Détermination d'un élément primitif de l'extension $\mathbf{F}_q(T)^{Aut_{F_q}(\mathbf{F}_q(T))}/\mathbf{F}_q$

Bruno DESCHAMPS — Université de Saint-Etienne

Abstract: *In this article, we determine the minimal polynomial of T over $\mathbf{F}_q(T)^{Aut_{\mathbf{F}_q}(\mathbf{F}_q(T))}$ and give explicitely an element $Y(T) \in \mathbf{F}_q(T)$ such that $\mathbf{F}_q(T)^{Aut_{\mathbf{F}_q}(\mathbf{F}_q(T))} = \mathbf{F}_q(Y(T))$.*

Si K désigne un corps et $K(T)$ son corps de fractions rationnelles, il est célèbre que le groupe $Aut_K(K(T))$ est isomorphe au groupe $PGL_2(K)$ (voir Bourbaki, Algèbre, ch. V, ex. 5, page 105), l'isomorphisme étant donné par :

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in PGL_2(K) \longmapsto T \mapsto \frac{aT+b}{cT+d}$$

Si K est un corps infini, il est facile de voir que le corps des invariants, $K(T)^{Aut_K(K(T))}$, de $K(T)$ sous l'action de $Aut_K(K(T))$ est égal à K. Si K est fini, il n'en est rien. Si l'on pose $L = \mathbf{F}_q(T)^{Aut_{\mathbf{F}_q}(\mathbf{F}_q(T))}$ (ou q désigne la puissance d'un nombre premier), le théorème d'Artin assure que l'extension $\mathbf{F}_q(T)/L$ est galoisienne de degré $\sharp PGL_2(\mathbf{F}_q) = q^3 - q$. Le théorème de Lüroth assure alors qu'il existe un élément $Y(T) \in K(T)$ tel que $L = \mathbf{F}_q(Y(T))$. L'objet de cette note est de déterminer explicitement la fraction $Y(T)$ en fonction de q.

L'élément $T \in \mathbf{F}_q(T)$ est un élément primitif de l'extension $\mathbf{F}_q(T)/L$. Le polynôme minimal de T sur L est :

$$\begin{aligned} P(X) &= \prod_{s \in Aut_{\mathbf{F}_q}(\mathbf{F}_q(T))} (X - s(T)) \\ &= \prod_{\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in PGL_2(\mathbf{F}_q)} \left(X - \frac{aT+b}{cT+d}\right) \\ &= \frac{\displaystyle\prod_{a,b,d \in \mathbf{F}_q} \left(X - \frac{aT+b}{T+d}\right) \prod_{a \in \mathbf{F}_q^*,\ b \in \mathbf{F}_q} (X - (aT+b))}{\displaystyle\prod_{a,d \in \mathbf{F}_q} (X-a)} \end{aligned}$$

Dans la suite du calcul de P, on note $\omega = (T^q - T)$. Pour simplifier les expressions, on utilisera les relations :

$$\prod_{\alpha \in \mathbf{F}_q^*} (u - \alpha v) = u^{q-1} - v^{q-1}, \quad \prod_{\alpha \in \mathbf{F}_q} (u - \alpha v) = u\left(u^{q-1} - v^{q-1}\right)$$

On a :

$$\begin{aligned} \prod_{a,d \in \mathbf{F}_q} (X-a) &= \left(\prod_{a \in \mathbf{F}_q} (X-a)\right)^q \\ &= (X^q - X)^q \end{aligned}$$

De même,

$$\begin{aligned}\prod_{a\in\mathbf{F}_q^*,\ b\in\mathbf{F}_q}(X-(aT+b)) &= \prod_{a\in\mathbf{F}_q^*}\prod_{b\in\mathbf{F}_q}((X-aT)-b)\\ &= \prod_{a\in\mathbf{F}_q^*}((X-aT)^q-(X-aT))\\ &= \prod_{a\in\mathbf{F}_q^*}((X^q-X)-a(T^q-T))\\ &= (X^q-X)^{q-1}-\omega^{q-1}\end{aligned}$$

Enfin,

$$\prod_{a,b,d\in\mathbf{F}_q}\left(X-\frac{aT+b}{T+d}\right)=\prod_{a,b,d\in\mathbf{F}_q}\left(X-a-\frac{b-ad}{T+d}\right)$$

$$=\prod_{a,d\in\mathbf{F}_q}\prod_{b\in\mathbf{F}_q}\left(\left(X-a+\frac{ad}{T+d}\right)-\frac{b}{T+d}\right)$$

$$=\prod_{a,d\in\mathbf{F}_q}\frac{1}{(T+d)^q}\prod_{b\in\mathbf{F}_q}(((X-a)(T+d)+ad)-b)$$

$$=\frac{1}{(T^q-T)^{q^2}}\prod_{a,d\in\mathbf{F}_q}\prod_{b\in\mathbf{F}_q}(((X-a)(T+d)+ad)-b)$$

$$=\frac{1}{\omega^{q^2}}\prod_{a,d\in\mathbf{F}_q}\prod_{b\in\mathbf{F}_q}(((X-a)(T+d)+ad)-b)$$

$$= \frac{1}{\omega^{q^2}} \prod_{a,d\in\mathbf{F}_q} (((X-a)(T+d)+ad)^q - ((X-a)(T+d)+ad))$$

$$= \frac{1}{\omega^{q^2}} \prod_{a,d\in\mathbf{F}_q} (((X^q-a)(T^q+d)+ad) - ((X-a)(T+d)+ad))$$

$$= \frac{1}{\omega^{q^2}} \prod_{a,d\in\mathbf{F}_q} (XT)^q - (XT) - a(T^q-T) + d(X^q-X)$$

$$= \prod_{d\in\mathbf{F}_q} \prod_{a\in\mathbf{F}_q} \left(\frac{(XT)^q - (XT) + d(X^q-X)}{\omega} - a \right)$$

$$= \prod_{d\in\mathbf{F}_q} \left[\frac{(XT)^{q^2} - (XT)^q + d(X^q-X)^q}{\omega^q} - \frac{(XT)^q - (XT) + d(X^q-X)}{\omega} \right]$$

$$= \frac{1}{\omega^{q^2}} \prod_{d\in\mathbf{F}_q} \left[(XT)^{q^2} - (XT)^q + d(X^q-X)^q - \omega^{q-1}((XT)^q - (XT) + d(X^q-X)) \right]$$

$$= \frac{1}{\omega^{q^2}} \prod_{d\in\mathbf{F}_q} \left[\left((XT)^{q^2} - (XT)^q - \omega^{q-1}((XT)^q - (XT)) \right) + d(X^q-X)\left((X^q-X)^{q-1} - \omega^{q-1} \right) \right]$$

Posons

$$\begin{cases} P_1(X) &= (XT)^{q^2} - (XT)^q - \omega^{q-1}((XT)^q - (XT)) \\ P_2(X) &= (X^q-X)^{q-1} - \omega^{q-1} \quad \left(= \prod_{a\in\mathbf{F}_q^*,\ b\in\mathbf{F}_q} (X - (aT+b)) \right) \end{cases}$$

On a alors :

$$\prod_{a,b,d\in\mathbf{F}_q} \left(X - \frac{aT+b}{T+d} \right) = \frac{1}{\omega^{q^2}} \prod_{d\in\mathbf{F}_q} P_1(X) + d(X^q-X)P_2(X)$$

$$= \frac{P_1(X)\left(P_1^{q-1}(X) - (X^q-X)^{q-1}P_2^{q-1}(X) \right)}{\omega^{q^2}}$$

De sorte que :

$$P(X) = \frac{P_1^q(X)P_2(X) - (X^q-X)^{q-1}P_2^q(X)P_1(X)}{\omega^{q^2}(X^q-X)^q}$$

$$= \frac{(X^q-X)P_2(X)P_1^q(X) - ((X^q-X)P_2(X))^q P_1(X)}{\omega^{q^2}(X^q-X)^{q+1}}$$

On a

$$\begin{cases} (X^q-X)P_2(X) &= X^{q^2} - (1+\omega^{q-1})X^q + \omega^{q-1}X \\ P_1^q(X) &= T^{q^3}X^{q^3} - T^{q^2}(1+\omega^{q(q-1)})X^{q^2} + \omega^{q(q-1)}T^qX^q \end{cases}$$

et donc $(X^q - X)P_2(X)P_1^q(X) =$

$$\begin{array}{l} T^{q^3}X^{q^3+q^2} - T^{q^3}(1+\omega^{q-1})X^{q^3+q} + \omega^{q-1}T^{q^3}X^{q^3+1} - T^{q^2}(1+\omega^{q(q-1)})X^{2q^2} \\ + \left(\omega^{q(q-1)}T^q + (1+\omega^{q-1})(1+\omega^{q(q-1)})T^{q^2}\right)X^{q^2+q} \\ -\omega^{q-1}(1+\omega^{q(q-1)})T^{q^2}X^{q^2+1} - \omega^{q(q-1)}(1+\omega^{q-1})T^qX^{2p} + \omega^{q^2-1}T^qX^{q+1} \end{array}$$

De même, on a :

$$\left\{\begin{array}{rcl} ((X^q - X)P_2(X))^q & = & X^{q^3} - (1+\omega^{q(q-1)})X^{q^2} + \omega^{q(q-1)}X^q \\ P_1(X) & = & T^{q^2}X^{q^2} - T^q(1+\omega^{q-1})X^q + \omega^{q-1}TX \end{array}\right.$$

et donc $((X^q - X)P_2(X))^q P_1(X) =$

$$\begin{array}{l} T^{q^2}X^{q^3+q^2} - T^q(1+\omega^{q-1})X^{q^3+q} + \omega^{q-1}TX^{q^3+1} - T^{q^2}(1+\omega^{q(q-1)})X^{2q^2} \\ + \left(\omega^{q(q-1)}T^{q^2} + (1+\omega^{q-1})(1+\omega^{q(q-1)})T^p\right)X^{q^2+q} \\ -\omega^{q-1}(1+\omega^{q(q-1)})TX^{q^2+1} - \omega^{q(q-1)}(1+\omega^{q-1})T^qX^{2p} + \omega^{q^2-1}TX^{q+1} \end{array}$$

On en déduit que $\omega^{q^2}(X^q - X)^{q+1}P(X) =$

$$\begin{array}{l} (T^{q^3} - T^{q^2})X^{q^3+q^2} - (T^{q^3} - T^q)(1+\omega^{q-1})X^{q^3+q} + (T^{q^3} - T)\omega^{q-1}X^{q^3+1} \\ + \left(\omega^{q(q-1)}(T^q - T^{q^2}) + (1+\omega^{q-1})(1+\omega^{q(q-1)})(T^{q^2} - T^q)\right)X^{q^2+q} \\ -\omega^{q-1}(1+\omega^{q(q-1)})(T^{q^2} - T)X^{q^2+1} + \omega^{q^2-1}(T^q - T)X^{q+1} \end{array}$$

c'est-à-dire $\omega^{q^2}(X^q - X)^{q+1}P(X) =$

$$\begin{array}{l} \omega^{q^2}X^{q^3+q^2} - (\omega^q + \omega^{q^2})(1+\omega^{q-1})X^{q^3+q} + \omega^{q-1}(\omega + \omega^q + \omega^{q^2})X^{q^3+1} \\ + \left(-\omega^{q^2} + \omega^q(1+\omega^{q-1})(1+\omega^{q(q-1)})\right)X^{q^2+q} \\ -\omega^{q-1}(1+\omega^{q(q-1)})(\omega + \omega^q)X^{q^2+1} + \omega^{q^2}X^{q+1} \end{array}$$

En posant

$$\begin{array}{rcl} \alpha(\omega) & = & (\omega^q + \omega^{q^2})(1+\omega^{q-1}) \\ & = & \omega^q(1+\omega^{q(q-1)})(1+\omega^{q-1}) \end{array}$$

et

$$\begin{array}{rcl} \beta(\omega) & = & \alpha(\omega) - \omega^{q^2} \\ & = & -\omega^{q^2} + \omega^q(1+\omega^{q(q-1)})(1+\omega^{q-1}) \\ & = & \omega^q(1+\omega^{q-1}+\omega^{q^2-1}) \end{array}$$

on a :

$$\begin{array}{l} \omega^{q^2}(X^q - X)^{q+1}P(X) = \omega^{q^2}\left(X^{q^3+q^2} + X^{q+1}\right) \\ -\alpha(\omega)\left(X^{q^3+q} + X^{q^2+1}\right) + \beta(\omega)\left(X^{q^3+1} + X^{q^2+q}\right) \end{array}$$

c'est-à-dire

$$\begin{array}{rcl} P(X) & = & \dfrac{\left(X^{q^3+q^2} + X^{q+1} - X^{q^3+q} - X^{q^2+1}\right)}{(X^q - X)^{q+1}} \\ & & + \dfrac{\beta(\omega)}{\omega^{q^2}}\dfrac{\left(X^{q^3+1} + X^{q^2+q} - X^{q^3+q} - X^{q^2+1}\right)}{(X^q - X)^{q+1}} \\ & = & \dfrac{(X^{q^2} - X^q)(X^{q^3} - X)}{(X^q - X)^{q+1}} \\ & & - \dfrac{\beta(\omega)}{\omega^{q^2}}\dfrac{(X^q - X)(X^{q^3} - X^{q^2})}{(X^q - X)^{q+1}} \end{array}$$

On obtient, pour finir

$$P(X) = (X^q - X)^{q^2-1} - \frac{\beta(\omega)}{\omega^{q^2}}(X^q - X)^{q^2-q} + (X^q - X)^{q-1} + 1$$

Comme $P(X) \in L[X]$, on a $\frac{\beta(\omega)}{\omega^{q^2}} \in L$ et donc $\mathbf{F}_q\left(\frac{\beta(\omega)}{\omega^{q^2}}\right) \subset L$. Par ailleurs, l'écriture de P assure que $P(X) \in \mathbf{F}_q\left(\frac{\beta(\omega)}{\omega^{q^2}}\right)[X]$ qui est alors un polynôme irréductible. Comme T est racine de P, le corps de rupture de P sur $\mathbf{F}_q\left(\frac{\beta(\omega)}{\omega^{q^2}}\right)$ est $\mathbf{F}_q(T)$ ce qui assure, pour des raisons de degrés, que $L = \mathbf{F}_q\left(\frac{\beta(\omega)}{\omega^{q^2}}\right)$. On en déduit donc que $\mathbf{F}_q(T)^{Aut_{\mathbf{F}_q}(\mathbf{F}_q(T))} = \mathbf{F}_q(Y(T))$ avec

$$Y(T) = \frac{\left(T^{q^3} - T\right)\left(T^{q^2} - T^q\right)}{(T^q - T)(T^{q^3} - T^{q^2})}$$

Les racines dans $\overline{\mathbf{F}}_q$ de $(T^{q^3} - T)$ sont simples (ce sont les éléments de $\mathbf{F}_{q^3}$), on en déduit donc la forme irréductible de $Y(T)$ suivante :

$$Y(T) = \frac{(T^{q^3} - T)/(T^q - T)}{(T^q - T)^{q^2-q}} = \frac{\sum_{i=0}^{q^2+q}\left(T^{q-1}\right)^i}{(T^q - T)^{q^2-q}}$$

Remarque : Une fois l'écriture de $Y(T)$ donnée, on peut trés facilement retrouver le fait que $\mathbf{F}_q(T)^{Aut_{\mathbf{F}_q}(\mathbf{F}_q(T))} = \mathbf{F}_q(Y(T))$. En effet, l'élément $Y(T)$ est invariant sous l'action de $PGL_2(\mathbf{F}_q)$: si $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in PGL_2(\mathbf{F}_q)$, on a

$$\begin{aligned}
Y\left(\frac{aT+b}{cT+d}\right) &= \frac{\left(\frac{aT+b}{cT+d}\right)^{q^3} - \left(\frac{aT+b}{cT+d}\right)}{\left(\left(\frac{aT+b}{cT+d}\right)^q - \left(\frac{aT+b}{cT+d}\right)\right)^{q^2-q+1}} \\
&= \frac{\frac{(aT^{q^3}+b)(cT+d) - (aT+b)(cT^{q^3}+d)}{(cT+d)^{q^3+1}}}{\frac{((aT^q+b)(cT+d) - (aT+b)(cT^q+d))^{q^2-q+1}}{(cT+d)^{(q^2-q+1)(q+1)}}} \\
&= \frac{(ad-bc)(T^{q^3} - T)}{(ad-bc)^{q^2-q+1}(T^q - T)^{q^2-q+1}} \\
&= Y(T)
\end{aligned}$$

Par ailleurs, si K désigne un corps et $f(T) = \frac{P(T)}{Q(T)} \in K(T)$ est écrite sous forme irréductible, alors le degré de l'extension $K(T)/K(f(T))$ est égale à la hauteur $h(f) = Max(d^\circ P, d^\circ Q)$ (voir Bourbaki, Algèbre, ch. V, ex. 5, page 105). Comme ici, $h(Y) = q^3 - q$, on en déduit bien que $\mathbf{F}_q(T)^{Aut_{\mathbf{F}_q}(\mathbf{F}_q(T))} = \mathbf{F}_q(Y(T))$.

Bruno Deschamps, Equipe de théorie des nombres, Faculté des sciences et techniques, Université Jean Monnet, 23 rue du docteur Paul Michelon, 42023 Saint-Etienne, Cedex 2, France.
E-mail: Bruno.Deschamps@univ-st-etienne.fr