

# Corrigé, premier contrôle continu, théorie des corps, mars 2025

Durée : 3 heures

**Exercice 1.** (a) Tout sous-anneau de  $E$  qui contient  $A$  et  $B$  contient tout produit  $ab$  et toute somme comme dans la définition de  $\mathcal{X}(A, B)$ , il contient donc  $\mathcal{X}(A, B)$ .

(b) Soit  $x \in \mathcal{X}(A, B) \setminus \{0\}$ . Comme  $x \in E$  et  $E$  est de dimension finie,  $x$  est algébrique sur  $K$ . Soit  $P$  le polynôme minimal de  $x$ . On écrit  $P(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$ . On a  $a_0 \neq 0$ , parce que  $P$  est irréductible et  $x$  est non nul (le seul polynôme unitaire irréductible divisible par  $X$  est  $X$ ). On écrit  $P(x) = 0$ , on multiplie par  $x^{-1}$  qui est un élément de  $E$ , et on trouve  $-a_0 x^{-1} = x^{n-1} + \sum_{i=1}^{n-1} a_i x^{i-1}$ . Puisque  $a_0$  est inversible dans  $K$ , on a trouvé que l'élément  $x^{-1}$  de  $E$  est égal à un polynôme à coefficients dans  $K$  de  $x$ . Comme  $K \subset \mathcal{X}(A, B)$  et  $x \in \mathcal{X}(A, B)$  et  $\mathcal{X}(A, B)$  est un anneau, on a  $x^{-1} \in \mathcal{X}(A, B)$ . Donc tout élément non nul de cet anneau (commutatif) est inversible dans l'anneau, donc cet anneau est un corps.

(c) Soit  $(x_1, x_2, \dots, x_n)$  une base de  $A$  sur  $K$ . Alors c'est une famille génératrice de  $AB$  sur  $B$ . En effet, on écrit un élément de  $AB$  sous la forme  $\sum a_i b_i = \sum (\sum \lambda_j x_j) b_i$  et ceci est une combinaison linéaire des  $x_j$  à coefficients dans  $B$  car  $\lambda_j \in K$  et  $b_i \in B$ .

(d) Supposons qu'une base  $X$  de  $A$  sur  $K$  est une base de  $AB$  sur  $B$ . Alors  $[AB : B] = [A : K]$ . On en déduit  $[AB : K] = [AB : B][B : K] = [A : K][B : K]$ .

Réciproquement, supposons que  $[AB : B] = [A : K]$ . On a vu qu'une base  $Y$  de  $A$  sur  $K$  était une famille génératrice de  $AB$  sur  $B$ . Or, on a  $[AB : K] = [AB : B][B : K] = [A : K][B : K]$ . (La première égalité par le théorème de la base télescopique, la seconde par l'énoncé présent.) Donc  $[AB : B] = [A : K]$ . Alors le cardinal de la famille  $Y$  génératrice sur  $B$  (voir (c)) est égal à  $[A : K]$  parce que c'est une base de  $A$  sur  $K$ , donc à  $[AB : B]$  par ce qu'on vient de voir, et donc cette famille est une base de  $AB$  sur  $B$  parce qu'on est en dimension finie et toute famille génératrice de cardinal égal à la dimension de l'espace est une base.

**Exercice 2.** Je pose  $z := e^{\frac{2i\pi}{n}}$ . Alors on a  $z + z^{-1} = 2 \cos(\frac{2\pi}{n})$ . Donc  $\cos(\frac{2\pi}{n}) \in \mathbb{Q}(z)$ , donc  $\mathbb{Q}(\cos(\frac{2\pi}{n})) \subset \mathbb{Q}(z) \cap \mathbb{R}$ .

Montrons l'autre inclusion. On remarque que  $z \notin \mathbb{R}$ , et donc  $[\mathbb{Q}(z) : (\mathbb{Q}(z) \cap \mathbb{R})] \geq 2$ . Mais  $[\mathbb{Q}(z) : \mathbb{Q}(\cos(\frac{2\pi}{n}))] \leq 2$ , parce que  $i \sin(\frac{2\pi}{n})$  annule le polynôme  $X^2 + \cos^2(\frac{2\pi}{n})$  à coefficients dans  $\mathbb{Q}(\cos(\frac{2\pi}{n}))$ . Puisque nous avons montré  $\mathbb{Q}(\cos(\frac{2\pi}{n})) \subset (\mathbb{Q}(z) \cap \mathbb{R})$ , on en déduit que ces corps sont égaux.

On sait par le cours que  $\mathbb{Q}(z)$  est de degré  $\phi(n)$  sur  $\mathbb{Q}$ . Comme, au passage, on a montré que  $\mathbb{Q}(z)$  était de degré 2 sur  $\mathbb{Q}(\cos(\frac{2\pi}{n}))$ , on a par le théorème de la base télescopique que  $\mathbb{Q}(\cos(\frac{2\pi}{n}))$  est de degré  $\frac{\phi(n)}{2}$  sur  $\mathbb{Q}$ . Donc le degré du polynôme minimal de  $\cos(\frac{2\pi}{n})$  sur  $\mathbb{Q}$  est  $\frac{\phi(n)}{2}$ .

**Exercice 3.** Je pose  $y := \sqrt[4]{2}$ . Il est facile de constater que le corps de décomposition de  $X^4 - 2$  sur  $\mathbb{Q}$  est  $\mathbb{Q}(y, i)$ . Or, si on pose  $u := e^{\frac{2i\pi}{8}} = \frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}}$  de sorte que  $u^4 = -1$ , alors les racines de  $X^4 + 2$  sont  $\pm uy$  et  $\pm iuy$ . Donc le corps de décomposition de  $X^4 + 2$  est  $\mathbb{Q}(y, u)$  (parce que  $u^2 = i$ ).

Puisque  $\sqrt{2} = y^2 \in \mathbb{Q}(y, i)$ , on a  $u \in \mathbb{Q}(y, i)$  et donc  $\mathbb{Q}(y, u) \subset \mathbb{Q}(y, i)$ . Comme  $i = u^2 \in \mathbb{Q}(y, u)$ , on a  $\mathbb{Q}(y, i) \subset \mathbb{Q}(y, u)$ . D'où l'égalité cherchée par double inclusion.

**Exercice 4.** (a) Soit  $E/\mathbb{Q}$  une extension de degré 2, avec  $E \subset \mathbb{C}$ . Soit  $x \in E \setminus \mathbb{Q}$ . Alors  $E = \mathbb{Q}(x)$  par les dimensions. Le polynôme minimal de  $x$  sur  $\mathbb{Q}$  est de la forme  $X^2 + aX + b$ . Donc  $x$  est égal à  $u + v\sqrt{\Delta}$  avec  $u, v \in \mathbb{Q}$  et  $\Delta$  le discriminant de l'équation. Il est facile de vérifier que  $x \in \mathbb{Q}(\sqrt{\Delta})$  et  $\sqrt{\Delta} \in \mathbb{Q}(x)$ , donc  $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{\Delta})$ .

(b1) On se ramène à résoudre

$$8 \cos^3\left(\frac{2k\pi}{9}\right) - 6 \cos\left(\frac{2k\pi}{9}\right) + 1 = 0$$

et  $8 \cos^3\left(\frac{2k\pi}{9}\right) - 6 \cos\left(\frac{2k\pi}{9}\right) = 2 \cos\left(\frac{2k\pi}{3}\right)$ , on doit résoudre  $2 \cos\left(\frac{2k\pi}{3}\right) = -1$ . Or,  $\cos\left(\frac{2\pi}{3}\right) = -\frac{1}{2}$ . On trouve  $\frac{2k\pi}{3} \in \left\{\frac{2\pi}{3}, \frac{2\pi}{3} + 2\pi, \frac{2\pi}{3} + 4\pi\right\}$ .

On trouve  $k = 1, 4, 7$ . Mais on peut remplacer le 7 par 2.

(b2) Par la formule de  $\cos(2\theta)$ , on trouve que  $D = \mathbb{Q}(\cos(\frac{2\pi}{9}))$ , parce que les deux autres racines y appartiennent. De plus, le polynôme est irréductible (il est de degré 3 et si on cherche une racine dans  $\mathbb{Q}$  on voit par des divisibilités qu'il devrait s'agir de 1 ou  $-1$ ). Donc  $[D : \mathbb{Q}] = \deg(P) = 3$ . Et, par la théorie des extensions monogènes (car  $D/\mathbb{Q}$  est monogène), le nombre de  $\mathbb{Q}$ -automorphismes de  $E$  est égal au nombre de racines de  $P$  dans  $D$ , qui est 3.

(b3) Supposons que  $D = \mathbb{Q}(\sqrt[3]{x})$ . Comme l'extension est monogène, le polynôme minimal de  $\sqrt[3]{x}$  est de degré 3. Le polynôme  $X^3 - x$  est unitaire de degré 3 et s'annule en  $\sqrt[3]{x}$ ; c'est donc le polynôme minimal cherché. Par la théorie des extensions monogènes, le nombre des  $\mathbb{Q}$ -automorphismes de  $D$  est égal au nombre de racines de  $X^3 - x$  dans  $D$ . Mais  $D$  est inclus dans  $\mathbb{R}$ , donc le polynôme  $X^3 - x$  a une seule racine dans  $D$ . Contradiction avec (b2).

**Exercice 5.** Si  $P$  est scindé sur  $E$ ,  $E$  contient une racine  $x$  de  $P$ , donc  $K(x)$  qui est un corps de rupture de  $P$ , donc  $\deg(P) = [K(x) : K]$  divise  $[E : K]$  par le théorème de la base télescopique.

Réciproque : supposons que  $n$  divise  $[E : K]$ . Alors  $E$  contient un corps  $K'$  qui est une extension de degré  $n$  de  $K$  (cours). Il suffit donc de montrer que  $P$  est scindé sur toute extension de  $K$  de degré  $n$ . Mais elle sont toutes isomorphes entre elles (cours), donc à  $K[X]/(P)$ . Il suffit donc de montrer que  $P$  est scindé sur  $K' := K[X]/(P)$ . Or,  $K'$  contient une racine  $x$  de  $P$ . Alors  $x$  annule  $x^{|K'|} - X$ . Donc  $P$ , qui est le polynôme minimal de  $x$ , divise  $X^{|K'|} - X$ . Or, ce dernier est scindé sur  $K'$  (cours; facile). Donc  $P$  aussi.

(b) Soient  $P_1$  et  $P_2$  deux polynômes unitaires qui divisent  $P$  dans  $E[X]$ . Soit  $E'$  un corps de rupture de  $P_1$  sur  $E$ . Alors  $P_1$  a une racine  $x$  dans  $E'$ .  $x$  annule alors  $P$ . Donc  $P$  est le polynôme minimal de  $x$  sur  $K$ . Donc  $P$  divise  $X^{|E'|} - X$  qui s'annule en  $x$ . Donc  $P$  est scindé sur  $E'$ , parce que  $X^{|E'|} - X$  l'est. Donc  $P_2$  est scindé sur  $E'$ . Donc  $\deg(P_2)$  divise  $[E' : E]$  parce que  $E'$  contient un corps de rupture de  $P_2$ . Or,  $[E' : E] = \deg(P_1)$ . Nous avons prouvé que  $\deg(P_2) | \deg(P_1)$ . Par le même procédé on montre que  $\deg(P_1) | \deg(P_2)$ . D'où l'égalité.