Algèbre II

Examen du 13 janvier 2017. Durée 3h00.
Seul document autorisé : le poly du cours. Smartphones éteints.

Exercice 1. i. Soit $f = X^{10} + X^5 + 1$. Décrire le groupe de Galois de f et l'ensemble ordonné (par inclusion) des sous-extensions de son corps de décomposition.

ii. Trouver un élément primitif du corps de décomposition de $X^5 - 3$ sur $\mathbb{Q}$.

iii. Soit A un anneau factoriel et $f \in A[X]$ irréductible et de terme constant irréductible dans A. Soit α une racine de f dans une clôture algébrique $\overline{K}$ du corps des fractions de A. Montrer que α engendre un idéal premier du sous-anneau $A[\alpha]$ de $\overline{K}$.

Exercice 2. Soit k un corps et $\overline{k}$ une clôture algébrique de k. On suppose que k **est infini**. Pour $f \in \overline{k}[X_1, \cdots, X_n]$ un polynôme, on note $V(f) = \{z = (z_1, \cdots, z_n) \in \overline{k}^n, f(z) = 0\}$.

i. On veut montrer que si $V(f)$ contient un sous-k-espace vectoriel W de $\overline{k}^n$, alors il contient aussi le sous-$\overline{k}$-espace vectoriel $\overline{k} \cdot W$ engendré par W.

(a) Soient x et $y \in \overline{k}^n$. Montrer que la fonction $\lambda \in \overline{k} \mapsto f(x + \lambda y)$ est polynômiale en λ. En déduire que si $x + k.y \subset V(f)$ alors $x + \overline{k}.y \subset V(f)$.

(b) Montrer plus généralement que si $k.x_1 + \cdots + k.x_r \subset V(f)$ alors $\overline{k}.x_1 + \cdots + \overline{k}.x_r \subset V(f)$. Conclure.

ii. Soit $K \supset k$ une extension finie, et soient $\iota_1, \cdots, \iota_n \in \mathrm{Hom}_{k-\mathrm{alg}}(K, \overline{k})$ les k-plongements de K dans $\overline{k}$. On veut démontrer que $\iota_1, \cdots, \iota_n$ sont *algébriquement indépendants*, au sens suivant :

$$\forall f \in \overline{k}[X_1, \cdots, X_n],\ (\forall x \in K,\ f(\iota_1(x), \cdots, \iota_n(x)) = 0) \Rightarrow f = 0.$$

On notera $\iota(x) := (\iota_1(x), \cdots, \iota_n(x)) \in \overline{k}^n$.

(a) Montrer que l'ensemble $W := \iota(K)$ est un sous-k-espace vectoriel qui engendre $\overline{k}^n$ comme $\overline{k}$-espace vectoriel (i.e. $\overline{k} \cdot W = \overline{k}^n$). Indication : c'est une conséquence immédiate d'un résultat du cours. Expliquer lequel et pourquoi.

(b) Soit $f \in \overline{k}[X_1, \cdots, X_n]$. Montrer que si $z \mapsto f(z)$ est la fonction nulle sur $\overline{k}^n$ alors $f = 0$.

(c) Montrer que $\iota_1, \cdots, \iota_n$ sont algébriquement indépendants.

TSVP

iii. Supposons maintenant l'extension $K \supset k$ Galoisienne et notons $G := \mathrm{Gal}(K/k)$. On veut montrer qu'il existe $x \in K$ tel que $\{\sigma(x), \sigma \in G\}$ est une k-base de K.

   (a) Soit $(\lambda_\sigma)_{\sigma\in G}$ des éléments de k tels que $\sum_\sigma \lambda_\sigma \sigma(x) = 0$. Montrer que pour tout $\tau \in G$, on a aussi $\sum_\sigma \lambda_\sigma(\tau\sigma)(x) = 0$. En déduire que si la famille $\{\sigma(x), \sigma \in G\}$ est k-linéairement liée, alors la matrice carrée $M(x) := ((\tau\sigma)(x))_{\tau,\sigma\in G}$ a un déterminant nul.

   (b) Montrer qu'il existe $x \in K$ tel que $\{\sigma(x), \sigma \in G\}$ est une k-base de K.

   (c) Soit x comme au (b). Montrer que l'application $k[G] \longrightarrow K$, $\sum_{\sigma\in G} \lambda_\sigma e_\sigma \mapsto \sum_{\sigma\in G} \lambda_\sigma \sigma(x)$ est un isomorphisme de $k[G]$-modules (à gauche). Est-ce un isomorphisme de $k[G]$-algèbres ?

iv. On suppose maintenant que k est **finie**, disons $k = \mathbb{F}_q$, avec $q = p^r$ une puissance d'un nombre premier. Soit $K = \mathbb{F}_{q^n}$, et notons $F_q : K \longrightarrow K$, $x \mapsto x^q$.

   (a) Rappeler pourquoi il existe sur K une unique structure de $k[X]$-module telle que X agisse par F_q.

   (b) En utilisant le théorème de structure des $k[X]$-modules, montrer que K est isomorphe au $k[X]$-module $k[X]/(X^n - 1)$.

   (c) En conclure que K est isomorphe à $k[G]$ comme $k[G]$-module.

Exercice 3. Soit $n > 2$ un entier et p, q deux premiers distincts.

i. Montrer que pour tout entier m, il existe un polynôme irréductible de degré m dans $\mathbb{F}_p[X]$.

ii. Montrer qu'il existe un polynôme unitaire irréductible $f \in \mathbb{Z}[X]$ de degré n tel que $(f \bmod p)$ possède un facteur irréductible de degré $n-1$ dans $\mathbb{F}_p[X]$ et $(f \bmod q)$ soit séparable et possède un unique facteur irréductible de degré pair, ce degré étant égal à 2, dans $\mathbb{F}_q[X]$.

iii. Pour un tel f, montrer que $G_f = \mathfrak{S}_n$.