

Corrigé du deuxième contrôle continu, avril 2025

Durée : 3 heures

Exercice 1. Soit $P \in K[X]$ un polynôme irréductible qui a une racine x dans E . Alors x appartient à l'un des L_i . Alors P est scindé sur L_i parce que L_i/K est normale. Donc P est scindé sur E .

Exercice 2. Notons f l'endomorphisme. Un morphisme de corps est toujours injectif, son noyau étant un idéal propre du corps de départ, donc égal forcément à $\{0\}$. Nous voulons montrer que f est surjectif. Soit x dans E . On veut montrer que x appartient à l'image de f . Soit P le polynôme minimal de x . Soient $x_1 = x, x_2, \dots, x_k$ les racines (distinctes) de P dans E . Comme f envoie une racine de P sur une racine de P , f induit une application h de $\{x_1, x_2, \dots, x_k\}$ dans lui-même. Comme f est injectif, h est injectif. Alors h est bijectif, parce que entre deux ensembles de même cardinal fini. Donc x est dans l'image de h . Donc x est dans l'image de f .

Exercice 3. Soit $P \in K[X]$ irréductible, tel que P a une racine x dans L . Alors P est scindé sur E parce que E/K est normale. Si, par l'absurde, P n'est pas scindé sur L , alors P a une racine y dans E qui n'appartient pas à L . Soit \bar{E} une clôture algébrique de E . Il existe un K -morphisme $u : K(x) \rightarrow \bar{E}$ qui envoie x sur y (théorème de plongement des extensions monogènes). Alors u se prolonge à un K -plongement v de E dans \bar{E} par le théorème de prolongement. L'image de v est E parce que E/K est normale. Donc v induit un automorphisme f de E . On a $f(L) = L$ par l'énoncé. Mais cela contredit le fait que $x \in L$, $f(x) = y$ et $y \notin L$.

Exercice 4. Je pose $x := \sqrt{2 + \sqrt{2}}$. x annule le polynôme $P(X) = (X^2 - 2)^2 - 2 = X^4 - 4X^2 + 2$. Les autres racines de P sont de la forme $\pm\sqrt{2} \pm \sqrt{2}$, comme on peut le vérifier rapidement sur la formule $P(X) = (X^2 - 2)^2 - 2$. Si les quatre racines appartiennent à $\mathbb{Q}(x)$, alors $\mathbb{Q}(x)$ est un corps de décomposition de P et donc $\mathbb{Q}(x)/\mathbb{Q}$ est normale. Or, on a $x^2 \in \mathbb{Q}(x)$, d'où $\sqrt{2} \in x$. On a aussi $\sqrt{2} - \sqrt{2} = \sqrt{2}x^{-1}$, donc $\sqrt{2} - \sqrt{2} \in \mathbb{Q}(x)$. Il est clair alors que les quatre racines de P se trouvent dans $\mathbb{Q}(x)$. (Noter qu'on n'a pas eu besoin de savoir si P est irréductible ou pas.)

On pose $z := \sqrt{3 + \sqrt{3}}$. Il annule le polynôme $Q(X) := (X^2 - 3)^2 - 3$. Cette formule montre qu'on a $Q(X) = X^4 - 6X^2 + 6$ et que les racines de Q sont $\pm\sqrt{3} \pm \sqrt{3}$. De plus, Q est irréductible par le critère d'Eisenstein appliqué à 2, donc l'extension $\mathbb{Q}(z)/\mathbb{Q}$ est de degré 4.

Notons que $\mathbb{Q}(z)$ contient z^2 , donc $\sqrt{3}$. Posons $z' := \sqrt{3} - \sqrt{3}$. On suppose par l'absurde que $z' \in \mathbb{Q}(z)$. Alors $zz' = \sqrt{6} \in \mathbb{Q}(z)$ et donc $\sqrt{2} \in \mathbb{Q}(z)$ parce que $\sqrt{3} \in \mathbb{Q}(z)$. Puisque $\mathbb{Q}(\sqrt{3}, \sqrt{2})/\mathbb{Q}$ est de degré 4, on a alors $\mathbb{Q}(z) = \mathbb{Q}(\sqrt{3}, \sqrt{2})$.

En posant cet exercice, j'étais conscient qu'à partir d'ici il est difficile à conclure; c'était pour tester votre capacité d'aller jusqu'au bout sans vous décourager parce que l'exercice ne tombe pas après une première étape. De plus, la difficulté de montrer que $\sqrt{2}$ n'appartient pas à $\mathbb{Q}(z)$ illustre l'intérêt de la théorie de Galois (vue après) qui montre ici que les groupes de Galois de ces extensions sont différents, donc il ne s'agit pas de la même extension. Cette approche montre la différence profonde entre les deux types d'extensions. Il s'agit de celles qui ont un groupe cyclique versus celles qui ont un groupe isomorphe au groupe de Klein.

Suite de la preuve :

Un élément de cette dernière peut s'écrire de façon unique $u + v\sqrt{2}$, avec $u, v \in \mathbb{Q}(\sqrt{3})$. Mais alors on peut écrire $z = u + v\sqrt{2}$, et en prenant le carré on trouve $2uv\sqrt{2} \in \mathbb{Q}(\sqrt{3})$. On en déduit que $uv = 0$ donc u ou v est nul. Si v est nul, on a $z = u$, donc $z \in \mathbb{Q}(\sqrt{3})$, donc $\mathbb{Q}(z)/\mathbb{Q}$ est de degré

au plus 2, contradiction. Donc $z = v\sqrt{2}$, avec $v \in \mathbb{Q}(\sqrt{3})$. Par le même type de raisonnement, $z' = v'\sqrt{2}$ avec $v' \in \mathbb{Q}(\sqrt{3})$. Alors $zz' \in \mathbb{Q}(\sqrt{3})$. Mais $zz' = \sqrt{6}$. Donc $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$. Contradiction.

Autre preuve : par le polynôme minimal de z sur $\mathbb{Q}(\sqrt{2})$, qui est unitaire, de degré 2, et divise $Q(X) = (X - z)(X - z')(X + z)(X + z')$.

Exercice 5. Supposons par l'absurde que $E \neq K(x)$. Soit $y \in E \setminus K(x)$. Alors le polynôme minimal de y sur $K(x)$ est de degré au moins 2, et comme il est séparable par l'énoncé, il a une racine z dans \bar{E} différente de y . Soit $f : K(x) \rightarrow \bar{E}$ le morphisme qui envoie t sur t (qui induit $Id_{K(x)}$). Alors f se prolonge à $K(x)(y)$ par $f(y) = z$ (théorème de plongement des extensions monogènes). Et le nouveau f se prolonge à un plongement de E dans \bar{E} . Or, ce plongement n'est pas l'identité sur E parce qu'il envoie y sur z , mais il envoie x sur x ce qui contredit l'énoncé.