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

TD d'algèbre n°23 : corrigé

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

Références : [Per82, III.1], voir aussi Artin, Escofier.

Exercice 0 (Prolégomènes)**.** Pour la première assertion, supposons que $\bar{Q}$ soit un diviseur de zéro dans $\Bbbk[X]/(P)$. Alors, il existe un polynôme R non divisible par P, tel que $\bar{Q}\bar{R} = 0$. Cela signifie que P divise QR. Comme P ne divise pas R, il existe un facteur irréductible de P qui divise QR et pas R, il divise donc Q. Réciproquement, si Q admet un facteur commun M non trivial avec P, on écrit $P = MP_2$ et alors $\bar{Q}\bar{P}_2 = 0$ dans $\Bbbk[X]/(P)$.

Si A est une $\Bbbk$-algèbre intègre de dimension finie, et si $x \in A$ est non nul, par définition, l'application $x : A \to A$ de multiplication par x est linéaire et injective. Comme A est de dimension finie, cette application est bijective, il existe donc un y tel que $xy = 1$.

Pour la dernière assertion, on commence par constater que si $\Bbbk = \mathbb{A}$, P est un polynôme scindé. Dans ce cas, on voit facilement que si P admet une racine double α, $(X - \alpha)$ divise P et P'. En revanche, si α est une racine simple, on a $P = (X - \alpha)Q$ et $P' = (X - \alpha)Q' + Q$, et $(X - \alpha)$ ne divise pas Q donc pas P' : en faisant ce raisonnement pour toutes les racines de P, on en conclut que P et P' n'ont pas de facteur commun. Pour le cas général, on remarque que le PGCD de P et P' est le même dans $\Bbbk$ et $\mathbb{A}$.

Exercice 1 (Corps de rupture, corps de décomposition)**.** Pour chaque $\Bbbk$ et P, dire si le corps de rupture de P est un corps de décomposition. Quel est le degré du corps de décomposition ?

- $\Bbbk = \mathbb{R}$, $P = X^2 + 1$: le corps de rupture de P est $\mathbb{C}$, qui est de degré 2 sur $\mathbb{R}$. C'est un corps de décomposition, les racines de P sont i et $-i$.
- $\Bbbk = \mathbb{Q}$, $P = X^2 + X + 1$: le corps de rupture de P est de degré 2 sur $\mathbb{Q}$, et contient les deux racines j et j^2 de P, c'est un corps de décomposition.
- $\Bbbk = \mathbb{Q}$, $P = X^3 - 2$: le corps de rupture est isomorphe à $\mathbb{Q}[\sqrt[3]{2}]$, qui ne contient pas $j\sqrt[3]{2}$, par exemple. Le corps de décomposition de $X^3 - 2$ est de degré 6.
- $\Bbbk = \mathbb{Z}/2\mathbb{Z}$, $P = X^3 + X^2 + 1$: le polynôme P n'admet pas de racine dans $\mathbb{F}_2$, il est donc bien irréductible. On vérifie que si α est une racine de P dans le corps de rupture $\Bbbk[X]/(P)$, α^2 est aussi une racine. Or la somme des racines est 1, donc la dernière racine est $1 + \alpha + \alpha^2$.
  On peut d'ailleurs vérifier que $\alpha^4 = \alpha^3 + \alpha = 1 + \alpha + \alpha^2$.

Exercice 2 (Le théorème de l'élément primitif [Per82, Ex. III.1.6], voir aussi [FG97, 4.7] et [Art91, 14.4.

Les applications $f_{ij} : t \mapsto x_i + ty_j$ de $\Bbbk$ dans L sont distinctes, et deux d'entre elles ne peuvent admettre une valeur commune que pour une seule valeur de t. Il n'y a donc qu'un nombre fini de valeurs interdites pour t. Si $\Bbbk$ est infini (ce qui est le cas en caractéristique zéro), il existe une valeur de t telle que $f_{ij}(t)$ soit différent de $x + ty$ pour tous i et j.

2. Avec $z = x + ty$, z est un élément de L. Si $F(X) = P(z - tX)$, F est un polynôme à coefficients dans L. Supposons que $F(u) = Q(u) = 0$. Alors u est une racine de Q : noter que $u = y$ convient. Si $u = y_j$ est différent de y, $z - ty_j$ est une racine de P, nécessairement différente de $z - ty = x$, et on peut écrire $z = x_i + ty_j$ pour un $x_i \neq x$, ce qui est impossible.
   Comme F et Q n'ont pas de racine double, le PGCD de F et Q est $X - y$.

3. Comme les coefficients de F et de Q appartiennent à $\Bbbk[z]$, $X - y$ est aussi à coefficients dans $\Bbbk[z]$, donc y et $x = z - ty$ appartiennent à $\Bbbk[z]$, qui est en fait tout L.
4. Soit L une extension finie de $\Bbbk$. Il existe donc un système fini de générateurs de L. Considérons un système de générateurs de taille minimale, et $x \neq y$ des éléments de ce système. Par la construction précédente, on peut remplacer x et y par un seul élément $z \in \Bbbk[x, y]$, ce qui contredit le fait qu'on a choisi un système de générateurs de taille minimale.

Un contre-exemple simple en caractéristique p est donné par $K = \mathbb{F}_p(X^p, Y^p)$ et $L = \mathbb{F}_p(X, Y)$. En effet, L est de degré p^2 sur K et si x est un élément de L, $x^p \in K$, donc x n'engendre qu'un corps de degré p sur K.

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

1. Comme α est une racine de P, L est une algèbre intègre de dimension finie sur $\Bbbk$, c'est donc une extension de corps. De plus, L est isomorphe à $\Bbbk[X]/(P)$, qui est de degré n. Comme $(1, X, \ldots, X^{n-1})$ est une base de cette dernière, $(1, \alpha, \ldots, \alpha^{n-1})$ est une base de L.
2. Soit $A \in \mathcal{M}_n(\Bbbk)$ la matrice de l'application $x \mapsto \alpha x$. Si Q est un polynôme, $Q(A)$ est alors la matrice de la multiplication par $Q(\alpha)$. Le polynôme minimal de A est donc P, qui est scindé à racines simples dans $\mathbb{A}$.

   La matrice A est diagonalisable dans L si et seulement si son polynôme minimal est scindé à racines simples dans L, c'est-à-dire si L est un corps de décomposition de P.
3. Puisque qu'on a toujours $\lambda(ax) = a(\lambda x)$ dans L, les matrices M_λ et A commutent. Comme A est diagonalisable, à valeurs propres simples, M_λ et A sont codiagonalisables, dans l'unique base de diagonalisation de A.
4. Par conséquent, si L est un corps de décomposition, M_λ est codiagonalisable avec A sur L : le polynôme minimal de λ est donc scindé à racines simples *dans* L.

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)

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

[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)