A REMARK ON GROUPS OF BIRATIONAL TRANSFORMATIONS AND THE WORD PROBLEM (AFTER YVES DE CORNULIER)

SERGE CANTAT

ABSTRACT. In these notes, I present a result due to Yves de Cornulier. According to it, any finitely generated subgroup of the Cremona group has a solvable word problem. This provides examples of finitely presented groups that can not be embedded into any Cremona group $\mathsf{Cr}_n(\mathbf{k})$ (see [3]).

1.– Introduction. The Cremona group in n variables over a field $\mathbf{k}$ is the group of $\mathbf{k}$-automorphisms of the field of rational functions $\mathbf{k}(X_1,...,X_n)$, where the X_i are n independent indeterminates. Equivalently, the Cremona group $\mathsf{Cr}_n(\mathbf{k})$ is the group of birational transformations of the projective space of dimension n over the field $\mathbf{k}$: $\mathsf{Cr}_n(\mathbf{k}) \simeq \mathsf{Bir}(\mathbb{P}^n_{\mathbf{k}})$.

Not much is known concerning groups, let us say finitely presented groups, that can be embedded into some Cremona group. For example, it is not yet known whether there exists a finite group G which does not embed into $\mathsf{Cr}_4(\mathbf{C})$. In this short manuscript, we remark that the word problem is solvable for finitely generated subgroups of $\mathsf{Cr}_n(\mathbf{k})$, for all integers $n \geq 1$ and all fields $\mathbf{k}$. Thus, there are finitely presented groups that do not embed into any Cremona group.

Remark.— There are $2^{\aleph_0}$ non-isomorphic quotients of the free group of rank 2 (see Neumann's Theorem, [6], Theorem 3.2 page 188). Since there is only a countable family of pairwise non-isomorphic fields, there are only countably many finitely generated groups that can be embedded into Cremona groups. Thus, most finitely generated groups are not realized as groups of birational transformations.

Remark.— When $n = 1$, the Cremona group $\mathsf{Cr}_1(\mathbf{k})$ coincides with the group $\mathsf{PGL}_2(\mathbf{k})$ of automorphisms of $\mathbb{P}^1_{\mathbf{k}}$. For $n \geq 2$, $\mathsf{Cr}_n(\mathbf{k})$ contains finitely generated, non-linear groups (see [2, 3]).

2.– Word Problem. Let Γ be a group, and $A = \{a_1,\ldots,a_k\}$ be a finite set of generators for Γ; hence, Γ is a quotient of the free group $\mathbb{F}(A) \simeq \mathbb{F}_n$ by a normal subgroup $N < \mathbb{F}(A)$.

The word problem for Γ asks for the existence of an algorithm that decides which elements w of $\mathbb{F}(A)$ are elements of N. In other words, the problem is to decide whether $N < \mathbb{F}(A)$ is a recursive subset of the countable set $\mathbb{F}(A)$. The existence or the non-existence of such an algorithm does not depend on the finite set of generators that is chosen to generate Γ.

The following famous result is due to Novikov and to Boone (see [6], chap. IV).

Novikov-Boone Theorem . *There exist finitely presented groups for which the word problem is not solvable.*

We refer to [10] for an account on the word problem in finitely generated groups that includes an introduction to Turing machines and recursive sets (see also [4] for introductory surveys).

3.– Linear Groups. The word problem is solvable for finitely presented linear groups. For instance, Malcev's Theorem says that finitely generated subgroups of a linear group $\mathsf{GL}_n(\mathbf{k})$ ($\mathbf{k}$ any field) are residually finite, and the word problem is solvable in all residually finite, finitely presented groups (see [6], Theorem 4.6 page 195). We now describe a different proof, due to Rabin (see [9]), which does not need finite presentation.

Theorem. *The word problem is solvable for all finitely generated linear groups.*

More precisely, given a subgroup Γ in $\mathsf{GL}_n(\mathbf{k})$, for some integer $n \geq 1$ and some field $\mathbf{k}$, generated by a finite number of matrices $a_1, \ldots, a_k$, there is an algorithm that decides whether a given word w in the a_i is, or is not, the identity matrix $\mathrm{Id} \in \mathsf{GL}_n(\mathbf{k})$. To prove this, one can argue as follows.

First, the set of all entries of the matrices a_i form a finite subset of $\mathbf{k}$; the subfield of $\mathbf{k}$ which is generated by these coefficients is a field of finite type $\mathbf{k}_0$. Such a field is computable, in the sense of [9] (see also [8]). More precisely, the field $\mathbf{k}_0$ is a finite extension of a transcendental extension $k(x_1, \ldots, x_d)$, where k is the prime subfield ($k = \mathbf{Q}$ or $\mathbf{F}_p$ for some prime p); hence, Γ can be written as a finitely generated subgroup of $\mathsf{GL}_m(k(x_1, \ldots, x_d))$ for some multiple m of n: Computing in $\mathsf{GL}_m(k(x_1, \ldots, x_d))$ amounts to compute sums and products of rational fractions with coefficients in the prime field k.

Now, given such a set of matrices a_i in $\mathsf{GL}_m(k(x_1, \ldots, x_d))$, deciding whether a word w in the a_i is the identity is easy: One only needs to algorithmically compute the corresponding product of matrices, and check whether it is equal to Id or not.

4.– Cremona Groups. In the same spirit, one can prove the following theorem.

Theorem A. *Let* $\mathbf{k}$ *be a field, and* $n \geq 1$ *be an integer. If* Γ *is a group of birational transformations of the Cremona group* $\mathsf{Cr}_n(\mathbf{k})$*, and if* Γ *is finitely generated, then the word problem is solvable in* Γ.

Let $[x_0 : \ldots : x_n]$ be homogeneous variables on $\mathbb{P}^n(\mathbf{k})$. To prove this statement, let $f_1, \ldots, f_k$ be a finite, symmetric set of generators of Γ; each f_i is defined by $n+1$ homogeneous polynomial functions, of some degree d_i, in the variables $(x_0, \ldots, x_n)$:

$$f_i[x_0 : \ldots : x_n] = [P_{i,0} : \ldots : P_{i,n}].$$

The coefficients of the P_i, j generate a subfield of finite type $\mathbf{k}_0 \subset \mathbf{k}$. Since this field is computable, there is an algorithm which, given any word w in the f_i, computes the corresponding birational transformation $g_w = w(f_i, 1 \leq i \leq k)$: The output is a list of $n+1$ homogeneous polynomial functions Q_j, such that

$$g_w[x_0 : \ldots : x_n] = [Q_0 : \ldots : Q_n].$$

Checking whether g_w is the identity amounts to decide whether there exists a homogeneous polynomial function Q such that

$$Q_i = x_i Q$$

for all $1 \leq i \leq n$. In other words, one has to decide whether x_i divides Q_i and, if yes, whether the quotient Q_i/x_i depends on i. This, again, can be decided algorithmically.

As a corollary, one gets the following result.

Theorem B. *There exist finitely presented groups with no faithful morphism in any Cremona group. There exists a non-trivial finitely presented group* Γ_M *such that for every* $n \geq 1$ *and every field* $\mathbf{k}$ *all morphisms from* Γ_M *to* $\mathsf{Cr}_n(\mathbf{k})$ *are trivial.*

The first assertion follows from Novikov-Boone Theorem and from Theorem A. The second assertion is a consequence the following construction, due to Miller III (see [7]): There exists a non-trivial finitely presented group Γ_M such that the only quotient of Γ_M having solvable word problem is $\{1\}$.

Remark.— Kharlampovich constructed a finitely presented, solvable group of derived length 3 for which the word problem is not solvable. Such a group does not embed into any Cremona group (see [5]).

Every countable group embeds into a simple group generated by six elements (see [6], Theorem 3.5 page 190). From this result, due to Hall, one obtains the existence of a finitely generated, simple group that does not embed into any Cremona group.

The algorithm given in the proof of Theorem A solves the word problem in exponential time for subgroups of $\mathsf{Cr}_n(\mathbf{k})$; in the case of linear groups, the complexity is polynomial. Since there are finitely presented groups for which the word problem is solvable but is not solvable in exponential time (see [11] Theorem 1.3, and also [1]), there are finitely presented groups with solvable word problem that cannot be embedded into Cremona groups. It is not clear to us whether there does exist a procedure which solves the word problem in polynomial time (for finitely generated or finitely presented subgroups of $\mathsf{Cr}_n(\mathbf{k})$).

REFERENCES

[1] J.-C. Birget, A. Yu. Ol′shanskii, E. Rips, and M. V. Sapir. Isoperimetric functions of groups and computational complexity of the word problem. *Ann. of Math. (2)*, 156(2):467–518, 2002.

[2] Dominique Cerveau and Julie Déserti. Transformations birationnelles de petit degré. *Cours Spécialisés, Société Mathématique de France, à paraître*, pages 1–213, 2011.

[3] Yves de Cornulier. Soficity of cremona groups and sofic profiles. *preprint*, pages 1–16, 2012.

[4] Timothy Gowers, June Barrow-Green, and Imre Leader, editors. *The Princeton companion to mathematics*. Princeton University Press, Princeton, NJ, 2008.

[5] O. G. Kharlampovich. A finitely presented solvable group with unsolvable word problem. *Izv. Akad. Nauk SSSR Ser. Mat.*, 45(4):852–873, 928, 1981.

[6] Roger C. Lyndon and Paul E. Schupp. *Combinatorial group theory*. Classics in Mathematics. Springer-Verlag, Berlin, 2001. Reprint of the 1977 edition.

[7] Charles F. Miller, III. The word problem in quotients of a group. In *Aspects of effective algebra (Clayton, 1979)*, pages 246–250. Upside Down A Book Co. Yarra Glen, Vic., 1981.

[8] Russell Miller. Computable fields and Galois theory. *Notices Amer. Math. Soc.*, 55(7):798–807, 2008.

[9] Michael O. Rabin. Computable algebra, general theory and theory of computable fields. *Trans. Amer. Math. Soc.*, 95:341–360, 1960.

[10] Joseph J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995.

[11] Mark V. Sapir, Jean-Camille Birget, and Eliyahu Rips. Isoperimetric and isodiametric functions of groups. *Ann. of Math. (2)*, 156(2):345–466, 2002.

DÉP. MATHÉMATIQUES ET APPLICATIONS, ENS-ULM, UMR 8553 DU CNRS, 75230 PARIS CEDEX 05

E-mail address: cantat@dma.ens.fr