Exercice 1. (a) $P(X) = X^2 + 1$ ($\mathbb{Q}(i)$ contient aussi $-i$) et $Q(X) = X^3 - 2$ (irréductible par Eisenstein, le corps de rupture $\mathbb{Q}(\sqrt[3]{2})$ est strictement inclus dans le corps de décomposition qui contient forcément des éléments non réels comme $j\sqrt[3]{2}$ etc.).

(b) $X^4 + 2$ est irréductible sur $\mathbb{Z}$ par Eisenstein, et donc sur $\mathbb{Q}$ parce qu'il est non constant. Soit t une racine d'ordre 4 de -2 dans $\mathbb{C}$. On a $X^4 + 2 = (X - t)(X + t)(X - it)(X + it)$ dans $\mathbb{C}$. Un corps de rupture est de degré 4 sur $\mathbb{Q}$. Pour montrer qu'il n'est pas un corps de décomposition il suffit de montrer que $\mathbb{Q}(t, it) = \mathbb{Q}(i, t)$ est de dimension plus que 4 sur $\mathbb{Q}$. Or, en supposant qu'il est de dimension 4, on aurait que le polynôme minimal de t sur $\mathbb{Q}(i)$ est de degré 2. Mais il doit aussi diviser P, et il est donc de la forme $(X - t)H(X)$ sur $\mathbb{C}$, avec $H(X)$ l'une des parenthèses $X + t$, $X - it$, $X + it$. Or, dans tous les cas, le produit $(X - t)H(X)$ a un coefficient constant qui n'est pas dans $\mathbb{Q}(i)$ (on peut par exemple expliquer que les éléments de $\mathbb{Q}(i)$ sont les $a + ib$ dans $\mathbb{C}$ avec $a, b \in \mathbb{Q}$, ou bien que $\mathbb{Q}(\sqrt{2})$ est de degré 2 sur $\mathbb{Q}$ mais est contenu dans $\mathbb{R}$ et ne contient donc pas i, etc.).

Exercice 2. (a) L'ordre de l'élément divisant l'ordre du groupe dans $\mathbb{F}_q^\times$, on a $x^{q-1} = 1$ pour tout $x \in \mathbb{F}_q^\times$. Donc $x^q = x$ pour tous $x \in \mathbb{F}_q^\times$. Mais cette relation est vérifiée aussi par 0.

(b) F est injectif parce que c'est un morphisme entre deux corps. Il est alors surjectif parce que les cardinaux de son domaine de définition et de son domaine d'arrivée sont finis et égaux.

(c) Si $F^k = Id$, avec $k \geq 1$, alors $x^{p^k} = x$ pour tout $x \in \mathbb{F}_q$. Mais un polynôme non nul de degré p^k ne peut pas avoir plus de p^k racines, donc $k \geq n$.

(d) $\{Id, F, F^2, ..., F^{n-1}\}$ contient n éléments distincts (se montre par l'absurde en utilisant (b)). Montrons que $Aut(\mathbb{F}_q)$ ne peut pas avoir plus de n éléments et on aura fini. Soit u un générateur de $\mathbb{F}_q^\times$, dont on sait qu'il est cyclique. Alors $\mathbb{F}_p(u) = \mathbb{F}_q$ et donc le polynôme minimal de u est de degré n (degré de l'extension). Mais tout automorphisme de $\mathbb{F}_q$ fixe tous les éléments de $\mathbb{F}_p$. Donc il envoie u sur une racine de son polynôme minimal. Mais un automorphisme de $\mathbb{F}_q$ est déterminé par l'image de u (parce que les puissances de u couvrent tous les éléments à part zéro). Il y a donc au plus n automorphismes.

(e) $\mathbb{F}_q$ est un espace vectoriel sur K et donc $p^q = |\mathbb{F}_q| = |K|^a$, d'où : le seul diviseur premier de $|K|$ est p et donc $|K| = p^m$ avec $ma = n$.

(f) L'unicité est plus simple : si K est un sous-corps à p^m éléments, alors tous ses éléments vérifient $x^{p^m} = x$ et sont donc exactement les racines du polynôme $X^{p^m} - X$ dans $\mathbb{F}_q$. D'où l'unicité de K ; et l'idée pour montrer l'existence : on va montrer que $X^{p^m} - X$ divise $X^q - X$ et alors cela implique que $X^{p^m} - X$ est scindé sur $\mathbb{F}_q$. En prenant alors ses p^m racines dans K, on montre assez facilement, comme dans le cours, qu'elles forment un corps. Montrons donc que si $m|n$, alors $X^{p^m} - X | X^{p^n} - X$. Il suffit après avoir passé X et facteur de montrer que $X^{p^m-1} - 1 | X^{p^n-1} - 1$. Maintenant, si $m|n$, alors dans un anneau commutatif quelconque on a $a^m - b^m | a^n - b^n$ (utiliser la formule $x^k - y^k = (x-y)(....)$ avec $x = a^m, y = b^m$ et $k = n/m$). Dès lors, $p^m - 1$ divise $p^n - 1$ (appliquer le résultat dans $\mathbb{Z}$) et par conséquent $X^{p^m-1} - 1 | X^{p^n-1} - 1$ (appliquer le résultat dans $\mathbb{F}_p[X]$).

Exercice 3. (a) $X^{p^k n} - 1 = (X^n - 1)^{p^k}$ et donc les racines du polynôme de gauche sont exactement les racines de la parenthèse de droite.

(b) Les éléments x de U_k vérifient par définition $x^k = 1$. Par la théorie des groupes, ils vérifient aussi $x^{|U_k|} = 1$. Si d est le pgcd de k et $|U_k|$, on a une relation de Bézout $uk + v|U_k| = d$, et alors on voit que $x^d = 1$ (ou par l'ordre de l'élément qui doit diviser à la fois k et $|U_k|$). Mais $X^d - 1$ ne peut pas avoir plus de d racines, et comme il a au moins $|U_k|$, avec $d||U_k|$, on a $d = |U_k|$. Mais d divise k, donc $|U_k|$ divise k.

(c) Soit G un sous-groupe fini de $K^\times$. Supposons que G a k éléments. Alors tous ses éléments vérifient $x^k = 1$ (l'ordre de l'élément divise l'ordre du groupe). Mais alors $G \subset U_k$, et U_k a au plus k éléments, donc $G = U_k$.

Exercice 4. Soit Q un polynôme irréductible sur K, unitaire, qui divise $X^{mn} - a$. Soit K' un corps de rupture de Q sur K. Alors $X^{mn} - a$ possède une racine x dans K'. On a $x^{mn} = a$. Mais on a alors $(x^n)^m = a$ et $(x^m)^n = a$. Donc K' contient une racine de $X^m - a$ et une racine de $X^n - a$. Alors K' contient un corps de rupture de $X^m - a$ et un corps de rupture de $X^n - a$. Mais ceux-ci sont de degré m et respectivement n sur K. Par le théorème de la base télescopique on a $m|[K' : K]$ et $n|[K' : K]$. Comme m et n sont premiers entre eux, on a $mn|[K' : K]$. Mais $[K' : K] = \deg(Q)$. Comme $\deg(Q) \leq \deg(P) \leq mn$, on a $Q = P$, soit P est irréductible.