Université de Bordeaux

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

# Devoir maison n°2

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 $\varphi_A$ 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 $\varphi_A$ 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 $\varphi_A$ 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 $\varphi_A$ l'application $x\mapsto x^q$ où $q=\#K$.*

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

Solution : (0) • Si $k\in\{1,\dots,p-1\}$, on a $\binom{p}{k}=\frac{p!}{k!(p-k)!}\equiv 0 \mod p$ : cela implique que si $x,y\in A$, on a $\varphi_A(x+y)=(x+y)^p=\sum_{k=0}^{p}\binom{p}{k}x^ky^{p-k}=x^p+y^p=\varphi_A(x)+\varphi_A(y)$. Comme on a bien sûr $\varphi_A(xy)=\varphi_A(x)\varphi_A(y)$ et $\varphi_A(1)=1$, l'application $\varphi_A$ est un morphisme d'anneaux.

• Si $K$ est un corps fini, alors $\varphi_K$ est injectif, donc bijectif par cardinalité.

(1) • Écricons $P(X)=a_dX^d+\cdots+a_0$ : on a $P'(X)=da_dX^{d-1}+\cdots+a_1$. On a donc $P'=0$ si et seulement si $ia_i=0$ pour tout $i\in\mathbf{Z}$, soit encore si et seulement si $a_i=0$ pour tout $i\in\mathbf{Z}\setminus p\mathbf{Z}$ (l'image de $i\in\mathbf{Z}\setminus p\mathbf{Z}$ dans $K$ est inversible). C'est précisément équivalent à $P\in K[X^p]$.

• Si $K$ est parfait, et si $P(X)=Q(X^p)$ avec $Q\in K[X]$, écrivons $Q(X)=b_mX^m+\cdots+b_0$. Pour tout $i\in\{0,\dots,m\}$, il existe $c_i\in K$ (unique) tel que $b_i=\varphi_K(c_i)=c_i^p$ (parce que $K$ est parfait). On a alors $P(X)=\sum_{i=0}^{m}c_i^pX_{pi}=R(X)^p$ avec $R(X)=\sum_{i=0}^{m}c_iX^i\in K[X]$.

(2) Comme $P$ est irréductible, on a $\mathsf{pgcd}(P',P)\in\{1,P\}$.

(a) Comme $P$ est irréductible, on a $\deg(P)>0$, et comme $\mathsf{car}(K)=0$, on a $P'\neq 0$. Cela implique que $0\leq\deg(P')<\deg(P)$ : on a nécessairement $\mathsf{pgcd}(P',P)=1$.

(b) • On a $\mathsf{pgcd}(P',P)=P$ si et seulement si $P\mid P'$. Comme $\deg(P')<\deg(P)$, cela équivaut à $P'=0$, *i.e.* à $P\in K[X^p]$ en vertu de la question (1).

• Si $K$ est parfait et $P'=0$, on sait qu'il existe $R\in K[X]$ tel que $P(X)=R(X)^p$ : le polynôme $P$ ne peut être irréductible dans ce cas. Si $P$ est irréductible, on a donc $\mathsf{pgcd}(P',P)=1$.

(c) Le polynôme $P(X)=X^p-T$ est irréductible dans $(\mathbf{Z}/p\mathbf{Z})[T][X]$ en vertu du critère d'Eisenstein appliqué avec l'élément premier $T\in(\mathbf{Z}/p\mathbf{Z})[T]$. Il est *a fortiori* irréductible dans $(\mathbf{Z}/p\mathbf{Z})(T)[X]$ (rappelons que $(\mathbf{Z}/p\mathbf{Z})[T]$ est factoriel), et $P'(T)=pX^{p-1}=0$.

(3) On a $P' = \sum_{i=1}^{r} \alpha_i P_i' \prod_{j=1}^{r} P_j^{\alpha_j - \delta_{i,j}}$ (où $\delta_{i,j}$ désigne le symbole de Kronecker). Cela implique que $\prod_{i=1}^{r} P_i^{\alpha_i - 1} \mid P'$, et donc que $\prod_{i=1}^{r} P_i^{\alpha_i - 1} \mid \mathsf{pgcd}(P', P)$. On a donc $\mathsf{pgcd}(P', P) = \prod_{i=1}^{r} P_i^{\beta_i}$ avec $\alpha_i - 1 \leq \beta_i \leq \alpha_i$ pour tout $i \in \{1, \ldots, r\}$.

(a) Pour tout $i \in \{1, \ldots, r\}$, on a $P' \equiv \alpha_i P_i' \prod_{j=1}^{r} P_j^{\alpha_j - \delta_{i,j}} \mod P_i^{\alpha_i}$. Comme $\alpha_i \neq 0$ et $P_i \nmid P_i'$ (parce que $\mathsf{car}(K) = 0$), on a $P_i^{\alpha_i} \nmid P'$ : on a $\beta_i = \alpha_i - 1$. Comme c'est vrai pour tout $i \in \{1, \ldots, r\}$, on a $\mathsf{pgcd}(P', P) = \prod_{i=1}^{r} P_i^{\alpha_i - 1}$.

(b) Pour tout $i \in \{1, \ldots, r\}$, on a $P' \equiv \alpha_i P_i' \prod_{j=1}^{r} P_j^{\alpha_j - \delta_{i,j}} \mod P_i^{\alpha_i}$. Si $p \nmid \alpha_i$ et $P_i' \neq 0$, on a $P_i \nmid \alpha_i P_i'$, et donc $P_i^{\alpha_i} \nmid P'$ : on a $\beta_i = \alpha_i - 1$ dans ce cas. Si $p \mid \alpha_i$ ou $P_i' = 0$, on a $P' \equiv 0 \mod P_i^{\alpha_i}$, donc $\beta_i = \alpha_i$.

(4) Le cas où $\mathsf{car}(K) = 0$ résulte de la question (3) (a). Supposons $K$ parfait de caractéristique $p > 0$. D'après la question (2) (b), on sait que $P_i' \neq 0$ pour tout $i \in \{1, \ldots, r\}$. Si $\mathsf{pgcd}(P', P) = 1$, on a $\alpha_i = 1$ pour tout $i \in \{1, \ldots, r\}$ (on ne peut avoir $p \mid \alpha_i = 1$), de sorte que $P$ est séparable. Si $\mathsf{pgcd}(P', P) = P$, on a $\beta_i = \alpha_i$ *i.e.* $p \mid \alpha_i$ pour tout $i \in \{1, \ldots, r\}$, ce qui implique $P' = 0$. Les réciproques sont triviales.

(5) • La division euclidienne par $P$ dans $K[X]$ implique que $(1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{d-1})$ est une $K$-base de $A$ (où $d = \deg(P)$ et $\overline{X}$ l'image de $X$ dans $A$). Cela implique en particulier que $\dim_K(A) = \deg(P)$.

• Comme $P$ est séparable, on a $P = P_1 \cdots P_r$ : pour tout $i \in \{1, \ldots, r\}$, posons alors $K_i = K[X]/\langle P_i \rangle$, c'est une extension finie de $K$. D'après le théorème des restes chinois, le morphisme naturel

$$\xi \colon A \to \prod_{i=1}^{r} K_i$$

est un isomorphisme d'anneaux. Comme $\varphi_A$ induit l'identité sur $K$, c'est en outre une application $K$-linéaire.

(6) (a) • On a $x^p = x$ pour tout $x \in K = \mathbf{Z}/p\mathbf{Z}$ : le polynôme $X^p - X$ est scindé dans $K[X]$, en particulier ses racines appartiennent toutes à $K$, ce qui montre que si $x \in L$, on a $x^p = x \Leftrightarrow x \in K$.

• Soit $x \in A$ : écrivons $\xi(x) = (x_1, \ldots, x_r)$ avec $x_i \in K_i$ pour tout $i \in \{1, \ldots, r\}$. On a $\xi(\varphi_A(x)) = (x_1^p, \ldots, x_r^p)$. On a donc $x \in E$ si et seulement si $x_i^p = x_i$ soit encore $x_i \in K$ pour tout $i \in \{1, \ldots, r\}$ d'après ce qui précède. Cela montre que $\xi$ induit un isomorphisme $K$-linéaire $E \xrightarrow{\sim} K^r \subset \prod_{i=1}^{r} K_i$, et donc que $\dim_K(E) = r$.

(b) • Pour tout $\lambda \in K$, on a $\mathsf{pgcd}(P(X), (X) - \lambda) \mid P(X)$. Par ailleurs, si $\lambda_1, \lambda_2 \in K$ sont disctincts, on a $\mathsf{pgcd}(Q(X) - \lambda_1, Q(X) - \lambda_2) = 1$, donc $\mathsf{pgcd}(P(X), Q(X) - \lambda_1)$ et $\mathsf{pgcd}(P(X), Q(X) - \lambda_2)$ sont premiers entre eux, et $\prod_{\lambda \in K} \mathsf{pgcd}(P(X), Q(X) - \lambda)$ divise $P(X)$. Par ailleurs, on a $\varphi_A(\overline{Q}) = \overline{Q}$, *i.e.* $P(X) \mid Q(X)^p - Q(X) = \prod_{\lambda \in K} (Q(X) - \lambda)$ (rappelons que $T^p - T = \prod_{\lambda \in K} (T - \lambda)$), et donc $P(X) \mid \prod_{\lambda \in K} \mathsf{pgcd}(P(X), Q(X) - \lambda)$.

• Si la factorisation était triviale, il existerait $\lambda \in K$ tel que $P(X) \mid Q(X) - \lambda$, et donc $Q(X) = \lambda$ vu que $\deg(Q - \lambda) < \deg(P)$, contrairement à l'hypothèse (on a $\deg(Q) \geq 1$).

**Remarque.** L'algorithme présenté ci-dessus s'appelle l'*algorithme de Berlekamp*.

(7) On se place dans la base $\mathfrak{B} = (1, \overline{X}, \overline{X}^2, \dots, \overline{X}^{p-1})$ de $A = (\mathbf{Z}/p\mathbf{Z})[X]/\langle X^p - X - 1\rangle$. On a $\varphi_A(1) = 1$, $\varphi_A(\overline{X}) = \overline{X}^p = \overline{X} + 1$ et donc $\varphi_A(\overline{X}^k) = (\overline{X}+1)^k = \sum_{j=0}^{k} \binom{k}{j} \overline{X}^j$ pour tout $k \in \{1, \dots, p-1\}$. On a donc

$$M = \mathsf{M}_{\mathfrak{B}}(\varphi_A) = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & p-1 \\ \vdots & \ddots & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & p-1 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

On a $\mathsf{rg}(M - \mathrm{I}_p) = p - 1$, ce qui implique que $\dim_{\mathbf{Z}/p\mathbf{Z}}(\mathsf{Ker}(\varphi_A - \mathsf{Id}_A)) = 1$ : le polynôme $X^p - X - 1$ est irréductible dans $(\mathbf{Z}/p\mathbf{Z})[X]$.