UNIVERSITÉ D'ARTOIS
FACULTÉ DES SCIENCES JEAN PERRIN

ANNÉE UNIVERSITAIRE 2016-2017
LICENCE 3 MATHS

THÉORIE DE GALOIS

FICHE I : EXTENSIONS DE CORPS

Exercice 1. Soit $P = aX^2 + bX + c$ un polynôme de degré 2 dans $K[X]$ où K est un corps. Montrer l'équivalence des points suivants :

(1) P n'est pas irréductible ;

(2) P a une racine dans K ;

(3) P a deux racines (ou une racine double) dans K ;

(4) Le discriminant $\Delta = b^2 - 4ac$ est un carré dans K.

Exercice 2. Soit $P = \sum_{i=0}^{n} a_i X^i$ un polynôme dans $\mathbb{Z}[X]$. Soit une racine de P dans $\mathbb{Q}$ écrite $\frac{p}{q}$ avec p et q premiers entre eux. Montrer que p divise a_0 et q divise a_n. Application : montrer que le polynôme $4X^3 - 4X + 7$ n'a pas de racine dans $\mathbb{Q}$. Est-il irréductible sur $\mathbb{Q}$?

Exercice 3. Fabriquer une famille de polynômes de tous degrés irréductibles sur $\mathbb{Q}$, soit à la main, soit par le critère d'Eisenstein.

Exercice 4. Soit p un nombre premier. Vérifier l'irréducibilité du polynôme cyclotomique $1 + X + \cdots + X^{p-1}$ en effectuant un changement de variables $X = Y + 1$ et en utilisant un critère bien connu. (On rappelle que p est premier si et seulement s'il divise $\binom{p}{i}$ pour $1 \leq i \leq p-1$.)

Exercice 5. Déterminer si les polynômes $X^n - X - 1$ pour $n = 2, 3, 4$ et 5 sont irréductibles sur $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.

Exercice 6. Soient m et n dans $\mathbb{N}$. Montrer que $X^m - 1$ divise $X^{mn} - 1$ en se plaçant dans un quotient approprié.

Exercice 7. Dans chacun des cas suivants, déterminer si l'anneau quotient est un corps ou pas.

(1) $\mathbb{Q}[X]/(X - 1)$;

(2) $\mathbb{Q}[X]/(X^2 + 2)$;

(3) $\mathbb{R}[X]/(X^2 - 1)$;

(4) $\mathbb{R}[X]/(X^2 + 1)$.

Dans les cas où c'est un corps, déterminer si (la classe de) X et de $X^2 + 1$ sont inversible, et trouver leurs inverses le cas échéant.

Exercice 8. Le but de cet exercice est de montrer que quand p est premier, le polynôme $X^p - X - 1$ est irréductible sur $\mathbb{Q}$.

(1) On considère son image dans $\mathbb{F}_p[X]$. Montrer qu'il n'a pas de racine dans $\mathbb{F}_p$.

(2) Soit α une racine de $X^p - X - 1$ dans une extension de $\mathbb{F}_p$. Montrer que $\alpha + 1$ est encore racine.

(3) En déduire la décomposition de $X^p - X - 1$ sur $\mathbb{F}_p(\alpha)$.

(4) En déduire qu'il est irréductible sur $\mathbb{F}_p$, puis sur $\mathbb{Q}$. On pourra considérer la somme des racines d'un éventuel facteur.

Exercice 9. On considère la sous-algèbre $\mathbb{Q}[i]$ de $\mathbb{C}$. Est-ce un corps ? La décrire comme un quotient d'un anneau de polynômes (i.e. donner un isomorphisme $\mathbb{Q}[X]/(P) \to \mathbb{Q}(i)$ pour un certain P).

Exercice 10. On considère la sous-algèbre $\mathbb{Q}[\sqrt{2}]$ de $\mathbb{C}$.

(1) La décrire comme un quotient d'un anneau de polynômes. À quelle condition l'élément $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$ est-il inversible ? Donner alors son inverse, sous la même forme.

(2) La sous-algèbre $\mathbb{Q}[\sqrt{2}]$ est-elle un corps ?

(3) Existe-t-il un morphisme de corps de $\mathbb{Q}(\sqrt{2})$ dans lui-même qui envoie $\sqrt{2}$ sur $-\sqrt{2}$?

(4) Trouver tous les morphismes de corps de $\mathbb{Q}(\sqrt{2})$ dans lui-même.

Exercice 11. Existe-t-il un morphisme de corps de $\mathbb{C}$ dans lui-même qui envoie $\sqrt{2}$ sur $\sqrt{3}$?

Exercice 12. Soit α une racine complexe du polynôme $X^5 + 2X + 2$. Exprimer sous forme d'un polynôme en α de degré ≤ 4 à coefficients dans $\mathbb{Q}$ les nombres : $(\alpha^3 + 1)(\alpha^2 - 5)$, α^{-1} et $\frac{\alpha^2+1}{\alpha+3}$.

Exercice 13. Une extension est dite *quadratique* si elle est de degré 2. Soit E/K une telle extension.

(1) Soit e un élément de E hors de (l'image de) K, de polynôme minimal P. Montrer que P est de degré 2, et qu'on a alors un isomorphisme $E \simeq K[X]/(P)$.

(2) Montrer que pour tout élément e de E hors de K, on a $E = K[e] = K(e)$.

(3) Montrer que si $\mathrm{car}(K) \neq 2$, alors on peut trouver $\alpha \in E$ tel que $E = K(\alpha)$ et $\alpha^2 \in K$. On utilise la notation $E = K(\sqrt{d})$ si $\alpha^2 = d$.

(4) Montrer que si $K = \mathbb{Q}$, alors il existe un unique entier d sans facteur carré tel que $E = \mathbb{Q}(\sqrt{d})$.

Exercice 14. Montrer que toute extension quadratique de $\mathbb{R}$ est isomorphe à $\mathbb{C}$.

Exercice 15. Soit L/K une extension. Montrer que deux polynômes irréductibles (unitaires) différents de $K[X]$ ne peuvent avoir de facteur commun non trivial dans $L[X]$. En déduire qu'ils ne peuvent avoir de racine commune dans L.

Exercice 16. Montrer qu'une extension finie L/K de degré premier n'a pas de sous-extension autre que K et L.

Exercice 17. Soit K E, F et L des corps tels que $K \subseteq E \subseteq L$ et $K \subseteq F \subseteq L$. On note EF le plus petit sous-corps de L contenant E et F.

(1) Montrer que si E et F sont finies, alors EF est aussi la sous-K-algèbre de L engendrée par les éléments de E et de F, autrement dit que celle-ci est bien un corps.

(2) Toujours si E et F sont finies, montrer qu'il en est de même de EF et qu'on a $[EF : K] \leq [E : K][F : K]$, avec égalité si $[E : K]$ et $[F : K]$ sont premiers entre eux.

Exercice 18. Calculer $[\mathbb{Q}(j, \sqrt[5]{2}) : \mathbb{Q}]$ et montrer que $\mathbb{Q}(j)$ est le seul sous-corps de $\mathbb{Q}(j, \sqrt[5]{2}]$ de degré 2 sur $\mathbb{Q}$.

Exercice 19. Soit K un corps et soit $P \in K[X]$ un polynôme irréductible de degré p premier impair. Soit a une racine de P dans un extension de K.

(1) Quel est le polynôme minimal de a sur K ?

(2) Soit $b = a + 1/a$. Montrer que $K(b) = K(a)$.

Exercice 20. Quel est le degré de $\mathbb{Q}(\sqrt[3]{5})$?

Exercice 21. Comparer les extensions de $\mathbb{Q}$ dans $\mathbb{C}$ de la forme $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$, et $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. De quelles extensions l'élément $\sqrt{2} - \sqrt{3}$ fait-il partie ?

Exercice 22. L'élément $\sqrt{2 + \sqrt{2}} + \sqrt[3]{5}$ est il algébrique sur $\mathbb{Q}$?

Exercice 23. Soit K un corps, $a \in K$, et m, n deux entiers premiers entre eux. Le but de cet exercice est de montrer que $X^{mn} - a$ est irréductible sur K si et seulement si $X^n - a$ et $X^m - a$ sont irréductibles sur K.

(1) Montrer que $X^{mn} - a$ irréductible implique $X^n - a$ et $X^m - a$ irréductibles.

(2) Pour montrer l'implication réciproque, supposons que P est un facteur irréductible de $X^{mn} - a$ et considérons l'extension $L = K[X]/(P)$. Fabriquer un morphisme de $K[X]/(X^n - a)$ vers L (resp. de $K[X]/(X^m - a)$ vers L).

(3) En déduire que m et n divisent le degré de P, et conclure.