

Corrigé du premier contrôle continu, théorie des corps, mars 2024

Exercice 1. (a) Puisque $\sqrt{2} \notin \mathbb{Q}$, la dimension est au moins 2. Puisque $\sqrt{2}$ annule $X^2 - 2$, le polynôme minimal de $\sqrt{2}$ est de degré au plus 2, donc $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \leq 2$. Donc $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

(b) Puisque $i \notin \mathbb{R}$, on a $i \notin \mathbb{Q}(\sqrt{2})$. Mais i annule $X^2 + 1$. Par le même raisonnement que (a), on a $[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})] = 2$, donc $[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}] = 4$ par le théorème de la base télescopique.

(c) Posons $K := \mathbb{Q}(\sqrt[13]{5}, \sqrt[5]{13})$.

Les polynômes $P(X) = X^{13} - 5$ et $Q(X) = X^5 - 13$ sont irréductibles par le critère d'Eisenstein. Donc $\mathbb{Q}(\sqrt[13]{5})$ qui est un corps de rupture de P est de dimension 13 sur $\mathbb{Q}$, tandis que $\mathbb{Q}(\sqrt[5]{13})$ qui est un corps de rupture de Q est de dimension 5 sur $\mathbb{Q}$. On a $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[13]{5})][\mathbb{Q}(\sqrt[13]{5}) : \mathbb{Q}]$ donc $[K : \mathbb{Q}]$ est divisible par 13, et $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[5]{13})][\mathbb{Q}(\sqrt[5]{13}) : \mathbb{Q}]$ donc $[K : \mathbb{Q}]$ est divisible par 5. Comme 13 et 5 sont premiers entre eux, $[K : \mathbb{Q}]$ est divisible par leur produit qui est 65. Par ailleurs, en utilisant $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[13]{5})][\mathbb{Q}(\sqrt[13]{5}) : \mathbb{Q}]$, on voit que $[K : \mathbb{Q}]$ est inférieur ou égal à 65, parce que $[K : \mathbb{Q}(\sqrt[13]{5})]$ est inférieur ou égal à 5. En effet, le degré de $K/\mathbb{Q}(\sqrt[13]{5})$ est égal au degré du polynôme minimal de $\sqrt[5]{13}$ sur $\mathbb{Q}(\sqrt[13]{5})$. Ce polynôme divise polynôme minimal de $\sqrt[5]{13}$ sur $\mathbb{Q}$ qui est Q et est de degré 5.

Exercice 2. (a) Puisque P et Q sont premiers entre eux dans $\mathbb{Q}[X]$, il existe $U, V \in \mathbb{Q}[X]$ tels que $UP + VQ = 1$. Tout diviseur commun de P et Q dans $\mathbb{C}[X]$ divise alors 1 dans $\mathbb{C}[X]$, c'est donc une constante.

(b) P a une décomposition en produit de polynômes irréductibles sur $\mathbb{Q}$, $P(X) = \prod_{i=1}^k P_i^{a_i}$. Alors $\prod_{i=1}^k P_i$ est un polynôme de $\mathbb{Q}[X]$ qui a les mêmes racines $z_1, z_2, \dots, z_n$ que P . Mais les racines de ce produit sont de multiplicité 1 parce qu'un polynôme irréductible de $\mathbb{Q}[X]$ a des racines simples dans $\mathbb{C}$ (il ne peut pas avoir de racine commune avec son polynôme dérivé vu qu'ils sont premiers entre eux), et parce que si $i \neq j$ alors P_i et P_j n'ont aucune racine commune dans $\mathbb{C}$ par (a) puisqu'ils sont premiers entre eux. Donc le produit $\prod_{i=1}^k P_i$ est égal à $\prod_{i=1}^n (X - z_i)$.

Exercice 3. (a) Soit E/K une extension de degré 2. Fixons $u \in E \setminus K$. Alors $K \subsetneq K(u) \subset E$, donc $K(u) = E$. Alors le polynôme minimal de u sur K est de la forme $X^2 + bX + c$ qui s'écrit parce que 2 est inversible $(X + \frac{b}{2})^2 - \Delta$, où $\Delta := \frac{b^2 - 4c}{4}$. On a $\Delta = (u + \frac{b}{2})^2$ donc $\sqrt{\Delta} = \pm(u + \frac{b}{2})$ dans E . Alors $K(\sqrt{\Delta})$ contient u , c'est donc E (donc notre Δ est le x de l'énoncé).

(b) $x^2 = y^2$ ssi $(x - y)^2 = 0$ ssi $x = y$. Donc l'application est injective. Comme K est fini, elle est bijective. Donc tout élément x de K a une racine carrée u dans K . De plus, il ne peut pas avoir une autre dans une extension parce que $x^2 = y^2$ implique $x = y$, que ce soit dans K ou dans une extension. Donc, si $x \in K$, $K(\sqrt{x}) = K$, donc pas d'extension quadratique de ce type.

(c) On pose $E := \mathbb{F}_2(t)$ et K son sous-corps $\mathbb{F}_2(t^2)$. On a $E = K(\sqrt{t^2})$. Montrons que E/K est de degré 2. Elle est de degré au moins 2, parce que $t \notin \mathbb{F}_2(t^2)$. En effet, les éléments non nuls de $\mathbb{F}_2(t^2)$ s'écrivent $P(t^2)/Q(t^2)$ avec $P, Q \neq 0$, et $P(t^2)/Q(t^2) = t$ implique $P(t^2) = tQ(t^2)$ ce qui est impossible parce qu'à gauche on a un polynôme de degré impair et à droite un polynôme de degré pair. Mais aussi E/K est de degré au plus 2 parce que c'est une extension monogène engendrée par t , et elle a le degré du polynôme minimal de t , qui divise $X^2 - t^2 \in K[X]$.

Exercice 4. $E = \mathbb{Q}(i, \sqrt[4]{2})$ (parce qu'il contient $\sqrt[4]{2}$ et $i\sqrt[4]{2}$, donc il contient i et $\sqrt[4]{2}$, puis un corps qui contient ces deux-là contient toutes les racines). La dimension est $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$. Le premier crochet vaut 2 parce que i n'est pas réel donc n'appartient pas à $\mathbb{Q}(\sqrt[4]{2})$, et le deuxième vaut 4 parce que $X^4 - 2$ est irréductible sur $\mathbb{Q}$ par Eisenstein et $\sqrt[4]{2}$ est une racine de ce polynôme. La réponse finale est 8.

Exercice 5. Supposons que E/K est algébrique. Soit $\frac{P}{Q}$ un élément de $E(t)$, avec $P, Q \in E[t]$. Les coefficients de P et Q se trouvent dans E , donc ils sont algébriques sur K . Alors ils sont algébriques sur $K(t)$. Ils engendrent une extension algébrique de $K(t)$. Cette extension contient $\frac{P}{Q}$, parce qu'elle contient

t et les coefficients de P et de Q . Donc $\frac{P}{Q}$ est algébrique sur $K(t)$. Donc tous les éléments de $E(t)$ sont algébriques sur $K(t)$.

Supposons que $E(t)/K(t)$ est algébrique. Soit $x \in E$. Alors x est algébrique sur $K(t)$ donc il existe un polynôme non nul à coefficients dans $K(t)$ qui s'annule en x . Les coefficients du polynôme sont des fractions rationnelles en t . Quitte à multiplier par les dénominateurs, on obtient une relation non triviale $\sum_{k=0}^n P_k x^k = 0$, avec $P_k \in K[t]$. Quitte à passer le pgcd des P_k en facteur et à simplifier par lui parce que $K[t]$ est intègre, on peut supposer que les P_k sont premiers entre eux dans leur ensemble. Alors ils ne sont pas tous divisibles par t . Ainsi dans la relation $\sum_{k=0}^n P_k(0)x^k = 0$ (obtenue à partir de $\sum_{k=0}^n P_k x^k = 0$) tous les $P_k(0)$ ne sont pas nuls¹. Nous tenons un polynôme non nul à coefficients dans K qui s'annule en x . Donc x est algébrique sur K . (Remarque : au lieu de simplifier par le pgcd, il suffisait de simplifier par une puissance de t , la plus grande qui divise tous les P_k .)

1. On a utilisé que, si un polynôme est le polynôme nul, la fonction polynomiale associée est nulle. C'est la réciproque qui peut poser problème sur les corps finis