Exercice 1.
Soit $K = \mathbb{Q}(\sqrt{3}+\sqrt{7})$. Montrez que $[K : \mathbb{Q}] = 4$.

Solution. It holds that $\mathbb{Q}(\sqrt{3}+\sqrt{7}) \subseteq \mathbb{Q}(\sqrt{3},\sqrt{7})$. We show that indeed it holds that $\mathbb{Q}(\sqrt{3}+\sqrt{7}) = \mathbb{Q}(\sqrt{3},\sqrt{7})$. For this, it is enough to show that $\sqrt{3} \in \mathbb{Q}(\sqrt{3}+\sqrt{7})$ and $\sqrt{7} \in \mathbb{Q}(\sqrt{3}+\sqrt{7})$. We denote $K = \mathbb{Q}(\sqrt{3}+\sqrt{7})$. It holds that $(\sqrt{3}+\sqrt{7})^3 = 24\sqrt{3}+16\sqrt{7} \in K$. With this, and using that $-16\sqrt{3}-16\sqrt{7} \in K$, it follows that their sum is contained in K as well,

$$(24\sqrt{3}+16\sqrt{7}) + (-16\sqrt{3}-16\sqrt{7}) = 8\sqrt{3}.$$

Now using that $\frac{1}{8} \in K$, and $8\sqrt{3} \in K$ we deduce that their product $\sqrt{3} \in K$. From $\sqrt{3} \in K$, it immediately follows that $\sqrt{7} \in K$ as well, since $\sqrt{7} = (\sqrt{3}+\sqrt{7}) - \sqrt{3}$. This shows that indeed $K = \mathbb{Q}(\sqrt{3},\sqrt{7})$.

The degree of the field extension $[\mathbb{Q}(\sqrt{3},\sqrt{7}) : \mathbb{Q}]$ is by definition the dimension of $\mathbb{Q}(\sqrt{3},\sqrt{7})$ as a $\mathbb{Q}$-vector space. Using exercise 3.2, it follows that the degree is 4. $\{1, \sqrt{3}, \sqrt{7}, \sqrt{3}\sqrt{7}\}$ forms a basis of this vector space.

Exercice 2.
Dans tous les cas suivants, calculez le degré de l'extension.

1. $[\mathbb{R}(e^{2i\pi/p}) : \mathbb{R}]$ pour p un nombre premier;
2. $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ pour α une racine de $t^{42}+t^{41}+\cdots+t^2+t+1$;
3. $[\mathbb{Q}(i, \sqrt[5]{13}) : \mathbb{Q}]$;
4. $[\mathbb{F}_3(\alpha) : \mathbb{F}_3]$ où α est une racine de $t^4-t^3-t^2-t-[1]_3 \in \mathbb{F}_3[t]$ (disons que α vit dans le corps de décomposition de ce polynôme sur $\mathbb{F}_3$ pour fixer les idées) La réponse peut changer en fonction de la racine considérée.
5. $[\mathbb{Q}(\sqrt{14+6\sqrt{5}}, \sqrt{3}) : \mathbb{Q}]$ (on pourra calculer $(3+\sqrt{5})^2$ pour commencer);
6. $[\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}((\sqrt[6]{7})^2)\,]$;
7. $[\mathbb{F}_2(\alpha) : \mathbb{F}_2(\alpha^2)\,]$ où α est une racine de $t^3+t+[1]_2 \in \mathbb{F}_2[t]$.

Solution.

1. If $p = 2$, then $e^{2i\pi/2} = -1$, which is contained in $\mathbb{R}$, and hence $\mathbb{R}(e^{2i\pi/p}) = \mathbb{R}$. From this, it follows that the degree of the extension is equal to 1.

   For $p \neq 2$, it holds that $e^{2i\pi/p}$ is a complex number, and not contained in $\mathbb{R}$. By example 4.2.14 (a), we know that $[\mathbb{C} : \mathbb{R}] = 2$. Using exercise 1.2, it follows that $\mathbb{R}(e^{2i\pi/p}) = \mathbb{C}$, and hence $[\mathbb{R}(e^{2i\pi/p}) : \mathbb{R}] = [\mathbb{C} : \mathbb{R}] = 2$.

2. By definition, α vanishes over $t^{42}+t^{41}+\cdots+t^2+t+1$. Furthermore, using the fact that 43 is prime, and Example 3.9.4(b), it follows that $t^{42}+t^{41}+\cdots+t^2+t+1$ is irreducible over $\mathbb{Q}$. Hence we get that $m_{\alpha,\mathbb{Q}} = t^{42}+t^{41}+\cdots+t^2+t+1$, and so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 42$.

3. We follow the same steps as example 4.2.16(a). First, we note that we have the following field extensions, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[5]{13}) \subseteq \mathbb{Q}(\sqrt[5]{13}, i)$. We can calculate the degree of the extension $\mathbb{Q}(\sqrt[5]{13}, i)$ over $\mathbb{Q}$ using proposition 4.2.15. It holds that

$$[\mathbb{Q}(\sqrt[5]{13}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{13}, i) : \mathbb{Q}(\sqrt[5]{13})] \cdot [\mathbb{Q}(\sqrt[5]{13}) : \mathbb{Q}].$$

First, we calculate $[\mathbb{Q}(\sqrt[5]{13}) : \mathbb{Q}]$. The polynomial $x^5 - 13$ vanishes at $\sqrt[5]{13}$. Furthermore, the polynomial is irreducible over $\mathbb{Q}$: By Gauss III, it is equivalent to showing that the polynomial is irreducible over $\mathbb{Z}$. We can apply Eisensteins criterion with $p = 13$, form which irreducibility over $\mathbb{Z}$ follow. Therefore, $m_{\sqrt[5]{13},\mathbb{Q}} = x^5 - 13$, and the degree of the field extension is 5.

Secondly, we calculate $[\mathbb{Q}(\sqrt[5]{13}, i) : \mathbb{Q}(\sqrt[5]{13})]$. Since $\mathbb{Q} \subseteq \mathbb{R}$, and $\sqrt[5]{13} \in \mathbb{R}$, it follows that $\mathbb{Q}(\sqrt[5]{13}) \subseteq \mathbb{R}$. Hence $i \notin \mathbb{Q}(\sqrt[5]{13})$. Using that i is a root of $x^2 + 1$, we get that the degree of i over $\mathbb{Q}(\sqrt[5]{13})$ is 2, and hence $[\mathbb{Q}(\sqrt[5]{13}, i) : \mathbb{Q}(\sqrt[5]{13})] = 2$.

By the formula above, it follows that

$$[\mathbb{Q}(\sqrt[5]{13}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{13}, i) : \mathbb{Q}(\sqrt[5]{13})] \cdot [\mathbb{Q}(\sqrt[5]{13}) : \mathbb{Q}] = 2 \cdot 5 = 10.$$

4. There are two possibilities. The first possibility is that α is the root $\alpha = [1]_3$. In that case, $\mathbb{F}_3(\alpha) = \mathbb{F}_3$, and hence $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = 1$. We can therefore write the polynomial $t^4 - t^3 - t^2 - t - [1]_3 = (t - [1]_3)(t^3 - t + [1]_3)$. If $\alpha \neq [1]_3$, then α is a root of the polynomial $t^3 - t + [1]_3$. But this polynomial is irreducible over $\mathbb{F}_3$, since neither $[0]_3, [1]_3$ or $[2]_3$ is a root of $t^3 - t + [1]_3$. We conclude with the fact that $m_{\alpha,\mathbb{F}_3} = t^3 - t + [1]_3$, and hence $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = 3$.

5. We note that $(3+\sqrt{5})^2 = 14+6\sqrt{5} \Rightarrow 3+\sqrt{5} = \sqrt{14 + 6\sqrt{5}}$. Therefore, $\mathbb{Q}(\sqrt{14 + 6\sqrt{5}}, \sqrt{3}) = \mathbb{Q}(3 + \sqrt{5}, \sqrt{3}) = \mathbb{Q}(\sqrt{5}, \sqrt{3})$. It follows that $[\mathbb{Q}(\sqrt{5}, \sqrt{3}) : \mathbb{Q}] = 4$. $\{1, \sqrt{3}, \sqrt{5}, \sqrt{3}\sqrt{5}\}$ forms a basis of $\mathbb{Q}(\sqrt{5}, \sqrt{3})$ as a $\mathbb{Q}$-vector space.

6. We calculate the degree of the extension using proposition 4.2.15 for the extension $\mathbb{Q} \subseteq \mathbb{Q}((\sqrt[6]{7})^2) \subseteq \mathbb{Q}(\sqrt[6]{7})$, from which it follows that

$$[\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}((\sqrt[6]{7})^2)] \cdot [\mathbb{Q}((\sqrt[6]{7})^2) : \mathbb{Q}].$$

We first calculate $[\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}]$. The polynomial $x^6 - 7 \in \mathbb{Q}[x]$ is zero for $\sqrt[6]{7}$. Furthermore, by Gauss III, it is irreducible if it is irreducible over $\mathbb{Z}$. Applying Eisenstein with $p = 7$, this holds. Hence $m_{\sqrt[6]{7},\mathbb{Q}} = x^6 - 7$, and the degree of the field extension is 6.

Secondly, we calculate $[\mathbb{Q}((\sqrt[6]{7})^2) : \mathbb{Q}]$. It holds that $(\sqrt[6]{7})^2 = \sqrt[3]{7}$. The polynomial $x^3 - 7 \in \mathbb{Q}[x]$ is zero for $\sqrt[3]{7}$. Furthermore, by Gauss III, it is irreducible if it is irreducible over $\mathbb{Z}$. Applying Eisenstein with $p = 7$, this holds. Hence $m_{\sqrt[3]{7},\mathbb{Q}} = x^3 - 7$, and the degree of the field extension is 3.

Using the formula above, we get that $[\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}((\sqrt[6]{7})^2)] = 2$.

7. We apply the same technique as in the exercise above, noting that we have an extension as follows, $\mathbb{F}_2 \subseteq \mathbb{F}_2(\alpha^2) \subseteq \mathbb{F}_2(\alpha)$, and hence

$$[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = [\mathbb{F}_2(\alpha) : \mathbb{F}_2(\alpha^2)] \cdot [\mathbb{F}_2(\alpha^2) : \mathbb{F}_2].$$

On the left hand side, the degree is equal to 3, since $m_{\alpha,\mathbb{F}_2} = t^3 + t + [1]_2$. Hence on the right hand side, one of the factors is 1, and the other one is three. We note that $[\mathbb{F}_2(\alpha^2) : \mathbb{F}_2]$ can not be 1, since $\alpha^2 \notin \mathbb{F}_2$. If α^2 was contained in $\mathbb{F}_2$, then the polynomial $t^2 - \alpha^2 \in \mathbb{F}_2[t]$ vanishes at α, which contradicts the fact that $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 3$. Therefore, $[\mathbb{F}_2(\alpha^2) : \mathbb{F}_2] = 3$, and so $[\mathbb{F}_2(\alpha) : \mathbb{F}_2(\alpha^2)] = 1$.

Exercice 3. 1. Considérons la situation suivante:

- $\phi : K \to K'$ est un isomorphisme des corps,
- $K \subseteq L$ et $K' \subseteq L'$ sont deux extensions de corps
- $L = K(\alpha)$ et $L' = K'(\alpha')$ avec α et α' algébriques sur K et K' respectivement
- si $\xi : K[x] \to K'[x]$ est l'isomorphisme induit par ϕ, alors $\xi(m_{\alpha,K}) = m_{\alpha',K'}$

Démontrez qu'il existe une extension unique de ϕ à un isomorphisme $\eta : L \to L'$ tel que $\eta(\alpha) = \alpha'$

2. Démontrez que $K(x)[\sqrt{x+1}] \cong K(x)[\sqrt{x+2}]$
3. Démontrez que $K(x,y)[\sqrt{xy}] \cong K(x,y)[\sqrt{x(x+y)}]$

Solution.

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 4.
Soit $\xi = e^{\frac{2\pi i}{n}}$ pour un entier $n > 2$. Démontrez que les corps de décomposition de $x^n - 2$ et de $x^{2n} - 3x^n + 2$ sur $\mathbb{Q}$ sont isomorphes entre eux, et aussi isomorphes à

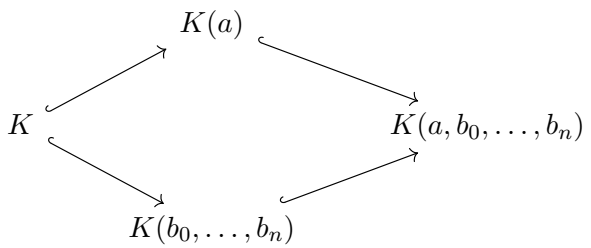
$$\mathbb{Q}(\xi, \sqrt[n]{2}) \subseteq \mathbb{C}.$$

Solution. 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.
Soient $K \subset L \subset F$ des extensions de corps. Si $K \subset L$ et $L \subset F$ sont algébriques, montrez qu'il en est de même pour $K \subset F$.

Solution. 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 $b_0, \ldots, b_n \in L$ tels que $m_{a,L}(t) = \sum_{i=0}^{n} b_i t^i$. En particulier, a est algébrique sur le sous-corps $K(b_0, \ldots, b_n)$.

Nous allons comparer les deux chaînes d'extensions suivantes :



On prétend que les degrés

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

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

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

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

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

On en déduit que l'extension intermédiaire $K \subset K(a) \subset K(a, b_0, \ldots, b_n)$ 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 6.
Soit $\mathbb{Q}(x)$ le corps de fractions de l'anneau polynomial $\mathbb{Q}[x]$, et considérons

$$s := \frac{x^3 + 2}{x} \in \mathbb{Q}(x).$$

On a les extensions successives $\mathbb{Q} \subset \mathbb{Q}(s) \subset \mathbb{Q}(x)$.

1. Montrez que $\mathbb{Q}(x)$ est une extension algébrique de $\mathbb{Q}(s)$.
2. Calculez $[\mathbb{Q}(s) : \mathbb{Q}]$ et $[\mathbb{Q}(x) : \mathbb{Q}(s)]$.

Solution. 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 7.
Soit $f = x^7 - y^5 \in \mathbb{C}[x, y]$. Le but de cet exercice est de démontrer que f est irréductible dans $\mathbb{C}[x, y]$. Soit $K = \mathbb{C}(y)$ et L le corps de décomposition de f sur K. Soit α une racine de f dans L, et $\beta = \frac{\alpha^3}{y^2}$.

1. Montrez que $[K(\beta) : K] = 7$. *Indication: Trouvez un polynôme sur K dont β est une racine.*
2. Montrez que $K(\beta) = K(\alpha)$.
3. Déduisez que f est irréductible dans $\mathbb{C}[x, y]$.

Solution.

1. We show that the minimal polynomial $m_{\beta,K} = x^7 - y \in K[x]$. It holds that the polynomial vanishes at β, since

$$\beta^7 - y = \left(\frac{\alpha^3}{y^2}\right)^7 - y = \frac{(\alpha^7)^3}{y^{14}} - y \overset{*}{=} \frac{(y^5)^3}{y^{14}} - y = y - y = 0,$$

   where in the equation $*$, we use the fact that α is a root of f in L, and hence $\alpha^7 = y^5$. Furthermore, the polynomial is irreducible in $K[x]$: We use Gauss III to deduce that f is irreducible in $K[x] = (\mathbb{C}(y))[x]$ if and only if f is irreducible in $(\mathbb{C}[y])[x]$. Since y is irreducible in $\mathbb{C}[y]$, we may use Eisenstein with $p = y$ to deduce that $x^7 - y$ is irreducible in $(\mathbb{C}[y])[x]$, and hence in $K[x]$. This proves that the minimal polynomial $m_{\beta,K} = x^7 - y \in K[x]$. We conclude that $[K(\beta) : K] = 7$.

2. To show that $K(\alpha) = K(\beta)$, we show that $K(\alpha) \subseteq K(\beta)$ and $K(\beta) \subseteq K(\alpha)$.

   We note that

$$\beta^5 = \left(\frac{\alpha^3}{y^2}\right)^5 = \frac{\alpha^{15}}{(y^5)^2} = \frac{\alpha^{15}}{(\alpha^7)^2} = \alpha.$$

   From this, it follows that $\alpha = \beta^5 \in K(\beta)$, and hence $K(\alpha) \subseteq K(\beta)$. On the other hand, $\beta = \frac{\alpha^3}{y^2} \in K(\alpha)$, and hence $K(\beta) \subseteq K(\alpha)$.

3. We first remark that by Gauss III, f is irreducible in $\mathbb{C}[x, y] = (\mathbb{C}[y])[y]$ if and only if f is irreducible in $(\mathbb{C}(y))[x] = K[x]$. By the first and second part of this exercise, it holds that $[K(\alpha) : K] = 7$. From this, it follows that the degree of the minimal polynomial $m_{\alpha,K}$ is 7. Now since α is a root of $x^7 - y^5 \in K[x]$, it follows that $m_{\alpha,K} | x^7 - y^5$. Since both polynomials are of degree 7, it follows that $m_{\alpha,K} \sim x^7 - y^5$, and from $m_{\alpha,K}$ being irreducible in $K[x]$ it follows that $x^7 - y^5$ is irreducible in $K[x]$ as well. Applying Gauss III, with $x^7 - y^5$ being primitive, it follows that $x^7 - y^5$ is irreducible in $\mathbb{C}[x, y]$.