

Corrigé du deuxième contrôle continu, théorie des corps, avril 2024

Exercice 1 (a) E/K est dite normale si tout polynôme de $K[X]$ qui a une racine dans E est scindé sur E .

E/K est normale si et seulement si l'image de tout K -plongement de E dans une extension de E est E .

(Puisque E/K est finie) E/K est normale si et seulement s'il existe $P \in K[X]$ non constant tel que E est le corps de décomposition de P .

(b) K est algébriquement clos si tout polynôme $P \in K[X]$ non constant est scindé sur K .

(c) E est une clôture algébrique de K si E/K est une extension algébrique et E est algébriquement clos.

(d) Soit P le polynôme minimal de x sur K . Soit k le plus grand entier de \mathbb{N} tel que p^k divise toutes les puissances de X qui apparaissent avec un coefficient non nul dans P . Alors on peut écrire $P(X) = Q(X^{p^k})$, avec p qui ne divise pas toutes les puissances de X qui apparaissent avec un coefficient non nul dans Q . En particulier, la dérivée formelle de Q est non nulle. Mais Q est irréductible parce que P l'est. En effet, toute écriture $Q = UV$ avec $U, V \in K[X]$ implique une écriture $P(X) = U(X^{p^k})V(X^{p^k})$. Donc Q est le polynôme minimal de x^{p^k} , parce qu'en plus il est unitaire, comme P . Donc x^{p^k} a un polynôme minimal dont la dérivée formelle est non nulle, et il est donc séparable sur K d'après le cours.

Par exemple, si $P(X) = X^{p^2} + 1$, alors $k = 2$ et $Q(X) = X + 1$ et x^{p^2} est séparable sur K .

Exercice 2. Remarquons que $K \setminus A$ est non vide, puisque A est un ensemble fini et K est infini.

(a) Soit α une racine commune de \tilde{P} et Q dans \bar{E} . Alors il existe j tel que $\alpha = y_j$ (α racine de Q). De plus (parce que α racine de \tilde{P}), il existe i tel que $z - u\alpha = x_i$. Alors $x + uy - uy_j = x_i$, d'où $x - x_i = u(y_j - y)$. Si $y \neq y_j$, alors $u = -\frac{x_i - x}{y_j - y}$ appartient à A – impossible. Donc $y = y_j$. Donc, s'il y a une racine commune α , il s'agit de y . Réciproquement, y est une racine commune, car $\tilde{P}(y) = P(x)$.

(b) Par (a), le pgcd unitaire de \tilde{P} et Q dans $\bar{E}[X]$ est de la forme $(X - y)^k$ avec $k \geq 1$, mais y est racine simple de Q qui est séparable par l'énoncé, donc le pgcd unitaire de \tilde{P} et Q dans $\bar{E}[X]$ est $X - y$.

On a $Q \in K[X] \subset K'[X]$, et $\tilde{P} \in K'[X]$ parce que $P \in K[X]$. Soit D le pgcd unitaire de \tilde{P} et Q dans $K'[X]$ où ils sont tous les deux définis. Alors on sait que c'est un pgcd dans $\bar{E}[X]$ également. $X - y$ étant unitaire, on a $D(X) = X - y$.

(c) Par (c), on a $y \in K'$ parce que y est un coefficient d'un polynôme à coefficients dans K' . Mais K' contient $z = x + uy$, donc K' contient aussi x s'il contient y . Donc K' contient K , x et y , ce qui prouve $K' = E$.

(d) $x = \sqrt[3]{2}$, $y = j\sqrt[3]{2}$, $x + y = (1 + j)\sqrt[3]{2}$. Alors $E = \mathbb{Q}(x, y) = \mathbb{Q}(j, \sqrt[3]{2})$ est de degré 6 sur \mathbb{Q} . Or, $1 + j = -j^2$, donc $K(x + y) = K(j^2\sqrt[3]{2})$ et ce corps est une extension de degré 3 de \mathbb{Q} parce qu'il est engendré par une racine de $X^3 - 2$, tout comme $K(x)$ et $K(y)$. Aucun des trois corps $K(x)$, $K(y)$ et $K(x + y)$ n'est égal à E .