \subset F$ comme dans l'énoncé. Pour montrer que F est algébrique sur K, il suffit de montrer que chaque $a \in F$ est algébrique sur K. Puisque a est algébrique sur L, il existe $b_0, \dots, b_n \in L$ tels que $m_{a,L}(t) = \sum_{i=0}^{n} b_i t^i$. En particulier, a 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 $[\mathbb{Q}(x) : \mathbb{Q}(s)] = 3$.

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.

Voici une autre méthode pour montrer que ce polynôme est irréductible. 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.

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 Corollary 4.3.5 that the splitting fields are the same and they are given by $\mathbb{Q}(\xi, \sqrt[n]{2})$.

Exercice 5. 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 $L \cong L'$, so we have proven the existence of η. The uniqueness follows from the fact L is generated by K and α by definition, so knowing the image of K and that of α entirely determines the image of L.

2. Consider the ϕ: $K(x) \to K(x)$ 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 $x \mapsto x - 1$.

   Let $K = K' = K(x)$, $L = K(x)(\sqrt{x+1})$ and $L' = K(x)[\sqrt{x+2}]$. Then ϕ sends the minimal polynomial of $\sqrt{x+1}$ to that of $\sqrt{x+2}$, so by (1) we deduce that $L \cong L'$.

3. Use point (1) and the same idea as in (2) 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 $y \mapsto y-x$.

Exercice Bonus. 1. Soit $F = \mathbb{F}_p(x, y^p)$. Calculons les degrés des extensions $K \subseteq F$ et $F \subseteq L$. Nous calculerons uniquement le degré de $K \subseteq F$, car l'autre calcul est identique.

Montrons que le polynôme $f(t) = t^p - x^p \in K[t] = \mathbb{F}_p(x^p, y^p)[t]$ est irréductible. Si on pouvait écrire $f(t) = g(t)h(t)$ avec $g, h \in K[t]$, alors on a aussi l'égalité

$$t^p - x^p = f(t) = g(t)h(t)$$

dans $\mathbb{F}_p(x,y)$!

Or, on peut écrire $t^p - x^p = (t-x)^p$ dans $\mathbb{F}_p(x,y)[t]$ (on ne pouvait pas le faire dans $K[t]$, vu que $x \notin K$). Cela implique qu'à unité près, on a $g(t) = (t-x)^a$ et $h(t) = (t-x)^b$ avec $a+b = p$. Le coefficient constant de $(t-x)^a$ est x^a, et vu que $g(t) \in K[t]$, cela force $x^a \in K$. Le seul cas ou c'est possible est que $a = 0$ ou $a = p$, i.e. $g(t) = f(t)$ ou est constant (à unité près). On a donc montré que $f(t)$ était irréductible de degré p, et donc

$$[F : K] = p.$$

Le même calcul montre que $[L : F] = p$, et donc

$$[L : K] = [L : F][F : K] = p^2.$$

2. Soit $\sigma \in \mathrm{Gal}(L/K)$, et soit $\alpha \in L$. Notons que $\alpha^p \in K$. En effet, c'est le cas pour x et y, et vu que ces deux éléments génèrent L/K et que la puissance p est un morphisme d'anneaux (on est en caractéristique p), c'est aussi le cas de tout $\alpha \in L$.

On a donc

$$\alpha^p = \sigma(\alpha^p) = \sigma(\alpha)^p,$$

ou la première égalité vient que $\alpha^p \in K$ et $\sigma|_K = id_K$.

On a donc

$$(\sigma(\alpha) - \alpha)^p = \sigma(\alpha)^p - \alpha^p = 0,$$

donc on a forcément que $\sigma(\alpha) = \alpha$. On a donc montré que $\sigma = id$, et donc

$$\mathrm{Gal}(L/K) = \{id\}.$$

3. Supposons que L/K soit générée par un élément, disons β. Vu que $\beta^p \in K$ (cf plus haut), on déduit que β satisfait l'équation algébrique $t^p - \beta^p \in K[t]$. Soit m le polynôme minimal de β sur K. Alors automatiquement m divise $t^p - \beta^p$, et on a donc

$$p^2 = [L : K] = [K(\beta) : K] = \deg(m) \leq \deg(t^p - \beta^p) = p,$$

ce qui est une contradiction.

4. Pour tout $\gamma \in K$, considérons l'extension intermédiaire

$$F_\gamma := K(x + \gamma y) \subseteq L.$$

Montrons que pour $\gamma \neq \gamma'$, on a $F_\gamma \neq F_{\gamma'}$. Cela conclura la preuve, car K est infini.

Soient $\gamma \neq \gamma' \in K$, et supposons par l'absurde que $F_\gamma = F_{\gamma'}$. Notons F ce corps. Alors par construction, on a que

$$\begin{cases} x + \gamma y \in F \\ x + \gamma' y \in F. \end{cases}$$

On peut alors sousraire et obtenir que

$$(\gamma - \gamma')y \in F.$$

Comme $\gamma \neq \gamma'$ et que K est un corps, on peut diviser et déduire que

$$y \in F.$$

Or si $x + \gamma y \in F$ et $y \in F$, on a donc que $x \in F$. Vu que $x, y \in F$, on déduit alors que $F = L$. Or, F est généré par un éléments, ce qui contredit le point précédent.