TD9 : Théorie de Galois II

Diego Izquierdo

Les exercices 0, 1, 5 (sans la question 3(b)) et 12 sont à préparer avant le TD. Pendant la séance de TD, les exercices seront traités dans l'ordre suivant : 0, 1, 5 (sans la question 3(b)), 12, 16, 20. Si le temps le permet nous traiterons aussi l'exercice 10. ***Ce TD (comme le précédent) est particulièrement important.*** *Je vous conseille donc fortement de faire plus d'exercices de cette feuille que ceux qui seront traités pendant la séance.*

Exercice 0 (à préparer) : TD8
Faire les questions (iii), (vi), (xiii) et (xvi) de l'exercice 7 du TD8.

Exercice 1 (à préparer) : Sous-corps d'un corps cyclotomique
Faire la liste des sous-corps de $\mathbb{Q}(\zeta_{20})$.

Exercice 2 : Sous-extensions de degré 3 d'extensions cyclotomiques

1. Déterminer l'entier positif minimal n tel que l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ contient une sous-extension E de degré 3. Montrer que cette sous-extension est unique.
2. Montrer que $E/\mathbb{Q}$ est galoisienne et exhiber un polynôme unitaire irréductible à coefficients entiers dont c'est le corps de décomposition.

Exercice 3 : Irréductibilité des polynômes cyclotomiques
Soient m et n deux entiers naturels premiers entre eux. Montrer que Φ_n est irréductible dans $\mathbb{Q}(\zeta_m)$.

Exercice 4 : Examen 2014
Soit $n > 2$. Soient $K_n = \mathbb{Q}(\zeta_{2^n})$ et $K_n^{\pm} = \mathbb{Q}(\zeta_{2^n} \pm \zeta_{2^n}^{-1})$.

1. Identifier les groupes $\mathrm{Gal}(K_n/\mathbb{Q})$ et $\mathrm{Gal}(K_n^{\pm}/\mathbb{Q})$.
2. Montrer que l'on a, pour chaque choix de $n-3$ signes :

$$K_n^+ = \mathbb{Q}\left(\sqrt{2 \pm \sqrt{2 \pm \sqrt{\dots \pm \sqrt{2 \pm \sqrt{2}}}}}\right),$$

$$K_n^- = \mathbb{Q}\left(i\sqrt{2 \pm \sqrt{2 \pm \sqrt{\dots \pm \sqrt{2 \pm \sqrt{2}}}}}\right).$$

3. Faire un diagramme représentant les sous-corps de K_n.

Exercice 5 (à préparer sans la question 3(b)) : Sous-extensions quadratiques d'extensions cyclotomiques

1. Soit $n \in \mathbb{Z} \setminus \{0\}$. Combien d'extensions quadratiques de $\mathbb{Q}$ sont contenues dans $\mathbb{Q}(\zeta_n)$? Vérifier en particulier qu'il y en a 7 pour $n = 60$.

2. (a) Soit p un nombre premier impair. Calculer le discriminant de ϕ_p et en déduire que l'unique extension quadratique de $\mathbb{Q}$ contenue dans $\mathbb{Q}(\zeta_p)$ est $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$.

(b) Quelles sont les extensions quadratiques de $\mathbb{Q}$ contenues dans $\mathbb{Q}(\zeta_8)$?

(c) En déduire la liste des extensions quadratiques de $\mathbb{Q}$ contenues dans $\mathbb{Q}(\zeta_{60})$.

3. (a) Montrer que toute extension quadratique de $\mathbb{Q}$ est contenue dans une extension cyclotomique de $\mathbb{Q}$.

(b) *(Difficile)* Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteurs carrés. Soit n le plus petit entier naturel n tel que $\sqrt{d} \in \mathbb{Q}(\zeta_n)$. Montrer que $n = |d|$ si $d \equiv 1 \mod 4$ et que $n = 4|d|$ si $d \not\equiv 1 \mod 4$.

Exercice 6 : Polynômes cyclotomiques

Soient a et b deux entiers naturels non nuls premiers entre eux. Le théorème de Dirichlet (1837) affirme qu'il existe une infinité de nombres premiers p tels que $p \equiv b \mod a$. Le but de cet exercice est d'établir ce théorème dans le cas particulier où $b = 1$.

1. Soit $P \in \mathbb{Z}[X] \setminus \mathbb{Z}$. Montrer que l'ensemble $\{d \in \mathbb{N} \mid \exists n \in \mathbb{N},\ d \mid P(n)\}$ est infini.

2. Soit $P = \frac{X^a - 1}{\phi_a} \in \mathbb{Z}[X]$. Montrer qu'il existe un nombre premier p et un entier x tels que p divise $\phi_a(x)$ mais pas $P(x)$.

3. Calculer l'ordre de x dans $\mathbb{Z}/p\mathbb{Z}$ et en déduire que $p \equiv 1 \mod a$.

4. Conclure.

Exercice 7 : Galois inverse sur $\mathbb{Q}$, cas abélien fini

On utilisera à bon escient les résultats :

– sur la structure des groupes abéliens finis ;
– sur la progression arithmétique faible de Dirichlet (exercice 6).

En pensant aux corps cyclotomiques, montrer que tout groupe abélien fini est groupe de Galois d'une extension galoisienne sur $\mathbb{Q}$.

Exercice 8 : Examen 2014

Pour quelles valeurs de $n \geq 1$ le corps $\mathbb{Q}(\zeta_n)$ (resp. $\mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$) s'écrit-il sous la forme $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, ..., \sqrt{a_r})$ où $a_j \in \mathbb{Q}^\times$? Expliciter les a_j

dans chaque cas.

Exercice 9 : Cyclotomie sur $\mathbb{F}_q$
Soient p un nombre premier, q une puissance de p et $r \geq 1$ un entier.

1. Déterminer le groupe $\mu_{p^r}(\mathbb{F}_q)$ des racines p^r-èmes de l'unité dans $\mathbb{F}_q$.
2. Montrer que toute extension finie de $\mathbb{F}_q$ est cyclotomique, c'est-à-dire engendrée par des racines de l'unité.

Soient $n \geq 1$ un entier et $\Phi_n \in \mathbb{Z}[X]$ le n-ème polynôme cyclotomique sur $\mathbb{C}$. On note $\overline{\Phi}_n^{(p)}$ la réduction de Φ_n modulo p, que l'on peut voir comme un polynôme sur $\mathbb{F}_q$.
Supposons n premier à p.

3. Montrer que les racines de $\overline{\Phi}_n^{(p)}$ sont exactement les racines primitives n-èmes de l'unité dans $\mathbb{F}_q$.
4. Montrer que $\overline{\Phi}_n^{(p)}$ est irréductible sur $\mathbb{F}_q$ si et seulement si q est un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$.
5. En déduire que la réduction de Φ_8 modulo p est réductible pour tout nombre premier p.

Exercice 10 : Extensions de Kummer
Soit $P = X^n - a \in \mathbb{Q}[X]$ avec $n \in \mathbb{N}^*$ et $a \in \mathbb{Q}^\times$.

1. Vérifier que P est résoluble par radicaux sur $\mathbb{Q}$.
2. On suppose que n est égal à un premier p et que $a \notin (\mathbb{Q}^\times)^p$. Soit L un corps de décomposition de P sur $\mathbb{Q}$. Montrer que $\mathrm{Gal}(L/\mathbb{Q}) \cong GA_1(\mathbb{F}_p)$.
3. On suppose que $n = 4$, $|a| \notin (\mathbb{Q}^\times)^2$. Soit L un corps de décomposition de P sur $\mathbb{Q}$. Montrer que $\mathrm{Gal}(L/\mathbb{Q}) \cong GA_1(\mathbb{Z}/4\mathbb{Z})$.

Exercice 11 : Irréductibilité de polynômes
Soient K un corps, $a \in K$, $r \geq 1$ et p un nombre premier. Soit $P = X^{p^r} - a \in K[X]$.

1. On suppose que $p \neq 2$ ou $\mathrm{Car}(K) = p$ ou $r = 1$. Montrer que P est irréductible si, et seulement si, $a \notin K^p$.
2. On suppose que $p = 2$, $\mathrm{Car}(K) \neq 2$ et $r \neq 1$. Montrer que P est irréductible si, et seulement si, $a \notin K^2$ et $-4a \notin K^4$.

Exercice 12 (à préparer) : Extensions abéliennes
Soient K un corps de caractéristique nulle et n un entier naturel. On suppose que, pour toute extension finie L de K, l'indice $[L^\times : (L^\times)^n]$ est fini. Montrer que le corps K possède un nombre fini d'extensions abéliennes de degré n.

Exercice 13 : Extensions cycliques

Soient K un corps et $\overline{K}$ une clôture algébrique de K.

1. Soit $\sigma \in \mathrm{Aut}(\overline{K}/K)$. Montrer que toute extension finie de $\overline{K}^{\langle\sigma\rangle}$ dans $\overline{K}$ est cyclique.

2. Montrer que si toute extension finie de K dans $\overline{K}$ est cyclique, alors il existe $\sigma \in \mathrm{Aut}(\overline{K}/K)$ tel que $K = \overline{K}^{\langle\sigma\rangle}$.

Exercice 14 : Sous-corps d'un corps algébriquement clos

Soit Ω un corps algébriquement clos de caractéristique nulle. Soit K un sous-corps de Ω tel que l'extension Ω/K est de degré fini. Le but de cet exercice est de montrer que $\Omega = K(\sqrt{-1})$.

1. Expliquer pourquoi Ω/K est galoisienne.

Soit i une racine de X^2+1 dans Ω. On pose $G = \mathrm{Gal}(\Omega/K(i))$. On suppose que G n'est pas trivial et on se donne p un nombre premier divisant l'ordre de G.

2. Montrer qu'il existe un sous-corps L de Ω contenant $K(i)$ tel que Ω/L est une extension galoisienne de degré p.

3. Montrer qu'il existe $a \in L$ tel que le polynôme $P = X^p - a \in L[X]$ est irréductible et $\Omega = L[X]/(P)$.

4. Soit $\alpha \in \Omega$ une racine de P. Calculer $N_{\Omega/L}(\alpha)$.

5. Conclure.

6. Montrer qu'un élément non trivial de $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ d'ordre fini est forcément d'ordre 2.

Exercice 15 : Partiel 2013

Soit $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$ et soit $a \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$.

1. Montrer qu'il existe un sous-corps K de $\overline{\mathbb{Q}}$ tel que $a \notin K$ et que tout sous-corps de $\overline{\mathbb{Q}}$ contenant strictement K contient a ; on dit que K est un sous-corps de $\overline{\mathbb{Q}}$ maximal sans a.

On choisit un nombre premier p divisant $[K(a) : K]$. Soit L une extension finie non triviale de K contenue dans $\overline{\mathbb{Q}}$. On note M la clôture normale de L dans $\overline{\mathbb{Q}}$ et $G := \mathrm{Gal}(M/K)$.

2. Montrer que p divise $[L : K]$.

3. Montrer que $[L : K]$ est une puissance de p.

4. Montrer que $[K(a) : K] = p$ et que $K(a)$ est la seule sous-extension de $\overline{\mathbb{Q}}/K$ de degré p sur K.

5. Montrer que G est cyclique, puis que toute extension finie de K est galoisienne cyclique.

6. Montrer qu'il existe $b \in K(a)$, avec $b^p \in K$, tel que $K(a) = K(b)$.

Exercice 16 : Extensions d'Artin-Schreier
Soient K un corps de caractéristique $p > 0$ et L/K une extension galoisienne de degré p. Soit σ un générateur de $\mathrm{Gal}(L/K)$.

1. Montrer qu'il existe $x \in L$ vérifiant $\sigma(x) - x = 1$.
2. Montrer qu'il existe $a \in K^\times$ tel que L soit le corps de décomposition de $X^p - X - a$.

Exercice 17 : Partiel 2011
Considérons le polynôme $P = X^4 - X - 1 \in \mathbb{Q}[X]$.

1. Montrer que P a exactement deux racines réelles distinctes x_1 et x_2.
2. On écrit $(X - x_1)(X - x_2) = X^2 + aX + b$. Calculer $[\mathbb{Q}(a^2) : \mathbb{Q}]$.
3. En déduire qu'aucune des racines de P n'est constructible à la règle et au compas.

Exercice 18 : Constructibilité et angles
Soit n un entier naturel. Montrer que l'angle de $n°$ est constructible si, et seulement si, 3 divise n.

Exercice 19 : Examen 2012
Le polynôme $X^5 - 5X^2 + 1 \in \mathbb{Q}[X]$ est-il résoluble par radicaux ?

Exercice 20 : Une extension non résoluble
Soit $f \in \mathbb{Q}[X]$ de degré 7 irréductible. On suppose que f contient exactement 3 racines réelles. Montrer que f n'est pas résoluble par radicaux.

Exercice 21 : Résolubilité par radicaux réels
Soient K un sous-corps de $\mathbb{R}$, $p > 2$ un nombre premier et $a \in K$ qui n'est pas une puissance p-ème dans K. Soit $x \in \mathbb{R}$ vérifiant $x^p = a$.

1. Montrer que $K \subseteq K(x)$ n'est pas galoisienne.

Une extension $K \subseteq L$ est dite *radicale réelle* s'il existe une tour d'extensions

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R}$$

telle que $L \subseteq K_n$ et, pour tout i, $K_{i+1} = K_i(x_i)$ avec $x_i^{n_i} \in K_i$ pour un certain entier $n_i \geq 1$. Un polynôme est dit *résoluble par radicaux réels* si son corps de décomposition l'est.
Soit $K \subseteq L$ une extension galoisienne radicale réelle.

2. En se ramenant à une tour avec degrés successifs premiers, montrer que $[L : K]$ est une puissance de 2.
3. Donner un exemple de telle extension.
4. Montrer que l'extension $\mathbb{Q} \subseteq \mathbb{Q}\big(\cos(\frac{2\pi}{7})\big)$ est radicale mais pas radicale réelle.

Soit $P \in K[X]$ un polynôme irréductible de degré 3.

5. Montrer que si P a trois racines réelles x, y, z, alors aucune des extensions $K(x)/K$, $K(y)/K$ et $K(z)/K$ n'est radicale réelle (résultat dû à Hölder).

On rappelle les formules de Tartaglia-Cardan : les zéros du polynôme $X^3 + bX + c$ sont les

$$\xi\sqrt[3]{-\frac{c}{2}+\sqrt{\frac{c^2}{4}+\frac{b^3}{27}}}+\xi^2\sqrt[3]{-\frac{c}{2}-\sqrt{\frac{c^2}{4}+\frac{b^3}{27}}}$$

pour ξ parcourant les racines 3-èmes de l'unité.

6. Montrer que si P n'a qu'une racine réelle x, alors $K(x)/K$ est radicale réelle.

Exercice 22 : Descente pour les espaces vectoriels

Soit $n \geq 1$ un entier. Soient $F \subseteq E$ une extension galoisienne (ie. normale et séparable) finie, de base $\{1, x_1, \ldots, x_{n-1}\}$. Notons $G = \mathrm{Gal}(E/F)$.

1. Rappeler pourquoi les éléments de G sont linéairement indépendants sur E.

Soit V un espace vectoriel sur E, muni d'une action semi-linéaire de G, c'est-à-dire d'une action telle que, pour $g \in G, \lambda \in E, v \in V$, on a $g\cdot(\lambda v) = g(\lambda)v$. On définit son sous-$F$-espace vectoriel des G-invariants $V^G = \{v \in V \mid \forall g \in G,\ gv = v\}$.

2. Vérifier que l'application E-linéaire $V^G \otimes_F E \xrightarrow{\eta} V$ canonique est compatible à l'action de G.

3. Montrer que η est un isomorphisme.

Exercice 23 : Hilbert 90 et applications

Soient K un corps et L/K une extension galoisienne finie. Soit $G = \mathrm{Gal}(L/K)$. On rappelle que les éléments de G sont linéairement indépendants.

1. On suppose que l'extension L/K est cyclique de degré n. Soient σ un générateur de G et $x \in L$.

(a) Montrer que x est de norme 1 si et seulement si il existe $y \in L^\times$ tel que l'on ait $x = \dfrac{\sigma(y)}{y}$.

(b) En utilisant la question précédente appliquée à une extension L/K bien choisie, exhiber deux fractions rationnelles $F, G \in \mathbb{Q}(X, Y)$ telles que l'application $\mathbb{Q}^2 \setminus \{(0,0)\} \to \mathbb{R}^2, (x, y) \mapsto (F(x, y), G(x, y))$ est bien définie et son image est exactement constituée des points à coordonnées rationnelles du cercle de centre $(0, 0)$ et de rayon 1.

2. On ne suppose plus L/K cyclique.

(a) Soit $f : G \to L^\times$ une fonction telle que, pour tous $s, t \in G$, on a $f(st) = s(f(t))f(s)$. Montrer qu'il existe $x \in L^\times$ tel que, pour tout $s \in G$, on a $f(s) = s(x)x^{-1}$.

(b) Étant donnés un corps E et un entier naturel n, on note $\mathbb{P}^n(E)$ l'espace projectif de dimension n, c'est-à-dire l'ensemble des droites de E^{n+1}. Montrer que l'action naturelle de G sur L^{n+1} induit une action de G sur $\mathbb{P}^n(L)$. Montrer que $\mathbb{P}^n(L)^{\mathrm{Gal}(L/K)} = \mathbb{P}^n(K)$.

Exercice 24 : Extensions cycliques et normes

Soit $n \geq 2$. Soit K un corps tel que $|\mu_n(K)| = n$ et $\mathrm{Car}(K) \nmid n$. Soit $a \in K^\times$ pour lequel le corps $L = K(\sqrt[n]{a})$ vérifie $[L : K] = n$. Le but de cet exercice est de montrer que les assertions suivantes sont équivalentes :

(i) il existe une extension finie galoisienne M/K contenant L telle que $\mathrm{Gal}(M/K) \cong \mathbb{Z}/n^2\mathbb{Z}$;

(ii) $\mu_n \subseteq N_{L/K}(L^\times)$.

1. On suppose (i) et on note σ un générateur de $\mathrm{Gal}(M/K)$.

(a) Montrer qu'il existe $b \in L$ tel que $M = L(\sqrt[n]{b})$.

(b) Soit $c = \frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}$. Montrer que $c \in L$.

(c) Montrer que $N_{L/K}(c)$ est un générateur de μ_n. En déduire (ii).

2. On suppose (ii) et on note τ un générateur de $\mathrm{Gal}(L/K)$. Soit $z \in L$ tel que $N_{L/K}(z)$ est un générateur de μ_n.

(a) En utilisant la question 1.(a) de l'exercice 23, montrer qu'il existe $b \in L^\times$ tel que $z^n = \frac{\tau(b)}{b}$.

(b) Soit $M = L(\sqrt[n]{b})$. Montrer que τ se prolonge en un automorphisme de corps $\sigma \in \mathrm{Aut}(M/K)$.

(c) En utilisant que $z^n = \frac{\tau(b)}{b}$, montrer que $\frac{\sigma^n(\sqrt[n]{b})}{\sqrt[n]{b}}$ est un générateur de μ_n.

(d) En déduire que M/K est galoisienne cyclique de degré n^2.