Fiche 1 - Algèbre sur un anneau - Théorie de Galois

SOUANEF Rafik - 2024/2025

1 Groupes de Galois

1.1 Groupe de Galois complexe

1. Montrer que $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ n'est constitué que de id et la conjugaison complexe.
2. Montrer que les seuls endomorphismes continus de $\mathbb{C}$ sont id et la conjugaison complexe.

1.2 Calcul de groupe de Galois (1)

Soit $\mathbb{K} = \mathbb{Q}(\sqrt{2}, i)$.

1. Quel est le degré de $\mathbb{K}/\mathbb{Q}$?
2. A quel groupe usuel est isomorphe $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$?

1.3 Le cas des corps finis

Soit $q = p^r$ une puissance d'un nombre premier p. Soit $n \in \mathbb{N}$.

1. Montrer que l'extension $\mathbb{F}_{q^a}/\mathbb{F}_q$ est galoisienne.
2. Montrer que le groupe $\mathrm{Gal}(\mathbb{F}_{q^a}/\mathbb{F}_q)$ est cyclique, engendré par

$$\mathrm{frob} : \left| \begin{array}{ccc} \mathbb{F}_{q^a} & \longrightarrow & \mathbb{F}_{q^a} \\ x & \longmapsto & x^q \end{array} \right. .$$

1.4 Sur les compositum

Soit $\mathbb{K}$ un corps et soient $\mathbb{L}_1, \mathbb{L}_2$ deux extensions finies de $\mathbb{K}$ (que l'on suppose vivre dans une même extension Ω de $\mathbb{K}$).

On appelle compositum de $\mathbb{L}_1$ et $\mathbb{L}_2$ le plus petit (au sens de l'inclusion) sous-corps de Ω contenant $\mathbb{L}_1$ et $\mathbb{L}_2$; on le note $\mathbb{L}_1\mathbb{L}_2$.

Si $\mathbb{L}_1/\mathbb{K}$ est galoisienne, on dit que $\mathbb{L}_1$ et $\mathbb{L}_2$ sont linéairement indépendantes si l'on a

$$\mathbb{L}_1 \cap \mathbb{L}_2 = \mathbb{K}.$$

1. Montrer que l'on a
$$\mathbb{L}_1\mathbb{L}_2 = \left\{ \sum_{i=1}^{r} x_i y_i : x_i \in \mathbb{L}_1, y_i \in \mathbb{L}_2, r \in \mathbb{N} \right\}$$
2. Supposons $\mathbb{L}_1/\mathbb{K}$ galoisienne. Montrer que $\mathbb{L}_1$ et $\mathbb{L}_2$ sont linéairement indépendantes si et seulement si l'on a
$$[\mathbb{L}_1\mathbb{L}_2 : \mathbb{K}] = [\mathbb{L}_1 : \mathbb{K}][\mathbb{L}_2 : \mathbb{K}]$$

3. Le résultat précédent est-il toujours vrai si l'on suppose uniquement

$$\mathbb{L}_1 \cap \mathbb{L}_2 = \mathbb{K}?$$

1.5 Calcul de groupe de Galois (2)

Soit $\mathbb{K}$ le corps de décomposition de $X^3 - 7 \in \mathbb{Q}[X]$.

1. Les extensions $\mathbb{Q}(7^{1/3})/\mathbb{Q}$ et $\mathbb{K}/\mathbb{Q}$ sont-elles galoisiennes ?
2. Montrer que l'on a $\mathbb{K} = \mathbb{Q}(7^{1/3}, j)$ (où $j = e^{2i\pi/3}$).
3. En déduire $[\mathbb{K} : \mathbb{Q}]$ puis $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \simeq \mathcal{S}_3$.

1.6 Groupe de Galois des corps cyclotomiques

Montrer que l'on a $\mathrm{Gal}(\mathbb{Q}(e^{2i\pi/n})/\mathbb{Q}) \simeq \mathbb{Z}/n\mathbb{Z}^*$.

1.7 Calcul de groupe de Galois (3)

Soit $\mathbb{K}$ le corps de décomposition de $X^4 - 2 \in \mathbb{Q}[X]$.

1. Les extensions $\mathbb{Q}(2^{1/4})/\mathbb{Q}$ et $\mathbb{K}/\mathbb{Q}$ sont-elles galoisiennes ?
2. Montrer que l'on a $\mathbb{K} = \mathbb{Q}(2^{1/4}, i)$.
3. Donner $[\mathbb{K} : \mathbb{Q}]$ et donner le cardinal de $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.
4. Montrer qu'il existe un unique automorphisme σ de $\mathbb{K}$ tel que $\sigma(2^{1/4}) = i2^{1/4}$ et $\sigma(i) = i$. Quel est l'ordre de σ ?
5. Montrer qu'il existe un unique automorphisme τ de $\mathbb{K}$ tel que $\tau(2^{1/4}) = 2^{1/4}$ et $\tau(i) = -i$. Quel est l'ordre de τ ?
6. Montrer que l'on a $\tau\sigma\tau^{-1} = \sigma^{-1}$.
7. A quel groupe usuel est isomorphe $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$?

1.8 Extensions et conjugués

Soit x un nombre algébrique de degré n sur $\mathbb{K}$, soit $\mathbb{L}$ une extension finie de $\mathbb{K}$ de degré premier à n. Montrer que les $\mathbb{K}$-conjugués de x sont exactement les $\mathbb{L}$-conjugués de x.

1.9 Caractérisation de la normalité

Soit $\mathbb{L}/\mathbb{K}$ une extension de corps. Montrer qu'elle est normale si et seulement si pour tout $x \in \mathbb{L} \setminus \mathbb{K}$, il existe $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ tel que $\sigma(x) \neq x$.

1.10 Résultat en caractéristique nulle

Soient $\mathbb{K}$ un corps de caractéristique nulle, P un irréductible de $\mathbb{K}[X]$, x et y deux racines distinctes de P dans un surcorps de $\mathbb{K}$. Montrer que $x - y$ n'appartient pas à $\mathbb{K}$. Montrer que ce résultat tombe en défaut en caractéristique p.

1.11 Autour de la décomposition de Dunford

1. Rappeler l'énoncé de la décomposition de Dunford.
2. Soit $\mathbb{K}$ un corps de caractéristique 0 et soit $M \in \mathcal{M}_n(\mathbb{K})$. En s'appuyant sur la décomposition de Dunford, donner une décomposition intéressante de M de dans $\mathcal{M}_n(\mathbb{K})$.

1.12 Passage à un surcorps

Soient $\mathbb{L}/\mathbb{K}$ une extension normale finie et $P \in \mathbb{K}[X]$ un irréductible. Montrer que les facteurs irréductibles de P dans $\mathbb{L}[X]$ ont tous même degré.

1.13 Générateurs d'extensions

Soit $\mathbb{K}$ un corps, soient $\mathbb{L}_1/\mathbb{K}$ et $\mathbb{L}_2/\mathbb{K}$ deux extensions galoisiennes finies.

1. On suppose que $\mathbb{K}$ est de caractéristique nulle et que l'on a $\mathbb{L}_1 \cap \mathbb{L}_2 = \mathbb{K}$. Montrer que si x (resp. y) est un élément primitif de $\mathbb{L}_1$ (resp. $\mathbb{L}_2$) alors $x+y$ est un élément primitif de $\mathbb{L}_1\mathbb{L}_2$.

   Indication: On pourra montrer que si $\sigma \in \mathrm{Gal}(\mathbb{L}_1\mathbb{L}_2/\mathbb{K})$ fixe $x+y$ alors σ est l'identité.
2. On suppose que $[\mathbb{L}_1 : \mathbb{K}]$ est premier avec $[\mathbb{L}_2 : \mathbb{K}]$. Montrer que si x (resp. y) est un élément primitif de $\mathbb{L}_1$ (resp. $\mathbb{L}_2$) alors xy est un élément primitif de $\mathbb{L}_1\mathbb{L}_2$.

1.14 Génération de polynômes irréductibles

1. Soient p un nombre premier, $\mathbb{K}$ un corps de caractéristique p et a un élément de $\mathbb{K}$ tel que $X^p - X - a$ n'ait pas de racine dans $\mathbb{K}$. Montrer que le groupe de Galois sur $\mathbb{K}$ de ce polynôme est cyclique d'ordre p et que ce polynôme est irréductible sur $\mathbb{K}$.
2. Montrer que $X^p - X - 1$ est irréductible dans $\mathbb{Q}[X]$.

1.15 Extensions abéliennes

Soit $\mathbb{M}/\mathbb{K}$ une extension abélienne finie.

1. Montrer que tout corps intermédiaire $\mathbb{L}$ est tel que $\mathbb{L}/\mathbb{K}$ est abélienne.
2. Supposons $\mathbb{K} = \mathbb{Q}$ et que $\mathbb{M}$ n'est pas un corps réel. Montrer que $\mathbb{M}$ a un unique sous-corps réel maximal $\mathbb{M}^+$ et que l'on a $[\mathbb{M} : \mathbb{L}] = 2$.
3. Donner un générateur de $\mathbb{Q}(\zeta_n)^+$.

1.16 Détermination d'un groupe de Galois

Soit $x = \sqrt{2+\sqrt{2+\ldots}}$ (avec n racines carrées). Exprimer x sous la forme $2\cos\theta$. En déduire que $\mathbb{Q}(x)/\mathbb{Q}$ est galoisienne et calculer $\mathrm{Gal}(\mathbb{Q}(x)/\mathbb{Q})$.

1.17 Corps cyclotomiques

A quelle condition sur n l'extension $\mathbb{Q}(e^{2i\pi/n})/\mathbb{Q}$ contient-elle une unique sous-extension de degré 2 ?

(*) Dans ce cas, donner cette sous-extension.

1.18 Produit de groupes

Caractériser les extensions galoisiennes finies $\mathbb{L}/\mathbb{K}$ dont le groupe de galois est produit direct de deux sous-groupes non triviaux.

1.19 Sous-extensions

1. Lister les sous-extensions de $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$.
2. Donner le treillis des sous-groupes de D_8.
3. Donner le treillis des sous-extensions de $\mathbb{Q}(2^{1/4}, i)/\mathbb{Q}$.

1.20 Calcul de norme

Soit p un nombre premier et soit $\zeta = e^{2i\pi/p}$. Montrer que l'on a $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta) = p$.

1.21 Paramétrisation rationnelle du cercle

En s'aidant de $\mathbb{Q}(i)$, montrer que les solutions rationnelles à l'équation $x^2 + y^2 = 1$ sont de la forme

$$(\frac{c^2 - d^2}{c^2 + d^2}, \frac{-2cd}{c^2 + d^2})$$

pour certains $c, d \in \mathbb{Q}$.

1.22 Génération de groupes cycliques*

Soit $d > 1$ un entier. Soit p tel que $d \mid p - 1$. Exhiber $\alpha \in \mathbb{C}$ algébrique tel que $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne et $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \simeq \mathbb{Z}/d\mathbb{Z}$.

1.23 Galois inverse pour $\mathcal{S}_p$**

Soient $\mathbb{K}$ un sous-corps de $\mathbb{C}$, p un nombre premier, P un irréductible de degré p de $\mathbb{K}[X]$ admettant $p-2$ racines réelles et 2 racines irréelles conjuguées. Montrer que le groupe de Galois de P est isomorphe à $\mathcal{S}_p$.

1.24 Le groupe de Galois absolu

Montrer que $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ est équipotent à $\mathbb{R}$.

1.25 Racines de l'unité sur un corps fini

Soit q une puissance d'un nombre premier. Montrer que chaque facteur irréductible du n^{eme} polynôme cyclotomique Φ_n, vu comme un polynôme à coefficients dans $\mathbb{F}_q$, est de degré r, où r désigne l'ordre de q dans $\mathbb{Z}/n\mathbb{Z}^*$.

1.26 Indépendance des morphismes

Soit $\mathbb{L}/\mathbb{K}$ une extension galoisienne finie de groupe G. Notons $\mathcal{L}_{\mathbb{K}}(\mathbb{L})$ l'algèbre des endomorphismes du $\mathbb{K}$-espace vectoriel $\mathbb{L}$. Montrer que l'on a

$$\mathcal{L}_{\mathbb{K}}(\mathbb{L}) = \oplus_{g\in G}\mathbb{L}g.$$

1.27 Tour cyclotomique

Montrer qu'il y a un isomorphisme entre $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ et

$$\left\{(a_n)_{n\in\mathbb{N}} : a_n \in \mathbb{Z}/p^n\mathbb{Z} \text{ et } a_{n+1} = a_n \mod p^n\right\}.$$