Université de Nice-Sophia-Antipolis
16 novembre 2009
Préparation à l'agrégation (Rémy Oudompheng)

TD d'algèbre n°25 : corps de rupture, corps de décomposition, corps finis

Exercice 1 (Extensions de Kummer)**.** On suppose que $\Bbbk$ est un corps contenant les racines p-ièmes de l'unité, où p est un nombre premier. Par exemple, $\Bbbk = \mathbb{Q}[\sqrt{-3}]$ et $p = 3$.

1. Soit L une extension galoisienne de $\Bbbk$ de degré p. Montrer que les automorphismes $\Bbbk$-linéaires de L sont de la forme σ^k, où σ est un certain automorphisme et $k = 0, \dots, (p-1)$.
2. Montrer que l'action de σ sur L est diagonalisable, et qu'il existe $x \in L$ tel que $\sigma(x) = \zeta x$, où ζ est une racine primitive p-ième de l'unité.
3. En déduire que le polynôme minimal de x est de la forme $X^p - a$ où $a \in \Bbbk$. On a ainsi montré que $L \simeq \Bbbk[\sqrt[p]{a}]$.

Exercice 2 (La méthode de Cardan, voir Artin 14.2)**.** Soit $P = X^3 + pX + q$ un polynôme de degré 3 sur $\Bbbk$, n'admettant pas de racine dans $\Bbbk$, et α l'une de ses racines dans $\mathbb{A}$. On note α_2 et α_3 ses autres racines.

Le discriminant de P est la quantité

$$\Delta = (\alpha - \alpha_2)^2(\alpha - \alpha_3)^2(\alpha_2 - \alpha_3)^2$$

1. Montrer que si $\Bbbk$ ne contient pas de racine cubique de l'unité (notée j), le corps $\Bbbk' = \Bbbk[j]$ ne contient pas non plus de racine de P. Dans la suite, on supposera que $j \in \Bbbk$.
2. Montrer (ou admettre) que $\Delta = -4p^3 - 27q^2$.
3. Soit $K = \Bbbk[\alpha]$ et L le corps de décomposition de P. Montrer que L est de degré 1 ou 2 sur K. En déduire que si Δ n'est pas un carré dans $\Bbbk$, L est une extension quadratique de K, de la forme $K[\sqrt{\Delta}]$.

   Remarque : si Δ est un carré, $L = K$ (ceci découle de la théorie de Galois).
4. Montrer que L est une extension normale de $Q = \Bbbk[\sqrt{\Delta}]$, de degré 3. En déduire que $L = Q[\alpha]$ est une extension de Kummer, et qu'il existe un automorphisme Q-linéaire de L, noté σ, tel que $\sigma(\alpha) = \alpha_2$ et $\sigma(\alpha_2) = \alpha_3$.

   D'après ce qui précède, $Q[\alpha]$ est un corps de la forme $Q[\sqrt[3]{u}]$: la racine α s'exprime donc de façon simple à l'aide de la racine cubique d'un élément $u \in Q$. Dans la suite, on va chercher la valeur de u.
5. On pose $u = \alpha + j\alpha_2 + j^2\alpha_3$ et $v = \alpha + j^2\alpha_2 + j\alpha_3$. Exprimer α en fonction de u et v, et montrer que u et v sont des vecteurs propres de σ. Établir la relation $uv = -3p$.
6. Utiliser les techniques de l'exercice précédent pour montrer que $U = u^3$ est un élément de Q, et montrer que $L \simeq Q[\sqrt[3]{U}]$. On peut vérifier que $2U = -27q + 3\sqrt{-3\Delta}$: c'est bien un élément de Q.

La formule

$$\alpha = \sqrt[3]{-\frac{q}{2} + \frac{\sqrt{-\Delta/27}}{2}} + \sqrt[3]{-\frac{q}{2} - \frac{\sqrt{-\Delta/27}}{2}}$$

est appelée *formule de Cardan.*

Exercice 3 (Les corps finis [Per82, 3.2])**.** Ici, $\mathbb{F}$ est un corps possédant un nombre fini d'éléments, noté q.

1. Montrer que si $x \in \mathbb{F}$ est non nul, $x^{q-1} = 1$.
2. On note ϕ_d le nombre d'éléments d'ordre d dans le groupe $\mathbb{Z}/(q-1)\mathbb{Z}$. Montrer que $\sum \phi_d = q - 1$. On note μ_d le nombre d'éléments d'ordre d dans le groupe multiplicatif $\mathbb{F}^\times$. Montrer que $\sum \mu_d = q - 1$.
3. Soit x un élément d'ordre d dans $\mathbb{F}^\times$. Montrer que x et ses puissances sont les seules racines de $X^d - 1$. En déduire que $\mu_d \leq \phi_d$.
4. Montrer qu'il existe un élément d'ordre multiplicatif $q - 1$ dans $\mathbb{F}$. Donner un polynôme dont $\mathbb{F}$ est le corps de décomposition (sur son sous-corps premier) : en déduire que tout corps fini de cardinal q est isomorphe à $\mathbb{F}$.

Exercice 4 (L'automorphisme de Frobenius)**.** Soit $q = p^n$ une puissance d'un nombre premier p. On considère un corps fini de cardinal q noté $\mathbb{F}_q$.

1. Soit F l'application définie par $F(x) = x^p$. Montrer que F est un automorphisme de corps de $\mathbb{F}_q$. Il est appelé *automorphisme de Frobenius*.
2. Soit $G : \mathbb{F}_q \to \mathbb{F}_q$ un morphisme de corps. Montrer que G est un isomorphisme, de la forme $x \mapsto x^k$ avec $k < p^n$.
3. Montrer que l'entier k ci-dessus est un multiple de p. (On pourra étudier la valeur de $F(ax)$ pour $a \in \mathbb{Z}/p\mathbb{Z}$.)
4. Montrer que $x \mapsto x^{k/p}$ est aussi un morphisme de corps. En conclure que k doit être une puissance de p.

On a ainsi montré que le groupe $\mathrm{Aut}(\mathbb{F}_q)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et engendré par l'automorphisme de Frobenius.

Exercice 5 (Le théorème de l'élément primitif (encore !))**.** Voici une autre façon de démontrer le théorème de l'élément primitif :

1. Soit P un polynôme irréductible sur $\Bbbk$, et L son corps de décomposition. Montrer que P est à racines simples.
2. Soit $K \subset \mathbb{A}$ une extension finie de $\Bbbk$, de degré n. On choisit une base $\mathcal{B}$ de K comme $\Bbbk$-espace vectoriel. Soit z un élément de K et M_z la matrice de l'application $\omega \mapsto z\omega$. Montrer que M_z est diagonalisable dans $\mathbb{A}$, et que $K = \Bbbk[z]$ si et seulement si les valeurs propres de M_z sont distinctes.
3. On suppose que K est engendrée par deux éléments x et y. Montrer que les matrices M_x et M_y sont codiagonalisables. On note
$$x = x_0, x_1, \dots x_{n-1}$$
$$y = y_0, y_1, \dots y_{n-1}$$
les valeurs propres des matrices M_x et M_y. En déduire que pour tout z, M_z est diagonalisable.
4. Montrer que l'application $z \to \tau_i(z)$ qui à $z \in K$ associe la i-ième valeur propre de M_z est un morphisme de corps $K \to \mathbb{A}$. En s'inspirant de l'exercice précédent, montrer que les matrices-lignes associées aux τ_i sont les lignes d'une matrice Σ telles que $\Sigma M_z \Sigma^{-1}$ est diagonale.
5. En déduire que les τ_i sont des applications distinctes. En raisonnant par l'absurde, conclure qu'il existe une combinaison $\Bbbk$-linéaire $z_0 = ax + by$ dont les valeurs propres sont toutes distinctes, et qu'alors $K = \Bbbk[z_0]$.
6. Démontrer le théorème. (*Indication* : considérer un ensemble de générateurs de K de taille minimale ≥ 2, et obtenir une contradiction.)

[Art91] Michael Artin, *Algebra*, Prentice Hall Inc., Englewood Cliffs, NJ, 1991. MR 1129886 (92g :00001)

[Per82] Daniel Perrin, *Cours d'algèbre*, Collection de l'École Normale Supérieure de Jeunes Filles, vol. 18, École Normale Supérieure de Jeunes Filles, Paris, 1982 (French). Edited with the collaboration of Marc Cabanes and Martine Duchene. MR 749037 (86a :00001)