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

TD d'algèbre n°23 : corps de rupture, corps de décomposition

Dans cette feuille d'exercices, $\mathbb{k}$ est un corps, et $\mathbb{A}$ est un corps algébriquement clos contenant $\mathbb{k}$. Par exemple $\mathbb{k} = \mathbf{Q}$ et $\mathbb{A} = \mathbf{C}$. Sauf indication contraire, on supposera que $\mathbb{k}$ est de caractéristique zéro.

Références : Perrin [Per82, III.1], Escofier [Esc04] voir aussi Artin [Art91], Jacobson [Jac85].

Exercice 0 (Prolégomènes)**.** Démontrer les propriétés suivantes :
- soient P, Q des polynômes à coefficients dans $\mathbb{k}$, et $\bar{Q}$ la classe de Q dans $\mathbb{k}[X]/(P)$; alors $\bar{Q}$ est un diviseur de zéro si et seulement si $\bar{Q}$ et P ont un facteur commun (non trivial) ;
- soit A une $\mathbb{k}$-algèbre commutative intègre de dimension finie sur $\mathbb{k}$; alors A est un corps ;
- soit $P \in \mathbb{k}[X]$; P est à racines simples dans $\mathbb{A}$ si et seulement si P et P' sont premiers entre eux.

Exercice 1 (Corps de rupture, corps de décomposition ?)**.** Pour chaque $\mathbb{k}$ et P, dire si le corps de rupture de P est un corps de décomposition. Quel est le degré du corps de décomposition ?
- $\mathbb{k} = \mathbb{R}$, $P = X^2 + 1$;
- $\mathbb{k} = \mathbb{Q}$, $P = X^2 + X + 1$;
- $\mathbb{k} = \mathbb{Q}$, $P = X^3 - 2$;
- $\mathbb{k} = \mathbb{Z}/3\mathbb{Z}$, $P = X^3 + X^2 + 2$.

Exercice 2 (Le théorème de l'élément primitif [Per82, Ex. III.1.6], voir aussi [FG97, 4.7] et [Art91, 14.4.1])**.** On va démontrer le théorème suivant :

> Soit $\mathbb{k}$ un corps de caractéristique zéro, et L une extension finie de $\mathbb{k}$. Il existe un élément $x \in L$ tel que $L = \mathbb{k}[x]$.

1. Soit $L = \mathbb{k}[x, y]$ une extension finie de $\mathbb{k}$ engendrée par deux éléments, de polynômes minimaux $P, Q \in \mathbb{k}[X]$. Montrer qu'il existe $t \in \mathbb{k}$ tel que pour toute racine $x_i \neq x$ de P et $y_j \neq y$ de Q, $x + ty \neq x_i + ty_j$.
2. On pose $z = x + ty$ et $F(X) = P(z - tX)$. Montrer que y est la seule racine commune à F et Q. En déduire le PGCD de F et Q : il s'agit d'un élément de $K[X]$, où $K = \mathbb{k}[z]$.
3. Montrer que y appartient à K, ainsi que x.
4. Démontrer le théorème, par récurrence sur le degré de l'extension.

Remarque : le théorème de l'élément primitif est encore valable en caractéristique p, à condition de supposer que L est *séparable*.

Application : montrer que $\sqrt{2} + \sqrt{3}$ engendre le corps $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ en tant qu'extension de $\mathbb{Q}$. Ce corps est-il un corps de décomposition ? Quel est le polynôme minimal de $\sqrt{2} + \sqrt{3}$? Donner des polynômes P_2 et P_3 tels que $\sqrt{2}$ et $\sqrt{3}$ soient $P_2(\sqrt{2} + \sqrt{3})$ et $P_3(\sqrt{2} + \sqrt{3})$.

Exercice 3 (Un peu d'algèbre linéaire)**.** Soit P un polynôme irréductible de degré n sur $\mathbb{k}$, et α une racine de P dans $\mathbb{A}$.

1. Montrer que la sous-algèbre $L = \mathbb{k}[\alpha] \subset \mathbb{A}$ est une extension de corps de degré n sur $\mathbb{k}$. Montrer que $(1, \alpha, \ldots, \alpha^{n-1})$ est une base de L comme $\mathbb{k}$-espace vectoriel.
2. Soit $A \in \mathcal{M}_n(\mathbb{k})$ la matrice de l'application $x \mapsto \alpha x$ dans la base choisie précédemment. Montrer que A est diagonalisable en tant que matrice de $\mathcal{M}_n(\mathbb{A})$. Montrer que de plus, A est diagonalisable dans $\mathcal{M}_n(L)$ si et seulement si L est un corps de décomposition de P.

3. Montrer que pour tout $\lambda \in L$, la matrice M_λ de l'application $x \to \lambda x$ est aussi diagonalisable, *dans la même base* que A.
4. En déduire la propriété suivante : si $L = \Bbbk[\alpha]$ est un corps de décomposition de P, le polynôme minimal d'un élément quelconque $\lambda \in L$ est scindé dans L, à racines simples. On dit que L est une extension *normale* de $\Bbbk$ (on dit aussi que L est une extension *galoisienne*, lorsque L est de plus *séparable*).

Exercice 4 (Le groupe de Galois)**.** Ici encore, P est un polynôme irréductible de degré n et $L = \Bbbk[\alpha] \simeq \Bbbk[X]/(P)$ est un corps de rupture de P. En suivant les notations de l'exercice précédent, si $x \in L$, on note M_x la matrice de l'application $a \mapsto xa$ dans la base $(1, \alpha, \ldots, \alpha^{n-1})$.

1. Rappeler pourquoi il existe une base de vecteurs propres (à coordonnées dans $\mathbb{A}$), commune à toutes les matrices M_x.
   On posera $M_x = PD_xP^{-1}$, où D est une matrice diagonale. Les lignes de P^{-1} sont notées $\sigma_1, \ldots, \sigma_n$, et fournissent des formes $\Bbbk$-linéaires $L \to \mathbb{A}$.
2. On note $\tau_i(\lambda) \in \mathbb{A}$ la i-ième valeur propre de M_λ. Montrer que $\tau_i : L \to \mathbb{A}$ est un morphisme de corps, et montrer que les τ_i sont deux à deux distincts.
3. Montrer que pour tous λ et x dans L, $\sigma_i(\lambda x) = \tau_i(\lambda)\sigma_i(x)$. En déduire que σ_i et τ_i sont proportionnels, et qu'on peut choisir $\sigma_i = \tau_i$. Les σ_i sont appelés *caractères* de la $\Bbbk$-algèbre L.
4. Montrer que Σ^{-1} est une matrice de Vandermonde. Quelle est la relation entre son déterminant et le *discriminant* du polynôme ?
5. Montrer qu'il y a au plus n morphismes de corps $L \to \mathbb{A}$. En déduire que les seuls caractères de L (i.e. morphismes de $\Bbbk$-algèbres de L dans $\mathbb{A}$) sont les σ_i.
   Si L est un corps de décomposition, l'image de σ_i est contenue dans L : en déduire que les σ_i sont tous les morphismes de corps $L \to L$ qui sont $\Bbbk$-linéaires. Ils forment un groupe appelé *groupe de Galois* de L.

Remarque : si $\Bbbk$ est de caractéristique p, les résultats démontrés sont encore valables à condition de supposer que P est *séparable*, ce qui signifie que P et P' (son polynôme dérivé) sont premiers entre eux. Par exemple, si $\Bbbk = \mathbb{F}_p(t)$, le polynôme $P(X) = X^p - t$ n'est pas séparable.

Exemple : on choisit $L = \mathbb{Q}[z]$ où $z = \sqrt{2} + \sqrt{3}$, et la base $L = \mathbb{Q} \oplus \mathbb{Q}\sqrt{2} \oplus \mathbb{Q}\sqrt{3} \oplus \mathbb{Q}\sqrt{6}$. Écrire la matrice M_z. Est-elle diagonalisable dans L ? Trouver 4 automorphismes de L et en déduire la diagonalisation de M_z.

Exercice 5 (Trace et norme)**.** Soit L une extension de $\Bbbk$. La trace et la norme d'un élément $\lambda \in L$ sont respectivement la trace et le déterminant de l'application linéaire $x \mapsto \lambda x$. On les note $\mathrm{Tr}_{L/\Bbbk}(\lambda)$ et $N_{L/\Bbbk}(\lambda)$.

1. Montrer que l'application $(x, y) \to \mathrm{Tr}_{L/\Bbbk}(xy)$ définit une forme bilinéaire non dégénérée sur le $\Bbbk$-espace vectoriel L. (Indice : comment choisir y pour que $\mathrm{Tr}(xy)$ soit très facle à calculer ?)
2. Si L est une extension galoisienne de $\Bbbk$, exprimer la trace et la norme en fonction des éléments du groupe de Galois.

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

[Esc04] J.-P. Escofier, *Théorie de Galois : cours et exercices*, Dunod, 2004.

[FG97] S. Francinou and H. Gianella, *Exercices de mathématiques pour l'agrégation : tome 1. Algèbre*, Dunod, 1997.

[Jac85] Nathan Jacobson, *Basic algebra. I*, 2nd ed., W. H. Freeman and Company, New York, 1985. MR 780184 (86d :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)