Exercice 1.
We note that $\mathbb{F}_{27}^\times \cong \mathbb{Z}/26\mathbb{Z}$, see Theorem 3.4.17 (g). Let $\alpha \in \mathbb{F}_{27}^\times$. Then $\mathrm{ord}(\alpha) \in \{1, 2, 13, 26\}$. As $\alpha \neq 1, -1$, it follows that $\mathrm{ord}(\alpha) \in \{13, 26\}$. If $\mathrm{ord}(\alpha) = 13$, then $(-\alpha)^{13} = -1$ and so $\mathrm{ord}(-\alpha) = 26$.

Exercice 2. 1. Par le Corollaire 3.4.22, $\mathbb{F}_{p^r}$ contient un et un seul sous-corps isomorphe à $\mathbb{F}_{p^n}$ pour n divisant r. Si $\mathbb{F}_{p^s}$ est l'un d'eux, alors les corps intermédiaires de l'extension $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^r}$ sont les $\mathbb{F}_{p^n}$ où s divise n et n divise r.

2. Les sous-corps de $\mathbb{F}_{16}$, en vertu du premier point, sont $\mathbb{F}_2$ et $\mathbb{F}_4$, et ils forment une chaîne. Donc $\mathbb{F}_2(a) = \mathbb{F}_{16}$ si et seulement si $a \notin \mathbb{F}_4$. Par le Théorème 3.2.17 on a

$$\mathbb{F}_{16}^\times \cong \mathbb{Z}/15\mathbb{Z}, \quad \mathbb{F}_4^\times \cong \mathbb{Z}/3\mathbb{Z}$$

et $\mathbb{F}_4^\times \subset \mathbb{F}_{16}^\times$ est un sous-groupe. Un élément $0 \neq a \in \mathbb{F}_{16}$ vérifie $\mathbb{F}_2(a) = \mathbb{F}_{16}$ si et seulement si son image dans $\mathbb{F}_{16}^\times$ n'est pas contenue dans ce sous-groupe. D'un autre côté, il y a $\varphi(15) = 8$ éléments qui génèrent $\mathbb{F}_{16}^\times$, où φ est la fonction de comptage d'Euler. Remarquons aussi qu'un élément contenu dans le sous-groupe $\mathbb{F}_4^\times$ ne saurait générer le groupe $\mathbb{F}_{16}^\times$. Il y a ainsi

$$|\mathbb{F}_{16}^\times| - |\mathbb{F}_4^\times| - \varphi(15) = 15 - 3 - 8 = 4$$

éléments $0 \neq a \in \mathbb{F}_{16}$ tels que $\mathbb{F}_2(a) = \mathbb{F}_{16}$ et $\langle a \rangle \neq \mathbb{F}_{16}^\times$.

3. L'argument est semblable à celui du point précédent. Les sous-corps de $\mathbb{F}_{p^4}$ sont $\mathbb{F}_p \subset \mathbb{F}_{p^2}$, et on a $\mathbb{F}_p(a) = \mathbb{F}_{p^4}$ si et seulement si $a \notin \mathbb{F}_{p^2}$. Par le Théorème 3.2.17 on a

$$\mathbb{F}_{p^4}^\times \cong \mathbb{Z}/(p^4-1)\mathbb{Z}, \quad \mathbb{F}_{p^2} \cong \mathbb{Z}/(p^2-1)\mathbb{Z}.$$

Notons $E := \{0 \neq a \in \mathbb{F}_{16} \mid \langle a \rangle = \mathbb{F}_{16}^\times\}$. Alors $|E| = \varphi(p^4-1)$. Remarquons aussi que E et $\mathbb{F}_{p^2}^\times$ sont des sous-ensembles disjoints de $\mathbb{F}_{p^4}^\times$. Ainsi

$$\begin{aligned} |\{0 \neq a \in \mathbb{F}_{p^4} \mid \mathbb{F}_p(a) = \mathbb{F}_{p^4} \text{ et } \langle a \rangle \neq \mathbb{F}_{p^4}^\times\}| &= |\mathbb{Z}/(p^4-1)\mathbb{Z} \setminus (E \sqcup \mathbb{F}_{p^2}^\times)| \\ &= p^4 - 1 - (p^2-1) - \varphi(p^4-1) \\ &= p^4 - p^2 - \varphi(p^4-1). \end{aligned}$$

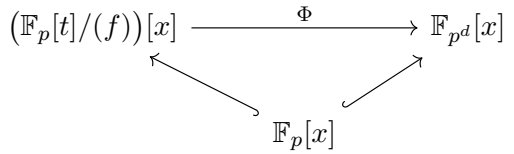
Exercice 3. 1. Notons $q := \mathrm{pgdc}(f, x^{p^d} - x)$. Comme f est irréductible, on a $q = 1$ ou $q = f$. On va montrer que $q = 1$ n'est pas possible. Puisque f est irréductible de degré d, le quotient $\mathbb{F}_p[t]/(f(t))$ est un corps de degré d sur $\mathbb{F}_p$. En particulier il contient p^d éléments. Par le Théorème 3.4.17, on obtient un isomorphisme

$$\phi \colon \mathbb{F}_p[t]/(f(t)) \cong \mathbb{F}_{p^d}$$

qui se restreint à l'égalité sur $\mathbb{F}_p$ (puisqu'il envoie 1 vers 1). Ainsi l'isomorphisme

$$\Phi \colon \big(\mathbb{F}_p[t]/(f)\big)[x] \cong \mathbb{F}_{p^d}[x]$$

induit par ϕ fait commuter le diagramme



On en conclut que l'extension $\mathbb{F}_p \subset \mathbb{F}_{p^d}$ contient une racine de $\Phi(f) = f \in \mathbb{F}_p[x]$. Notons $\alpha \in \mathbb{F}_{p^d}$ cette racine. Par le Théorème 3.2.17 à nouveau, α est aussi une racine de $x^{p^d} - x \in \mathbb{F}_p[x]$. Donc $x - \alpha$ divise à la fois f et $x^{p^d} - x$ dans $\mathbb{F}_{p^d}[x]$. Cela implique que $(f, x^{p^d} - x) \subseteq (x - \alpha)$ dans l'anneau $\mathbb{F}_{p^d}[x]$.

Si $q = 1$, alors par Bézout il existerait $a, b \in \mathbb{F}_p[x]$ tels que $af + b(x^{p^d} - x) = 1$. Cette relation serait encore vraie dans le plus gros anneau $\mathbb{F}_{p^d}[x]$. Or on vient d'établir que $(f, x^{p^d} - x) \subseteq (x - \alpha)$ dans $\mathbb{F}_{p^d}[x]$, c'est donc une contradiction. Ainsi $q = f$, d'où f divise $x^{p^d} - x$.

2. Le Théorème 3.2.17 nous indique que $x^{p^d} - x$ se scinde sur $\mathbb{F}_{p^d}$. Or f divise $x^{p^d} - x$, donc (par unicité de la décomposition en facteurs premiers) le polynôme f se scinde sur $\mathbb{F}_{p^d}$.

3. Puisque f se scinde sur $\mathbb{F}_{p^d}$ et divise $x^{p^d} - x$ dans $\mathbb{F}_{p^d}[x]$, il suffit de montrer que $x^{p^d} - x$ n'a pas de racines multiples dans $\mathbb{F}_{p^d}$. Or le Théorème 3.2.17 implique que

$$x^{p^d} - x \quad \text{est divisible par} \quad \prod_{\alpha \in \mathbb{F}_{p^d}} (x - \alpha) \quad \text{dans } \mathbb{F}_{p^d}[x].$$

En comparant les degrés et les coefficients dominants, on voit qu'il y a en fait égalité entre ces deux polynômes. Donc $x^{p^d} - x$ n'a pas de racine multiple.

4. Par le second point, f et g se scindent sur $\mathbb{F}_{p^d}$. S'ils ont une racine β en commun dans $\mathbb{F}_{p^d}$, alors l'idéal $(f, g) \subseteq (x - \beta)$ n'est pas égal à $\mathbb{F}_{p^d}[x]$. Mais si $\text{pgdc}(f, g) = 1$ dans $\mathbb{F}_p[x]$, alors par Bézout on obtient comme dans le premier point que $(f, g) = \mathbb{F}_{p^d}[x]$. Donc $\text{pgdc}(f, g) \neq 1$. Comme f et g sont irréductibles, on en déduit que $f = g$ modulo une unité (c'est-à-dire modulo multiplication par un scalaire de $\mathbb{F}_p^\times$).

5. Le premier point montre que $x^{p^d} - x$ est divisible par tous les polynômes irréductibles de degré d. La preuve du Corollaire 3.4.22 montre que $x^{p^s} - x$ divise $x^{p^d} - x$ pour tous les s divisant d. Donc

$$\prod_{\substack{h \text{ unitaire irréd.} \\ \text{dans } \mathbb{F}_p[x] \\ \deg h \text{ divise } d}} h \quad \text{divise} \quad x^{p^d} - x.$$

Il reste à montrer qu'il n'existe pas d'autre polynôme irréductible divisant $x^{p^d} - x$. Soit g un polynôme irréductible dont le degré ne divise pas d. Si g divise $x^{p^d} - x$, alors g se scinde sur $\mathbb{F}_{p^d}$, et donc $\mathbb{F}_p[x]/(g)$ s'identifie à un sous-corps de $\mathbb{F}_{p^d}$, c'est-à-dire à un $\mathbb{F}_{p^s}$ où s divise d. Mais dans ce cas

$$\deg g = [\mathbb{F}_p[x]/(g) : \mathbb{F}_p] = [\mathbb{F}_{p^s} : \mathbb{F}_p] = s$$

divise d, ce qui est une contradiction. On a donc l'égalité désirée.

Exercice 4.
Cette solution est adaptée de l'article *Counting Irreducible Polynomials over Finite Fields Using the Inclusion-Exclusion Principle* de S.K.Chebolu et J. Minác, dans *Math. Mag.* **84** (2011) 369-371.

1. On a vu dans l'Exercice 5 que tout polynôme f irréductible de degré d se scinde sur $\mathbb{F}_{p^d}$. On a vu dans le même exercice que f n'a pas de racines doubles, et que deux polynômes unitaires irréductibles de même degré n'ont pas de racines en commun. Si $f_1, \ldots, f_{N_d}$ sont les polynômes unitaires irréductibles de degré d et $R_{f_i} \subset \mathbb{F}_{p^d}$ les ensembles de racines, on a donc montré que

$$|R_{f_i}| = d \quad \text{et} \quad R_{f_i} \cap R_{f_j} = \emptyset \text{ si } i \neq j.$$

Ainsi on obtient

$$dN_d = |R_{f_1} \sqcup \cdots \sqcup R_{f_{N_d}}|.$$

Il reste à déterminer quels éléments de $\mathbb{F}_{p^d}$ sont des racines de polynômes irréductibles de degré d. Remarquons que si $a \in \mathbb{F}_{p^d}$ est une racine de f_i, alors

$$\mathbb{F}_p(a) \cong \mathbb{F}_p[t]/(f_i(t))$$

et en prenant les degrés sur $\mathbb{F}_p$ on obtient $[\mathbb{F}_p(a) : \mathbb{F}_p] = d$. Donc $\mathbb{F}_p(a) = \mathbb{F}_{p^d}$. Ainsi si a est une racine de f_i, il n'appartient à aucun sous-corps strict $L \subsetneq \mathbb{F}_{p^d}$. Inversément, supposons que $a \in \mathbb{F}_{p^d}$ n'appartienne à aucun sous-corps strict. Par le Théorème 3.2.17, a est racine de $x^{p^d} - x \in \mathbb{F}_p[x]$, donc de l'un de ses facteurs irréductibles de degré e. Alors $[\mathbb{F}_p(a) : \mathbb{F}] = e$, et si $e < d$ on obtient $\mathbb{F}_p(a) \subsetneq \mathbb{F}_{p^d}$, ce qui est une contradiction avec le choix de de a. En définitive nous avons montré que

$$R_{f_1} \sqcup \cdots \sqcup R_{f_{N_d}} = \mathbb{F}_{p^d} \setminus \bigcup_{L \subsetneq \mathbb{F}_{p^d}} L$$

où L parcourt les sous-corps stricts de $\mathbb{F}_{p^d}$.

2. Le problème pour tirer une formule générale du point précédent est que les sous-corps L ne sont pas tous inclus les uns dans les autres, et que leurs intersections sont non-triviales. Pour les petites valeurs de d, il est cependant facile passer en revue les sous-corps et leurs intersections. Nous utilisons sans plus y faire référence le Corollaire 3.4.22.
   (a) $d = 2$. Le seul sous-corps strict de $\mathbb{F}_{p^2}$ est $\mathbb{F}_p$. Donc

   $$N_2 = \frac{p^2 - p}{2}.$$

   (b) $d = 3$. Le seul sous-corps strict de $\mathbb{F}_{p^3}$ est $\mathbb{F}_p$. Donc

   $$N_3 = \frac{p^3 - p}{3}.$$

   (c) $d = 4$. Les sous-corps stricts de $\mathbb{F}_{p^4}$ sont $\mathbb{F}_p \subset \mathbb{F}_{p^2}$. Donc

   $$N_4 = \frac{p^4 - p^2}{4}.$$

   (d) $d = 5$. Le seul sous-corps strict de $\mathbb{F}_{p^5}$ est $\mathbb{F}_p$. Donc

   $$N_5 = \frac{p^5 - p}{5}.$$

   (e) $d = 6$. Le premier cas non-trivial. Les sous-corps stricts sont

   $$\mathbb{F}_{p^2} \supset \mathbb{F}_p \subset \mathbb{F}_{p^3}.$$

   Ainsi

   $$|\mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})| = |\mathbb{F}_{p^6}| - |\mathbb{F}_{p^2}| - |\mathbb{F}_{p^3}| + |\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3}|.$$

   L'intersection $\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3}$ est un corps fini de caractéristique p, donc un corps de la forme $\mathbb{F}_{p^s}$ où s divise à la fois 2 et 3. Donc $s = 1$ et le cardinal de l'intersection vaut p. Il s'ensuit que

   $$N_6 = \frac{p^6 - p^3 - p^2 + p}{6}.$$

3. Observez que le Corollaire 3.4.22 permet d'écrire explicitement le réseau de sous-corps de n'importe quel corps fini. Puisque $\mathbb{F}_{p^{d/n}} \cap \mathbb{F}_{p^{d/m}}$ est un sous-corps à la fois de $\mathbb{F}_{p^{d/n}}$, de $\mathbb{F}_{p^{d/m}}$ et de $\mathbb{F}_{p^d}$, on utilise le Corollaire 3.4.22 pour indentifier cette intersection. Elle est donnée par $\mathbb{F}_{p^s}$, où s est le plus grand entier qui divise à la fois d/n et d/m. Puisque n et m sont premiers entre eux, en considérant la décomposition de d en facteurs premiers on voit que $s = d/nm$.

4. Passons au cas général. Dans la formule établie au premier point, on peut évidemment prendre l'union sur l'ensemble des sous-corps stricts L qui sont maximaux. Par le Corollaire 3.4.22, ces sous-corps sont donnés par

$$F_j := \mathbb{F}_{p^{d/s_j}} \quad \text{avec } d = \prod_{j=1}^{n} s_j^{i_j} \text{ la décomposition en nombres premiers.}$$

Ecrivons $F_{j_1\dots j_r} := F_{i_1} \cap \dots \cap F_{j_r}$. En utilisant le point précédent par induction sur t, on voit que $|F_{j_1\dots j_t}| = p^{d/s_{j_1}\cdots s_{j_t}}$. La formule d'inclusion-exclusion nous donne alors

$$\begin{aligned} dN_d &= \left|\mathbb{F}_{p^d}\right| - \left|\bigcup_{j=1}^{n} F_j\right| \\ &= p^d - \sum_{t=1}^{n}(-1)^{t+1} \sum_{j_1<\dots<j_t} |F_{j_1\dots j_t}| \\ &= p^d - \sum_{t=1}^{n}(-1)^{t+1} \sum_{j_1<\dots<j_t} p^{d/s_{j_1}\cdots s_{j_t}} \\ &= \sum_{t=0}^{n}(-1)^{t} \sum_{j_1<\dots<j_t} p^{d/s_{j_1}\cdots s_{j_t}} \end{aligned}$$

où on pose $p^{d/s_{j_1}\cdots s_{j_t}} = p^d$ pour $t = 0$. Considérons maintenant un entier r divisant d. On a

$$r = \prod_{j=1}^{n} s_j^{k_j} \quad \text{avec } 0 \le k_j \le i_j, \quad \text{donc} \quad \frac{d}{r} = \prod_{j=1}^{n} s_j^{i_j - k_j}.$$

Par la définition de la fonction de Möbius, on obtient

$$\mu\left(\frac{d}{r}\right) = \begin{cases} 0 & \text{si } k_j \le i_j - 2 \text{ pour au moins un } j, \\ 1 & \text{si } \forall j:\ k_j \ge i_j - 1 \text{ avec inégalité pour un nombre pair de } j, \\ -1 & \text{si } \forall j:\ k_j \ge i_j - 1 \text{ avec inégalité pour un nombre impair de } j. \end{cases}$$

Il s'ensuit que

$$\sum_{t=0}^{n}(-1)^{t} \sum_{j_1<\dots<j_t} p^{d/s_{j_1}\cdots s_{j_t}} = \sum_{r|d} \mu\left(\frac{d}{r}\right) p^r$$

ce qui conclut l'exercice.

Exercice 5. 1. By corollary 4.4.22 we know that for every j K_{j+1} contains a subfield isomorphic to K_j. We can then considered the induced inclusion homomorphism $\iota_j : K_j \to K_{j+1}$ for every $j \ge 1$.

2. Recall that if $K_0 \overset{\iota_0}{\hookrightarrow} K_1 \overset{\iota_1}{\hookrightarrow} K_2 \overset{\iota_2}{\hookrightarrow} \dots$ is an infinite sequence of fields with injectiv homomorphisms between each K_j and K_{j+1}. Then the direct limit is given by

$$\varinjlim_i K_i = \bigsqcup_{i\in\mathbb{N}} K_i \Big/ \begin{array}{l} \text{- } x \equiv \iota_{s-1} \circ \dots \circ \iota_r(x) \text{ et } \iota_{s-1} \circ \dots \circ \iota_r(x) \equiv x \text{ pour chaque entier} \\ \quad s > r, \text{ et } x \in K_r \\ \text{- } x \equiv x \text{ pour chaque } x \in K_r \end{array}$$

is a field with sum given by $[x] + [y]$ and product given by $[x] \cdot [y]$ for $x \in K_r$ and $y \in K_s$ are defined as follows : if $s > r$, then $[x] = [\iota_{s-1} \circ \dots \circ \iota_r(x)]$ which means that we can suppose $s = r$, and thus we define

(a) $[x] + [y] = [x + y]$

(b) $[x] \cdot [y] = [x \cdot y]$

It is clear that the unit and zero element are given by the inclusion of each the zero and unit element in each field. And since each K_i is a field the sum and multiplication defined as above endow the direct limit with a ring structure. It is also not difficult to see that each element $[x] \in \bigsqcup_{i\in\mathbb{N}} K_i$ has an inverse, since $x \in K_n$ for some $n \in \mathbb{N}$

Moreover the inclusion $K_0 \hookrightarrow \bigsqcup_{i\in\mathbb{N}} K_i$ gives us an embedding $K_0 \hookrightarrow \varinjlim_i K_i$.

3. Note that $\mathbb{F}_p \subset K$. Moreover each extension $K_j \subset K_{j+1}$ is a finite extension therefore it is an algebraic extension. Thus we have that each K_j is algebraic over $\mathbb{F}_p$. We then have that K is algebraic over $\mathbb{F}_p$ because each of its element lives in one of the K_j.
4. Let g be a polynomial in $K[t]$. Since g has a finite sum of coefficients, then there exists $n \in \mathbb{N}$ such that $g \in K_n[t]$. Let α be a root of g, then $K_n \subset K_n(\alpha)$ is a finite extension of degree r, for some $r \in \mathbb{N}$. Therefore $K_n(\alpha)$ is a field with p^{rn} elements. Hence $K_n(\alpha)$ is also a finite field containing F_p. Then we have that $K_n(\alpha) = K_{rn}$. So the root α is also an element of K since $\alpha \in K_{rn} \subset K$. Thus K is the algebraic closure of $\mathbb{F}_p$.