Université de Bordeaux

Licence 3 - année 2020-2021
Structures algébriques 2 - 4TMFF502U

Devoir maison n°2

À rendre le 27 novembre (version scannée sur Moodle)

Dans ce qui suit, tous les anneaux considérés sont supposés commutatifs, et K désigne un corps.

(0) Si p est un nombre premier et A un anneau de caractéristique p, rappeler pourquoi l'application

$$\begin{aligned}\varphi_A\colon A &\to A\\ x&\mapsto x^p\end{aligned}$$

est un morphisme d'anneaux. On dit que A est *parfait* lorsque φ_A est un isomorphisme. Montrer qu'un corps fini est parfait.

On fixe $P \in K[X]$. Si $P(X) = a_d X^d + \cdots + a_0 \in K[X]$, on pose $P'(X) = d a_d X^{d-1} + \cdots + a_1$ (c'est le polynôme dérivé de P).

(1) Supposons $\mathsf{car}(K) = p > 0$. Montrer l'équivalence entre
  (i) $P' = 0$;
  (ii) $P \in K[X^p]$ (*i.e.* il existe $Q \in K[X]$ tel que $P(X) = Q(X^p)$) ;
et que si K est supposé parfait, ces conditions sont en outre équivalentes à
  (iii) il existe $R \in K[X]$ tel que $P(X) = R(X)^p$.

(2) Supposons P irréductible dans $K[X]$.
  (a) Montrer que si $\mathsf{car}(K) = 0$, alors $\mathsf{pgcd}(P', P) = 1$.
  (b) Montrer que si $\mathsf{car}(K) = p > 0$, on a $\mathsf{pgcd}(P', P) = \begin{cases} P & \text{si } P \in K[X^p] \\ 1 & \text{sinon} \end{cases}$. Si K est supposé parfait, montrer qu'on a $\mathsf{pgcd}(P', P) = 1$.
  (c) Donner un exemple de polynôme irréductible dans $(\mathbf{Z}/p\,\mathbf{Z})(T)[X]$ et dont la dérivée est nulle.

Désormais, on ne suppose plus P irréductible : soit $P = \prod_{i=1}^{r} P_i^{\alpha_i}$ avec $P_1, \ldots, P_r \in K[X]$ irréductibles deux à deux premiers entre eux et $\alpha_1, \ldots, \alpha_r \in \mathbf{N}_{>0}$ sa factorisation en produit d'éléments irréductibles.

(3) Exprimer P' en fonction de $P_1, \ldots, P_r$ et $\alpha_1, \ldots, \alpha_r$; montrer que $\prod_{i=1}^{r} P_i^{\alpha_i - 1} \mid \mathsf{pgcd}(P', P)$.
  (a) Montrer que si $\mathsf{car}(K) = 0$, on a $\mathsf{pgcd}(P', P) = \prod_{i=1}^{r} P_i^{\alpha_i - 1}$.
  (b) Montrer que si $\mathsf{car}(K) = p > 0$, on a $\mathsf{pgcd}(P', P) = \prod_{i=1}^{r} P_i^{\beta_i}$ avec

$$\beta_i = \begin{cases} \alpha_i - 1 & \text{si } p \nmid \alpha_i \text{ et } P_i' \neq 0 \\ \alpha_i & \text{sinon} \end{cases}.$$

On dit que P est *séparable* si $\alpha_1 = \cdots = \alpha_r = 1$ (*i.e.* si P est sans facteur carré).

(4) Supposons K de caractéristique 0 (resp. parfait de caractéristique $p > 0$). Montrer que $\mathsf{pgcd}(P', P) \in \{1, P\}$ si et seulement si P est séparable (resp. P est séparable ou $P' = 0$).

Ce qui précède montre que si K est de caractéristique nulle ou parfait de caractéristique $p > 0$, la factorisation des polynômes se ramène à celle des polynômes séparables.

On suppose désormais que $K = \mathbf{Z}/p\mathbf{Z}$ et que P est séparable. On pose $A = K[X]/\langle P \rangle$.

(5) Que vaut $\dim_K(A)$? Montrer que l'anneau A est produit de r extensions finies de K et que l'application φ_A est K-linéaire.

(6) Posons $E = \mathsf{Ker}(\varphi_A - \mathsf{Id}_A) \subset A$.

(a) Montrer que si L/K est une extension finie et $x \in L$, on a $\varphi_L(x) = x \Leftrightarrow x \in K$. En déduire que $\dim_K(E) = r$.

(b) Montrer que si $Q \in K[X]$ est tel que $\overline{Q} \in E$ (où $\overline{Q}$ désigne l'image de Q dans A) et $1 \leq \deg(Q) < \deg(P)$, alors on a

$$P(X) = \prod_{\lambda \in K} \mathsf{pgcd}(P(X), Q(X) - \lambda)$$

et que ce produit est une factorisation non triviale de P dans $K[X]$.

Cela fournit un algorithme de factorisation des polynômes à coefficients dans $K = \mathbf{Z}/p\mathbf{Z}$: on calcule la matrice de φ_A dans une base, puis le sous-espace propre associé à la valeur propre 1. S'il est de dimension 1, le polynôme P est irréductible dans $K[X]$, sinon un vecteur propre n'appartenant pas à la droite $K1$ fournit une factorisation non triviale, et on peut appliquer l'algorithme sur chaque facteur. Bien entendu, l'algorithme s'étend à un corps fini K quelconque : il suffit de prendre pour φ_A l'application $x \mapsto x^q$ où $q = \#K$.

(7) Appliquer l'algorithme à $X^p - X - 1 \in (\mathbf{Z}/p\mathbf{Z})[X]$.