Partiel Algèbre 2

Responsable : Mr O. DEBARRE

Important : vous avez droit de consulter le cours et d'utiliser sans démonstration ses résultats (sauf ceux des exercices ou des TD). Si vous voulez utiliser des résultats hors du cours, il faut les démontrer (sauf mention explicite du contraire).

Exercice 1. a) Quel est le groupe de Galois du polynôme $X^3 - 10$ sur $\mathbf{Q}$? Sur $\mathbf{Q}(\sqrt{-3})$?

b) Trouver un polynôme de groupe de Galois $\mathbf{Z}/4\mathbf{Z}$ sur $\mathbf{Q}$. Même question avec $\mathbf{Z}/3\mathbf{Z}$ (*Indication :* penser aux polynômes cyclotomiques !).

Exercice 2. Soient p et q deux nombres premiers distincts, avec p impair. Soit $K \supset \mathbf{F}_q$ un corps de décomposition du polynôme séparable $X^p - 1 \in \mathbf{F}_q[X]$ et soit ω une racine primitive p-ième de l'unité dans K. On a $\omega^p = 1$, donc l'écriture ω^i, où $i \in \mathbf{Z}/p\mathbf{Z}$, a un sens. Pour toute partie Z de $\mathbf{Z}/p\mathbf{Z}$, on pose $P_Z(X) := \prod_{i\in Z}(X - \omega^i) \in K[X]$. Pour tout entier r premier à p, on note aussi $rZ \subset \mathbf{Z}/p\mathbf{Z}$ l'image de Z par la bijection $z \mapsto rz$ de $\mathbf{Z}/p\mathbf{Z}$.

a) Montrer l'équivalence :

$$P_Z(X) \in \mathbf{F}_q[X] \iff qZ = Z.$$

b) Quels sont les degrés des facteurs irréductibles de $X^7 - 1$ dans $\mathbf{F}_2[X]$? Dans $\mathbf{F}_3[X]$? De $X^{17} - 1$ dans $\mathbf{F}_2[X]$?

On pose

$$Z_p^+ = \{x \in (\mathbf{Z}/p\mathbf{Z})^* \mid \exists y \in (\mathbf{Z}/p\mathbf{Z})^* \quad x = y^2\} \qquad et \qquad Z_p^- = (\mathbf{Z}/p\mathbf{Z})^* - Z_p^+$$

et on suppose à partir de maintenant que la classe de q modulo p est dans Z_p^+.

c) Quels sont les cardinaux de Z_p^+ et de Z_p^- ?

d) Montrer $P_{Z_p^\pm}(X) \in \mathbf{F}_q[X]$. En déduire que le polynôme cyclotomique $\Phi_p(X) := \frac{X^p-1}{X-1}$ n'est pas irréductible dans $\mathbf{F}_q[X]$.

On suppose à partir de maintenant $q = 2$ et p tel que $2 \in Z_p^+$.

e) On pose $Q^\pm(X) := \sum_{i\in Z_p^\pm} X^i \in \mathbf{F}_2[X]$. Calculer $Q^+(X)^2$ et en déduire $\{Q^+(\omega), Q^-(\omega)\} = \{0, 1\}$.

On suppose à partir de maintenant $Q^+(\omega) = 0$ et $Q^-(\omega) = 1$, ce qu'on peut toujours faire quitte à changer de racine primitive ω.

f) Montrer $P_{Z_p^\pm} = \Phi_p \wedge Q^\pm$.

g) Décomposer le polynôme $X^7 - 1$ en produit de facteurs irréductibles dans $\mathbf{F}_2[X]$. *Si vous calculez bien,* même question avec le polynôme $X^{17} - 1$.

Exercice 3. Soit $K \hookrightarrow L$ une extension finie de corps.

a) Si $K \neq L$ et que tout élément de $L - K$ est inséparable sur K, montrer que la caractéristique de K est un nombre premier p, que $[L : K]_s = 1$ et que $[L : K]$ est une puissance de p.

b) On revient au cas général. Montrer que $[L : K]_s$ divise $[L : K]$ et que soit le quotient est 1, soit la caractéristique de K un nombre premier p et le quotient est une puissance de p (*Indication :* on pourra introduire la clôture séparable de K dans L et utiliser a)).

Exercice 4. Soit $\overline{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$ et soit $a \in \overline{\mathbf{Q}} - \mathbf{Q}$.

a) Montrer qu'il existe un sous-corps $K \subset \overline{\mathbf{Q}}$ tel que $a \notin K$ et que tout sous-corps de $\overline{\mathbf{Q}}$ contenant strictement K contient a ; on dit que K est un sous-corps de $\overline{\mathbf{Q}}$ maximal sans a (*Indication :* utiliser le lemme de Zorn).

On choisit un nombre premier p divisant $[K(a) : K]$. Soit $K \subset L \subset \overline{\mathbf{Q}}$ une extension finie non triviale de K. On note M la clôture normale de L dans $\overline{\mathbf{Q}}$ et $G := \mathrm{Gal}(M/K)$.

b) Montrer que p divise $[L : K]$.

c) Montrer que $[L : K]$ est une puissance de p (*Indication :* on pourra appliquer la théorie de Galois à l'extension $K \subset M$ et utiliser (sans le démontrer !) le théorème de Sylow donné plus bas).

d) Montrer que $[K(a) : K] = p$ et que $K(a)$ est la seule sous-extension de $K \subset \overline{\mathbf{Q}}$ de degré p sur K (*Indication :* on pourra utiliser la théorie de Galois et le théorème de Sylow donné plus bas).

e) Montrer que G est cyclique, puis que toute extension finie de K est galoisienne cyclique (*Indication :* on pourra utiliser le théorème de Sylow donné plus bas).

f) Montrer qu'il existe $b \in K(a)$, avec $b^p \in K$, tel que $K(a) = K(b)$.

Théorème de Sylow. *Soit p un nombre premier et soit G un groupe fini de cardinal mp^r, avec $m \wedge p = 1$. Il existe un sous-groupe de G de cardinal p^r. Plus précisément, pour tout sous-groupe H de G de cardinal p^s, avec $0 \leq s \leq r$, et tout $s \leq t \leq r$, il existe un sous-groupe de G contenant H et de cardinal p^t.*

Corrigé du partiel Algèbre 2

Responsable : Mr O. DEBARRE

Exercice 1. *a) Quel est le groupe de Galois d'un corps de décomposition du polynôme $X^3 - 10$ sur $\mathbf{Q}$? Sur $\mathbf{Q}(\sqrt{-3})$?*

Le corps de décomposition est $\mathbf{Q}(\sqrt[3]{10}, j)$. Le groupe de Galois sur $\mathbf{Q}$ est un sous-groupe de $\mathfrak{S}_3$ de cardinal $[\mathbf{Q}(\sqrt[3]{10}, j) : \mathbf{Q}] = [\mathbf{Q}(\sqrt[3]{10}, j) : \mathbf{Q}(\sqrt[3]{10})][\mathbf{Q}(\sqrt[3]{10}) : \mathbf{Q}] = 2 \times 3 = 6$. C'est donc $\mathfrak{S}_3$. L'extension $\mathbf{Q}(\sqrt{-3}) = \mathbf{Q}(j) \subset \mathbf{Q}(\sqrt[3]{10}, j)$ est galoisienne de degré 3, donc son groupe de Galois est $\mathbf{Z}/3\mathbf{Z}$.

b) Trouver un polynôme de groupe de Galois $\mathbf{Z}/4\mathbf{Z}$ sur $\mathbf{Q}$. Même question avec $\mathbf{Z}/3\mathbf{Z}$.

Pour tout nombre premier p, le polynôme Φ_p est irréductible sur $\mathbf{Q}$. Son groupe de Galois est isomorphe à $((\mathbf{Z}/p\mathbf{Z})^*, \times)$ (prop. 8.6 du cours), qui est cyclique d'ordre $p-1$. En particulier, le groupe de Galois sur $\mathbf{Q}$ du polynôme $X^5 - 1$ est $\mathbf{Z}/4\mathbf{Z}$.

De même, le groupe de Galois sur $\mathbf{Q}$ du polynôme $X^9 - 1$ (donc le groupe de Galois de l'extension $\mathbf{Q} \subset \mathbf{Q}(e^{2i\pi/9})$) est $((\mathbf{Z}/9\mathbf{Z})^*, \times)$, groupe abélien d'ordre 6 donc cyclique (on peut aussi vérifier directement que 2 est un générateur) donc le groupe de Galois de l'extension $\mathbf{Q} \subset \mathbf{Q}(\cos(2\pi/9))$ est $\mathbf{Z}/3\mathbf{Z}$. On a vu en cours que le réel $2\cos(2\pi/9)$ est racine du polynôme $P(X) = X^3 - 3X - 1$, donc le groupe de Galois de P est $\mathbf{Z}/3\mathbf{Z}$.

Autre exemple : le groupe de Galois sur $\mathbf{Q}$ du polynôme $X^7 - 1$ est $\mathbf{Z}/6\mathbf{Z}$, donc le groupe de Galois de l'extension $\mathbf{Q} \subset \mathbf{Q}(\cos(2\pi/7))$ est $\mathbf{Z}/3\mathbf{Z}$. Le polynôme minimal de $e^{2i\pi/7}$ est

$$P(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = X^3((X^3 + X^{-3}) + (X^2 + X^{-2}) + (X + X^{-1}) + 1).$$

Posons $Y := X + X^{-1}$. On a $P(X)X^{-3} = Y^3 - 3Y + Y^2 - 2 + Y + 1$, donc le polynôme minimal de $2\cos(2\pi/7)$ est $Y^3 + Y^2 - 2Y + 1$, polynôme dont le groupe de Galois est ainsi $\mathbf{Z}/3\mathbf{Z}$.

On a vu aussi en TD que le groupe de Galois de $X^3 - tX^2 + (t-3)X + 1$ est $\mathbf{Z}/3\mathbf{Z}$ pour tout $t \in \mathbf{Z}$ (mais il faudrait le redémontrer !).

Exercice 2. *Soient p et q deux nombres premiers distincts, avec p impair. Soit $K \supset \mathbf{F}_q$ un corps de décomposition du polynôme séparable $X^p - 1 \in \mathbf{F}_q[X]$ et soit ω une racine primitive p-ième de l'unité dans K. On a $\omega^p = 1$, donc l'écriture ω^i, où $i \in \mathbf{Z}/p\mathbf{Z}$, a un sens. Pour toute partie Z de $\mathbf{Z}/p\mathbf{Z}$, on pose $P_Z(X) := \prod_{i \in Z}(X - \omega^i) \in K[X]$. Pour tout entier r premier à p, on note aussi $rZ \subset \mathbf{Z}/p\mathbf{Z}$ l'image de Z par la bijection $z \mapsto rz$ de $\mathbf{Z}/p\mathbf{Z}$.*

a) Montrer l'équivalence : $P_Z(X) \in \mathbf{F}_q[X] \iff qZ = Z$.

Comme on est en caractéristique q, on a $P_Z(X)^q = \prod_{i \in Z}(X^q - \omega^{iq}) = P_{qZ}(X^q)$. Comme $\mathbf{F}_q = \{x \in K \mid x^q = x\}$, un polynôme $Q \in K[X]$ est dans $\mathbf{F}_q[X]$ si et seulement si $Q(X)^q = Q(X^q)$. Comme $P_Z(X) = P_{Z'}(X)$ si et seulement si $Z = Z'$, on a ce qu'on veut.

b) Quels sont les degrés des facteurs irréductibles de $X^7 - 1$ dans $\mathbf{F}_2[X]$? Dans $\mathbf{F}_3[X]$? De $X^{17} - 1$ dans $\mathbf{F}_2[X]$?

Par a), et puisque q est inversible dans $\mathbf{Z}/p\mathbf{Z}$, les facteurs irréductibles de $X^p - 1$ dans $\mathbf{F}_q[X]$ sont les P_Z, où Z est une partie du type $Z = \{q^m z \mid m \in \mathbf{N}\}$, pour $z \in \mathbf{Z}/p\mathbf{Z}$ fixé.

Pour $p = 7$ et $q = 2$, on obtient $\{0\}$, $\{1, 2, 4\}$ et $\{3, 6, 5\}$, donc des facteurs irréductibles de degré 1, 3 et 3.

Pour $p = 7$ et $q = 3$, on obtient $\{0\}$ et $\{1, 3, 2, 6, 4, 5\}$, donc des facteurs irréductibles de degré 1 et 6. La décomposition est $X^7 - 1 = (X - 1)\Phi_7(X)$.

Pour $p = 17$ et $q = 2$, on obtient $\{0\}$, $\{1, 2, 4, 8, 9, 13, 15, 16\}$ et $\{3, 5, 6, 7, 10, 11, 12, 14\}$, donc des facteurs irréductibles de degré 1, 8 et 8.

c) On pose $Z_p^+ = \{x \in (\mathbf{Z}/p\mathbf{Z})^* \mid \exists y \in (\mathbf{Z}/p\mathbf{Z})^* \quad x = y^2\}$ *et* $Z_p^- = (\mathbf{Z}/p\mathbf{Z})^* - Z_p^+$ *et on suppose à partir de maintenant que la classe de* q *modulo* p *est dans* Z_p^+*. Quels sont les cardinaux de* Z_p^+ *et de* Z_p^- *?*

On a $\mathrm{Card}(Z_p^\pm) = (p-1)/2$ (on a pris p impair).

d) Montrer $P_{Z_p^\pm}(X) \in \mathbf{F}_q[X]$*. En déduire que le polynôme cyclotomique* $\Phi_p(X) := \frac{X^p-1}{X-1}$ *n'est pas irréductible dans* $\mathbf{F}_q[X]$*.*

Par a), il suffit de remarquer que $Z_p^\pm$ (qui est non vide par c)) est stable par multiplication par q, ce qui est le cas puisque la classe de q modulo p est dans Z_p^+. Ensuite, on a $\Phi_p(X) = P_{Z_p^+}(X)P_{Z_p^-}(X)$.

e) On suppose à partir de maintenant $q = 2$ *et* p *tel que* $2 \in Z_p^+$*. On pose* $Q^\pm(X) := \sum_{i \in Z_p^\pm} X^i \in \mathbf{F}_2[X]$*. Calculer* $Q^+(X)^2$ *et en déduire* $\{Q^+(\omega), Q^-(\omega)\} = \{0, 1\}$*.*

Comme on est en caractéristique 2, on a $Q^+(X)^2 = \sum_{i \in Z_p^+} X^{2i} = \sum_{k \in 2Z_p^+} X^k$ et comme $2 \in Z_p^+$, on a $2Z_p^+ = Z_p^+$ dans $\mathbf{Z}/p\mathbf{Z}$. On en déduit $Q^+(X)^2 = Q^+(X)$ dans $\mathbf{F}_2[X]/(X^p - 1)$. Cela entraîne $Q^+(\omega)^2 = Q^+(\omega)$, donc $Q^+(\omega) \in \{0, 1\}$. D'autre part, on a $1 + Q^+(X) + Q^-(X) = \Phi_p(X)$, donc $Q^+(\omega) + Q^-(\omega) = 1$ et $\{Q^+(\omega), Q^-(\omega)\} = \{0, 1\}$.

f) On suppose à partir de maintenant $Q^+(\omega) = 0$ *et* $Q^-(\omega) = 1$*, ce qu'on peut toujours faire quitte à changer de racine primitive* ω*. Montrer* $P_{Z_p^\pm} = \Phi_p \wedge Q^\pm$ [1]*.*

Soit $j \in Z_p^\pm$; on a alors

$$Q^+(\omega^j) = \sum_{i \in Z_p^+} \omega^{ji} = \sum_{k \in jZ_p^+} \omega^k = Q^\pm(\omega)$$

puisque $jZ_p^+ = Z_p^\pm$ dans $\mathbf{Z}/p\mathbf{Z}$. On a donc $Q^+(\omega^j) = 0$ pour tout $j \in Z_p^+$, ce qui signifie que $P_{Z_p^+}$ divise Q^+, donc aussi $D^+ := \Phi_p \wedge Q^+$, et $Q^-(\omega^j) = 0$ pour tout $j \in Z_p^-$, ce qui signifie que $P_{Z_p^-}$ divise Q^-, donc aussi $D^- := \Phi_p \wedge Q^-$.

Comme $1 = \Phi_p - Q^+ - Q^-$, on a $D^+ \wedge D^- = 1$. On a donc $D^+D^- \mid \Phi_p$, donc $\deg(D^+) + \deg(D^-) \leq p - 1$. D'autre part, $P_{Z_p^\pm} \mid D^\pm$ et $\deg(P_{Z_p^\pm}) = (p-1)/2$. On a donc $P_{Z_p^\pm} = D^\pm$.

g) Décomposer le polynôme $X^7 - 1$ *en produit de facteurs irréductibles dans* $\mathbf{F}_2[X]$*. Même question avec le polynôme* $X^{17} - 1$*.*

Il résulte de b) que les facteurs irréductibles de $X^7 - 1$ dans $\mathbf{F}_2[X]$ sont $X - 1$ et les $P_{Z_7^\pm}$. Comme $Q^+(X) = X^4 + X^2 + X$, on a par f) $P_{Z_7^+} = 1 + X + X^3$; de même, comme $Q^-(X) = X^6 + X^5 + X^3$, on a par f) $P_{Z_7^+} = X^3 + X^2 + 1$ et $X^7 - 1 = (X - 1)(X^3 + X + 1)(X^3 + X^2 + 1)$.

De la même façon, les facteurs irréductibles de $X^{17} - 1$ dans $\mathbf{F}_2[X]$ sont $X - 1$ et les $P_{Z_{17}^\pm}$. On a

$$\begin{aligned} Q^+(X) &= X^{16} + X^{15} + X^{13} + X^9 + X^8 + X^4 + X^2 + X \\ Q^-(X) &= X^{14} + X^{12} + X^{11} + X^{10} + X^7 + X^6 + X^5 + X^3 \end{aligned}$$

---

1. Il y avait une coquille dans l'énoncé : on demandait de montrer $P_{Z_p^\pm} = (X^p - 1) \wedge Q^\pm$, ce qui est faux lorsque $p \equiv 1 \pmod 4$, puisqu'alors $Q^\pm(1) = (p-1)/2 = 0 \in \mathbf{F}_2$, donc $X - 1$ divise $Q^\pm$, donc aussi le pgcd, alors qu'il ne divise pas $P_{Z_p^\pm}$. Toutes mes excuses !

et on peut calculer à la main

$$\begin{aligned} D^+(X) &= \Phi_{17} \wedge Q^+(X) = X^8 + X^7 + X^6 + X^4 + X^2 + X + 1 \\ D^-(X) &= \Phi_{17} \wedge Q^-(X) = X^8 + X^5 + X^4 + X^3 + 1. \end{aligned}$$

On a donc dans $\mathbf{F}_2[X]$

$$X^{17} - 1 = (X-1)(X^8 + X^7 + X^6 + X^4 + X^2 + X + 1)(X^8 + X^5 + X^4 + X^3 + 1).$$

Exercice 3. *Soit $K \hookrightarrow L$ une extension finie de corps.*

a) Si $K \neq L$ et que tout élément de $L - K$ est inséparable sur K, montrer que la caractéristique de K est un nombre premier p, que $[L:K]_s = 1$ et que $[L:K]$ est une puissance de p.

Le fait qu'il existe une extension finie non séparable de K entraîne par le cours que la caractéristique de K est un nombre premier p. Soit $x \in L - K$ et soit $P \in K[X]$ son polynôme minimal. Comme x est inséparable sur K, on peut écrire $P(X) = Q(X^p)$. Le polynôme Q est encore irréductible, et $Q(x^p) = 0$. C'est donc le polynôme minimal de x^p. Soit $x^p \in K$, soit on peut recommencer le processus. Il existe donc $n \geq 1$ tel que $a := x^{p^n} \in K$ et $P(X) = X^{p^n} - a$. Si Ω est une extension algébriquement close de K, tout prolongement de l'inclusion $K \subset \Omega$ en une injection $L \hookrightarrow \Omega$ doit envoyer x sur l'unique racine p^n-ième de a dans Ω. Il est donc unique et $[L:K]_s = 1$.

Pour montrer que $[L:K]$ est une puissance de p, on peut procéder par récurrence sur $[L:K]$. Comme $[K(x):K] = p^n$, il suffit de montrer que tout élément y de $L - K(x)$ est inséparable sur $K(x)$, pour pouvoir appliquer l'hypothèse de récurrence à l'extension $K(x) \subset L$. On vient de voir que le polynôme minimal de y sur K n'a donc qu'une seule racine dans un corps de décomposition ; il en est donc de même pour le polynôme minimal de y sur $K(x)$, qui est bien inséparable sur ce corps.

b) On revient au cas général. Montrer que $[L:K]_s$ divise $[L:K]$ et que soit le quotient est 1, soit la caractéristique de K un nombre premier p et le quotient est une puissance de p.

Soit $K \subset K^s \subset L$ la clôture séparable de K dans L. Il résulte du th. 5.17 du cours que soit $K^s = L$, auquel cas L est une extension séparable de K et $[L:K]_s = [L:K]$, soit l'extension $K^s \subset L$ vérifie les hypothèses de a). Dans le second cas, on a alors $[L:K^s]_s = 1$ et $[L:K^s] = p^n$, de sorte que

$$[L:K]/[L:K]_s = ([L:K^s][K^s:K])/([L:K^s]_s[K^s:K]_s) = [L:K^s] = p^n.$$

Exercice 4. *Soit $\overline{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$ et soit $a \in \overline{\mathbf{Q}} - \mathbf{Q}$.*

a) Montrer qu'il existe un sous-corps $K \subset \overline{\mathbf{Q}}$ tel que $a \notin K$ et que tout sous-corps de $\overline{\mathbf{Q}}$ contenant strictement K contient a ; on dit que K est un sous-corps de $\overline{\mathbf{Q}}$ maximal sans a.

On considère la famille $\mathscr{E}$ des sous-corps $K \subset \overline{\mathbf{Q}}$ tel que $a \notin K$. Elle est non vide car $\mathbf{Q}$ est dedans. Si $(K_i)_{i \in I}$ est une famille non vide totalement ordonnée d'éléments de $\mathscr{E}$, alors $\bigcup_{i \in I} K_i$ est encore un sous-corps de $\overline{\mathbf{Q}}$ qui ne contient pas a, donc c'est un majorant. L'existence d'un élément maximal de $\mathscr{E}$ résulte alors du lemme de Zorn.

b) On choisit un nombre premier p divisant $[K(a):K]$. Soit $K \subset L \subset \overline{\mathbf{Q}}$ une extension finie non triviale de K. On note M la clôture normale de L dans $\overline{\mathbf{Q}}$ et $G := \mathrm{Gal}(M/K)$. Montrer que p divise $[L:K]$.

Par maximalité de K, on a $a \in L$, donc $K(a) \subset L$ et $[K(a):K]$ divise $[L:K]$.

c) Montrer que $[L:K]$ est une puissance de p.

On pose $\mathrm{Card}(G) := mp^r$, avec $m \wedge p = 1$. Le théorème de Sylow nous dit qu'il existe un sous-groupe H de G d'indice m. Par la théorie de Galois, il correspond à une extension $K \subset M^H$ de degré m. Le point b) entraîne $m = 1$. On a donc $[M : K] = p^r$ et son diviseur $[L : K]$ est aussi une puissance de p.

d) Montrer que $[K(a) : K] = p$ et que $K(a)$ est la seule sous-extension de $K \subset \overline{\mathbf{Q}}$ de degré p sur K.

Le théorème de Sylow nous dit qu'il existe un sous-groupe H de G d'indice p, qui correspond par la théorie de Galois à une extension $K \subset M^H$ de degré p. Par maximalité de K, celle-ci doit contenir $K(a)$, donc $[K(a) : K] = p$. La seconde partie de la question résulte du fait que toute extension non triviale de K doit contenir $K(a)$.

e) Montrer que G est cyclique, puis que toute extension finie de K est galoisienne.

La question d) nous dit, avec la théorie de Galois, que G, de cardinal p^r, a un unique sous-groupe d'indice p ; notons-le H. Si $g \in G - H$, on peut appliquer le théorème de Sylow au sous-groupe $\langle g \rangle$ de G : s'il est distinct de G, il est contenu dans H, ce qui est absurde. Le groupe G est donc cyclique, engendré par g. Le reste résulte du fait que toute extension finie de K se plonge dans $\overline{\mathbf{Q}}$ (lemme 3.17) et que toute sous-extension d'une extension finie galoisienne cyclique est galoisienne cyclique.

f) Montrer qu'il existe $b \in K(a)$, avec $b^p \in K$, tel que $K(a) = K(b)$.

Cela résulte de la théorie de Kummer (th. 8.16 du cours), sous réserve que l'on sache montrer que toutes les racines p-ièmes de l'unité sont dans K. Or si ζ est une telle racine, on sait que $[K(\zeta) : K] \leq p - 1$, donc $K(\zeta) = K$ par b).