Algebraic Geometry

Birational permutations

Serge Cantat

Département de mathématiques, Université de Rennes, 35042 Rennes, France

Abstract

We prove that every permutation of $\mathbb{P}^n(K)$, where K is a finite field with odd characteristic, is induced by a birational transformation with no rational indeterminacy point. ***To cite this article: S. Cantat, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***
© 2009 Published by Elsevier Masson SAS on behalf of Académie des sciences.

Résumé

Bijections birationnelles. Nous montrons que toute bijection de $\mathbb{P}^n(K)$, pour K un corps fini de caractéristique impaire, est induite par une transformation birationnelle sans point d'indétermination rationnel. ***Pour citer cet article : S. Cantat, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***
© 2009 Published by Elsevier Masson SAS on behalf of Académie des sciences.

Version française abrégée

Soit p un nombre premier. Soit K un corps fini de caractéristique p, et m l'entier positif tel que le cardinal q de K soit égal à p^m. Le groupe de Cremona $\mathsf{Cr}_n(K)$ est le groupe des K-automorphismes du corps $K(x_1, \ldots, x_n)$. Ce groupe coïncide avec le groupe des transformations birationnelles de l'espace projectif $\mathbb{P}^n_K$. Si $f : \mathbb{P}^n_K \dashrightarrow \mathbb{P}^n_K$ est une transformation birationnelle, il existe alors $n + 1$ polynômes homogènes $P_i(x_0, \ldots, x_n)$ de même degré d et sans facteur commun tels que $f[x_0, \ldots, x_n] = [P_0 : \cdots : P_n]$. Le lieu d'indétermination $\mathrm{Ind}(f)$ de f est l'ensemble fini des points satisfaisant le système d'équations $P_i(x_0, \ldots, x_n) = 0$ pour tout $i = 0, \ldots, n$. Si $\mathrm{Ind}(f)$ et $\mathrm{Ind}(f^{-1})$ ne contiennent pas de point à coordonnées dans K, alors f induit une bijection de l'ensemble fini $\mathbb{P}^n(K)$. Notons

$$\mathsf{BCr}_n(K) = \left\{ f \in \mathsf{Cr}_n(K) \mid \mathrm{Ind}(f)(K) = \mathrm{Ind}(f^{-1})(K) = \emptyset \right\}$$

le groupe formé de ces transformations rationnelles. Le but de cette Note est de montrer le théorème suivant :

Théorème 0.1. *Soit K un corps fini de caractéristique impaire, et soit n un entier supérieur ou égal à 2. Toute bijection de l'ensemble fini $\mathbb{P}^n(K)$ est réalisée par un élément de $\mathsf{BCr}_n(K)$.*

E-mail address: serge.cantat@univ-rennes1.fr.

Lorsque la caractéristique de K est égale à 2, nous montrerons que *toute bijection alternée est réalisée par un élément de* $\mathsf{BCr}_n(K)$. Si le cardinal de K vaut 2, toute bijection est en fait réalisable, mais lorsqu'il vaut 2^m avec $m > 1$, je ne sais pas si l'on peut réaliser les transpositions.

Remarque 0.2. (1) Ce résultat et la preuve qui en est donnée sont analogues à plusieurs énoncés obtenus par Biswas, Huisman, Kollár, Lukackiĭ et Mangolte à propos des transformations birationnelles de $\mathbb{P}^2(\mathbf{R})$ qui n'ont pas de point d'indétermination réel (voir [2,4,5] et [7]).

(2) Il doit également être comparé à l'énoncé de Maubach affirmant que les automorphismes polynomiaux du plan affine induisent toutes les permutations de K^2 si la caractéristique de K est impaire, et les permutations paires si $|K| = 2^m$ avec $m > 1$ (voir [8]).

(3) La proportion d'entiers $n \leqslant N$ qui sont cardinal d'un espace projectif $P^k(K)$ avec K corps fini et k entier $\geqslant 1$ tend vers 0 comme $1/\log(N)$ lorsque N tend vers l'infini. In fine, peu de bijections sont donc réalisées par des transformations birationnelles.

1. Introduction

Let p be a prime number. Let K be a finite field of characteristic p, let q be the cardinal of K and m the positive integer such that $q = p^m$. The Cremona group $\mathsf{Cr}_n(K)$ is the group of K-automorphisms of the field $K(x_1, \ldots, x_n)$. It coincides with the group of birational transformations of the projective space $\mathbb{P}^n_K$.

Let $f : \mathbb{P}^n_K \dashrightarrow \mathbb{P}^n_K$ be a birational transformation. There exists $n + 1$ homogeneous polynomial $P_i \in K[x_0, \ldots, x_n]$, $0 \leqslant i \leqslant n$, with the same degree d and without common factor, such that

$$f\big([x_0 : \cdots : x_n]\big) = [P_0 : \cdots : P_n].$$

The system of equations $P_i(x_0, \ldots, x_n) = 0$, $0 \leqslant i \leqslant n$, determines a (finite) algebraic subvariety of the projective space $\mathbb{P}^n_K$. This algebraic variety is the indeterminacy locus $\mathrm{Ind}(f)$ of f. When $\mathrm{Ind}(f)$ and $\mathrm{Ind}(f^{-1})$ contain no rational point (i.e. no point in $\mathbb{P}^n(K)$), the birational transformation f induces a bijection $\overline{f}$ of the finite set $\mathbb{P}^n(K)$. We shall denote by

$$\mathsf{BCr}_n(K) = \big\{ f \in \mathsf{Cr}_n(K) \,|\, \mathrm{Ind}(f)(K) = \mathrm{Ind}(f^{-1})(K) = \emptyset \big\}$$

the group made of these birational transformations. Restriction to $\mathbb{P}^n(K)$ defines a morphism

$$f \mapsto \overline{f}$$

from the group $\mathsf{BCr}_n(K)$ to the group $\mathsf{Bij}(\mathbb{P}^n(K))$ of all permutations of the finite projective plane $\mathbb{P}^n(K)$. Since this plane contains $q^n + \cdots + q^2 + q + 1$ elements, we get a subgroup of the finite permutation group $\mathsf{Bij}(\{1, 2, \ldots, (q^{n+1} - 1)/(q - 1)\})$.

Theorem 1.1. *Let K be a finite field and let n be an integer with $n \geqslant 2$. If the characteristic of K is odd, the morphism $f \mapsto \overline{f}$ from $\mathsf{BCr}_n(K)$ to $\mathsf{Bij}(\mathbb{P}^n(K))$ is onto.*

In other words, every permutation of $\mathbb{P}^n(K)$ is induced by a birational transformation without rational indeterminacy point (if the characteristic of K is odd). If the characteristic of K is equal to 2, we shall prove that *the image of $f \mapsto \overline{f}$ contains all even permutations*. If K has two elements, then every permutation is indeed realizable as a birational permutation, but I don't know whether transpositions of the finite set $\mathbb{P}^n(K)$ are in the image of $f \mapsto \overline{f}$ when $|K| = 2^m$, with $m > 1$.

Remark 1.2. This result and its proof are analogous to several statements due to Biswas, Huisman, Kollár, Lukackiĭ, and Mangolte. They proved that the group of birational transformations of the real projective plane $\mathbb{P}^2(\mathbf{R})$ without real indeterminacy points embeds as a dense subgroup into the group of diffeomorphisms of the plane, and acts n-transitively on $\mathbb{P}^2(\mathbf{R})$ for all $n \geqslant 0$. The interested reader may consult [2,4,5] and [7].

Remark 1.3. This result should also be compared to a similar statement due to Maubach for automorphisms of the affine plane (see [8]). In Maubach's case, a set of generators for $\mathsf{Aut}(K^2)$ is known and may be used to prove that odd permutations are not realized by automorphisms when $|K| = 2^r$, $r > 1$.

Remark 1.4. The proportion of positive integers $n \leqslant N$ that are equal to $|\mathbb{P}^k(K)|$ for at least one pair (k, K) where k is an integer and K is a finite field goes to 0 when N goes to $+\infty$. This proportion is $43/100$ for $N = 100$.

The proof follows easily from the prime number theorem. If $n \leqslant N$ is an integer of type $n = |\mathbb{P}^1(K)|$, where K is a finite field, then n is equal to $p^m + 1$ for some pair (m, p) with $m \geqslant 1$ and p a prime such that $p^m < N$. The number of primes $p \leqslant N$ is approximately $N/\log(N)$. If $p^m < N$ and $m \geqslant 2$, then $p \leqslant \sqrt{N}$ and $m \leqslant \log(N)/\log(2)$ because $p \geqslant 2$. In particular, for each prime p, the sequence $p^k + 1$, $k = 1, \dots$ counts at most $\log(N)/\log(2)$ terms before it reaches N. This implies that the number of integers $n \leqslant N$ of type $|\mathbb{P}^1(K)|$ is bounded from above by

$$\frac{N}{\log(N)} + \frac{\log(N)}{\log(2)} \sqrt{N}.$$

For integers $n \leqslant N$ of type $|\mathbb{P}^k(K)|$ with $|K| = p^m$ and $k \geqslant 2$ we have $p \leqslant \sqrt{N}$, $m \leqslant \log(N)/\log(2)$ and $k \leqslant \log(N)/\log(2)$. This gives at most

$$\left(\frac{\log(N)}{\log(2)} \right)^2 \sqrt{N}$$

terms. Hence, the proportion of integers $n \leqslant N$ of type $|\mathbb{P}^k(K)|$ for some finite field K and integer $k \geqslant 1$ goes to 0 as $1/\log(N)$ when N goes to infinity.

2. From projective transformations to arbitrary permutations

The group of automorphisms of the projective space $\mathbb{P}^n(K)$ coincides with the group of projective transformations $\mathsf{PGL}_n(K)$. This group is a strict subgroup of $\mathsf{Bij}(\mathbb{P}^n(K))$. The group of permutations of $\mathbb{P}^n(K)$ preserving collinearity is an intermediate subgroup, that is usually denoted $\mathsf{P\Gamma L}_n(K)$:

$$\mathsf{PGL}_n(K) \subset \mathsf{P\Gamma L}_n(K) \subset \mathsf{Bij}(\mathbb{P}^n(K)).$$

The group $\mathsf{P\Gamma L}_n(K)$ is generated by $\mathsf{PGL}_n(K)$ and automorphisms of the field K. Depending on K, $\mathsf{P\Gamma L}_n(K)$ may be contained, or not, in the group $\mathsf{Alt}(\mathbb{P}^n(K))$ of alternating permutations (i.e. with signature $+1$).

Theorem 2.1. *(List [6]; Bhattacharya [1].) Let K be a finite field and $n > 1$ be an integer. Let G be a subgroup of $\mathsf{Bij}(\mathbb{P}^n(K))$ which contains the automorphism group $\mathsf{PGL}_n(K)$. Either G is contained in $\mathsf{P\Gamma L}_n(K)$, or G contains the alternating subgroup $\mathsf{Alt}(\mathbb{P}^n(K))$.*

The group $\mathsf{BCr}_n(K)$ contains the group of automorphisms of $\mathbb{P}^n_K$. Hence, all what we have to do in order to prove Theorem 1.1, is to construct a birational transformation f of $\mathbb{P}^n(K)$ such that

(1) f and its inverse f^{-1} do not have any rational indeterminacy point;
(2) f does not preserve collinearity;
(3) the signature of the permutation $f : \mathbb{P}^n(K) \to \mathbb{P}^n(K)$ is -1.

In what follows, we focus on the first non-trivial case, namely $n = 2$. The general case is obtained along similar lines.

In order to construct the desired transformation $f : \mathbb{P}^2_K \dashrightarrow \mathbb{P}^2_K$, we shall first construct a birational transformation g of a smooth quadric Q, and then transport the construction onto the plane by stereographic projection.

3. A smooth quadric

Lemma 3.1. *There exists a field extension K' of K of degree 2, a smooth quadric $Q \subset \mathbb{P}^3_K$, a line $L \subset \mathbb{P}^3_K$, and a rational point $N \in Q(K)$ (all defined over K) such that*:

- *the line L does not intersect $Q(K)$;*
- *the tangent plane $T_N Q$ intersects $Q(K')$ in two conjugate lines D and D', but does not intersect $Q(K) \setminus \{N\}$;*

- *the plane $T_N Q$ contains the line L;*
- *there is a rational point $M \in Q(K)$ such that the plane H spanned by L and M cuts Q on a smooth conic.*

Proof. Let K' be an extension of K of degree 2, and let a be an element of $K' \setminus K$. Since the extension has degree 2, there are elements u, and v in K such that a and its conjugate a' are the two roots of $X^2 + uX + v = 0$. Let us first assume that the characteristic of K is different from 2. In this case, we can choose u to be 0; we then choose $Q \subset \mathbb{P}^3_K$ to be the quadric

$$x^2 + vy^2 + z^2 = t^2,$$

where $[x : y : z : t]$ are homogeneous coordinates for the projective space $\mathbb{P}^3_K$. The point $N = [0 : 0 : 1 : 1]$ is on the conic Q, and the tangent plane to Q at N intersects Q on the pair of lines $(x - ay)(x - a'y) = 0$.

The line L defined by $z = t = 0$ does not intersect $Q(K)$. For M, we choose the point $[1 : 0 : 0 : 1]$. The plane H which contains L and M is the plane $z = 0$. It intersects Q along the conic $x^2 + vy^2 = t^2$. This conic is smooth because the equation $X^2 + uX + v$ does not have any rational root.

When the characteristic of K is equal to 2, the previous formula does not define a smooth quadric, but one can choose Q to be given by the following equation $x^2 + uxy + vy^2 + z^2 + x(z + t) + y(z + t) + zt = 0$. $\quad\square$

Let us now use this lemma. By a projective change of coordinates, we can and shall assume that N is the point $[0 : 0 : 1 : 1]$, M is the point $[1 : 0 : 0 : 1]$, L is the line $z = t = 0$, and H is the plane $z = 0$, where $[x : y : z : t]$ are the (new) chosen homogeneous coordinates of $\mathbb{P}^3_K$. The plane H is isomorphic to $\mathbb{P}^2_K$, with projective coordinates $[x : y : t]$.

Let Φ_N be the stereographic projection from the pole N to the plane H. By definition, $\Phi_N : Q \to H = \mathbb{P}^2_K$ is a birational map which blows down the two lines of Q through N on two distinct points of $\mathbb{P}^2(K')$, namely $[a : 1 : 0]$ and $[a' : 1 : 0]$, and blows up N into the line through these two points, i.e. to the line L.

Let g be a birational transformation of Q, which is defined over K. Let us assume that g does not have any indeterminacy point on $Q(K)$, and that g fixes both lines tangent to Q through N pointwise (in particular, the differential of g at N is the identity). Then $\Phi_N \circ g \circ \Phi_N^{-1}$ does not have any rational indeterminacy point either. We shall use this fact to construct our desired birational transformation.

4. Construction and conclusion

Let $\pi : \mathbb{P}^3_K \dashrightarrow \mathbb{P}^1_K$ be the projection from $\mathbb{P}^3_K$ to the pencil of planes containing the line L. In coordinates,

$$\pi([x : y : z : t]) = [z : t].$$

This rational map has indeterminacies along the line L (i.e. along $z = t = 0$). This line does not contain any rational point of the quadric Q. If $[x : y : z : t]$ is a point of Q, we shall denote by $H_{[z:t]}$ the fiber of $\pi : \mathbb{P}^3_K \dashrightarrow \mathbb{P}^1_K$ through $[x : y : z : t]$; this is a plane which intersects Q on a conic containing $[x : y : z : t]$. For example, starting with the point $M = [1 : 0 : 0 : 1]$, the plane $H_{[0:1]}$ coincides with the plane H in Lemma 3.1, and intersects Q along a smooth conic.

Let G be the group of birational transformations of $\mathbb{P}^3_K$ which preserve Q and the fibers of π, acting in each fiber $H_{[z:t]}$ of π by a projective automorphism which lets $H_{[z:t]} \cap Q$ invariant. In affine coordinates (x, y, z), with $t = 1$, elements of G are of the form

$$g(x, y, z) = (A_z(x, y), z)$$

where $A : z \mapsto A_z$ takes its values in the group $\mathsf{Aut}(\mathbb{P}^2_K) = \mathsf{PGL}_3(K)$. Let us now construct an element g of G without indeterminacy point in $Q(K)$.

Being a smooth conic with a rational point, $H_{[0:1]} \cap Q$ is isomorphic to $\mathbb{P}^1_K$ (the stereographic projection from a rational point is defined over K). Moreover, if h is a homographic transformation of $\mathbb{P}^1(K)$ there is a projective transformation h' of the plane $H_{[0:1]}$ such that h' preserves the conic and the restriction of h to the conic is conjugate to h by the stereographic projection. We call h' a *lift* of h.

Let c be a generator of the cyclic group K^*. Multiplication by c determines a linear transformation of K, and therefore a homographic transformation h_c of $\mathbb{P}^1(K)$, namely $h_c([a : b]) = [ca : b]$. The multiplicative group K^* has $q - 1$ elements, and multiplication by c is a cyclic transitive permutation of this set. As a consequence, the signature

of the permutation h_c is equal to -1 if the characteristic of K is odd, and $+1$ if the characteristic is 2. Let h'_c be a lift of h_c to $H_{[0:1]}$.

Remark 4.1. If we replace h_c by the translation $g_c([a:b]) = [a+cb:b]$, where c is an element of K, then g_c fixes $[1:0]$, and the cardinal of all other orbits is equal to the order of c in the abelian group $(K,+)$. In particular, g_c is a transposition if K is the field with 2 elements and $c = 1$. In all other cases, the signature of the permutation $g_c : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ is equal to $+1$.

Interpolation in finite fields shows that there is a rational map $A : z \mapsto A_z$, with values in $\mathsf{PGL}_3(K)$, such that A_0 coincides with h'_c and A_z is the identity for all other values of z, $z = \infty$ included (see [9], Chapter I.6 for interpolation in finite fields). The rational transformation $g \in G$ which is defined by such a choice for A

(1) is an element of the group G;
(2) does not have any indeterminacy point in $Q(K)$;
(3) is the identity at the north pole N (fixing the two lines contained in $Q(K')$ through N pointwise).

As a consequence, the stereographic projection Φ_N conjugates g to an element f of $\mathsf{BCr}_2(K)$, such that

(1) f fixes the whole line L pointwise (the "image" of N by Φ_N);
(2) f preserves the image C of the conic $Q \cap H_{[0:1]}$: this conic C is smooth (isomorphic to $\mathbb{P}^1(K)$) and does not intersect the line L;
(3) f fixes two points on C, and permutes the $q - 1$ remaining points of C cyclically;
(4) all other points of $\mathbb{P}^2(K)$ are fixed by f;
(5) if the characteristic of K is different from 2, the permutation $\overline{f}$ of $\mathbb{P}^2(K)$ has signature -1, as for h_c.

Let m be one of the fixed points of f along C. Let m' be a point of C which is not fixed by f (such a point exists as soon as $|K| \neq 2$). The line containing m and m' intersects L on a third point m''. Both m and m'' are fixed points of f, m' is not fixed, and m' is the unique point of $C \setminus \{m\}$ on the line (mm''). This shows that

(6) if K has more than 2 elements, f does not preserve collinearity.

Hence, if $|K| > 2$, f is an element of $\mathsf{BCr}_2(K)$ that does not preserve collinearity. The existence of f and Theorem 2.1 show that the image of the morphism

$$\begin{cases} \mathsf{BCr}_2(K) & \to & \mathsf{Bij}(\mathbb{P}^2(K)) \\ f & \mapsto & \overline{f} \end{cases}$$

contains the alternating group. Property (5) concludes the proof of the theorem.

Remark 4.2. Let us assume that K has two elements. With the help of Remark 4.1, one can change h_c into the translation $g_1[a:b] = [a+b:b]$. Doing that, the bijection f of $\mathbb{P}^2(K)$ becomes a transposition. Since $\mathsf{PGL}_3(K)$ is 2-transitive, all transpositions are in the image of the morphism $f \mapsto \overline{f}$, and the image coincides with $\mathsf{Bij}(\mathbb{P}^2(K))$.

5. Complement

Higher dimension. The proof is the same in higher dimension. In order to construct the required element $f : \mathbb{P}^n_K \dashrightarrow \mathbb{P}^n_K$, we start with a smooth quadric Q in $\mathbb{P}^{n+1}_K$ and a line L which does not intersect $Q(K)$. The family of planes of dimension 2 that contain L cuts Q along a family of conics. We may assume that one of this planes H intersects Q along a smooth conic. The birational transformation g of Q is defined as in the previous section: It preserves the family of planes, coincides with h'_c along H, and is the identity for the remaining planes. We choose a point N in $Q(K)$ such that the plane through N containing L is tangent to Q at N. We then conjugate g to an element f of $\mathsf{BCr}_n(K)$ by a stereographic projection Φ_N from the pole N. The map f does not preserve collinearity, and its signature is -1 if p is odd or $|K| = 2$.

Question. Let us fix the dimension n and the field K. Let $\mathsf{BCr}_{n,d}(K)$ be the finite set of elements $f \in \mathsf{BCr}_n(K)$ which are defined by homogeneous polynomials of degree at most d. Let σ be an element of $\mathsf{Bij}(\mathbb{P}^n(K))$, and $N(d, \sigma)$ be the number of elements f in $\mathsf{BCr}_{n,d}(K)$ such that $\overline{f} = \sigma$. What is the asymptotic behaviour of $N(d, \sigma)/|\mathsf{BCr}_{n,d}(K)|$? If σ is an element of $\mathsf{Bij}(\mathbb{P}^n(K))$, let $L(\sigma)$ be the length of its longest orbit. What is the expectation of $L(\overline{f})$ for f in $\mathsf{BCr}_{n,d}(K)$? Similar questions have been studied for projective transformations instead of birational transformations (see [3]).

References

[1] Prabir Bhattacharya, On groups containing the projective special linear group, Arch. Math. (Basel) 37 (4) (1981) 295–299.
[2] Indranil Biswas, Johannes Huisman, Rational real algebraic models of topological surfaces, Doc. Math. 12 (2007) 549–567.
[3] Jason Fulman, Random matrix theory over finite fields, Bull. Amer. Math. Soc. (N.S.) 39 (1) (2002) 51–85 (electronic).
[4] Johannes Huisman, Frédéric Mangolte, The group of automorphisms of a real rational surface is n-transitive, preprint, 2008, pp. 1–7.
[5] Janos Kollár, Frédéric Mangolte, Cremona transformations and diffeomorphisms of surfaces, preprint, 2008, pp. 1–17.
[6] R. List, On permutation groups containing $\mathrm{PSL}_n(q)$ as a subgroup, Geom. Dedicata 4 (2/3/4) (1975) 373–375.
[7] A.M. Lukackiĭ, The structure of Lie algebras of spherical vector fields and the diffeomorphism groups of S^n and RP^n, Sibirsk. Mat. Zh. 18 (1) (1977) 161–173, 239.
[8] Stefan Maubach, Polynomial automorphisms over finite fields, Serdica Math. J. 27 (4) (2001) 343–350.
[9] Gary L. Mullen, Carl Mummert, Finite Fields and Applications, Student Mathematical Library, vol. 41, American Mathematical Society, Providence, RI, 2007.