ANNALES DE L'INSTITUT FOURIER

P. RIVOIRE

Fonctions rationnelles sur un corps fini

Annales de l'institut Fourier, tome 6 (1956), p. 121-124

<http://www.numdam.org/item?id=AIF_1956__6__121_0>

FONCTIONS RATIONNELLES SUR UN CORPS FINI

par Paul **RIVOIRE**

I. — GÉNÉRALITÉS

Etant donnés un corps de base K, et son corps des fractions rationnelles à une indéterminée K(X), rappelons qu'un K-automorphisme s de K(X) est bien déterminé par la fraction rationnelle $s(X)$; celle-ci est nécessairement de la forme $\frac{aX+b}{cX+d}(ad-bc\neq 0)$.

Une telle propriété permet de caractériser le groupe G des K-automorphismes de K(X) comme groupe des homographies régulières $X\to\frac{aX+b}{cX+d}$, a, b, c, d étant des éléments de K tels que $ad-bc\neq 0$. (c. f. Van der Waerden, Moderne Algebra, § 63).

— Si K est infini, le corps des invariants K_G de K(X) par le groupe G est évidemment réduit à K.

— Si K est fini, donc nécessairement de caractéristique $p>0$, G est fini, donc K_G contient des fractions rationnelles non constantes, et le théorème de Lüroth montre d'ailleurs que c'est une extension transcendante pure de K.

Dans ces conditions, il est possible d'appliquer les résultats de la théorie classique de Galois — extensions galoisiennes de degré fini — à l'étude de G et de ses sous-groupes. On rappelle que G est isomorphe au groupe projectif des matrices carrées régulières d'ordre 2, à éléments sur K. Il est d'ordre q^3-q, q désignant le nombre d'éléments de $K=F_q$.

II. — CORPS DES INVARIANTS DE G

Le transformé de $X^q - X$ par $s = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est :

$$(ad - bc)\frac{X^q - X}{(cX+d)^{q+1}}.$$

Celui de $X^{q^2} - X$ est : $(ad-bc)\dfrac{X^{q^2}-X}{(cX+d)^{q^2+1}}$. Cela montre que la fraction rationnelle $I(X) = \dfrac{(X^{q^2}-X)^{q+1}}{(X^q - X)^{q^2+1}}$ est invariante par s. Cette fraction, que nous pouvons mettre sous la forme : $I(X) = \dfrac{\left[\sum_0^q X^{(q-1)(q-j)}\right]^{q+1}}{(X^q-X)^{q^2-q}}$, est de hauteur inférieure à $q^3 - q$.

Puisque $I(X)$ est invariante par s, $K(I)$ est contenu dans K_G : $(K(I) \subset K_G \subset K(X))$, et l'inégalité $(K(X)/K(I)) \leqslant q^3 - q$ implique:

$$(K_G/K(I)) \leqslant 1,$$

puisque $(K(X)/K_G) = q^3 - q$.

On en conclut alors que $K_G = K(I)$, i. e. :

$$\boxed{K_G = F_q\left(\frac{(X^{q^2}-X)^{q+1}}{(X^q-X)^{q^2+1}}\right).}$$

III. — SOUS-GROUPE DE G. CORPS DES INVARIANTS CORRESPONDANTS

Le groupe des « similitudes » H : $X \to aX + b$, est d'ordre $q(q-1)$ et admet, pour corps d'invariants :

$$\boxed{K_H = F_q((X^q - X)^{q-1}).}$$

Le groupe des translations H' : $X \to X + b$, est d'ordre q. C'est un sous-groupe distingué de H, et son corps des invariants

$$\boxed{K_{H'} = F_q(X^q - X)}$$

est une extension galoisienne (même cyclique) de K_H.

Le groupe des homothéties $H_1 : X \to aX$, qui est aussi le groupe relatif de $K_{H'}$ sur K_H, est d'ordre $q-1$. Son corps des invariants est évidemment $K_{H_1} = F_q(X^{q-1})$. Rappelons que H est le produit semi-direct de H' par H_1.

Deux sous-groupes conjugués de H, désignés par G_1 et G_2, sont respectivement définis par les conditions

(1) « $a + b = c + d$ »
(2) « $a + c = b + d$ »

En caractérisitique 2, ils sont identiques.

En caractéristique $\neq 2$, leur intersection $G_1 \cap G_2$, d'ordre $q-1$, est l'ensemble des automorphismes $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$. Le corps des invariants de G_1 est :

$$K_{G_1} = F_q\left(\frac{(X-1)^{q(q-1)}}{[(X-1)^{q-1}-1]^{q-1}}\right)$$

Celui de G_2 est :

$$K_{G_2} = F_q\left(\frac{(X+1)^{q(q-1)}}{[(X+1)^{q-1}-1]^{q-1}}\right)$$

Les groupes $H_+ = H \cap G_1$ et $H_- = H \cap G_2$ sont définis par les conditions « dégénérées »

(1') $a + b = 1$
(2') $a - b = 1.$

Ils sont d'ordre $q-1$, et admettent respectivement pour corps d'invariants :

$$K_{H_+} = F_q((X-1)^{q-1}-1) \quad \text{et} \quad K_{H_-} = F_q((X+1)^{q-1}-1)$$

Désignons par Q l'ensemble des carrés de F_q. C'est un sous-groupe multiplicatif de F_q^*, d'indice 2 en caractéristique $p \neq 2$, et s'identifiant à F_q^* en caractéristique 2. Nous supposons, dans ce qui suit, $p \neq 2$.

Le groupe H_Q, ensemble des automorphismes $X \to aX + b$

pour lesquels $a \in Q$, est d'ordre $q(q-1)/2$, et son corps des invariants est :

$$\boxed{K_{H_Q} = F_q\left((X^q - X)^{\frac{q-1}{2}}\right).}$$

C'est une extension cyclique de K_H. Si nous envisageons, de la même manière, les groupes $H_{+,Q} = H_Q \cap G_1$ et $H_{-,Q} = H_Q \cap G_2$, ils sont d'ordre $\frac{q-1}{2}$, distingués relativement à H_+ et H_-, et admettent pour corps d'invariants :

$$\boxed{\begin{aligned} K_{H_{+,Q}} &= F_q((X-1)^{q-1/2} - 1) \\ K_{H_{-,Q}} &= F_q((X+1)^{q-1/2} - 1) \end{aligned}}$$

Le groupe $\mathfrak{G}$, qui se compose de tous les automorphismes pour lesquels $D(s) = 1$, est d'indice 2 en caractéristique $\neq 2$, et s'identifie à G en caractéristique 2.

Rappelons qu'il est simple, sauf si $q = 2$ ou $q = 3$ (cf. E. Dickson, Linear Groups, Leipzig 1901). En caractéristique $\neq 2$, son corps des invariants est une extension cyclique de K_G.