A SHORT PROOF OF GREENBERG’S THEOREM

GARETH A. JONES

Abstract. Greenberg proved that every countable group $A$ is isomorphic to the automorphism group of a Riemann surface, which can be taken to be compact if $A$ is finite. We give a short and explicit algebraic proof of this for finitely generated groups $A$.

1. Introduction

In 1960 Greenberg [6] proved that every countable group $A$ is isomorphic to the automorphism group of a non-compact Riemann surface, which can be taken to have finite type, that is, to have a finitely generated fundamental group, if $A$ is finite. His proof is quite complicated, using notions of $N$-equivalence and $N$-maximality which he introduced and developed in [7] (however, see [1] for a more elementary geometric proof by Allcock). In 1973 he proved in [9, Theorem 6′] that every finite group is isomorphic to the automorphism group of a compact Riemann surface. (This was also stated without proof in [8, Theorem 4].) His proof of this depends on a delicate construction [9, Theorem 4] of maximal Fuchsian groups with a given signature. Here we give a short algebraic proof of his results in the case of finitely generated groups $A$, based on well-known properties of triangle groups and their finite quotient groups (see Theorem 1). The author is grateful to Alexander Mednykh for asking whether such a proof might be possible, and to David Singerman for many helpful comments concerning Fuchsian groups.

2. The proof

We will prove the following restricted version of Greenberg’s Theorem:

Theorem 1 (Greenberg). Every finitely generated group $A$ is isomorphic to the automorphism group of a Riemann surface, which can be taken to be compact if $A$ is finite.

Proof. Let $\Delta$ be a hyperbolic triangle group

$$\Delta(l, m, n) = \langle X, Y, Z \mid X^l = Y^m = Z^n = XYZ = 1 \rangle,$$

so that $l^{-1} + m^{-1} + n^{-1} < 1$ and $\Delta$ acts by isometries on the hyperbolic plane $\mathbb{H}$. Dirichlet’s Theorem on primes in arithmetic progressions implies that there are infinitely many prime powers $q \equiv -1 \mod (k)$ where $k := \text{lcm}(2l, 2m, 2n)$. For any such $q$ there is a smooth (surface-kernel) epimorphism $\Delta \to G := \text{PSL}_2(\mathbb{F}_q)$, so that the images $x, y$ and $z$ of $X, Y$ and $Z$ have orders $l, m$ and $n$ (see [4, Corollary C] or [17], for example). These orders divide $(q + 1)/2$, so $x, y$ and $z$ act semiregularly.
in the natural action of $G$ on the projective line $\mathbb{P}^1(\mathbb{F}_q)$. Since this action is primitive, the subgroup $H = G_\infty$ of $G$ fixing $\infty$ is a maximal subgroup of index $q + 1$ in $G$, and hence its inverse image $N$ in $\Delta$ is a maximal subgroup of index $q + 1$ in $\Delta$. Since $X, Y$ and $Z$ induce semiregular permutations of orders $l, m$ and $n$ on the cosets of $N$ in $\Delta$, none of their non-identity powers are conjugate to elements of $N$. Thus $N$ has no elliptic elements, so being cocompact (since $\Delta$ is), it is a surface group

$$N = \langle A_i, B_i \mid i = 1, \ldots, g \rangle \bigg/ \prod_i [A_i, B_i] = 1$$

of genus $g$ given by the Riemann–Hurwitz formula

$$g = \frac{q + 1}{2} \left( 1 - \frac{1}{l} - \frac{1}{m} - \frac{1}{n} \right) + 1.$$

Clearly, not every generator $A_i$ or $B_i$ of $N$ can be contained in the core $K$ of $N$ in $\Delta$, since this is the kernel of the action of $\Delta$ on $\mathbb{P}^1(\mathbb{F}_q)$ and $N$ acts non-trivially. Without loss of generality (renaming generators if necessary) we may assume that $B_1 \notin K$.

Now $g > (q + 1)/84$ by (1), so given any finitely generated group $A$ one can choose $q$ so that $g \geq d$, where $d$ is the rank (minimum number of generators) of $A$. One can then find an epimorphism $\theta : N \to A$ by sending the generators $A_i$ of $\Delta$ to a generating set for $A$, and the generators $B_i$ to the identity.

Let $M = \ker \theta$, so $M$ is normal in $N$ with $N/M \cong A$. Clearly $N_\Delta(M) \geq N$, so by the maximality of $N$ in $\Delta$ we must have $N_\Delta(M) = N$ or $\Delta$. In the latter case $M$ is normal in $\Delta$ and is therefore contained in $K$, which is impossible since $B_1 \notin M \setminus K$. Thus $N_\Delta(M) = N$.

The argument so far, which applies to any hyperbolic triple $(l, m, n)$, shows that $A$ is isomorphic to the automorphism group $\text{Aut} M \cong N_\Delta(M)/M = N/M$ of the oriented hypermap $M$ of type $(l, m, n)$ corresponding to the subgroup $M$ of $\Delta$. Indeed, if $A$ is finite then so is $|\Delta : M|$, so that the underlying Riemann surface $S = \mathbb{H}/M$ is compact, of genus $|A|(g - 1) + 1$, and $M$ is a dessin d’enfant in Grothendieck’s sense [10], with automorphism group $A$. (See [16] for background on hypermaps and dessins.) However, we wish to realise $A$ as the automorphism group of $S$, rather than $M$; certainly $\text{Aut} S$ contains $\text{Aut} M$, but it could be larger. Since $N$ has no elliptic elements, neither has $M$, so $M$ acts without fixed points on $\mathbb{H}$; it follows from this (see [14] Theorem 5.9.4, for instance) that $\text{Aut} S \cong N(M)/M$ where $N(M)$ is the normaliser of $M$ in $\text{Aut} \mathbb{H} = \text{PSL}_2(\mathbb{R})$. (Note that $N(M)$ is a Fuchsian group since $M$ is a non-cyclic Fuchsian group, see [14] Theorem 5.7.5 for instance.) Clearly $N_\Delta(M) \leq N(M)$, and we need to prove equality here.

In order to do this, let us choose the triple $(l, m, n)$ so that $\Delta$ is maximal (as a Fuchsian group) and non-arithmetic. (By results of Singerman [20] and Takeuchi [22] these conditions are satisfied by ‘most’ hyperbolic triples: see Remark 2, following this proof, for specific examples.) Since $\Delta$ is non-arithmetic, a theorem of Margulis [18] §IX.7 implies that its commensurator $\Delta$ in $\text{PSL}_2(\mathbb{R})$ is a Fuchsian group. Since $\Delta$ contains $\Delta$, the maximality of $\Delta$ implies that $\Delta = \Delta$ and hence $\Delta$ is the commensurator of each of its subgroups of finite index, including $N$.

Now let $g \in N(M)$, so $\Delta^g \geq N^g = M^g = M$ and $N(M)$ contains both $N$ and $N^g$; moreover, it must do so with finite index, since these groups are cocompact, so $N \cap N^g$ has finite index in $N$ and $N^g$. Since $\Delta$ is the commensurator of $N$ it follows that $g \in \Delta$, so $g \in N_\Delta(M)$ as required.
One cannot regard this as an elementary proof of Greenberg’s results (Allcock gives one in [11]), since those of Margulis, Singerman and Takeuchi which it uses are far from elementary. Nevertheless, the route from them to the required destination is both short and straightforward.

As an example of a triple for which $\Delta$ is non-arithmetic and maximal, one could take $(2,3,n)$ for any prime $n \geq 13$ (or indeed any integer $n > 30$). If $n = 13$, for instance, we require $q \equiv -1 \pmod{156}$; the smallest such prime power is the prime 311, giving genus $g = 15$, so that all groups $A$ of rank $d \leq 15$ are realised. Taking triples $(2,3,21)$ or $(2,4,9)$ allows smaller primes $q = 83$ or 71, both giving $g = 6$. The triple $(4,6,12)$ allows an even smaller prime $q = 23$, but leads to a larger genus $g = 7$.

In the above proof $g$ (and hence $d$) has linear growth as $q \to \infty$. Faster growth can be obtained by replacing the natural representation of $G = PSL_2(q)$ with a different primitive representation. For example, if $3 < q \equiv \pm 3$ or $\pm 13 \mod{40}$ then $G$ has a conjugacy class of maximal subgroups $H \cong A_4$ of index $q(q^2 - 1)/24$ (see [3] Ch. XII, for example). If $l, m$ and $n$ are coprime to 6 then no non-identity powers of $x, y$ or $z$ are conjugate to elements of $H$, so the inverse image $N$ of $H$ in $\Delta$ is a surface group of genus

$$g = \frac{q(q^2 - 1)}{48} \left(1 - \frac{1}{l} - \frac{1}{m} - \frac{1}{n}\right) + 1 > \frac{q(q^2 - 1)}{120},$$

(since $l, m, n \geq 5$), giving cubic growth of $g$ as $q \to \infty$. Again one must choose $(l, m, n)$ so that $\Delta$ is maximal and non-arithmetic: the smallest such example in this case is $(7, 11, 13)$. One must also choose $q$ so that $G$ has generators $x, y$ and $z$ of orders $l, m$ and $n$: for examples, see [4] or [17].

There are many other possibilities for $\Delta$, $G$ and $H$ in this proof: one example, giving even faster growth of $g$, is to use the action of the symmetric group $G = S_p$, for primes $p \geq 5$, on the $(p - 2)!$ cosets of its subgroup $H = AGL_1(p)$ (maximal by the classification of finite simple groups, which includes that of groups of prime degree). Now $H$ is a Frobenius group, that is, non-identity elements of $H$ have at most one fixed point in the natural action of $G$ of degree $p$, so one can ensure that $N$ is a surface group by choosing generators $x, y$ and $z$ for $G$ each with at least two fixed points. One can choose such a triple to generate $G$ as follows. Provided $G_0 := \langle x, y, z \rangle$ is transitive it is primitive since the degree $p$ is prime, so if at least one of $x, y$ and $z$ is a cycle with at least three fixed points then an extension of Jordan’s Theorem in [13] implies that $G_0$ contains the alternating group $A_p$. If, in addition, at least one of $x, y$ and $z$ is odd then $G_0 = S_p$, as required. If $l, m$ and $n$ are the orders of $x, y$ and $z$ then the inverse image $N$ of $H$ in $\Delta = \Delta(l, m, n)$ is a surface group of genus

$$g = \frac{(p - 2)!}{2} \left(1 - \frac{1}{l} - \frac{1}{m} - \frac{1}{n}\right) + 1 > \frac{(p - 2)!}{84},$$

giving super-exponential growth. As an example, if $p = 2l - 3$ one could take $x = (1, 2, \ldots, l)$ and take $y$ to be the cycle $(4,3,2,1,l+1,l+2,\ldots,p)$ of length $m = l + 1$, so that $z = (xy)^{-1}$ is the cycle $(p,p-1,\ldots,4)$ of length $n = p - 3 = 2l - 6$; in this case, since $l,m,n \to \infty$ with $p$, we have $g \sim (p - 2)!/2$ as $p \to \infty$. The lists of exceptions in [20] and [22] show that here $\Delta(l,m,n)$
is maximal and non-arithmetic for each prime $p \geq 13$; for instance, if $p = 13$ then $\Delta = \Delta(8, 9, 10)$, with $g = 13250161$ large enough to realise most finitely generated groups of current interest.

5 The proof in Section 2 is adapted from one in [12, Theorem 3(a)] that for any hyperbolic triple $(l, m, n)$ there are $\aleph_0$ non-isomorphic dessins (finite oriented hypermaps) of type $(l, m, n)$ with a given finite automorphism group $A$. (See [11] for related results by Hidalgo on realising groups as automorphism groups of dessins.) The Riemann surfaces $S$ underlying these dessins have automorphism group containing $A$. It would be interesting to determine whether they can be chosen so that $\text{Aut} S = A$ in those cases where the corresponding triangle group is arithmetic or non-maximal.

6 In [12] it is also shown that for many hyperbolic triples (including all of non-cocompact type and many of cocompact type), every countable group can be realised as the automorphism group of $2^{\aleph_0}$ non-isomorphic oriented hypermaps of that type. It would be interesting to try to deduce Greenberg’s more general theorem for all countable groups $A$ from this type of argument. The main difficulty is that one needs $N$ to have infinite rank, and hence to have infinite index in $\Delta$, so that commensurability cannot be used as in the last paragraph of Section 2 (See also [5] for similar applications of commensurability, and for examples of how arithmetic and non-arithmetic triangle groups behave differently.)

7 In all the above variations of this proof, if $A$ is finite then since the subgroups $M$ have finite index in triangle groups $\Delta$, Belyi’s Theorem [2], as reinterpreted by Grothendieck [10], implies that the Riemann surfaces $S = \mathbb{H}/M$ are defined, as projective algebraic curves, over algebraic number fields. (See [16] Ch. 1] for background on Belyi’s Theorem.) What can be said about these fields? For example, can every finite group $A$ be realised as the automorphism group of a curve (or dessin) defined over $\mathbb{Q}$? By Cayley’s Theorem, $A$ is contained in such a group: the standard generating triples for $S_n$, consisting of cycles of lengths $2, n - 1$ and $n$, are mutually conjugate, so they correspond to a unique regular dessin $D$ with automorphism group $S_n$; the absolute Galois group $\text{Gal} \mathbb{Q}/\mathbb{Q}$ (where $\mathbb{Q}$ is the field of algebraic numbers) preserves the automorphism group and passport (triple of cycle-structures of generators) of any dessin [15], so it preserves $D$ and hence $D$ is defined over $\mathbb{Q}$. (See [19] §4.4, §7.4.1, §8.3.1] for a Galois-theoretic interpretation by Serre of this example of rigidity.)

References

[1] D. Allcock, Hyperbolic surfaces with prescribed infinite symmetry groups, Proc. Amer. Math. Soc. 134 (2006), 3057–3057.
[2] G. V. Belyi, On Galois extensions of a maximal cyclotomic field, Izv. Akad. Nauk SSSR Ser. Mat. 43 (1979), 267–276, 479.
[3] L. E. Dickson, Linear Groups, Dover, New York, 1958.
[4] S. Garion, On Beauville structures for $PSL_2(q)$, J. Group Theory 18 (2015), 981–1019.
[5] E. Girondo, D. Torres-Teigell and J. Wolfart, Shimura curves with many uniform dessins, Math. Z. 271 (2012), 757–779.
[6] L. Greenberg, Conformal transformations of Riemann surfaces, Amer. J. Math. 82 (1960), 749–760.
[7] L. Greenberg, Discrete groups of motions, Canad. J. Math. 12 (1960), 415–426.
[8] L. Greenberg, Maximal Fuchsian groups, Bull. Amer. Math. Soc. 69 (1963), 569–573.
[9] L. Greenberg, Maximal groups and signatures, in Discontinuous Groups and Riemann Surfaces, Proc. Conf. Maryland 1973, ed. L. Greenberg, Princeton University Press, Princeton NJ, 1974, 207–226.
[10] A. Grothendieck, Esquisse d’un Programme (1984), in Geometric Galois Actions 1, ed. L. Schneps and P. Lochak, London Math. Soc. Lecture Note Ser. 242, Cambridge University Press, Cambridge, 1997, 5–47.
[11] R. Hidalgo, Automorphism groups of dessins d’enfants, Arch. Math. (Basel) 112 (2019), 13–18.
[12] G. A. Jones, Realisation of groups as automorphism groups in categories, [arXiv:1807.00547v3 [math.GR]].
[13] G. A. Jones, Primitive permutation groups containing a cycle, Bull Aust. Math. Soc. 89 (2014), 159–165.
[14] G. A. Jones and D. Singerman, Complex Function Theory, Cambridge University Press, Cambridge, 1987.
[15] G. A. Jones and M. Streit, Galois groups, monodromy groups and cartographic groups, in Geometric Galois Actions 2, ed. P. Lochak and L. Schneps, London Math. Soc. Lecture Note Ser. 243, Cambridge University Press, Cambridge, 25–65.
[16] G. A. Jones and J. Wolfart, Dessins d’Enfants on Riemann Surfaces, Springer, Cham, 2016.
[17] A. M. Macbeath, Generators of the linear fractional groups, in Number Theory (Houston 1967), ed. W. J. Leveque and E. G. Straus, Proc. Sympos. Pure Math. 12, Amer. Math. Soc., Providence RI, 1969, 14–32.
[18] G. Margulis, Discrete Subgroups of Semisimple Lie Groups, Springer-Verlag, Berlin, 1991.
[19] J-P. Serre, Topics in Galois Theory, Jones and Bartlett, Boston Mass., 1992
[20] D. Singerman, Finitely maximal Fuchsian groups, J. London Math. Soc. (2) 6 (1972), 29–38.
[21] D. Singerman and R. I. Syddall, The Riemann surface of a uniform dessin, Beiträge Algebra Geom. 44 (2003), 413–430.
[22] K. Takeuchi, Arithmetic triangle groups, J. Math. Soc. Japan 29 (1977), 91–106.

School of Mathematical Sciences, University of Southampton, Southampton SO17 1BJ, UK
E-mail address: G.A.Jones@maths.soton.ac.uk