Séminaire Dubreil.
Algèbre et théorie
des nombres

L. Kaloujnine

Corps fini ou champ de Galois

Séminaire Dubreil. Algèbre et théorie des nombres, tome 1 (1947-1948), exp. n° 2, p. 1-14
<http://www.numdam.org/item?id=SD_1947-1948__1__A2_0>

Faculté des Sciences de Paris
-:-:-:-
Séminaire A. CHÂTELET et P. DUBREIL
(ALGÈBRE et THÉORIE DES NOMBRES)
Année 1947/48
-:-:-:-

Exposé n° 2

CORPS FINI OU CHAMP DE GALOIS

par L. KALOUJNINE

1. Formule d'inversion de Möbius.

On appelle fonction arithmétique $f(n)$, une fonction dont la variable n est un entier positif et dont la valeur appartient à un groupe abélien G (additif ou multiplicatif).

La formule d'inversion de Möbius est exprimée par l'équivalence des deux formules :

(1) $F(n) = \sum f(d)$;

(1') $f(n) = \sum [\mu(d).F(n : d)]$;

d diviseur de n.

le signe $\sum$ indique la composition dans G et le $.$ indique l'itération de cette composition (multiplication ou exponentiation) par l'entier $\mu(d)$. Cet entier est la fonction arithmétique définie par :

$\mu(1) = 1$;

$\mu(m) = 0$, si m a un facteur carré ;

$\mu(m) = (-1)^r$, si m est produit de r facteurs premiers.

en particulier :

$$F(1) = f(1) .$$

En designant par "intégrale arithmétique" ou "fonction sommatoire" d'une fonction arithmétique $g(n)$, la somme :

$$G(n) = \sum g(d) \quad (d \text{ diviseur de } n)$$

la formule de Möbius exprime que si $F(n)$ est fonction sommatoire de $f(d)$, inversement $f(n)$ est fonction sommatoire de $[\mu(n : d).F(d)]$; et réciproquement.

La fonction $\mu(n)$ vérifie les deux propriétés des fonctions sommatoires :

$$M(n) = \sum \mu(d) = \begin{cases} 1 , & \text{si } n = 1 \\ 0 , & \text{si } n > 1 ; \end{cases}$$

car si n a r facteurs premiers, le deuxième membre est la somme (des coefficients du binôme) :

$$1 - C_r^1 + C_r^2 + \ldots + (-1)^r C_r^r = 0$$

La somme inverse est :

$$\sum \mu(d).M(n : d) = \mu(n) ;$$

elle n'a en effet qu'un terme non nul, pour $d = n$.

Je suppose l'égalité (1) , et je calcule le 2e membre de 1' .

$$\sum \mu(d).F(n : d) = \sum \sum \mu(d).f(\delta) \quad \begin{cases} d \text{ diviseur de } n \\ \delta \text{ diviseur de } n : d . \end{cases}$$

j'associe les termes en $f(\delta)$, en remarquant que δ , diviseur de $n : d$ est équivalent à d , diviseur de $n : \delta$. La somme est égale à

$$\sum f(\delta).\left[\sum \mu(d')\right] \quad \begin{cases} \delta \text{ diviseur de } n ; \\ d' \text{ diviseur de } n : \delta . \end{cases}$$

Le coefficient de $f(\delta)$ est $M(n : \delta)$, il n'est différent de 0 que pour $\delta = n$; la somme est égale au seul terme $f(n)$.

Je suppose l'égalité (1') , et je calcule le 2e membre de 1 .

$$\sum f(d) = \sum \sum \mu(d : \delta').F(\delta') \quad \begin{cases} d \text{ diviseur de } n \\ \delta' \text{ diviseur de } d . \end{cases}$$

J'associe les termes en $F(\delta')$ en remarquant que d , multiple de δ' et diviseur de n , est équivalent à $d : \delta' = \delta''$, diviseur de $n : \delta'$. La somme est égale à :

$$\sum F(\delta').\left[\sum \mu(\delta'')\right] = \sum F(\delta').M(n : \delta') ;$$

elle n'a qu'un terme non nul pour $\delta' = n$ et elle est égale à $F(n)$.

Une fonction arithmétique est <u>factorisable</u> si elle est définie dans un anneau (dont G est le groupe additif) et si :

(a , b premiers entre eux) $\longrightarrow$ $f(a \times b) = f(a) \times f(b)$.

La fonction $\mu(n)$ est factorisable. La propriété se conserve par multiplication. La fonction sommatoire d'une fonction factorisable (définie par l'addition de l'anneau) est elle-même factorisable et réciproquement :

$$F(a \times b) = \sum f(a) \times f(b) = \sum f(d_a) \times \sum f(d_b) = F(d_a) \times F(d_b)$$

$$f(a \times b) = \sum \mu(d_a \times d_b).F(ab : d_a\ d_b) = \sum \mu(d_a)F(a : d_a) \times \sum \mu(d_b)F(b : d_b)$$

d_a et d_b diviseurs respectifs de a et b .

APPLICATIONS. - L'indicateur d'Euler $\varphi(n)$ (nombre de classes premières avec n) est factorisable ; sa fonction sommatoire est n .

$$n = \sum \varphi(d) , \qquad \varphi(n) = \sum \mu(d).(n : d) .$$

Le polynôme :

$$\delta(x , n) = \prod (x - \xi^i) \quad \begin{cases} i \text{ classe première avec } n \\ \xi \text{ racine primitive } n\text{-ième de } 1 . \end{cases}$$

de degré $\varphi(n)$ est une fonction arithmétique de n et il en est de même de :

$$\Delta(x , n) = \prod (x^n - 1)$$

$\Delta(x , n)$ est la fonction sommatoire de $\delta(x , n)$, le groupe G étant multiplicatif :

$$\Delta(x , n) = \prod \delta(x , d) ; \quad \delta(x , n) = \prod (\Delta(x , n : d))^{\mu(d)}$$

(les produits étant étendus aux diviseurs d de n) .

La formule de Möbius s'étend à une fonction dont la variable est un facteur d'un domaine d'intégrité à factorisation unique.

2. Propriétés nécessaires d'un champ de Galois.

Un champ de Galois est un corps commutatif d'un nombre fini d'éléments. Un premier exemple en est l'ensemble $M(p)$ des p classes d'entiers, définis, mod p : c'est un groupe additif (ou module) de p éléments et les $p - 1$ éléments non nuls constituent un groupe multiplicatif (cyclique).

Un corps commutatif fini doit avoir pour caractéristique un nombre premier p : si e est son unité et m un entier ordinaire :

$$(e + e + \ldots + e) = m.e = 0 \Longleftrightarrow m = 0 \pmod p .$$

En effet les éléments $m.e$ du corps sont en nombre fini, les multiplicateurs de ceux qui sont nuls constituent un module de nombres entiers, donc l'ensemble des multiples d'un entier p .

Cet entier p est premier, car s'il était produit de deux entiers $a \times b$,

supérieurs à 1 , le produit des facteurs du corps (a.e) × (b.e) = (p.e) serait nul sans qu'aucun des facteurs le soit (et il y aurait des diviseurs de 0) .

Au point de vue de l'addition, le corps doit être un espace vectoriel, d'une dimension finie f , relativement au corps M(p) . Ses éléments, en nombre $q = p^f$, doivent être de la forme :

$$\alpha = \sum u_i . \omega_i \qquad (u_i \text{ entiers mod } p . \ i \text{ de } 1 \text{ à } f)$$

les élements ω_i de base étant supposés indépendants ($\alpha = 0 \longrightarrow u_i = 0$).

Les éléments α constituent un groupe additif ; chaque élément α, non nul est, comme l'élément unité e , d'ordre p ; les invariants du groupe sont en nombre f , égaux à p .

Les $q - 1 = m$ éléments non nuls doivent constituer un groupe multiplicatif G(p , f) , de sorte que tout élément non nul est d'ordre (multiplicatif) diviseur de m :

$\alpha \neq 0 \longrightarrow \alpha^m - 1 = 0$; ou $\alpha^q - \alpha = 0$, tout α ;

il appartient à un exposant d , (diviseur de m) :

$$\alpha^x = 1 \iff x \equiv 0 , \pmod{d} .$$

3. Construction du corps M(p , f) .

Il existe un et un seul corps M(p , f) , fini commutatif, de caractéristique p , de $q = p^f$ éléments. Pour l'obtenir, il suffit de décomposer le polynôme $x^q - x$ en facteurs irréductibles dans le corps M(p) et d'adjoindre à M(p) , (successivement ou simultanément) les zéros de ces polynômes. L'extension ainsi réalisée ne contient que les zéros de ces polynômes :

Les éléments de M(p) sont notamment les zeros de $x^p - x$, diviseur de $x^q - x$.

D'une part si α et β sont des zéros (non nuls) de $x^m - 1$:

$$(\alpha^i \times \beta^j)^m = (\alpha^m)^i \times (\beta^m)^j = 1 ;$$

quels que soient i , j entiers, le monôme est encore zéro de ce polynôme.

D'autre part, quels que soient α et β , zéros de $x^q - x$:

$$(\alpha + \beta)^q \equiv (\alpha^q + \beta^q) , \mod p = \alpha + \beta$$

leur somme est zéro du même polynôme.

4. Ordre d'un élément.

Dans le corps M(p , f) (dont l'existence et l'unicité sont ainsi démontrées), j'associe tous les éléments α (s'ils existent) appartenant à l'exposant d , diviseur de m , et je forme le polynôme qui les a pour zéros :

$$\delta(x , d) = \prod (x - \alpha) \quad (\alpha \text{ d'ordre } d) .$$

Manifestement :

$$\prod \delta(x , d) = x^m - 1$$

$$\sum (\text{degrés de } \delta(x , d)) = m \qquad (d \text{ diviseur de } m) .$$

Par application de la formule de Möbius :

$$\delta(x , d) = \prod (x^{d : d'} - 1)^{\mu(d')} \qquad (d' \text{ diviseur de } d) .$$

$$\text{degré } \delta = \varphi(d) \quad (\text{indicateur de } d)$$

Il y a $\varphi(d)$ éléments appartenant à l'exposant d , et, en particulier, $\varphi(m)$ appartenant à l'exposant m .

Comme dans M(p) , le groupe multiplicatif G(p , f) est cyclique. Le polynôme $\delta(x , d)$ est égal, mod p , à celui qui a pour zéros les racines primitives, d'indice d , de l'unité.

Les seuls éléments d'ordre diviseur de p - 1 (tels que $\beta^{p-1} = 1$) sont les éléments de M(p) non nuls; qui sont les zéros de :

$$x^{p-1} - 1 = \prod (x - a_i) \quad (a_i \text{ de } 1 \text{ à } p-1)$$

5. Extension simple.

On peut construire un corps fini en utilisant un polynôme f(x) , de degré f' , à coefficients dans M(p) et irréductible (on démontrera a posteriori l'existence de tels polynômes pour tout degré f') . Il suffit de constituer l'ensemble des expressions rationnelles, à coefficients dans M(p) , d'un zéro α de f(x) ; c'est un corps isomorphe de l'ensemble des fonctions rationnelles, de λ , considéré comme une indéterminée, à coefficients entiers, définis au double module près : p et f(q)

$$\beta = h(\lambda) \mod (p , f(\lambda)) .$$

Tout polynôme a une (et une seule) forme canonique qui est un polynôme en α , de degré f' - 1 :

$$\beta = \sum b_i . \alpha^i \quad (b_i \mod p , \quad i \text{ de } 0 \text{ a } f' - 1) .$$

Il y a $q' = p^{f'}$ éléments qui forment un corps $M(p , f')$. Tout élément non nul est d'ordre diviseur de $m' = q' - 1 = p^{f'} - 1$.

Il en résulte que : tout polynôme $f(x)$, de degré f' , à coefficients dans $M(p)$ et irréductible, divise $x^m - 1$.

En effet un zéro α de $f(x)$, dans $M(p , f')$, y annule $x^m - 1$; il y a donc divisibilité dans $M(p)$.

On en conclut que tous les zeros de $f(x)$ sont dans $M(p , f)$ puisque zéros de $x^m - 1$.

6. Groupe d'isomorphismes de l'extension simple.

Dans $M(p , f')$, le polynôme $f(x)$ a pour zéros les f' puissances :

$$\alpha , \alpha^p , \alpha^{p^2} , \ldots , \alpha^{p(f'-1)} .$$

D'une part α étant un zéro quelconque de $f(x)$, α^p en est un autre, car :

$$0 = (f(\alpha))^p \equiv f(\alpha^p) \pmod p.$$

D'autre part ces puissances sont différentes, si non les valeurs inégales constitueraient un système de h valeurs qui seraient zéros d'un polynôme $g(x , \alpha)$, à coefficients fonctions de α , dans $M(p)$.

Mais ce polynôme $g(x , \alpha)$ reste égal à lui-même, en remplaçant α par α^p , ses coefficients sont donc dans $M(p)$, comme il divise $f(x)$, irréductible, il ne peut que lui être égal.

Il en résulte notamment que :

$$\alpha^{px} = \alpha \iff x \equiv 0 \pmod{f'}$$

On pourrait encore établir cette propriété en vérifiant que les exposants x sont toutes les valeurs positives d'un module d'entiers.

La base h (p.g.c.d.) de ce module est d'une part diviseur de f' (qui est une valeur de x) . D'autre part elle ne peut lui être inférieure, si non, d'après la propriété :

$$\beta^{p^h} = (\sum b_i \alpha^i)^{p^h} = \sum b_i \alpha^i = \beta$$

tout élément β (de $M(p , f')$) serait d'ordre $p^h - 1$, inférieur à m' , et on a montré qu'il existe effectivement des éléments d'ordre $m' = p^{f'} - 1$.

L'extension $M(p , f')$ est donc normale (et galoisienne) ; elle contient tous

les conjugués de son élément générateur α . Son groupe d'isomorphismes est cyclique, formé par les f' premières puissances de la transformation (réversible) :

$$\alpha \cdot \varphi = \alpha^p \qquad (\alpha . \varphi^i = \alpha^{p^i})$$

7. Degré d'un élément.

Revenant au corps $M(p , f)$, tout élément α y annule un (et un seul, à un coefficient près) polynôme $f(x)$, d'un certain degré f' , à coefficients dans $M(p)$, et irréductible.

En effet les puissances α^i successives de α , considérées comme des vecteurs de l'espace vectoriel $M(p , f)$, relativement à $M(p)$, ne sont pas indéfiniment indépendantes. Si $\alpha^{f'}$ est la première puissance fonction linéaire des précédentes

$$\alpha^{f'} = \sum a_i \alpha^i , \qquad f(x) = x^{f'} - \sum a_i x^i .$$

$f(x)$ ne peut avoir de diviseur $g(x)$, car $g(\alpha)$ serait diviseur de 0 .

Ce degré f' du polynôme est le degré de l'élément α . Il est encore défini par la condition :

$$\alpha^{p^x} = \alpha \iff x \equiv 0 , \pmod{f'} .$$

En effet α engendre une extension $M(p , f')$; qui est sous-corps de $M(p , f)$. La condition vraie dans cette extension le reste dans le sur-corps.

Le degré f' est l'exposant de la plus petite puissance q' , $q' = p^{f'}$ (de p) telle que $\alpha^{q'} = \alpha$.

Il en résulte que f' est un diviseur de f (qui est une valeur particulière de x .

Dans le corps $M(p , f)$, pour chaque diviseur f' de f , il y a des éléments de degré f' . En particulier, il y a des éléments de degré f lui-même, et le corps est constitué par l'extension simple défini par l'adjonction de l'un quelconque d'entre eux ω, à $M(p)$.

La démonstration est analogue à celle de l'existence d'éléments d'un ordre d (diviseur de m) .

Un élément de degré f' , s'il existe, annule un polynôme $a(x , f')$, à coefficients dans $M(p)$ et irréductible. Formons le produit de ces divers polynômes (distincts) :

$$\theta(x , f') = \prod a(x , f') \quad (a \text{ de degré } f' , \text{ irréductible})$$

Ce polynôme, à coefficients dans $M(p)$, a pour zéros (dans $M(p , f)$) tous les éléments de degré f' . En particulier :

$$\theta(x , 1) = x^p - x .$$

Manifestement :

$$\begin{cases} \prod \theta(x , f') = x^{p^f} - x \\ \sum (\text{degrés } \theta) = p^f \end{cases} \quad (f' \text{ diviseur de } f) .$$

Par application de la formule de Möbius :

$$\theta(x , f') = \prod (x^{p^{f' : d'}} - x)^{\mu(d')} \quad (d' \text{ diviseur de } f') .$$

$$\text{degré de } \theta = \sum \mu(d') . p^{f' : d'}$$

Le degré de θ ainsi obtenu est divisible par f' et le quotient est le nombre de polynômes $a(x , f')$ irréductibles de degré f' , dans le corps $M(p)$.

Il résulte encore de ce qui précède que : dans le corps $M(p , f)$, tout polynôme, à coefficients dans $M(p)$, de degré f' , diviseur de f , est décomposable en facteurs du premier degré.

Dans $M(p)$, les polynômes $\zeta(x , d)$ (aux racines primitives d'indice d , diviseur de $p^f - 1$, de l'unité) sont décomposables en polynômes irréductibles dont les degrés f' sont tels que $p^{f'} - 1$ est divisible par d .

8. Base normale.

Tout corps $M(p , f)$ peut être engendré comme un espace vectoriel, relativement à $M(p)$, par une base constitué par les f conjugués d'un élément générateur (ou primitif) ω (qui en sont, comme il a été dit, les puissances d'exposants p^i) . C'est dire que les $q = p^f$ éléments du corps sont exprimés par :

$$\beta = \sum b_i \omega^{p^i} \quad (b_i \mod p , \ i \text{ de } 0 \text{ à } f - 1) .$$

Il suffit de montrer qu'on peut trouver au moins un élément ω , dont les puissances d'exposant p^i soient indépendantes, ou telles que :

$$\sum u_i \omega^{p^i} = 0 \longrightarrow (u_i \equiv 0 , \text{ pour tout } i) .$$

9. Etude des p-polynômes.

Dans ce but, on peut étudier systématiquement des polynômes particuliers,

appelés p-polynômes, de la forme :

$$A(x) = \sum a_i \, x^{p^i} \quad (i \text{ de } 0 \text{ à } n \,,\ a_i \bmod p) \,,$$

auxquels on associe respectivement des polynômes (ordinaires) en y

$$a(y) = \sum a_i \, y^i \,.$$

Si $a_n \not\equiv 0$, le polynôme $A(x)$ est effectivement de degré p^n et son associé est de degré n ; ils sont normés, si $a_n = 1$.

On définit, pour ces polynômes : la multiplication par une constante, l'addition et une multiplication (symbolique) :

$$u.A(x) + v.B(x) = \sum (ua_i + vb_i) \, x^{p^i} \quad (u \,,\ v \in M(p)) \,;$$

$$A(x) \times B(x) = A(B(x)) = B(A(x)) = \sum \left(\sum a_i \, b_j\right) x^{p^k} \quad (i + j = k) \,,$$

auxquels sont associés les opérations (ordinaires) de même nom sur les polynômes associés.

Les polynômes $A(x)$ forment par suite un anneau $P(x)$, isomorphe à l'anneau $P(y)$ des polynômes associés $a(y)$. Tout idéal (symbolique) y est donc principal, c'est-à-dire constitué par les multiples (symboliques) d'un polynôme de base $D(x)$, qui peut être pris normé :

$$M(D(x)) \,, \quad M(x) \text{ p-polynôme quelconque.}$$

Un p-polynôme $A(x)$ est décomposable (comme son associé $a(y)$) d'une seule façon en un produit (symbolique) de puissances (symboliques) de p-polynômes, irréductibles, normés.

10. Zéros des p-polynômes.

L'ensemble $\mathcal{G}(x)$ des p-polynômes $A(x)$, qui sont, au sens ordinaire, divisibles par un polynôme (ordinaire) $h(x)$ c'est-à-dire tels que :

$$A(x) = h(x).q(x) \qquad (h(x) \text{ donné}, \ q(x) \text{ quelconque})$$ est un idéal (symbolique), nécessairement principal.

L'ensemble $\mathcal{G}(x)$, ainsi formé contient la différence de deux de ses éléments quelconques :

$$\left.\begin{aligned} A(x) &= h(x).q(x) \\ A'(x) &= h(x).q'(x) \end{aligned}\right\} \longrightarrow A(x) - A'(x) = h(x).(q(x) - q'(x))$$

Il contient aussi le produit (symbolique) de l'un quelconque de ses éléments par tout p-polynôme :

$$A(x) = h(x).q(x) \longrightarrow E(A(x)) = h(x).q'(x) \ .$$

(tous les termes de $E(x)$ contenant une puissance non nulle de x, la substitution à x de $A(x)$, y met $h(x)$ en facteur).

Ceci s'applique notamment à des p-polynômes, considérés dans un champ de Galois, $M(p\ ,\ f)$, et donne immédiatement les resultats suivants :

l'ensemble des p-polynômes $A(x)$ qui s'annulent pour une valeur α, non nulle, de $M(p\ ,\ f)$ (et, par suite, sont divisibles dans $M(p)$ par le polynôme fondamental de α) forment un idéal, nécessairement principal.

Si un p-polynôme $A(x)$ est annulé dans $M(p\ ,\ f)$ par une valeur α, il en est de même de tout multiple (symbolique) $E(A(x))$, et notamment de toute puissance symbolique $(A(x))^{(m)}$.

Si deux p-polynômes $A(x)$ et $B(x)$ s'annulent, dans $M(p\ ,\ f)$, pour une même valeur α (non nulle), ils ont un diviseur (symbolique) commun (dans $M(p)$), qui est annulé par α.

Si deux p-polynômes $A(x)$ et $B(x)$ sont (symboliquement) premiers entre eux :

ext $U(x)$ et $V(x)$: $U(A(x)) + V(B(x)) = x$ (dans $M(p)$)

quel que soit le corps $M(p\ ,\ f)$, ils n'y ont aucun zéro commun (sauf 0)

11. Formation de la base normale.

Les zéros d'une puissance (symbolique) $(A(x))^{(m)}$ d'un p-polynôme irréductible $A(x)$, de degré p^h constituent un espace vectoriel sur $M(p)$, de dimension p^{hm}, et dont une base est le système des puissances d'exposants p^i (i de 0 à $mh - 1$) d'un zéro convenablement choisi α.

On peut toujours former un champ de Galois où $(A(x))^{(m)}$ soit entièrement décomposable. Nous raisonnerons dans ce champ.

Considérons d'abord le cas d'un polynôme irréductible (à la puissance 1). Si α est un de ses zéros, quelconque, tout élement :

$$\beta = \sum b_i \alpha^{p^i} \quad (i \text{ de } 0 \text{ à } h - 1\ ,\ b_i \bmod p)$$

en est encore un zéro, car :

$$\sum b_i\, x^{p^i} = B(x)\ , \quad 0 = B(A(\alpha)) = A(B(\alpha)) = A(\beta) \ .$$

Ces éléments, en nombre p^h sont tous différents (ou bien encore les éléments α^{p^i} sont indépendants et constituent une base d'espace vectoriel), car :

$$0 = \sum b_i \alpha^{p^i} = B(\alpha)$$

entraîne l'existence d'un zéro commun (non nul) au p-polynôme $A(x)$ irréductible (de degré p^h) et au p-polynôme $B(x)$ de degré p^{h-1} (inférieur) donc premier avec $A(x)$, ce qui exige que $B(x)$ soit (identiquement) nul.

Les éléments β (considérés dans un même champ de Galois de degré convenable $f \geqslant h$) sont fonctions rationnelles les uns des autres, à coefficients dans $M(p)$. Leurs polynômes fondamentaux $f_i(x)$ sont donc tous de même degré, et le produit de ceux qui sont distincts est égal à $A(x)$.

Pour une puissance $(A(x))^{(m)}$, la propriété peut être démontrée par récurrence sur m. Nous supposons que les zéros de $(A(x))^{m-1}$ forment un espace vectoriel de dimension $p^{h(m-1)}$. Le p-polynôme $(A(x))^{(m)}$, de degré p^{mh}, et sans zéro double (sa dérivée étant égale au coefficient de son terme en x, non nul) a au moins un zéro qui n'est pas dans cet espace, donc qui n'annule pas le polynôme précédent ; soit α.

Les éléments

$$B(\alpha) = \sum b_i \alpha^{p^i} \qquad (i \text{ de } 0 \text{ à } mh-1)$$

annulent $A(x)^{(m)}$, le raisonnement déjà fait restant valable. En outre ils sont tous différents, car $B(\alpha)$ nul exige que les p-polynômes $B(x)$ et $(A(x))^{(m)}$ aient un diviseur commun (qui ne peut être qu'une puissance (symbolique) de $A(x)$). Comme α n'annule pas $(A(x))^{(m-1)}$, c'est $(A(x))^{(m)}$ lui-même, de sorte que $B(x)$ est (identiquement) nul.

Ceci acquis, considérons un champ de Galois $M(p , f)$ et décomposons le p-polynôme $x^{p^f} - x$, en un produit symbolique de puissances de p-polynômes irréductibles (qui forment des p-polynômes premiers entre eux deux à deux) :

$$x^{p^f} - x = A(x) \dot{\times} B(x) \dot{\times} \ldots$$

les p-polynômes $A(x)$, $B(x)$, ... (exposants sous-entendus) définissent chacun des espaces vectoriels (sur $M(p)$), engendrés par des zéros convenables $\alpha , \beta , \ldots$ (et sans élément commun, puisqu'ils n'ont pas de zéro commun). Le champ de Galois considéré a une base normale constituée par les puissances d'exposant p^i (i de 1 à f-1) de l'élément :

$$\omega = \alpha + \beta + \ldots$$

Raisonnons sur deux facteurs (ce qui s'étendra aisément).

Cet élément n'annule ni $A(x)$, ni $B(x)$:

$A(\omega) = A(\alpha + \beta) = A(\alpha) + A(\beta) = A(\beta) \neq 0$;
$B(\omega) = B(\alpha + \beta) = B(\alpha) + B(\beta) = B(\alpha) \neq 0$.

Mais ω annule le produit symbolique $A(x) \times B(x)$, car

$$B(A(\omega)) = B(A(\alpha)) + B(A(\beta)) = 0 + B(A(\beta) = A(B(\beta)) = 0 .$$

En outre ω n'annule aucun diviseur du produit symbolique puisqu'il annulerait soit $A(x)$, soit $B(x)$. Les puissances considérées de ω sont donc bien indépendantes et constituent une base du champ de Galois.

12 Application de la formule de Mobius.

Appelons p-polynôme fondamental (ou minimal) d'un élément α , d'un domaine de Galois la base $A(x)$ de l'idéal formé par les p-polynômes qui s'annulent pour α .

Nous avons établi, dans ce qui precède, que tout p-polynôme est fondamental pour certains éléments α :

un p-polynôme irréductible (symboliquement) est fondamental pour tous ses zéros (non nuls) ;
une puissance, d'exposant m , d'un p-polynôme irréductible, est fondamentale pour ceux de ses zéros qui n'annulent pas la puissance d'exposant $m - 1$;
un produit de p-polynômes premiers entre eux, deux à deux, est fondamental pour les sommes des zéros non nuls, pour lesquels les p-polynômes facteurs sont respectivement fondamentaux.

Appelons $\Pi(A)$ le nombre d'éléments dont $A(x)$ est polynôme fondamental. C'est une fonction des $A(x)$, qui sont éléments d'un anneau à factorisation unique. Elle vérifie évidemment la formule sommatoire :

$$\sum \Pi(D) = \text{degré } A , \quad (D \text{ diviseurs (symboliques) de } A) .$$

Donc, par application de la formule de Mobius :

$$\Pi(A) = \sum \mu(D).\text{degré } (A : D) , \quad (D \text{ diviseurs de } A) .$$

Le nombre $\Pi(A)$ ainsi déterminé est nécessairement divisible par l'exposant

h du degré de A ; le quotient est le nombre de bases normales (de chacune h éléments) de l'espace vectoriel construit par les zéros de A(x) . Si A(x) est de le forme $x^{p^h} - x$, cet espace est le corps de Galois M(p , h) .

L'application de ces formules suppose connues les décompositions des p-polynômes en facteurs. On peut les obtenir en cherchant les décompositions des polynômes associés a(y) , d(y), ...

EXEMPLES. - p = 2 .

1° M(2,3). - Le polynôme associé à $x^8 - x$ est $y^3 + 1$, dont la décomposition mod 2, est :

$$y^3 + 1 \equiv (y + 1)(y^2 + y + 1) \pmod 2.$$

L'application de la formule de Mobius donne :

$\pi(x^8+x)$ = degré (x^8+x) - degré(x^2+x) - degré(x^4+x^2+x) + degré(x)= 8-2-4+1 = 3 .

Il n'y a qu'une base normale de 3 éléments obtenus en additionnant le zéro (non nul) de $x^2 + x$ avec les zéros (non nuls) de $x^4 + x^2 + x$.

$$1 + \alpha, \quad 1 + \alpha^2, \quad 1 + \alpha^4, \qquad \alpha^3 + \alpha + 1 = 0$$

Ces éléments annulent le polynôme $x^3 + x^2 + 1$; la décomposition (ordinaire) de $x^8 + x$ en polynômes irréductibles est d'ailleurs :

$$x^8 + x \equiv x(x+1)(x^3+x+1)(x^3+x^2+x) \pmod 2 .$$

2° M(2,4). - La décomposition (ordinaire) de $x^{16} + x$ en polynômes, dont les zéros sont respectivement de degrés diviseurs de 4, donne :

degré 1 : $x^2 + x$
degré 2 : $x^2 + x + 1$
degré 4 : $x^{12} + x^9 + x^6 + x^3 + 1 = (x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$

La décomposition de $x^{15} + 1$ en polynômes (mod 2) dont les zéros sont d'ordres diviseurs de 15 donne :

ordre 1 : $x + 1$
ordre 3 : $x^2 + x + 1$
ordre 5 : $x^4 + x^3 + x^2 + x + 1$
ordre 15: $x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$

Les éléments de degré 1 sont d'ordre 1 ; ceux de degré 2 sont d'ordre 3 ; dans ceux de degré 4 , 4 éléments sont d'ordre 5 et les deux autres systèmes de 4 sont d'ordre 15.

Le polynôme associé à $x^{16} + x$ est $y^4 + 1$, dont la décomposition, mod 2, est :

$$y^4 + 1 \equiv (y + 1)^4 \pmod 2 .$$

L'application de la formule de Möbius donne :

$$\pi(x^{16} + x) = \text{degré}(x^{16} + x) - \text{degré}(x^8 + x) = 16 - 8 = 8 .$$

Il y a 2 bases normales de 4 éléments. Ce sont ceux qui n'annulent pas le p-polynôme à qui est associé :

$$(y + 1)^3 \equiv y^3 + y^2 + y + 1 \pmod 2 ;$$

c'est-à-dire :

$$x^8 + x^4 + x^2 + x \equiv (x^2 + x)(x^2 + x + 1)(x^4 + x + 1) .$$

Ce sont donc les 2 systèmes de 4 éléments qui annulent les 2 polynômes :

$$x^4 + x^3 + 1 , \quad x^4 + x^3 + x^2 + x + 1 .$$

La vérification est immédiate.