Recasages possibles : 123, 141, 142.
Référence : Objectif agrégation, Beck, Malick, Peyré (p. 244-248)

Développement

Théorème 1 Soient p premier, $n \in \mathbb{N}^*$, $q = p^n$, et $P \in \mathbb{F}_q[X]$ non constant et sans facteurs carrés. On considère la $\mathbb{F}_q$-algèbre $A = \mathbb{F}_q[X]/(P)$ et

$$\beta : \left| \begin{array}{ccc} A & \longrightarrow & A \\ \overline{Q(X)} & \longmapsto & \overline{Q(X)}^q \end{array} \right.$$

Alors, le nombre r de facteurs irréductibles de P est $\dim\big(\mathrm{Ker}(\beta - \mathrm{id}_A)\big)$. Si $r > 1$, et si $\overline{V(X)} \in \mathrm{Ker}(\beta - \mathrm{id}_A)$ n'est pas la classe d'un polynôme constant de $\mathbb{F}_q[X]$, alors on a la factorisation non triviale

$$P = \prod_{\alpha \in \mathbb{F}_q} P \wedge (V - \alpha).$$

Application 2 Le polynôme $X^p - X + 1 \in \mathbb{F}_p[X]$ est irréductible sur $\mathbb{F}_p$.

- *Preuve du Théorème 1* : Notons A la $\mathbb{F}_q$-algèbre $\mathbb{F}_q[X]/(P)$ et construisons l'application β. Considérons les morphismes de $\mathbb{F}_q$-algèbres suivants :

$$\mathcal{F} : \left| \begin{array}{ccc} \mathbb{F}_q[X] & \longrightarrow & \mathbb{F}_q[X] \\ Q(X) & \longmapsto & Q(X^q) \end{array} \right. \quad \text{et} \quad \pi : \left| \begin{array}{ccc} \mathbb{F}_q[X] & \longrightarrow & A \\ R(X) & \longmapsto & \overline{R(X)} \end{array} \right.$$

  Remarquons que $\mathcal{F}$ coïncide avec l'élévation avec la puissance q. En effet, si $Q(X) = \sum_{i=0}^{d} a_i X^i \in \mathbb{F}_q[X]$, on a pour tout $i \in [\![0, d]\!]$, $a_i = a_i^q$ (d'après le théorème de Lagrange si $a_i \neq 0$ et trivial si $a_i = 0$) donc

$$\mathcal{F}\big(Q(X)\big) = \sum_{i=0}^{d} a_i (X^q)^i = \sum_{i=0}^{d} a_i^q (X^i)^q = \left(\sum_{i=0}^{d} a_i X^i \right)^q = Q(X)^q.$$

  Le morphisme composé $\pi \circ \mathcal{F} : \mathbb{F}_q[X] \to A$ envoie donc $Q(X)$ sur $\overline{Q(X)}^q$. Remarquons que $(\pi \circ \mathcal{F})(P) = \overline{P(X)}^q = \overline{0}$ donc $P \in \mathrm{Ker}(\pi \circ \mathcal{F})$, puis $(P) \subset \mathrm{Ker}(\pi \circ \mathcal{F})$. Ainsi, $\pi \circ \mathcal{F}$ induit par factorisation le morphisme de $\mathbb{F}_q$-algèbre β introduit par l'énoncé. Remarquons tout de suite que β, en tant qu'endomorphisme d'un $\mathbb{F}_q$-espace vectoriel, admet 1 comme valeur propre. En effet, si $\alpha \in \mathbb{F}_q$,

$$\beta(\overline{\alpha}) = \overline{\alpha}^q = \overline{\alpha^q} = \overline{\alpha}.$$

  Ainsi, la droite vectorielle des classes des constantes $\mathrm{Vect}_{\mathbb{F}_q}(\overline{1})$ est contenue dans $\mathrm{Ker}(\beta - \mathrm{id}_A)$ et en particulier, $\dim\big(\mathrm{Ker}(\beta - \mathrm{id}_A)\big) \geqslant 1$. Écrivons $P = P_1 \cdots P_r$ une décomposition en produit d'irréductibles de $\mathbb{F}_q[X]$ (unique à l'ordre des facteurs et à association près), et montrons que $r = \dim\big(\mathrm{Ker}(\beta - \mathrm{id}_A)\big)$. Pour cela, on utilise le lemme chinois pour mieux comprendre l'action de β sur A. Comme P est supposé sans facteurs carrés, les P_i sont deux-à-deux distincts, donc ils sont deux-à-deux premiers entre eux car irréductibles sur $\mathbb{F}_q$. Ainsi, ce lemme nous donne l'isomorphisme de $\mathbb{F}_q$-algèbre suivant :

$$A \simeq \Big(\mathbb{F}_q[X]/(P_1)\Big) \times \cdots \times \Big(\mathbb{F}_q[X]/(P_r)\Big),$$

  qui est donné par la formule $\overline{Q} \mapsto \big(Q \bmod P_1, \ldots, Q \bmod P_r\big)$. Or, comme les P_i sont irréductibles sur $\mathbb{F}_q$, les anneaux $\mathbb{F}_q[X]/(P_i)$ sont des corps. Or, on sait que $\dim_{\mathbb{F}_q}\big(\mathbb{F}_q[X]/(P_i)\big) = \deg(P_i) =: n_i$, donc $\mathbb{F}_q[X]/(P_i)$ est de cardinal q^{n_i}. Par unicité des corps finis à isomorphisme près, on obtient donc un isomorphisme

$$A \simeq \mathbb{F}_{q^{n_1}} \times \cdots \times \mathbb{F}_{q^{n_r}}.$$

  Notons φ cet isomorphisme, puis notons $\widetilde{\beta} = \varphi \circ \beta \circ \varphi^{-1} : \prod_{i=1}^{r} \mathbb{F}_{q^{n_i}} \to \prod_{i=1}^{r} \mathbb{F}_{q^{n_i}}$. Les endomorphismes β et $\widetilde{\beta}$ sont semblables, donc ont les mêmes espaces propres. Plus précisément, on a $\varphi\big(\mathrm{Ker}(\beta - \mathrm{id}_A)\big) = \mathrm{Ker}\big(\widetilde{\beta} - \mathrm{id}_{\mathbb{F}_{q^{n_1}} \times \cdots \times \mathbb{F}_{q^{n_r}}}\big)$. Il suffit donc d'identifier la dimension de l'espace propre de $\widetilde{\beta}$ associé à la valeur propre 1. Pour cela, identifions $\widetilde{\beta}$: si $(\alpha_1, \ldots, \alpha_r) \in \prod_{i=1}^{r} \mathbb{F}_{q^{n_i}}$ et si $V \in \mathbb{F}_q[X]$ est tel que $\varphi(\overline{V}) = (\alpha_1, \ldots, \alpha_r)$, on a

$$\widetilde{\beta}(\alpha_1, \ldots, \alpha_r) = \varphi\big(\beta(\overline{V})\big) = \varphi\big(\overline{V}^q\big) = \varphi\big(\overline{V}\big)^q = (\alpha_1, \ldots, \alpha_r)^q = (\alpha_1^q, \ldots, \alpha_r^q).$$

  Ainsi, $(\alpha_1, \ldots, \alpha_r) \in \mathrm{Ker}\big(\widetilde{\beta} - \mathrm{id}_{\mathbb{F}_{q^{n_1}} \times \cdots \times \mathbb{F}_{q^{n_r}}}\big)$ si et seulement si $\forall i \in [\![1, r]\!]$, $\alpha_i^q = \alpha_i$, soit $\alpha_i \in \mathbb{F}_q$. En effet, on a déjà vu que les q éléments de $\mathbb{F}_q$ vérifient $\alpha^q = \alpha$ et comme $X^q - X$ ne peut avoir qu'au plus q racines dans toute extension de $\mathbb{F}_q$ (car de degré q), ce sont exactement les éléments de $\mathbb{F}_q$. Finalement, on a $\mathrm{Ker}\big(\widetilde{\beta} - \mathrm{id}_{\mathbb{F}_{q^{n_1}} \times \cdots \times \mathbb{F}_{q^{n_r}}}\big) = \mathbb{F}_q \times \cdots \times \mathbb{F}_q = \mathbb{F}_q^r$. En particulier, cet espace propre est de dimension r sur $\mathbb{F}_q$ ce qui montre bien que $\dim\big(\mathrm{Ker}(\beta - \mathrm{id}_A)\big) = r$. Si

$r = 1$, le polynôme P est irréductible et sa factorisation est triviale. Sinon, on va expliciter une factorisation de P à partir d'un vecteur fixé par β.

Supposons $r > 1$. On a déjà vu que $\mathrm{Vect}_{\mathbb{F}_q}(\overline{1}) \subset \mathrm{Ker}(\beta - \mathrm{id}_A)$, mais comme $r > 1$, cette inclusion est stricte donc il existe $V \in \mathbb{F}_q[X]$ tel que $\overline{V} \in \mathrm{Ker}(\beta - \mathrm{id}_A)$ et $\overline{V} \neq \overline{\alpha}$ pour tout $\alpha \in \mathbb{F}_q$. Comme $\overline{V} \in \mathrm{Ker}(\beta - \mathrm{id}_A)$, on sait d'après l'étude vue précédemment que $\varphi(\overline{V}) = (V \bmod P_1, \dots, V \bmod P_r) = (\alpha_1, \dots, \alpha_r) \in \mathbb{F}_q^r$. Montrons alors qu'on a la factorisation

$$P = \prod_{\alpha \in \mathbb{F}_q} P \wedge (V - \alpha).$$

Soit $\alpha \in \mathbb{F}_q$. Le polynôme $P \wedge (V - \alpha)$ divise P, donc ses diviseurs irréductibles sont parmi les P_i. Il existe donc $I_\alpha \subset [\![1, r]\!]$ tel que

$$P \wedge (V - \alpha) = \prod_{i \in I_\alpha} P_i.$$

Identifions I_α : pour $i \in [\![1, r]\!]$ fixé, on a $i \in I_\alpha \Leftrightarrow P_i \mid V - \alpha$. En effet, l'implication directe est triviale par construction de I_α et réciproquement, si $P_i \mid V - \alpha$, comme $P_i \mid P$, on a $P_i \mid P \wedge (V - \alpha)$, donc P_i apparaît dans la factorisation en irréductibles de $P \wedge (V - \alpha)$, *i.e* $i \in I_\alpha$. Regardons les choses modulo P_i : on a

$$i \in I_\alpha \Leftrightarrow V \equiv \alpha \ [P_i] \Leftrightarrow \alpha_i \equiv \alpha \ [P_i] \Leftrightarrow \alpha_i = \alpha,$$

la dernière équivalence provenant du fait que si P_i divise le polynôme constant $\alpha_i - \alpha$ (c'est là qu'on se sert du fait que $\alpha_i \in \mathbb{F}_q$!), alors ce dernier est nul pour des raisons de degré, d'où $\alpha_i = \alpha$. Ainsi, on a

$$P \wedge (V - \alpha) = \prod_{\substack{i=1 \\ \alpha_i = \alpha}}^{r} P_i,$$

puis

$$P = \prod_{i=1}^{r} P_i = \prod_{\alpha \in \mathbb{F}_q} \prod_{\substack{i=1 \\ \alpha_i = \alpha}}^{r} P_i = \prod_{\alpha \in \mathbb{F}_q} P \wedge (V - \alpha).$$

Enfin, montrons que cette factorisation est non triviale. Si ce n'était pas le cas, elle serait de la forme $1 \times \cdots \times P \cdots \times 1$, donc il existerait $\alpha \in \mathbb{F}_q$ tel que $P \wedge (V - \alpha) = P$, c'est à dire $P \mid (V - \alpha)$, puis $\overline{V} = \overline{\alpha}$, ce qui est absurde par choix de V. On a bien trouvé des facteurs non triviaux de P, auxquels on peut appliquer de nouveau le raisonnement pour les factoriser, jusqu'à n'obtenir que des polynômes irréductibles, ce qui factorisera complètement P : c'est l'algorithme de Berlekamp.

- *Preuve de l'Application 2* : Considérons $P = X^p - X + 1 \in \mathbb{F}_p[X]$ et gardons les notations du théorème, *i.e* $A = \mathbb{F}_q[X]/(P)$, et $\beta : \overline{Q(X)} \in A \mapsto \overline{Q(X)}^p \in A$. L'idée pour déterminer $r = \dim\big(\mathrm{Ker}(\beta - \mathrm{id}_A)\big)$ est de déterminer la matrice de β dans une $\mathbb{F}_q$-base bien choisie de A. La base la plus naturelle est bien sûr $\mathcal{B} = (\overline{1}, \overline{X}, \dots, \overline{X}^{p-1})$ par division euclidienne dans $\mathbb{F}_q[X]$. On calcule donc les images des $\overline{X}^i$ pour $i \in [\![0, p-1]\!]$ dans la base $\mathcal{B}$:
  - $\beta(\overline{1}) = \overline{1}$ (on a déjà vu que les classes des constantes sont dans $\mathrm{Ker}(\beta - \mathrm{id}_A)$.
  - $\beta(\overline{X}) = \overline{X}^p = \overline{X} - \overline{1}$ car $\overline{P(X)} = \overline{X}^p - \overline{X} + \overline{1} = \overline{0}$.
  - Pour $k \in [\![2, p-1]\!]$,

$$\beta\big(\overline{X}^k\big) = \overline{X}^{kp} = \big(\overline{X} - \overline{1}\big)^k = \overline{X}^k - \binom{k}{1}\overline{X}^{k-1} + \cdots + (-1)^{k-1}\binom{k}{k-1}\overline{X} + (-1)^k\overline{1}.$$

  Donc on obtient la matrice triangulaire suivante :

$$M := \mathrm{Mat}_{\mathcal{B}}(\beta) = \begin{pmatrix} 1 & -1 & & & (*) \\ 0 & 1 & -2 & & \\ \vdots & \ddots & \ddots & \ddots & \\ \vdots & & \ddots & \ddots & -k \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

  où au signe près, on retrouve le triangle de Pascal dans le triangle supérieur. On voit alors que $\mathrm{rang}(M - I_p) = p - 1$ car la sous-matrice obtenue à partir de $M - I_p$ en supprimant la première colonne et la dernière ligne est clairement inversible (triangulaire supérieure avec coefficients diagonaux non nuls). Ainsi, par le théorème du rang, $\dim\big(\mathrm{Ker}(M - \mathrm{id}_A)\big) = p - (p-1) = 1$, ce qui montre d'après le **Théorème 2** que le polynôme P est irréductible sur $\mathbb{F}_p$.

Commentaires et prolongements :

- L'algorithme de Berlekamp semble être un bon outil (théorique au moins) pour détecter l'irréductibilité de certains polynômes à coefficients dans un corps fini, mais est restreint par l'hypothèse P sans facteur carré. Cette hypothèse peut être contournée comme suit : Soit $P \in \mathbb{F}_q[X]$ quelconque. On considère le polynôme $P \wedge P'$, qui divise P, et alors plusieurs possibilités se présentent :

- Si $P \wedge P' = 1$, alors P est sans facteur carré. En effet, si $D^2 \mid P$, alors en dérivant, on voit que $D \mid P'$, ce qui est asburde si D est non constant. On peut dans ce cas appliquer l'algorithme de Berlekamp directement.
- Si $P \wedge P' \notin \{1, P\}$, alors $P \wedge P'$ est un facteur non trivial de P donc on a trouvé une décomposition de P non triviale : $P = (P \wedge P') \times \frac{P}{P \wedge P'}$, et on réitère le processus à ces deux facteurs.
- Si $P \wedge P' = P$, alors $P \mid P'$ donc pour des raisons de degré, cela signifie que que $P' = 0$. Montrons que cela implique l'existence de $Q(X) \in \mathbb{F}_q[X]$ tel que $P(X) = Q(X)^p$. Écrivons $P = \sum_{i=0}^{d} a_i X^i$, avec $d \in \mathbb{N}^*$ et $a_0, \ldots, a_d \in \mathbb{F}_q$. On a

$$0 = P' = \sum_{i=1}^{d} i a_i X^{i-1}.$$

  Ainsi, pour tout $i \in [\![1, d]\!]$, $ia_i = 0$, *i.e*, $p \mid i$ ou $a_i = 0$. Ainsi, dans l'écriture de P n'apparaissent que des indices multiples de p, *i.e* il existe $d' \in \mathbb{N}^*$ tel que

$$P = \sum_{i=0}^{d'} a_{ip} X^{ip}.$$

  Comme vu dans la preuve du théorème, par Lagrange, si $\alpha \in \mathbb{F}_q$ on a $\alpha^q = \alpha$. Ainsi, $\alpha^{p^n} = \left(\alpha^{p^{n-1}}\right)^p = \alpha$. Posons alors pour $i \in [\![0, d']\!]$, $b_i = a_{ip}^{p^{n-1}} \in \mathbb{F}_q$. Par ce qui précède, on a $\forall i \in [\![0, d']\!]$, $b_i^p = a_{ip}$. Ainsi, par le Frobenius, on a

$$P = \sum_{i=0}^{d'} b_i^p (X^i)^p = \left(\sum_{i=0}^{d'} b_i X^i \right)^p = Q(X)^p.$$

  Ceci montre qu'on peut construire facilement un facteur non trivial de P (ici Q), auquel on peut à nouveau appliquer le processus.

Cet algorithme complété permet de factoriser tous les polynômes dans $\mathbb{F}_q[X]$.