Exercice 1. (a) Soit A un anneau intègre. Si $a_1, \ldots, a_n \in A$ sont des racines distinctes de $f(x) \in A[x]$, montrer que $\prod_{i=1}^{n}(x - a_i)$ divise $f(x)$.

(b) Soient p et q deux nombres premiers distincts dans $\mathbb{Z}$. Montrer que le polynôme $t^2 - t$ de $(\mathbb{Z}/pq\mathbb{Z})[t]$ possède quatre racines distinctes $a_1, a_2, a_3, a_4 \in \mathbb{Z}/pq\mathbb{Z}$, mais que $(t - a_1)(t - a_2)(t - a_3)(t - a_4)$ ne divise pas $t^2 - t$.

(c) Soient $f, g \in \mathbb{Z}[t]$ des polynômes primitifs. Montrer que si f divise g dans $\mathbb{Q}[t]$, alors f divise g dans $\mathbb{Z}[t]$.

(d) Décomposer les polynômes $t^4 + 1$ et $t^8 - 1$ en facteurs irréductibles dans les anneaux $\mathbb{C}[t]$, $\mathbb{R}[t]$, $\mathbb{Q}[t]$, $\mathbb{Z}[t]$, $\mathbb{F}_2[t]$ et $\mathbb{F}_7[t]$.

Solution.

(a) On mène la division euclidienne de $f(x)$ par $x - a_1$ pour obtenir un $f_1(x) \in A[x]$ tel que

$$f(x) = (x - a_1)f_1(x) + a$$

pour $a \in A$. En évaluant en a_1, on obtient que $a = 0$. *Maintenant, on utilise de manière cruciale que A est intègre* pour voir que pour $i \geq 2$ on a $f_1(a_i) = 0$. En effet en évaluant en a_i on a

$$0 = (a_i - a_1)f_1(a_i),$$

et donc comme $a_1 \neq a_i$ et que A est intègre, on voit que $f_1(a_i) = 0$. Ainsi, on peut continuer par récurence sur $2 \leq i \leq p + 1$ obtenir par le même procédé que

$$f(x) = (x - a_1) \cdots (x - a_n)g(x)$$

pour un $g(x) \in A[x]$.

(b) Par le théorème des restes chinois

$$\mathbb{Z}/pq\mathbb{Z} = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Ainsi $(1, 0)$, $(0, 1)$, $(0, 0)$ et $(1, 1)$ sont des racines. Comme les polynômes en jeu sont moniques, on peut voir avec le degré que le produit des $(t - a_i)$ ne peut diviser $t^2 - t$.

(c) As $f|g$ in $\mathbb{Q}[t]$, there exists $h \in \mathbb{Q}[t]$ such that $g(t) = f(t)h(t)$. Now, as $h \in \mathbb{Q}[t|$, we can write $h(t) = c \cdot h_1(t)$, where $h_1(t) \in \mathbb{Z}[t]$ is primitive and $c \in \mathbb{Q}$. Then:

$$g(t) = c \cdot f(t)h_1(t).$$

By Lemma 3.8.9, we have that $f(t)h_1(t)$ is primitive and, since $g(t)$ is also primitive, we use Lemma 3.8.11 to determine that $c \in \mathbb{Z}^\times$, i.e. $c = \pm 1$. Then

$$g(t) = \pm f(t)h_1(t) \text{ in } \mathbb{Z}[t], \text{ therefore } f|g \text{ in } \mathbb{Z}[t].$$

(d) The roots of x^4+1 over $\mathbb{C}$ are $e^{i(\frac{\pi}{4}+\frac{k\pi}{2})}$, where $0 \leq k \leq 3$, and we have:

$$x^4+1 = \prod_{k=0}^{3}(x - e^{i(\frac{\pi}{4}+\frac{k\pi}{2})}).$$

We group the conjugate complex roots and obtain the decomposition over $\mathbb{R}[x]$

$$x^4+1 = (x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1).$$

By Example 3.9.2 (4), it follows x^4+1 does not admit roots in $\mathbb{Q}$, as it does not admit roots in $\mathbb{R}$. If $x^4+1 = f(x)g(x)$, where $f(x), g(x) \in \mathbb{Q}[x]$ are polynomials of degree 2, then $f(x) = (x-a_1)(x-a_2)$ and $g(x) = (x-a_3)(x-a_4)$, where $a_1, a_2, a_3, a_4 \in \{e^{i(\frac{\pi}{4}+\frac{k\pi}{2})} | \, 0 \leq k \leq 3\}$ are distinct. One checks that for every choice of a_i a_j the polynomial $(x-a_i)(x-a_j)$ does not have coefficients in $\mathbb{Q}$. We conclude that x^4+1 is irreducible in $\mathbb{Q}[x]$. Lastly, we note that, as it is primitive., by Lemma 3.8.13, it is also irreducible in $\mathbb{Z}[x]$.

In $\mathbb{F}_2[x]$ we have $x^4+[1]_2 = (x+[1]_2)^4$.

The squares in $\mathbb{F}_7$ are $[0]_7, [1]_7, [2]_7, [4]_7$ and $[9]_7$ and we deduce that $x^4+[1]_7$ does not admit roots in $\mathbb{F}_7$. But it can still be possible that $x^4+[1]_7$ admits a decomposition into a product of two polynomials of degree 2. It is the case: indeed, as

$$([3]_7)^2 = [2]_7$$

we see from the above decomposition that

$$x^4+1 = (x^2+[3]_7x+1)((x^2-[3]_7x+1)).$$

Since $x^8-1 = (x^4+1)(x^4-1)$ it suffices to factor x^4-1:

- in $\mathbb{C}[x]$ we have: $x^4-1 = (x+i)(x-i)(x+1)(x-1)$.
- in $\mathbb{R}[x]$, $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$ we have: $x^4-1 = (x^2+1)(x+1)(x-1)$.
- in $\mathbb{F}_2[x]$ we have: $x^4-[1]_2 = x^4+[1]_2 = (x+[1]_2)^4$.
- in $\mathbb{F}_7[x]$ we have: $x^4-[1]_7 = (x^2+[1]_7)(x-[1]_7)(x+[1]_7)$, where we have seen earlier that $x^2+[1]_7$ is irreducible.

Exercice 2 (Polynômes irréductibles I). (a) Montrer que $\frac{2}{9}x^5+\frac{5}{3}x^4+x^3+\frac{1}{3}$ est un polynôme irréductible de $\mathbb{Q}[x]$.

(b) Montrer que $x^4+[2]_5$ est un polynôme irréductible de $\mathbb{F}_5[x]$ et conclure que x^4+15x^3+7 est un polynôme irréductible de $\mathbb{Q}[x]$.

(c) Montrer que x^2+y^2+1 est un polynôme irréductible de $\mathbb{R}[x,y]$.

(d) Montrer que $x^2+y^2+[1]_2$ n'est pas un polynôme irréductible de $\mathbb{F}_2[x,y]$.

(e) Montrer que $y^4+x^3+x^2y^2+xy+2x^2-x+1$ est un polynôme irréductible de $\mathbb{Q}[x,y]$.

(f) Montrer que $4x^3+120x^2+8x-12$ est un polynôme irréductible de $\mathbb{Q}[x]$.

(g) Montrer que t^6+t^3+1 est un polynôme irréductible de $\mathbb{Q}[t]$.

(h) Montrer que $y^4+xy^3+xy^2+x^2y+3x^2-2x$ est un polynôme irréductible de $\mathbb{Q}[x,y]$.

Solution.

(a) We write $\frac{2}{9}x^5 + \frac{5}{3}x^4 + x^3 + \frac{1}{3} = \frac{1}{9}(2x^5 + 15x^4 + 9x^3 + 3) \in \mathbb{Q}[x]$.

Now $\frac{1}{9} \in \mathbb{Q}[x]^\times$, as $\frac{1}{9} \in \mathbb{Q}^\times$. Therefore $\frac{2}{9}x^5 + \frac{5}{3}x^4 + x^3 + \frac{1}{3}$ is irreducible in $\mathbb{Q}[x]$ if and only if $2x^5 + 15x^4 + 9x^3 + 3$ is. As $\gcd(2, 15, 9, 3) = 1$, we have that $2x^5 + 15x^4 + 9x^3 + 3$ is primitive, hence it is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$ (Lemma 3.8.13). Using Eisenstein for $p = 3$, where $3 \in \mathbb{Z}$ is irreducible, we deduce that $2x^5 + 15x^4 + 9x^3 + 3$ is irreducible in $\mathbb{Z}[x]$.

(b) Let $f(x) = x^4 + [2]_5 \in \mathbb{F}_5[x]$. Note that for all $a \in \mathbb{F}_5$ we have $a^2 \in \{[0]_5, [1]_5, [4]_5\}$. Therefore f does not admit roots in $\mathbb{F}_5$. We will now show that f is not a product of two polynomials of degree 2. As $\mathbb{F}_5$ is a field, we can assume that these polynomials are unitary and so assume there exist $a, b, c, d \in \mathbb{F}_5$ such that

$$f(x) = x^4 + [2]_5 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (bc + ad)x + bd.$$

Then $c = -a$ and $d = [2]_5 b^{-1}$ and substituting in the above gives:

$$x^4 + [2]_5 = x^4 + (b - a^2 + [2]_5 \cdot b^{-1})x^2 + (-ab + [2]_5 \cdot ab^{-1})x + [2]_5.$$

Thus $-ab + [2]_5 \cdot ab^{-1} = a(-b + [2]_5 \cdot b^{-1}) = 0$ and

- if $a = 0$, then $b^2 = -[2]_5$, a contradiction.
- if $-b + [2]_5 b^{-1} = 0$, then $b^2 = [2]_5$, a contradiction.

We conclude that f is irreducible in $\mathbb{F}_5[x]$.

Lastly, let $x^4 + 15x^3 + 7 \in \mathbb{Q}[x]$. As the dominant coefficient is 1, this polynomial is primitive, hence it is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$ (Lemma 3.8.13). Let $\phi_5 : \mathbb{Z} \to \mathbb{F}_5$ be the quotient homomorphism and let $\pi_5 : \mathbb{Z}[x] \to \mathbb{F}_5[x]$ be its induced homomorphism. We have that:

$$\pi_5(x^4 + 15x^3 + 7) = x^4 + [2]_5$$

and, as $x^4 + [2]_5$ is irreducible in $\mathbb{F}_5[x]$, we use Proposition 3.9.1 to conclude that $x^4 + 15x^3 + 7$ is irreducible in $\mathbb{Z}[x]$.

(c) First we note that $x^2 + y^2 + 1 \in \mathbb{R}[x, y]$ is primitive as its dominant coefficient is 1. Secondly, $y^2 + 1 \in \mathbb{R}[y]$ is irreducible. We now apply Eisenstein with $p = y^2 + 1$ to conclude that $x^2 + y^2 + 1$ is irreducible in $\mathbb{R}[x, y]$.

(d) We have $x^2 + y^2 + [1]_2 = (x + y + [1]_2)^2$ in $\mathbb{F}_2[x, y]$.

(e) The evaluation homomorphism $\mathrm{ev}_0 : \mathbb{Q}[y] \to \mathbb{Q}$, $\mathrm{ev}_0(y) = 0$, induces the homomorphism $\xi : \mathbb{Q}[y][x] \to \mathbb{Q}[x]$ with $\xi(y) = 0$ and $\xi(x) = x$. We have that:

$$\xi(y^4 + x^3 + x^2y^2 + xy + 2x^2 - x + 1) = x^3 + 2x^2 - x + 1$$

and, by Proposition 3.9.1, $y^4 + x^3 + x^2y^2 + xy + 2x^2 - x + 1$ is irreducible in $\mathbb{Q}[x, y]$ if $x^3 + 2x^2 - x + 1$ is irreducible in $\mathbb{Q}[x]$. Now $\deg(x^3 + 2x^2 - x + 1) = 3$ and thus $x^3 + 2x^2 - x + 1$ is irreducible in $\mathbb{Q}[x]$ if and only if it does not admit roots in $\mathbb{Q}$. Assume $\frac{p}{r} \in \mathbb{Q}$, where $p, r \in \mathbb{Z}$ and $\gcd(p, r) = 1$, is a root of $x^3 + 2x^2 - x + 1$. Then

$$\left(\frac{p}{r}\right)^3 + 2\left(\frac{p}{r}\right)^2 - \left(\frac{p}{r}\right) + 1 = 0.$$

As $\gcd(p, r) = 1$, it follows that $p|1$, $r|1$ and so $\frac{p}{r} \in \{-1, 1\}$. One checks that neither -1, nor 1 is a root of $x^3 + 2x^2 - x + 1$ and thus $x^3 + 2x^2 - x + 1$ is irreducible in $\mathbb{Q}[x]$.

(f) We have $4x^3 + 120x^2 + 8x - 12 = 4(x^3 + 30x^2 + 2x - 3) \in \mathbb{Q}[x]$. Now $4 \in \mathbb{Q}[x]^\times$ and so $4x^3 + 120x^2 + 8x - 12$ is irreducible in $\mathbb{Q}[x]$ if and only if $x^3 + 30x^2 + 2x - 3$ is. As $\deg(x^3+30x^2+2x-3) = 3$ it follows that x^3+30x^2+2x-3 is irreducible in $\mathbb{Q}[x]$ if and only if it does not admit roots in $\mathbb{Q}$. Assume there exist $\frac{p}{r} \in \mathbb{Q}$, where $p, r \in \mathbb{Z}$ and $\gcd(p, r) = 1$, such that:

$$\left(\frac{p}{r}\right)^3 + 30\left(\frac{p}{r}\right)^2 + 2\left(\frac{p}{r}\right) - 3 = 0.$$

As $\gcd(p, r) = 1$, it follows that $p|3$ and $r|1$. Therefore $\frac{p}{r} \in \{-3, -1, 1, 3\}$. One checks that none of the elements in $\{-3, -1, 1, 3\}$ is a root of $x^3 + 30x^2 + 2x - 3$. We conclude that $x^3 + 30x^2 + 2x - 3$ is irreducible in $\mathbb{Q}[x]$. .

(g) As the polynomial t^6+t^3+1 is primitive, it follows that it is irreducible in $\mathbb{Q}[t]$ if and only if it is irreducible in $\mathbb{Z}[x]$ (Lemma 3.8.13). We consider the quotient homomorphism $\phi_2 : \mathbb{Z} \to \mathbb{F}_2$ and its induced homomorphism $\pi_2 : \mathbb{Z}[t] \to \mathbb{F}_2[t]$ under which

$$\pi_2(t^6 + t^3 + 1) = t^6 + t^3 + [1]_2.$$

By Proposition 3.9.1, $t^6 + t^3 + 1$ is irreducible in $\mathbb{Z}[t]$ if $t^6 + t^3 + [1]_2$ is irreducible in $\mathbb{F}_2[t]$.

Now, one checks that $t^6+t^3+[1]_2$ does not admit roots in $\mathbb{F}_2[t]$. Secondly, the only irreducible polynomial of degree 2 in $\mathbb{F}_2[t]$ is $t^2 + t + [1]_2$ and one checks that this does not divide $t^6 + t^3 + [1]_2$. Lastly, we assume that $t^6 + t^3 + [1]_2$ is a product of two polynomials of degree 3. As $\mathbb{F}_2$ is a field, we can assume that these polynomials are unitary and we have:

$$\begin{aligned} t^6 + t^3 + [1]_2 &= (t^3 + a_2t^2 + a_1t + a_0)(t^3 + b_2t^2 + b_1t + b_0) \\ &= t^6 + (a_2 + b_2)t^5 + (a_1 + a_2b_2 + b_1)t^4 + (a_0 + a_1b_2 + a_2b_1 + b_0)t^3 + \\ &\quad + (a_0b_2 + a_1b_1 + a_2b_0)t^2 + (a_0b_1 + a_1b_0)t + a_0b_0. \end{aligned}$$

Then $a_0 = b_0 = [1]_2$, $a_2 = b_2$ and

$$\begin{cases} a_0b_1 + a_1b_0 = [0]_2 \\ a_0b_2 + a_1b_1 + a_2b_0 = [0]_2 \\ a_0 + a_1b_2 + a_2b_1 + b_0 = [1]_2 \\ a_1 + a_2b_2 + b_1 = [0]_2 \end{cases} \to \begin{cases} b_1 + a_1 = [0]_2 \\ a_1b_1 = [0]_2 \\ b_2(a_1 + b_1) = [1]_2 \\ a_2b_2 = [0]_2 \end{cases} \to [1]_2 = [0]_2.$$

We conclude that $t^6 + t^3 + [1]_2$ is irreducible in $\mathbb{F}_2[t]$.

(h) We first note that the ring $\mathbb{Q}[x]$ is factorial, as $\mathbb{Q}$ is (Theorem 3.8.1), and that $x \in \mathbb{Q}[x]$ is irreducible. Secondly the polynomial $y^4 + xy^3 + xy^2 + x^2y + 3x^2 - 2x \in \mathbb{Q}[x, y]$ is primitive, as its dominant coefficient is 1. We now apply Eisenstein with $p = x$ to conclude that $y^4 + xy^3 + xy^2 + x^2y + 3x^2 - 2x$ is irreducible in $\mathbb{Q}[x, y]$.

Exercice 3 (Polynômes irréductibles II).
Soit $f(t) = t^4 + 4t^3 + 3t^2 + 7t - 4$ dans $\mathbb{Z}[t]$.

(a) Montrer que $\pi_2(f)$, la réduction modulo 2, n'est pas irréductible.

(b) Montrer que $\pi_3(f)$, la réduction modulo 3, n'est pas irréductible.

(c) Utiliser les décompositions des parties précédentes pour conclure néanmoins que f est irréductible.

Solution.
Let $f(t) = t^4 + 4t^3 + 3t^2 + 7t - 4 \in \mathbb{Z}[t]$.

(a) We have $\pi_2(f(t)) = t^4+t^2+t = t(t^3+t+[1]_2) \in \mathbb{F}_2[t]$. Moreover, we remark that $t^3+t+[1]_2$ is irreducible in $\mathbb{F}_2[t]$, as it does not admit roots in $\mathbb{F}_2$.

(b) We have $\pi_3(f(t)) = t^4 + t^3 + t - [1]_3 = (t^2 + [1]_3)(t^2 + t - [1]_3) \in \mathbb{F}_3[t]$.

(c) Assume that $f(t)$ is reducible in $\mathbb{Z}[t]$. Then either $f(t) = (t-a)g(t)$, where $a \in \mathbb{Z}$ and $g(t) \in \mathbb{Z}[t]$ is a polynomial of degree 3, or $f(t) = f_1(t)f_2(t)$, where $f_1(t), f_2(t) \in \mathbb{Z}[t]$ are two polynomials of degree 2.

In the first case, $a|4$ but none of the elements of $\{\pm 1, \pm 2, \pm 4\}$ are roots of f. Hence, we only need to consider the case when $f(t) = f_1(t)f_2(t)$, where $\deg(f_1(t)) = \deg(f_2(t)) = 2$, and we have:

$$\pi_2(f(t)) = \pi_2(f_1(t)f_2(t)) = \pi_2(f_1(t))\pi_2(f_2(t).$$

Now, as $\deg(\pi_2(f(t))) = 4$ and as $\deg(\pi_2(f_1(t))) = \deg(\pi_2(f_2(t))) \leq 2$, it follows that $\deg(\pi_2(f_1(t))) = 2$ and $\deg(\pi_2(f_2(t))) = 2$.

On the other hand, we have $\pi_2(f(t)) = t^4 + t^2 + t = t(t^3 + t + [1]_2)$, where $t^3 + t + [1]_2 \in \mathbb{F}_2[t]$ is irreducible. We have arrived at a contradiction. We conclude that $f(t) \in \mathbb{Z}[t]$ is irreducible.

Exercice 4.
Soit K un corps et L une extension quadratique, i.e. $[L : K] = 2$.

1. Montrez que toute extension de K de degré 1 est égale à K.
2. Montrez qu'il existe un élément $\alpha \in L$ tel que $L = K(\alpha)$.
3. Soit K de caractéristique différente de 2. Montrez qu'il existe un élément $\delta \in L$ avec $\delta^2 = d \in K$ tel que $L = K(\delta) = K(\sqrt{d})$.
4. Soit M une extension de K et $\delta \in M \setminus K$ un élément avec $\delta^2 \in K$. Montrez que $K(\delta)$ est une extension quadratique de K.

Solution.

1. Let L' denote the field extension of K of degree 1. This means that L' is a field that contains K, and that has a K- vector space structure such that the dimension of L' as a K-vector space is 1.The K-subspace of L' generated by 1 is equal to K, and equal to L' as well, due to the dimension of L' over K being 1. Hence K and L' coincide.

2. We take any $\alpha \in L \setminus K$. Then we have the following field extensions, $K \subseteq K(\alpha) \subseteq L$. From this, it follows using Proposition 4.2.15 that

$$\underbrace{[L : K]}_{=2} = [L : K(\alpha)] \cdot [K(\alpha) : K].$$

Since we take $\alpha \notin K$, it holds that $K \neq K(\alpha)$, and hence by the first point, $[K(\alpha) : K] \neq 1$. From this, it follows using the equation above that $[K(\alpha) : K] = 2$. But that means that $[L : K(\alpha)] = 1$, from which it follows by the first point that $L = K(\alpha)$.

3. Since $L = K(\alpha)$, and $[L : K] = 2$, it holds that $\{1, \alpha\}$ forms a K-linear basis of $K(\alpha)$. This means in particular that α^2 is a K-linear combination of 1 and α. There exists $a, b \in K$ such that $\alpha^2 = b \cdot 1 + a \cdot \alpha \Leftrightarrow \alpha^2 - a\alpha - b = 0$. We define d to be $d = a^2 + 4b$, the discriminant of the quadratic equation. We now show that d is a square in $K(\alpha)$. We do so by multiplying the quadratic equation by 4 (note that the characteristic of K is not equal to 2), and completing the square, to find:

$$4\alpha^2 - 4a\alpha - 4b = 0 \Leftrightarrow (2\alpha - a)^2 - a^2 - 4b = 0 \Leftrightarrow (2\alpha - a)^2 = a^2 + 4b = d.$$

Hence d is a square in $K(\alpha)$, and we let $\delta = 2\alpha - a \in K(\alpha) \setminus K$, with $\delta^2 = d$. By the second part of this exercise, it holds that $L = K(\delta) = K(\sqrt{d})$.

Let us give an alternative proof that illuminates the role of the discriminant. Since the characteristic of K is different from 2, the well-known theory of quadratic equations with coefficients in $\mathbb{C}$ can be carried over verbatim to K to obtain the following: if $p(x) = ax^2 + bx + c \in K[x]$ is a degree 2 polynomial, then the roots ξ_1, ξ_2 of $p(x)$ in any extension F of K can be written

$$\xi_1 = \frac{-2b + \sqrt{\Delta(p)}}{2a}, \quad \xi_2 = \frac{-2b - \sqrt{\Delta(p)}}{2a}$$

where $\Delta(p) = b^2 - 4ac$ and $\sqrt{\Delta(p)} \in F$ denotes a square root of $\Delta(p)$. Now observe that:

(a) $K(\xi_i) = K(\xi_1, \xi_2)$ for any $i = 1, 2$. We can write in $K(\xi_1)[x]$ that

$$p(x) = (x - \xi_1)q(x)$$

where necessarily $\deg q(x) = 1$. Thus $q(x) = x - \xi_2$, and so $\xi_2 \in K(\xi_1)$. Hence $K(\xi_1) = K(\xi_1, \xi_2)$, and by exchanging the roles of ξ_1 and ξ_2 we also obtain $K(\xi_2) = K(\xi_1, \xi_2)$.

(b) $K(\xi_1, \xi_2) = K\left(\sqrt{\Delta(p)}\right)$. Indeed $\sqrt{\Delta(p)} = 2a(\xi_1 - \xi_2)$ so the inclusion $\supseteq$ holds. Also it follows from the formulae for ξ_1 and ξ_2 that $\subseteq$ holds.

So we obtain that $K(\xi_1) = K(\xi_2) = K(\xi_1, \xi_2) = K\left(\sqrt{\Delta(p)}\right)$ as subfields of F. Taking $F = L$ and $p(x) = m_{\alpha,K}$, we obtain an alternative proof of the exercise.

4. From the definition of δ, it immediately follows that $\{1, \delta\}$ forms a K-linear basis of $K(\delta)$ as a K-vector space. By definition, $[K(\delta) : K]$ is the dimension of $K(\delta)$ as a K-vector space, which is 2.

Exercice 5.
Soient $a, b \in \mathbb{Z}$.

1. Quand est-ce que les corps $\mathbb{Q}(\sqrt{a})$ et $\mathbb{Q}(\sqrt{b})$ sont isomorphes en tant que $\mathbb{Q}$-espaces vectoriels?
2. Quand est-ce que les corps $\mathbb{Q}(\sqrt{a})$ et $\mathbb{Q}(\sqrt{b})$ sont isomorphes en tant que corps?

Solution.

1. There are two options for $\mathbb{Q}(\sqrt{a})$. If a is a square in $\mathbb{Q}$, then it holds that $\sqrt{a}$ is contained in $\mathbb{Q}$, and hence $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}$, and so $[\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 1$. If a is no square, then $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{a})$, and the degree of this field extension is equal to 2, since the polynomial $x^2 - a$ is zero for $\sqrt{a}$, and the polynomial is irreducible (since a is no square). The same holds for $\mathbb{Q}(\sqrt{b})$. We now use the fact (seen in Linear Algebra) that any two vector spaces over the same field are isomorphic if and only if they are of the same dimension. In our case, both $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$ can be of dimension 1 or 2 over $\mathbb{Q}$, depending on whether or not a resp. b is a square. We conclude that $\mathbb{Q}(\sqrt{a})$ is of the same dimension over $\mathbb{Q}$ as $\mathbb{Q}(\sqrt{b})$, and hence isomorphic, if and only if both a and b are simultaneously squares in $\mathbb{Q}$, or both are simultaneously not squares.

2. We now assume that $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$ are isomorphic as fields. We claim that this holds if and only if they are equal as subfields of $\mathbb{C}$. This means that there exists $c \in \mathbb{Q}$ such that $\sqrt{a} = c\sqrt{b}$.

   First, we assume that $\sqrt{a} = c\sqrt{b}$. Then, $\sqrt{a}$ and $\sqrt{b}$ generate the same field extension of $\mathbb{Q}$, and hence clearly the two fields are isomorphic.

   Secondly, assume that the fields $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$ are isomorphic. Denote the isomorphism $\varphi : \mathbb{Q}(\sqrt{a}) \to \mathbb{Q}(\sqrt{b})$. We note that from $\varphi(1) = 1$, it follows that φ acts as the identity on $\mathbb{Z}$, and furthermore on $\mathbb{Q}$. On one hand, we have that $\varphi(\sqrt{a}) = u + \sqrt{b}v$ for some $u, v \in \mathbb{Q}$. On the other hand, with $a \in \mathbb{Q}$, it holds that

$$a = \varphi(a) = \varphi(\sqrt{a}^2) = \varphi(\sqrt{a})^2 = (u + \sqrt{b}v)^2 = (u^2 + bv^2) + \sqrt{b}(2uv).$$

   We now distinguish between two cases.

- If $\sqrt{b} \in \mathbb{Q}$, then $\varphi(\sqrt{a}) \in \mathbb{Q}$, and hence $\sqrt{a} \in \mathbb{Q}$. (If $\sqrt{a}$ was not contained in $\mathbb{Q}$, then φ would be an isomorphism from $\mathbb{Q}(\sqrt{a}) \neq \mathbb{Q}$ to $\mathbb{Q}$. This is a contradiction to φ being injective.) Then,
$$\sqrt{a} = \frac{\sqrt{a}}{\sqrt{b}} \cdot \sqrt{b},$$
and $\sqrt{a} = c\sqrt{b}$ with $c := \frac{\sqrt{a}}{\sqrt{b}} \in \mathbb{Q}$.
- If $\sqrt{b} \notin \mathbb{Q}$, then
$$a = (u^2 + bv^2) + \sqrt{b}(2uv),$$
with $\sqrt{b} \notin \mathbb{Q}$. Since $a \in \mathbb{Q}$, it follows that $2uv = 0$, and hence either $u = 0$ or $v = 0$. If $u = 0$, then $a = bv^2 \Rightarrow \sqrt{a} = \sqrt{b}v$, and hence the property is satisfied. If $v = 0$, then $\varphi(\sqrt{a}) = u \in \mathbb{Q}$. It then follows that the image of φ is contained in $\mathbb{Q}$, which means that φ can not be an isomorphism. Hence this case does not occur.

Exercice 6. 1. Soit L une extension de K avec $[L : K]$ impair. Montrer que $K(\alpha) = K(\alpha^2)$ pour tout $\alpha \in L \setminus K$.

2. Soient $p, q \in \mathbb{Z}$ deux nombres premiers distincts. Montrez que $\sqrt{p} \notin \mathbb{Q}(\sqrt{q})$ et $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$. Calculez $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}]$.

3. Soit L une extension de K et soient $\alpha, \beta \in L$ des éléments tels que $[K(\alpha) : K] = m$ et $[K(\beta) : K] = n$ sont premiers entre eux. Montrer que $[K(\alpha, \beta) : K] = mn$.

Solution.

1. We have the following field extensions,
$$K \subset K(\alpha^2) \subset K(\alpha) \subset L.$$
By proposition 4.2.15, it follows that
$$[L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K(\alpha^2)] \cdot [K(\alpha^2) : K].$$
Since the degree of the field extension L over K is odd, it follows that the degrees on the right hand side of the equality above are odd as well. We now look at the extension $K(\alpha)$ over $K(\alpha^2)$. The degree of this extension is at most 2, since the polynomial $x^2 - \alpha^2 \in K(\alpha^2)[x]$ vanishes at α. But since the degree needs to be odd, it follows that it is 1. Hence $K(\alpha) = K(\alpha^2)$.

2. We first show that $\sqrt{p} \notin \mathbb{Q}(\sqrt{q})$. If $\sqrt{p}$ is contained in $\mathbb{Q}(\sqrt{q})$, then there are $r, s \in \mathbb{Q}$ such that $\sqrt{p} = r + s\sqrt{q}$. From this, it follows that
$$p = (r + s\sqrt{q})^2 = (r^2 + s^2 q) + (2rs)\sqrt{q}.$$
Using the fact that $p \in \mathbb{Q}$, we compare the right hand side and left hand side, and note that $2rs = 0$. If $r = 0$, then $p = s^2 q$ which is a contradiction with p, q prime and distinct.

If $s = 0$, then $\sqrt{p} = r \Rightarrow p = r^2$, which is a contradiction to p prime.

It follows that $\sqrt{p} \notin \mathbb{Q}(\sqrt{q})$. The same argument, with the roles of p and q reversed shows that $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$.

We now compute the degree of the field extension $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ over $\mathbb{Q}$. We have the following extensions of fields,
$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\sqrt{p}, \sqrt{q}).$$
From proposition 4.2.15 it follows that
$$[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})] \cdot [\mathbb{Q}(\sqrt{p}) : \mathbb{Q}].$$

We calculate both degrees on the right hand side separately. Firstly, $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$. This holds because $\sqrt{p} \notin \mathbb{Q}$. The polynomial $x^2 - p \in \mathbb{Q}[x]$ vanishes at $\sqrt{p}$, and combining Gauss III with Eisenstein for the prime p, it follows that the polynomial is irreducible over $\mathbb{Q}$. Hence it is the minimal polynomial, and the degree is 2.

Secondly, $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})] = 2$. This holds because $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$. Therefore, the degree of the extension is not equal to 1. Furthermore, the degree of the extension is at most 2, since $\sqrt{q}^2 = q \in \mathbb{Q}$, and hence $\sqrt{q}^2 \in \mathbb{Q}(\sqrt{p})$. Combining these restrictions, the degree of the extension is equal to 2, and hence the product of the two extensions is 4, meaning that $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = 4$.

3. We have the following extension of fields, $K \subset K(\alpha) \subset K(\alpha, \beta)$. Using proposition 4.2.15, it follows that

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)] \cdot [K(\alpha) : K].$$

From this, it follows that $m = [K(\alpha) : K]$ divides $[K(\alpha, \beta) : K]$. The same argument for the extension of fields $K \subset K(\beta) \subset K(\alpha, \beta)$ shows that n divides $[K(\alpha, \beta) : K]$. Using the fact that m and n are coprime, it follows that mn divides $[K(\alpha, \beta) : K]$. This means that the degree of the field extension is a multiple of mn. We show that it is equal to mn by considering the first field extension again, $K \subset K(\alpha) \subset K(\alpha, \beta)$. Since $[K(\beta) : K] = n$, it holds in particular that the degree of the field extension $K(\alpha, \beta)$ over $K(\alpha)$ is at most n. Hence $[K(\alpha, \beta) : K]$ is at most nm. On the other hand, as we have seen above, it is at least mn, from which we conclude that it is exactly mn.

The two field extensions are illustrated below.