Exercice 5. 1. $\dim_F(F[x]/(x^6+x^4, x^2+x))$. It holds that

$$\begin{aligned} F[x]/(x^2+x, x^6+x^4) &\cong F[x]/(x^2+x, (x^2)^3+(x^2)^2) \cong F[x]/(x^2+x, (-x)^3+(-x)^2) \\ &\cong F[x]/(x^2+x, -x\cdot x^2+x^2) \cong F[x]/(x^2+x, -x\cdot(-x)+(-x)) \\ &\cong F[x]/(x^2+x, x^2-x) \cong F[x]/(x^2+x, -x-x) \cong F[x]/(x^2+x, -2x). \end{aligned}$$

Now if $\mathrm{char}(F)=2$, then $F[x]/(x^2+x, x^6+x^4) \cong F[x]/(x^2+x)$, and according to Proposition 3.1.9, the dimension $\dim_F(F[x]/(x^6+x^4, x^2+x)) = 2$.
If $\mathrm{char}(F)\neq 2$, then $F[x]/(x^6+x^4, x^2+x) \cong F[x]/(x^2+x, x) \cong F[x]/(x)$, and according to Proposition 3.1.9, the dimension $\dim_F(F[x]/(x^6+x^4, x^2+x)) = 1$.

2. $\dim_F(F[x,y]/(x^2, y^3)) = 6$, since $\{1, x, y, y^2, xy, xy^2\}$ forms a basis.

Exercice 6. 1. We show that $\phi^e(I)$ is a left-ideal in C. According to Lemma 1.4.2, it suffices to show that

— $\forall x, y \in \phi^e(I), x+y \in \phi^e(I)$
— $\forall x \in \phi^e(I), c \in C, c\cdot x \in \phi^e(I)$.

This holds.

— Let $x = \sum_{i=1}^n c_i\cdot\phi(b_i), y = \sum_{j=1}^m d_j\cdot\phi(a_j)$, where $c_i, d_j \in C, b_i, a_j \in I$. Then,

$$x+y = \sum_{i=1}^n c_i\cdot\phi(b_i) + \sum_{j=1}^m d_j\cdot\phi(a_j) = \sum_{i=1}^{n+m} c_i\cdot\phi(b_i),$$

where we define $c_i = d_{i-n}$ and $b_i = a_{i-n}$ for all $i \in \{n+1, \dots, n+m\}$. Hence $x+y$ is of the correct form, and contained in $\phi^e(I)$.

— Let x as above, and $c \in C$. Then, using the fact that the multiplication in a ring is distributive, it holds that

$$c\cdot x = c\cdot\left(\sum_{i=1}^n c_i\cdot\phi(b_i)\right) = \sum_{i=1}^n c\cdot c_i\cdot\phi(b_i)$$

is contained in $\phi^e(I)$, since $c\cdot c_i \in C \forall i$.

2. We first remark that ι acts as the identity on the elements of $\mathbb{Z}$, sending $z \in \mathbb{Z}$ to $\iota(z) = \frac{z}{p^0} = z \in A$. Secondly, for any ideal $I \in A$, by definition $\iota^{-1}(I)$ contains all elements $z \in \mathbb{Z}$ for which there exists an element $a \in A$ such that $\iota(z) = a$. But as ι acts as the identity on z, this is equivalent to $\iota(z) = z = a$, form which it follows that $\iota^{-1}(I)$ contains all elements of I that are simultaneously contained in $\mathbb{Z}$.
Now let J be an ideal in A. To show that $\iota^e(\iota^{-1}(J)) = J$, we show that both inclusions hold. First, let $j \in J$. We want to show that $j \in \iota^e(\iota^{-1}(J))$. By definition, j is of the form $j = \frac{a}{p^n}$ for some $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. Since J is an ideal and since $p^n \in A$, it holds that the product $p^n\cdot j = p^n\cdot\frac{a}{p^n} = a$ is contained in J as well. By the remark, it follows that $a \in \iota^{-1}(J)$, and hence $j = \frac{1}{p^n}\cdot a$ is contained in $\iota^e(\iota^{-1}(J))$, since $\frac{1}{p^n} \in A$. From this, it follows that $J \subseteq \iota^e(\iota^{-1}(J))$.
Now, let $x \in \iota^e(\iota^{-1}(J))$. We want to show that $x \in J$. We let $x = \sum_{i=1}^n a_i\cdot\iota(b_i)$ for some $a_i \in A$ and $b_i \in \iota^{-1}(J)$. If we show that $\iota(b_i) \in J$, then we are done, since then, $a_i\cdot\iota(b_i) \in J$, and the sum is contained in J as well. We now show that $\iota(b_i) \in J$. Since by assumption, $b_i \in \iota^{-1}(J)$, it follows form the remark that $b_i \in J$, and hence $\iota(b_i) = b_i \in J$. With this, $\iota^e(\iota^{-1}(J)) \subseteq J$ holds.

3. We denote the prime element by q, and its ideal by (q). We have

$$\begin{aligned}\iota^e(q) &= \left\{ \sum_{i=1}^{n} \frac{a_i}{p^n} \cdot \iota(b_i) \middle| a_i \in \mathbb{Z}, n \in \mathbb{N}, b_i \in (q) \right\} \\ &= \left\{ \sum_{i=1}^{n} \frac{a_i}{p^n} \cdot \iota(m_i \cdot q) \middle| a_i \in \mathbb{Z}, n \in \mathbb{N}, m_i \in \mathbb{Z} \right\} \\ &= \left\{ \sum_{i=1}^{n} \frac{a_i}{p^n} \cdot m_i \cdot q \middle| a_i \in \mathbb{Z}, n \in \mathbb{N}, m_i \in \mathbb{Z} \right\} \\ &= \left\{ \sum_{i=1}^{n} \frac{z_i}{p^n} \cdot q \middle| z_i \in \mathbb{Z}, n \in \mathbb{N} \right\}\end{aligned}$$

Now if $p = q$, and hence $p \in (q)$, then $1 \in \iota^e(q)$, since $1 = \frac{1}{p} \cdot q$. By the remark at the beginning of the second exercise, it follows that $1 \in \iota^{-1}(\iota^e(q))$, and hence $\iota^{-1}(\iota^e(q)) = \mathbb{Z}$.
If $p \notin (q)$, then again by the same remark, $\iota^{-1}(\iota^e(q))$ contains all elements of $\iota^e(q)$ that are contained in $\mathbb{Z}$. By the description of $\iota^e(q)$ those are precisely the elements $z_i \cdot q$, with $z_i \in \mathbb{Z}$, which is precisely (q).

Exercice 7.
Soient K un corps, $f \in \mathbb{K}[x]$ un polynôme de degré n, et L son corps de décomposition. On suppose que $G := \mathrm{Gal}(L/K) \cong S_n$.

1. Montrons que L est Galois sur K. En premier lieu, soient $\gamma_1, \ldots, \gamma_{n'} \in L$ les racines distinctes de f, avec $n' \leq n$. On a $L = K(\gamma_1, \ldots, \gamma_{n'})$. Si $\sigma \in G$, alors chaque $\sigma(\gamma_i)$ est une racine de f. Donc γ induit une permutation des racines de f. Ceci induit une fonction

$$\begin{aligned}\Phi \colon G &\to \mathrm{Bij}(\gamma_1, \ldots, \gamma_{n'}) \\ \sigma &\mapsto \sigma|_{\{\gamma_1, \ldots, \gamma_{n'}\}}\end{aligned}$$

qui est en fait un morphisme de groupes (nous n'aurons pas besoin de cette structure additionnelle). Par la Proposition 3.6.3.b, on obtient que Φ est une fonction injective. En particulier

$$n! = |S_n| = |G| = |\Phi(G)| \leq |\mathrm{Bij}(\gamma_1, \ldots, \gamma_{n'})| = (n')!$$

et puisque $n' \leq n$, on en déduit que $n' = n$ et que Φ est bijective.
Puisque $n' = n$, on voit que f n'a pas de racines répétées. Donc f est séparable sur K, et par le Théorème 3.6.15 on obtient que L est Galois sur K.

2. Supposons que f est réductible dans $K[x]$, avec $f = gh$ où $\deg g = r > 0, \deg h = s > 0$ et $r + s = n$. Sans perte de généralité, on peut supposer que $\gamma_1, \ldots, \gamma_r$ sont les racines de g, et $\gamma_{r+1}, \ldots, \gamma_n$ sont les racines de h.
Prenons $\sigma \in G$, qui s'étend en un automorphisme de $L[x]$ en agissant sur les coefficients. Puisque $g, h \in K[x]$, les polynômes g et h sont fixés par σ. En particulier, σ permute les racines de g entre elles, et les racines de h entre elles. Ainsi la fonction Φ du point précédent se factorise en

$$\begin{aligned}\Phi \colon G &\to \mathrm{Bij}(\gamma_1, \ldots, \gamma_r) \times \mathrm{Bij}(\gamma_{r+1}, \ldots, \gamma_n) \\ \sigma &\mapsto \left(\sigma|_{\{\gamma_1, \ldots, \gamma_r\}}, \sigma|_{\{\gamma_{r+1}, \ldots, \gamma_n\}}\right)\end{aligned}$$

Puisque Φ est injective, on a

$$n! = |S_n| = |G| \leq |\mathrm{Bij}(\gamma_1, \ldots, \gamma_r)| \cdot |\mathrm{Bij}(\gamma_{r+1}, \ldots, \gamma_n)| = r! \cdot s!$$

Puisque $r + s = n$ et que $r > 0$, en se servant du coefficient binomial $\binom{n}{r}$, on voit que $n! \geq r! \cdot s!$ avec égalité si et seulement si $n = 2$.

Si $n > 2$, on a ainsi obtenu une contradiction, et f est irréductible.

Si $n = 2$ et que f n'est pas irréductible, alors les deux racines de f appartiennent à K et $L = K$. Dans ce cas le groupe de Galois G est trivial, ce qui n'est pas le cas de S_2. Donc f est aussi irréductible dans le cas $n = 2$.

3. Soit γ une racine de f. Quitte à renommer les racines de f, on peut supposer que $\gamma = \gamma_1$. Supposons que $\sigma \in \mathrm{Gal}(K(\gamma_1)/K)$ soit un automorphisme non-trivial. Puisque l'extension est générée sur K par le seul élément γ_1, on voit que $\sigma(\gamma) \neq \gamma$. De plus $\sigma(\gamma_1)$ est aussi une racine de f. Sans perte de généralité, on peut supposer que $\sigma(\gamma_1) = \gamma_2$. On en déduit que $K(\gamma_1)$ contient au moins deux racines distinctes de f.

   Appliquons maintenant le théorème fondamental de la théorie de Galois (ce qui est possible, puisque L est Galois sur K par le premier point). L'extension intermédiaire $K(\gamma_1)$ correspond à un sous-groupe $H \leq G$, en ce qu'on peut écrire $K(\gamma_1) = L^H$. On a alors $[L : K(\gamma_1)] = |H|$, tandis que $[K(\gamma_1) : K] = \deg f = n$ par le second point. Par multiplicativité des degrés, on trouve alors

$$n! = |S_n| = |G| = [L : K] = [L : K(\gamma_1)][K(\gamma_1) : K] = |H| \cdot n$$

   et ainsi $|H| = (n-1)!$.

   Montrons que cela conduit à une contradiction si $n > 2$. Reprenons la fonction injective (en fait, bijective) Φ du premier point et identifions $\Phi(H)$. Puisque $L^H = K(\gamma_1)$, les éléments de H doivent fixer les racines de f contenues dans $K(\gamma_1)$. Or il y en a au moins deux, γ_1 et γ_2. Donc $\Phi(H)$ est un sous-ensemble (en fait, un sous-groupe) de $\mathrm{Fix}(\gamma_1, \gamma_2) = \{\tau \in \mathrm{Bij}(\gamma_1, \ldots, \gamma_n) \mid \tau(\gamma_1) = \gamma_1, \tau(\gamma_2) = \gamma_2\}$. Ainsi

$$(n-1)! = |H| = |\Phi(H)| \leq |\mathrm{Fix}(\gamma_1, \gamma_2)| = (n-2)!,$$

   ce qui est une contradiction pour $n > 2$. On a donc montré que $\mathrm{Gal}(K(\gamma_1)/K)$ est le groupe trivial.

   Remarquez que si $n = 2$, alors $K(\gamma_1) = L$ et donc $\mathrm{Gal}(K(\gamma_1)/K) = G \cong S_2$.

Exercice 8.

We first show that the polynomial $x^3 - i\sqrt{3} \in K[x]$ is irreducible over K. As this is a polynomial of degree 3, it is irreducible in $K[x]$ if and only if it does not admit roots in K. Assume by contradiction that there exists $\alpha \in K$ such that $\alpha^3 - i\sqrt{3} = 0$. Now, remark that the extension $\mathbb{Q} \subseteq K$ is of degree 2 ($i\sqrt{3} \notin \mathbb{Q}$ is a root of the polynomial $x^2 + 3 \in \mathbb{Q}[x]$), hence $\dim_{\mathbb{Q}}(K) = 2$ and the set $\{1, i\sqrt{3}\}$ is a basis of K over $\mathbb{Q}$. Therefore, there exist $a, b \in \mathbb{Q}$ such that $\alpha = a + bi\sqrt{3}$ and we have :

$$(a + bi\sqrt{3})^3 - i\sqrt{3} = a^3 + 3a^2bi\sqrt{3} - 9ab^2 - 3b^3i\sqrt{3} - i\sqrt{3} = 0.$$

As the set $\{1, i\sqrt{3}\}$ is a basis of K, it follows that $\begin{cases} a^3 - 9ab^2 = 0 \\ 3a^2b - 3b^3 - 1 = 0 \end{cases}$.

Moreover, since $a^3 - 9ab^2 = a(a^2 - 9b^2) = a(a - 3b)(a + 3b) = 0$, we distinguish the cases :

— if $a = 0$, then $-3b^3 - 1 = 0$ and, as $b \in \mathbb{Q}$, it follows that the irreducible polynomial $3x^3 + 1 \in \mathbb{Q}[x]$ admits a root in $\mathbb{Q}$, a contradiction. (As this is a polynomial of degree 3 it is straightforward to see that it is irreducible in $\mathbb{Q}[x]$ since it does not admit roots in $\mathbb{Q}$).

— if $a = 3b$ or $a = -3b$, then $24b^3 - 1 = 0$ and, as $b \in \mathbb{Q}$, it follows that the irreducible polynomial $24x^3 - 1 \in \mathbb{Q}[x]$ admits a root in $\mathbb{Q}$, a contradiction.

We have just shown that $x^3 - i\sqrt{3} \in K[x]$ is irreducible over K.

Let $\alpha \in L$ be a root of $x^3 - i\sqrt{3}$. Then the other roots are $\omega\alpha$ and $\omega^2\alpha$, where $\omega = e^{2i\pi/3} = \frac{-1+i\sqrt{3}}{2} \in K$. We deduce that $L = K(\alpha, \omega\alpha, \omega^2\alpha) = K(\alpha)$. Lastly, since α is a root of the irreducible polynomial $x^3 - i\sqrt{3} \in K[x]$, we conclude that $[L : K] = 3$. Moreover, as the extension $K \subseteq L$ is Galois ($K \subseteq L$ is a finite separable extension and L is the splitting field of a polynomial in $K[x]$), we have $|\mathrm{Gal}(L/K)| = 3$ and so $\mathrm{Gal}(L/K) \cong \mathbb{Z}/3\mathbb{Z}$.