Des extensions plus petites que leurs groupes de Galois

Bruno DESCHAMPS

Laboratoire de Mathématiques Nicolas Oresme et Université du Maine

Abstract: In this article we construct some Galois extensions L/K with finite Galois groups and such that $|\mathrm{Gal}(L/K)| > [L : K]$. Using an analog of the Noether method, we explain how to obtain, with a fixed center, such a Galois curiosity with a Galois group as large as we want.

1.— Introduction.

Un des points centraux de la théorie de Galois est que, pour toute extension finie L/K de corps commutatifs, on a toujours l'inégalité $|\mathrm{Aut}(L/K)| \leq [L : K]$ et que le cas d'égalité caractérise le fait que l'extension soit galoisienne. Dans le cas des extensions de corps non commutatifs, ce résultat n'est plus vrai en général : comme nous allons le voir dans les exemples qui suivent, il est en effet facile de construire des extensions galoisiennes de degrés finis et de groupes de Galois infinis.

La notion d'extension galoisienne que nous considérons est la plus générale possible, c'est celle introduite par Artin : une extension L/K est dite *galoisienne*, si le corps des invariants de L sous l'action du groupe $\mathrm{Aut}(L/K)$ est égal au corps K.

Quelques exemples : 1/ Dans le cas commutatif, "être galoisienne" équivaut pour une extension algébrique au fait d'être normale et séparable.

2/ Dans le cas commutatif et transcendant on peut voir par exemple que si k désigne un corps alors l'extension $k(t)/k$ est galoisienne si et seulement si k est infini, son groupe de Galois s'identifiant alors à $\mathrm{PGL}_2(k)$. Dans la même veine, l'extension $k((t))/k$ est toujours galoisienne, quel que soit le corps commutatif k.

Pour l'extension $k(t)/k$, on observe une inversion du caractère galoisien des sous-extensions, par rapport au cas algébrique : le théorème de Lüroth affirmant qu'une extension intermédiaire $k(t)/L/k$ non triviale est de la forme $k(f)$, il s'ensuit que $k(f)/k$ est toujours galoisienne. Pour autant, l'extension $k(t)/k(f)$ l'est assez rarement, car cette extension est finie et qu'il y a peu de sous-groupes finis dans $\mathrm{PGL}_2(k)$.

3/ Dans le cas non-commutatif, pour tout corps K de dimension finie sur son centre C (i.e. K est un corps qui est une algèbre simple centrale), l'extension K/C est galoisienne. En effet, d'après le théorème de Skolem-Noether, le groupe $\mathrm{Aut}(K/C)$ est composé de tous les automorphismes intérieurs de K. Le corps des invariants sous l'action de $\mathrm{Aut}(K/C)$ est donc le centre de K et donc K/C est bien galoisienne. On voit que dans cette situation $\mathrm{Gal}(K/C) = \{I(a)/\ a \in K\} \simeq K^*/C^*$ (où $I(a)$ désigne l'automorphisme intérieur associé à l'élément a) et donc que ce groupe est infini dès que $K \neq C$.

L'objectif de cet article est de donner un exemple d'extension galoisienne à groupe de Galois fini et tel que $|\mathrm{Gal}(L/K)| > [L : K]$. Pour permettre au lecteur non familiarisé à la théorie des corps gauches de comprendre la suite de ce texte, nous allons rappeler dans cette introduction les éléments de cette théorie que nous allons utiliser. Pour le détail des propriétés, nous renvoyons à [Jac] et [Coh].

Dans le cas non commutatif, la notion de groupe de Galois est reliée à celle de N-groupe : si L est un corps de centre C, on dit d'un groupe d'automorphismes G de L que c'est un N-groupe si

[0]2010 Mathematics Subject Classification 12E15, 12F10

l'ensemble $A = \{a \in L^* / I(a) \in G\} \cup \{0\}$ est un corps. Le groupe de Galois d'une extension galoisienne L/K est toujours un N-groupe, le corps A associé étant juste le centralisateur du corps K dans L. On a réciproquement la proposition suivante, qui constitue une généralisation du théorème d'Artin :

Soient G un N-groupe d'automorphismes de L, $G_0 = \{I(a)/ a \in A\}$ le sous-groupe de G composé des automorphismes intérieurs et K le corps des invariants de L par G. On a

$$[L:K]_g = [L:K]_d = [G:G_0][A:C]$$

et lorsque ces dimensions sont finies, l'extension est galoisienne et l'on a $\mathrm{Gal}(L/K) = G$.

Ici les degrés $[L:K]_g$ et $[L:K]_d$ désignent les dimensions de L en tant que K-espace vectoriel gauche et droite et quand elles seront égales (ce qui sera toujours le cas pour les extensions galoisiennes) nous le noterons plus simplement $[L:K]$. La quantité $[G:G_0][A:C]$ est appelée "l'ordre réduit" de G. On dit d'une extension galoisienne qu'elle est intérieure (resp. extérieure), si $G = G_0$ (resp. $G_0 = 1$).

Pour construire notre exemple, nous aurons besoin de la notion de *polynômes tordus* due à Ore. Etant donnés un corps k et un automorphisme α de k, l'anneau de polynômes tordus $k[T,\alpha]$ est défini comme l'ensemble des polynômes $T^n a_n + \cdots + T a_1 + a_0$ muni du produit qui vérifie $aT = T\alpha(a)$. Cet anneau possède un corps de fractions, noté $k(T,\alpha)$, et tout élément de ce corps peut s'écrire sous la forme PQ^{-1} où P et Q sont deux polynômes.

2.— Une curiosité galoisienne.

Nous nous intéressons ici au cas où le groupe de Galois est fini.

Théorème.— *Soit L/K une extension galoisienne <u>de groupe de Galois G fini</u>. On a* $[L:K] \le |G|$ *et*

$$[L:K] = |G| \Longleftrightarrow L/K \textit{ extérieure}$$

Si $[L:K] < |G|$ alors le centre C de L est nécessairement un corps fini, disons $C = \mathbb{F}_q$, et il existe un entier $n \ge 2$ tel que

$$n.|G| = \left(\frac{q^n - 1}{q - 1}\right).[L:K]$$

En particulier :

a) Si C est infini, alors L/K est extérieure et $[L:K] = |G|$.

b) Le sous-groupe de G constitué des automorphismes intérieurs est abélien.

Preuve : Soit G_0 le sous-groupe de G composé des automorphismes intérieurs. Posons $A = \{a \in L/ I(a) \in G_0\} \cup \{0\}$, il s'agit d'un sous-corps de L et l'on voit que $G_0 \simeq A^*/C^*$. Puisque G est fini, A^*/C^* l'est aussi et donc, il existe une famille finie $a_1, \cdots, a_n \in L$ telle que

$$A^* = a_1 C^* \sqcup \cdots \sqcup a_n C^*$$

On en déduit que, en tant que C-espace vectoriel, le corps A est la réunion de n droites vectorielles distinctes deux à deux. Si C est infini, ceci n'est possible que si $n = 1$ et l'on a donc $G_0 = 1$, ce qui assure que L/K est extérieure et que $[L:K] = |G|$.

Si $C = \mathbb{F}_q$ alors A est aussi un corps fini et il existe donc un entier $n \ge 1$ tel que $A = \mathbb{F}_{q^n}$. On a alors

$$[L:K] = (G:G_0).[A:C] = (|G|/|G_0|).[\mathbb{F}_{q^n}:\mathbb{F}_q] = |G|\frac{|\mathbb{F}_q^*|}{|\mathbb{F}_{q^n}^*|}.n = |G|\left(\frac{q-1}{q^n-1}\right)n \le |G|$$

On voit alors que, dans cette situation, l'égalité $[L:K]=|G|$ équivaut à $n=1$, c'est-à-dire $A=C$ ou encore $G_0=1$ (i.e. L/K est extérieure). L'égalité $n.|G|=\left(\frac{q^n-1}{q-1}\right).[L:K]$ découle de l'égalité précédente. Le a) est évident et le b) vient du fait que si $G_0\neq 1$, alors G_0 s'identifie à $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$ pour un certain entier $n\geq 2$.

Nous allons maintenant montrer que, pour tout $q=p^h\geq 2$ puissance d'un nombre premier p, et tout entier $n\geq 1$, il existe une extension galoisienne intérieure L/K de groupe de Galois fini G telle que

$$n.|G|=\left(\frac{q^n-1}{q-1}\right).[L:K]$$

Pour cela, considérons $\alpha=f^h$ l'itérée h-ième du frobénius dans $\overline{\mathbb{F}}_q$ et le corps de fractions tordues $K=\overline{\mathbb{F}}_q(T,\alpha)$.

• Le centre C de K est égal à $\mathbb{F}_q$. En effet, $P(T)=T^na_n+\cdots+a_0$ et $Q(T)=T^mb_m+\cdots+b_0$ deux polynômes tordus tels que $R=PQ^{-1}$ soit un élément non nul de C. Par centralité, on a $QR=RQ$, ce qui implique que $PQ=QP$ et, par suite, que $PQ^{-1}=Q^{-1}P$. Ainsi, pour tout $x\in\overline{\mathbb{F}}_q$, $xPQ^{-1}=PQ^{-1}x=Q^{-1}Px$ et donc $PxQ=QxP$.

Le terme de degré $n+m$ de $PxQ-QxP$ vaut $\alpha^m(a_n)\alpha^m(x)b_m-\alpha^n(b_m)\alpha^n(x)a_n=0$. On en déduit que, pour tout $t\in\overline{\mathbb{F}}_q$, on a

$$\alpha^{m-n}(t)=\left(\alpha^m(a_n^{-1})\alpha^n(b_m)\right)t\left(a_nb_m^{-1}\right)=\left(\alpha^m(a_n^{-1})\alpha^n(b_m)a_nb_m^{-1}\right)t$$

Puisque α^{m-n} est un automorphisme de $\overline{\mathbb{F}}_q$, on a alors nécessairement $n=m$ et $\alpha^m(a_m^{-1}b_m)=a_m^{-1}b_m$, ce qui montre qu'il existe $\lambda\in\mathbb{F}_{q^m}^*$ tel que $b_m=\lambda a_m$.

Pour $0\leq d\leq m-1$, le terme de degré $m+d$ de $PxQ-QxP$ vaut

$$\sum_{i+j=m+d}\alpha^j(x)\left[\alpha^j(a_i)b_j-\alpha^j(b_i)a_j\right]=\sum_{j=d}^{m}\alpha^j(x)\left[\alpha^j(a_{m+d-j})b_j-\alpha^j(b_{m+d-j})a_j\right]=0$$

Puisque cette dernière égalité est valable pour tout $x\in\overline{\mathbb{F}}_q$ et que l'automorphisme α est d'ordre infini, le lemme d'indépendance linéaire de Dedekind assure que chaque terme de la somme est nul. En prenant $j=m$, on en déduit que $\alpha^m(a_d)b_m=\alpha^m(b_d)a_m$. Ceci prouve que $b_d=\lambda a_d$ et finalement que $PQ^{-1}=\lambda\in\mathbb{F}_{q^m}$. On vient donc de montrer que $C\subset\overline{\mathbb{F}}_q$, mais les seuls éléments de $\overline{\mathbb{F}}_q$ qui commutent avec T sont les éléments de $\mathbb{F}_q$, ce qui montre finalement que $C=\mathbb{F}_q$.

• Considérons maintenant un entier $n\geq 1$ et posons

$$G_0=\{I(a)/\ a\in\mathbb{F}_{q^n}\}$$

Ce groupe est un N-groupe d'automorphismes de K. En effet, si $R_0\in A^*=\{R\in K/\ I(R)\in G_0\}$ alors il existe $a\in\mathbb{F}_{q^n}$ tel que $I(R_0)=I(a)$ et donc il existe $\lambda\in C=\mathbb{F}_q$ tel que $R_0=\lambda a\in\mathbb{F}_{q^n}$. Ceci montre aussi que le corps A associé au N-groupe G_0 vaut $A=A^*\cup\{0\}=\mathbb{F}_{q^n}$.

Si l'on note D_0 le corps des invariants de K par G_0, d'après la généralisation du théorème d'Artin rappelée dans l'introduction, on peut affirmer que l'extension K/D_0 est galoisienne (intérieure) de groupe de Galois G_0 et que l'on a

$$[K:D_0]=(G_0:G_0)[A:C]=[\mathbb{F}_{q^n}:\mathbb{F}_q]=n$$

Le groupe de Galois G_0 étant isomorphe à A^*/C^*, il eſt cyclique et compte $(q^n-1)/(q-1) > n$ éléments, ce qui donne donc un exemple d'extension galoisienne à groupe fini d'ordre ſtrictement plus grand que le degré de l'extension.

En peut voir qu'en fait

$$D_0 = \overline{\mathbb{F}}_q(T^n, \alpha^n)$$

Il eſt déjà clair que, T^n étant invariant sous l'action de G_0, on a $\overline{\mathbb{F}}_q(T^n, \alpha^n) \subset D_0$. Pour voir l'inclusion réciproque, établissons préalablement un lemme :

Lemme.— *Pour tout polynôme $P \in \overline{\mathbb{F}}_q[T, \alpha]$ de degré m, il exiſte un polynôme $P_0 \in \overline{\mathbb{F}}_q[T, \alpha]$ non nul de degré $h \leq (n-1)m$ tel que $P(T)P_0(T) \in \overline{\mathbb{F}}_q[T^n, \alpha^n]$.*

Preuve : Posons formellement

$$\begin{aligned} P(T) &= T^m a_m + \cdots + a_0 \\ P_0(T) &= T^h b_h + \cdots + b_0 \end{aligned}$$

où $h = (n-1)m$. On a alors

$$P(T)P_0(T) = \sum_{d=0}^{nm} T^d \left(\sum_{i=0}^{d} \alpha^i (a_{d-j}) b_j \right)$$

Pour tout $d = 0, \cdots, nm$, considérons l'équation

$$(E_d) \qquad \sum_{i=0}^{d} \alpha^i (a_{d-j}) x_j = 0$$

Le polynôme $P_0(T)$ vérifie le lemme si et seulement si le $(h+1)$-uplet $(b_0, \cdots, b_h)$ eſt solution du syſtème d'équations $\{(E_d)\}_{0 \leq d \leq nm,\ n \nmid d}$. Ce syſtème eſt un syſtème linéaire de $nm+1-(m+1) = (n-1)m = h$ équations à $h+1$ indéterminées $b_0, \cdots, b_h$, il possède donc une solution non triviale, ce qui achève la preuve.

———

Considérons maintenant une fraction $R(T) = P(T)Q(T)^{-1} \in \overline{\mathbb{F}}_q(T, \alpha)$ et, grâce au lemme, prenons $Q_0 \in \overline{\mathbb{F}}_q[T, \alpha]$ tel que $Q(T)Q_0(T) = H(T^n)$ pour un certain $H \in \overline{\mathbb{F}}_q[T, \alpha]$. On a alors

$$P(T)Q(T)^{-1} = P(T)Q_0(T)Q_0(T)^{-1}Q(T)^{-1} = P(T)Q_0(T)(Q(T)Q_0(T))^{-1} = A(T)H(T^n)^{-1}$$

avec $A(T) = P(T)Q_0(T) \in \overline{\mathbb{F}}_q[T, \alpha]$. On a alors $R(T) \in D_0 \iff A(T) \in D_0$, mais il eſt très facile de voir que $A(T) \in D_0$ si et seulement si $A(T) \in \overline{\mathbb{F}}_q[T^n, \alpha]$, ce qui prouve finalement que $D_0 \subset \overline{\mathbb{F}}_q(T^n, \alpha^n)$.

Analogue commutatif.— On considère maintenant l'automorphisme trivial $\alpha = Id$, si bien que $\overline{\mathbb{F}}_q(T, \alpha)$ s'identifie au corps commutatif classique $\overline{\mathbb{F}}_q(T)$ des fractions rationnelles à coefficients dans $\overline{\mathbb{F}}_q$. On suppose ici que $(n, q) = 1$, l'extension $\overline{\mathbb{F}}_q(T)/\overline{\mathbb{F}}_q(T^n)$ étant alors galoisienne de groupe $\mu_n(\overline{\mathbb{F}}_q) \subset \mathbb{F}_{q^{\varphi(n)}}$.

On voit alors que dans les deux situations $\alpha = Id, f^h$, les éléments σ du groupe de Galois de l'extension de degré n, $\overline{\mathbb{F}}_q(T, \alpha)/\overline{\mathbb{F}}_q(T^n, \alpha^n)$, sont entièrement déterminés par les formules

$$\begin{aligned} &\sigma(T) = Ta \\ &\sigma(x) = x \text{ pour tout } x \in \overline{\mathbb{F}}_q \end{aligned}$$

avec

- si $\alpha = Id$, $a \in \mu_n(\overline{\mathbb{F}}_q)$,

• si $\alpha = f^h$, $a \in \mathbb{F}_{q^n}^*/\mathbb{F}_q^*$.

Ainsi, "tordre" l'extension usuelle $\overline{\mathbb{F}}_q(T)/\overline{\mathbb{F}}_q(T^n)$ par le frobenius ne change pas son degré mais fait grossir son groupe de Galois!

Treillis des sous-extensions : Dans la théorie de Galois des corps gauches, le théorème des correspondances galoisiennes reste valable sous la forme suivante : *si L/k est une extension galoisienne de degré fini, les correspondances galoisiennes établissent des bijections réciproques l'une de l'autre entre les corps intermédiaires de l'extension L/k et les sous-N-groupes du groupe* $\mathrm{Gal}(L/k)$ (voir [Coh, Th.3.3.11.]).

Si l'on veut décrire le treillis des extensions intermédiaires de $\overline{\mathbb{F}}_q(T,\alpha)/\overline{\mathbb{F}}_q(T^n,\alpha^n)$ il faut donc décrire les sous-N-groupes de G_0. Si H est un sous-N-groupe, alors son corps associé A_H est un sous-corps de $\mathbb{F}_{q^n}$ et il est donc de la forme $\mathbb{F}_{q^d}$. Réciproquement, pour tout $d|n$, le sous-groupe $H_d = \{I(a)/\ a \in \mathbb{F}_{q^d}\}$ est un N-groupe dont le corps associé vaut $\mathbb{F}_{q^d}$. On en déduit que la l'ensemble des sous-N-groupes de G_0 est $\{H_d\}_{d|n}$. Pour $d|n$ donné, le corps des invariants $\overline{\mathbb{F}}_q(T,\alpha)$ par l'action de H_d est $\overline{\mathbb{F}}_q(T^d,\alpha^d)$ (même preuve que précédemment).

En conclusion, même si $\overline{\mathbb{F}}_q(T,\alpha)/\overline{\mathbb{F}}_q(T^n,\alpha^n)$ voit son groupe de Galois plus gros que son analogue commutatif $\overline{\mathbb{F}}_q(T)/\overline{\mathbb{F}}_q(T^n)$, on vient de montrer que, tout comme leur degré, les treillis de leurs extensions intermédiaires sont similairement les mêmes.

3.— Application de la méthode de Noether dans le cas non-commutatif.

Dans la formule du théorème l'entier $\left(\frac{q^n-1}{q-1}\right)$ représente l'ordre du sous-groupe des automorphismes intérieurs. Dans l'exemple $\overline{\mathbb{F}}_q(T)/\overline{\mathbb{F}}_q(T^n)$, puisque l'extension est intérieure, on a

$$\begin{array}{rcl} |G| & = & \left(\dfrac{q^n-1}{q-1}\right) \\ [L:K] & = & n \end{array}$$

On va maintenant montrer comment, à q et n fixés, on peut faire "grossir" arbitrairement G (et donc $[L:K]$) en "rajoutant" des automorphismes extérieurs. Nous allons utiliser un analogue non commutatif de la méthode de Noether : considérons un groupe Γ d'ordre m, plongé dans S_m. On définit alors la suite de corps

$$\begin{array}{rcl} K_1 & = & \overline{\mathbb{F}}_q(X_1,\alpha) \\ K_2 & = & K_1(X_2, I(X_1^{-1})) \\ K_3 & = & K_2(X_3, I(X_2^{-1})) \\ & \vdots & \end{array}$$

et l'on pose $\overline{\mathbb{F}}_q(X_1,\cdots,X_m,\alpha) = K_{m-1}(X_m, I(X_{m-1}^{-1}))$.

Un petit calcul sans difficulté montre que, dans $\overline{\mathbb{F}}_q(X_1,\cdots,X_m,\alpha)$, l'on a $X_iX_j = X_jX_i$ et que, pour tout (i,j) et pour tout $a \in k$, l'on a

$$aX_m^{k_m}\cdots X_1^{k_1} = X_m^{k_m}\cdots X_1^{k_1}\alpha^{k_m+\cdots+k_1}(a)$$

si bien que, les éléments de $\overline{\mathbb{F}}_q(X_1,\cdots,X_m,\alpha)$ peuvent être écrits comme des rapports de polynômes

$$\left(\sum X_m^{k_m}\cdots X_1^{k_1}\lambda_{k_m,\cdots,k_1}\right)\left(\sum X_m^{k_m}\cdots X_1^{k_1}\mu_{k_m,\cdots,k_1}\right)^{-1}$$

Cette propriété s'établit sans peine par récurrence sur l'entier m.

On voit alors que, pour toute permutation $\sigma \in S_m$, on a

$$\overline{\mathbb{F}}_q(X_{\sigma(1)}, \cdots, X_{\sigma(m)}, \alpha) = \overline{\mathbb{F}}_q(X_1, \cdots, X_m, \alpha)$$

où $\overline{\mathbb{F}}_q(X_{\sigma(1)}, \cdots, X_{\sigma(m)}, \alpha)$ est obtenu par la construction précédente en permutant les variables. Ceci montre que le groupe S_m agît fidèlement sur $\overline{\mathbb{F}}_q(X_1, \cdots, X_m, \alpha)$ par permutation des variables.

Le centre de $\overline{\mathbb{F}}_q(X_1, \cdots, X_m, \alpha)$ est contenu dans celui de $\overline{\mathbb{F}}_q(X_1, \alpha)$, il est donc égal à $\mathbb{F}_q$. Comme précédemment, on en déduit que le groupe $G_0 = \{I(a)/\ a \in \mathbb{F}^*_{q^n}\}$ est un N-groupe et que son corps associé est $A = \mathbb{F}_{q^n}$.

Aucun élément non trivial de S_m n'est intérieur. En effet, considérons σ est une permutation non triviale, disons par exemple $\sigma(X_1) = X_2$. S'il existait $R \in L$ telle que $\sigma(X_1) = I(R)(X_1)$ on aurait $X_1 R = R X_2$. On peut considérer R comme une fraction rationnelle de la variable X_1 et à coefficients dans $\overline{\mathbb{F}}_q(X_2, \cdots, X_m, \alpha)$, et donc, on aurait

$$d^\circ_{X_1}(R) + 1 = d^\circ_{X_1}(X_1 R) = d^\circ_{X_1}(R X_2) = d^\circ_{X_1} R$$

ce qui est absurde. Ceci montre que S_m (et donc Γ) est un N-groupe dont le corps associé est $\mathbb{F}_q$.

Puisque S_m agît trivialement sur $\overline{\mathbb{F}}_q$, on voit que les éléments de S_m et de G_0 commutent deux à deux, si bien que, le sous-groupe G de $\mathrm{Aut}(\overline{\mathbb{F}}_q(X_1, \cdots, X_m, \alpha))$ engendré par $\Gamma \subset S_m$ et G_0 s'identifie au produit direct $G = \Gamma \times G_0$. Il s'agit d'un N-groupe dont le sous-groupe d'automorphismes intérieurs vaut G_0 et le corps associé reste $A = \mathbb{F}_{q^n}$.

Si l'on note K le corps des invariants de $\overline{\mathbb{F}}_q(X_1, \cdots, X_m, \alpha)$ par l'action de G, alors $\overline{\mathbb{F}}_q(X_1, \cdots, X_m, \alpha)/K$ est galoisienne de groupe G et l'on a

$$\begin{array}{rcl} |G| & = & \left(\dfrac{q^n - 1}{q - 1}\right).m \\ {[\overline{\mathbb{F}}_q(X_1, \cdots, X_m, \alpha) : K]} & = & n.m \end{array}$$

En application des éléments de théorie de Galois rappelés plus haut, l'extension se décompose de la manière suivante :

$$\begin{tikzcd}
& \overline{\mathbb{F}}_q(X_1, \cdots, X_m, \alpha) \arrow[dl, dash, "G_0"', "n"] \arrow[dr, dash, "m", "\Gamma"'] \arrow[dd, dash, bend left=80, "nm"', "G=G_0\times\Gamma"] & \\
L \arrow[dr, dash, "\Gamma"', "m"] & & \Omega \arrow[dl, dash, "G_0"', "n"] \\
& K &
\end{tikzcd}$$

Le sous-corps L est composé des fractions

$$\left(\sum X_m^{k_m} \cdots X_1^{k_1} \lambda_{k_m, \cdots, k_1}\right)\left(\sum X_m^{k_m} \cdots X_1^{k_1} \mu_{k_m, \cdots, k_1}\right)^{-1}$$

où chaque monôme $X_m^{k_m} \cdots X_1^{k_1}$ est de degré total $k_1 + \cdots + k_m$ un multiple de l'entier n.

Bibliographie

[Coh] P.M. Cohn, *Skew fields - Theory of general division rings*, Encyclopedia of Mathematics and its applications Vol. 57, Cambridge University Press (1995).

[Jac] N. Jacobson, *Structure of rings*, AMS Colloquium Publications Vol. 37 (1956).

Bruno Deschamps :

Laboratoire de Mathématiques Nicolas Oresme (CNRS UMR 6139)
Université de Caen Normandie BP 5186
14032 Caen Cedex

Département de Mathématiques
Université du Maine
Avenue Olivier Messiaen, 72085 Le Mans cedex 9

E-mail : Bruno.Deschamps@univ-lemans.fr