A Minkowski-style bound for the orders of the finite subgroups of the Cremona group of rank 2 over an arbitrary field

Jean-Pierre Serre

Let k be a field. Let $\mathrm{Cr}(k)$ be the Cremona group of rank 2 over k, i.e. the group of k-automorphisms of $k(X, Y)$, where X and Y are two indeterminates.

We shall be interested in the finite subgroups of $\mathrm{Cr}(k)$ of order prime to the characteristic of k. The case $k = \mathbf{C}$ has a long history, going back to the 19-th century (see the references in [Bl 06] and [DI 07]), and culminating in an essentially complete (but rather complicated) classification, see [DI 07]. For an arbitrary field, it seems reasonable to simplify the problem à la Minkowski, as was done in [Se 07] for semisimple groups; this means giving a sharp multiplicative bound for the orders of the finite subgroups we are considering.

In §6.9 of [Se 07], I had asked a few questions in that direction, for instance the following :

If $k = \mathbf{Q}$, is it true that $\mathrm{Cr}(k)$ does not contain any element of prime order $\geqslant 11$?

More generally, what are the prime numbers ℓ, distinct from $\mathrm{char}(k)$, such that $\mathrm{Cr}(k)$ contains an element of order ℓ ?

This question has now been solved by Dolgachev and Iskovskikh ([DI 08]), the answer being that there is equivalence between :

$\mathrm{Cr}(k)$ contains an element of order ℓ

and

$[k(z_\ell) : k] = 1, 2, 3, 4$ or 6, where z_ℓ is a primitive ℓ-th root of unity.

As we shall see, a similar method can handle arbitrary ℓ-groups and one obtains an explicit value for the Minkowski bound of $\mathrm{Cr}(k)$, in terms of the size of the Galois group of the cyclotomic extensions of k (cf. Th.2.1 below). For instance :

Theorem - *Assume k is finitely generated over its prime subfield. Then the finite subgroups of $\mathrm{Cr}(k)$ of order prime to $\mathrm{char}(k)$ have bounded order. Let $M(k)$ be the least common multiple of their orders .*

a) If $k = \mathbf{Q}$, we have $M(k) = 120960 = 2^7.3^3.5.7.$

b) If k is finite with q elements, we have :

$$M(k) = \begin{cases} 3.(q^4-1)(q^6-1) & \textit{if } q \equiv 4 \textit{ or } 7 \pmod 9 \\ (q^4-1)(q^6-1) & \textit{otherwise}. \end{cases}$$

For more general statements, see §2. These statements involve the cyclotomic invariants of k introduced in [Se 07, §6]; their definition is recalled in §1. The proofs are given in §3 (existence of large subgroups) and in §4 (upper bounds). For the upper bounds, we use a method introduced by Manin ([Ma 66]) and perfected by Iskovskikh ([Is 79], [Is 96]) and Dolgachev-Iskovskikh ([DI 08]); it allows us to realize any finite subgroup of $\mathrm{Cr}(k)$ as a subgroup of $\mathrm{Aut}(S)$, where S is either a del Pezzo surface or a conic bundle over a conic. A few conjugacy results are given in §5. The last § contains a series of open questions on the Cremona groups of rank > 2.

§1 The cyclotomic invariants t and m

In what follows, k is a field, k_s is a separable closure of k and $\overline{k}$ is the algebraic closure of k_s.

Let ℓ a prime number distinct from $\mathrm{char}(k)$; the ℓ-adic valuation of $\mathbf{Q}$ is denoted by v_ℓ, or sometimes simply by v. If A is a finite set, with cardinal $|A|$, we write $v_\ell(A)$ instead of $v_\ell(|A|)$.

There are two invariants $t = t(k, l)$ and $m = m(k, l)$ which are associated with the pair (k, l), cf. [Se 07, §4]. Recall their definitions :

1.1 Definition of t

Let $z \in k_s$ be a primitive ℓ-th root of unity if $l > 2$ and a primitive 4-th root of unity if $\ell = 2$. We put

$$t = [k(z) : k].$$

If $\ell > 2$, t divides $\ell - 1$. If $\ell = 2$ or 3, then $t = 1$ or 2.

1.2 Definition of m

For $\ell > 2$, m is the upper bound (possibly infinite) of the n's such that $k(z)$ contains the ℓ^n-th roots of unity. We have $m \geqslant 1$.

For $\ell = 2$, m is the upper bound (possibly infinite) of the n's such that k contains $z(n) + z(n)^{-1}$, where $z(n)$ is a primitive 2^n-root of unity. We have $m \geqslant 2$. [The definition of m given in [Se 07, §4.2] looks different, but it is equivalent to the one here.]

Remark. Knowing t and m amounts to knowing the image of the ℓ-th cyclotomic character $\mathrm{Gal}(k_s/k) \to \mathbf{Z}_l^*$, cf. [Se 07, §4].

1.3 Example : $k = \mathbf{Q}$

Here, t takes its largest possible value, namely $t = \ell - 1$ for $\ell > 2$ and $t = 2$ for $\ell = 2$. And m takes its smallest possible value, namely $m = 1$ for $\ell > 2$ and $m = 2$ for $\ell = 2$.

1.4 Example : k finite with q elements

If $\ell > 2$, one has :

$t =$ order of q in the multiplicative group $\mathbf{F}_\ell^*$

$m = v_\ell(q^t - 1) = v_\ell(q^{l-1} - 1)$.

If $\ell = 2$, one has :

$t =$ order of q in $(\mathbf{Z}/4\mathbf{Z})^*$

$m = v_2(q^2 - 1) - 1$.

§2 Statement of the main theorem

Let $K = k(X, Y)$, where X, Y are indeterminates, and let $\mathrm{Cr}(k)$ be the Cremona group of rank 2 over k, i.e. the group $\mathrm{Aut}_k\, K$. Let ℓ be a prime number, distinct from $\mathrm{char}(k)$, and let t and m be the cyclotomic invariants defined above.

2.1 Notation

Define a number $M(k, \ell) \in \{0, 1, 2, ..., \infty\}$ as follows :

For $\ell = 2$, $M(k, \ell) = 2m + 3$.

$$\text{For } \ell = 3,\ M(k,\ell) = \begin{cases} 4 & \text{if } t = m = 1 \\ 2m+1 & \text{otherwise.} \end{cases}$$

$$\text{For } \ell > 3,\ M(k,\ell) = \begin{cases} 2m & \text{if } t = 1 \quad \text{or } 2 \\ m & \text{if } t = 3, 4 \quad \text{or } 6 \\ 0 & \text{if } t = 5 \quad \text{or } t > 6. \end{cases}$$

2.2 The main theorem

Theorem 2.1.(i) *Let A be a finite subgroup of* $\mathrm{Cr}(k)$*. Then $v_\ell(A) \leqslant M(k, \ell)$.*

(ii) *Conversely, if n is any integer $\geqslant 0$ which is $\leqslant M(k, \ell)$ then* $\mathrm{Cr}(k)$ *contains a subgroup of order ℓ^n.*

(In other words, $M(k, \ell)$ is the upper bound of the $v_\ell(A)$.)

The special case where A is cyclic of order ℓ gives :

Corollary 2.2 ([DI 08]). *The following properties are equivalent* :

a) $\mathrm{Cr}(k)$ *contains an element of order ℓ*

b) $\varphi(t) \leq 2$*, i.e.* $t = 1, 2, 3, 4$ *or* 6.

Indeed, b) is equivalent to $M(k, \ell) > 0$.

2.3 Small fields

Let us say that k is *small* if it has the following properties :

(2.3.1) $m(k, \ell) < \infty$ for every $\ell \neq \mathrm{char}(k)$

(2.3.2) $t(k, \ell) \to \infty$ when $\ell \to \infty$.

Proposition 2.3. *A field which is finitely generated over* $\mathbf{Q}$ *or* $\mathbf{F}_p$ *is small.*

Proof. The formulae given in §1.3 and §1.4 show that both $\mathbf{F}_p$ and $\mathbf{Q}$ are small. If k'/k is a finite extension, one has

$$[k' : k].t(k', \ell) \geqslant t(k, \ell) \ \text{ and } \ m(k', \ell) \leqslant m(k, \ell) + \log_\ell([k' : k]),$$

which shows that k small $\Rightarrow k'$ small. If k' is a regular extension of k , then

$$t(k',\ell) = t(k,\ell) \quad \text{and} \quad m'(k',\ell) = m(k,\ell),$$

which also shows that k small $\Rightarrow k'$ small. The proposition follows.

Assume now that k is small. We may then define an integer $M(k)$ by the following formula

$$M(k) = \prod_{\ell} \ell^{M(k,\ell)}, \tag{2.3.3}$$

where ℓ runs through the prime numbers distinct from $\mathrm{char}(k)$. The formula makes sense since $M(k,\ell)$ is finite for every ℓ and is 0 for every ℓ but a finite number. With this notation, Th. 2.1 can be reformulated as :

Theorem 2.4. *If k is small, then the finite subgroups of* $\mathrm{Cr}(k)$ *of order prime to* $\mathrm{char}(k)$ *have bounded order, and the l.c.m. of their orders is the integer $M(k)$ defined above.*

Note that this applies in particular when k is finitely generated over its prime subfield.

2.4 Example : the case $k = \mathbf{Q}$

By combining 1.3 and 2.1, one gets

$$M(\mathbf{Q},\ell) = \begin{cases} 7 & \text{for} \quad \ell = 2, \\ 3 & \text{for} \quad \ell = 3, \\ 1 & \text{for} \quad \ell = 5, 7 \\ 0 & \text{for} \quad \ell > 7. \end{cases}$$

This can be summed up by :

Theorem 2.5. $M(\mathbf{Q}) = 2^7.3^3.5.7.$

2.5 Example : the case of a finite field

Theorem 2.6. *If k is a finite field with q elements, we have*

$$M(k) = \begin{cases} 3.(q^4-1)(q^6-1) & \textit{if} \;\; q \equiv 4 \;\; \textit{or} \; 7 \pmod 9 \\ (q^4-1)(q^6-1) & \textit{otherwise}. \end{cases}$$

Proof. Denote by $M'(k,\ell)$ the ℓ-adic valuation of the right side of the formulae above.

If ℓ is not equal to 3, $M'(k,\ell)$ is equal to

$$v_\ell(q^4-1) + v_\ell(q^6-1)$$

and we have to check that $M'(k,\ell)$ is equal to $M(k,\ell)$.

Consider first the case $\ell = 2$. It follows from the definition of m that

$v_2(q^2 - 1) = m + 1$, and hence $v_2(q^4 - 1) = m + 2$ and $v_2(q^6 - 1) = m + 1$. This gives $M'(k, \ell) = 2m + 3 = M(k, \ell)$.

If $\ell > 3$, the invariant t is the smallest integer > 0 such that $q^t = 1 \pmod{l}$. If $t = 5$ or $t > 6$, this shows that $M'(k, \ell) = 0$.

If $t = 3$ or 6, $q^4 - 1$ is not divisible by ℓ and $q^6 - 1$ is divisible by ℓ ; moreover, one has $v_\ell(q^6 - 1) = m$. This gives $M'(k, \ell) = m = M(k, \ell)$. Similarly, when $t = 4$, the only factor divisible by ℓ is $q^4 - 1$ and its ℓ-adic valuation is m. When $t = 1$ or 2, both factors are divisible by ℓ and their ℓ-adic valuation is m.

The argument for $\ell = 3$ is similar : we have

$$v_3(q^4 - 1) = m \quad \text{and} \quad v_3(q^6 - 1) = m + 1.$$

The congruence $q \equiv 4$ or $7 \pmod 9$ means that $t = m = 1$.

For instance :

$M(\mathbf{F}_2) = 3^3.5.7$; $M(\mathbf{F}_3) = 2^7.5.7.13$; $M(\mathbf{F}_4) = 3^4.5^2.7.13.17$;
$M(\mathbf{F}_5) = 2^7.3^3.7.13.31$; $M(\mathbf{F}_7) = 2^9.3^4.5^2.19.43$.

2.6 Example : the p-adic field $\mathbf{Q}_p$

For $\ell \neq p$, the t, m invariants of $\mathbf{Q}_p$ are the same as those of $\mathbf{F}_\ell$, and for $\ell = p$ they are the same as those of $\mathbf{Q}$.

This shows that $\mathbf{Q}_p$ is " small ", and a simple computation gives

$$M(\mathbf{Q}_p) = c(p).(p^4 - 1)(p^6 - 1),$$

with

$c(2) = 2^7$; $c(3) = 3^3$; $c(5) = 5$; $c(7) = 3.7$;
$c(p) = 3$ if $p > 7$ and $p \equiv 4$ or $7 \pmod 9$;
$c(p) = 1$ otherwise.

For instance :

$M(\mathbf{Q}_2) = 2^7.3^3.5.7$; $M(\mathbf{Q}_3) = 2^7.3^3.5.7.13$; $M(\mathbf{Q}_5) = 2^7.3^3.5.7.13.31$;
$M(\mathbf{Q}_7) = 2^9.3^4.5^2.7.19.43$; $M(\mathbf{Q}_{11}) = 2^7.3^3.5^2.7.19.37.61$.

2.7 Remarks

1. The statement of Th.2.6 is reminiscent of the formula which gives the order of $G(k)$, where G is a split semisimple group and $|k| = q$. In such a formula, the factors have the shape $(q^d - 1)$, where d is an invariant degree of the Weyl group, and the number of factors is equal to the rank of G. Here also the number of factors is equal to the rank of Cr, which is 2. The exponents 4 and 6 are less easy to interpret. In the proofs below, they occur as the maximal orders of the torsion elements of the " Weyl group " of Cr, which is $\mathbf{GL}_2(\mathbf{Z})$. See also §6.

2. Even though Th.2.6 is a very special case of Th.2.1, it contains almost as much information as the general case. More precisely, we could deduce Th.2.1.(i)

[which is the hard part] from Th.2.6 by the Minkowski method of reduction (mod p) explained in [Se 07, §6.5].

3. In the opposite direction, if we know Th.2.1.(i) for fields of characteristic 0 (in the slightly more precise form given in §4.1), we can get it for fields of characteristic $p > 0$ by lifting over the ring of Witt vectors; this is possible : all the cohomological obstructions vanish.

4. For large fields, the invariant m can be ∞. If t is not $1, 2, 3, 4$ or 6, Cor.2.2 tells us that $\mathrm{Cr}(k)$ is ℓ-torsion-free. But if t is one of these five numbers, the above theorems tell us nothing. Still, as in [Se 07, §14, Th.12 and Th.13] one can prove the following :

a) If $t = 3, 4$ or 6, then $\mathrm{Cr}(k)$ contains a subgroup isomorphic to $\mathbf{Q}_\ell/\mathbf{Z}_\ell$ and does not contain $\mathbf{Q}_\ell/\mathbf{Z}_\ell \times \mathbf{Q}_\ell/\mathbf{Z}_\ell$.

b) If $t = 1$ or 2, then $\mathrm{Cr}(k)$ contains a subgroup isomorphic to $\mathbf{Q}_\ell/\mathbf{Z}_\ell \times \mathbf{Q}_\ell/\mathbf{Z}_\ell$ and does not contain a product of three copies of $\mathbf{Q}_\ell/\mathbf{Z}_\ell$.

§3 Proof of Theorem 2.1.(ii)

We have to construct large ℓ-subgroups of $\mathrm{Cr}(k)$. It turns out that we only need two constructions, one for the very special case $\ell = 3, t = 1, m = 1$, and one for all the other cases.

3.1 The special case $\ell = 3,\ t = 1,\ m = 1$

We need to construct a subgroup of $\mathrm{Cr}(k)$ of order 3^4. To do so we use the Fermat cubic surface S given by the homogeneous equation

$$x^3 + y^3 + z^3 + t^3 = 0.$$

It is a smooth surface, since $p \neq 3$. The fact that $t = 1$ means that k contains a primitive cubic root of unity. This implies that the 27 lines of S are defined over k, and hence S is k-rational : its function field is isomorphic to $K = k(X, Y)$. Let A be the group of automorphisms of S generated by the two elements

$$(x, y, z, t) \mapsto (rx, y, z, t) \quad \text{and} \quad (x, y, z, t) \mapsto (y, z, x, t)$$

where r is a primitive 3-rd root of unity.

We have $|A| = 3^4$ and A is a subgroup of $\mathrm{Aut}(S)$, hence a subgroup of $\mathrm{Cr}(k)$.

3.2 The generic case

Here is the general construction :

One starts with a 2-dimensional torus T over k , with an ℓ-group C acting faithfully on it. Let B be an ℓ-subgroup of $T(k)$. Assume that B is stable under C, and let A be the semi-direct product $A = B.C$. If we make B act on the variety T by translations, we get an action of A, which is faithful. This gives an embedding of A in $\mathrm{Aut}(k(T))$, where $k(T)$ is the function field of T. By a theorem of Voskresinskii (see [Vo 98, §4.9]) $k(T)$ is isomorphic to $K = k(X,Y)$. We thus get an embedding of A in $\mathrm{Cr}(k)$. Note that B is *toral*, i.e. is contained in the k-rational points of a maximal torus of Cr.

It remains to explain how to choose T, B and C. We shall define T by giving the action of $\Gamma_k = \mathrm{Gal}(k_s/k)$ on its character group ; this amounts to giving an homomorphism $\Gamma_k \to \mathbf{GL}_2(\mathbf{Z})$.

3.2.1 The case $\ell = 2$

Let n be an integer $\leqslant m$. If $z(n)$ is a primitive 2^n-root of unity, k contains $z(n) + z(n)^{-1}$. The field extension $k(z(n))/k$ has degree 1 or 2, hence defines a character $\Gamma_k \to 1, -1$. Let T_1 be the 1-dimensional torus associated with this character. If $k(z(n)) = k$, T_1 is the split torus $\mathbf{G}_m$ and we have $T_1(k) = k^*$. If $k(z(n))$ is quadratic over k, $T_1(k)$ is the subgroup of $k(z(n))^*$ made up of the elements of norm 1. In both cases, $T_1(k)$ contains $z(n)$. We now take for T the torus $T_1 \times T_1$ and for B the subgroup of elements of T of order dividing 2^n. We have $v_2(B) = 2n$. We take for C the group of automorphisms generated by $(x, y) \mapsto (x^{-1}, y)$ and $(x, y) \mapsto (y, x)$; the group C is isomorphic to the dihedral group D_4 ; its order is 8. We then have $v_2(A) = v_2(B) + v_2(C) = 2n + 3$, as wanted.

(Alternate construction : the group $\mathrm{Cr}_1(k) = \mathbf{PGL}_2(k)$ contains a dihedral subgroup D of order 2^{n+1} ; by using the natural embedding of $(\mathrm{Cr}_1(k)\times\mathrm{Cr}_1(k)).2$ in $\mathrm{Cr}(k)$ we obtain a subgroup of $\mathrm{Cr}(k)$ isomorphic to $(D \times D).2$, hence of order 2^{2n+3}.)

3.2.2 The case $\ell > 2$

We start similarly with an integer $n \leqslant m$. We may assume that the invariant t is equal to $1, 2, 3, 4$ or 6 ; if not we could take $A = 1$. Call C_t the Galois group of $k(z)/k$, cf.§1. It is a cyclic group of order t. Choose an embedding of C_t in $\mathbf{GL}_2(\mathbf{Z})$, with the condition that, if $t = 2$, then the image of C_t is $\{1, -1\}$. The composition map

$$r : \Gamma_k \to \mathrm{Gal}(k(z)/k) = C_t \to \mathbf{GL}_2(\mathbf{Z})$$

defines a 2-dimensional torus T.

The group B is the subgroup $T(k)[l^n]$ of $T(k)$ made up of elements of order dividing l^n . We take C equal to 1, except when $l = 3$ where we choose it of order 3 (this is possible since $t = 1$ or 2 for $\ell = 3$, and the group of k-automorphisms of T is isomorphic to $\mathbf{GL}_2(\mathbf{Z})$). We thus have :

$v_\ell(A) = v_\ell(B)$ if $\ell > 3$ and $v_\ell(A) = 1 + v_\ell(B)$ if $\ell = 3$.

It remains to estimate $v_\ell(B)$. Namely :

(3.2.3) $v_\ell(B) = 2n$ if $t = 1$ or 2

This is clear if $t = 1$ because in that case T is a split torus of dimension 2, and k contains $z(n)$.

If $t = 2$, then $T = T_1 \times T_1$, where T_1 is associated with the quadratic character $\Gamma_k \to \mathrm{Gal}(k(z)/k)$. We may identify $T_1(k)$ with the elements of norm 1 of $k(z)$, and this shows that $z(n)$ is an element of $T_1(k)$ of order 2^n. We thus get $v_\ell(B) = 2n$.

(3.2.4) $v_\ell(|B|) \geqslant n$ if $t = 3, 4$ or 6

We use the description of T given in [Se 07, §5.3] : let L be the field $k(z)$. It is a cyclic extension of k of degree t. Let s be a generator of $C_t = \mathrm{Gal}(L/k)$. Let $T_L = R_{L/k}(\mathbf{G}_m)$ be the torus ' multiplicative group of L " ; we have $\dim T_L = t$, and s acts on T_L. We have $s^t - 1 = 0$ in $\mathrm{End}(T_L)$. Let $F(X)$ be the cyclotomic polynomial of index t, i.e.

$$\begin{array}{ll} F(X) = X^2 + X + 1 & \text{if } t = 3 \\ F(X) = X^2 + 1 & \text{if } t = 4 \\ F(X) = X^2 - X + 1 & \text{if } t = 6. \end{array}$$

This polynomial divides $X^t - 1$; let $G(X)$ be the quotient $(X^t - 1)/F(X)$, and let u be the endomorphism of T_1 defined by $u = G(s)$. One checks (loc.cit.) that the image T of $u : T_1 \to T_1$ is a 2-dimensional torus, and s defines an automorphism s_T of T of order t, satisfying the equation $F(s_T) = 0$. This shows that T is the same as the torus also called T above. Moreover, it is easy to check that the element $z(n)$ of $T_1(k)$ is sent by u into an element of $T(k)$ of order l^n . This shows that $v_\ell(B) \geqslant n$.

[When $t = 3$, we could have defined T as the kernel of the norm map $N : T_1 \to \mathbf{G}_m$. There is a similar definition for $t = 4$, but the case $t = 6$ is less easy to describe concretely.]

This concludes the proof of the "existence part" of Th.2.1.

§4 Proof of Theorem 2.1.(i)

4.1 Generalization

In Th.2.1.(i), the hypothesis made on the ℓ-group A is that it is contained in $\mathrm{Cr}(k)$. This is equivalent to saying that A is contained in $\mathrm{Aut}(S)$, where S is a k-rational surface, cf. e.g. [DI 07,Lemma 6]. We now want to relax this hypothesis : we will merely assume that S is a surface which is " geometrically rational ", i.e. becomes rational over $\overline{k}$; for instance S can be any smooth cubic surface in $\mathbf{P}_3$. In other words, we will be interested in field extensions L of k with the property :

(4.1.1) $\overline{k} \otimes L$ is $\overline{k}$-isomorphic to $\overline{k}(X, Y)$.

We shall say that a group A has " property Cr_k " if it can be embedded in $\mathrm{Aut}(L)$, for some L having property (4.1.1). The bound given in Th.2.1.(i) is valid for such groups. More precisely :

Theorem 4.1. *If a finite ℓ-group A has property Cr_k , then $v_\ell(A) \leqslant M(k, \ell)$, where $M(k, \ell)$ is as in §2.1.*

This is what we shall prove. Note that we may assume that k is perfect since replacing k by its perfect closure does not change the invariants t, m and $M(k, l)$.

[As mentioned in §2.7, we could also assume that k is finite, or, if we preferred to, that $\mathrm{char}(k) = 0$. Unfortunately, none of these reductions is really helpful.]

4.2 Reduction to special cases

We start from an ℓ-group A having property Cr_k. As explained above, this means that we can embed A in $\mathrm{Aut}(S)$, where S is a smooth projective k-surface, which is geometrically rational. Now, the basic tool is the " minimal model theorem " (proved in [DI 07, §2]) which allows us to assume that S is of one of the following two types :

a) (*conic bundle case*) There is a morphism $f : S \to C$, where C is a smooth genus zero curve, such that the generic fiber of f is a smooth curve of genus 0. Moreover, A acts on C and f is compatible with that action.

b) (*del Pezzo*) S is a del Pezzo surface, i.e. its anticanonical class $-K_S$ is ample.

In case b), the degree $\deg(S)$ is defined as $K_S.K_S$ (self-intersection) ; one has $1 \leqslant \deg(S) \leqslant 9$.

We shall look successively at these different cases. In the second case, we shall use without further reference the standard properties of the del Pezzo surfaces ; one can find them for instance in [De 80], [Do 07], [DI 07], [Ko 96], [Ma 66] and [Ma 86].

Remark. In some of these references, the ground field is assumed to be of characteristic 0, but there is very little difference in characteristic $p > 0$; moreover, as pointed out above, the characteristic 0 case implies the characteristic p case, thanks to the fact that $|A|$ is prime to $\mathrm{char}(k)$.

4.3 The conic bundle case

Let $f : S \to C$ be as in a) above, and let A_o be the subgroup of $\mathrm{Aut}(C)$ given by the action of A on C. The group $\mathrm{Aut}(C)$ is a k-form of $\mathbf{PGL_2}$. By using (for instance) [Se 07, Th.5] we get :

$$v_\ell(A_o) \leqslant \begin{cases} m+1 & \text{if} \quad l = 2, \\ m & \text{if} \quad l > 2 \ \text{ and } \ t = 1 \ \text{ or } \ 2, \\ 0 & \text{if} \quad t > 2. \end{cases}$$

Let B be the kernel of $A \to A_o$. The group B is a subgroup of the group of automorphisms of the generic fiber of f. This fiber is a genus 0 curve over the function field k_C of C. Since k_C is a regular extension of k, the t and m invariants of k_C are the same as those of k. We then get for $v_\ell(B)$ the same bounds as for $v_\ell(A_o)$, and by adding up this gives :

$$v_\ell(A) \leqslant \begin{cases} 2m+2 & \text{if} \quad \ell = 2 \\ 2m & \text{if} \quad \ell > 2 \;\text{ and }\; t = 1 \;\text{ or }\; 2 \\ 0 & \text{if} \quad t > 2. \end{cases}$$

In each case, this gives a bound which is at most equal to the number $M(k, \ell)$ defined in §2.1.

4.4 The del Pezzo case : degree 9

Here S is $\overline{k}$-isomorphic to the projective plane $\mathbf{P}_2$; in other words, S is a Severi-Brauer variety of dimension 2. The group $\mathrm{Aut}\, S$ is an inner k-form of $\mathbf{PGL}_3$. By using [Se 07, §6.2] one finds :

$$v_\ell(A) \leqslant \begin{cases} 2m+1 & \text{if} \quad \ell = 2 \\ 2m+1 & \text{if} \quad \ell = 3, t = 1 \\ \leq m+1 & \text{if} \quad \ell = 3, t = 2 \\ \leq 2m & \text{if} \quad \ell > 3, t = 1 \\ \leq m & \text{if} \quad \ell > 3, t = 2 \;\text{ or }\; 3 \\ = 0 & \text{if} \quad t > 3. \end{cases}$$

Here again, these bounds are $\leqslant M(k, \ell)$.

4.5 The del Pezzo case : degree 8

This case splits into two subcases :

a) S is the blow up of $\mathbf{P}_2$ at one rational point. In that case A acts faithfully on $\mathbf{P}_2$ and we apply 4.4.

b) S is a smooth quadric of $\mathbf{P}_3$. The connected component $\mathrm{Aut}^o(S)$ of $\mathrm{Aut}(S)$ has index 2. It is a k-form of $\mathbf{PGL}_2 \times \mathbf{PGL}_2$. If we denote by A_o the intersection of A with $\mathrm{Aut}^o(S)$, we obtain, by [Se 07, Th.5], the bounds :

$$v_\ell(A_0) \leqslant \begin{cases} 2m+2 & \text{if} \quad \ell = 2 \\ 2m & \text{if} \quad \ell > 2 \;\text{ and }\; t = 1 \;\text{ or }\; 2 \\ m & \text{if} \quad t = 3, 4 \;\text{ or }\; 6 \\ 0 & \text{if} \quad t = 5 \;\text{ or }\; t > 6. \end{cases}$$

Since $v_\ell(A) = v_\ell(A_o)$ if $\ell > 2$ and $v_\ell(A) \leqslant v_\ell(A_o) + 1$ if $\ell = 2$, we obtain a bound for $v_\ell(A)$ which is $\leqslant M(k, \ell)$.

Remarks. 1) Note the case $\ell = 2$, where the $M(k, \ell)$ bound $2m + 3$ can be attained.

2) In the case $t = 6$, the bound $v_\ell(A_o) \leqslant m$ given above can be replaced by $v_\ell(A_o) = 0$, but this is not important for what we are doing here.

4.6 The del Pezzo case : degree 7

This is a trivial case; there are 3 exceptional curves on S (over $\overline{k}$), and only one of them meets the other two. It is thus stable under A, and by blowing it down, one is reduced to the degree 8 case. [This case does not occur if one insists, as in [DI 08], that the rank of $\mathrm{Pic}(S)^A$ be equal to 1.]

4.7 The del Pezzo case : degree 6

Here the surface S has 6 exceptional curves (over $\overline{k}$), and the corresponding graph L is an hexagon. There is a natural homomorphism

$$g : \mathrm{Aut}(S) \to \mathrm{Aut}(L)$$

and its kernel T is a 2-dimensional torus. Put $A_o = A \cap T(k)$. The index of A_o in A is a divisor of 12. By [Se 07, Th.4], we have

$$v_\ell(A_o) \leqslant \begin{cases} 2m & \text{if} \quad t = 1 \ \text{ or } \ 2 \qquad \text{(i.e. if } \ \varphi(t) = 1) \\ m & \text{if} \quad t = 3, \ 4 \ \text{ or } \ 6 \qquad \text{(i.e. if } \ \varphi(t) = 2) \\ 0 & \text{if} \quad t = 5 \ \text{ or } \ t > 6. \end{cases}$$

Hence :

$$v_\ell(A) \leqslant \begin{cases} 2m+2 & \text{if} \quad \ell = 2 \\ 2m+1 & \text{if} \quad \ell = 3 \\ 2m & \text{if} \quad \ell > 3 \ \text{ and } \ t = 1 \ \text{ or } \ 2 \\ m & \text{if} \quad t = 3, \ 4 \ \text{ or } \ 6 \\ 0 & \text{if} \quad t = 5 \ \text{ or } \ t > 6. \end{cases}$$

These bounds are $\leqslant M(k, \ell)$.

Remarks. 1) Note the case $t = 6$, where the bound m can actually be attained.

2) In the case $t = 4$, the bound $v_\ell(A) \leqslant m$ given above can be replaced by $v_\ell(A) = 0$.

4.8 The del Pezzo case : degree 5

As above, let L be the graph of the exceptional curves of S. Since $\deg(S) \leqslant 5$, the natural map $\mathrm{Aut}(S) \to \mathrm{Aut}(L)$ is injective. We can thus identify A with its image A_L in $\mathrm{Aut}(L)$. In the case $\deg(S) = 5$, $\mathrm{Aut}(L)$ is isomorphic to the symmetric group S_5. In particular we have

$$v_\ell(A) \leqslant \begin{cases} 3 & \text{if} \quad \ell = 2 \\ 1 & \text{if} \quad \ell = 3 \ \text{ or } \ 5 \\ 0 & \text{if} \quad \ell > 5, \end{cases}$$

and we conclude as before.

4.9 The del Pezzo case : degree 4

This case is similar to the preceding one. Here $\mathrm{Aut}(L)$ is isomorphic to the group $2^4.S_5 = \mathrm{Weyl}(D_5)$; its order is $2^7.3.5$. We get the same bounds as above, except for $\ell = 2$ where we find $v_\ell(A) \leqslant 7$, which is $\leqslant M(k, 2)$ [recall that $M(k, 2) = 2m + 3$ and that $m \geqslant 2$ for $\ell = 2$].

4.10 The del Pezzo case : degree 3

Here S is a smooth cubic surface, and A embeds in $\mathrm{Weyl}(E_6)$, a group of order $2^7.3^4.5$. This gives a bound for $v_\ell(A)$ which gives what we want, except when $\ell = 3$. In the case $\ell = 3$, it gives $v_\ell(A) \leqslant 4$, but $Th.2.1$ claims $v_\ell(A) \leqslant 3$ unless k contains a primitive cubic root of unity. We thus have to prove the following lemma :

Lemma 4.2 - *Assume that* $|A| = 3^4$ *, that* A *acts faithfully on a smooth cubic surface* S *over* k*, and that* $\mathrm{char}(k) \neq 3$. *Then* k *contains a primitive cubic root of unity.*

Proof. The structure of A is known since A is isomorphic to a 3-Sylow subgroup of $\mathrm{Weyl}(E_6)$. In particular the center $Z(A)$ of A is cyclic of order 3 and is contained in the commutator group de A. Since A acts on S, it acts on the sections of the anticanonical sheaf of S ; we get in this way a faithful linear representation $r : A \to \mathbf{GL}_4(k)$. Over $\overline{k}$, r splits as $r = r_1 + r_3$ where r_1 is 1-dimensional and r_3 is irreducible and 3-dimensional. If z is a non trivial element of $Z(A)$, the eigenvalues of z are $\{1, r, r, r\}$ where r is a primitive third root of unity. This shows that r belongs to k.

4.11 The del Pezzo case : degree 2

Here A embeds in $\mathrm{Weyl}(E_7)$, a group of order $2^{10}.3^4.5.7$. This gives a bound for $v(A)$, but this bound is not good enough. However, the surface S is a 2-sheeted covering of $\mathbf{P}_2$ (the map $S \to \mathbf{P}_2$ being the anticanonical map) and we get a homomorphism $g : A \to \mathbf{PGL}_3(k)$ whose kernel has order 1 or 2. We then find the same bounds for $v_\ell(A)$ as in §4.2, except that, for $\ell = 2$, the bound is $2m + 2$ instead of $2m + 1$.

4.12 The del Pezzo case : degree 1

We use the linear series $| - 2K_S|$. It gives a map $g : S \to \mathbf{P}_3$ whose image is a quadratic cone Q, cf. e.g. [De 80, p.68]. This realizes S as a quadratic covering of Q. If B denotes the automorphism group of Q defined by A, we have $v_\ell(A) = v_\ell(B)$ if $\ell > 2$ and $v_\ell(A) \leqslant v_\ell(B) + 1$ if $\ell = 2$. But B is isomorphic to a subgroup of $k^* \times \mathrm{Aut}(C)$, where C is a curve of genus 0. This implies

$$v_\ell(B) \leqslant \begin{cases} m+m+1 & \text{if} \quad \ell = 2 \\ m+m & \text{if} \quad t = 1 \\ 0+m & \text{if} \quad t = 2,\ l > 2 \\ 0+0 & \text{if} \quad t > 2. \end{cases}$$

The corresponding bound for $v_\ell(A)$ is $\leqslant M(k, \ell)$.

This concludes the proof of Th.4.1 and hence of Th.2.1.

§5 Structure and conjugacy properties of ℓ-subgroups of $\mathrm{Cr}(k)$

5.1 The ℓ-subgroups of $\mathrm{Cr}(k)$

The main theorem (Th.2.1) only gives information on the order of an ℓ-subgroup A of $\mathrm{Cr}(k)$, assuming as usual that $\ell \neq \mathrm{char}(k)$. As for the structure of A, we have :

Theorem 5.1. (i) *If $\ell > 3$, A is abelian of rank* $\leqslant 2$ (i.e. can be generated by two elements).

(ii). *If $\ell = 3$* (resp. $\ell = 2$) *A contains an abelian normal subgroup of rank $\leqslant 2$ with index $\leqslant 3$* (resp. with index $\leqslant 8$).

Proof. Most of this is a consequence of the results of [DI 07]; see also [Bl 06] and [Be07]. The only case which does not seem to be explicitly in [DI 07] is the case $\ell = 2$, when A is contained in $\mathrm{Aut}(S)$, where S is a conic bundle. Suppose we are in that case and let $f : S \to C$ and A_o, B be as in 4.3, so that we have an exact sequence $1 \to B \to A \to A_o \to 1$, with $A_o \subset \mathrm{Aut}(C)$, and $B \subset \mathrm{Aut}(F)$ where F is the generic fiber of f (which is a genus zero curve over the function field $k(C)$ of C). We use the following lemma :

Lemma 5.2. *Let $a \in A$ and $b \in B$ be such that a normalizes the cyclic group $\langle b \rangle$ generated by b. Then aba^{-1} is equal to b or to b^{-1}.*

Proof of the lemma. Let n be the order of b. If $n = 1$ or 2, there is nothing to prove. Assume $n > 2$. By extending scalars, we may also assume that k contains the primitive n-th roots of unity. Since b is an automorphism of F of order n, it fixes two rational points of Fwhich one can distinguish by the eigenvalue of b on their tangent space : one of them gives a primitive n-th root of unity z, and the other one gives $z' = z^{-1}$. [Equivalently, b fixes two sections of $f : S \to C$.] The pair (z, z') is canonically associated with b. Hence the pair associated with aba^{-1} is also (z, z'). On the other hand, if $aba^{-1} = b^i$ with $i \in \mathbf{Z}/n\mathbf{Z}$, then the pair associated to a^i is (z^i, z'^i). This shows that z^i is equal to either z or z^{-1}, hence $i \equiv 1$ or $-1 \pmod n$. The result follows.

End of the proof of Theorem 5.1 in the case $\ell = 2$. Since B is a finite 2-subgroup of a $k(C)$-form of $\mathbf{PGL}_2$, it is either cyclic or dihedral. In both cases, it contains a characteristic subgroup B_1 of index 1 or 2 which is cyclic. Similarly, A has a cyclic subgroup A_1 which is of index 1 or 2. Let $a \in A$ be such that its image in A_o generates A_1. If b is a generator of B_1, Lemma 5.2 shows that a^2 commutes with b. Let $\langle b, a^2\rangle$ be the abelian subgroup of A generated by b and a^2. It is normal in A, and the inclusions $\langle b, a^2\rangle \subset \langle b, a\rangle \subset B.\langle a\rangle \subset A$ show that its index in A is at most 8.

Remark. Similar arguments can be applied to prove a Jordan-style result on the finite subgroups of $\mathrm{Cr}(k)$, namely :

Theorem 5.3. *There exists an integer $J > 1$, independent of the field k, such that every finite subgroup G of* $\mathrm{Cr}(k)$*, of order prime to* $\mathrm{char}(k)$*, contains an abelian normal subgroup A of rank $\leqslant 2$, whose index in G divides J.*

The proof follows the same pattern : the conic bundle case is handled via Lemma 5.2 and the del Pezzo case via the fact that G has a subgroup of bounded index which is contained in a reductive group of rank $\leqslant 2$, so that one can apply the usual form of Jordan's theorem to that group. As for the value of J, a crude computation shows that one can take $J = 2^{10}.3^4.5^2.7$; the exponents of 2 and 3 can be somewhat lowered, but those of 5 and 7 cannot since $\mathrm{Cr}(\mathbf{C})$ contains $A_5 \times A_5$ and $\mathbf{PSL}_2(\mathbf{F}_7)$.

5.2 The cases $\mathbf{t} = 3, 4, 6$

More precise results on the structure of A depend on the value of the invariant $t = t(k, \ell)$. Recall that $t = 1, 2, 3, 4$ or 6 if $A \neq 1$, cf. Cor.2.2. We shall only consider the cases $t = 3, 4$ or 6 which are the easiest. See [DI 08, §4] for a (more difficult) conjugation theorem which applies when $t = 1$ or 2. Recall (cf. §3.2) that A is said to be *toral* if there exists a 2-dimensional subtorus T of Cr (in the sense of [De 70]) such that A is contained in $T(k)$. We have :

Theorem 5.4. *Assume that $t = 3, 4$ or 6. Then :*
(a) *A is cyclic of order ℓ^n with $n \leqslant m$.*
(b) *A is toral, except possibly if $|A| = 5$.*
(c) *If A' is a subgroup of* $\mathrm{Cr}(k)$ *of the same order as A, then A' is conjugate to A in* $\mathrm{Cr}(k)$*, except possibly if $|A| = 5$.*

Note that the hypothesis $t = 3, 4$ or 6 implies $\ell \geqslant 5$. Moreover, if $\ell = 5$, then $t = 4$ and, if $\ell = 7$, then $t = 3$ or 6.

Proof of (a) *and* (b). We follow the same method as above, i.e. we view A as a subgroup of $\mathrm{Aut}(S)$, where S is either a conic bundle or a del Pezzo surface. The bounds given in §4.3 show that $A = 1$ if S is a conic bundle (this is why this case is easier than the case $t = 1$ or 2). Hence we may assume that S is a del Pezzo surface. Let d be its degree. We have an exact sequence :

$$1 \to G(k) \to \mathrm{Aut}(S) \to E \to 1,$$

where $G = \mathrm{Aut}(S)^o$ is a connected linear group of rank $\leqslant 2$ and E is a subgroup of a Weyl group W depending on d (e.g. $W = \mathrm{Weyl}(E_8)$ if $d = 1$).

Consider first the case $\ell > 7$. The order of W is not divisible by ℓ ; hence A is contained in $G(k)$. Since A is commutative, there exists a maximal torus T of G such that A is contained in the normalizer N of T, cf. e.g. [Se 07, §3.3] ; since $\ell > 3$, the order of N/T is prime to ℓ, hence A is contained in $T(k)$ and this implies $\dim(T) \geqslant 2$ by [Se 07, §4.1]. This proves (b), and (a) follows from Lemma 5.5 below.

Suppose now that $\ell = 5$ or 7, and let $n = v_\ell(A)$. If $n = 1$ and $\ell = 5$, there is nothing to prove. If $n = 1$ and $\ell = 7$, then (a) is obvious and (b) is proved in [DI 08, prop.3] (indeed Dolgachev and Iskovskikh prove (b) when $v_\ell(A) = 1$, and they also prove (c) for $\ell = 7$). We may thus assume that $n > 1$. If $d \leqslant 5$, then $G = 1$ and A embeds in E ; but E does not contain any subgroup of order ℓ^2 (see the tables in [DI 07] and [Bl 06]) ; hence this case does not occur. If $d > 5$, then the order of E is prime to ℓ, hence A is contained in $G(k)$ and the proof above applies.

Proof of (c). By (b), we have $A \subset T(k)$ and $A' \subset T'(k)$ where T and T' are 2-dimensional subtori of Cr. By Lemma 5.5 below, these tori are isomorphic ; by a standard argument (see e.g. [De 70, §6] this implies that T and T' are conjugate by an element of $\mathrm{Cr}(k)$; moreover A (resp. A') is the unique subgroup of order ℓ^n of $T(k)$ (resp. of $T'(k)$). Hence A and A' are conjugate in $\mathrm{Cr}(k)$.

Remark. The case $|A| = 5$ is indeed exceptional : there are examples of such A's which are not toral, cf. [Be 07], [Bl 06], [DI 07].

5.3 A uniqueness result for 2-dimensional tori

We keep the assumption that $t = 3, 4$ or 6. We have seen in §3.2.2 that there exists a 2-dimensional k-torus T such that $T(k)$ contains an element of order ℓ.

Lemma 5.5. (a) *Such a torus is unique, up to k-isomorphism.*
(b) *If* $n \leqslant m = m(k, \ell)$*, then* $T(k)[\ell^n]$ *is cyclic of order* ℓ^n.

Proof of (a). Let $L = \mathrm{Hom}_{k_s}(\mathbf{G}_m, T)$ be the group of cocharacters of T. It is a free $\mathbf{Z}$-module of rank 2, with an action of $\Gamma_k = \mathrm{Gal}(k_s/k)$. If we identify L with $\mathbf{Z}^2$, this action gives a homomorphism $r : \Gamma_k \to \mathbf{GL}_2(\mathbf{Z})$ which is well defined up to conjugation. Let G be the image of r. Since G is a finite subgroup of $\mathbf{GL}_2(\mathbf{Z})$, its order divides 24, and hence is prime to ℓ.

The Γ_k-module $T(k_s)[\ell]$ of the ℓ-division points of $T(k_s)$ is canonically isomorphic to $L/\ell L \otimes \mu_\ell$, where μ_ℓ is the group of ℓ-th roots of unity in k_s. This means that $L/\ell L$ contains a rank-1 submodule I which is isomorphic to the dual μ_ℓ^* of μ_ℓ. The action of G on $L/\ell L$ is semisimple since $|G|$ is prime to ℓ. Hence there exists a rank-1 submodule J of $L/\ell L$ such that $L/\ell L = I \bigoplus J$. By a well-known lemma of Minkowski (see e.g. [Se 07, Lemma 1]), the action of G on $L/\ell L$ is faithful. This shows that G is commutative. Moreover, the character giving the action of Γ_k on I has an image which is cyclic of order t. Since $t = 3, 4$

or 6, this shows that G contains an element of order 3 or 4. One checks that these properties imply $G \subset \mathbf{SL}_2(\mathbf{Z})$ i.e. $\det(r) = 1$, hence the Γ_k-modules I and J are dual of each other, i.e. $J \simeq \mu_\ell$. We thus have $L/\ell L \simeq \mu_l \oplus \mu_\ell^*$. We may then identify r with the homomorphism $\Gamma_k \to C_t \to \mathbf{GL}_2(\mathbf{Z})$, where C_t is the Galois group of $k(\mu_\ell/k)$ and $C_t \to \mathbf{GL}_2(\mathbf{Z})$ is an inclusion. Since any two such inclusions only differ by an inner automorphism of $\mathbf{GL}_2(\mathbf{Z})$, this shows that the Γ_k-module L is unique, up to isomorphism; hence the same is true for T.
Proof of (b). Assertion (b) follows from the description of T given in §3.2.2. It can also be checked by writing explicitly the Γ_k-module $L/\ell^n L$; when $n \leqslant m$ this module is isomorphic to the direct sum of μ_{ℓ^n} and its dual.

Remarks.

1). If $n > m$ we have $T(k)[\ell^n] = T(k)[\ell^m]$. This can be seen, either by a direct computation of ℓ-adic representations, or by looking at §3.2.2

2) When $t = 1$ or 2, it is natural to ask for a 2-dimensional torus T such that $T(k)$ contains $\mathbf{Z}/\ell Z \oplus \mathbf{Z}/\ell\mathbf{Z}$. Such a torus exists, as we have seen in §3.2. If $\ell > 2$, it is unique, up to isomorphism. There is a similar result for $\ell = 2$, if one asks not merely that $T(k)$ contains $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ but that it contains $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

§6 The Cremona groups of rank > 2

For any $r > 0$ the Cremona group $\mathrm{Cr}_r(k)$ of rank r is defined as the group $\mathrm{Aut}_k\, k(T_1, ..., T_r)$ where $(T_1, ..., T_r)$ are r indeterminates. When $r > 2$ not much seems to be known on the finite subgroups of $\mathrm{Cr}_r(k)$, even in the classical case $k = \mathbf{C}$. For instance :

6.0. *Does there exist a finite group which is not embeddable in* $\mathrm{Cr}_3(\mathbf{C})$?

This looks very likely, but I do not see how to prove it. Still, it is natural to ask for much more, e.g. :

6.1 (Jordan bound, cf. Th.5.5). *Does there exist an integer $N(r) > 0$, depending only on r, such that, for every finite subgroup G of* $\mathrm{Cr}_r(k)$ *of order prime to* $\mathrm{char}(k)$, *there exists an abelian normal subgroup A of G, of rank $\leqslant r$, whose index divides $N(r)$?*

Note that this would imply that, for ℓ large enough (depending on r), every finite ℓ-subgroup of $\mathrm{Cr}_r(k)$ is abelian of rank $\leqslant r$.

6.2 (cf. [Se 07, §6.9]). *Is it true that $r \geqslant \varphi(t)$ if* $\mathrm{Cr}_r(k)$ *contains an element of order ℓ ?*

6.3. *Let $G \subset$* $\mathrm{Cr}_r(k)$ *be as in* 6.1, *and assume that k is small* (cf. §2.3).*Is it true that $|G|$ is bounded by a constant depending only on r and k ?*

If the answer to 6.3 is " yes " we may define $M_r(k)$ as the l.c.m. of all such $|G|$'s, and ask for an estimate of $M_r(k)$. For instance, in the case $r = 3$:

6.4. *Is it true that $M_3(k)$ is equal to $M_1(k).M_2(k)$?*

If k is finite with q elements, this means (cf. §2.5) :

6.5. *Is it true that*

$$M_3(k) = \begin{cases} 3.(q^2-1)(q^4-1)(q^6-1) & \textit{if } q \equiv 4 \textit{ or } 7 \pmod 9 \\ (q^2-1)(q^4-1)(q^6-1) & \textit{otherwise } ? \end{cases}$$

For larger r's the polynomial $(X^2-1)(X^4-1)(X^6-1)$ of 6.5 should be replaced by the polynomial $P_r(X)$ defined by the formula

$$P_r(X) = \prod_d \Phi_d(X)^{[r/\varphi(d)]} \quad ,$$

where $\Phi_d(X)$ is the d-th cyclotomic polynomial ($\Phi_1(X) = X-1,\ \Phi_2(X) = X+1,\ \Phi_3(X) = X^2+X+1,\ \Phi_4(X) = X^2+1, ...$).

Examples. $P_4(X) = (X^6-1)(X^8-1)(X^{10}-1)(X^{12}-1)$; $P_5(X) = (X^2-1)P_4(X)$.

With this notation, the natural question to ask seems to be :

6.6. *Is it true that there exists an integer $c(r) > 0$ such that $M_r(\mathbf{F}_q)$ divides $c(r).P_r(q)$ for every q ?*

Unfortunately, I do not see any way to attack these questions; the method used for rank 2 is based on the very explicit knowledge of the "minimal models", and this is not available for higher ranks. Other methods are needed.

Acknowlegment. I wish to thank A.Beauville for a series of e-mails in 2003 − 2005 which helped me to correct the naive ideas I had on the Cremona group.

References

[Be 07] A.Beauville, *p-elementary subgroups of the Cremona group*, J.of Algebra **314** (2007), 553 − 564.

[Bl 06] J.Blanc, *Finite abelian subgroups of the Cremona group of the plane*, Univ.Genève, thèse no 3777 (2006). See also C.R.A.S. **344** (2006), 21 − 26.

[De 70] M.Demazure, *Sous-groupes algébriques de rang maximum du groupe de Cremona*, Ann.Sci.ENS (4) **3** (1970), 507 − 588. MR 44.1672.

[De 80] M.Demazure, *Surfaces de Del Pezzo*, I-IV, Lect.Notes in Math.**777**, Springer-Verlag, 1980, pp.21 − 69.

[Do 07] I.V.Dolgachev, *Topics in Classical Algebraic Geometry, Part I*, Lecture notes, Univ. Michigan, Ann Arbor 2007.

[DI 07] I.V.Dolgachev and V.A.Iskovskikh, *Finite subgroups of the plane Cremona group*, ArXiv :math/0610595v2, to appear in *Algebra, Arithmetic and Geometry, Manin's Festschrift*, Progress in Math. Birkhäuser Boston, 2008.

[DI 08] I.V.Dolgachev and V.A.Iskovskikh, *On elements of prime order in the plane Cremona group over a perfect field*, ArXiv :math/0707.4305, to appear.

[Is 79] V.A.Iskovskikh, *Minimal models of rational surfaces over arbitrary fields* (in Russian), Izv.Akad.Nauk **43** (1979) , 19 − 43; English translation : Math.USSR Izvestija **14**(**1980**), 17 − 39. MR 80m :14021.

[Is 96] V.A.Iskovskikh, *Factorization of birational maps of rational surfaces from the viewpoint of Mori theory* (in Russian), Uspekhi Math.Nauk **51**(**1996**), 3 − 72; English translation : Russian Math.Surveys **51** (1996), 585 − 652. MR 97k :14016.

[Ko 96] J.Kollár, *Rational Curves on Algebraic Varieties*, Ergebn.Math. (3) **32**, Springer-Verlag, 1996. MR 98c :14001.

[Ma 66] Y.I.Manin, *Rational surfaces over perfect fields* (in Russian, with English résumé), Publ.Math.IHES **30**(**1966**), 415 – 475. MR 37.1373.

[Ma 86] Y.I.Manin, *Cubic Forms : Algebra, Geometry, Arithmetic*, 2nd edition, North Holland, Amsterdam, 1986. MR 87d :11037.

[Se 07] J-P.Serre, *Bounds for the orders of the finite subgroups of* $G(k)$*,* in *Group Representation Theory*, eds. M.Geck, D.Testerman & J. Thévenaz, EPFL Press, Lausanne, 2007, pp. 403 – 450.

[Vo 98] V.E.Voskresenskii, *Algebraic Groups and Their Birational Invariants*, Translations Math. Monographs **179**, AMS, 1998. MR 99g :20090.

Collège de France
3, rue d'Ulm
F-75231 Paris Cedex 05

e-mail : serre@noos.fr