Calcul Formel - Master 1 - Univ. Paris-Saclay

Chapitre 4 - Partie 1

I Généralités, caractéristique.

Soit A un anneau (commutatif, unitaire). On dispose de $\varphi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & A \\ n & \longmapsto & n 1_A \end{array}$ hom. d'anneaux.
Ou bien $\ker \varphi = \{0\}$: on dit que A est de caract. nulle.
Ou bien $\ker \varphi = d\mathbb{Z}$ avec $d \in \mathbb{N}^*$: on dit que A est de caractéristique d.
Si A est un corps alors sa caractéristique est soit 0, soit un nombre premier.

Th : Soit $\mathbb{K}$ un corps fini. Alors le cardinal de $\mathbb{K}$ est de la forme p^d, avec p sa caractéristique (qui est un nombre premier) et $d \in \mathbb{N}^*$.

Preuve : étant donné un corps $\mathbb{K}$ de caractéristique p, l'ensemble des $n 1_{\mathbb{K}}$ avec $n \in \mathbb{Z}$ forme un sous-corps de $\mathbb{K}$ appelé sous-corps premier de $\mathbb{K}$, qui est isomorphe au corps $\mathbb{Z}/p\mathbb{Z}$.
On constate que $\mathbb{K}$ peut être muni d'une structure d'espace vectoriel sur ce sous-corps premier $\mathbb{K}_0$ en posant $\lambda \cdot x = \lambda x$ pour $\lambda \in \mathbb{K}_0$ et $x \in \mathbb{K}$. Si $\mathbb{K}$ fini $d = \dim_{\mathbb{K}_0}(\mathbb{K}) < \infty$.

Désormais on réserve la lettre p aux nombres premiers
et la lettre q aux entiers de la forme p^d, avec $d \in \mathbb{N}^*$.

NB : $\mathbb{Z}/p\mathbb{Z}$ est un corps de cardinal p. ⚠ $\mathbb{Z}/p^2\mathbb{Z}$ N'EST PAS un corps de cardinal p^2.
↳ c'est un anneau qui n'est même pas intègre.

Propriété : Soit A un anneau de caractéristique p, avec p premier. Alors :

$$\forall a, b \in A \quad (a+b)^p = a^p + b^p.$$

Preuve : Binôme de Newton ; $\forall i \in [\![1, p-1]\!] \quad p \mid \binom{p}{i}$ donc $\binom{p}{i} a^i b^{p-i} = 0_A$.

Déf : Soit A un anneau de caractéristique p, avec p premier. On appelle morphisme de Frobenius l'application $\varphi : A \longrightarrow A$, $a \mapsto a^p$. C'est un homomorphisme d'anneaux.

Prop : Soit $\mathbb{K}$ un corps fini de cardinal $q = p^d$. Alors : $\forall x \in \mathbb{K}^* \quad x^{q-1} = 1$.

Preuve : vrai si $x = 0$; sinon, $x \in \mathbb{K}^*$ avec $\mathbb{K}^*$ groupe de cardinal $q-1$ donc $x^{q-1} = 1$.

Notons $\varphi : \mathbb{K} \to \mathbb{K}$, $x \mapsto x^p$; alors pour tout $i \in \mathbb{N}$, $\varphi^i = \underbrace{\varphi \circ \varphi \circ \dots \circ \varphi}_{i} : \mathbb{K} \longrightarrow \mathbb{K}$, $x \mapsto x^{p^i}$ donc la proposition précédente affirme que $\varphi^d = Id_{\mathbb{K}}$ si $\mathrm{Card}\,\mathbb{K} = p^d$. Notamment : $\varphi = Id_{\mathbb{K}}$ si $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$.

[Réciproquement si $\varphi = Id_{\mathbb{K}}$ alors $\mathrm{Card}\,\mathbb{K} = p$ car $X^p - X$ possède au plus p racines].

NB : $\forall i \in \mathbb{N} \quad \forall a, b \in A \quad (a+b)^{p^i} = a^{p^i} + b^{p^i}$ si A est un anneau de caractéristique p.

Th : Soit $\mathbb{K}$ un corps fini. Alors le groupe $\mathbb{K}^*$ est cyclique : il existe $\omega \in \mathbb{K}^*$ tel que tout élément non nul de $\mathbb{K}$ soit de la forme ω^j avec $j \in \mathbb{Z}$.

Chapitre 4 - Partie 2

II Terminologie générale

Préambule : représentation pratique des corps finis.

Th : Soit k un corps et $P \in k[X]$ irréductible. Alors $\mathbb{K} = \frac{k[X]}{(P)}$ est un corps.

Ex : $k = \mathbb{Z}/2\mathbb{Z}$, $P(X) = X^2 + X + 1$, $\mathbb{K} = \frac{(\mathbb{Z}/2\mathbb{Z})[X]}{(X^2+X+1)}$.

Th (suite) : $\mathbb{K}$ est un espace vectoriel de dimension $\deg P$ sur le corps k ; une base de cet e.v. est $(1, x, x^2, \dots, x^{\deg P - 1})$ où x est la classe de X modulo P.

Ex (suite) : $\mathbb{K}$ est un $\mathbb{Z}/2\mathbb{Z}$ - espace vectoriel de dimension 2 donc $\mathrm{Card}\,\mathbb{K} = 2^2 = 4$.

Th (fin) : $\mathrm{Card}\,\mathbb{K} = (\mathrm{Card}\,k)^{\deg P}$ si k corps fini ; comme groupe abélien $\mathbb{K}$ est isomorphe à $k^{\deg P}$.

En pratique on peut construire un corps fini de cardinal $q = p^d$ en choisissant $P \in (\mathbb{Z}/p\mathbb{Z})[X]$ irréductible de degré d et en considérant $\mathbb{K} = \frac{(\mathbb{Z}/p\mathbb{Z})[X]}{(P)}$.

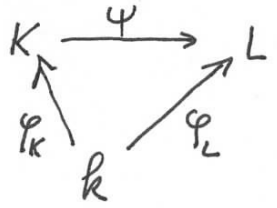
Intérêt algorithmique : si on sait calculer dans $\mathbb{Z}/p\mathbb{Z}$ alors on sait calculer dans $\frac{(\mathbb{Z}/p\mathbb{Z})[X]}{(P)}$.

1) Extensions, degrés. Soient k et K deux corps.

Définitions : ⊛ On dit que K est une extension de k (et on note K/k) si on dispose d'un homomorphisme de corps $\varphi : k \to K$ (appelé aussi plongement). [En effet tout hom. de corps est injectif] [Alors $\varphi(k)$ est un sous-corps de K isomorphe à k ; réciproquement si K possède un sous-corps isomorphe à k alors K est une extension de k].

⊛ Soient K et L deux extensions d'un même corps k. On appelle k-plongement de K dans L tout homomorphisme de corps $\psi : K \to L$ qui induise l'identité sur k (si on voit k comme sous-corps de K et L), i.e. si :

$$\forall x \in k \quad \psi\big(\underbrace{\varphi_K(x)}_{x \text{ vu dans } K}\big) = \underbrace{\varphi_L(x)}_{x \text{ vu dans } L}$$

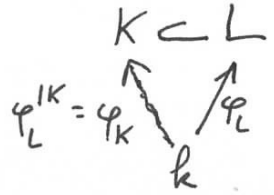


i.e. $\psi \circ \varphi_K = \varphi_L$.

⊛ Deux extensions K et L d'un même corps k sont dites isomorphes s'il existe un k-plongement bijectif $K \to L$.

⊛ Une extension K/k est dite finie si la dimension de K vu comme k-e.v. est finie. En effet on a une structure d'espace vectoriel en posant $\lambda \cdot y = \underbrace{\varphi(\lambda)}_{\in K}\,\underbrace{y}_{\in K}$ (produit dans K) avec $\varphi : k \to K$, $\lambda \in k$, $y \in K$. Dans ce cas, le degré de K/k est $[K:k] = \dim_k K$.

⊛ Si L est une extension de k, un k-sous-corps de L est un sous-corps K de L tel que $\varphi_L(k) \subset K$.



Th : Si K/k et L/K sont finies alors L/k aussi, et $[L:k] = [L:K]\cdot[K:k]$.

Prop : Soit k un corps et A une k-algèbre, qui est de dim finie comme k-e.v.
Si A est intègre alors A est un corps.

Calcul Formel - Master 1 - Univ. Paris-Saclay

Chapitre 4 - Partie 3

2.) Corps de rupture.

Soit k un corps. Soit $P \in k[X]$ irréductible.

Déf : Un corps de rupture de P sur k est une extension K de k munie d'un isomorphisme de k-extensions $K \xrightarrow{\sim} k[X]/(P)$.

Nb : Alors $[K : k] = \deg P$.

Ex : Si $P(X) = X^2 - \alpha$ avec $\alpha \in k$, et si $\beta \in K$ racine de P, alors $k(\beta)$ est un corps de rupture de P sur k en le munissant $k[X]/(P) \to k(\beta)$, $Q \mapsto Q(\beta)$. On obtient un autre corps de rupture en munissant $k(\beta)$ de $k[X]/(P) \to k(\beta)$, $Q \mapsto Q(-\beta)$. ↳ si k est de caractéristique $\neq 2$

Prop : Soit K un corps de rupture de P sur k, et L une extension de k. Alors se donner un k-plongement $K \to L$ revient à se donner un élément $x \in L$ tel que $P(x) = 0$.

Preuve : ⊛ Si $\sigma : K \to L$ alors on a $k[X]/(P) \xrightarrow{\sim} K \xrightarrow{\sigma} L$ et on note $x \in L$ l'image de la classe de X.

⊛ A partir de x on construit $k[X]/(P) \to L$, $Q \mapsto Q(x)$ puis $K \xrightarrow{\sim} k[X]/(P) \to L$.

Corollaire : Se donner un corps de rupture de P sur k revient à se donner une extension K de k et un élément $x \in K$ tel que $\begin{cases} P(x) = 0 \\ K = k(x) \end{cases}$

Prop : Soit K/k une extension (finie) de corps et $x \in K$. Alors il existe un unique polynôme unitaire, irréductible sur k, qui s'annule en x : c'est le polynôme minimal de x sur k. Le plus petit sous-corps de K contenant k et x est noté $k(x)$; c'est un corps de rupture de P (polynôme minimal de x sur k) quand on le munit de la racine x.
On a $k(x) \simeq k[X]/(P)$; c'est un espace vectoriel sur k de degré $\deg P$.
On note $[k(x):k] = \deg P$, et on a $k(x) = \{Q(x),\ Q \in k[X],\ \deg Q < \deg P\}$.

Notation : $k(x_1, \dots, x_m) = \big(k(x_1, \dots, x_{m-1})\big)(x_m)$ pour $x_1, \dots, x_m \in K$ extension finie de k.

Déf : On appelle élément primitif d'une extension K/k tout $x \in K$ tel que $K = k(x)$.

Th [facile] Toute extension de corps finis possède un élément primitif.

Preuve : Soit K/k une extension, avec K fini. Notons x un générateur de K^*. Alors $K = k(x)$.

Propriété : Soit $P \in k[X]$ de degré $d \geq 2$, avec k corps. Alors : P irréductible $\Leftrightarrow$ P n'a aucune racine dans aucune extension de k de degré $\leq \lfloor d/2 \rfloor$.

Preuve : $\Leftarrow$ Si P réductible, $P = P_1 P_2 \dots P_\ell$ avec $\ell \geq 2$ et P_j irréductibles sur k. On part supposer $\deg P_1 \leq \frac{d}{2}$.
Notons K un corps de rupture de P_1 sur k. Alors $[K:k] \leq \lfloor d/2 \rfloor$ et P possède une racine dans K.

$\Rightarrow$ Soit K une extension de k de degré $e \leq \lfloor d/2 \rfloor$. Soit $x \in K$ une racine de P.
Notons Q le polynôme minimal de x sur k. Alors Q est irréductible sur k, et Q divise P puisque $P(x) = 0$. Enfin $\deg Q = [k(x):k] \leq [K:k] \leq \lfloor \frac{d}{2} \rfloor < d = \deg P$.
Donc P est réductible.

Chapitre 4 - Partie 4

3) Polynômes scindés et corps de décomposition.

Soit k un corps et $P \in k[X]$.

Déf : P est dit *scindé* sur k si il existe $\lambda, a_1, \dots, a_n \in k$ tels que $P(X) = \lambda \prod_{i=1}^{n} (X - a_i)$.

Prop : Soit $P \in k[X]$. Il existe une extension finie K de k sur laquelle P est scindé.

Preuve : Récurrence sur $\deg P$. ⊛ Si P n'est pas irréductible, $P = QR$ avec $\deg Q, \deg R < \deg P$. Par hyp. de réc. il existe L/k (finie) telle que Q soit scindé sur L. On applique à nouveau l'hyp. de réc. à $R \in L[X]$: on obtient K/L (finie) telle que R soit scindé sur K.

⊛ Si P est irréductible, il existe un corps de rupture L de P sur k. Notons $\alpha \in L$ une racine de P, et $P(X) = (X - \alpha) S(X)$ avec $S \in L[X]$. Par hyp. de récurrence il existe K/L finie telle que S soit scindé sur K ; alors P est scindé sur K.

Déf : Soit k un corps et $P \in k[X]$. On appelle *corps de décomposition* de P sur k toute extension K/k telle que : (i) P est scindé sur K

(ii) $K = k(x_1, \dots, x_n)$ où $x_1, \dots, x_n$ sont les racines de P dans K.

Prop : Si K/k et L/k sont deux corps de décompositions de P, alors les extensions K/k et L/k sont isomorphes.

Preuve : on peut supposer que K et L sont contenus dans une même extension (finie) M de k.
Alors on a : $K = k(x_1, \dots, x_m) = L$ en notant $x_1, \dots, x_m$ les racines de P dans M.

Exemple : $k = \mathbb{Q}$, $P(X) = X^3 - 2$. Racines complexes : $\sqrt[3]{2}$, $j\sqrt[3]{2}$, $j^2\sqrt[3]{2}$ avec $j = e^{2i\pi/3}$.
Corps de décomposition : $\mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, j)$ est l'unique sous-corps de $\mathbb{C}$ qui soit un corps de décomposition de P.
Corps de rupture : si on s'intéresse à ceux qui sont des sous-corps de $\mathbb{C}$, il y en a 3 : $\left(\mathbb{Q}(\sqrt[3]{2}), \sqrt[3]{2}\right)$; $\left(\mathbb{Q}(j\sqrt[3]{2}), j\sqrt[3]{2}\right)$; $\left(\mathbb{Q}(j^2\sqrt[3]{2}), j^2\sqrt[3]{2}\right)$.

En général Si $k = \mathbb{Q}$ et $P \in \mathbb{Q}[X]$, notons $\alpha_1, \dots, \alpha_m$ les racines complexes de P.
Alors ~~(si P est irréductible sur $\mathbb{Q}$)~~ il y a un et un seul sous-corps de $\mathbb{C}$ qui est un corps de décomposition de P : c'est $\mathbb{Q}(\alpha_1, \dots, \alpha_m)$.
⊛ (si P est irréductible sur $\mathbb{Q}$) il y a m sous-corps de $\mathbb{C}$ qui sont des corps de rupture de P : ce sont les $\left(\mathbb{Q}(\alpha_i), \alpha_i\right)$.
⚠ les corps $\mathbb{Q}(\alpha_i)$ ne sont pas forcément distincts.

Chapitre 4 - Partie 5

4) Polynômes séparables.

Soit k un corps. Pour $P \in k[X]$, $P = \sum_{i=0}^{n} a_i X^i$, on note $P' = \sum_{i=1}^{n} i a_i X^{i-1}$.

Prop : Si P est scindé sur k, notons $P(X) = \lambda \prod_{i=1}^{n} (X - a_i)$ avec $\lambda, a_1, \dots, a_n \in k$ et $\lambda \neq 0$.
Alors les assertions suivantes sont équivalentes :

(i) $\operatorname{pgcd}(P, P') = 1$.

(ii) P et P' n'ont aucune racine commune dans k.

(iii) $a_1, \dots, a_n$ sont 2 à 2 distincts.

Quand elles sont vérifiées on dit que P est scindé à racines simples dans k.

Preuve : (i) $\Leftrightarrow$ (iii) P est scindé donc $\operatorname{pgcd}(P, P')$ est aussi scindé sur k.

((**NB :** pour $P = (X^2+1)^2$ dans $\mathbb{R}[X]$, (i) est fausse mais (ii) est vraie))

(ii) $\Leftrightarrow$ (iii) La dérivée d'un produit $Q_1 Q_2 \cdots Q_n$ est : $\sum_{j=1}^{n} Q_j' \prod_{i \neq j} Q_i$. D'où :

$$P'(X) = \lambda \sum_{j=1}^{n} \prod_{\substack{1 \leq i \leq n \\ i \neq j}} (X - a_i).$$ D'où $\forall k \in [\![1, n]\!]$ $P'(a_k) = \lambda \prod_{\substack{1 \leq i \leq n \\ i \neq k}} (a_k - a_i)$.

D'où : $P'(a_k) = 0 \iff \exists i \neq k$ tel que $a_i = a_k$.

Prop Déf : Soit k un corps et $P \in k[X]$ non nul. Alors les assertions suivantes sont équivalentes :

(i) $P \wedge P' = 1$.

(ii) Il existe une extension K de k sur laquelle P est scindé et telle que P et P' n'ont aucune racine commune dans K.

(iii) Pour toute extension K de k sur laquelle P est scindé, P et P' n'ont aucune racine commune dans K.

(iv) Il existe une extension K de k sur laquelle P possède $\deg P$ racines distinctes.

(v) Sur toute extension K de k sur laquelle P est scindé, les racines de P sont 2 à 2 distinctes.

Quand elles sont vérifiés on dit que P est *séparable*.

NB : P séparable $\Leftrightarrow$ sur une extension K de k sur laquelle P est scindé, P est scindé à racines simples.

Lemme : Soit $P, Q \in k[X]$. Alors le pgcd de P et Q, calculé dans $K[X]$ où K est une extension quelconque de K, est toujours le même : il ne dépend pas de K.

Preuve : pgcd(P, Q) se calcule par l'algorithme d'Euclide dont le déroulement est le même sur K que sur k.

Prop : Soit $P \in k[X]$ irréductible. Alors : P séparable $\Leftrightarrow P' \neq 0$.

Corollaire : Si k est de caractéristique nulle et si P est irréductible alors P est séparable.

Preuve : $P \wedge P'$ est $= 1$ ou alors associé à P. Donc : P non séparable $\Leftrightarrow P \wedge P'$ associé à P
$\Leftrightarrow P$ divise P'
$\Leftrightarrow P' = 0$ (sinon car $\deg P' < \deg P$).

Chapitre 4 - Partie 6

III Existence, unicité, plongements.

Th : Soient p premier et $n \in \mathbb{N}^*$. Alors il existe un corps fini de cardinal p^n.

Preuve : Notons $\mathbb{K}$ un corps de décomposition de $X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$, avec $q = p^n$.

Notons $B = \{x \in \mathbb{K},\ x^q = x\}$.

(i) $X^q - X$ est scindé sur $\mathbb{K}$, et séparable donc $\mathrm{Card}\, B = q$.

(ii) B est l'ensemble des points fixes de $\psi : \mathbb{K} \to \mathbb{K}$, $x \mapsto x^q$. Or $\psi = \varphi^n$ où $\varphi : \mathbb{K} \to \mathbb{K}$, $x \mapsto x^p$, et $\varphi^n = \underbrace{\varphi \circ \dots \circ \varphi}_{n \text{ fois}}$. Or φ hom. de $\mathbb{Z}/p\mathbb{Z}$-algèbres donc ψ aussi.

(iii) B est un sous-anneau de $\mathbb{K}$ contenant $\mathbb{Z}/p\mathbb{Z}$. Donc $\mathbb{K} = B$. D'où $\mathrm{Card}\, \mathbb{K} = p^n$.

A retenir : tous les éléments de $\mathbb{K}$ vérifient $x^q = x$.

Notation : on note $\mathbb{F}_q$ un corps à q éléments, lorsque q est de la forme p^n.

Th : Soient $\mathbb{K}$ et $\mathbb{K}'$ deux corps finis de même cardinal.
Alors $\mathbb{K}$ et $\mathbb{K}'$ sont isomorphes.

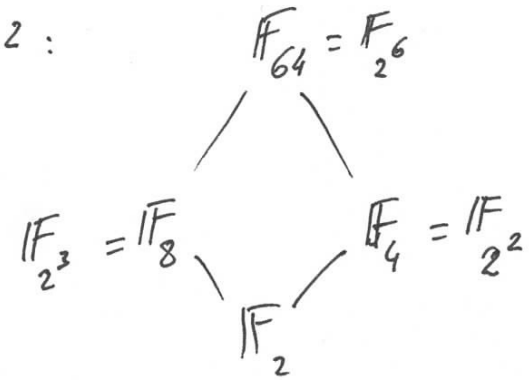
Th : Soit p, p' deux nombres premiers, et $n, n' \in \mathbb{N}^*$.
Soient $\mathbb{K}, \mathbb{K}'$ deux corps finis, avec $\mathrm{Card}\,\mathbb{K} = p^n$ et $\mathrm{Card}\,\mathbb{K}' = p'^{n'}$. Alors :
(il existe un plongement $\mathbb{K} \to \mathbb{K}'$) $\iff$ ($p = p'$ et n divise n').

Preuve : $\boxed{\Rightarrow}$ $n' = [\mathbb{K}' : \mathbb{F}_p] = [\mathbb{K}' : \mathbb{K}]\,[\mathbb{K} : \mathbb{F}_p] = n\,[\mathbb{K}' : \mathbb{K}]$.

$\boxed{\Leftarrow}$ Soit $d \in \mathbb{N}^*$ tel que $n' = dn$. Notons $\mathbb{K}''$ un corps fini qui contient $\mathbb{K}$ et $\mathbb{K}'$.
Alors $\mathbb{K} = \{x \in \mathbb{K}'',\ x^{p^n} = x\}$ et $\mathbb{K}' = \{x \in \mathbb{K}'',\ x^{p^{n'}} = x\}$. Or $x^{p^n} = x \Rightarrow x^{p^{dn}} = x$
(car en notant $\varphi : x \mapsto x^q$, avec $q = p^n$, on a $\varphi^d(x) = x^{q^d}$ avec $q^d = (p^n)^d = p^{dn}$) : $\mathbb{K} \subset \mathbb{K}'$.

A retenir : Soient p premier et $n \in \mathbb{N}^*$. Soit $\mathbb{K} = \mathbb{F}_{p^n}$. Alors pour tout m diviseur de n, $\mathbb{K}$ possède un unique sous-corps de cardinal p^m qui est $\{x \in \mathbb{K},\ x^{p^m} = x\}$.

Exemple : $p = 2$:



⚠ $\mathbb{F}_4$ n'est PAS isomorphe à un sous-corps de $\mathbb{F}_8$ car 2 ne divise pas 3

Chapitre 4 - Partie 7

IV Polynômes irréductibles sur un corps fini.

1) Théorème principal.

Notation : Soit $\mathbb{F}_q$ un corps fini de cardinal $q = p^n$. et $\mathbb{K}$ une extension de $\mathbb{F}_q$. On note $\varphi_q : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & x^q \end{array}$ le morphisme de Frobenius relatif à $\mathbb{F}_q$.

Th : Soit $\mathbb{F}_q$ un corps fini à q éléments, et $P \in \mathbb{F}_q[X]$ irréductible unitaire de degré d.
Notons $\mathbb{E}$ un corps de rupture de P sur $\mathbb{F}_q$, avec $x \in \mathbb{E}$ racine de P. Alors :

(i) $d = \deg P$ est le plus petit entier $k \geq 1$ tel que $\varphi_q^k(x) = x$.

(ii) $P = \prod_{i=0}^{d-1} (X - \varphi_q^i(x))$: P est scindé (sur $\mathbb{E}$) et ses racines sont les $\varphi_q^i(x)$, $0 \leq i \leq d-1$.

(iii) $\mathbb{E}$ est un corps de décomposition de P.

(iv) P est séparable.

Corollaire : Sur un corps fini, tout polynôme irréductible est séparable.

Corollaire : Pour un polynôme irréductible P sur un corps fini, tout corps de rupture est aussi un corps de décomposition. En outre toutes les racines de P s'obtiennent à partir de l'une d'entre elles par applications successives de φ_q. [appliquer φ_q se fait efficacement par exponentiation rapide]

Preuve : ⊛ $x^{q^d} = x$ car $\mathrm{Card}\,\mathbb{E} = q^d$ donc k existe, et $k \leq d$.

⊛ $\mathbb{Z}$ agit sur $\mathbb{E}$ en posant $m \cdot y = \varphi_q^m(y)$. Action de $\mathbb{Z}$ sur $\mathbb{E}$: homom. $\mathbb{Z} \to \mathfrak{S}(\mathbb{E})$.

L'orbite de x est $\{x, \varphi_q(x), \dots, \varphi_q^{k-1}(x)\}$ est de cardinal k.

⊛ Comme $P \in \mathbb{F}_q[X]$ on a : $\forall y \in \mathbb{E}$ $\quad P(\varphi_q(y)) = \varphi_q(P(y))$. Donc φ_q stabilise l'ensemble des racines de P dans $\mathbb{E}$.

⊛ Notons $Q = \prod_{i=0}^{k-1} (X - \varphi_q^i(x))$: alors Q divise P, et les coefficients de Q sont des polynômes symétriques élémentaires en $\varphi_q^0(x) = x, \varphi_q(x), \dots, \varphi_q^{k-1}(x)$. Or cet ensemble de k racines est fixé globalement par φ_q. Donc les coeff. de Q sont fixés par φ_q : $Q \in \mathbb{F}_q[X]$.

⊛ P irréductible dans $\mathbb{F}_q[X]$, P et Q unitaires, donc $Q = P$ et $k = d$.

⊛ P scindé sur $\mathbb{E}$ et $\mathbb{E} = \mathbb{F}_q(x) = \mathbb{F}_q(x, \varphi_q(x), \dots, \varphi_q^{d-1}(x))$ d'où (iii).

Corollaire : Soit $\mathbb{E}$ une extension finie de $\mathbb{F}_q$ de degré d. Alors $\mathrm{Aut}(\mathbb{E}/\mathbb{F}_q)$ est un groupe cyclique d'ordre d engendré par φ_q.

Preuve : Notons H le sous-groupe de $\mathrm{Aut}(\mathbb{E}/\mathbb{F}_q)$ engendré par φ_q.

On a $\mathrm{Card}\,H = d$. Notons $x \in \mathbb{E}$ tel que $\mathbb{E} = \mathbb{F}_q(x)$. Notons P le polynôme minimal de x sur $\mathbb{F}_q$. Alors un $\mathbb{F}_q$-homomorphisme de corps $\mathbb{E} \to \mathbb{E}$ est donné par le choix d'une racine de P dans $\mathbb{E}$.

Calcul Formel - Master 1 - Univ. Paris-Saclay

Chapitre 4 - Partie 8

2) Factorisation de $X^{q^n}-X$ et comptage des polynômes irréductibles.

Th : Soit $\mathbb{F}_q$ un corps fini. Soit $n \in \mathbb{N}^*$. Alors, dans $\mathbb{F}_q[X]$, $X^{q^n}-X$ est le produit des polynômes irréductibles unitaires de $\mathbb{F}_q[X]$ dont le degré divise n.

NB : Pour $n=1$, $X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X-\alpha)$.

Preuve : Considérons $\mathbb{E}$ une extension de $\mathbb{F}_q$ de degré n, et l'action de $\mathbb{Z}$ sur $\mathbb{E}$ donnée par $m \cdot y = \varphi_q^{\,m}(y)$ où $\varphi_q(y) = y^q$. On montre que l'application suivante est bijective : $\{\text{orbites}\} \xrightarrow{\sim} \{P \in \mathbb{F}_q[X] \text{ irréductibles unitaires de degré divisant } n\}$

$\mathcal{O} \longmapsto$ polynôme minimal de x sur $\mathbb{F}_q$ pour $x \in \mathcal{O}$

⊛ Soit $x, x' \in \mathbb{E}$. Alors : (x et x' sont dans la même orbite) $\Leftrightarrow$ (x et x' ont même pol. minimal).

Notons $x \in \mathbb{E}$ et P son pol. minimal. Alors $P(X) = \prod_{i=0}^{\deg P - 1} (X - x^{q^i})$.

⊛ Si $x \in \mathbb{E}$, notons P son pol. minimal. Alors $\deg P = [\mathbb{F}_q(x) : \mathbb{F}_q]$ divise $[\mathbb{E} : \mathbb{F}_q] = n$.

⊛ Soit $P \in \mathbb{F}_q[X]$ irréductible unitaire. Notons $\mathbb{K}$ un corps de rupture de P sur $\mathbb{F}_q$, avec $x \in \mathbb{K}$ racine de P. Si $\deg P$ divise n alors $[\mathbb{K} : \mathbb{F}_q]$ divise $[\mathbb{E} : \mathbb{F}_q]$ donc $\mathbb{K}$ est isomorphe à une sous-extension de $\mathbb{E}$ donc $\exists x' \in \mathbb{E}$ racine de P.

Finalement $\mathbb{E} = \bigsqcup_{\substack{P \text{ irréd. unit.} \\ \text{tq } \deg P \text{ divise } n}} \{\text{racines de } P\}$ donc $X^{q^n} - X = \prod_{x \in \mathbb{E}} (X-x) = \prod_{\substack{P \text{ irréd. unit.} \\ \text{tq } \deg P \text{ divise } n}} \underbrace{\prod_{\substack{x \text{ racine} \\ \text{de } P}} (X-x)}_{P(X)}$.

NB : $X^{q^n} - X = \prod_{d|n} \prod_{\substack{P \text{ irréd. unit.} \\ \text{de degré } d}} P$. Notons N_d le nombre de polynômes irréductibles unitaires de degré d sur $\mathbb{F}_q$.

NB : $\boxed{N_d \geq 1}$. En effet il existe $\mathbb{E}$ extension de $\mathbb{F}_q$ de degré d, et il existe $x \in \mathbb{E}$ tq $\mathbb{F}_q(x) = \mathbb{E}$. Alors le polynôme minimal de x sur $\mathbb{F}_q$ est irréd. unitaire de degré d.

Corollaire : Pour tout $n \geq 1$ (et pour tout q) : $q^n = \sum_{d|n} d N_d$. "$d|n$" : d divise n

Def : Fonction de Möbius : si $n = \prod_{i=1}^{k} p_i^{e_i}$ avec $p_1, \dots, p_k$ premiers 2 à 2 $\neq$ et $e_1, \dots, e_k \in \mathbb{N}^*$,

$\mu(n) = \begin{cases} 0 & \text{si } \exists i \in [\![1,k]\!] \ e_i \geq 2 \\ (-1)^k & \text{si } e_1 = \dots = e_k = 1 \end{cases}$

NB : $\mu(1) = 1$.

Corollaire : $N_n = \frac{1}{n} \sum_{d|n} \mu(d)\, q^{n/d}$.

Preuve : $\sum_{d|n} \mu(d) q^{n/d} = \sum_{d|n} \mu(d) \sum_{e|n/d} e N_e = \sum_{e|n} e N_e \underbrace{\sum_{\substack{d|n \\ \text{tq } e|\frac{n}{d}}} \mu(d)}_{\chi_{e,n}}$

Montrons que $\chi_{e,n} = \begin{cases} 0 & \text{si } e|n,\ e \neq n \\ 1 & \text{si } e = n \end{cases}$

En effet $\chi_{e,n} = \sum_{d|\frac{n}{e}} \mu(d)$; notons $\frac{n}{e} = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $\alpha_i \in \mathbb{N}^*$ et $p_1, \dots, p_r$ premiers 2 à 2 $\neq$

$$\chi_{e,n} = \sum_{\substack{(\beta_1,\dots,\beta_r) \in \mathbb{N}^r \\ \text{tq } \forall i\ 0 \leq \beta_i \leq \alpha}} \mu\left(p_1^{\beta_1} \cdots p_r^{\beta_r}\right) = \sum \mu\left(p_1^{\beta_1}\right) \cdots \mu\left(p_r^{\beta_r}\right) = \prod_{i=1}^{r} \left(\sum_{\beta=0}^{\alpha_i} \mu\left(p_i^{\beta}\right) \right) = \prod_{i=1}^{r} \underbrace{(1 - 1 + 0 + \dots + 0)}_{=0}$$

Chapitre 4 - Partie 9

V Recherche de générateurs

1) Cas d'un groupe cyclique.

Soit G cyclique d'ordre n noté multiplicativement.

Hypothèse : on sait factoriser n.

Algorithme pour tester si $x \in G$ est un générateur : (i) calculer $x^{n/p}$ pour p premier, $p \mid n$.

(ii) Si on trouve p tel que $x^{n/p} = 1$ alors x n'est pas générateur.

(iii) Sinon, alors x est générateur.

Correction : x non générateur $\iff \exists k \in \mathbb{N}^*$, $k \mid n$, $k \neq n$, $x^k = 1$; prendre $p \mid \frac{n}{k}$.

Alors $k \mid \frac{n}{p}$

Complexité : $O(\omega(n) \log n)$ produits dans le groupe,

où $\omega(n)$ est le nombre de p premiers qui divisent n.

Comment trouver un générateur de G ?

* choisir $x \in G$ aléatoirement.
* Tester si x est générateur.
* Si x n'est pas générateur, recommencer.

Proportion de générateurs dans G : $\frac{\varphi(n)}{n} = \prod_{\substack{p \mid n \\ p \text{ premier}}} \left(1 - \frac{1}{p}\right)$.

2) Application à un corps fini $\mathbb{F}_q$.

$G = \mathbb{F}_q^*$ cyclique d'ordre $n = q-1$.

Hypothèse : on sait factoriser $q-1$.

Test pour savoir si $x \in \mathbb{F}_q^*$ est générateur : $O(\omega(q-1)\log q)$ multiplications dans $\mathbb{F}_q$.

Proportion de générateurs dans $\mathbb{F}_q^*$: $\dfrac{\varphi(q-1)}{q-1} = \prod_{\substack{p \text{ premier} \\ p \mid q-1}} \left(1 - \dfrac{1}{p}\right)$.

Ex. : p nombre premier de Sophie Germain : $q = 2p+1$ est premier ; $\mathbb{F}_q \simeq \mathbb{Z}/q\mathbb{Z}$.

Alors $\dfrac{\varphi(q-1)}{q-1} = \dfrac{1}{2}\left(1 - \dfrac{1}{p}\right) \approx \dfrac{1}{2}$ si p est très grand.