Séminaire BOURBAKI Novembre 2008
61ème année, 2008-2009, n° 1000

LE GROUPE DE CREMONA ET SES SOUS-GROUPES FINIS

par **Jean–Pierre SERRE**

Qu'est-ce que le *groupe de Cremona*? Pour un géomètre, c'est le groupe des transformations birationnelles du plan (affine ou projectif, peu importe) dans lui-même. Pour un algébriste, c'est le groupe des k-automorphismes du corps $k(t_1, t_2)$ où t_1, t_2 sont des indéterminées, et k est un corps (le plus souvent $\mathbf{C}$). Ces groupes ont été beaucoup étudiés dans les 150 dernières années. Le présent exposé se bornera à en décrire les *sous-groupes finis*, dans un cadre un peu plus large que celui où $k = \mathbf{C}$; nous nous intéresserons par exemple au cas où le corps k est égal à $\mathbf{Q}$ ou à un corps fini, cf. §§ 2-5. Le § 1 contient quelques définitions préliminaires, ainsi qu'un « théorème de fusion » pour le tore standard du groupe de Cremona.

1. TORE STANDARD ET FUSION

1.1. Définitions et exemples

Soit k un corps et soit n un entier ≥ 1. On note $\mathrm{Cr}_n(k)$ le groupe des k-automorphismes de $k(t_1, ..., t_n)$ où les t_i sont des indéterminées indépendantes ; c'est le groupe de Cremona de rang n (ou plutôt le groupe de ses k-points, cf. [De 70, § 1]).

On a par exemple $\mathrm{Cr}_1(k) = \mathbf{PGL}_2(k)$. Par la suite, on s'intéressera surtout[(1)] au cas $n = 2$ et l'on écrira alors Cr à la place de Cr_2.

Soit X une k-variété géométriquement irréductible réduite dont le corps des fonctions $k(X)$ soit isomorphe à $k(t_1, ..., t_n)$ (autrement dit une variété k-rationnelle). Choisissons un isomorphisme entre $k(X)$ et $k(t_1, ..., t_n)$. Tout élément de $\mathrm{Cr}_n(k)$ peut alors être identifié à un automorphisme birationnel $X \dashrightarrow X$, autrement dit à un « pseudoautomorphisme » de X au sens de [De 70, § 1.2]. Suivant ce que l'on veut faire, on prendra pour X l'espace affine $\mathbf{Aff}^n$, l'espace projectif $\mathbf{P}_n$ ou le tore standard $T = (\mathbf{G}_m)^n$, cf. § 1.2 ci-dessous.

[(1)]On trouvera dans [Se 09, § 6] quelques conjectures (ou « questions ») sur le cas $n \geqslant 3$, mais je ne suis pas sûr qu'elles soient raisonnables.

Exemples de sous-groupes de $\mathrm{Cr}_n(k)$ pour $n = 2$

a) Prenons $X = \mathbf{P}_2$. On a $\mathrm{Aut}_k(X) = \mathbf{PGL}_3(k)$; comme un automorphisme birégulier est *a fortiori* birationnel, on obtient un plongement de $\mathbf{PGL}_3(k)$ dans $\mathrm{Cr}(k)$. (Du point de vue de [De 70], où l'on regarde Cr comme un foncteur en groupes, on a un plongement de $\mathbf{PGL}_3$ dans Cr ; on n'a pas besoin de mentionner k.)

b) Prenons $X = \mathbf{P}_1 \times \mathbf{P}_1$; on obtient ainsi un plongement de $\mathbf{PGL}_2 \times \mathbf{PGL}_2$ dans Cr.

c) (de Jonquières) Soit $a \in \mathbf{PGL}_2(k)$, et soit $b_t \in \mathbf{PGL}_2(k(t))$. Le couple (a, b_t) définit un élément g_{a,b_t} de $\mathrm{Cr}(k)$ par

$$(t_1,\ t_2) \ \mapsto \ (a(t_1),\ b_{t_1}(t_2)).$$

[*Exemple* : $(t_1,\ t_2) \ \mapsto (1/t_1,\ (t_1^3 + t_2)/(t_1 t_2 + 1))$.]

Les g_{a,b_t} forment un sous-groupe de $\mathrm{Cr}(k)$ isomorphe au produit semi-direct de $\mathbf{PGL}_2(k)$ par $\mathbf{PGL}_2(k(t))$. On peut l'interpréter comme le groupe des transformations birationnelles de $\mathbf{P}_1 \times \mathbf{P}_1$ qui sont compatibles avec la première projection : $\mathbf{P}_1 \times \mathbf{P}_1 \ \to \ \mathbf{P}_1$.

1.2. Le tore standard et son normalisateur

Soit T le produit de n exemplaires du groupe multiplicatif $\mathbf{G}_m$. Ce tore opère de façon évidente (par multiplication des coordonnées) sur $\mathbf{Aff}^n$, et aussi d'ailleurs sur $\mathbf{P}_n$, ce qui donne un plongement $T \to \mathrm{Cr}_n$. Nous dirons que T est le « tore standard » de Cr_n.

Le dual $T^* = \mathrm{Hom}(T, \mathbf{G}_m)$ de T est $\mathbf{Z}^n$. Le groupe d'automorphismes de T^* (qui est aussi celui de T) est le groupe $\Gamma = \mathbf{GL}_n(\mathbf{Z})$. Le produit semi-direct $N(k)$ de Γ par $T(k)$ opère sur T, donc se plonge dans $\mathrm{Cr}_n(k)$, ce que nous écrirons simplement $N = T.\Gamma \hookrightarrow \mathrm{Cr}_n$.

Lorsque k est algébriquement clos, on démontre que $T(k)$ est son propre centralisateur dans $\mathrm{Cr}_n(k)$ et que $N(k)$ est son normalisateur (cf. [De 70, prop.10, cor. 5], dans un cadre un peu différent). Cette situation ressemble à celle que l'on a pour les groupes semi-simples, T jouant le rôle d'un tore maximal et Γ celui du groupe de Weyl (qui est toutefois infini si $n > 1$). Il y a aussi des analogues des racines (ce sont les éléments primitifs de T^*) et des sous-groupes additifs radiciels (il y en a une infinité pour chaque racine si $n > 1$, cf. [De 70, § 2]). On verra par la suite d'autres cas où l'analogie

$$\text{groupe de Cremona de rang } n \longleftrightarrow \text{ groupe semi-simple de rang } n$$

est à peu près justifiée – et aussi d'autres où elle ne l'est vraiment pas !

1.3. Le théorème de fusion

Dans un groupe fini, si un p-Sylow est commutatif, son normalisateur contrôle sa fusion (i.e. deux sous-groupes d'un p-Sylow qui sont conjugués dans le groupe le sont déjà dans le normalisateur du Sylow). De même, dans un groupe semi-simple, le groupe de Weyl contrôle la fusion du tore maximal. Ce sont là des résultats qui sont à la fois faciles à démontrer et très utiles (Borel, par exemple, en faisait grand usage).

Nous allons voir qu'il y a un résultat analogue pour les groupes de Cremona. Nous devrons toutefois faire l'hypothèse suivante :

(D) $$n \leqslant 2 \quad \text{ou} \quad \mathrm{car}(k) = 0.$$

[La lettre D est l'initiale de « désingularisation » : celle-ci intervient dans la démonstration, cf. fin du § 1.5.]

Voici l'énoncé du théorème :

THÉORÈME 1.1. — *Faisons l'hypothèse* (D) *ci-dessus. Soient A et B deux parties de $T(k)$ et soit $g \in \mathrm{Cr}_n(k)$ tel que $gAg^{-1} = B \subset \mathrm{Cr}_n(k)$. Il existe alors un élément γ de $\Gamma = \mathbf{GL}_n(\mathbf{Z})$ tel que $\gamma a \gamma^{-1} = gag^{-1}$ pour tout $a \in A$.*
(En particulier A et B sont conjugués dans $N(k)$.)

La démonstration sera donnée au § 1.6 ; comme on le verra, elle repose de façon essentielle sur des résultats de Reichstein et Youssin [RY 02].

Exemples

a) Deux éléments de $T(k)$ qui sont conjugués dans $\mathrm{Cr}_n(k)$ le sont dans $N(k)$, cf. [Bl 06b, prop.6].

b) Soit $m \geqslant 1$ premier à $\mathrm{car}(k)$. Supposons que k contienne les racines m-ièmes de l'unité. Soit T_m le groupe des éléments $x \in T(k)$ tels que $x^m = 1$; ce groupe est abélien de type $(m, ..., m)$; on a $\mathrm{Aut}(T_m) = \mathbf{GL}_n(\mathbf{Z}/m\mathbf{Z})$. Le théorème 1.1, appliqué à $A = B = T_m$, dit que les seuls éléments de $\mathrm{Aut}(T_m)$ qui soient induits par des automorphismes intérieurs de $\mathrm{Cr}_n(k)$ sont ceux dont le déterminant dans $(\mathbf{Z}/m\mathbf{Z})^\times$ est égal à ± 1. Sous une forme un peu différente, ce résultat est dû à Reichstein et Youssin [RY 02].

Problème. — Y a-t-il une forme « infinitésimale » du théorème 1.1 ? Autrement dit, remplaçons dans l'énoncé l'hypothèse $A, B \subset T(k)$ par $A, B \subset \mathrm{Lie}(T)$; est-ce que le théorème est encore valable[(2)] ? Même le cas où A et B n'ont qu'un seul élément ne paraît pas évident. Lorsque $k = \mathbf{C}$, il est possible que la question puisse se traiter par voie analytique, en utilisant les feuilletages associés aux éléments non nuls de $\mathrm{Lie}(T)$.

1.4. Un lemme

Supposons k algébriquement clos.

LEMME 1.2. — *Soient V et V' deux sous-variétés fermées de T et soient V_o et V'_o des sous-ensembles denses de V et V'. Soit $g \in \mathrm{Cr}_n(k)$ tel que $g.V_o.g^{-1} = V'_o \subset \mathrm{Cr}_n(k)$. On a alors $g.V.g^{-1} = V'$ et l'application $v \mapsto g.v.g^{-1}$ est un isomorphisme de variétés de V sur V'.*

[(2)] Il faut d'abord se convaincre qu'il a un sens. C'est clair du point de vue de [De 70], où $\mathrm{Lie}(\mathrm{Cr}_n)$ est défini comme le noyau de $\mathrm{Cr}_n(k[t]/(t^2)) \to \mathrm{Cr}_n(k)$. Plus concrètement, on peut voir un élément de $\mathrm{Lie}(T)$ comme une section rationnelle du fibré tangent à $\mathbf{Aff}^n$, et l'on peut donc le transformer par $g \in \mathrm{Cr}_n(k)$.

(Précisons que par « sous-variété » nous entendons « sous-schéma réduit, séparé et de type fini sur k » et que nous identifions une telle variété à l'ensemble de ses k-points. Cela donne une correspondance bijective entre parties fermées de $T(k)$ et sous-variétés fermées de T.)

Démonstration. — Identifions $\mathrm{Cr}_n(k)$ au groupe des automorphismes birationnels de T. L'application rationnelle $g : T \dashrightarrow T$ a un domaine de définition U qui est un ouvert dense de T ; elle définit un morphisme birationnel $g : U \to T$. D'autre part, si x est un élément de T on l'identifie à l'élément de $\mathrm{Cr}_n(k)$ donné par la translation τ_x de T : $\tau_x : z \mapsto z.x$. Si $v \in V_o$ et si $v' = gvg^{-1}$, on a $g \circ \tau_v = \tau_{v'} \circ g$ en tout point de $U \cap Uv^{-1}$. Soit U_2 l'ouvert de $V \times T$ formé des couples (v, z) tels que $z \in U$ et $z.v \in U$. Si $(v, z) \in U_2$, posons $F(v, z) = g(z.v).g(z)^{-1}$. L'application $F : U_2 \to T$ est un morphisme. De plus, si $v \in V_o$ et si $v' = gvg^{-1}$ comme ci-dessus, on a $F(v, z) = v'$ pour tout z tel que $(v, z) \in U_2$; or de tels points sont denses dans U_2 puisque V_o est dense dans V. Il en résulte, par continuité, que $F(U_2)$ est contenu dans V'. Ainsi, F se factorise en $U_2 \to V \to V'$. Comme la projection $U_2 \to V$ est surjective, on obtient ainsi un morphisme $f : V \to V'$, et par construction on a $f(v) = gvg^{-1}$ si $v \in V_o$. Le même argument, appliqué à V' donne un morphisme $f' : V' \to V$ qui est inverse de f. Cela démontre le lemme.

1.5. Démonstration du théorème 1.1

Revenons à la démonstration du th. 1.1. On peut supposer que k est algébriquement clos, et que A et B sont des sous-groupes de $T(k)$. Soient $\overline{A}$ et $\overline{B}$ leurs adhérences pour la topologie de Zariski ; ce sont des sous-groupes algébriques réduits (donc lisses) du tore T.

D'après le lemme 1.2, on a $g\overline{A}g^{-1} = \overline{B}$. Il suffit donc de prouver le théorème pour $\overline{A}$ et $\overline{B}$; autrement dit, on peut supposer que A et B sont des sous-groupes algébriques lisses de T. De plus, le lemme 1.2 dit que l'application $f : a \mapsto gag^{-1}$ est un isomorphisme du groupe algébrique A sur le groupe algébrique B. Soient A^* et B^* les duaux de A et de B. On a par définition

$$A^* = \mathrm{Hom}(A, \mathbf{G}_m) \quad \text{et} \quad B^* = \mathrm{Hom}(B, \mathbf{G}_m).$$

Les injections $A \to T$ et $B \to T$ donnent par dualité des surjections $\mathbf{Z}^n \to A^*$ et $\mathbf{Z}^n \to B^*$; de même f donne un isomorphisme $f^* : B^* \to A^*$. Tout revient à trouver un automorphisme de $\mathbf{Z}^n$ qui rende commutatif le diagramme

$$\begin{tikzcd} \mathbf{Z}^n \arrow[r] \arrow[d] & B^* \arrow[d, "f^*"] \\ \mathbf{Z}^n \arrow[r] & A^*. \end{tikzcd}$$

Pour le prouver, on va utiliser les constructions et les résultats de [RY 02]. Si E est un groupe commutatif, engendrable par n éléments, le groupe $\wedge^n E$ est cyclique ; notons $I(E)$ l'ensemble de ses générateurs et notons $J(E)$ le quotient de $I(E)$ par la relation d'équivalence $x \sim \pm x'$. Si $E = \mathbf{Z}^n$, $I(E)$ a deux éléments et $J(E)$ en a un seul. La surjection $\mathbf{Z}^n \to B^*$ applique cet élément sur un certain élément j_B de $J(B^*)$. On définit de même $j_A \in J(A^*)$, et l'isomorphisme f^* transforme j_B en un élément $f^*(j_B)$ de $J(A^*)$.

LEMME 1.3. — *Pour qu'il existe un automorphisme de $\mathbf{Z}^n$ rendant commutatif le diagramme ci-dessus, il faut et il suffit que $f^*(j_B) = j_A$.*

Cela résulte du lemme 2.4 de [RY 02].

Nous sommes ainsi ramenés à montrer que les éléments j_A et $f^*(j_B)$ de $J(A^*)$ sont égaux. On considère pour cela les deux représentations linéaires r et r' de A données respectivement par $A \to T \to \mathbf{GL}_n$ et $A \to B \to T \to \mathbf{GL}_n$. Ce sont des représentations fidèles. Or, toute représentation linéaire fidèle ρ de A de degré n a un invariant $\mathrm{inv}(\rho)$ dans $J(A^*)$, qui se définit de la manière suivante (cf. [RY 02, § 7]) : on décompose ρ en somme directe de n représentations de degré 1, données par des caractères $\chi_1, ..., \chi_n$ et l'on forme le produit extérieur $\chi_1 \wedge ... \wedge \chi_n \in \wedge^n A^*$. Comme ρ est fidèle, cet élément est un générateur de $\wedge^n A^*$. Il est bien défini au signe près. Son image dans $J(A^*)$ est l'invariant $\mathrm{inv}(\rho)$ cherché.

On peut appliquer cette construction aux deux représentations r et r' définies ci-dessus ; on a évidemment $\mathrm{inv}(r) = j_A$ et $\mathrm{inv}(r') = f^*(j_B)$. Or l'élément g de $\mathrm{Cr}_n(k)$ transforme r en r' ; ces deux représentations sont donc birationnellement équivalentes. D'après [RY 02, th. 7.1], cela entraîne que $\mathrm{inv}(r) = \mathrm{inv}(r')$, i.e. $j_A = f^*(j_B)$, ce qui achève la démonstration du théorème.

Remarque. — En fait, Reichstein et Youssin, dans [RY 02], se limitent au cas où $\mathrm{car}(k) = 0$, car ils utilisent la résolution équivariante des singularités (cf. [BM 97], [AW 97] et [Ko 07]). En caractéristique $p > 0$ un tel résultat n'est connu que si $n = 1$ ou 2 [méthode : itérer le processus « éclatement des points singuliers et normalisation »], et les démonstrations de [RY 02] sont valables sans changement (elles deviennent même plus simples). C'est pour cela que nous avons dû faire l'hypothèse (D) au § 1.3. On retrouvera cette restriction au § 2, dans l'énoncé du th. 2.1.

1.6. Complément : la topologie de Zariski de $\mathrm{Cr}_n(k)$

Continuons à supposer k algébriquement clos. Soit X une k-variété (au sens du § 1.5) et soit f un élément du groupe $\mathrm{Cr}_n(X)$, autrement dit un pseudo-automorphisme du X-schéma $X \times \mathbf{Aff}^n$, cf. [De 70, § 1]. La donnée de f définit une application $X(k) \to \mathrm{Cr}_n(k)$. Nous définirons la *topologie de Zariski de* $\mathrm{Cr}_n(k)$ comme la topologie la plus fine qui rende continues les applications $X(k) \to \mathrm{Cr}_n(k)$, quels que soient les choix de X et de $f \in \mathrm{Cr}_n(X)$. Une partie Y de $\mathrm{Cr}_n(k)$ est fermée pour cette topologie si et seulement si $f^{-1}(Y)$ est fermée dans $X(k)$ pour tout X et pour tout $f \in \mathrm{Cr}_n(X)$, cf. Bourbaki TG I.14. On définit de manière analogue la topologie de Zariski de $\mathrm{Cr}_n(k) \times \mathrm{Cr}_n(k)$ et l'on montre facilement que l'application produit $\mathrm{Cr}_n(k) \times \mathrm{Cr}_n(k) \to \mathrm{Cr}_n(k)$ est continue.

Exemples. — Le centralisateur dans $\mathrm{Cr}_n(k)$ d'une partie quelconque de $\mathrm{Cr}_n(k)$ est fermé. Une partie du tore $T(k)$ est fermée dans $\mathrm{Cr}_n(k)$ si et seulement si elle est fermée dans $T(k)$ pour la topologie de Zariski de $T(k)$. (L'injection $T(k) \to \mathrm{Cr}_n(k)$ est une immersion fermée.)

Problème. — Si $n > 2$, est-il vrai que $\mathrm{Cr}_n(k)$ est connexe ? C'est vrai pour $n = 2$ à cause du théorème de Max Noether suivant lequel $\mathrm{Cr}(k)$ est engendré par ses deux sous-groupes $\mathbf{PGL}_3(k)$ et $\mathbf{PGL}_2(k) \times \mathbf{PGL}_2(k)$.

Ce problème revient à déterminer un « H^0 ». On peut aller plus loin. Si C est un groupe abélien fini (d'ordre premier à la caractéristique, pour être prudent) on peut définir pour tout i le groupe de cohomologie étale $H^i_{et}(\mathrm{Cr}_n, C)$ comme la limite projective des $H^i_{et}(X, C)$, cette limite étant prise sur la catégorie des couples (X, f) comme ci-dessus. Le cas $i = 1$ est particulièrement intéressant car il équivaut à l'étude des « revêtements » finis abéliens de Cr_n. Hélas, je ne vois aucun moyen de calculer effectivement ces groupes.

2. SOUS-GROUPES FINIS (GÉNÉRALITÉS)

À partir de maintenant, on suppose que le corps de base k est un corps parfait, et l'on appelle « corps de fonctions » sur k toute extension K/k qui est de type fini et k-régulière (i.e. k est algébriquement fermé dans K).

2.1. Un résultat préliminaire

Nous allons nous intéresser aux sous-groupes finis du groupe de Cremona $\mathrm{Cr}_n(k)$ ou, ce qui revient au même aux groupes finis de k-automorphismes de $k(t_1, ..., t_n)$. Commençons par un résultat général, qui permet de passer des corps de fonctions (simples à définir mais difficiles à contrôler) aux variétés projectives (plus concrètes). Si K est un corps de fonctions sur k, on appelle *modèle* de K une k-variété algébrique irréductible réduite séparée X dont le corps des fonctions est K. On peut voir X, à la Chevalley-Nagata, comme un ensemble de sous-anneaux locaux de K contenant k. Si un groupe fini G opère sur K, cela donne un sens à l'expression « X est stable par G ». De tels modèles existent, et on peut même leur imposer un certain nombre de propriétés agréables. C'est ce que dit le théorème suivant :

THÉORÈME 2.1. — *Soit K un corps de fonctions sur k et soit G un sous-groupe fini de* $\mathrm{Aut}_k(K)$. *Alors :*

a) *Il existe un modèle projectif normal X de K stable par G.*

b) *Soit $n = \mathrm{deg.tr}_k K$. Si $n \leqslant 2$ ou si* $\mathrm{car}(k) = 0$, *on peut en outre choisir X lisse sur k.*

Démonstration. — a) Soit K^G le sous-corps de K fixé par G. Choisissons une k-variété projective irréductible X' dont le corps des fonctions soit K^G (l'existence d'une telle variété est claire). Soit X la normalisée de X' dans l'extension K/K^G. La variété X répond à la question. Si l'on avait choisi X' normale (ce qui était évidemment possible), on aurait $X/G = X'$.

b) On choisit X comme dans a) et on la remplace par une désingularisation équivariante, ce qui est possible vu les hypothèses faites sur n ou sur $\mathrm{car}(k)$, comme on l'a dit au § 1.5.

Si l'on applique ceci au cas $K = k(t_1, t_2)$, on voit que tout sous-groupe fini G de $\mathrm{Cr}(k)$ peut se réaliser comme sous-groupe de $\mathrm{Aut}(X)$, où X est une surface projective lisse k-rationnelle. Bien entendu, il n'y a pas en général unicité (on peut faire éclater tout sous-ensemble fini de $X(\overline{k})$ stable par G et par $\mathrm{Gal}(\overline{k}/k)$). Mais on va voir plus bas (th. 2.2) que l'ensemble des modèles X possibles possède des éléments ayant une forme spécialement simple.

2.2. Classe anticanonique et surfaces de Del Pezzo (rappels)

Dans ce qui suit, « surface » est une abréviation pour « k-surface projective lisse géométriquement connexe », et « surface k-rationnelle » signifie « surface dont le corps des fonctions est isomorphe à $k(t_1, t_2)$ ». Une surface est dite « géométriquement rationnelle » si elle devient rationnelle sur une clôture algébrique $\overline{k}$ de k.

Rappelons quelques définitions.

Classe anticanonique : l'opposée de la classe canonique $K_X \in \mathrm{Pic}(X)$. C'est la classe du fibré inversible $\omega^{-1} = \det(\mathcal{T}_X)$, où $\mathcal{T}_X$ est le faisceau tangent de X et ω est le faisceau dualisant. Exemple : si $X = \mathbf{P}_2$, la classe anticanonique de X est $3L$, où L est la classe des droites ; le faisceau inversible correspondant est le faisceau $\mathcal{O}(3)$.

Surface de Del Pezzo : surface telle que la classe anticanonique $-K_X$ soit ample. Références : [Ko 96, pp. 172-176], [De 80], [Do 07, chap. 8], [Ma 66, § 24]. Une telle surface a un *degré* d, défini par

$$d = K_X \,.\, K_X.$$

Il peut prendre n'importe quelle valeur entre 1 et 9. Sur $\overline{k}$, une surface de Del Pezzo de degré $\neq 8$ est isomorphe ([Ma 66, th. 24.4]) au plan projectif $\mathbf{P}_2$ dont on a éclaté $9 - d$ points en position suffisamment générale (pas 3 points sur une même droite, pas 6 points sur une même conique, et encore une autre condition lorsque $d = 1$, cf. [De 80, p. 27, th. 1]) ; pour $d = 8$ il y a deux possibilités : la quadrique $\mathbf{P}_1 \times \mathbf{P}_1$ et le plan projectif dont on a éclaté un point. En particulier, une surface de Del Pezzo est géométriquement rationnelle ; elle n'est pas toujours k-rationnelle.

Les propriétés géométriques et arithmétiques de ces surfaces sont fort intéressantes (on a écrit des volumes rien que sur le cas $d = 3$) ; ces propriétés interviennent de façon essentielle dans les démonstrations des §§ 3-4 ci-dessous (ce qui est d'ailleurs regrettable, car on ne peut pas espérer quelque chose d'aussi précis pour Cr_n si $n > 2$).

L'une des propriétés les plus utiles est la suivante : si X est une surface de Del Pezzo, le groupe $\mathrm{Aut}_k X$ des k-automorphismes de X se plonge dans une suite exacte :

$$1 \to \mathrm{A}^{\mathrm{o}}(k) \to \mathrm{Aut}_k X \to W,$$

où A^{o} est un groupe linéaire connexe (égal à 1 si $d < 6$) et W est le groupe de Weyl d'un système de racines de rang $9 - d$ (si $d < 7$), cf. [Ma 66, §§ 25-26] et [De 80]. Par exemple :

Si $d = 9$, X est une surface de Severi-Brauer (autrement dit une k-forme de $\mathbf{P}_2$) et A^{o} est de type A_2 : c'est une k-forme intérieure de $\mathbf{PGL}_3$; on a $W = 1$.

Si $d = 8$, X est, ou bien l'éclatée de $\mathbf{P}_2$ en un point rationnel, ou bien une k-forme de quadrique (surface de degré 2 dans une variété de Severi-Brauer de dimension 3) ; dans le second cas, A^{o} est un groupe adjoint de type $A_1.A_1$ et le groupe W est d'ordre 2.

Si $d = 6$, le groupe $T = \mathrm{A}^{\mathrm{o}}$ est un tore de dimension 2 ; il y a 6 courbes exceptionnelles sur $\overline{k}$; le graphe de leurs relations d'incidence est un hexagone ; le complémentaire dans X de leur réunion est un T-torseur et X est une variété toroïdale ; le groupe W est un groupe diédral d'ordre 12. [Pour une description explicite de ce cas, voir [CKM 07, § 4.2].]

Si $d = 5$, on a $\mathrm{A}^{\mathrm{o}} = 1$ et W est isomorphe au groupe symétrique $\mathfrak{S}_5$; il y a 10 courbes exceptionnelles sur $\overline{k}$; le graphe de leurs relations d'incidence est le graphe de Petersen[(3)] ; la flèche $\mathrm{Gal}(\overline{k}/k) \to W = \mathfrak{S}_5$ induit une correspondance bijective entre les classes de surfaces de Del Pezzo de degré 5 et les k-algèbres étales de rang 5, cf. Skorobogatov [Sk 01, § 3.1].

Si $d = 1, 2$ ou 3, on a $\mathrm{A}^{\mathrm{o}} = 1$ et W est un groupe de Weyl de type E_8, E_7 ou E_6 ; les classes dans $\mathrm{Pic}(X_{/\overline{k}})$ des courbes exceptionnelles correspondent aux poids $\neq 0$ d'une représentation irréductible de E_8, E_7 ou E_6 de dimension 248, 56 ou 27.

2.3. Sous-groupes finis et modèles minimaux

Soit G un groupe fini, et soit X une G-surface, c'est-à-dire une surface (au sens défini au début du § 2.2) munie d'un plongement de G dans $\mathrm{Aut}_k X$. On dit que X est « G-k-minimale » si les conditions équivalentes suivantes sont satisfaites :

(2.3.1) Tout morphisme birationnel $f : X \to X'$ de G-surfaces est un isomorphisme.

(2.3.2) Il n'existe pas de famille finie non vide (C_i) de courbes de $X_{/\overline{k}}$ ayant les trois propriétés suivantes :

i) les C_i sont deux à deux disjointes ;

ii) chaque C_i est une courbe exceptionnelle, i.e. lisse de genre 0 et de self-intersection -1 ;

[(3)] Le graphe de Petersen s'obtient de la manière suivante : on se donne un ensemble Ω à 5 éléments, et l'on prend pour sommets du graphe les parties à 2 éléments de Ω ; deux sommets sont joints par une arête si les parties correspondantes de Ω sont disjointes. C'est un graphe de valence 3 ; son groupe d'automorphismes s'identifie au groupe des permutations de Ω (on peut reconstituer canoniquement Ω à partir du graphe).

iii) la famille (C_i) est stable à la fois par l'action de G et par celle de $\mathrm{Gal}(\overline{k}/k)$.

L'équivalence de ces deux conditions résulte des propriétés standard des courbes exceptionnelles, cf. par exemple [Ha 77, Chap.V, § 3 et § 5, th. 5.7].

Nous pouvons maintenant énoncer le théorème suivant, qui jouera un rôle essentiel dans toute la suite :

Théorème 2.2. — *Avec les notations du th.* 2.1 *et en supposant* $n = 2$, *alors* :
a) *On peut choisir la* G*-surface* X *de telle sorte qu'elle soit* G-k*-minimale.*
b) *Si* X *est géométriquement rationnelle, et* G-k*-minimale,* X *est de l'un des deux types suivants* :

b1) *Il existe une courbe projective lisse* C *de genre* 0, *munie d'une action de* G, *et un morphisme* $\pi : X \to C$ *qui commute à l'action de* G *et fait de* X *un fibré en coniques*[(4)]. *On a* $\mathrm{Pic}(X)^G \cong \mathbf{Z}^2$.

b2) X *est une surface de Del Pezzo ; on a* $\mathrm{Pic}(X)^G \cong \mathbf{Z}$.

Démonstration. — L'assertion a) est immédiate. Pour b), voir [DI 08, § 2].

Remarque. — Si X est k-rationnelle, alors, dans le cas b1), la courbe C est isomorphe à la droite projective, puisqu'elle a des points rationnels. C'est le cas le plus intéressant pour la suite.

Historique. — Le cas $G = 1$ et $k = \mathbf{C}$ est dû à Castelnuovo. Il entraîne par exemple que toute surface rationnelle minimale est, soit le plan projectif, soit une surface réglée (fibré en coniques sans fibres singulières). Il y a eu ensuite toute une série de progrès, dus notamment à la théorie de Mori, cf. [Mo 82] ; on en trouvera une description dans [DI 07, § 3.3]. Je signale en particulier le texte de Manin [Ma 67] qui traite à la fois le cas $G = 1$ (k étant quelconque) et le cas où G est commutatif et k algébriquement clos ; l'hypothèse de commutativité a été supprimée plus tard par Iskovskikh [Is 79]. Voir aussi [Zh 01] et [Ko 96, III.2.1].

3. SOUS-GROUPES FINIS (k ALGÉBRIQUEMENT CLOS)

Dans ce paragraphe, on suppose k algébriquement clos. La détermination (à conjugaison près, si possible) de tous les sous-groupes finis de $\mathrm{Cr}(k)$ est une question très ancienne, qui est maintenant à peu près résolue : le lecteur curieux pourra consulter les longues listes données dans [DI 07] et [Bl 06]. Je vais me borner à en résumer les aspects les plus saillants.

[(4)] On dit que $\pi : X \to C$ est un *fibré en coniques* si la fibre générique de π est lisse de genre 0, et si les fibres spéciales sont, soit lisses, soit formées de deux courbes de genre 0 se coupant transversalement en un point (conique dégénérant en deux droites distinctes). Noter que, lorsqu'il n'y a pas de fibre singulière, on a un véritable « fibré » au sens topologique.

3.1. Un analogue d'un théorème de Jordan

Il s'agit du théorème qui dit qu'un sous-groupe fini d'un groupe réductif L ne peut être « gros » qu'à cause de sa partie abélienne. De façon plus précise, il existe un entier J_L tel que, pour tout sous-groupe fini G de $L(k)$, d'ordre premier à $\mathrm{car}(k)$, il existe un sous-groupe abélien normal A de G dont l'indice divise J_L. (*Démonstration.* Il suffit de le prouver lorsque $L = \mathbf{GL}_n$, et un argument simple de relèvement en caractéristique 0 permet de se ramener au cas $k = \mathbf{C}$, qui est connu depuis longtemps, cf. par exemple [Fr 11].)

Le même énoncé vaut pour le groupe de Cremona :

Théorème 3.1 ([Se 09, § 5.4]). — *Il existe un entier $J > 0$ ayant la propriété suivante : tout sous-groupe fini de $\mathrm{Cr}(k)$ d'ordre premier à $\mathrm{car}(k)$ contient un sous-groupe abélien normal d'indice divisant J.*

La démonstration consiste à examiner les différents cas du th. 2.2. On obtient une valeur explicite pour J : par exemple on peut prendre $J = 2^{10}3^4 5^2 7$, et même un peu mieux.

3.2. Sous-groupes simples non abéliens

Soit G un groupe fini simple non abélien, plongeable dans $\mathrm{Cr}(k)$. Supposons d'abord que $|G|$ soit premier à $\mathrm{car}(k)$. Le th. 3.1 montre que $|G|$ divise J ; à isomorphisme près, il n'y a donc qu'un nombre fini de possibilités pour G. En fait, ces possibilités se réduisent à trois (et même à zéro si $\mathrm{car}(k) = 2$ ou 3, à une si $\mathrm{car}(k) = 5$, et à deux si $\mathrm{car}(k) = 7$) :

Théorème 3.2. — *Le groupe G est isomorphe à $A_1(q) = \mathbf{PSL}_2(\mathbf{F}_q)$ avec $q = 5$, 7 ou 9.*

Autrement dit, G est d'ordre 60, 168 ou 360 ; noter que ce sont les plus petits ordres possibles pour un groupe simple non abélien. Noter aussi que ces groupes sont plongeables dans $\mathrm{Cr}(k)$, puisqu'ils le sont dans $\mathbf{PGL}_3(k)$, cf. e.g. [Mi 11].

Supposons maintenant que G soit d'ordre divisible par $p = \mathrm{car}(k)$, et ne soit isomorphe à aucun des trois groupes du th. 3.2. Alors :

Théorème 3.3. — *Le groupe G est isomorphe, soit à un groupe simple de type*[5] *$A_1(p^m), A_2(p^m)$ ou ${}^2A_2(p^m)$, soit à l'un des groupes suivants :*

lorsque $p = 2$, le groupe ${}^2A_3(2)$;

lorsque $p = 5$, le groupe alterné $\mathfrak{A}_7$.

---

[5] Rappelons que A_1, A_2, ${}^2A_2$ et ${}^2A_3$ désignent respectivement $\mathbf{PSL}_2$, $\mathbf{PSL}_3$, $\mathbf{PSU}_3$ et $\mathbf{PSU}_4$.

(Le groupe ${}^2A_3(2)$ est le groupe d'automorphismes de la surface cubique d'équation $x^3+y^3+z^3+t^3=0$ en caractéristique 2. Il est isomorphe au sous-groupe $W(E_6)^+$ du groupe de Weyl $W(E_6)$; son ordre est $2^6 3^4 5$. Quant au groupe $\mathfrak{A}_7$, il est plongeable dans $\mathbf{PGL}_3(k)$ si $p=5$.)

Démonstration. — On applique le th. 2.2, et l'on est ramené aux trois cas suivants :

i) X est un fibré en coniques : ce cas donne seulement les $A_1(p^m)$ et le groupe $\mathfrak{A}_5$;

ii) $X=\mathbf{P}_2$: on utilise la classification des sous-groupes finis de $\mathbf{PGL}_3(k)$, cf. [Bl 67] et [Mi 11] ;

iii) X est une surface de Del Pezzo de degré 1,2,...,8 : ce cas ne donne aucun nouveau groupe à l'exception de ${}^2A_3(2)$ pour $p=2$.

3.3. Sous-groupes abéliens élémentaires d'ordre premier à car(k)

Supposons G fini et contenu dans $\mathrm{Cr}(k)$. Nous dirons que G est *toral* si l'un de ses conjugués est contenu dans le tore standard T.

Théorème 3.4. — *Soit ℓ un nombre premier distinct de* $\mathrm{car}(k)$.

i) *Si $\ell>5$, tout ℓ-sous-groupe G de* $\mathrm{Cr}(k)$ *est toral* ; *en particulier, G est commutatif de rang* $\leqslant 2$.

ii) *Pour $\ell=2,3$ ou 5, il existe des sous-groupes cycliques d'ordre ℓ de* $\mathrm{Cr}(k)$ *qui ne sont pas toraux. De plus, le rang maximum d'un ℓ-sous-groupe abélien est* 4 (resp. 3, resp. 2) *si* $\ell=2$ (resp. $\ell=3$, resp. $\ell=5$).

Démonstration. — Voir [Be 07] , [BB 04] et [Bl 06].

Je renvoie aussi à ces textes pour les descriptions des classes de conjugaison non torales citées dans ii). Le cas $\ell=2$ est particulièrement intéressant, car certaines de ces classes (celles dites « de de Jonquières ») correspondent aux classes d'isomorphisme de courbes hyperelliptiques de genre quelconque $\geqslant 1$. (Si $y^2=f(x)$ est l'équation d'une telle courbe on lui fait correspondre l'involution $(x,y)\mapsto(x,f(x)/y)$.) Ces classes ont donc à la fois un « module discret » (le genre) et des « modules continus » (ceux de la courbe - par exemple son invariant modulaire si c'est une courbe elliptique).

Il est intéressant de comparer au cas des groupes semi-simples (cf. [Se 99]) : les nombres 2,3,5 se comportent comme les nombres premiers dits « de torsion ». Il y a toutefois des différences importantes : dans un groupe semi-simple, il n'y a qu'un nombre fini de classes pour un ordre fixé, et tout sous-groupe cyclique d'ordre premier à la caractéristique est toral.

3.4. Éléments d'ordre une puissance de $p = \mathrm{car}(k)$

Supposons que la caractéristique p de k soit > 0. Le groupe additif W_n des vecteurs de Witt de longueur n est un espace affine de dimension n ; en faisant opérer W_n sur lui-même par translations, on obtient un plongement de W_n dans $\mathrm{Aut}(\mathbf{Aff}^n)$, donc aussi dans Cr_n. Cela montre que $\mathrm{Cr}_n(k)$ contient des éléments d'ordre p^n. On peut se demander s'il contient des éléments d'ordre p^{n+1}. La réponse est « non » lorsque $n = 1$ ou 2 : c'est clair pour $n = 1$ et le cas $n = 2$ vient d'être traité par Dolgachev :

Théorème 3.5 ([Do 08]). — *Si* $p = \mathrm{car}(k)$*, le groupe* $\mathrm{Cr}(k)$ *ne contient pas d'élément d'ordre* p^3*.*

Vu le th. 2.2, il suffit de prouver que, ni un fibré en coniques, ni une surface de Del Pezzo n'a d'automorphisme d'ordre p^3. C'est immédiat pour les fibrés en coniques (utiliser le fait que $\mathbf{PGL}_2$ n'a pas d'élément d'ordre p^2). Il faut ensuite examiner les surfaces de Del Pezzo. Lorsque $p > 2$, c'est facile. Pour $p = 2$, il y a plusieurs cas non évidents, le plus délicat étant celui du degré 1, où un calcul détaillé est nécessaire, cf. [Do 08, § 5].

Remarque. — Ici, l'analogie entre le groupe de Cremona et les groupes semi-simples ne fonctionne pas bien. En effet, si S est un groupe semi-simple de rang 2, et si $p > 5$, le groupe $S(k)$ ne contient pas d'élément d'ordre p^2.

3.5. Points fixes

Soit X une G-surface rationnelle et soit X^G la sous-variété des points fixes de G. Il est souvent utile d'avoir des renseignements sur la structure de X^G. En voici quelques-uns :

3.5.1. Si G est cyclique, on a $X^G \neq \varnothing$. — Plus généralement, soit V une variété projective lisse rationnelle, et soit $f : V \to V$ un endomorphisme de V ; supposons en outre $\dim V \leqslant 2$ ou $\mathrm{car}(k) = 0$. Alors f a un point fixe.

En effet, les hypothèses entraînent que $H^i(V, \mathcal{O}_V)$ est 0 pour $i > 0$ et est égal à k si $i = 0$. Le nombre de Lefschetz de f en cohomologie cohérente est donc égal à 1. D'après la formule de Woods Hole ([Il 77, cor. 6.12]), cela entraîne que f a un point fixe.

3.5.2. Si G est un p-groupe, et si $p = \mathrm{car}(k)$, alors $X^G \neq \varnothing$. — En effet, X est p-acyclique (pour la cohomologie étale à coefficients dans $\mathbf{Z}/p\mathbf{Z}$) : cela résulte de la suite exacte d'Artin-Schreier

$$0 \to \mathbf{Z}/p\mathbf{Z} \to \mathbf{G}_a \xrightarrow{\wp} \mathbf{G}_a \to 0,$$

et de la nullité des $H^i(X, \mathcal{O}_X)$ pour $i > 0$. On peut alors appliquer la théorie de Smith, sous la forme donnée dans [Se 08, § 7.4] ; on en déduit que X^G est p-acyclique, et en particulier est non vide.

Variante (dans le style de [Se 08]). S'il existait un contre-exemple sur k, il en existerait aussi un sur $\overline{\mathbf{F}}_p$. Le couple (G, X) serait alors défini sur un corps $\mathbf{F}_q$, et le groupe G opérerait sans point fixe sur l'ensemble fini $X(\mathbf{F}_q)$, ce qui entraînerait $|X(\mathbf{F}_q)| \equiv 0 \pmod p$. Quitte à augmenter $\mathbf{F}_q$, on peut supposer que X est $\mathbf{F}_q$-rationnelle. On a alors $|X(\mathbf{F}_q)| \equiv 1 \pmod q$ car c'est vrai pour $X = \mathbf{P}_2$ et la classe de $|X(\mathbf{F}_q)| \pmod q$ ne change pas par éclatements. Contradiction.

3.5.3. Si $|G|$ est premier à car(k)*, X^G est lisse.* — Cela résulte de la lissité de X, cf. [Fo 73] et [Iv 72, lemme 2.3].

3.5.4. Invariance des composantes de X^G de genre > 0. — Parmi les diverses composantes irréductibles de X^G, il peut y en avoir qui soient des courbes de genre > 0. Ces composantes *ne dépendent pas du modèle X choisi.* Cela provient de ce que éclatements et contractions ne peuvent créer ou détruire que des courbes de genre 0. Noter que, si G est toral, il n'y a aucune telle courbe. Cela donne une condition nécessaire (et souvent suffisante, cf. [Bl 06]) pour qu'un sous-groupe de $\mathrm{Cr}(k)$ soit toral.

3.5.5. Invariance de X^G lorsque G est commutatif d'ordre premier à car(k). — Soient (G, X) et (G, Y) deux G-surfaces et soit $f : X \dashrightarrow Y$ un G-isomorphisme birationnel (pas nécessairement un morphisme). Disons que deux points $x \in X$ et $y \in Y$ se correspondent si (x, y) est contenu dans l'adhérence du graphe de f. Alors, pour tout $y \in Y^G$, il existe $x \in X^G$ qui correspond à y (sous réserve que G soit commutatif d'ordre premier à car(k)).

Démonstration. — Après éclatement de X, on peut supposer que f est un morphisme. On applique alors un résultat (bien plus général) de J. Kollár et E. Szabó, cf. [KS 00] et [RY 02, prop. 6.2].

Une conséquence de ce résultat est que, si G n'a pas de point fixe (sur un modèle quelconque), il n'est pas toral puisqu'un groupe toral a au moins 3 points fixes dans son action sur $\mathbf{P}_2$. Ceci s'applique par exemple aux sous-groupes de type (3,3) de $\mathbf{PGL}_3(k)$ en caractéristique $\neq 3$ dont l'image réciproque dans $\mathbf{SL}_3$ est non commutative : ces sous-groupes sont « non toraux » dans le groupe de Cremona.

3.6. Application : la dimension essentielle du groupe $\mathfrak{A}_6$

Supposons car$(k) = 0$ (et k algébriquement clos, comme ci-dessus). Si G est un groupe fini, on définit (cf. par exemple [BR 97], [RY 00] ou [Se 03, § 5]) sa *dimension essentielle* relativement à k comme la dimension minimum d'un G-torseur versel. C'est un invariant de G que l'on note $\mathrm{ed}_k(G)$. Lorsque G est un groupe alterné $\mathfrak{A}_n$, on savait calculer $\mathrm{ed}_k(G)$ pour $n \leqslant 5$ alors que, pour $n = 6$, on savait seulement que $\mathrm{ed}_k(G)$ est égal à 2 ou à 3 (cf. [BR 97, § 6.4]). En fait :

Théorème 3.6. — *On a* $\mathrm{ed}_k(\mathfrak{A}_6) = 3$.

Tout revient à montrer que $\mathrm{ed}_k(\mathfrak{A}_6)$ n'est pas égal à 2. Si c'était le cas, le corps de définition d'un $\mathfrak{A}_6$-torseur versel de dimension minimum serait le corps des fonctions d'une surface X. Le fait que ce torseur soit versel entraîne que X est unirationnelle, donc rationnelle vu les hypothèses faites sur k. Cela permet de supposer que X est, soit un fibré en coniques, soit une surface de Del Pezzo de degré 1,2,..., ou 9. On élimine facilement toutes ces possibilités, sauf la dernière, en utilisant le fait que tout homomorphisme de $\mathfrak{A}_6$ dans $\mathbf{GL}_i(k)$ (resp. dans $\mathbf{PGL}_j(k)$) est trivial si $i < 5$ (resp. $j < 3$) [pour les cas de degrés 1,2,3, remarquer que $\mathfrak{A}_6$ opère sur $H^0(X, \omega^{-1})$, qui est de dimension 2,3,4 respectivement]. Il reste seulement la possibilité $\deg(X) = 9$, i.e. $X = \mathbf{P}_2$ et $\mathfrak{A}_6 \subset \mathbf{PGL}_3(k)$. Mais dans ce cas on constate qu'un 3-Sylow de $\mathfrak{A}_6$ agit sans point fixe sur $\mathbf{P}_2$ (cf. fin du § 3.5.5), et ce n'est pas possible pour une action verselle d'après [RY 00, prop. 5.3].

Remarques. — 1) En utilisant des arguments analogues, A. Duncan a récemment déterminé tous les groupes finis G tels que $\mathrm{ed}_k(G) = 2$, où k est comme ci-dessus.

2) L'hypothèse $\mathrm{car}(k) = 0$ a été utilisée pour assurer que « unirationnel » entraîne « rationnel ». En caractéristique $p > 0$, il faudrait être capable de remplacer « unirationnel » par « séparablement unirationnel », mais je ne vois pas comment y parvenir.

4. SOUS-GROUPES FINIS (k PARFAIT)

4.1. Invariants cyclotomiques

Au lieu d'essayer de décrire tous les sous-groupes finis G possibles, on peut se borner, comme l'avait fait Minkowski dans [Mi 87] pour $\mathbf{GL}_n$, à donner une majoration multiplicative de $|G|$. Cela revient à majorer les ordres des ℓ-sous-groupes de Sylow de G, pour tout ℓ premier $\neq \mathrm{car}(k)$. Il se trouve (ce n'était nullement évident *a priori*) que le résultat ne dépend que de l'image $\mathrm{Im}(\chi)$ du ℓ-ième caractère cyclotomique $\chi : \mathrm{Gal}(\overline{k}/k) \to \mathbf{Z}_\ell^\times$ associé à ℓ et k. Pour exprimer le résultat, il est commode d'associer au couple (k, ℓ) les invariants numériques (t, m) définis de la façon suivante (cf. [Se 07, § 4] et [Se 09, § 1]) :

4.1.1. Supposons $\ell > 2$. Le groupe $\mathbf{Z}_\ell^\times$ se décompose en produit direct

$$\mathbf{Z}_\ell^\times = C_{\ell-1} \ \times \ \{1 + \ell.\mathbf{Z}_\ell\},$$

où $C_{\ell-1} = (\mathbf{Z}/\ell\mathbf{Z})^\times$ est cyclique d'ordre $\ell - 1$ et $1 + \ell.\mathbf{Z}_\ell$ est un pro-ℓ-groupe isomorphe au groupe additif $\mathbf{Z}_\ell$. Comme $\ell - 1$ est premier à ℓ, tout sous-groupe fermé de $\mathbf{Z}_\ell^\times$ est produit direct de ses intersections avec les deux facteurs. En particulier, on a

$$\mathrm{Im}(\chi) = C_t \ \times \ \{1 + \ell^m.\mathbf{Z}_\ell\},$$

où t est un diviseur de $\ell - 1$, C_t est un groupe cyclique d'ordre t et m appartient à $\{1, 2, \ldots, \infty\}$, avec la convention que $\ell^\infty = 0$. Cela définit t et m sans ambiguïté ; si l'on désire préciser k et ℓ, on les note $t(k, \ell)$ et $m(k, \ell)$.

[Autre définition de t : on a $t = [k(z_\ell) : k]$ où z_ℓ est une racine primitive ℓ-ième de l'unité dans $\overline{k}$. Quant au groupe C_t, c'est $\mathrm{Gal}(k(z_\ell)/k)$.]

4.1.2. Le cas $\ell = 2$. On pose $t = [k(i) : k]$ et l'on définit $m \in \{2, ..., \infty\}$ par la formule $\mathrm{Im}(\chi^2) = 1 + 2^{m+1}\mathbf{Z}_2$.

Exemples. — 1) Si $k = \mathbf{Q}$, on a $(t, m) = (\ell - 1, 1)$ si $\ell > 2$ et $(t, m) = (2, 2)$ si $\ell = 2$.

2) Si k est un corps fini à q éléments, et si $\ell > 2$, t est l'ordre de l'image de q dans $(\mathbf{Z}/\ell\mathbf{Z})^\times$ et m est égal à $v_\ell(q^t - 1) = v_\ell(q^{\ell-1} - 1)$; si $\ell = 2$, on a $m = v_2(q^2 - 1) - 1$, $t = 1$ si $q \equiv 1 \pmod 4$ et $t = 2$ si $q \equiv -1 \pmod 4$.

(Ici et dans toute la suite on note $v_\ell(x)$ la valuation ℓ-adique d'un entier x. Si A est un ensemble fini, on écrit $v_\ell(A)$ à la place de $v_\ell(|A|)$).

4.2. Le théorème principal

Fixons un nombre premier ℓ distinct de $\mathrm{car}(k)$, et soient t, m les entiers correspondants. Définissons $M(k,\ell) \in \{0, 1, ..., \infty\}$ par la recette suivante :

$$\text{Si } \ell = 2, \quad M(k,\ell) = 2m + 3.$$

$$\text{Si } \ell = 3, \quad M(k,\ell) = \begin{cases} 4 & \text{si } t = m = 1 \\ 2m+1 & \text{sinon.} \end{cases}$$

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

Théorème 4.1 ([Se 09, § 2.2]). — *Soit c un entier $\geqslant 0$. Pour qu'il existe un sous-groupe de $\mathrm{Cr}(k)$ d'ordre ℓ^c, il faut et il suffit que l'on ait $c \leqslant M(k,l)$.*

Démonstration. — Voir § 4.4 pour « il suffit » et § 4.5 pour « il faut ».

Corollaire. — *Il y a équivalence entre :*

a) $\mathrm{Cr}(k)$ *contient un élément d'ordre ℓ.*

b) *Le degré de l'extension cyclotomique $k(z_\ell)/k$ est égal à* $1, 2, 3, 4$ *ou* 6.

En effet, b) est équivalent à $M(k,\ell) > 0$.

En particulier $\mathrm{Cr}(\mathbf{Q})$ contient un élément d'ordre ℓ si et seulement si $\ell = 2, 3, 5$ ou 7.

Exercice. Écrire explicitement des éléments de $\mathrm{Cr}(\mathbf{Q})$ d'ordre 2, 3, 5 et 7 (difficulté : trivial, facile, pas très difficile, difficile).

4.3. Cas particuliers

Disons que k est « petit » si ses invariants $t(k,\ell)$ et $m(k,\ell)$ ont les deux propriétés suivantes :

(4.3.1) $$m(k,\ell) < \infty \text{ pour tout } \ell \neq \mathrm{car}(k)$$

(4.3.2) $$t(k,\ell) \to \infty \text{ quand } \ell \to \infty.$$

Bien sûr, un corps fini est petit ; même chose pour $\mathbf{Q}$. Il en est de même d'un corps de nombres, et plus généralement de tout corps qui est extension de type fini d'un corps qui est petit. Tout corps local à corps résiduel petit est petit. Si k est petit, les $M(k,\ell)$

du § 4.2 sont 0 pour ℓ assez grand, et sont finis pour tout ℓ. On peut alors définir un entier $M(k)$ par la formule

$$M(k) = \prod_{\ell} \ell^{M(k,\ell)}, \tag{4.3.3}$$

et le th. 4.1 entraîne :

THÉORÈME 4.2. — *Supposons que k soit petit au sens ci-dessus. Alors les sous-groupes finis de* $\mathrm{Cr}(k)$ *d'ordre premier à* $\mathrm{car}(k)$ *sont d'ordre borné, et le ppcm de leurs ordres est égal à l'entier* $M(k)$ *défini par la formule* (4.3.3).

Exemples de calcul de $M(k)$:

a) $k = \mathbf{Q}$. On trouve :

$$M(\mathbf{Q}) = 2^7.3^3.5.7. \tag{4.3.4}$$

b) $k = \mathbf{F}_q$. On trouve (cf. [Se 09, § 2.5]) :

$$M(\mathbf{F}_q) = \begin{cases} 3.(q^4-1)(q^6-1) & \text{si } q \equiv 4 \text{ ou } 7 \pmod 9 \\ (q^4-1)(q^6-1) & \text{sinon.} \end{cases} \tag{4.3.5}$$

Par exemple :

$$M(\mathbf{F}_2) = 3^3.5.7\,; \quad M(\mathbf{F}_3) = 2^7.5.7.13\,; \quad M(\mathbf{F}_4) = 3^4.5^2.7.13.17.$$

Remarque. — Il y a une analogie frappante entre la formule (4.3.5) et la formule correspondante pour un groupe algébrique semi-simple déployé de rang 2 : si S est un tel groupe, le ppcm des ordres des sous-groupes de $S(\mathbf{F}_q)$ d'ordre premier à $\mathrm{car}(k)$ est $(q^a-1)(q^b-1)$, où les entiers (a,b) sont égaux à (2,2), (2,3), (2,4) ou (2,6) si S est de type $A_1.A_1$, A_2, B_2 ou G_2. Pour le groupe de Cremona, le couple (a,b) est égal à (4,6), et il y a un facteur exceptionnel égal à 3 lorsque k contient les racines 3-ièmes de l'unité mais pas les racines 9-ièmes. L'analogie n'est donc pas parfaite.

4.4. Construction de ℓ-sous-groupes de $\mathrm{Cr}(k)$

Pour prouver la partie « il suffit » du théorème 4.1, on doit construire, pour tout $c \leqslant M(k,\ell)$, un sous-groupe de $\mathrm{Cr}(k)$ d'ordre ℓ^c. On peut supposer que l'invariant $t = t(k,\ell)$ est égal à 1, 2, 3, 4 ou 6, car sinon on a $M(k,\ell) = 0$ d'où $c = 0$. Comme au § 4.1, notons C_t le groupe $\mathrm{Gal}(k(z_\ell)/k)$; c'est un groupe cyclique d'ordre t ; il est donc plongeable dans le groupe $\mathbf{GL}_2(\mathbf{Z}) = \mathrm{Aut}(T)$. Choisissons un tel plongement $i : C_t \to \mathbf{GL}_2(\mathbf{Z})$, en imposant la condition que, si t est pair, on a $-1 \in \mathrm{Im}(i)$. En composant

$$\mathrm{Gal}(\overline{k}/k) \to \mathbf{Z}_\ell^\times \to C_t \to \mathbf{GL}_2(\mathbf{Z}) = \mathrm{Aut}(T),$$

on obtient un homomorphisme $\varphi : \mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}(T)$. Soit T_φ le tore déduit de T par torsion galoisienne au moyen de φ. D'après un théorème de Voskresenskiĭ (cf. [Vo 98, § 4.9]) T_φ est une variété k-rationnelle. En faisant agir par translation T_φ sur elle-même, on obtient un plongement de T_φ dans Cr, donc de $T_\varphi(k)$ dans $\mathrm{Cr}(k)$. De plus, le groupe

C_t opère sur T_φ par automorphismes. Cela donne un plongement du produit semi-direct $P = T_\varphi(k).C_t$ dans $\mathrm{Cr}(k)$. Lorsque $t = 1$ ou 2, on peut faire un peu mieux : le groupe diédral D_4 d'ordre 8 opère sur T_φ, et l'on obtient ainsi un plongement de $P' = T_\varphi(k).D_4$ dans $\mathrm{Cr}(k)$. Il ne reste plus qu'à vérifier que le groupe P (resp. P' si $t = 1$ ou 2) contient un sous-groupe d'ordre ℓ^c, ce qui ne présente pas de difficulté (cf. [Se 09, § 3]), sauf dans un cas particulier : celui où $\ell = 3, t = 1, m = 1, c = 4$; dans ce cas, la construction ci-dessus fournit au plus un groupe d'ordre 3^3 ; pour obtenir un groupe d'ordre 3^4, on doit utiliser un 3-Sylow du groupe d'automorphismes de la surface cubique d'équation

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

cf. [Se 09, § 3.1].

Exemple. — Prenons $k = \mathbf{Q}$ et $\ell = 7$. On a alors $t = 6$, et le tore T_φ se compactifie de façon T_φ-équivariante en une surface de Del Pezzo X de degré 6, dont les 6 courbes exceptionnelles sont permutées transitivement par le groupe C_6. Le groupe $T_\varphi(\mathbf{Q})$ contient un unique sous-groupe cyclique C_7 d'ordre 7, qui est normalisé par C_6 ; le produit semi-direct $C_7.C_6$ opère sur X.

Remarque. — Au lieu d'utiliser des tores, comme nous l'avons fait, on aurait pu se servir de surfaces de Del Pezzo, et même seulement de celles de degré $d = 3, 6, 8$ ou 9, suivant la valeur de l'invariant t :

pour $t = 1, 2$, on prend $d = 8$ (sauf si $p = 3$, où l'on a besoin de $d = 6$ et de $d = 3$) ;
pour $t = 3$ (resp. 4, resp. 6), on prend $d = 9$ (resp. 8, resp. 6).

4.5. Majoration de l'ordre d'un ℓ-sous-groupe de $\mathrm{Cr}(k)$

Pour achever la démonstration du th. 4.1, il faut prouver que, si G est un sous-groupe fini de $\mathrm{Cr}(k)$, on a $v_\ell(G) \leqslant M(k, \ell)$. On va faire un peu mieux : au lieu de ne s'intéresser qu'aux k-automorphismes du corps $k(t_1, t_2)$, on va considérer une k-forme L de $k(t_1, t_2)$, autrement dit un corps de fonctions sur k jouissant de la propriété suivante :

(4.5.1) $\quad \overline{k} \otimes_k L$ est $\overline{k}$-isomorphe à $\overline{k}(t_1, t_2)$.

Une surface dont le corps des fonctions est L est géométriquement rationnelle, mais pas nécessairement k-rationnelle.

Théorème 4.3 ([Se 09, § 4.1]). — *Soit G un sous-groupe fini de $\mathrm{Aut}_k(L)$, où L satisfait à* (4.5.1). *Soit ℓ un nombre premier $\neq \mathrm{car}(k)$. On a $v_\ell(G) \leqslant M(k, \ell)$.*

Démonstration. — Vu les th. 2.1 et 2.2, on peut supposer que G est contenu dans $\mathrm{Aut}_k(X)$ où X est, soit un fibré en coniques G-équivariant de base une courbe C de genre 0, soit une surface de Del Pezzo de degré 1, 2, . . . ou 9. On examine ces dix cas les uns après les autres. En voici deux, à titre d'exemples (pour les autres voir [Se 09, §§ 4.3 - 4.12]) :

— *Le cas où X est un fibré en coniques.* Le groupe G opère sur la base C de la fibration, et définit donc un sous-groupe G_C de $\mathrm{Aut}_k(C)$. Le noyau N de $G \to G_C$ est un sous-groupe de $\mathrm{Aut}_{k(C)}(F)$, où F est la fibre générique de $X \to C$, et $k(C)$ est le corps des fonctions de C. Comme C (resp. F) est une courbe de genre 0, son groupe d'automorphismes est une k-forme (resp. une $k(C)$-forme) de $\mathbf{PGL}_2$. Cela permet, en appliquant par exemple [Se 07, th. 5], de majorer les ordres de G_C et de N en termes des invariants (t, m) [noter que k et $k(C)$ ont les mêmes invariants, car l'extension $k(C)/k$ est régulière, donc linéairement disjointe des extensions cyclotomiques de k]. On trouve ainsi :

$$v_\ell(G_C) \ \text{ et } \ v_\ell(N) \leqslant \begin{cases} m+1 & \text{si} \quad \ell = 2, \\ m & \text{si} \quad \ell > 2 \ \text{ et } \ t = 1 \ \text{ ou } \ 2, \\ 0 & \text{si} \quad t > 2. \end{cases}$$

Comme $v_\ell(G) = v_\ell(G_C) + v_\ell(N)$, on en tire :

$$v_\ell(G) \ \leqslant \begin{cases} 2m+2 & \text{si} \quad \ell = 2, \\ 2m & \text{si} \quad \ell > 2 \ \text{ et } \ t = 1 \ \text{ ou } \ 2, \\ 0 & \text{si} \quad t > 2. \end{cases}$$

En comparant avec la définition de $M(k, \ell)$, on constate que cette majoration entraîne $v_\ell(G) \leqslant M(k, \ell)$.

— *Le cas où X est une surface de Del Pezzo de degré* 3. La classe anticanonique est très ample ; elle donne un plongement de X dans $\mathbf{P}_3$ qui identifie X à une surface cubique. Le groupe G se plonge ainsi à la fois dans $\mathbf{GL}_4(k)$ (par son action sur $H^0(X, \omega^{-1})$) et dans le groupe de Weyl $W(E_6)$ (par son action sur $\mathrm{Pic}(X_{/\overline{k}})$). L'ordre de $W(E_6)$ est $2^7 3^4 5$. Cela donne une borne pour $v_\ell(G)$ qui est $\leqslant M(k, \ell)$ sauf lorsque $\ell = 3$ et $t = 2$ (autrement dit k ne contient pas z_3) ; dans ce cas exceptionnel, on a en effet $M(k, \ell) = 3$. Il reste donc à prouver que, si $\ell = 3$ et si $|G| = 3^4$, le corps k contient z_3. Cela se démontre en considérant le plongement de G dans $\mathbf{GL}_4(k)$: si g est un élément non trivial du centre de G, on trouve que ses valeurs propres sont de la forme $\{1, z_3, z_3, z_3\}$, cf. [Se 09, § 4.10]. D'où $z_3 \in k$.

5. DE LA CARACTÉRISTIQUE p À LA CARACTÉRISTIQUE 0

Dans le genre de questions que l'on vient de discuter, on a souvent envie de remplacer la caractéristique $p > 0$ par la caractéristique 0. En effet, dans cette dernière, on dispose d'outils plus puissants (méthodes analytiques, « vanishing theorem », etc.), et l'on a bien davantage de références. Il y a même des différences sérieuses en ce qui concerne les surfaces de Del Pezzo de degré 1 et 2. Ainsi, en caractéristique 0, toute surface de Del Pezzo de degré 2 est un revêtement quadratique du plan projectif (un « plan double ») dont le lieu de ramification (la « courbe de diramation ») est une quartique lisse ; par contre, en caractéristique 2, le lieu de ramification est une conique (comptée avec multiplicité 2), et cette conique peut ne pas être lisse : elle peut être formée de deux droites, et elle peut même être une droite double, cf. [CO 90].

En fait, tant que l'on ne s'intéresse qu'à des actions de groupes d'ordres premiers à la caractéristique, la théorie des « relèvements » (ou des « déformations ») de Grothendieck montre que tout ce qui existe en caractéristique $p > 0$ existe aussi en caractéristique 0. Ce n'est pas difficile à démontrer : il suffit de suivre pas à pas ce qu'il a expliqué au séminaire Bourbaki en 1959 ([Gr 59] - voir aussi [Il 05, th. 8.5.9 (b)]), en y incorporant l'action du groupe G. C'est ce que nous allons faire.

5.1. Énoncé du théorème

On se donne un anneau noethérien complet A de corps résiduel k, ainsi qu'une k-variété projective lisse X, géométriquement connexe, et un groupe fini G qui opère sur X. On s'intéresse à un « relèvement » de ces données sur A ; cela signifie un A-schéma X_A lisse et projectif sur A, muni d'une action de G, dont la fibre spéciale est G-isomorphe à X.
[Le cas le plus intéressant pour nous est celui où k est de caractéristique $p > 0$, A est l'anneau $W(k)$ des vecteurs de Witt, et X est une surface géométriquement rationnelle munie d'une action de G, cf. § 5.4 ci-dessous.]

Nous ferons les hypothèses suivantes :

(5.1.1) $|G|$ n'est pas divisible par $\mathrm{car}(k)$.

(5.1.2) On a $H^2(X, \mathcal{O}_X) = 0$, où $\mathcal{O}_X$ est le faisceau des anneaux locaux de X.

(5.1.3) On a $H^2(X, \mathcal{T}_X) = 0$, où $\mathcal{T}_X$ est le faisceau tangent de X, i.e. le dual de Ω^1_X.

THÉORÈME 5.1. — *Si les trois hypothèses ci-dessus sont satisfaites, il existe un relèvement de* (G, X) *à* A.

5.2. Démonstration du théorème quand A est artinien

On procède par récurrence sur la longueur de A. Si cette longueur est 1, on a $A = k$ et l'on prend $X_A = X$. Si elle est > 1, on choisit un idéal non nul I de A tel que $\mathfrak{m}.I = 0$, où $\mathfrak{m}$ est l'idéal maximal de A. Vu l'hypothèse de récurrence, on dispose d'un relèvement $(G, X_{A/I})$ de (G, X) à l'anneau A/I. L'hypothèse (5.1.3) permet de relever $X_{A/I}$ à A, cf. [Gr 59, th. 9]. De plus, l'ensemble des classes de relèvements possibles a une structure naturelle d'espace affine (i.e. de torseur) sur le k-espace vectoriel $H^1(X, \mathcal{T}_X) \otimes_k I$ ([Gr 59, cor. 2 au th. 9]), et le groupe G opère de façon naturelle sur cet ensemble. Or un groupe fini d'automorphismes d'un espace affine, qui est d'ordre premier à la caractéristique, a un point fixe (prendre le barycentre d'une orbite). On peut donc choisir un relèvement X_A de $X_{A/I}$ qui soit G-invariant. Cela signifie que, pour tout $g \in G$, il existe un automorphisme de X_A qui relève l'action de g sur $X_{A/I}$. Notons E_g l'ensemble de ces automorphismes, et soit E la réunion des E_g ; l'ensemble E est un sous-groupe de $\mathrm{Aut}_A(X_A)$, et l'on a une suite exacte :

$$1 \longrightarrow N \longrightarrow E \longrightarrow G \longrightarrow 1,$$

où $N = \mathrm{Ker} : \mathrm{Aut}_A(X_A) \to \mathrm{Aut}_{A/I}(X_{A/I})$. Le groupe N est isomorphe à $H^0(X, \mathcal{T}_X) \otimes_k I$; il a une structure naturelle de k-espace vectoriel. Comme G est d'ordre premier à $\mathrm{car}(k)$, on a $H^i(G, N) = 0$ pour tout $i > 0$ et en particulier $H^2(G, N) = 0$. Cela montre que la suite exacte ci-dessus est scindée : elle admet une section $G \to E$. Cela permet de faire agir G sur X_A, ce qui démontre le théorème dans le cas considéré.

5.3. Fin de la démonstration du théorème

On applique ce que l'on vient de démontrer aux quotients $A/\mathfrak{m}^r$ pour $r = 1, 2, \ldots$. En passant à la limite sur r on obtient un A-schéma formel muni d'une action de G. L'hypothèse (5.1.2) entraîne d'après [Gr 59, th. 4] que ce schéma est algébrisable, et cela de façon unique (« GAGA formel »). Cela fournit le A-schéma X_A cherché, ainsi que l'action de G sur X_A. Le fait que X_A soit projectif sur A résulte aussi de [Gr 59, th. 4].

5.4. Le cas des surfaces géométriquement rationnelles

Soit X une k-surface géométriquement rationnelle.

Lemme 5.2. — *Les conditions* (5.1.2) *et* (5.1.3) *sont satisfaites, autrement dit l'on a* $H^2(X, \mathcal{O}_X) = 0$ *et* $H^2(X, \mathcal{T}_X) = 0$.

Soit $\omega = \det(\Omega^1)$ le faisceau dualisant de X. Par dualité, il suffit de voir que les deux espaces $\mathbf{T}_1(X) = H^0(X, \omega)$ et $\mathbf{T}_2(X) = H^0(X, \omega \otimes \Omega^1)$ sont 0. Quitte à faire une extension finie de k on peut supposer que X est une surface rationnelle. Or, de façon générale, si $\mathbf{T}$ est un foncteur tensoriel covariant (comme ici $E \mapsto \det(E)$ et $E \mapsto \det(E) \otimes E$), l'espace des sections de $\mathbf{T}(\Omega^1)$ est un invariant birationnel de la variété (projective lisse) considérée [lorsque $\mathbf{T}$ est le foncteur $\det^{\otimes m}$, c'est l'invariance birationnelle du m-ième plurigenre - le cas général se démontre de la même manière]. Il suffit donc de vérifier que $\mathbf{T}_1(X) = \mathbf{T}_2(X) = 0$ lorsque $X = \mathbf{P}_1 \times \mathbf{P}_1$, ce qui est immédiat.

Supposons maintenant que k soit de caractéristique $p > 0$. On peut appliquer le th. 5.1 à (G, X), où G est un sous-groupe de $\mathrm{Aut}(X)$ d'ordre premier à p. Choisissons pour A l'anneau $W(k)$ des vecteurs de Witt à coefficients dans k et soit $F = A[1/p]$ le corps des fractions de A. Le th. 5.1 fournit un couple (G, X_A) sur A, d'où par le changement de base $A \to F$ un couple (G, X_F) sur F.

Lemme 5.3. — *La surface X_F est géométriquement rationnelle.*

Comme F est de caractéristique 0, on peut appliquer à X_F le critère de Castelnuovo classique (cf. e.g. [Ko 96, III.2.4]). D'après ce critère, il y a deux choses à démontrer :

a) Que le F-espace vectoriel $V_F = H^0(X_F, \omega^{\otimes 2})$ est 0.
Posons $V_A = H^0(X_A, \omega^{\otimes 2})$; c'est un A-module de type fini, et l'on a $V_F = F \otimes_A V_A$; d'autre part, $V_A/p.V_A$ se plonge dans $H^0(X, \omega^{\otimes 2})$, qui est 0 puisque X est géométriquement rationnelle. D'après le lemme de Nakayama, on a donc $V_A = 0$, d'où $V_F = 0$.

b) Que le F-espace vectoriel $H^0(X_F, \Omega^1)$ est 0.
La démonstration est la même : on utilise le fait que $H^0(X, \Omega^1) = 0$.

[*Variante* : prouver b) en utilisant le fait que les genres arithmétiques de X et de X_F sont les mêmes.]

Remarque. — Si X est une surface de Del Pezzo, il en est de même de X_F, et ces deux surfaces ont le même degré.

Application. — Supposons le th. 4.3 (celui qui dit que $v_\ell(G) \leqslant M(k,\ell)$) démontré en caractéristique 0, et montrons qu'il est vrai en caractéristique $p > 0$, si $\ell \neq p$. On peut supposer que G est un ℓ-groupe. Par hypothèse, il existe une k-surface géométriquement rationnelle dont le groupe d'automorphismes contient G. Grâce à ce qui précède, on en déduit une F-surface géométriquement rationnelle qui a les mêmes propriétés. D'où $v_\ell(G) \leqslant M(F,\ell)$, et l'on conclut en remarquant que $M(F,\ell) = M(k,\ell)$, car les corps F et k ont les mêmes invariants cyclotomiques (m,t) pour tout $\ell \neq p$.

Remarque. — Inversement, si l'on admet le th. 4.3 pour les corps finis, on l'en déduit pour tous les corps (même ceux de caractéristique 0) par la méthode de « réduction mod p » due à Minkowski ([Mi 87]), combinée avec un théorème de densité à la Chebotarev, cf. [Se 07, § 6.5].

RÉFÉRENCES

[AW 97] D. Abramovich et J. Wang, *Equivariant resolution of singularities in characteristic* 0, Math. Res. Letters **4** (1997), 427-433.

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

[BB 04] A. Beauville et J. Blanc, *On Cremona transformations of prime order*, C.R.A.S. **339** (2004), 257-259.

[BM 97] E. Bierstone et P.D. Milman, *Canonical desingularization in characteristic zero by blowing up the maximum strata of a local invariant*, Invent. math. **128** (1997), 207-302.

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

[Bl 06b] J. Blanc, *Conjugacy classes of affine automorphisms of K^n and linear automorphisms of* $\mathbf{P}^n$ *in the Cremona groups*, manuscripta math. **119** (2006), 225-241.

[Bl 67] D. Bloom, *The subgroups of* $\mathbf{PSL}(3,q)$ *for odd q*, Trans. AMS **127** (1967), 150-178.

[BR 97] J. Buhler et Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), 159-179.

[CKM 07] J-L. Colliot-Thélène, N.A. Karpenko et A.S. Merkur'ev, *Surfaces rationnelles et dimension canonique du groupe* $\mathbf{PGL}_6$ (en russe), Alg. i Analiz **19** (2007), 159-178 ; traduction anglaise : St. Petersburg Math. J. **19** (2008), 793-804.

[CO 90] P. Cragnolini et P.A. Olivero, *On the proof of Castelnuovo's rationality criterion in positive characteristic*, J. Pure Applied Math. **68** (1990), 297-323.

[De 70] M. Demazure, *Sous-groupes algébriques de rang maximum du groupe de Cremona*, Ann. Sci. ENS (4) **3** (1970), 507-588.1030

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

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

[DI 08] I.V. Dolgachev et V.A.I skovskikh, *On elements of prime order in the plane Cremona group over a perfect field*, ArXiv :math/0707.4305, à paraître.

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

[Do 08] I.V. Dolgachev, *On elements of order* p^s *in the plane Cremona group over a field of characteristic* p, à paraître.

[Fo 73] J. Fogarty, *Fixed point schemes*, Amer. J. Math. **95** (1973), 35-51.

[Fr 11] F.G. Frobenius, *Über den von L.Bieberbach gefundenen Beweis eines Satzes von C. Jordan*, Sitz. Kn. Preuss. Akad. Berlin (1911), 241-248 (= Ges. Abh., vol.III, 493-500).

[Gr 59] A. Grothendieck, *Géométrie formelle et géométrie algébrique*, Sém. Bourbaki 1958/1959, exposé **1182**, SMF, vol. 5 (1995), 193-220.

[Ha 77] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977.

[Il 77] L. Illusie, *Formule de Lefschetz pour les faisceaux cohérents*, SGA 5, Lect. Notes in Math. **589**, 73-137.

[Il 05] L. Illusie, *Grothendieck's existence theorem in formal geometry*, in *Fundamental Algebraic Geometry - Grothendieck's FGA explained*, Math. Surveys **123**, AMS (2005), 181-233.

[Is 79] V.A. Iskovskikh, *Modèles minimaux de surfaces rationnelles sur des corps quelconques* (en russe), Izv. Akad. Nauk **43** (1979), 19-43 ; traduction anglaise : Math. USSR Izvestija **14** (1980), 17-39.

[Is 96] V.A. Iskovskikh, *Factorisation des applications birationnelles de surfaces rationnelles du point de vue de la théorie de Mori* (en russe), Uspekhi Math. Nauk **51** (1996), 3-72 ; traduction anglaise : Russian Math. Surveys **51** (1996), 585-652.

[Iv 72] B. Iversen, *A fixed point formula for action of tori on algebraic varieties*, Invent. math. **16** (1972), 229-236.

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

[Ko 07] J. Kollár, *Lectures on resolution of singularities*, Ann. Math. Studies **166**, Princeton Univ. Press, Princeton, 2007.

[KS 00] J. Kollár et E. Szabó, *Fixed points of group actions and rational maps*, Canadian J. Math. **52** (2000), 1054-1056.

[Ma 66] Y.I. Manin, *Les surfaces rationnelles sur les corps parfaits* (en russe, avec résumé anglais), Publ. Math. IHÉS **30** (1966), 415-475 ; traduction anglaise : AMS Translations **76** (1968), 137-185.

[Ma 67] Y.I. Manin, *Les surfaces rationnelles sur les corps parfaits. II* (en russe), Mat. Sbornik **72** (1967), 161-192 ; traduction anglaise : Math. USSR-Sbornik **1** (1967), 141-168.

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

[Mi 87] H. Minkowski, *Zur Theorie der positiven quadratischen Formen*, J. Crelle **101** (1887), 196–202 (= Ges. Abh., Band I, n° VI).

[Mi 11] H. Mitchell, *Determination of the ordinary and modular ternary linear groups*, Trans. AMS **12** (1911), 207-242.

[Mo 82] S. Mori, *Threefolds whose canonical bundles are not numerically effective*, Ann. Math. **116** (1982), 133-176.

[RY 00] Z. Reichstein et B. Youssin, *Essential dimension of algebraic groups and a resolution theorem for G-varieties*, Canadian J. Math. **52** (2000), 1018-1056.

[RY 02] Z. Reichstein et B. Youssin, *A birational invariant for algebraic group actions*, Pacific J. Math. **204** (2002), 223-246.

[Se 99] J-P. Serre, *Sous-groupes finis des groupes de Lie*, Sém. Bourbaki 1998/1999, exposé **864**, Astérisque **266**, 415-430 (= Séminaires 1950-1999, Doc. Math. **1**, 2-ième édition, SMF, 2008, 233-248).

[Se 03] J-P. Serre, *Cohomological invariants, Witt invariants, and trace forms* (Notes by Skip Garibaldi), in *Cohomological Invariants in Galois Cohomology*, ULS **28** , AMS 2003, 1-100.

[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, *How to use finite fields for problems concerning infinite fields*, Contemp. Math., AMS, à paraître.

[Se 09] J-P. Serre, *A Minkowski-style bound for the orders of the finite subgroups of the Cremona group of rank* 2 *over an arbitrary field*, Moscow Math. J. **9** (2009), à paraître.

[Sk 01] A. Skorobogatov, *Torsors and Rational Points*, Cambridge Tracts in Math. **144**, Cambridge Univ. Press, 2001.

[Vo 98] V.E. Voskresenskiĭ, *Algebraic Groups and their Birational Invariants*, Translations Math. Monographs **179**, AMS, 1998.

[Zh 01] D-Q. Zhang, *Automorphisms of finite order on rational surfaces* (with an Appendix by I. Dolgachev), J. Algebra **238** (2001), 560-589.

Jean–Pierre SERRE

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