

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi : Polynômes irréductibles à une indéterminée.

Autre sujet : Grps de symétrie. Exemples et applications.

17 00 copies amicalité : Pratoir 06 pages !!

Ré : a Tavel, Grps commutatifs et Théorie de Galois
* Gouard, Théorie de Galois

* Beck, Objectif Agrégation
* Perrin, Cours d'Algèbre
* Francine Guinette, Exercices pour l'agrégation, Algèbre

1/1

Soit A anneau, K corps et $\mathbb{R}$ ens. des nombres premiers <u>I - Iréductibilité</u> Ag Définitions Déf 1: Un polynôme $P \in A[X]$ est <u>iréductible</u> (dans $A[X]$) si $P \notin A$ et si $Q \in A[X]$ avec $Q \mid P$ alors : $\exists u \in A^*, Q = uP$ ou $Q = u$. Prop 2: Si P ir. alors λP l'est pour $\lambda \in A^*$. Prop 3: Soit $P \in K[X]$ • $\deg P = 1 \Rightarrow P$ ir. • Si P ir., alors P n'a pas de racine dans K. • Si P est de degré 2 ou 3 et n'a pas de racine dans K, alors P est ir. dans $K[X]$ • P ir. $\Leftrightarrow K[X]/(P)$ est un corps. Ex 4: $(x^2+1)^2$ n'a pas de racine dans $\mathbb{R}$ et est irréductible dans $\mathbb{R}[X]$. Rq 5: Soit $P \in K[X]$ ir. sur $K[X]$ et L/K ext. P peut être réductible sur $L[X]$. Ex 6: x^2+1 est ir. sur $\mathbb{R}[X]$ mais pas sur $\mathbb{C}[X]$. Rq 7: L'anneau $A[X]$ est factoriel si A l'est. s'écrit comme produit de polynômes irréductibles Ex 8: $x^3+2x^2+x+2 = (x^2+1)(x+2)$ dans $\mathbb{R}[X]$ $= (x-i)(x+i)(x+2)$ dans $\mathbb{C}[X]$ App 10: Si A est factoriel, via th. 8, on peut trouver un pgcd, un ppm de deux polynômes. On peut aussi effectuer la VES. Cr 11: L'ensemble des polynômes irréductibles de $K[X]$ est infini. B₆ Critères d'irréductibilité ICI A est factoriel et $K = \text{Frac}(A)$.	Déf 12: Soit $P \in A[X]$. Le contenu de P, noté $C(P)$, est le pgcd des coefficients de P. Déf 13: $P \in A[X]$ est primitif si $C(P) = 1$. Ex 14: $C(x^3+2) = 1$. Donc x^3+2 est primitif. Lemme 15: (Gauss) (i) Le produit de deux polynômes primitifs est primitif. (ii) Soit $(P, Q) \in A[X]$. Alors $C(PQ) = C(P) \cdot C(Q)$. Th 16: (Eisenstein) Soit $P = \sum_{i=0}^n a_i x^i \in A[X]$ avec $n \geq 1$. Soit $p \in A$ ir. avec $P \not\equiv 0 \pmod p$, P lue pour $1 \leq i \leq n$, $P \not\equiv 0 \pmod p$. Alors P est ir. sur $K[X]$. Ex 17: Soit $n \in \mathbb{N}^*$, $P \in \mathbb{Z}$. Soit $a \in \mathbb{Z}$ avec $P \not\equiv 0 \pmod a$, $P \not\equiv 0 \pmod a$. Alors x^n+a est ir. sur $\mathbb{Q}[X]$. Th 18: Soit $P \in A[X]$, $\deg P \geq 1$. Alors P ir. dans $A[X]$ si $(P$ ir. dans $K[X]$ et $C(P) = 1)$. Ex 19: x^3+2 est ir. sur $\mathbb{Z}[X]$. Prop 20: Soit $P \in \mathbb{Q}$. Alors $\prod_{i=0}^n x^i$ ir. sur $\mathbb{Z}[X]$. Th 21: Soit $\mathbb{I}$ idéal premier de A. On pose $B = A/\mathbb{I}$ et $L = \text{Frac}(B)$. Soit $P \in A[X]$. A de coefficient dominant en $\mathbb{I}$. Si $(P \text{ mod } \mathbb{I})$ est ir. dans $L[X]$, alors P est ir. dans $K[X]$. Ex 22: $x^3-257x^2+27134x+13$ est ir. dans $\mathbb{Z}[X]$. II - Extensions de corps et polynômes Ag Nombres algébriques Rq 23: Soit $a \in K$. Alors eval_a est un morphisme de K-algèbres Déf 24: Si eval_a n'est pas injectif, a est dit <u>algébrique</u>. Sinon il est dit <u>transcendant</u>. Déf 25: Soit $a \in K$ algébrique. Alors $K(a)$ est
---	---

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi :

Autre sujet :

un idéal principal de $K[X]$ non trivial. On appelle <u>polynôme minimal</u> de a sur K, noté $p_{a,K}$, générateur unitaire de $K[a]$ (voir ex 26). <u>Def 26</u>: Le degré de $p_{a,K}$ est le degré de a sur K noté $\deg_K(a)$. <u>Prop 27</u>: Soit $a \in K$ algébrique. Alors $K(a) \cong K[X]/(p_{a,K})$. <u>Cor 28</u>: $\deg_K(a) = [K(a) : K]$. <u>Prop 29</u>: Soit $a \in K$ algébrique et $P \in K[X]$. Alors $P = p_{a,K} Q$ avec $Q(a) = 0$. P unitaire et $\deg_K(a) = \deg_K(P)$. <u>Ex 30</u>: Soit $n \in \mathbb{N}^*$, $a = \sqrt[n]{2}$. Alors $p_{a,\mathbb{Q}} = X^n - 2$. <u>Prop 31</u>: $\deg(p_{a,K}) = 1 \iff a \in K$. <u>Th 32</u>: Soit L/K extension de corps et $a \in L$. Alors : (i) a alg. sur K. (ii) Le sev $K[a]$ de L est de dim. finie sur K. (iii) Le sev $K(a)$ de L est de dim. finie sur K. (iv) $K[a] = K(a)$. (v) si $a \neq 0$, $a^{-1} \in K[a]$. <u>Def 33</u>: Une extension L/K est <u>algébrique</u> si tout élément de L est algébrique sur K. <u>Prop 34</u>: Soit L/K ext. finie de corps. Alors L/K est algébrique et $\forall x \in L, [K(x) : K] \mid [L : K]$. <u>Prop 35</u>: Soit L/K et $S \subseteq L$. Supposons que tout élément de S est algébrique sur K. Alors $K(S)/K$ est alg. et si $\#S < \infty$, $[K(S) : K] < \infty$. <u>Prop 36</u>: Soit L/K. L'ensemble M des éléments de L alg. sur K est un sous-corps de L contenant K appelé <u>parture algébrique</u> de K dans L. <u>Def 37</u>: Soit $P \in K[X]$ un. Une extension L/K est <u>un</u> corps de rupture de P (sur K) si :	<u>Ex 32</u>: Si $\deg P = 1$, K est un corps de rupture de P (sur lui-même). <u>Ex 33</u>: On a vu que $X^2 + 2$ est ir. sur $\mathbb{Q}$. Les ext. de K, $L = \mathbb{Q}(\sqrt{-2})$ et $L' = \mathbb{Q}(\sqrt{2})$ sont corps de rupture de P mais $L \neq L'$. <u>Th 40</u>: Soit $P \in K[X]$ un. dans $K[X]$. Il existe un corps de rupture L de P. De plus, si $K(a)$ et $K(b)$ conviennent, il existe $\varphi : K(a) \rightarrow K(b)$ K-isom. avec $\varphi(a) = b$. <u>Ex 41</u>: $\mathbb{C}$ est un corps de rupture de $X^2 + 1$ sur $\mathbb{R}[X]$, tout comme $\mathbb{R}(\sqrt{-1})/(X^2 + 1)$. Un K-isom. est donné par $\varphi : \mathbb{R}(\sqrt{-1})/(X^2 + 1) \rightarrow \mathbb{C}$. <u>Cor 42</u>: Soit K corps et $P, \dots, P_n$ des polynômes de $K[X]$, tous de degré ≥ 1. Il existe une extension de K de deg. fini dans laquelle P_i possède au moins une racine $\forall i$. <u>Ex 43</u>: Soit $P = X^2 - 2$, $Q = X^3 - 3$ ir. sur $\mathbb{Q}[X]$. P et Q admettent des racines dans $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{R}$. <u>Appl 44</u>: $X^2 + X + 1$ est ir. sur $\mathbb{F}_2[X]$. D'où $L = \mathbb{F}_2[X]/(X^2 + X + 1)$ est un corps à 4 éléments. <u>Lef.</u> annexe 1 pour la table des opérations sur L. <u>Prop 45</u>: Soit $P \in K[X]$ un. de deg n. Soit L/K de deg m avec $n \mid m = 1$. Alors P est un. dans $L[X]$. <u>Ex 46</u>: $X^3 + X + 1$ est ir. sur $\mathbb{F}_2[X]$ et $3 \nmid 2^m = 1$ pour $m \in \mathbb{N}^*$. Donc $X^3 + X + 1$ est ir. sur $\mathbb{F}_{2^m}[X]$. <u>Th 47</u>: Soit $P \in K[X]$ avec deg $P = n > 0$. Alors P un. sur $K \iff P$ n'a pas de racines dans L/K avec $[L : K] \leq n/2$.
--	--

(Algèbre) ← Entourez l'épreuve → Analyse

Sujet choisi :

Autre sujet :

Ex 48: $X^4 + X + 1$ n'a pas de racine dans $\mathbb{F}_2$ ni dans $\mathbb{F}_4$. Il est donc irréductible dans $\mathbb{F}_2[X]$. Cf Corps de décomposition Def 49: Soit L/K ext. et $P \in K[X]$ de degré n. L est un corps de décomposition de P si: $\exists (\alpha_1, \dots, \alpha_n) \in L^n, P(X) = \prod (X - \alpha_i)$ et $L = K(\alpha_1, \dots, \alpha_n)$ Th 50: Soit $P \in K[X], K$. Alors P admet un unique corps de décomposition L ($\bar{K}$-isom. près) de P avec $[L:K] \mid \deg(P)$! E 51: Un corps de décomposition de $X^2 - 2$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt{2}, i)$ Appl 52: Soit $p \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Posons $q = p^n$. Il existe un unique corps ($\bar{\mathbb{F}}_p$-isom. près) fini à q éléments. On le note $\mathbb{F}_q$. Def 53: Un corps est dit algébriquement clos si tout polynôme irréductible sur celui-ci est de degré 1. Th 54: Tout corps K admet une extension alg. close. Def 55: Une extension L de K est appelée une clôture algébrique de K si elle est algébriquement close et algébrique sur K. E 56: $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$. Th 57: (Steinitz) $\rightarrow$ appl. m. g. o. Tout corps possède une clôture algébrique Gr 58: (Élément primitif) Soit L/K finite avec $\text{car}(K) = 0$ et $[L:K] = n$. Alors $\exists z \in L, L = K(z)$. III - Retour sur les corps finis AP Polyômes irréductibles sur $\mathbb{F}_p$. Th 59: Soit $p \in \mathbb{Z}, n \in \mathbb{N}^*$. Posons $q = p^n$. Alors il existe	$\pi \in \mathbb{F}_p[X]$ un. de degré n avec $\mathbb{F}_q = \mathbb{F}_p[X]/(\pi)$ Gr 60: Il existe des polynômes un. de tout degré dans $\mathbb{F}_p[X]$. Prop 61: Soit $\pi \in \mathbb{F}_p[X]$ de degré n. Alors $\pi X^q - X$ dans $\mathbb{F}_p[X]$. Ainsi son corps de rupture est emb. son corps de décomposition Prop 62: $X^{q^n} - 1 = \prod_{d n} \Phi_d(X)$ Gr 63: Soit $I(n, q) = \# \{P \in \mathbb{F}_q[X], \text{un. unitaire}, \text{avec } \deg P = n\}$ Alors $\sum_{d n} d I(d, q) = q^n$. Def 64: La fonction de Möbius est: $\mu: \mathbb{N}^* \rightarrow \{0, 1, -1\}$ $1 \mapsto 1$ $p \mapsto -1$ si p est un facteur premier $n \mapsto 0$ si n admet un carré Prop 65: Si $g(n) = \sum_{d n} \mu(d)$. Alors $f(n) = \sum_{d n} \mu(d) g(d)$ Gr 66: $I(n, q) = \frac{1}{n} \sum_{d n} \mu\left(\frac{n}{d}\right) q^d \sim \frac{q^n}{n}$ BG Décomposition dans $\mathbb{F}_q[X]$ Th 67: (Algorithme de Berlekamp) Il existe un algorithme qui permet de décomposer $P \in \mathbb{F}_q[X]$ en irréductibles [cf. annexe 2] Cor 68: $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$.
--	--

AnnexeAnnexe 1: Opérations dans $\mathbb{F}_4$.

Soit j la classe de x dans L . Alors :

+	0	1	j	j^2
0	0	1	j	j^2
1	1	0	j^2	j
j	j	j^2	0	1
j^2	j^2	j	1	0

x	0	1	j	j^2
0	0	0	0	0
1	0	1	j	j^2
j	0	j	j^2	1
j^2	0	j^2	1	j

Annexe 2: Algorithme de Berlekamp

Soit $P \in \mathbb{F}_q[x]$ sans facteurs carrés. On pose :

$$S_P : \begin{cases} \mathbb{F}_q[x]/(P) \rightarrow \mathbb{F}_q[x]/(P) \\ (Q \bmod P) \mapsto Q(x^q) \bmod P (= Q^q \bmod P) \end{cases}$$

On note $P = P_1 \dots P_n$ avec P_i irréductible et $K_i = \mathbb{F}_q[x]/(P_i)$ corps.

On définit l'isomorphisme de K -algèbres :

$$\psi : \begin{cases} \mathbb{F}_q[x]/(P) \rightarrow K_1 \times \dots \times K_n \\ Q \bmod P \mapsto (Q \bmod P_1, \dots, Q \bmod P_n) \end{cases}$$

Soit $\alpha = x \bmod P$ dans $\mathbb{F}_q[x]/(P)$ et $\mathcal{B} = \{1, \alpha, \dots, \alpha^{\deg P - 1}\}$ base de $\mathbb{F}_q[x]/(P)$. Alors le processus suivant s'arrête et décompose P :

- (i) On calcule la matrice $S_P - \text{id}$ dans $\mathcal{B}$, et on passe à (ii)
- (ii) Soit $r = \text{nbe d'in. décomposant } P$. Alors $r = \dim(\text{Ker}(S_P - \text{id}))$.
Si $r=1$, P est ir. et on s'arrête. Sinon on passe à (iii)
- (iii) Soit $v \in \mathbb{F}_q[x]$ non congru à une constante mod P
et $v \bmod P \in \text{Ker}(S_P - \text{id})$. Alors $P = \prod_{\alpha \in \mathbb{F}_q} \text{PGCD}(P, v - \alpha)$.

- Justifier l'irréductibilité. mentionner la factorisation
Une des 2 justif or les corps de rupture

- irred de deg ≤ 3
($\Rightarrow$ avoir une r)

- "spécialisation"

- Bertekamp: expliquer pourquoi c'est bien. Efficacité?

- Thm de la base hilbertienne

- Le corps de rupt. c'est le + pt tel qu'on obtient une $\mathbb{F}$

- Applica° : * corps finis $\rightarrow$ la plus grosse appli à mettre

* Irr de $\mathbb{R}$ ou $\mathbb{C} \rightarrow$ histoires de réduction, diagonalisation de $\mathbb{R}$

$\rightarrow$ irr de $\mathbb{C} \Rightarrow$ liste des irr de $\mathbb{R}$

appli: réduc° des endomorphes normaux

CH + Lemme noyau ...

* Hm de $\mathbb{R}^n$ prim

Hm de prolongement des morph $\left. \begin{matrix} \text{corps} \\ \text{(perm)} \end{matrix} \right\}$ appli alg

* polygones constructibles à la règle et au compas
Gauss Wantzel

$\leftarrow$ même poly cyclotomique est irréductible

- Desponilles : * # d'irred de deg n de $\mathbb{F}_q$ $\neq$ Demazure

$\hookrightarrow$ à quoi ça sert? permet de savoir bien lu ou de chance d'en avoir un en tirant au hasard

- Polygone de Newton: généraliser Eisenstein.

$P(\mathbb{Z}[X])$ eg $2X^5 + 2X^4 + 6X^3 + 8X^2 + 1$

ℓ premier eg $\ell - 2$

Critère de Oama

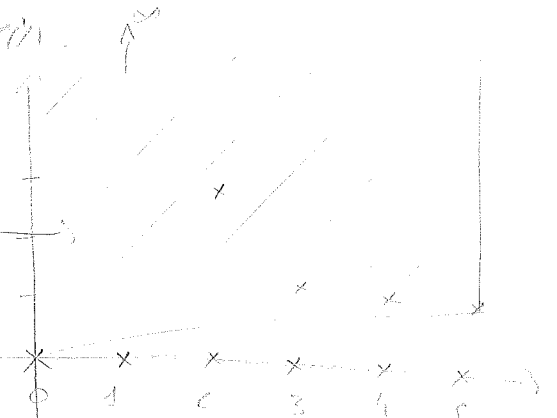
(Prasolov)

polygone = enveloppe
axe des gphe

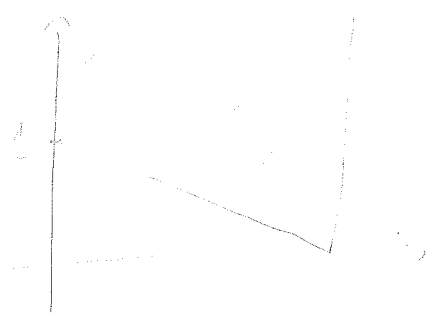
(i, l'val radique)

une pente $\Rightarrow$ irr

coeff d'ord $\leq$ puissance



Cas particulier: ensemble:
lfs de cette forme
une pente = irr.



Exercices

1 || p premier $\neq 2$. Ω_q p est irred de $\mathbb{Z}(i)$ si X^2+1 irred de $\mathbb{Z}/p\mathbb{Z}$.

$\mathbb{Z}(i)$ eucl car $1.1 \Rightarrow$ ppal $\Rightarrow$ (irr $\Leftrightarrow$ premier)

$$\mathbb{Z}(i) \simeq \mathbb{Z}[X]/(X^2+1)$$

ideal engendré premier

$$\mathbb{Z}[X]/(p) \simeq (\mathbb{Z}[X]/(X^2+1)) / (p) = \mathbb{Z}[X]/(p, X^2+1)$$

↑ idéal

← idéal engendré par p et X^2+1

$A/\text{ideal engendré}$ intègre.

$$\& \mathbb{Z}[X]/(p) \simeq \mathbb{Z}/p\mathbb{Z}[X] \text{ donc } \simeq (\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1) \xrightarrow{\mathbb{F}_p(X)} \mathbb{F}_p(X)/(X^2+1)$$

Donc p irred $\Leftrightarrow$ p premier $\Leftrightarrow \mathbb{Z}(i)/p$ intègre car $\mathbb{F}_p(X)/(X^2+1)$ intègre
 $\Leftrightarrow X^2+1$ irr sur $\mathbb{F}_p(X)$

↑ encore l'histoire de $\mathbb{F}_p(X)$ ppal $\Rightarrow$ (irr $\Leftrightarrow$ premier)
 ↑ car $\mathbb{F}_p = \text{corps}$.

|| En déduire que p somme de 2 carrés si $p \equiv 1 \pmod{4}$

Rappels: carrés de $\mathbb{F}_p$: $\forall a \in \mathbb{F}_p^*, a^{p-1} = 1 \pmod{p} \Rightarrow a^{\frac{p-1}{2}} = \pm 1 \pmod{p}$
 Si $x = y^2$ alors $x^{p-1/2} = y^{p-1} = 1 \pmod{p}$.
 ↑ pthm de Fermat ↑ p impair ↑ $X^2-1 = (X-1)(X+1)$ + intègre.

$$\prod_{x \in \mathbb{F}_p^*} (X-x) = X^{p-1} - 1 = (X^{p-1/2} - 1)(X^{p-1/2} + 1) \quad \# \{\text{carrés}\} = \frac{p-1}{2} = \# \{\text{non carrés}\}$$

Donc $\forall a \in \mathbb{F}_p^* \quad (a/p) \equiv a^{p-1/2} \pmod{p}$
 $= \begin{cases} 1 & \text{si } a \text{ carré, } a \in \mathbb{F}_p^* \\ -1 & \text{si } a \text{ non carré, } a \in \mathbb{F}_p^* \\ 0 & \text{si } p \mid a \end{cases}$

p somme de 2 carrés $\Leftrightarrow p = a^2 + b^2 = (a+ib)(a-ib)$, $a, b \in \mathbb{Z}$ ③
 $\Leftrightarrow X^2 + 1$ red. ds $\mathbb{F}_p[X]$ non inv car inv de $\mathbb{Z}(i)$
 $= \pm 1$ et $\pm i$
 $\xrightarrow{\text{mod de deg } \leq 3} \Leftrightarrow \exists a \in \mathbb{F}_p, a^2 = -1 \Leftrightarrow (-1)^{(p-1)/2} = 1 \Leftrightarrow p \equiv 1 \pmod{4}$
 $\Leftrightarrow p \equiv 1 \pmod{4} \in \mathbb{Z} \Leftrightarrow p = 1 \pmod{4}$ $-1 = \text{carré ds } \mathbb{F}_p$

[2] Soit $u \in \text{End}_{\mathbb{R}}(E)$, $\dim(E) = n < +\infty$. Alors il existe une drc
 ou un plan de E inv par u

Utiliser la décomp en irr de χ_u + lemme des noyaux

[3] Soit $P \in \mathbb{Z}[X]$, $\alpha_1, \dots, \alpha_n \in \mathbb{C}$. $m = \max |\alpha_i|$

Qq s'il existe $x_0 \in \mathbb{Z}$, $|x_0| > m+1$ tq $P(x_0)$ premier alors P irred ds $\mathbb{Z}[X]$

Si $P = QR$ ds $\mathbb{Z}[X]$, $P(x_0) = Q(x_0)R(x_0)$ dc $\begin{cases} Q(x_0) = 1 \\ R(x_0) = p \end{cases}$ (OPS).
 $|x_0 - \alpha_i| > 1$ dc $|\prod_{i \in I \subset \{1, \dots, n\}} (x_0 - \alpha_i)| > 1$ or $Q = \prod_{i \in I} (X - \alpha_i)$ pr un certain I .
 $I \neq \emptyset$

Ponc $I = \emptyset$ et $Q = 1$.

[4] Soit $P = p_n X^n + \dots + p_0$ $m = \text{Ent}(n+1/2)$

Supposons qu'il existe $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$ ar $0 < |P(\alpha_i)| < m! / 2^m$

Qq P irred ds $\mathbb{Z}[X]$

DV / : Critère d'Eisenstein
(Cassini, Algèbre 1)

chut
11

Dém du Lemme de Gauss

(i) On pose $P = \sum_{k=0}^n a_k X^k$; $Q = \sum_{k=0}^m b_k X^k$; $PQ = \sum_{k=0}^{n+m} c_k X^k$.

Raisonnons par l'absurde et donc supposons que $C(PQ) \neq 1$. Il existe alors $p \in A$ premier avec $p \mid a_k$, pour tout $k \in [0; n+m]$. On a alors dans $A_{(p)}[X]$:

$0 = \overline{PQ} = \overline{P} \cdot \overline{Q}$. Comme p est premier, $A_{(p)}[X]$ est intègre. On aurait donc $\overline{P} = 0$ ou $\overline{Q} = 0$ ce qui est impossible, car P et Q sont primitifs.

(ii) On remarque que $PQ = c(P) c(Q) \cdot \frac{P}{c(P)} \cdot \frac{Q}{c(Q)}$, avec $\frac{P}{c(P)}$ et $\frac{Q}{c(Q)}$ primitifs. Par (i), $C(\frac{P}{c(P)} \frac{Q}{c(Q)}) = 1$. Donc:

$$C(PQ) = C(P) C(Q).$$

Dém du critère

Raisonnons par l'absurde et supposons que P (et a fortiori $\tilde{P} := \frac{1}{c(P)} P$) est réductible dans $K[X]$.

$$\exists R, S \in K[X], \tilde{P} = RS.$$

$$\text{On: } \exists \alpha, \beta \in A_{(p)}, \alpha R \in A[X], \beta S \in A[X].$$

De plus, comme $\alpha \beta \tilde{P} = (\alpha R) \cdot (\beta S)$, on a:

$$\alpha \beta = c(\alpha R) \cdot c(\beta S).$$

$$\text{Ainsi: } P = \frac{c(P)}{\alpha \beta} \alpha \beta \tilde{P} = \underbrace{\left[\frac{c(P)}{c(\alpha R)} \alpha R \right]}_{=: U} \cdot \underbrace{\left[\frac{1}{c(\beta S)} \beta S \right]}_{=: W}$$

On sait que $U, W \in A[X]$. Donc P est réductible dans $A[X]$.

De plus, $\overline{P} = \overline{a_n} X^n = \overline{U} \cdot \overline{W}$. Si on écrit $U = \sum_{k=0}^i u_k X^k$ et

$W = \sum_{k=0}^j w_k X^k$, on trouve $\overline{u_i} \cdot \overline{w_j} = \overline{a_n} \neq 0$. Alors

$\deg \overline{U} = i$ et $\deg \overline{W} = j$. Par unicité de la décomposition en irréductibles, $\overline{U} = \overline{u_i} X^i$ et $\overline{W} = \overline{w_j} X^j$. Dans ce cas, $p \mid u_0$ et $p \mid w_0$. On aurait $p^2 \mid u_0 w_0 = a_0$ ce qui est impossible.

DV2 : Algorithme de Berlekamp (Beck, Objectif Agrégation)

On pose $P = P_1 \dots P_n \in \mathbb{F}_q[x]$, avec P_i irréductibles sur $\mathbb{F}_q[x]$
et pour $i \neq j$, $P_i \neq P_j$.

* Montrons que $1 = \dim(\text{Ker}(S_P - \text{id}))$ ← peu de + implt
after bcp bcp plus vite

$$\text{Soit } \tilde{S}_P = \varphi \circ S_P \circ \varphi^{-1} : K_1 \times \dots \times K_n \rightarrow K_1 \times \dots \times K_n$$

$$(x_1, \dots, x_n) \mapsto (x_1^q, \dots, x_n^q)$$

$$\text{Ainsi } (x_1, \dots, x_n) \in \text{Ker}(\tilde{S}_P - \text{id}) \Leftrightarrow (x_1^q, \dots, x_n^q) = (x_1, \dots, x_n)$$

$$\Leftrightarrow \forall i \in [1, n], x_i^q = x_i \text{ [dans } K_i \text{]}$$

Soit $\iota : \mathbb{F}_q \hookrightarrow K$ extension de corps. Montrons que $\iota(\mathbb{F}_q) = \{x \in K, x^q = x\} =:$

Par le théorème de Lagrange, on a :

$$\forall x \in \mathbb{F}_q^*, x^{q-1} = 1$$

Donc $\mathbb{F}_q \subseteq E$. Or le polynôme $x^q - x$ admet au plus q racines. On sait que $\#\iota(\mathbb{F}_q) = q$. Donc $E = \iota(\mathbb{F}_q)$.

$$\text{Ainsi } (x_1, \dots, x_n) \in \text{Ker}(\tilde{S}_P - \text{id}) \Leftrightarrow \forall i \in [1, n], x_i \in \mathbb{F}_q.$$

Cela revient à dire que $\text{Ker}(\tilde{S}_P - \text{id}) = \mathbb{F}_q^n$.

Comme $\text{Ker}(S_P - \text{id}) \subseteq \text{Ker}(\tilde{S}_P - \text{id})$, on a :

$$\dim \text{Ker}(S_P - \text{id}) = \dim \text{Ker}(\tilde{S}_P - \text{id}) = n$$

On a bien : $1 = \dim(\text{Ker}(S_P - \text{id}))$.

** Supposons que $n > 1$ par la suite. On sait que l'ensemble des polynômes $U \bmod P$, avec U non congru à une constante modulo P , est la droite vectorielle de $\mathbb{F}_q[x]/(P)$ dirigée par 1.

Comme $\dim \text{Ker}(S_P - \text{id}) > 1$, il existe

** Montrons que pour $\alpha \in \mathbb{F}_q$, $\text{PGCD}(V - \alpha, P) = \prod_{i: P_i | V - \alpha} P_i$

En effet, $\text{PGCD}(V - \alpha, P) \mid P$. Donc :

$$\exists I_\alpha \subseteq [1, n], \text{PGCD}(P, V - \alpha) = \prod_{i \in I_\alpha} P_i$$

Or $\text{PGCD}(P, V - \alpha) \mid V - \alpha$. Par le lemme de Gauss,

$P_i \mid V - \alpha$, pour $i \in I_\alpha$.

On a donc bien $\text{PGCD}(P, V - \alpha) = \prod_{i: P_i | V - \alpha} P_i$.

$$G_1 (V \bmod P) \in \ker (S_p - id) \Leftrightarrow V \bmod P_i \in \mathbb{F}_q, \forall i \in \llbracket 1, n \rrbracket \quad \text{d'après le lemme}$$

$$\Leftrightarrow \forall i, \exists \alpha_i \in \mathbb{F}_q, P_i \mid V - \alpha_i.$$

$$\text{Ainsi : } \alpha_i = \alpha \Leftrightarrow V - \alpha = 0 \bmod P_i \Leftrightarrow P_i \mid V - \alpha.$$

$$\text{Donc } I_\alpha = \{ i \in \llbracket 1, n \rrbracket, \alpha_i = \alpha \}.$$

$$\text{Alors } P = \prod_{\alpha} \prod_{i \in I_\alpha} P_i = \prod_{\alpha} \text{PGCD}(P, V - \alpha) \quad (*)$$

*** Montrons que l'algorithme se termine.

Si pour tout $i \neq j$, $\alpha_i = \alpha_j = \alpha$, alors $V \equiv \alpha \pmod{P}$, par le lemme chinois, ce qui est impossible.

Ainsi parmi les polynômes dans $(*)$ il en existe deux qui ne sont pas triviaux.

Donc $\# \{ Q \text{ irréductible}, Q \mid \text{PGCD}(P, V - \alpha) \} < n$.

Commentaires :

- ajouter ent on se ramène à P sans facteurs carrés
 $\hookrightarrow$ prendre $\text{PGCD}(P, P')$ et diviser P par ce PGCD (en faisant un peu attention)
- aller + vite à la première partie
- Efficacité : Prot de Gauss