Sorbonne Université — UFR de Mathématiques
Master Mathématiques et applications — 2024–2025

Théorie de Galois

Examen du 12 mai 2025. Durée 2h00.
Pas de documents autorisés.

Exercice 1. Soit K/k une extension Galoisienne finie de groupe de Galois $\mathfrak{S}_n$ pour $n \geqslant 5$. Montrer que le degré d'un élément $\alpha \in K$ sur k est soit 1, soit 2, soit $\geqslant n$.

Notons d le degré de α sur k, et $f_\alpha \in k[X]$ son polynôme minimal. Comme K/k est Galoisienne, f_α est scindé à racines simples dans $K[X]$. Soit K_α le corps engendré par les racines de f_α. C'est une extension Galoisienne de K, donc le groupe $\mathrm{Gal}(K/K_\alpha)$ est distingué dans $\mathfrak{S}_n$. Comme $n \geqslant 5$, les seuls sous-groupes distingués de $\mathfrak{S}_5$ sont $\{\mathrm{id}\}$, $\mathfrak{A}_5$, ou $\mathfrak{S}_5$. Si $\mathrm{Gal}(K/K_\alpha) = \mathfrak{S}_5$, alors $K_\alpha = k$ et α est de degré 1. Si $\mathrm{Gal}(K/K_\alpha) = \mathfrak{A}_5$, alors K_α/k est quadratique, donc α est de degré 2. Si $\mathrm{Gal}(K/K_\alpha) = \{\mathrm{id}\}$, alors $K_\alpha = K$, i.e. K est un corps de décomposition de f_α. On sait alors que $\mathrm{Gal}(K/k)$ se plonge dans $\mathfrak{S}_d$ après numérotation des racines de f_α. Ceci implique $d \geqslant n$.

Exercice 2. Soit $f \in k[X]$ un polynôme irréductible séparable, K_f/k un corps de décomposition et $G_f := \mathrm{Gal}(K_f/k)$ son groupe de Galois.

i. Montrer que si G_f est abélien, alors $|G_f| = \deg(f)$. (On pourra montrer que K_f/k est engendrée par une racine de f)

Soit α une racine de f. Comme G_f est abélien, tous ses sous-groupes sont distingués donc, par la correspondance de Galois, toute sous-extension de K_f est normale. En particulier $k(\alpha)/k$ est normale : elle contient toutes les racines de f (car $f = f_\alpha$) donc $k(\alpha) = K_f$ et $|G_f| = [K_f : k] = \deg(f)$.

ii. La réciproque est-elle vraie ? (Justifier!)

Non ! En effet, partons d'une extension Galoisienne K/k de groupe de Galois G non abélien. Soit α un élément primitif de K et $f := f_\alpha$. Alors $K = K_f$, et $|G| = [K_f : k] = \deg(f)$.

iii. L'énoncé i. est-il encore vrai si f est réductible (mais séparable) ?

Non ! Voici un contre-exemple : on prend $k = \mathbb{Q}$ et $f = (X^2 - 2)(X^2 - 3)(X^2 - 5)$. Alors $G_f = \{\pm 1\}^3$ est de cardinal 8 bien que f soit de degré 6.

Exercice 3. Soit $f := X^6 + 22X^5 + 6X^4 + 12X^3 - 52X^2 - 14X - 30 \in \mathbb{Q}[X]$.

TSVP

i. Montrer que f est irréductible dans $\mathbb{Q}[X]$. On note $K_f \subset \overline{\mathbb{Q}}$ son corps de décomposition et $G_f = \mathrm{Gal}(K_f/\mathbb{Q})$ son groupe de Galois.

On applique le critère d'Eisenstein en 2.

ii. Montrer que G_f contient un 5-cycle.

Réduisons modulo 3. On obtient une factorisation $\overline{f} = X(X^5 + X^4 - X + 1)$. Le polynôme $X^5 + X^4 - X + 1$ n'a pas de racine dans $\mathbb{F}_3$. On vérifie qu'il est premier à $X^9 - X$, donc il n'a pas de racine dans $\mathbb{F}_9$ non plus, donc pas de facteur de degré 2 dans $\mathbb{F}_3[X]$. Etant de degré 5, il est donc irréductible. Ainsi $\overline{f}$ est séparable de type de factorisation $(1, 5)$ donc, par le théorème de spécialisation, on en déduit que G_f contient un 5-cycle.

iii. Montrer que G_f contient une transposition.

Réduisons modulo 5. On vérifie que 0, 1, -1 et -2 sont racines de $\overline{f}$, d'où une factorisation $\overline{f} = X(X-1)(X+1)(X+2)(X^2+2)$. Comme X^2+2 n'a pas de racine dans $\mathbb{F}_5$, on voit que f est séparable de type de décomposition $(1, 1, 1, 1, 2)$. Par le théorème de spécialisation, on en déduit que G_f contient un 2-cycle.

iv. En déduire que $G_f = \mathfrak{S}_6$.

On sait que G_f est un sous-groupe transitif de $\mathfrak{S}_6$ (car f est irréductible) qui contient un 5-cycle et une transposition. Il s'agit de montrer qu'un tel groupe est égal à $\mathfrak{S}_6$. Cela a été fait en TD (pour n quelconque). Soit $\sigma \in G$ un 5-cycle, et $\tau \in G$ une transposition. Puisque G est transitif, on peut conjuguer τ par un élément de G de sorte que le support de la transposition obtenue ne soit pas contenu dans celui de σ. Quitte à conjuguer dans $\mathfrak{S}_n$, on peut donc supposer que G contient le 5-cycle $\sigma = (2, 3, 4, 5, 6)$ et la transposition $\tau = (1, 2)$. Il contient alors aussi $\sigma^i \tau \sigma^{-i} = (1, i+2)$ pour $i = 1, \cdots, 4$. Mais on sait que les transpositions $(1, i)$ engendrent $\mathfrak{S}_6$.

Exercice 4. Soit p un nombre premier et $f := (X^2 + 1) \prod_{k=1}^{p-2} (X - k) \in \mathbb{Q}[X]$.

i. Montrer qu'il existe un réel $\varepsilon > 0$ tel que, pour tout réel positif $\delta < \varepsilon$, le polynôme $f + \delta \in \mathbb{R}[X]$ admet exactement $p - 2$ racines réelles.

La fonction $x \mapsto f(x)$ possède au plus $p - 1$ extrema locaux (en les racines réelles de f'). Posons ε le minimum des valeurs absolues de ces extrema locaux. Montrons que ε convient. Soient $x_1 < \cdots < x_n$ les racines réelles de f' et posons $x_0 := -\infty$ et $x_{n+1} = \infty$. Comme f s'annule exactement en $x = 1, \cdots, p-2$, il y a exactement $p - 2$ indices j tels que f s'annule (et change de signe) sur l'intervalle $[x_j, x_{j+1}]$. Pour tout $\delta \in \mathbb{R}$, la fonction $f + \delta$ atteint ses extrema en les mêmes points que f. En particulier, elle s'annule en au plus un point de chaque intervalle $[x_j, x_{j+1}]$. Or, si on choisit δ tel que $|\delta| < \varepsilon$, alors $f(x_j) + \delta$ a le même signe que $f(x_j)$ pour tout j, donc $f + \delta$ s'annule sur les mêmes intervalles $[x_j, x_{j+1}]$ que f, ce qui nous donne exactement $p - 2$ racines distinctes.

ii. Soit ℓ un autre nombre premier, et soit $f_\ell := \ell^p f(X/\ell) + \ell$. Montrer que f_ℓ est irréductible dans $\mathbb{Q}[X]$.

Si $f = X^p + a_1 X^{p-1} + \cdots + a_p$, on a $f_\ell = X^p + \ell a_1 X^{p-1} + \cdots + \ell^{p-1} a_{p-1} X + (\ell^p a_p + \ell)$, donc f_ℓ satisfait le critère d'Eisenstein en ℓ.

iii. Montrer que pour ℓ assez grand, le groupe de Galois de f_ℓ est isomorphe à $\mathfrak{S}_p$.

Par la question précédente, f_ℓ est irréductible, donc $p||G_{f_\ell}|$ donc G_{f_ℓ} contient un p-cycle car p est premier. Par la question i, f_ℓ a exactement 2 racines non réelles si $\ell^{1-p} < \varepsilon$. Dans ce cas, comme un p-cycle et une transposition engendrent $\mathfrak{S}_p$, on a $G_{f_\ell} = \mathfrak{S}_p$.

iv. Soit G un groupe fini. Montrer que G est le groupe de Galois d'une extension Galoisienne L/K de corps de nombres (i.e. d'extensions finies de $\mathbb{Q}$).

En posant $n = |G|$, on a un plongement $G \hookrightarrow \mathfrak{S}_n$ en faisant agir G par translation sur lui-même. On peut alors choisir un premier $p > n$ et identifier $\mathfrak{S}_n$ au sous-groupe de $\mathfrak{S}_p$ qui fixe $n+1, \cdots, p$. D'où un plongement $G \hookrightarrow \mathfrak{S}_p$. Choissons alors f_ℓ comme dans iii, notons L son corps de décomposition et identifions $\mathrm{Gal}(L/\mathbb{Q})$ a $\mathfrak{S}_p$ en choisissant un ordre sur les racines de f_ℓ. Par la correspondance de Galois, si on pose $K := L^G$, alors $\mathrm{Gal}(L/K) = G$.