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 \( \text{Cr}(k) \) 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 \( \text{Cr}(k) \) of order prime to the characteristic of \( k \). The case \( k = \mathbb{C} \) 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], one finds a few questions in that direction, for instance the following:

If \( k = \mathbb{Q} \), is it true that \( \text{Cr}(k) \) does not contain any element of prime order \( \geq 11 \)?

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

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

\( \text{Cr}(k) \) contains an element of order \( \ell \)
and
\[ [k(z_\ell) : k] = 1, 2, 3, 4 \text{ or } 6, \] where \( z_\ell \) is a primitive \( \ell \)-th root of unity.

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

For instance:

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

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

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

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

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 \( \text{Cr}(k) \) as a subgroup of \( \text{Aut}(S) \), 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 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 \( \ell \) be a prime number distinct from \( \text{char}(k) \); the \( \ell \)-adic valuation of \( \mathbb{Q} \) is denoted by \( v_\ell \). If \( A \) is a finite set, with cardinal \( |A| \), we write \( v_\ell(A) \) instead of \( v_\ell(|A|) \).

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

1.1 Definition of \( t \)

Let \( z \in k_s \) be a primitive \( \ell \)-th root of unity if \( \ell > 2 \) 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 \( \ell^n \)-th roots of unity. We have \( m \geq 1 \).

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 \( m \geq 2 \). [The definition of \( m \) given in [Se 07, §4.2] looks different, but it is equivalent to the one here.]

Remark. When \( \ell > 2 \), knowing \( t \) and \( m \) amounts to knowing the image of the \( \ell \)-th cyclotomic character \( \text{Gal}(k_s/k) \to \mathbb{Z}_\ell^* \), cf. [Se 07, §4].

1.3 Example : \( k = \mathbb{Q} \)

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 :

$t = \text{order of } q \text{ in the multiplicative group } F_\ell^*$
$m = v_\ell(q^t - 1) = v_\ell(q^t - 1) - 1)$.

If $\ell = 2$, one has :

$t = \text{order of } q \text{ in } (\mathbb{Z}/4\mathbb{Z})^*$
$m = v_2(q^2 - 1) - 1$.

§2 Statement of the main theorem

Let $K = k(X,Y)$, where $X, Y$ are indeterminates, and let $\text{Cr}(k)$ be the Cremona group of rank 2 over $k$, i.e. the group $\text{Aut}_k K$. Let $\ell$ be a prime number, distinct from 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 $\ell = 2$, $M(k, \ell) = 2m + 3$.

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

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

2.2 The main theorem

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

(ii) Conversely, if $n$ is any integer $\geq 0$ which is $\leq M(k, \ell)$, then $\text{Cr}(k)$ contains a subgroup of order $\ell^n$.

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

The special case where $A$ is cyclic of order $\ell$ gives :

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

a) $\text{Cr}(k)$ contains an element of order $\ell$

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

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

3
2.3 Small fields

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

\begin{align*}
(2.3.1) & \quad m(k, \ell) < \infty \text{ for every } \ell \neq \text{char}(k) \\
(2.3.2) & \quad t(k, \ell) \to \infty \text{ when } \ell \to \infty.
\end{align*}

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

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

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

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

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

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

**Theorem 2.4.** If $k$ is small, then the finite subgroups of $\text{Cr}(k)$ of order prime to 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 $k = \mathbb{Q}$

By combining 1.3 and 2.1, one gets

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

This can be summed up by:

**Theorem 2.5.** $M(\mathbb{Q}) = 2^7.3^3.5.7.$
2.5 Example : the case of a finite field

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

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

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

If $\ell$ 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 $q^t = 1 \pmod{\ell}$. 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 $\ell$ and $q^6 - 1$ is divisible by $\ell$; 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 $\ell$ is $q^4 - 1$ and its $\ell$-adic valuation is $m$. When $t = 1$ or 2, both factors are divisible by $\ell$ and their $\ell$-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 :

$$M(F_2) = 3^2.5.7; \quad M(F_3) = 2^7.5.7.13; \quad M(F_4) = 3^4.5^2.7.13.17;$$

$$M(F_5) = 2^7.3^2.7.13.31; \quad M(F_7) = 2^9.3^4.5^2.19.43.$$  

2.6 Example : the $p$-adic field $Q_p$

For $\ell \neq p$, the $t, m$ invariants of $Q_p$ are the same as those of $F_\ell$ , and for $\ell = p$ they are the same as those of $Q$.

This shows that $Q_p$ is “ small ”, and a simple computation gives

$$M(Q_p) = c(p).p(p^4 - 1)(p^6 - 1),$$

with

$$\begin{align*}
\text{c}(2) &= 2^7; \quad \text{c}(3) = 3^3; \quad \text{c}(5) = 5; \quad \text{c}(7) = 3.7; \\
\text{c}(p) &= 3 \text{ if } p > 7 \text{ and } p \equiv 4 \text{ or } 7 \pmod{9}; \\
\text{c}(p) &= 1 \text{ otherwise.}
\end{align*}$$

For instance :

$$M(Q_2) = 2^7.3^2.5.7; \quad M(Q_3) = 2^7.3^2.5.7.13; \quad M(Q_5) = 2^7.3^3.5.7.13.31;$$

$$M(Q_7) = 2^9.3^4.5^2.7.19.43; \quad M(Q_{11}) = 2^7.3^3.5^2.7.19.37.61.$$
2.7 Remarks

1. The statement of Theorem 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 $GL_2(\mathbb{Z})$. See also §6.

2. Even though Theorem 2.6 is a very special case of Theorem 2.1, it contains almost as much information as the general case. More precisely, we could deduce Theorem 2.1.(i) [which is the hard part] from Theorem 2.6 by the Minkowski method of reduction (mod $p$) explained in [Se 07, §6.5].

3. In the opposite direction, if we know Theorem 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 (for a detailed proof, see [Se 08, §5]).

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

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

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

§3 Proof of Theorem 2.1.(ii)

We have to construct large $\ell$-subgroups of $Cr(k)$. 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 $Cr(k)$ 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-\( r \)d root of unity.

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

### 3.2 The generic case

Here is the general construction:

One starts with a 2-dimensional torus \( T \) over \( k \), with an \( \ell \)-group \( C \) acting faithfully on it. Let \( B \) be an \( \ell \)-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 \( \text{Aut}(k(T)) \), where \( k(T) \) is the function field of \( T \). By a theorem of Voskresinskiĭ (see [Vo 98, §4.9]) \( k(T) \) is isomorphic to \( K = k(X,Y) \).

We thus get an embedding of \( A \) in \( \text{Cr}(k) \). Note that \( B \) is toral, i.e. is contained in the \( k \)-rational points of a maximal torus of \( \text{Cr} \).

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

#### 3.2.1 The case \( \ell = 2 \)

Let \( n \) be an integer \( \leq m \). 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 \( \mathbb{G}_m \) 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 \( \text{Cr}_1(k) = \text{PGL}_2(k) \) contains a dihedral subgroup \( D \) of order \( 2^n+1 \); by using the natural embedding of \( (\text{Cr}_1(k)\times \text{Cr}_1(k)).2 \) in \( \text{Cr}(k) \) we obtain a subgroup of \( \text{Cr}(k) \) 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 \( n \leq m \). 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 \( \text{GL}_2(\mathbb{Z}) \), with the condition that, if \( t = 2 \), then the image of \( C_t \) is \( \{1,-1\} \). The composition map

\[ r : \Gamma_k \to \text{Gal}(k(z)/k) = C_t \to \text{GL}_2(\mathbb{Z}) \]

defines a 2-dimensional torus \( T \).

7
The group $B$ is the subgroup $T(k)[\ell^n]$ of $T(k)$ made up of elements of order dividing $\ell^n$. We take $C$ equal to 1, except when $\ell = 3$ 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 $\text{GL}_2(\mathbb{Z})$). We thus have:

$$v_t(A) = v_t(B) = 2n$$

It remains to estimate $v_t(B)$. Namely:

(3.2.3) $v_t(B) = 2n$ 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 $\Gamma_k \to \text{Gal}(k(z)/k)$. 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 $v_t(B) = 2n$.

(3.2.4) $v_t([B]) \geq n$ 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 $C_t = \text{Gal}(L/k)$. Let $T_L = R_{L/k}(G_m)$ 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 $\text{End}(T_L)$. Let $F(X)$ be the cyclotomic polynomial of index $t$, i.e.

$$F(X) = X^t - 1$$

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 $\ell^n$. This shows that $v_t(B) \geq n$.

[When $t = 3$, we could have defined $T$ as the kernel of the norm map $N : T_1 \to G_m$. 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 Theorem 2.1.

§4 Proof of Theorem 2.1.(i)

4.1 Generalization

In Theorem 2.1.(i), the hypothesis made on the $\ell$-group $A$ is that it is contained in $\text{Cr}(k)$. This is equivalent to saying that $A$ is contained in $\text{Aut}(S)$, 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 $K$; 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:

\[(4.1.1) \quad \overline{k} \otimes L \text{ is } \overline{k}\text{-isomorphic to } \overline{k}(X, Y).\]

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

**Theorem 4.1.** If a finite $\ell$-group $A$ has property $\text{Cr}_k$, then $v_\ell(A) \leq M(k, \ell)$, 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 $M(k, \ell)$.

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

### 4.2 Reduction to special cases

We start from an $\ell$-group $A$ having property $\text{Cr}_k$. As explained above, this means that we can embed $A$ in $\text{Aut}(S)$, 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 $1 \leq \deg(S) \leq 9$.

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 $\text{char}(k)$.

### 4.3 The conic bundle case

Let $f : S \to C$ be as in a) above, and let $A_o$ be the subgroup of $\text{Aut}(C)$ given by the action of $A$ on $C$. The group $\text{Aut}(C)$ is a $k$-form of $\text{PGL}_2$. By using (for instance) [Se 07, Theorem 5] we get:
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:

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

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

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

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

### 4.5 The Del Pezzo case: degree 8

This case splits into two subcases:

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

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

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

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

10
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 $v_\ell(A_0) \leq m$ given above can be replaced by $v_\ell(A_0) = 0$, 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 $\mathbb{F}$), 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 $\text{Pic}(S)^A$ be equal to 1.]

4.7 The Del Pezzo case: degree 6

Here the surface $S$ has 6 exceptional curves (over $\mathbb{F}$); their incidence graph $\Sigma$ is an hexagon. There is a natural homomorphism

$$g : \text{Aut}(S) \to \text{Aut}(\Sigma)$$

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, Theorem 4], we have

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

Hence:

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

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

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

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

4.8 The Del Pezzo case: degree 5

As above, let $\Sigma$ be the incidence graph of the exceptional curves of $S$. Since $\deg(S) \leq 5$, the natural map $\text{Aut}(S) \to \text{Aut}(\Sigma)$ is injective. We can thus identify $A$ with its image in $\text{Aut}(\Sigma)$. In the case $\deg(S) = 5$, the graph $\Sigma$ is the Petersen graph, and $\text{Aut}(\Sigma)$ is isomorphic to the symmetric group $S_5$. This shows that

$$v_\ell(A) \leq \begin{cases} 3 & \text{if } \ell = 2 \\ 1 & \text{if } \ell = 3 \text{ or } 5 \\ 0 & \text{if } \ell > 5, \end{cases}$$
and we conclude as before.

4.9 The Del Pezzo case: degree 4

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

4.10 The Del Pezzo case: degree 3

Here \( S \) is a smooth cubic surface, and \( A \) embeds in \( \text{Weyl}(E_6) \), 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 \( v_\ell(A) \leq 4 \), but Theorem 2.1 claims \( v_\ell(A) \leq 3 \) 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 \( \text{char}(k) \neq 3 \). 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 \( \text{Weyl}(E_6) \). In particular the center \( Z(A) \) of \( A \) is cyclic of order 3 and is contained in the commutator subgroup of \( A \). 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 \( r : A \to \text{GL}_4(k) \). 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 \( \text{Weyl}(E_7) \), a group of order \( 2^{10}.3^4.5.7 \). This gives a bound for \( v_\ell(A) \), but this bound is not good enough. However, the surface \( S \) is a 2-sheeted covering of \( \mathbb{P}_2 \) (the map \( S \to \mathbb{P}_2 \) being the anticanonical map) and we get a homomorphism \( g : A \to \text{PGL}_3(k) \) 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 \( g : S \to \mathbb{P}_3 \) 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 \( v_\ell(A) \leq v_\ell(B) + 1 \) if \( \ell = 2 \). But \( B \) is isomorphic to a subgroup of \( k^* \times \text{Aut}(C) \), where \( C \) is a curve of genus 0. This implies
\[ v_\ell(B) \leq \begin{cases} 
  m + m + 1 & \text{if } \ell = 2 \\
  m + m & \text{if } t = 1 \\
  0 + m & \text{if } t = 2, \ell > 2 \\
  0 + 0 & \text{if } t > 2.
\end{cases} \]

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

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

§5 Structure and conjugacy properties of \( \ell \)-subgroups of \( \text{Cr}(k) \)

5.1 The \( \ell \)-subgroups of \( \text{Cr}(k) \)

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

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

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

**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 \( \text{Aut}(S) \), 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 \( A_o \subset \text{Aut}(C) \), and \( B \subset \text{Aut}(F) \) 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 \( F \) which 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 \( i \in \mathbb{Z}/n\mathbb{Z} \), 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 \( \text{PGL}_2 \), 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 \( \text{Cr}(k) \), namely :

**Theorem 5.3.** There exists an integer \( J > 1 \), independent of the field \( k \), such that every finite subgroup \( G \) of \( \text{Cr}(k) \), of order prime to \( \text{char}(k) \), contains an abelian normal subgroup \( A \) of rank \( \leq 2 \), 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 \( \leq 2 \), 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 \( J = 2^{10} \cdot 3^4 \cdot 5^2 \cdot 7 \); the exponents of 2 and 3 can be somewhat lowered, but those of 5 and 7 cannot since \( \text{Cr}(C) \) contains \( A_5 \times A_5 \) and \( \text{PSL}_2(F_7) \).

### 5.2 The cases \( t = 3, 4, 6 \)

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 \( \text{Cr}(k) \) (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 \( \ell^n \) with \( n \leq m \).

(b) \( A \) is toral, except possibly if \( |A| = 5 \).

(c) If \( A' \) is a subgroup of \( \text{Cr}(k) \) of the same order as \( A \), then \( A' \) is conjugate to \( A \) in \( \text{Cr}(k) \), except possibly if \( |A| = 5 \).

Note that the hypothesis \( t = 3, 4 \) or 6 implies \( \ell \geq 5 \). 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 \( \text{Aut}(S) \), 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 :

\[ 1 \to G(k) \to \text{Aut}(S) \to E \to 1, \]
where \( G = \text{Aut}(S)^o \) is a connected linear group of rank \( \leq 2 \) and \( E \) is a subgroup of a Weyl group \( W \) depending on \( d \) (e.g. \( W = \text{Weyl}(E_8) \) if \( d = 1 \)).

Consider first the case \( \ell > 7 \). The order of \( W \) is not divisible by \( \ell \); 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. \([\text{Se} 07, \S 3.3]\); since \( \ell > 3 \), the order of \( N/T \) is prime to \( \ell \), hence \( A \) is contained in \( T(k) \) and this implies \( \dim(T) \geq 2 \) by \([\text{Se} 07, \S 4.1]\). 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 \([\text{DI} 08, \text{prop.3}]\) (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 \( d \leq 5 \), then \( G = 1 \) and \( A \) embeds in \( E \); but \( E \) does not contain any subgroup of order \( \ell^2 \) (see the tables in \([\text{DI} 07]\) and \([\text{Bl} 06]\)); hence this case does not occur. If \( d > 5 \), then the order of \( E \) is prime to \( \ell \), 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 \( \text{Cr} \). By Lemma 5.5 below, these tori are isomorphic; by a standard argument (see e.g. \([\text{De} 70, \S 6]\) this implies that \( T \) and \( T' \) are conjugate by an element of \( \text{Cr}(k) \); moreover \( A \) (resp. \( A' \)) is the unique subgroup of order \( \ell^n \) of \( T(k) \) (resp. of \( T'(k) \)). Hence \( A \) and \( A' \) are conjugate in \( \text{Cr}(k) \).

**Remark.** The case \( |A| = 5 \) is indeed exceptional: there are examples of such \( A \)'s which are not toral, cf. \([\text{Be} 07], [\text{Bl} 06], [\text{DI} 07]\).

### 5.3 A uniqueness result for 2-dimensional tori

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

**Lemma 5.5.** (a) Such a torus is unique, up to \( k \)-isomorphism.

(b) If \( n \leq m = m(k, \ell) \), then \( T(k)[\ell^n] \) is cyclic of order \( \ell^n \).

**Proof of (a).** Let \( L = \text{Hom}_{k}(G_m, T) \) be the group of cocharacters of \( T \). It is a free \( \mathbb{Z} \)-module of rank 2, with an action of \( \Gamma_k = \text{Gal}(k_s/k) \). If we identify \( L \) with \( \mathbb{Z}^2 \), this action gives a homomorphism \( r : \Gamma_k \to GL_2(\mathbb{Z}) \) which is well defined up to conjugation. Let \( G \) be the image of \( r \). Since \( G \) is a finite subgroup of \( GL_2(\mathbb{Z}) \), its order divides 24, and hence is prime to \( \ell \).

The \( \Gamma_k \)-module \( T(k_s)[\ell] \) of the \( \ell \)-division points of \( T(k_s) \) is canonically isomorphic to \( L/\ell L \otimes \mu_\ell \), where \( \mu_\ell \) is the group of \( \ell \)-th roots of unity in \( k_s \). This shows that \( L/\ell L \) contains a rank-1 submodule \( I \) which is isomorphic to the dual \( \mu_\ell^* \) of \( \mu_\ell \). The action of \( G \) on \( L/\ell L \) is semisimple since \( |G| \) is prime to \( \ell \). Hence there exists a rank-1 submodule \( J \) of \( L/\ell L \) such that \( L/\ell L = I \oplus J \). By a well-known lemma of Minkowski (see e.g. \([\text{Se} 07, \text{Lemma 1}]\)), the action of \( G \) on \( L/\ell L \) is faithful. This shows that \( G \) is commutative. Moreover, the character giving the action of \( \Gamma_k \) on \( I \) has an image which is cyclic of order \( \ell \). Since \( t = 3 \), 4
or 6, this shows that $G$ contains an element of order 3 or 4. One checks that these properties imply $G \subset \text{SL}_2(\mathbb{Z})$ i.e. $\det(r) = 1$, hence the $\Gamma_k$-modules $I$ and $J$ are dual of each other, i.e. $J \simeq \mu_\ell$. We thus have $L/\ell L \simeq \mu_\ell \oplus \mu_\ell^*$. We may then identify $r$ with the homomorphism $\Gamma_k \to C_\ell \to \text{GL}_2(\mathbb{Z})$, where $C_\ell$ is the Galois group of $k(\mu_\ell/k)$ and $C_\ell \to \text{GL}_2(\mathbb{Z})$ is an inclusion. Since any two such inclusions only differ by an inner automorphism of $\text{GL}_2(\mathbb{Z})$, this shows that the $\Gamma_k$-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 $\Gamma_k$-module $L/\ell^nL$; when $n \leq m$ this module is isomorphic to the direct sum of $\mu_{\ell^n}$ 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 $\ell$-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 $\mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$. 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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ but that it contains $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

§6 The Cremona groups of rank $> 2$

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

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

This looks very likely. It is natural to ask for much more, for instance:

6.1 (Jordan bound, cf. Theorem 5.3). Does there exist an integer $N(r) > 0$, depending only on $r$, such that, for every finite subgroup $G$ of $\text{Cr}_r(k)$ of order prime to $\text{char}(k)$, there exists an abelian normal subgroup $A$ of $G$, of rank $\leq r$, whose index divides $N(r)$?

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

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

6.3. Let $G \subset \text{Cr}_r(k)$ 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 the cyclotomic invariants $(t,m)$ of $k$?

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):

16
6.5. Is it true that
\[
M_3(k) = \begin{cases} 
3(q^2 - 1)(q^4 - 1)(q^6 - 1) & \text{if } q \equiv 4 \text{ or } 7 \pmod{9} \\
(q^2 - 1)(q^4 - 1)(q^6 - 1) & \text{otherwise}
\end{cases}
\]

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
\[
P_r(X) = \prod_d \Phi_d(X)^{[r/\varphi(d)]},
\]
where $\Phi_d(X)$ is the $d$-th cyclotomic polynomial.

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 $M_r(F_q)$ divides $c(r)P_r(q)$ for every $q$?

Unfortunately, I do not see how to attack these questions; the method used for rank 2 is based on the detailed knowledge of the “minimal models”, and this is not available for higher ranks.

Acknowledgment. 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 groups.

References

[Be 07] A. Beauville, p-elementary subgroups of the Cremona group, J. Algebra 314 (2007), 553-564.
[BI 06] J. Blanc, Finite abelian subgroups of the Cremona group of the plane, Univ. Genève, thèse n° 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.
[De 80] M. Demazure, Surfaces de Del Pezzo, I-IV, Lect. Notes in Math. 777, Springer-Verlag, 1980, 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.
[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.
[Ko 96] J.Kollár, *Rational Curves on Algebraic Varieties*, Ergebn.Math. (3) 32, Springer-Verlag, 1996.

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

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

[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, 403-450.

[Se 08] J-P. Serre, *Le groupe de Cremona et ses sous-groupes finis*, Sémin. Bourbaki 2008/2009, exposé 1000.

[Vo 98] V.E. Voskresenski˘ı, *Algebraic Groups and Their Birational Invariants*, Translations Math. Monographs 179, AMS, 1998.

Collège de France
3, rue d’Ulm
F-75231 Paris Cedex 05
e-mail : serre@noos.fr