How to Draw a Group

Alexander Zvonkin*

LaBRI, Université Bordeaux I, 351 cours da la Libération, F-33405 Talence Cedex France

Abstract

A map is at the same time a group. To represent a map (that is, a graph *drawn* on the sphere or on another surface) we usually use a pair of permutations on the set of the "ends" of edges. These permutations generate a group which we call a *cartographic group*. The main motivation for the study of the cartographic group is the so-called theory of "dessins d'enfants" of Grothendieck, which relates the theory of maps to Galois theory [24].

In the present paper we address the questions of identifying the cartographic group for a given map, and of constructing the maps with a given cartographic group.

1 Maps and cartographic groups

The same graph can be drawn in different topological ways, as is shown in Figure 1 (we consider these graphs as drawn on the sphere).

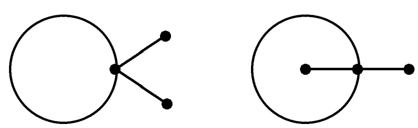

Figure 1: One graph, but two maps

The combinatorial structure that reflects not only the graph properties but also those of its embedding is called a map.

*E-mail: zvonkin@labri.u-bordeaux.fr. The author is partially supported by PRC Math-Info and by EC grant CHRX-CT93-0400.

Definition 1.1 A *map* is a connected graph (loops and multiple edges are allowed) which is "drawn" on (embedded into) a compact oriented two-dimensional surface in such a way that:

1. the edges do not intersect;

2. if we "cut" the surface along the edges, we get a disjoint union of sets which are homeomorphic to an open disk (these sets are called *faces* of the map).

In the example above the left-hand map has two faces, of degree 5 (the outer face) and 1, while the right-hand map has both faces of degree 3.

The additional information one needs to represent a map is the rotational order of edges around each vertex. Consider the set B of the "ends of edges" (each edge has two ends, hence the number of elements in B is twice the number of edges). Let α be the permutation on B that transposes the ends of each edge; let σ be the permutation that rotates the ends adjacent to each vertex counterclockwise (we use the fact that the surface on which the map is drawn is oriented).

The permutations α and σ must satisfy the following conditions:

1. All the cycles of α have the length 2, or, in other words, α is an involution without fixed points (this condition means that each edge has exactly two ends).

2. The permutation group $G = <\alpha, \sigma>$ generated by α and σ acts transitively on B (this condition means that the graph is connected).

The example that follows was a starting point for our interest in the combinatorics of the cartographic group. It was presented by Günter Malle in his talk on the conference "Dessins d'enfants (Cartes cellulaires de Riemann)" held at Luminy in April 1993.

Example 1.2 Consider the map with 6 edges drawn in Figure 2. We number the ends of edges by $1, 2, \ldots, 12$ in an arbitrary way, for example as in the figure. Then

$$\alpha = (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)$$

and

$$\sigma = (1,6,2)(4,11,8)(5,7,9).$$

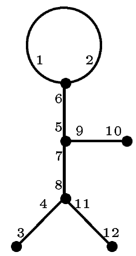

Figure 2: Example of G. Malle

The cycle type of σ is $3^3 1^3$, which corresponds to the vertex degrees. The faces of the map can be reconstructed as the cycles of the permutation $\varphi = \alpha\sigma^{-1}$ (we multiply the permutations from left to right: this notation corresponds to that used in MAPLE group package). In our example,

$$\varphi = (1, 6, 9, 10, 7, 11, 12, 4, 3, 8, 5).$$

The cycle type of this permutation is $11^1 1^1$, which corresponds to the face degrees. The pair of permutations (α, φ) corresponds to the map dual to that of (α, σ). If we remove the condition of α being an involution without fixed points, we get the definition of a *hypermap*; the *hyperedges* of a hypermap may have any number of ends. For details on this approach to the theory of maps and hypermaps see [12].

The definition of the cartographic group was "almost given" above.

Definition 1.3 The *cartographic group* of a map is the permutation group $G = <\alpha, \sigma>$ generated by the permutations α and σ. We also say that the map *represents* its cartographic group.

Remark 1.4 In some publications this group is called *effective cartographic group.*

Remark 1.5 A map and its dual obviously represent the same group, because $\varphi = \alpha\sigma^{-1}$ implies that $<\alpha, \sigma> = <\alpha, \varphi>$. For a planar map (α, σ), the map axially symmetric to it is described by the pair of permutations (α, σ^{-1}), which again gives us the same group.

Remark 1.6 For a bipartite map we may also consider a simpler object, its *monodromy group.* This is a permutation group on the set of *edges* generated by rotations of the edges around "black" vertices and around "white" ones. Note that each tree is bipartite.

Though the above combinatorial definition of a map is well-known, to the best of our knowledge very little attention has been paid to the study of the cartographic group. For the specialists in the theory of maps this group was always a kind of a "transparent object" through which they used to look directly at the maps. As for the group theorists, quite a lot of research was undertaken concerning the finite groups generated by two elements (see, for example, [6], [7], [20]); but an interest in maps as a specific object of study is very rarely manifested. There is a vast literature dedicated to the *groups of automorphisms* of maps; but this object is very different from the cartographic group.

The new interest in the structure of the cartographic group and its relations to the structure of the corresponding map arose in connection with the theory of "dessins d'enfants", where this group is supposed to play a fundamental role (see [24]).

2 Small maps

How do we recognize the cartographic group for a given map? For small maps, we may use the tables of transitive permutation groups given in [8].

Example 2.1 Let us consider the maps in Figure 1. It is a matter of a second for MAPLE to compute the order of the groups: for the left-hand map it is 120, for the right-hand one it is 24. Looking through the table [8] we find out that there is only one transitive subgroup of S_6 of order 120. This is the group $PGL_2(5)$ (as an abstract group it is isomorphic to S_5).

Example 2.2 As for the transitive subgroups of S_6 of order 24, there are three of them, not conjugate to each other in S_6. The following additional information is helpful in order to recognize the "right" group: the cycle types of the permutations α, σ, φ are 2^3, $4^1 1^2$ and 3^2. Looking through the cycle type distribution tables of the same paper [8] we find out that only one of the subgroups of order 24 has the elements of all the three cycle types. It is the group S_4 together with its natural action on 6 cyclic orders of 4 elements.

Remark 2.3 (G. Jones) The latter group is also isomorphic to the rotation group of an octahedron, permuting its six vertices. Indeed, one can "see" this from Figure 1, where the second map is just the quotient of the octahedron by the rotation group of order 4 fixing a vertex.

Example 2.4 The following map presents a "difficult" case.

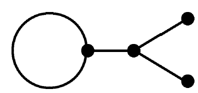

Figure 3: A map representing $PSL_2(7)$

The order of the group is 168. There are two permutation groups of degree 8 and of order 168: one is $PSL_2(7)$, the other one is the group of semi-affine transformations of the field $GF(8)$. Unfortunately, both of them contain elements of the cycle types 2^4, $3^2 1^2$ and $7^1 1^1$. In order to show that the correct answer is $PSL_2(7)$ we need a new method. We used the method presented below in the study of the group M_{12}. Roughly speaking, it consists in starting from the group, not from the map. Another proof was given by G. Jones (private communication).

Example 2.5 Consider the map of Figure 2. The order of the group is 95040. This case would be an easy one, had we a table of transitive groups of degree 12 (there are about 300 of them). In fact, it is not difficult to *prove* that there exists only one (up to a conjugation) permutation group of degree 12 and of order 95040, namely, the Mathieu group M_{12}. But we would like to maintain the purely experimental nature of this work.

3 The group M_{12}

Five Mathieu groups, traditionally denoted as M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, were constructed by Émile Mathieu in the last century [21], [22]. For more than 100 years they were the only sporadic simple finite groups known; nowadays they stand at the beginning of the famous list of 26 sporadic finite groups (see [14], [11]). For a more complete bibliography and more substantial information see [10].

The group M_{12}, as all the other Mathieu groups, has several dozens of equivalent definitions (see, for example, [10], [11]). We have chosen the one which is technically convenient for us, namely, when one of the generators is an involution without fixed points.

Definition 3.1 The group M_{12} is the permutation group of degree 12 generated by the following three permutations:

$$\begin{aligned}
\alpha &= (1,2)(3,4)(5,6)(7,8)(9,10)(11,12),\\
\beta &= (1,3,5,7,9,6,11,8,10,12,4),\\
\gamma &= (4,8,5,11)(6,7,12,9)
\end{aligned}$$

(see [14], section 2.2; the numeration of elements is changed).

The order of the group M_{12} is $95040 = 2^6 \times 3^3 \times 5 \times 11 = 12 \times 11 \times 10 \times 9 \times 8$. It is 5-*transitive*, i.e., it can take any 5 elements (out of 12) to any other 5 elements. It is *simple*, i.e., it does not have any proper normal subgroups.

Proposition 3.2 *The group* $<\alpha, \beta, \gamma>$ *of* Definition 3.1 *coincides with the group* $<\alpha, \sigma>$*, the cartographic group of the map of* Figure 2.

Proof

```
Script started on Wed Jul 27 16:53:25 1994
bash$ maple
    |\^/|     Maple V Release 2 (Universite de Bordeaux I)
._|\|   |/|_. Copyright (c) 1981-1992 by the University of Waterloo.
 \  MAPLE  /  All rights reserved. MAPLE is a registered trademark of
 <____ ____>  Waterloo Maple Software.
      |       Type ? for help.
> with(group);

  [DerivedS, LCS, NormalClosure, RandElement, Sylow, areconjugate, center,

      centralizer, core, cosets, cosrep, derived, groupmember, grouporder,

      inter, invperm, isabelian, isnormal, issubgroup, mulperms, normalizer,

      orbit, permrep, pres]

> alpha:=[[1,2],[3,4],[5,6],[7,8],[9,10],[11,12]];

          alpha := [[1, 2], [3, 4], [5, 6], [7, 8], [9, 10], [11, 12]]

> beta:=[[1,3,5,7,9,6,11,8,10,12,4]];

                 beta := [[1, 3, 5, 7, 9, 6, 11, 8, 10, 12, 4]]
```

```
> gamma:=[[4,8,5,11],[6,7,12,9]];

                    gamma := [[4, 8, 5, 11], [6, 7, 12, 9]]

> M:=permgroup(12,{alpha,beta,gamma});

M := permgroup(12,

    {[[1, 2], [3, 4], [5, 6], [7, 8], [9, 10], [11, 12]],

        [[1, 3, 5, 7, 9, 6, 11, 8, 10, 12, 4]], [[4, 8, 5, 11], [6, 7, 12, 9]]}

    )

> grouporder(M);

                                  95040

> sigma:=[[1,6,2],[4,11,8],[5,7,9]];

                  sigma := [[1, 6, 2], [4, 11, 8], [5, 7, 9]]

> groupmember(sigma,M);

                                   true

> G:=permgroup(12,{alpha,sigma});

   G := permgroup(12, {[[1, 2], [3, 4], [5, 6], [7, 8], [9, 10], [11, 12]],

                          [[1, 6, 2], [4, 11, 8], [5, 7, 9]]}              )

> grouporder(G);

                                  95040

> quit
bytes used=1119364, alloc=786288, time=5.45
bash$ exit
exit

script done on Wed Jul 27 17:11:03 1994
```

In this proof we first define the group $M_{12} = <\alpha, \beta, \gamma>$ according to Definition 3.1 (and verify that its order is equal to 95040, just in case). Then, using the `groupmember` function we verify that $\sigma \in M_{12}$; hence the group $G = <\alpha, \sigma>$ is a certain subgroup of M_{12}. Finally, the fact that $|G| = |M_{12}| = 95040$ implies that the group G coincides with M_{12}.

Remark 3.3 As is shown in [28], the least possible genus of a map that has M_{12} as its *group of automorphisms* is 3169. This remark is made in order to underline once more the difference between the notions of cartographic group and group of automorphisms.

The most difficult part of the proof is hidden in the choice of the permutation σ. We may agree to label the ends of edges by successive numbers, i.e., to take $\alpha = (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)$. But even after this convention there still exist $6! \times 2^6 = 46080$ possibilities of different ends labellings, and hence the choice of σ is far from being unique. Among 46080 possible choices of σ the majority leads not to the group M_{12} as it is defined in Definition 3.1 but to some of its conjugate copies inside S_{12}. In such a case the `groupmember` function will reply `false` and our proof will collapse. So the question is, how to find an appropriate candidate for σ?

What we suggest is trying a random element $\sigma \in M_{12}$ (the MAPLE function `RandElement` generates random elements of the permutation groups). This method, strange as it may seem, produces unexpectedly good results.

Given the permutation α as above, how many elements $\sigma \in M_{12}$ are there such that $<\alpha, \sigma> = M_{12}$? The complete search was carried out by N. Hanusse; it shows that there are 60960 such elements, i.e., more than 64%. Among them plane maps occur 12000 times, maps of genus 1 occur 29760 times, and maps of genus 2 occur 19200 times. But this huge work was undertaken only in order to get the final approval of the previously obtained results: in 20 minutes of computation we examined 500 randomly chosen elements of M_{12} and obtained more than 300 maps (in fact, twice as much, because together with each σ we also considered $\varphi = \alpha\sigma^{-1}$ and the corresponding map). Thus we established the complete list of plane maps having M_{12} as the cartographic group. This list consists of 50 maps. Here is a small sample of them:

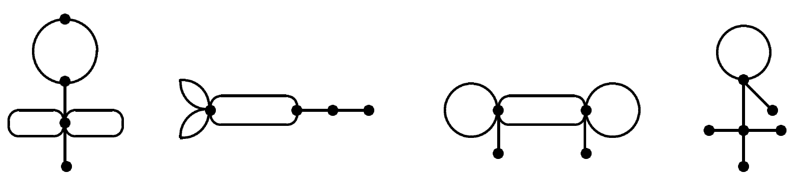

Figure 4: A sample of maps representing M_{12}

4 M_{24} and others

It goes without saying that the method described above works for many other groups (for example, for the group $PSL_2(7)$ mentioned in Section 2). Below we give two "portraits" of the Mathieu group M_{24}, which is, according to J. H. Conway [11], "the most remarkable finite group". There exist many other examples, but the list for M_{24} is not yet complete. See also [15]. (The least genus of a map with the symmetry group M_{24} is 10200961, see [9].)

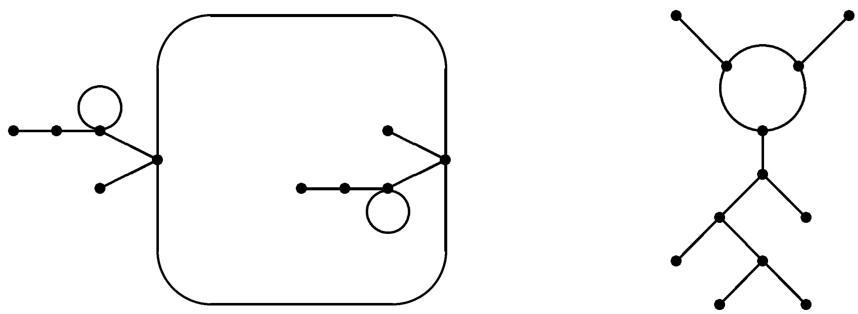

Figure 5: Two maps representing M_{24}

The groups M_{11} and M_{23} are generated as monodromy groups of bicolored plane trees in [1]. There are exactly 2 trees (with 11 edges) for M_{11}, and exactly 4 trees (with 23 edges) for M_{23}.

Remark 4.1 The possibility of generating finite groups by only two elements was studied by many authors; see, for example, [27], [3] and [20]. In [20] it is shown that every non-abelian finite simple group can be generated by two elements, one of which has order 2, so such a group is isomorphic to the cartographic group of a map.

5 Theory of "dessins d'enfant"

To any map of genus g there corresponds a Riemann surface X of the same genus together with a meromorphic function $f : X \to \overline{\mathbb{C}}$ which has only 3 critical values, namely, 0, 1 and ∞, and all pre-images of 1 are critical points of order 2. The map itself can be recovered as the pre-image of the segment $[1, \infty] \subset \overline{\mathbb{C}}$. The pair (X, f) is called a *(pure) Belyi pair*. For a given map, the corresponding Belyi pair is unique, up to an isomorphism of the Riemann surface X. In the planar case $X = \overline{\mathbb{C}}$, hence only one element of the pair is to be found, the *Belyi function* f, which in this case is rational. This correspondence was introduced in the famous paper [4] in connection with Galois theory. The relations to maps and cartographic groups were indicated by Grothendieck [16]. For the later development of the theory see, for example, [25], [5], [24], [26].

Both X and f are defined over the field $\overline{Q}$ of algebraic numbers. In a naïve language this means that "their coefficients are algebraic numbers". Let $\Gamma = \mathrm{Gal}(\overline{Q} \,|\, Q)$ be the absolute Galois group, i.e., the group of automorphisms of $\overline{Q}$. By acting on (X, f) this group acts also on maps. The action is faithful ([4]).

The main interest of the theory is to find combinatorial invariants of this action. Some of the invariants are rather simple. For example, the set of degrees of the vertices and faces of a map is one of such invariants; another one is the group of automorphisms of a map. The cartographic group is one of the most powerful invariants of the Galois group action (the theorem that it is really an invariant is proved in [18]).

Computing a Belyi pair corresponding to a given map is sometimes an extremely difficult task, incomparable with that of computing, say, the order of its cartographic group. This may provide us with the information inaccessible by other means.

Example 5.1 Consider the family of plane maps with the vertex degrees 6, 3, 2, 1, and the face degrees also 6, 3, 2, 1. There are 18 maps with this set of degrees. Computation of the corresponding Belyi functions proved to be incredibly difficult (see [19]). It took us several months of efforts and became possible only after N. Magot developed an interface between MAPLE and GB (the latter is a specialized package to compute Gröbner bases). The results show that the set of 18 maps splits into three Galois orbits, of size 4, 6 and 8 respectively.

But it is only a matter of minutes to find out that the 4 maps of the first orbit have a solvable group of order 648 as their cartographic group; the 6 maps of the second orbit have cartographic group A_{12}; and the 8 maps of the remaining orbit have cartographic group M_{12}. Thus the splitting of this set of maps into at least three orbits could be easily predicted on the basis of the Galois invariance of the cartographic group.

Example 5.2 There are some hints that the relations of cartographic groups to Galois theory are even closer than that. In the example of G. Malle considered above, the set of vertex-face degrees is 3, 3, 3, 1, 1, 1 for vertices and 11, 1 for faces. There are exactly two maps having this set of degrees. Hence the *field of definition* (i.e. the field to which belong all the coefficients of Belyi function) must be quadratic. We may even guess that it is an imaginary quadratic field, because one of the maps is axially symmetric to the other, so Galois action must coincide with the complex conjugation. But to find the field itself we must undertake huge computations. They were carried out by N. Magot. The corresponding Belyi function looks as follows:

$$f(z) = \frac{Kz}{(z^3 - z^2 + az + b)^3 (z^3 + cz^2 + dz + e)},$$

where

$$\begin{aligned}
K &= -\frac{16192}{301327047}a + \frac{10880}{903981141}, \\
a &= \frac{107 \pm 7\sqrt{-11}}{486}, \\
b &= -\frac{13}{567}a + \frac{5}{1701}, \\
c &= -\frac{17}{9}, \\
d &= \frac{23}{7}a + \frac{256}{567}, \\
e &= -\frac{1573}{567}a + \frac{605}{1701}.
\end{aligned}$$

If one takes $f(z) - 1$, its numerator is of the form $-B(z)^2$, where

$$\begin{aligned}
B(z) &= z^6 + \frac{1}{11}[(10c - 8)z^5 + (5a + 9d - 7c)z^4 + \\
&\quad (2b + 4ac + 8e - 6d)z^3 + (3ad + bc - 5e)z^2 + 2aez - be].
\end{aligned}$$

We see that the field in question is $\mathbb{Q}(\sqrt{-11})$. Now, if we look into the character tables of the groups M_{11} and M_{12} (see [10]), we will see that all the entries of both tables belong to the field $\mathbb{Q}(\sqrt{-11})$.

There exists one more quadratic orbit with the cartographic group M_{12}, its set of degrees being 4, 4, 1, 1, 1, 1 for vertices and 11, 1 for faces (see the right-most picture in Figure 4). The similar computations show that the field of definition of this orbit is once again $\mathbb{Q}(\sqrt{-11})$.

For the pair of trees with 11 edges and with monodromy group M_{11}, mentioned in the previous section, the computations are much more difficult. They were carried out by Yu. Matiyasevich by means of the techniques of LLL-algorithm first proposed in [13]. Some of the coefficients of *Shabat polynomial* (a simplified version of Belyi functions for trees) have up to 50 digits. But the field of definition is once more $\mathbb{Q}(\sqrt{-11})$!

We know nothing about the underlying mechanism that leads to these results.

Acknowledgments

The author would like to thank N. Adrianov, R. Cori, N. Hanusse, S. Kerov, M. Klin, Yu. Kochetkov, A. Machì, N. Magot, Yu. Matiyasevich and G. Shabat for numerous fruitful discussions. My special gratitude is due to Gareth Jones who elucidated to me many unclear points.

References

[1] N. Adrianov, Yu. Kochetkov, A. Suvorov and G. Shabat, Mathieu groups and plane trees, Fundamentalnaya i prikladnaya matematika 1 (1995) 377–384 (in Russian).

[2] N. Adrianov and A. Zvonkin, Composition of plane trees, Acta Appl. Math. (to appear).

[3] M. Aschbacher and R. M. Guralnik, Some applications of the first cohomology group, J. of Algebra 90 (1984) 446–460.

[4] G. Belyi, On Galois extensions of a maximal cyclotomic field, Math. USSR Izvestija 14 (1980) 247–256.

[5] J. Bétréma, D. Péré and A. Zvonkin, Plane trees and their Shabat polynomials. Catalog, Rapport interne du LaBRI, Bordeaux, 1992.

[6] J. Brenner and J. Wiegold, Two generator groups II, Bull. Austral. Math. Soc. 22 (1980) 113–124.

[7] J. Brenner, R. Guralnik and J. Wiegold, Two generator groups III, in Contributions to Group Theory, Contemporary Mathematics 33 (1984) 82–89.

[8] G. Butler and J. McKay, The transitive groups of degree up to eleven, Comm. in Algebra 11 (1983) 863–911.

[9] M. Conder, The symmetric genus of the Mathieu groups, Bull. of the London Math. Soc. 23 (1991) 445–453.

[10] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, Atlas of Finite Groups. Maximal Subgroups and Ordinary Characters for Simple Groups (Clarendon Press, Oxford, 1985).

[11] J. H. Conway and N. J. A. Sloane, Sphere Packings, Lattices and Groups (Springer-Verlag, 1988).

[12] R. Cori and A. Machì, Maps, hypermaps and their automorphisms: a survey, I, II, III, Exposition. Math. 10 (1992) 403–427, 429–447, 449–467.

[13] J.-M. Couveignes, Calcul et rationnalité de fonctions de Belyi en genre 0, Ann. de l'Inst. Fourier 44 (1994) 1–38.

[14] D. Gorenstein, Finite Simple Groups. An Introduction to their Classification (Plenum Press, 1982).

[15] L. Granboulan, Construction d'une extension régulière de $\mathbb{Q}(T)$ de groupe de Galois M_{24}, Experimental Math. 5 (1996) 3–14.

[16] A. Grothendieck, Esquisse d'un programme, Unpublished manuscript, 1984.

[17] G. A. Jones and S. A. Silver, The monodromy genus of the Suzuki groups, Contemporary Math. 184 (1995) 215–224.

[18] G. A. Jones and M. Streit, Galois groups and plane trees, Preprint, University of Southampton, 1994.

[19] N. Magot, Computing Belyi functions: A case study (in preparation).

[20] G. Malle, J. Saxl and T. Weigel, Generators of classical groups, Geom. Dedicata 49 (1994) 85–116.

[21] E. Mathieu, Mémoire sur le nombre de valeurs que peut acquérir une fonction quand on y permute ses variables de toutes les manières possibles, J. de Math. Pures et Appl. 5 (1860) 9–42.

[22] E. Mathieu, Sur la fonction cinq fois transitive de 24 quantités, J. de Math. Pures et Appl. 18 (1871) 25–46.

[23] Yu. Matiyasevich, Calculation of generalized Chebyshev polynomials on computer, Vestnik Moskovskogo Universiteta (1996) no. 6, 59–61 (in Russian).

[24] L. Schneps, ed., The Grothendieck Theory of Dessins d'Enfants (Cambridge University Press, cambridge, 1994).

[25] G. Shabat and V. Voevodsky, Drawing curves over number fields, in The Grothendieck Festschrift, vol. 3 (Birkhäuser, 1990) 199–227.

[26] G. Shabat and A. Zvonkin, Plane trees and algebraic numbers, Contemporary Mathematics 178 (1994) 233–275.

[27] R. Steinberg, Generators for simple groups, Canad. J. Math. 14 (1962) 277–283.

[28] A. J. Woldar, Representing M_{11}, M_{12}, M_{22} and M_{23} on surfaces of least genus, Comm. in Algebra 18 (1990) 15–86.