Sorbonne Université — UFR de Mathématiques
Master Mathématiques et applications — 2021–2022

Théorie de Galois

Partiel du 9 mars 2022. Durée 2h00.
Pas de documents autorisés.

Exercice 1. Soit k un corps et f un polynôme séparable dans $k[X]$ de degré $n := \deg(f)$. Notons K_f un corps de décomposition de f sur k et $G_f := \mathrm{Gal}(K_f/k) = \mathrm{Aut}_{k-\mathrm{alg}}(K_f)$ son groupe de Galois.

i. Rappeler pourquoi G_f permute les racines de f dans K_f et pourquoi, après numérotation des racines, on obtient un morphisme *injectif* $G_f \hookrightarrow \mathfrak{S}_n$.

Soit α une racine de f dans K_f et $\sigma \in G_f$. On a $f(\sigma(\alpha)) = \sigma(f)(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$ (la première égalité car $f \in k[X]$ donc $\sigma(f) = f$). On voit donc que $\sigma(\alpha)$ est encore une racine de f. Comme f est séparable, ses racines sont distinctes. Notons-les $\alpha_1, \cdots, \alpha_n$. Alors pour tout $\sigma \in G_f$, il existe une unique permutation $\tau_\sigma \in \mathfrak{S}_n$ telle que $\sigma(\alpha_i) = \alpha_{\tau_\sigma(i)}$ pour tout i. On obtient ainsi un morphisme de groupes $G_f \longrightarrow \mathfrak{S}_n$. Son noyau est formé des éléments qui fixent tous les α_i. Mais comme les α_i engendrent l'extension $k \subset K_f$, un tel élement est l'identité sur K_f. Donc $G_f \longrightarrow \mathfrak{S}_n$ est injectif.

ii. En déduire que $[K_f : k] \,|\, n!$. Pour $n = 3$, donner un exemple où $[K_f : k] = 3!$ et un exemple où $[K_f : k] = 3$.

Puisque K_f/k est Galoisienne, on a $[K_f : k] = |G_f|$. Par la question i, on sait que G_f s'identifie à un sous-groupe de $\mathfrak{S}_n$, donc $|G_f|$ divise $|\mathfrak{S}_n| = n!$ (thm de Lagrange)

Regardons $f = X^3 - 2$ et K_f le sous-corps de $\overline{\mathbb{Q}}$ engendré par les racines de f. On a vu que $K_f = \mathbb{Q}(\sqrt[3]{2}, j)$ est de degré 3 sur $\mathbb{Q}(j)$ qui est de degré 2 sur $\mathbb{Q}$. Donc $(k = \mathbb{Q}, f)$ est un exemple où $[K_f : k] = 3!$, et $(k = \mathbb{Q}(j), f)$ est un exemple où $[K_f : k] = 3$.

iii. Montrer que f est irréductible si et seulement si l'action de G_f sur les racines de f est transitive.

Comme $K_f \supset k$ est Galoisienne, on sait que pour tout $\alpha \in K$, le polynôme minimal f_α de α dans $k[X]$ est de la forme $f_\alpha = \prod_{\beta \in G_f.\alpha}(X - \beta)$ dans $K_f[X]$. Appliquons ceci à une racine α de f. Comme $f_\alpha | f$, on a les équivalences : f irréductible $\Leftrightarrow f_\alpha = f \Leftrightarrow \{\text{rac. de } f\} = G_f.\alpha$.

iv. Soit $f = f_1 \cdots f_r$ la décomposition de f en produit d'irréducibles et $n_k := \deg f_k$. Montrer que $G_f \hookrightarrow \mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_r} \subset \mathfrak{S}_n$ pour une numérotation convenable des racines de f.

On a une partition $\{\text{rac. de } f\} = \bigsqcup_{i=1}^r \{\text{rac. de } f_i\}$, qui est stable par G_f car G_f envoie les racines de f_i sur des racines de f_i (cf question i).

TSVP

v. On suppose ici que $k = \mathbb{F}_p$.

(a) Montrer que la permutation σ_φ qui donne l'action du Frobenius φ est un produit de r cycles disjoints de longueurs respectives $n_1, \cdots, n_r$.

Comme G_f est engendré par φ, on sait que l'action de φ sur $\{\text{rac. de } f_i\}$ est transitive (question ii.), et il s'ensuit que φ agit par permutation cyclique des racines de f_i. Ceci étant vrai pour tout $i = 1, \cdots, r$, on voit que φ agit par une permutation qui est un produit de cycles disjoints de longueurs respectives n_i.

(b) En déduire $[K_f : k]$ en fonction des n_i.

Par le (a), on sait que $\varphi^k = \mathrm{id}$ si et seulement si $n_i | k$ pour tout i. Donc l'ordre de φ est le ppcm des n_i.

Exercice 2. Soit $K \supset k$ une extension finie de corps. Pour $\alpha \in K$, la multiplication par α est un endomorphisme k-linéaire de K. Notons $\mathrm{Tr}_{K/k}(\alpha)$ sa trace, $\mathrm{N}_{K/k}(\alpha)$ son déterminant, et $\Phi_{K/k}(\alpha) \in k[X]$ son polynôme caractéristique.

i. Notons $f_\alpha = X^n + a_1 X^{n-1} + \cdots + a_n$ le polynôme minimal de α sur k.

(a) Rappeler pourquoi la famille $\{1, \alpha, \cdots, \alpha^{n-1}\}$ est une base de $k(\alpha)$ sur k, et écrire la matrice de la multiplication par α dans cette base.

Puisque α est algébrique, on a $k(\alpha) = k[\alpha]$. Par définition, $k[\alpha]$ est engendré k-linéairement par les $\alpha^i, i \in \mathbb{N}$, donc tout élément est de la forme $g(\alpha)$ pour un $g \in k[X]$. Or, $g(\alpha) = r(\alpha)$ si r est le reste de la division euclidienne de g par f_α. Comme $\deg r < n$, on en déduit que $k[\alpha]$ est k-linéairement engendré par les α^i, $i = 0, \cdots, n-1$. Par ailleurs toute relation de dépendance linéaire $\sum_{i=0}^{n-1} a_i \alpha^i = 0$ fournit un polynôme $h = \sum_{i=0}^{n-1} a_i X^i$ annulateur de α. On a alors $f_\alpha | h$ et $\deg h < n = \deg f_\alpha$, ce qui implique $h = 0$. Ceci montre que la famille de l'énoncé est libre.

(b) En déduire que $\Phi_{k(\alpha)/k}(\alpha) = f_\alpha$, puis $\mathrm{Tr}_{k(\alpha)/k}(\alpha) = -a_1$ et $\mathrm{N}_{k(\alpha)/k}(\alpha) = (-1)^n a_n$.

(c) Soit $\overline{k}$ une clôture algébrique de k et $\Sigma_{k(\alpha)/k} := \mathrm{Hom}_{k-\mathrm{alg}}(k(\alpha), \overline{k})$. Montrer que si α est séparable sur k, alors on a les égalités dans $\overline{k}$

$$\mathrm{Tr}_{k(\alpha)/k}(\alpha) = \textstyle\sum_{\sigma \in \Sigma_{k(\alpha)/k}} \sigma(\alpha) \text{ et } \mathrm{N}_{k(\alpha)/k}(\alpha) = \prod_{\sigma \in \Sigma_{k(\alpha)/k}} \sigma(\alpha).$$

ii. À l'aide d'un choix de base de K sur $k(\alpha)$, montrer $\Phi_{K/k}(\alpha) = \Phi_{k(\alpha)/k}(\alpha)^{[K:k(\alpha)]}$, et

$$\mathrm{Tr}_{K/k}(\alpha) = [K : k(\alpha)] \mathrm{Tr}_{k(\alpha)/k}(\alpha) \text{ et } \mathrm{N}_{K/k}(\alpha) = \mathrm{N}_{k(\alpha)/k}(\alpha)^{[K:k(\alpha)]}.$$

iii. Montrer que si K est séparable sur k, on a les égalités dans $\overline{k}$

$$\mathrm{Tr}_{K/k}(\alpha) = \textstyle\sum_{\sigma \in \Sigma_{K/k}} \sigma(\alpha) \text{ et } \mathrm{N}_{K/k}(\alpha) = \prod_{\sigma \in \Sigma_{K/k}} \sigma(\alpha).$$

On pourra montrer que les fibres de l'application de restriction $\Sigma_{K/k} \longrightarrow \Sigma_{k(\alpha)/k}$ sont de cardinal $[K : k(\alpha)]$.

TSVP

iv. On s'intéresse maintenant à la forme k-bilinéaire symétrique

$$\theta_{K/k} : K \times K \longrightarrow k,\ (x, y) \mapsto \mathrm{Tr}_{K/k}(xy).$$

On veut montrer que $\theta_{K/k}$ *est non-dégénérée si et seulement si* K *est séparable sur* k. Pour cela, posons $A := \overline{k} \otimes_k K$, qui est une $\overline{k}$-algèbre de dimension finie munie de la forme $\overline{k}$-bilinéaire $\theta_{A/\overline{k}} : A \times A \longrightarrow \overline{k},\ (x, y) \mapsto \mathrm{Tr}_{A/\overline{k}}(xy)$

(a) Montrer que $\theta_{K/k}$ est non-dégénérée si et seulement si $\theta_{A/\overline{k}}$ est non-dégénérée.

(b) Montrer que tout élément nilpotent $x \in A$ est dans le noyau de $\theta_{A/\overline{k}}$.

(c) Si A est réduite, montrer que $\theta_{A/\overline{k}}$ est non-dégénérée. On pourra utiliser le fait que $A = \bar{k} \times \cdots \times \bar{k}$ et expliciter $\theta_{A/\overline{k}}$.

(d) Conclure.