The Decomposition, Inertia and Ramification Groups in Birational Geometry

M.H.Gizatullin

Let X be an irreducible scheme, let $\mathrm{Bir}(X)$ be its group of birational automorphisms, let G be a subgroup of $\mathrm{Bir}(X)$. If $g \in G$, then $\mathrm{dom}(g)$ denotes the domain of definition of the map g, g^* denotes the corresponding automorphism of the total ring of fractions on X. Let Y be an irreducible reduced subscheme of X, let p_Y be the generic point of Y, let A_Y be the local ring of p_Y, let m_Y be the maximal ideal of A_Y.

The decomposition group of Y in G is

$$G_Y = \{g \in G \mid p_Y \in \mathrm{dom}(g) \cap \mathrm{dom}(g^{-1}), \quad g(p_Y) = p_Y\}.$$

In other words, G_Y is the stabilizer of p_Y in G. There is a natural homomorphism

$$r : G_Y \longrightarrow \mathrm{Bir}(Y). \tag{1}$$

The group G_Y operates on the local ring A_Y, G_Y preserves all the powers of the maximal ideal m_Y, therefore G_Y operates on A_Y/m_Y^{i+1}, $i \geq 0$. The i-th ramification group of Y in G is

$$G_{iY} = \{g \in G_Y \mid g \text{ operates trivially on} A_Y/m_Y^{i+1}\}.$$

In other words, G_{iY} consists of those elements of G_Y that operate trivially on the i-th infinitesimal neighbourhood of Y in X. Especially, G_{0Y} is the kernel of the homomorphism (1). The group G_{0Y} is called the inertia group of Y in G.

Example 1. This example is the origin of the terminology used in the paper. If A is a Dedekind domain, K is its field of fractions, L/K is a finite Galois extension, B is the integral closure of A in L, $X = \mathrm{Spec}B$, Y is a subscheme of X defined by a maximal ideal P of B, $G = \mathrm{Gal}(L/K)$, then G_Y, G_{0Y}, G_{iY} are respectively the decomposition, inertia and ramification groups of P in L/K in the usual sense (see [1], chap. 5, §10).

Example 2. This example indicates that a notion of congruence subgroup is a special case of the notion of the ramification group. Let X be $\mathrm{Proj}\mathbb{Z}[z_0, z_1]$, i.e. X is the projective line over $\mathbb{Z}$, let Y be a curve on X defined by a prime number p (see picture in Mumford's fifth lecture [2]). The group $\mathrm{Bir}(X)$ is isomorphic to $\mathrm{PGL}(2, \mathbb{Q})$, the group $\mathrm{Bir}(X)_Y$ consists of linear fractional transformations with integer coefficients and determinant coprime to p. If $G = \mathrm{PSL}(2,\mathbb{Z})$, $G \subset \mathrm{Bir}(X)$, then $G_Y = G$, G_{iY} is the congruence subgroup $\Gamma(p^{i+1})$.

Let us return to the general situation.

Theorem 1. *For each $i \geq 0$ the group G_{iY} is a normal subgroup of G_Y.*

Proof. G_{iY} is the kernel of a natural homomorphism

$$G_Y \longrightarrow \mathrm{Aut}(A_Y/m_Y^{i+1}).$$

Theorem 2. $(G_{iY}, G_{jY}) \subset G_{(i+j)Y}$, *where $i \geq 0$, $j \geq 0$, (A, B) is a subgroup generated by $a^{-1}b^{-1}ab$, $a \in A$, $b \in B$.*

Proof. If $a \in G_{iY}$, $b \in G_{jY}$, $x \in A_Y$, then

$$a^*(x) = x + \sum_l \Big(\prod_{k=0}^{i} y_{lk}\Big), \qquad b^*(x) = x + \sum_n \Big(\prod_{m=0}^{j} z_{nm}\Big),$$

where y_{lk}, z_{nm} are elements of m_Y. Further

$$b^*a^*(x) \in \left(x + \sum_n \Big(\prod_{m=0}^{j} z_{nm}\Big) + \sum_l \Big(\prod_{k=0}^{i} (y_{lk} + m_Y^{j+1})\Big)\right),$$

$$a^*b^*(x) \in \left(x + \sum_l \Big(\prod_{k=0}^{i} y_{lk}\Big) + \sum_n \Big(\prod_{m=0}^{j} (z_{nm} + m_Y^{i+1})\Big)\right),$$

hence

$$b^*a^*(x) - a^*b^*(x) \in m_Y^{i+j+1}, \qquad (bab^{-1}a^{-1})^*(x) - x \in m_Y^{i+j+1}.$$

Q.E.D.

Theorem 1 and example 2 motivate the following terminology. We shall say that a triple (X, Y, G_Y) has the positive solution of the congruence subgroups problem (briefly, (X, Y, G_Y) has p.s.c.s.p.), if each nontrivial normal subgroup of G_Y contains some nontrivial ramification subgroup G_{iY}. In the opposite case we shall say that this triple has the negative solution of that problem (briefly, (X, Y, G_Y) has p.s.c.s.p.). The congruence subgroup problem for some triples is connected with the unsolved problem of the simplisity of the Cremona group $\mathrm{Bir}(\mathbb{P}_2)$.

Theorem 3. *Let $\mathbb{P}_2$ be the projective plane over an algebraically closed field k, let P be a closed point on the plane, let $G = \mathrm{Bir}(\mathbb{P}_2)$ be the Cremona group. If the triple $(\mathbb{P}_2, P, G_P)$ has p.s.c.s.p., then the group G is simple. In other words, if G is not simple, then there exists a normal subgroup $H \subset G_P$ such that $\{e\} \neq (H \cap G_{iP}) \neq G_{iP}$ for each $i \geq 0$.*

Proof. Let H be a nontrivial normal subgroup of G.

Lemma 1. $H \cap G_P \neq \{e\}$.

Proof. Let g be a nontrivial element of H, $P_0 \in \mathrm{dom}(g) \cap \mathrm{dom}(g^{-1})$. A replacement of g by a suitable conjugate element makes $P_0 = P$. Suppose that $g(P) = Q$, $Q \neq P$ (if $Q = P$, then $g \in H \cap G_P$),

$$M = \{h \in \mathrm{Aut}(\mathbb{P}_2) \mid h(P) = Q, h(Q) = P\}.$$

The set M is a connected 4-dimensional subvariety of $\mathrm{Aut}(\mathbb{P}_2)$. There exists $h \in M$ such that $hgh^{-1} \neq g^{-1}$. Indeed, if g is a projective transformation, then the existence of h is evident, if g has a fundamental point, then a suitable h moves aside fundamental points of g apart ones of g^{-1}. Thus the transformation $hgh^{-1}g$ is nontrivial and belongs to $H \cap G_P$. Q.E.D.

If the triple $(\mathbb{P}_2, P, G_P)$ has p.s.c.s.p., then $H \cap G_P \supset G_{iP}$ for some natural i. Let x, y be the affine coordinates on the projective plane, let P be the origin. The transformation g, defined by the formulae

$$x' = x, \quad y' = y + x^{i+1} \tag{2}$$

belongs to G_{iP}, hence $g \in H$. It is sufficient to prove that the normal closure $\langle g \rangle$ of g in the group G is the whole G (normal closure of a subset is the smallest normal subgroup containing this subset). The transformation (2) preserves the pencil of lines $x = \text{const}$, therefore it is sufficient to prove the following lemma.

Lemma 2. *If a nontrivial birational transformation of the projective plane preserves a pencil of lines, then the normal closure of this transformation in the Cremona group is the whole Cremona group.*

Proof. *Case 1.* Let g be a projective transformation. Since the projective group $\mathrm{Aut}(\mathbb{P}_2)$ over an algebraically closed field is simple, we have $\langle g \rangle \supset \mathrm{Aut}(\mathbb{P}_2)$, therefore the involution h, defined by $x' = 1-x$, $y' = 1-y$, belongs to g. If s is the standard quadratic transformation $x' = 1/x$, $y' = 1/y$, then $s^2 = e$, $(hs)^3 = e$, hence $s = (hs)h(hs)^{-1} \in \langle g \rangle$. The set $\mathrm{Aut}(\mathbb{P}_2) \cup \{s\}$ generates G, therefore $\langle g \rangle = G$.

Case 2. Let g be an arbitrary nontrivial element of the group J of all the birational transformations preserving the pencil $x = \text{const}$. Elements of J are defined by the formulae of the following form

$$x' = (px+q)/(rx+s), \quad y' = \big(a(x)y + b(x)\big)/\big(c(x)y + d(x)\big), \tag{3}$$

where $p,\ q,\ r,\ s \in k,\ \ a,\ b,\ c,\ d \in k[x],\ \ ps - qr \neq 0,\ \ ad - bc \neq 0$. As well as in the proof of lemma 1, there is a transformation h of the form (3) with $p = s = 1,\ \ q = r = 0,\ \ \{a, b, c, d\} \subset k$ such that $ghg^{-1}h^{-1} \neq e$. Thus the transformation $g_0 = ghg^{-1}h^{-1}$ is nontrivial, g_0 is of the form (3) with $p = s = 1,\ \ q = r = 0$, i.e. g_0 is an element of the group

$$\mathrm{Aut}\big(k(x,y)/k(x)\big) = \mathrm{PGL}(2, k(x)).$$

Each nontrivial normal subgroup of the last group contains $\mathrm{PSL}(2, k(x))$, hence $\langle g \rangle$ contains a nontrivial projective transformation, therefore, as it was established in the first case, $\langle g \rangle = G$. Lemma 2 and theorem 2 are proved.

Corollary 1. *Let L be a line on the projective plane over an algebraically closed field, let G be the Cremona group. If the triple $(\mathbb{P}_2, L, G_L)$ has p.s.c.s.p., then the group G is simple.*

Proof. Let H be a nontrivial normal subgroup of G, let x, y be the affine coordinates on $\mathbb{P}_2$. Suppose that $x = 0$ is the equation of L, P is the origin, f is the Cremona transformation defined by $x' = x$, $y' = xy$. By lemma 1 there exists $g_0 \in H \cap G_P$, $g_0 \neq e$. The transformation $g_1 = f^{-1}g_0 f$ belongs to G_L, therefore $H \cap G_L \neq \{e\}$, hence this intersection contains some subgroup G_{iL}. The transformation g of the form (2) belongs to G_{iL}, hence $g \in H$. From lemma 2 it follows that $\langle g \rangle = G$. Q.E.D.

Corollary 2. *Let Y be a plane rational curve which admits a birational straightening, i.e. there is a Cremona transformation f such that the generic point p_Y of Y belongs to $\mathrm{dom}(f) \cap \mathrm{dom}(f^{-1})$ and $f(p_Y)$ is the generic point of some line L. If the triple $(\mathbb{P}_2, Y, G_Y)$ has p.s.c.s.p., then G is simple.*

Proof. If f is the straightening, H is a normal subgroup of G, then according to the proof of corollary 1 $H \cap G_L \neq \{e\}$, hence $H \cap f^{-1}G_L f \neq \{e\}$, i.e. $H \cap G_Y \neq \{e\}$. If H contains G_{iY}, then H contains $G_{iL} = fG_{iY}f^{-1}$. By corollary 1 $H = G$. Q.E.D.

Remark on lemma 2. The methods used in the proofs of lemmas 1, 2 lead to the following result. If a Cremona transformation g transforms some pencil of lines into a pencil of curves of degree d, $d \leq 4$, then $\langle g \rangle = G$. Especially, if $\deg(g) \leq 7$, then $\langle g \rangle = G$. We omit the proof.

Example 3, or more precisely, a construction of some elements of the decomposition group. Let $\mathbb{P}_n$ be the n-dimensional projective space over a field k of characteristic different from 2, $G = \mathrm{Bir}(\mathbb{P}_n)$, let Y be a reduced irreducible hypersurface in $\mathbb{P}_n$, $\deg Y = d$, $d \geq 2$, let P be a k-rational point of $\mathbb{P}_n$ such that the multiplicity of P on Y is equal to $d-2$. We shall construct two involutory transformations $T_P \in G_Y$ and $R_P \in G_{0Y}$. Both of these involutions preserve the general lines through P. Let L be such a line, $L \cap Y = \{P, A, B\}$. The involutions T_P and R_P are defined by the following conditions $T_P(A) = B$, $(T_P \mid L)(P) = P$, $R_P(A) = A$, $R_P(B) = B$. Especially, if $d = 2$, then P does not belong to the quadric Y, $T_P \in \mathrm{Aut}(\mathbb{P}_n)$, R_P is the quadratic inversion with the centre P and fixed quadric Y. If $d = 3$, then Y is a cubic hypersurface, the restriction $t_P = T_P \mid Y$ (i.e. t_P is the image of T_P by the homomorphism (1)) is the involution used by Yu.I. Manin in [3]. If $x = (x_1, ..., x_n)$ are the affine coordinates in $\mathbb{P}_n$, $P = (0, ..., 0)$, $f = 0$ is the equation of Y, where $f = F_{d-2}(x) + F_{d-1}(x) + F_d(x)$, $F_i \in k[x]$, F_i is a homogeneous polynomial of degree i, then the above transformations are defined by the following formulae

$$T_P: \quad x_i' = -x_i F_{d-2}/(F_{d-2} + F_{d-1}),$$

$$R_P: \quad x_i' = -x_i(F_{d-1} + 2F_{d-2})/(F_{d-1} + 2F_d),$$

$$i = 1, ..., n,$$

$$i = 1, ..., n,$$

or

$$R_P: \quad x_i' = x_i - \big(2x_i/(2F_d + F_{d-1})\big)f,$$

$$i = 1, ..., n.$$

Note that the condition char$k \neq 2$ is essential only for the construction of R_P.

Theorem 4. *There are the following relations between the above transformations T_P, R_P and $W \in \mathrm{Aut}(\mathbb{P}_n, Y)$ (i.e. W is a projective k-automorphism preserving Y)*

$$R_P^2 = e, \quad T_P R_P = R_P T_P, \quad W R_P W^{-1} = R_{W(P)}, \tag{4}$$

$$T_P^2 = e, \quad W T_P W^{-1} = T_{W(P)}. \tag{5}$$

Moreover if $A,\ B,\ C$ are three collinear points of the multiplisity $d-2$ on Y, then

$$(T_A T_B T_C)^2 = e. \tag{6}$$

Proof. The relations (4), (5) are evident consequences of the construction of $T_P,\ R_P$. Let L be the line containing $A,\ B,\ C$. Since the family of planes through L is invariant with respect to $T_A,\ T_B,\ T_C$, then it is sufficient to prove that the restriction of $T_A T_B T_C$ on the general plane of this family is involutory. Thus we shall deal with the case when $n = 2$, Y is a curve (maybe reducible) of degree d, $A,\ B,\ C$ are three collinear points of the multiplicity $d-2$ on Y. If $d \geq 4$, then $L \subset Y$ and either

(i) $Y = Z + (d-3)L$, where Z is a reduced curve of the degree 3, L is not a component of Z, the points $A,\ B,\ C$ are simple on Z, or

(ii) $Y = Z + (d-2)L$, where Z is a reduced conic, the points $A,\ B,\ C$ don't lie on the conic.

Let $x,\ y$ be the affine coordinates such that $y = 0$ is the equation of L, let $h = 0$ be the equation of Z, let Z_t be the general member of the pencil $h + ty^3 = 0$ (resp., $h + ty^2 = 0$) in the case (i) (resp., (ii)). The involutions $T_A^{(t)},\ T_B^{(t)},\ T_C^{(t)}$ constructed with the help of Z_t (instead of Z) are independent of the parameter t, i.e. they coincide with $T_A,\ T_B,\ T_C$ respectively. It is obvious that $\left((T_A T_B T_C) \mid Z_t\right)^2 = e$, therefore (6) is true. Q.E.D.

We shall touch upon the question of the surjectivity of the restriction map $r : G_Y \longrightarrow \mathrm{Bir}(Y)$ mentioned in (1). In the classical situation of the example 1 the map r is epimorphism (see [4], ch. 5, n^{0}2, Th.2, (ii)).

Theorem 5. *Let $\mathbb{P}_3$ be the projective space over a perfect field k, $G = \mathrm{Bir}(\mathbb{P}_3)$, let $Y \subset \mathbb{P}_3$ be a minimal smooth cubic surface defined over k. Then the map r is epimorphism, moreover the exact sequence*

$$\{e\} \longrightarrow G_{0Y} \longrightarrow G_Y \longrightarrow \mathrm{Bir}(Y) \longrightarrow \{e\}$$

splits, i.e. there exists a homomorphism $s : \mathrm{Bir}(Y) \longrightarrow G_Y$ such that $rs = id$.

Proof. Let L/k be a quadratic extension of k, A and B be two $\mathrm{Gal}(L/k)$-conjugate points of Y, $C \in Y(k)$ be a rational point collinear with A and B. Then the transformation $S_{AB} = T_A T_B T_C$ is defined over k. Indeed $\mathrm{Gal}(L/k)$-conjugate to S_{AB} is $T_B T_C T_A$ which coincides with S_{AB} by (6), hence $S_{AB} \in G$. The transformations $t_P = T_P \mid Y = r(T_P) \in \mathrm{Bir}(Y)$, $s_{AB} = S_{AB} \mid Y = r(S_{AB}) \in \mathrm{Bir}(Y)$ (where $P \in Y(k)$, $A, B \in Y(L)$ for some quadratic extension L/k, A and B are $\mathrm{Gal}(L/k)$-conjugate) together with the set $\mathrm{Aut}(\mathbb{P}_3, Y)$ generate the group $\mathrm{Bir}(Y)$ (see [3], ch. 5). Therefore r is epimorphic. Defining relations between the mentioned generators are the following

$$t_P^2 = e,\ s_{AB}^2 = e,\ (t_P t_Q t_R)^2 = e \text{ for each collinear triple } P,\ Q,\ R,$$
$$w t_P w^{-1} = t_{w(P)},\ w s_{AB} w^{-1} = s_{w(A)w(B)},\ \text{where } w \in \mathrm{Aut}(\mathbb{P}_3, Y) \mid Y$$

(see [3]). The analogous relations are true for the transformations $T_P,\ S_{AB}$ (see (5), (6)), therefore the definition of the required map s by $s(t_P) = T_P,\ s(s_{AB}) = S_{AB}$ is correct. Q.E.D.

Theorem 6. *If Y is a plane smooth cubic curve over a perfect field k, $Y(k) \neq \emptyset,\ G = \mathrm{Bir}(\mathbb{P}_2/k)$, then the map (1) is surjective.*

Proof. If $Y(k) \neq \emptyset$, then the group $\mathrm{Bir}(Y)$ is generated by the set $\mathrm{Aut}(\mathbb{P}_2, Y) \mid Y$ and the reflections $t_P = T_P \mid Y$, where $P \in Y(k)$. Q.E.D.

The next point is the nontriviality of the higher ramification groups.

Theorem 7. *If Y is an irreducible reduced k-hypersurface in the projective space $\mathbb{P}_n$ over a field k of characteristic different from two, the set $M(Y)$ of points $P \in \mathbb{P}_n(k)$ with $\mathrm{mult}_P(Y) = d-2$ is infinite, then all the groups G_{iY} (where $G = \mathrm{Bir}(\mathbb{P}_n/k)$) are different from $\{e\}$.*

Proof. Let $P \in M(Y),\ R_P$ be the transformation constructed in example 3, $f = 0$ be an affine equation of Y.

Lemma 1. $R_P^*(f) \equiv -f (\mathrm{mod}\ m_Y^2)$.

Proof. Let $x = (x_1, \ldots, x_n)$ be the affine coordinates in $\mathbb{P}_n,\ P = (0, \ldots, 0),\ f = F_{d-2} + F_{d-1} + F_d$, where $F_m = F_m(x)$ is a homogeneous polynomial of degree m. If $D = (F_{d-1} + 2F_{d-2})/(2F_d + F_{d-1}),\ E = 2/(2F_d + F_{d-1})$, then $D = -1 + Ef,\ R_P^*(x_i) = -x_i D,\ i = 1, \ldots, n$ (see example 3). Therefore

$$\begin{aligned} R_P^*(f) &= F_{d-2}(-xD) + F_{d-1}(-xD) + F_d(-xD) = (-D)^{d-2}(F_{d-2} - DF_{d-1} + D^2 F_d) \\ &= (-D)^{d-2}(F_{d-2} + F_{d-1} + F_d - Ef(F_{d-1} + 2F_d) + E^2 f^2 F_d) \\ &= (-D)^{d-2}(-f + E^2 f^2 F_d) \equiv -f (\mathrm{mod}\ m_Y^2). \end{aligned}$$

Q.E.D.

Lemma 2. *If $P,\ Q \in M(Y),\ P \neq Q$, then $R_P R_Q \neq e,\ (R_P R_Q)^*(f) \equiv f (\mathrm{mod}\ m_Y^2)$.*

Proof. The points $P,\ Q$ are among the fundamental points of the transformation $R_P R_Q$, hence this transformation is nonprojective. The congruence of the lemma follows from the preceding lemma. Q.E.D.

Lemma 3. *If $P,\ Q,\ U,\ V$ are four different points of $M(Y),\ a = R_P R_Q,\ b = R_U R_V,\ g = (a, b)$, i.e. $g = a^{-1} b^{-1} ab$, then $g \neq e,\ g \in G_{1Y}$.*

Proof. These four points belong to the set of fundamental points of g, hence $g \neq e$. If z is an element of the local ring A_Y, then $a^*(z) \equiv z + sf (\mathrm{mod}\ m_Y^2),\ b^*(z) \equiv z + tf (\mathrm{mod}\ m_Y^2)$ because of $a,\ b \in G_{0Y}$. By lemma 2 $b^* a^*(z) \equiv z + (s+t)f (\mathrm{mod}\ m_Y^2),\ a^* b^*(z) = z + (s+t)f (\mathrm{mod}\ m_Y^2)$, hence $b^* a^*(z) \equiv a^* b^*(z) (\mathrm{mod}\ m_Y^2),\ (a, b)^*(z) \equiv z (\mathrm{mod}\ m_Y^2)$, i.e. (a, b) is an element of G_{1Y}. Q.E.D.

Let $(P, Q, U, V), (P_1, Q_1, U_1, V_1), (P_2, Q_2, U_2, V_2), \ldots$ be disjoint quadruples of points of $M(Y)$, let $g,\ g_1,\ g_2, \ldots$ be the corresponding commutators constructed in lemma 3. Then these commutators belong to G_{1Y}, $(g, g_1) \in G_{2Y}$ by theorem 2, $(g, g_1) \neq e$ by the reason pointed in the proofs of lemmas 2, 3, $((g, g_1), g_2)$ is a nontrivial element of G_{3Y}, etc. Q.E.D.

References

[1] O. ZARISKI, P. SAMUEL. *Commutative algebra*, vol.1, Van Nostrand, 1958.

[2] D. MUMFORD. *Lectures on curves on an algebraic surface*, Princeton, 1966.

[3] Yu. I. MANIN. *Cubic forms*, Moscow, 1972 (Engl. transl.: North Holland, Amsterdam, 1974, 2-nd edition 1986).

[4] N. BOURBAKI. *Eléments de Mathématique: Algebre commutative*, chap. 1-7, Paris, Hermann, 1961-1965.