Calcul Formel - Master 1 - Univ. Paris-Saclay

Chapitre 5 - Partie 1

I Polynômes séparables et corps parfaits

k corps, $P \in k[X]$ non nul. P séparable si ses racines (dans une extension de k sur laquelle il est scindé) sont simples. Pour P irréductible : P séparable $\iff P' \neq 0$.

Déf : k est un corps parfait si : $\underset{P \in k[X]}{P \text{ irréductible}} \implies \underset{(\text{i.e. } P \text{ séparable})}{P' \neq 0}$

Ex : $\mathbb{F}_2(T)$ n'est pas parfait. En effet $X^2 - T$ est irréductible de dérivée nulle.
[Pas de racine dans $\mathbb{F}_2(T)$: si $R = \frac{A}{B} \in \mathbb{F}_2(T)$ vérifie $R^2 = T$ alors $\underbrace{A(T)^2}_{\text{deg. pair}} = \underbrace{T\,B(T)^2}_{\text{deg. impair}}$]

Th : Soit k un corps. Alors : k parfait $\iff \begin{cases} \text{ou bien } k \text{ est de caractéristique nulle} \\ \text{ou bien } k \text{ est de caract } p \text{ et le morphisme de} \\ \quad \text{Frobenius } \begin{array}{l} k \to k \\ x \mapsto x^p \end{array} \text{ est surjectif} \end{cases}$

Corollaire : Si k corps fini alors k est parfait.

Corollaire : Si $P \in \mathbb{F}_q[X]$ est irréductible alors $P' \neq 0$ et P est séparable.

Preuve du Th : Soit k un corps de caractéristique p.

⊛ Supposons le morphisme de Frobenius surjectif. Soit $P \in k[X]$ tel que $P' = 0$. On a

$P(X) = \sum_{k=0}^{d} a_k X^k$ avec $\sum_{k=1}^{d} k a_k X^{k-1} = 0$ donc $\forall k \in [\![1, d]\!]$, $p \nmid k$, $a_k = 0$.

$P(X) = \sum_{i=0}^{\lfloor d/p \rfloor} a_{pi} X^{pi}$; or $a_{pi} = b_i^p$ donc $P(X) = \sum_{i=0}^{\lfloor d/p \rfloor} b_i^p (X^i)^p = \left(\sum_{i=0}^{\lfloor d/p \rfloor} b_i X^i\right)^p = Q(X)^p$ avec $Q \in k[X]$.

⊛ Supposons $\exists a \in k$ tel que $X^p - a$ n'ait aucune racine dans k. Notons L une extension du corps k sur laquelle $X^p - a$ est scindé. Notons $b \in L$ une racine de $X^p - a$. Alors $X^p - a = X^p - b^p = (X - b)^p$. Montrons que $X^p - a \in k[X]$ est irréductible. Si ce n'était pas le cas on aurait $Q \in k[X]$ tel que $\deg Q \in [\![1, p-1]\!]$ et Q divise $X^p - a$. On peut supposer Q unitaire, et alors $Q(X) = (X - b)^{\deg Q}$. Le coeff de $X^{\deg Q - 1}$ dans Q est $-(\deg Q) b \in k$ car $Q \in k[X]$. Donc $b \in k$, contradiction.

Déf : $P \in k[X]$ est dit sans facteur carré si il n'existe pas de $Q \in k[X]$ non constant tel que Q^2 divise P.

NB : en décomposant P en produit d'irréductibles dans $k[X]$ cela signifie que les exposants sont tous $= 1$.

<u>Prop</u> : Soit k un corps parfait. Soit $P \in k[X]$ non nul. Alors :

P est sans facteur carré $\iff$ P est séparable.

<u>Preuve</u> : $\boxed{\Leftarrow}$ Si $P = Q^2 R$ avec $Q, R \in k[X]$ et Q non constant, alors
$P' = 2QQ'R + Q^2R' = Q(2Q'R + QR')$ donc Q divise pgcd(P, P').

$\boxed{\Rightarrow}$ Supposons $P = \prod_{i=1}^{r} P_i$ avec P_i irréductibles 2 à 2 distincts.
Supposons que P n'est pas séparable : pgcd$(P, P') \neq 1$. Quitte à renuméroter les P_i on peut supposer que P_1 divise P'. Or $P' = \sum_{i=1}^{r} P_i' \prod_{j \neq i} P_j \equiv P_1' \prod_{j=2}^{r} P_j \mod P_1$.
Or P_1 irréductible, premier avec $P_2, \dots, P_r$ donc P_1 divise P_1'. Donc P_1 n'est pas séparable. Or P_1 irréductible : contradiction car k est parfait.

Calcul Formel - Master 1 - Univ. Paris-Saclay
Chapitre 5 - Partie 2

II Comment se ramener à factoriser des polynômes sans facteur carré.

Soit k un corps parfait.

Lemme : Si k est de caractéristique p et parfait, et si $P \in k[X]$ vérifie $P' = 0$, alors il existe $Q \in k[X]$ tel que $P = Q^p$.

Rappel : Si $P' = 0$ alors $P(X) = \sum a_i X^{pi}$; on pose $b_i \in k$ tel que $b_i^p = a_i$, et $Q = \sum b_i X^i$ vérifie $Q^p = P$.

Comment trouver une racine $p^{\text{ième}}$ de $a \in k$?
→ Si $k = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, prendre a lui-même.
→ Si $k = \mathbb{F}_q$ avec $q = p^d$, prendre $b = a^{p^{d-1}}$.
En effet $b^p = a^{p^d} = a^q = a$.

Soit k un corps parfait dans lequel on sait trouver des racines $p^{\text{ièmes}}$ (par exemple $k = \mathbb{F}_q$).

Algorithme pour factoriser $P \in k[X]$ quelconque en supposant qu'on sait factoriser tout pol. sans facteur carré :

1. Si $P' = 0$: trouver $Q \in k[X]$ tel que $Q^p = P$, factoriser Q (récursivement).
2. Si $P' \neq 0$ calculer $Q = \mathrm{pgcd}(P, P')$.
   a) Si $Q = 1$: P séparable donc P sans facteur carré : on sait le factoriser.
   b) Si Q non constant : on factorise Q et $\frac{P}{Q}$ (récursivement).

III Algorithme de Berlekamp.

Soit $\mathbb{F}_q$ un corps fini, et $P \in \mathbb{F}_q[X]$ de degré $d \geq 1$.

Buts : ① Tester si P est irréductible. ② Factoriser P dans $\mathbb{F}_q[X]$. $\Big\}$ on peut supposer P unitaire, séparable

Notons $P = P_1 P_2 \dots P_e$ la décomposition de P en produit de pol. irréd. unitaires 2 à 2 $\neq$.

Posons $A = \mathbb{F}_q[X]/(P)$. Par le Th. chinois on a un isom. de $\mathbb{F}_q$-algèbres :

$$f : A = \mathbb{F}_q[X]/(P) \longrightarrow \mathbb{K}_1 \times \dots \times \mathbb{K}_e \quad \text{où } \mathbb{K}_i = \mathbb{F}_q[X]/(P_i) \text{ corps fini}$$

$$[\mathbb{K}_i : \mathbb{F}_q] = \deg P_i.$$

Notons $\varphi_q : \begin{array}{l} A \to A \\ a \mapsto a^q \end{array}$ et $A' = \{a \in A,\ a^q = a\}$.

Prop : A' est un $\mathbb{F}_q$-espace vectoriel de dimension e.

Preuve : $f(A') = \{(a_1, \dots, a_e) \in \mathbb{K}_1 \times \dots \times \mathbb{K}_e,\ \forall i \in [\![1,e]\!]\ a_i^q = a_i\} = \mathbb{F}_q \times \dots \times \mathbb{F}_q = \mathbb{F}_q^e$.

Notons x la classe de X modulo (P), i.e. l'image de X dans A, et $\mathcal{B} = (1, x, \dots, x^{d-1})$ base de A (vu comme e.v. sur $\mathbb{F}_q$). Notons $\Phi_q = \mathrm{Mat}_{\mathcal{B}}\, \varphi_q$. On a $A' = \mathrm{Ker}(\Phi_q - I_d)$.

Algorithme de Berlekamp pour déterminer le nombre de facteurs irréductibles de P :

Calculer $\dim \mathrm{Ker}(\Phi_q - I_d)$.

$j^{\text{ème}}$ colonne de Φ_q (pour $0 \leq j \leq d-1$) : x^{jq} revient à calculer X^{jq} mod P.

$X^{jq} = (X^{(j-1)q} \cdot X^q)$ mod P.

Recherche d'un facteur non trivial de P :

Prop : Soit $P \in \mathbb{F}_q[X]$ unitaire, séparable, de degré $d \geq 1$. Notons $Q \in \mathbb{F}_q[X]$ non constant, de degré $\leq d-1$, tel que $Q^q \equiv Q \bmod P$. Alors il existe $\lambda \in \mathbb{F}_q$ tel que $\operatorname{pgcd}(Q+\lambda, P)$ soit un facteur non trivial de P (i.e. soit non constant).

NB : l'hypothèse sur Q signifie que $Q(x)$ est vecteur propre de φ_q relatif à la valeur propre 1.

Algorithme de Berlekamp pour factoriser P :

- déterminer si $e = 1$ ou $e \geq 2$.
- Si $e \geq 2$ alors $\dim \operatorname{Ker}(\varphi_q - \mathrm{Id}) \geq 2$: déterminer un vecteur propre de Φ_q qui ne soit pas l'image dans A d'un polynôme constant. Cela correspond à $Q \in \mathbb{F}_q[X]$ non constant vérifiant les hypothèses de la Proposition. On parcourt $\mathbb{F}_q$ pour trouver λ qui donne un facteur non trivial S de P. On factorise récursivement S et P/S.

Preuve de la Prop : $f : A = \mathbb{F}_q[X]/(P) \longrightarrow \mathbb{K}_1 \times \dots \times \mathbb{K}_e$. Notons $f(Q \bmod P) = (a_1, \dots, a_e) \in \mathbb{F}_q^e$.
Comme Q n'est pas constant, les a_i ne sont pas tous égaux. Posons $\lambda = -a_1$.
Alors $f((Q+\lambda) \bmod P) = (0, a_2 - a_1, \dots, a_e - a_1) \neq (0, 0, \dots, 0)$. Donc $Q+\lambda \not\equiv 0 \bmod P$.
En outre $(Q+\lambda) \bmod P_1$ est nul donc $P_1 \mid Q+\lambda$. Donc $P_1 \mid \operatorname{pgcd}(Q+\lambda, P)$.