Université Pierre et Marie Curie - Paris VI — Faculté de Mathématiques
Master Mathématiques et applications — 2016–2017

Algèbre et théorie de Galois

Examen du 13 décembre 2016. Durée 3h00.
Seuls documents autorisés : poly et notes de cours. Smartphones éteints.

Exercice 1. i. Montrer que le groupe de Galois de $f = X^5 - 6X + 2$ sur $\mathbb{Q}$ est $\mathfrak{S}_5$.

ii. Montrer que si p est premier et $(a, p) = 1$, le polynôme $X^p - X + a$ est irréductible dans $\mathbb{Q}[X]$.

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

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 (i.e. de la forme $\lambda \mapsto \varphi_{x,y}(\lambda)$ pour un $\varphi_{x,y} \in \overline{k}[X]$).

(b) En déduire que si $x + k.y \subset V(f)$ alors $x + \overline{k}.y \subset V(f)$.

(c) 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 algébrique, 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) 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 $\sum_\sigma \lambda_\sigma(\tau\sigma)(x) = 0$.

(b) 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.

(c) Montrer que le déterminant d'une matrice carrée est une fonction polynômiale non nulle de ses entrées.

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

(e) Soit x comme au (d). 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).

Exercice 3. On veut ici montrer le même énoncé que dans le iii ci-dessus, mais lorsque k est fini. Supposons donc $k = \mathbb{F}_q$, avec $q = p^r$ une puissance d'un nombre premier, et $K = \mathbb{F}_{q^n}$, et notons $F_q : K \longrightarrow K$, $x \mapsto x^q$.

i. Décrire le groupe $G = \mathrm{Gal}(K/k)$.

ii. On considère F_q comme un endomorphisme k-linéaire de K.

(a) Montrer qu'il est annulé par le polynôme $X^n - 1$.

(b) Soit $f \in k[X]$ de degré $m < n$. Montrer que $\{x \in K, f(F_q)(x) = 0\} \subsetneq K$.

(c) En déduire que $X^n - 1$ est le polynôme minimal de F_q.

iii. (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) Montrer que pour tout isomorphisme $\varphi : k[X]/(X^n-1) \xrightarrow{\sim} K$ de $k[X]$-modules, l'image $x := \varphi(1)$ est telle que $\{\sigma(x), \sigma \in G\}$ est une k-base de K.