Des extensions galoisiennes à groupes de Galois d'ordres plus grands que leurs degrés

Etant donnée une extension finie L/K de corps commutatifs, il est bien connu que l'on a toujours $|\mathrm{Aut}_K(L)| \leq [L:K]$ et qu'il y a égalité si et seulement si l'extension L/K est galoisienne. Dans le cas non commutatif ce résultat n'est plus vrai en général. Nous allons donné ici des exemples de situations où $|\mathrm{Gal}(L/K)| > [L:K]$. Pour le lecteur non familisarisé avec la théorie des corps gauches, nous rappellerons en *italique* les éléments importants de la théorie nécessaires à la bonne compréhension du texte.

(La notion d'extension galoisienne en toutes généralités est à considérer du point de vue artinien : une extension L/K sera dite galoisienne si le corps des invariants de L par le groupe $\mathrm{Aut}_K(L)$ est égal au corps K. 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'automorphisme G de L que c'est un N-groupe si l'ensemble $A = \{a \in L^* / \ I(a) \in G\} \cup \{0\}$ est un corps (ici $I(a)$ désigne l'automorphisme intérieur de L associé à l'élément a). Le groupe de Galois d'une extension galoisienne L/K est un N-groupe, le corps A associé étant juste le centralisateur du corps K dans L. On a réciproquement la proposition suivante, qui constitue un analogue du théorème d'Artin : soit 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

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

(les degrés désignent les dimensions de L en tant que K-e.v gauche et droite) et lorsque ces dimensions sont finies, on a $\mathrm{Gal}(L/K) = G$. 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. $G_0 = 1$).)

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

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

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 $n \geq 2$ 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 $n \geq 1$ tel que $A = \mathbb{F}_{q^n}$. On a alors

$$[L : K] = (G : G_0).[A : C] = (|G|/|G_0|).[\mathbb{F}_{p^n} : \mathbb{F}_p] = |G|\frac{q-1}{q^n-1}.n \leq |G|$$

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 $n \geq 2$.

———

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

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

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

(Etant donné un corps k et un automorphisme α de k, l'anneau de polynômes tordus $k[T, \alpha]$ est défini comme l'ensemble des polynômes $T^n a_n + \cdots + a_0$ muni du produit qui vérifie $aT = T\alpha(a)$. Cet anneau possède un corps de fractions : $k(T, \alpha)$. Tout élément de ce corps peut s'écrire sous la forme PQ^{-1} où P et Q sont deux polynômes.)

Le centre C de K est égal à $\mathbb{F}_q$: considérons $R = PQ^{-1}$ un élément non nul de C avec P et Q des polynômes. Par centralité, on a $QR = RQ$, ce qui implique que $PQ = QP$ et, par suite, que $PQ^{-1} = Q^{-1}P$. On a donc, pour tout $x \in \overline{\mathbb{F}}_q$, $xPQ^{-1} = PQ^{-1}x = Q^{-1}Px$ et donc $PxQ = QxP$. Si $P(T) = T^n a_n + \cdots + a_0$ et $Q(T) = T^m b_m + \cdots + b_0$, on voit alors en regardant le terme de degré $n + m$ des produits que $\alpha^m(a_n)\alpha^m(x)b_m = \alpha^n(b_m)\alpha^n(x)a_n$. On en déduit que, pour tout $t \in \overline{\mathbb{F}}_q$, on a

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

Ainsi, α^{m-n} est un automorphisme intérieur et $\alpha^m(a_n^{-1})\alpha^n(b_m) = b_m a_n^{-1}$. Puisque α est d'ordre infini et que $\overline{\mathbb{F}}_q$ est commutatif, aucune des puissances non nulles de α n'est intérieure. On en déduit donc que $n = m$ et 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

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

Le lemme de Dedekind assure alors que chaque terme de cette somme est nul et donc, 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 $\mathbb{F}_q$, ceci 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, l'extension K/D_0 est galoisienne (intérieure) de groupe de Galois G_0 et 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 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

$$P(T) = T^m a_m + \cdots + a_0$$
$$P_0(T) = T^h b_h + \cdots + b_0$$

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 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 $\overline{\mathbb{F}}_q(T)/\overline{\mathbb{F}}_q(T^n)$ est 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 donnés par les formules

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

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.

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 notre exemple l'extension étant intérieure, on a

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

On peut faire "grossir" G (et donc $[L:K]$) en "rajoutant" des automorphismes extérieurs. Ceci peut être fait de manière arbitraire en utilisant un analogue non commutatif de la méthode de Noether : considérons un groupe Γ d'ordre m, regardé comme étant plongé dans S_m. On définit alors les corps

$K_1 = \overline{\mathbb{F}}_q(X_1, \alpha)$
$K_2 = K_1(X_2, I(X_1))$
$K_3 = K_2(X_3, I(X_2^{-1}))$
$\cdots$
$\overline{\mathbb{F}}_q(X_1, \cdots, X_m, \alpha) = K_{m-1}(X_m, I(X_{m-1}^{(-1)^m}))$

Les éléments de $L = \overline{\mathbb{F}}_q(X_1, \cdots, X_m, \alpha)$ sont des rapports de polynômes

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

Dans L, on a $X_i X_j = X_j X_i$ pour tout (i,j) et, pour tout $a \in k$, on a

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

Le groupe symétrique S_m agît sur $\overline{\mathbb{F}}_q(X_1, \cdots, X_m, \alpha)$ par permutation des variables. En effet, si $\sigma \in S_m$, alors on a

$$\begin{array}{rcl} \sigma(X_m^{k_m} \cdots X_1^{k_1} a. X_m^{l_m} \cdots X_1^{l_1} b) & = & \sigma(X_m^{k_m+l_m} \cdots X_1^{k_1+l_1} \alpha^{l_1+\cdots+l_m}(a) b) \\ & = & X_{\sigma(m)}^{k_m+l_m} \cdots X_{\sigma(1)}^{k_1+l_1} \alpha^{l_1+\cdots+l_m}(a) b \\ & = & X_m^{k_{\sigma^{-1}(m)}+l_{\sigma^{-1}(m)}} \cdots X_1^{k_{\sigma^{-1}(1)}+l_{\sigma^{-1}(1)}} \alpha^{l_{\sigma^{-1}(1)}+\cdots+l_{\sigma^{-1}(m)}}(a) b \\ & = & X_m^{k_{\sigma^{-1}(m)}} \cdots X_1^{k_{\sigma^{-1}(1)}} a X_m^{l_{\sigma^{-1}(m)}} \cdots X_1^{l_{\sigma^{-1}(1)}} b \\ & = & \sigma(X_m^{k_m} \cdots X_1^{k_1} a).\sigma(X_m^{l_m} \cdots X_1^{l_1} b) \end{array}$$

Puisque σ agît trivialement sur $\overline{\mathbb{F}}_q$, on voit que σ commute avec $I(a)$ pour tout $a \in \mathbb{F}_{q^n}^*$, si bien que le groupe d'automorphismes engendré par Γ et $G_0 = \{I(a)/\ a \in \mathbb{F}_{q^n}^*\}$ s'identifie à $G = \Gamma \times G_0$.

Maintenant, aucun élément non trivial de Γ 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.

Comme dans l'exemple précédent, on voit que G est un N-groupe fini et, si l'on note K le corps des invariants de L par l'action de G, alors L/K est galoisienne de groupe G. Le centre de L est égal à $\mathbb{F}_q$ (puisque le centre de K_1 est déjà égal $\mathbb{F}_q$). En reprenant le même argument que précédemment, on en déduit que

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