Cadre : Tous les anneaux considérés sont commutatifs et unitaires.

I) Algèbre de polynômes à n indéterminées

I. 1) Construction de $A[X_1, \dots, X_n]$

Def 1 : Soit A un anneau. Soit $n \geq 1$. On définit $A[X_1, \dots, X_n]$ l'ensemble des suites indexées par $\mathbb{N}^n$, à support fini, et à coefficients dans A.

Prop 2 : $A[X_1, \dots, X_n]$ muni de : $a \cdot (a_{i_1 \dots i_n})_{(i_1, \dots, i_n)} := (a a_{i_1 \dots i_n})_{(i_1, \dots, i_n)}$,

$(a_{i_1 \dots i_n})_{(i_1, \dots, i_n)} + (b_{i_1 \dots i_n})_{i_1, \dots, i_n} := (a_{i_1 \dots i_n} + b_{i_1 \dots i_n})_{(i_1, \dots, i_n)}$, $(a_{i_1 \dots i_n})_{(i_1, \dots, i_n)} \times (b_{i_1 \dots i_n})_{(i_1, \dots, i_n)} := (c_{j_1 \dots j_n})_{(j_1, \dots, j_n)}$

avec $c_{j_1, \dots, j_n} := \sum_{(i_1, \dots, i_n) + (k_1, \dots, k_n) = (j_1, \dots, j_n)} a_{i_1 \dots i_n} \cdot b_{k_1 \dots k_n}$ est une A-algèbre commutative unitaire.

Un élément $P \in A[X_1, \dots, X_n]$ est appelé polynôme à n indéterminées.

Notation 3 : $\forall 1 \leq j \leq n$, on note $X_j := \left(\delta_{(i_1, \dots, i_n), (0, \dots, 0, 1, 0, \dots, 0)}\right)_{(i_1, \dots, i_n)}$ la j-ème indéterminée de $A[X_1, \dots, X_n]$.

Pour $P \in A[X_1, \dots, X_n]$, $P = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n}$. ($i_j$: j-ème coordonnée)

Théorème 4 : $A[X_1, \dots, X_{n-1}][X_n] \underset{A\text{-algèbres}}{\cong} A[X_1, \dots, X_n]$

I. 2) Théorèmes de transfert

Prop 5 : Si A est intègre, alors $A[X]$ est intègre.

Prop 6 : Si A est intègre, alors $A[X]^\times = A^\times$.

Ex 7 : $\mathbb{Z}[X_1, \dots, X_n]$ est intègre, et $\mathbb{Z}[X_1, \dots, X_n]^\times = \{\pm 1\}$.

Prop 8 : A est un corps $\Leftrightarrow A[X]$ est principal.

Cor 9 : $A[X_1, \dots, X_n]$ n'est jamais principal $\forall n \geq 2$.

Contre-ex : $(2, X)$ n'est pas principal dans $\mathbb{Z}[X]$.

Théorème 11 : Si A est factoriel, alors $A[X]$ est factoriel.

Conséquences 12 : On a l'existence du PGCD, PPCM de deux polynômes. Pour P, Q, P unitaire, on a une division euclidienne de Q par P. Les théorèmes de Gauss sur les facteurs irréductibles sont vrais, mais pas le théorème de Bézout.

Ex 13 : $\mathbb{R}[X_1, \dots, X_n]$ est factoriel, $\mathbb{Q}[\sqrt{5}][X, Y]$ est factoriel, mais pas $\mathbb{Z}[\sqrt{5}][X, Y]$.

Théorème 14 : Si A est noethérien, alors $A[X]$ est noethérien.

I. 2) Degrés, polynômes homogènes

Def 15 : Le degré total de P est $\deg_{tot}(P) := \max\{i_1 + \dots + i_n, \text{ avec } a_{i_1 \dots i_n} \neq 0\}$.

$\forall 1 \leq j \leq n$, le j-ème degré partiel de P, $\deg_j(P)$, est le degré de P vue dans $A[X_1, \dots, X_{j-1}, X_{j+1}, \dots, X_n][X_j]$.

Prop 16 : $\deg_j(P) \leq \deg_{tot}(P)$, $\forall 1 \leq j \leq n$.

Si A est intègre, $\deg_{tot}(PQ) = \deg_{tot}(P) + \deg_{tot}(Q)$; $\deg_j(PQ) = \deg_j(P) + \deg_j(Q)$

$\deg_{tot}(P+Q) \leq \max\{\deg_{tot}(P); \deg_{tot}(Q)\}$; $\deg_j(P+Q) \leq \max\{\deg_j(P); \deg_j(Q)\}$.

Ex 17 : $\deg_{tot}(X^2 Y) = 3$.

Def 18 : Soit $k \geq 0$. Un polynôme P est dit k-homogène ssi chaque monôme de P est de degré total k.

On note H_k l'ensemble des polynômes k-homogènes de $A[X_1, \dots, X_n]$.

Rem 19 : $0 \in H_k$, $\forall k \geq 0$, et pour $P, Q \in H_k$, $P+Q \in H_k$. Donc H_k est un groupe additif.

Pour $P \in H_k$, $Q \in H_\ell$, $PQ \in H_{k+\ell}$.

Def 20 : Soit $1 \leq j \leq n$. Le j-ème polynôme dérivé partiel de P, $\frac{\partial P}{\partial X_j}$ vaut :

$$\frac{\partial P}{\partial X_j} := \sum_{\substack{(i_1, \dots, i_n) \in \mathbb{N}^n \\ i_j \geq 1}} i_j \cdot a_{i_1 \dots i_n} \cdot X_1^{i_1} \dots X_j^{i_j - 1} \dots X_n^{i_n}.$$

Théorème 21 : (d'Euler) Soit A de caractéristique nulle.

Alors $P \in H_k \Leftrightarrow \sum_{i=1}^{n} X_i \frac{\partial P}{\partial X_i} = kP$.

II) Fonctions polynôme

II. 1) Morphisme d'évaluation

Def 22 : Soit B une A-algèbre. On définit ev : $A[X_1, \dots, X_n] \to \mathcal{F}(B^n, B)$, $P \mapsto \left((x_1, \dots, x_n) \mapsto P(x_1, \dots, x_n)\right)$

le morphisme d'évaluation.

Prop 23 : ev est un morphisme de A-algèbres.

Prop 24 : Si A est intègre infini, ev est injectif.

Contre-ex 25 : Si $A = B = \mathbb{F}_2$, $ev(X_i - X_j)$ est la fonction nulle.

Prop 26 : Si A est intègre infini, $\{x \in A^n \mid P(x) \neq 0\}$ est infini.

Théorème 27 : (Prolongement des identités) Soit A intègre infini. Soit $P \in A[X_1, \dots, X_n]$ et $V = \{x \in A^n \mid P(x) = 0\}$. Soient F_1, F_2 tq $ev(F_1) = ev(F_2)$ sur $A^n \setminus V$. Alors $F_1 = F_2$.

Corollaire 28 : Soit A intègre. $\forall M, N \in M_n(A)$, $\chi_{MN} = \chi_{NM}$.

Prop 29 : Soit A intègre, $P \in A[X]$, $a \in A$.

Alors $P(a) = 0 \Leftrightarrow (X - a) \mid P(X)$.

Application 30 : Soit A intègre.
$X_m - Q(X_1, \dots, X_{m-1}) \mid P(X_1, \dots, X_m) \Leftrightarrow P(X_1, \dots, X_{m-1}, Q(X_1, \dots, X_{m-1})) \equiv 0$ dans $A[X_1, \dots, X_{m-1}]$.

Application 31 :
Soit $V_m := \begin{vmatrix} 1 & \cdots & 1 \\ X_1 & \cdots & X_m \\ \vdots & & \vdots \\ X_1^{m-1} & \cdots & X_m^{m-1} \end{vmatrix} \in \mathbb{Z}[X_1, \dots, X_m]$. Alors $V_m = \prod_{i<j} (X_i - X_j)$.

Application 32 : Soit A intègre.
$P = \begin{vmatrix} X_{11} & \cdots & X_{1n} \\ \vdots & & \vdots \\ X_{m1} & \cdots & X_{mn} \end{vmatrix}$ est irréductible dans $A[X_{11}, \dots, X_{mn}]$.

Théorème 33 : Soit A intègre. Soit $M \in M_n(A)$. Alors $\chi_M(M) = 0$.

V. 2) Fonctions polynômes sur des corps finis

Soit $q = p^\alpha$, $\alpha \in \mathbb{N}^*$, p premier. Soit $\mathbb{F}_q$ le corps à q éléments.

Théorème 34 : $\dfrac{\mathbb{F}_q[X_1, \dots, X_m]}{\langle X_1^q - X_1, \dots, X_m^q - X_m \rangle \mathbb{F}_q\text{-algèbres}} \overset{\text{som}}{\simeq} \mathrm{Fonct}(\mathbb{F}_q^m, \mathbb{F}_q)$

Développement 1 : Théorème de Chevalley-Warning.
Soient $P_1, \dots, P_n \in \mathbb{F}_q[X_1, \dots, X_m]$ tq $\sum_{i=1}^{n} \deg_{tot}(P_i) < m$.
Alors $\#\{x \in \mathbb{F}_q^m \text{ tq } P_1(x) = \dots = P_n(x) = 0\} \equiv 0 \mod (p)$.

Corollaire 35 :
Si $P_1, \dots, P_n$ sont annulés par $(0, \dots, 0)$, ils ont au moins une racine commune non-triviale dans $\mathbb{F}_q^m$.

Corollaire 36 :
Toute forme quadratique à au moins 3 variables sur $\mathbb{F}_q$ admet un zéro non-trivial.

V. 3) Classification des quadriques sur $\mathbb{R}$.

Def 37 : Soit $P \in \mathbb{R}[X_1, X_2, X_3]$, $P(X_1, X_2, X_3) = a X_1^2 + a' X_2^2 + a'' X_3^2 + 2b X_1 X_2 + 2b' X_1 X_3 + 2b'' X_2 X_3 + c X_1 + c' X_2 + c'' X_3 + d$, avec $\deg_{tot}(P) = 2$.
La quadrique Q associée à P est : $Q := \{(x, y, z) \in \mathbb{R}^3 \text{ tq } P(x, y, z) = 0\}$.
On définit $M_Q := \begin{pmatrix} a & b & b' \\ b & a' & b'' \\ b' & b'' & a'' \end{pmatrix}$ la partie quadratique de P, $L := \begin{pmatrix} c \\ c' \\ c'' \end{pmatrix}$ la partie linéaire de P,
$C := (d)$ la partie constante de P. On a $M_Q \neq 0$.
M_Q est symétrique réelle, donc diagonalisable dans $M_3(\mathbb{R})$. Soient $\lambda_1, \lambda_2, \lambda_3$ ses valeurs propres.

Théorème 38 : (classification des quadriques réelles)
Soit p le nombre de vp > 0 de M_Q. Soit q le nb de vp < 0 de M_Q.
Le couple (p, q), appelé signature de M_Q, permet de classifier les différentes quadriques.

(p, q)	Quadrique non dégénérée	Quadrique dégénérée
$(3,0)$ ou $(0,3)$	ellipsoïde	$\emptyset$ ou point
$(2,1)$ ou $(1,2)$	hyperboloïde à 1 ou 2 nappes	cône
$(2,0)$ ou $(0,2)$	paraboloïde elliptique ou cylindre elliptique	$\emptyset$ ou droite
$(1,1)$	paraboloïde hyperbolique ou cylindre hyperbolique	réunion de deux plans
$(1,0)$ ou $(0,1)$	cylindre parabolique	$\emptyset$ ou plan ou réunion de 2 plans

Exc 39 : Ellipsoïde : $\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} + \frac{z^2}{\gamma^2} = 1$; Hyperboloïde à 2 nappes : $\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} - \frac{z^2}{\gamma^2} = -1$.
Cylindre parabolique : $x^2 = 2py$.

VI) Polynômes symétriques, relations coefficients-racines

VI. 1) Polynômes symétriques

Def 40 : $\mathfrak{S}_n$ agit sur $A[X_1, \dots, X_m]$ par : $\sigma \cdot P(X_1, \dots, X_m) := P(X_{\sigma(1)}, \dots, X_{\sigma(m)})$.
On définit alors $A[X_1, \dots, X_m]^{\mathfrak{S}_n} := \{P \text{ tq } \sigma \cdot P = P, \forall \sigma \in \mathfrak{S}_n\}$, l'ensemble des polynômes symétriques de $A[X_1, \dots, X_m]$.

Prop 41 : $A[X_1, \dots, X_m]^{\mathfrak{S}_n}$ est une sous-A-algèbre de $A[X_1, \dots, X_m]$.

Def 42 : $\forall 1 \leq j \leq m$, on définit $\Sigma_j := \sum_{1 \leq i_1 < \dots < i_j \leq m} X_{i_1} \dots X_{i_j}$ le j-ème polynôme symétrique élémentaire.

Prop 43 : $\forall 1 \leq j \leq m$, $\Sigma_j \in A[X_1, \dots, X_m]^{\mathfrak{S}_n}$.

Ex 44 : $\Sigma_1 = X_1 + \dots + X_m$; $\Sigma_m = X_1 \dots X_m$; $\Sigma_2 = X_1X_2 + \dots + X_1X_m + X_2X_3 + \dots + X_2X_m + \dots + X_{m-1}X_m$

Théorème 45 : (Théorème de structure)
$\Phi : A[X_1, \dots, X_m] \to A[X_1, \dots, X_m]^{\mathfrak{S}_n}$ est un isomorphisme de A-algèbres.
$P(X_1, \dots, X_m) \mapsto P(\Sigma_1, \dots, \Sigma_m)$
$\forall P$ symétrique, $\exists ! Q \in A[X_1, \dots, X_m]$ tq $P(X_1, \dots, X_m) = Q(\Sigma_1, \dots, \Sigma_m)$.

Ex 46 : $\forall k \geq 0$, $S_k := X_1^k + \dots + X_m^k \in A[X_1, \dots, X_m]^{\mathfrak{S}_n}$.

Prop 47 : Soit $P(T) := \prod_{i=1}^{n} (T - X_i) \in A[X_1, \dots, X_n][T]$.
Alors $P(T) = \sum_{i=1}^{n} T^i \times (-1)^{n-i} \Sigma_{n-i} \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}[T]$, et $\mathrm{disc}(P) := \prod_{i<j} (X_i - X_j) \in A[X_1, \dots, X_n]^{\mathfrak{A}_n}$

Prop 48 (Formules de Newton) :

$\forall k \geq n$, $S_k - \Sigma_1 S_{k-1} + \dots + (-1)^n \Sigma_n S_{k-n} = 0$.

$\forall 1 \leq k \leq n$, $S_k - \Sigma_1 S_{k-1} + \dots + (-1)^{k-1} \Sigma_{k-1} S_1 + (-1)^k \Sigma_k \times k = 0$.

Appli 49 :
Si $\mathrm{car}(A) = 0$, $\{S_1, \dots, S_n\}$ est une base algébrique de l'algèbre $A[X_1, \dots, X_n]^{\mathfrak{S}_n}$

Appli 50 :
Soit A intègre. Soit $M \in M_n(A)$ tq $\mathrm{Tr}(M^k) = 0$ $\forall 1 \leq k \leq n$. Alors M est nilpotente.

Appli 51 :
Soit A intègre. Soit $P(X) = a_n X^n + \dots + a_0 \in A[X]$. Soit K le corps des fractions de A. Soit $\overline{K}$ une clôture algébrique de K. On a $P(X) = a_n \prod_{i=1}^{n} (X - \lambda_i)$ dans $\overline{K}[X]$.
Alors, $\forall k \geq 0$, $\lambda_1^k + \dots + \lambda_n^k \in A$ et sont calculables à partir des a_i sans avoir à déterminer les λ_i.

Exc 52 : $P(X) = X^5 - 5X - 5$. On a $a_0 = a_1 = -5$, $a_2 = a_3 = a_4 = 0$, $a_5 = 1$.
P est irréductible sur $\mathbb{Q}$. Ses racines ne sont pas radicales sur $\mathbb{Q}$ (admis)
Pourtant, $S_0 = 5$, $S_1 = S_2 = S_3 = 0$, $S_4 = 20$, $S_5 = 25$, $S_6 = 0$, $S_7 = 0$, $S_8 = 100$, ...
$\forall k \geq 5$, $S_k = -5 S_{k-4} - 5 S_{k-5} \in \mathbb{Z}$.

Développement 2 : Caractérisation des polynômes alternés

Soit A intègre. On définit $A[X_1, \dots, X_n]^{A_n} := \{P \text{ tq } \sigma P = P, \forall \sigma \in A_n\}$, l'ensemble des polynômes alternés. Soit $V_n := \prod_{i<j} (X_i - X_j)$, $\Theta_n := \prod_{i<j} (X_i + X_j)$, $W_n := \frac{1}{2}(V_n + \Theta_n)$.
Alors $W_n \in A[X_1, \dots, X_n]$, et $A[X_1, \dots, X_n]^{A_n} = A[X_1, \dots, X_n]^{\mathfrak{S}_n} \oplus W_n \cdot A[X_1, \dots, X_n]^{\mathfrak{S}_n}$.
On a : $\dfrac{A[X_1, \dots, X_n]^{\mathfrak{S}_n}[T]}{\langle T^2 - \Theta_n T + W_n^2 \rangle} \underset{A[X_1, \dots, X_n]^{\mathfrak{S}_n}\text{-algèbres}}{\simeq} A[X_1, \dots, X_n]^{A_n}$

Intérêt Polyg : calcul effectif relation coef - racines

Pas mis de plus : Résultant Grobner.

Manque Em, CEX

Auteurs : AGNIEL Vital
BERAUD Vivien

Références :

Ramis, Deschamps, Odoux ; Cours de mathématiques spéciales I, p185-209.
Goblot, Algèbre commutative, p174-213
Szpirglas, Algèbre commutative, p604-605 [Devpt 2]
Mérindol, Nombres et algèbre.
Serre, Cours d'Arithmétique [Devpt 1].

Rennes, 2016

Polynômes irréductibles sur $\mathbb{F}_q$

Soient p premier, $r \geq 1$ et $q = p^r$.
On note $I(n,q)$ l'ensemble des polynômes irréductibles unitaires de degré n sur $\mathbb{F}_q$ et $m(n,q) = |I(n,q)|$.

Théorème : $\forall n \geq 1,\ X^{q^n} - X = \prod_{d \mid n} \prod_{P \in I(d,q)} P$

Démonstration : Soit $n \geq 1$. $(X^{q^n} - X)' = -1$ donc $X^{q^n} - X$ est sans facteur carré, et est donc le produit de ses facteurs irréductibles unitaires.

Soit $P \in \mathbb{F}_q[X]$ un facteur irréductible de $X^{q^n} - X$ de degré d.
Alors P est scindé sur $\mathbb{F}_{q^n}$ et il existe une racine α de P dans $\mathbb{F}_{q^n}$.
Comme $P = \pi_{\alpha, \mathbb{F}_q}$, on a $d = \deg P = [\mathbb{F}_q(\alpha) : \mathbb{F}_q] \mid [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$.

Réciproquement, soient d un diviseur de n et $P \in I(d,q)$.
Alors $\mathbb{F}_q[X]/(P)$ est un corps de cardinal q^d, et donc $(X+(P))^{q^d} = X+(P)$.
Ainsi $(X+(P))^{q^n} = \underbrace{\left(\left((X+(P))^{q^d}\right)\cdots\right)^{q^d}}_{\frac{n}{d} \text{ fois}} = X+(P)$ et donc $P \mid X^{q^n} - X$.

Finalement $X^{q^n} - X = \prod_{d \mid n} \prod_{P \in I(d,q)} P$.

Définition : On note $\mu : \left| \begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \{-1, 0, 1\} \\ n & \longmapsto & \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n = p_1 \cdots p_r \text{ est sans facteur carré} \\ 0 & \text{sinon} \end{cases} \end{array} \right.$

Lemme :

- $\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geq 2 \end{cases}$
- Soient G un groupe abélien et $f, g : \mathbb{N}^* \to G$ telles que
$$\forall n \in \mathbb{N}^*,\ g(n) = \sum_{d \mid n} f(d)$$
Alors $\forall n \in \mathbb{N}^*,\ f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$.

Démonstration :

- Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \geqslant 2$, alors

$$\sum_{d|n} \mu(d) = \sum_{k=0}^{r} \sum_{i_1 < \cdots < i_k} \mu(p_{i_1} \cdots p_{i_k}) = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = (1-1)^r = 0$$

- Soit $n \geqslant 1$. On a :

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \sum_{d'|d} \mu\left(\frac{n}{d}\right) f(d') = \sum_{d'|n} \sum_{\substack{d \text{ multiple} \\ \text{de } d'}} \mu\left(\frac{n}{d}\right) f(d')$$

$$= \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d) = f(n)$$

Théorème : . $\forall n \geqslant 1$, $m(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$

. $m(n,q) \underset{n\to\infty}{\sim} \frac{q^n}{n}$

Démonstration :

- On a $\forall n \geqslant 1$, $q^n = \sum_{d|n} d \cdot m(n,q)$

donc $\forall n \geqslant 1$, $m(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$.

- Pour tout $n \geqslant 1$, $\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = q^n + \sum_{\substack{d|n \\ d \neq n}} \mu\left(\frac{n}{d}\right) q^d$

et $\left| \sum_{\substack{d|n \\ d\neq n}} \mu\left(\frac{n}{d}\right) q^d \right| \leqslant \sum_{d=1}^{\lfloor n/2 \rfloor} q^d = q \cdot \frac{q^{\lfloor n/2 \rfloor} - 1}{q-1} = o(q^n)$.

Ainsi $\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \underset{n\to\infty}{\sim} q^n$ et $m(n,q) \underset{n\to\infty}{\sim} \frac{q^n}{n}$.

Algorithme de Berlekamp

Soient q une puissance d'un nombre premier p et $P = P_1 \dots P_r \in \mathbb{F}_q[X]$ sans facteur carré et non constant.

Théorème : L'application $\varphi_P : \left| \begin{array}{ccc} \frac{\mathbb{F}_q[X]}{(P)} & \longrightarrow & \frac{\mathbb{F}_q[X]}{(P)} \\ R & \longmapsto & R^q \end{array} \right.$ est $\mathbb{F}_q$-linéaire

et $\dim \ker(\varphi_P - id) = r$.

De plus, si $r \geqslant 2$ et $Q \in \mathbb{F}_q[X]$ est tel que $1 \leqslant \deg Q < \deg P$ et $P \mid (Q^q - Q)$ alors $P = \prod_{\alpha \in \mathbb{F}_q} P \wedge (Q - \alpha)$ et tous les facteurs non constants sont non triviaux.

Démonstration :

- φ_P est un morphisme d'anneaux comme itéré du morphisme de Frobenius.
  De plus, pour tout $\alpha \in \mathbb{F}_q$, $\alpha^q = \alpha$, donc φ_P est un morphisme de $\mathbb{F}_q$-algèbres.
- D'après le théorème chinois, $\psi : \left| \begin{array}{ccc} \frac{\mathbb{F}_q[X]}{(P)} & \longrightarrow & \frac{\mathbb{F}_q[X]}{(P_1)} \times \dots \times \frac{\mathbb{F}_q[X]}{(P_r)} \\ Q + (P) & \longmapsto & (Q + (P_1), \dots, Q + (P_r)) \end{array} \right.$

est un isomorphisme d'anneaux.
Pour tout $i \in [\![1, r]\!]$, $\mathbb{F}_q \hookrightarrow \mathbb{F}_q[X] \twoheadrightarrow \frac{\mathbb{F}_q[X]}{(P_i)}$ est une extension de corps donc $T^q - T$ possède q racines dans $\frac{\mathbb{F}_q[X]}{(P_i)}$.
Or ψ induit une bijection de $\ker(\varphi_P - id)$ sur $\prod_{i=1}^{r} \{R_i \in \frac{\mathbb{F}_q[X]}{(P_i)} \mid R_i^q = R_i\}$.
En effet, si $(R_1, \dots, R_r) = \psi(R) \in \prod_{i=1}^{r} \{R_i \in \frac{\mathbb{F}_q[X]}{(P_i)} \mid R_i^q = R_i\}$, alors

$$\psi(R^q) = \psi(R)^q = (R_1, \dots, R_r) = \psi(R)$$

donc $R \in \ker(\varphi_P - id)$. Ainsi $|\ker(\varphi_P - id)| = q^r$ et $\dim \ker(\varphi_P - id) = r$.

- Supposons que $r \geqslant 2$ et soit $Q \in \mathbb{F}_p[X]$ tel que $1 \leqslant \deg Q < \deg P$ et $P \mid Q^q - Q$.
  Comme $X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha)$, on a $Q^q - Q = \prod_{\alpha \in \mathbb{F}_q} (Q - \alpha)$
  et par suite $P = P \wedge (Q^q - Q) = \prod_{\alpha \in \mathbb{F}_q} P \wedge (Q - \alpha)$.

Pour tout $\alpha \in \mathbb{F}_q$, $1 \leq \deg(Q-\alpha) < \deg P$ et donc $\deg(P \wedge (Q-\alpha)) < \deg P$.

Ainsi tous les facteurs non constants sont non triviaux.

Algorithme : Notons $x = X + (P) \in \frac{\mathbb{F}_q[X]}{(P)}$.

* On calcule la matrice de $\varphi_P - id$ dans la $\mathbb{F}_q$-base $(1, x, \dots, x^{\deg P - 1})$ de $\mathbb{F}_q[X]/(P)$ et son noyau, par la méthode du pivot de Gauss.
* Si $\dim \ker(\varphi_P - id) = 1$, alors P est irréductible et on arrête. Sinon on calcule un polynôme Q non constant modulo P tel que $Q + (P) \in \ker(\varphi_P - id)$ et on réapplique l'algorithme aux facteurs non triviaux $P \wedge (Q-\alpha)$ où $\alpha \in \mathbb{F}_q$.