PUBLIKACIJE ELEKTROTEHNIČKOG FAKULTETA UNIVERZITETA U BEOGRADU
PUBLICATIONS DE LA FACULTÉ D'ÉLECTROTECHNIQUE DE L'UNIVERSITÉ À BELGRADE

SERIJA: MATEMATIKA I FIZIKA — SÉRIE: MATHÉMATIQUES ET PHYSIQUE

№ 461 — № 497 (1974)

468. A PRESENTATION OF $PSL_2(F_7)$*

Dragomir Ž. Djoković

The simple group $G = PSL_2(F_7)$ has order 168. It is isomorphic to the group $PSL_3(F_2) = SL_3(F_2) = GL_3(F_2)$.

A presentation of all the groups $PSL_2(F_p)$, where p is a prime, is well-known (e. g. [**1**]). In the case when $p=7$ we find in [**1**], Table 6, p. 138 the following presentation:

$$R^3 = S^3 = (RS)^4 = (R^{-1}S)^4 = E,$$

where

$$R = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \qquad S = \begin{pmatrix} 2 & 0 \\ 1 & -3 \end{pmatrix}.$$

We shall give another presentation of this group which uses involutions as generators and possesses an obvious cyclic symmetry. It is well-known that the group of outer automorphisms $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is cyclic of order 2. One can exhibit an outer automorphism of G by cyclically shifting our generators.

Two involutions in a group generate always a dihedral group. Thus we need at least 3 involutions to generate G. In fact, G can be generated by 3 involutions but we shall start with 6 involutions.

Theorem 1. *Let the group H be generated by a_i $(1 \leqq i \leqq 6)$ with defining relations*

$$a_i^2 = 1 \qquad (1 \leqq i \leqq 6), \tag{1}$$

$$a_i = (a_{i-1}\, a_{i+1})^2 \qquad (1 \leqq i \leqq 6), \tag{2}$$

$$(a_i\, a_{i+3})^3 = 1 \qquad (1 \leqq i \leqq 3), \tag{3}$$

where $a_i = a_{i+6}$. Then H is isomorphic to $G = PSL_2(F_7)$ with

$$a_1 \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad a_2 \to \begin{pmatrix} 3 & -2 \\ -2 & -3 \end{pmatrix}, \quad a_3 \to \begin{pmatrix} 3 & -1 \\ 3 & -3 \end{pmatrix},$$

$$a_4 \to \begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix}, \quad a_5 \to \begin{pmatrix} 3 & 1 \\ -3 & -3 \end{pmatrix}, \quad a_6 \to \begin{pmatrix} 3 & 2 \\ 2 & -3 \end{pmatrix}.$$

Proof. The elements of G can be represented by matrices with determinant 1 over the Galois field F_7. We recall that two such matrices represent the same element of G if they differ in sign. It is easy to see that there exists a homomorphism $f: H \to G$ such that the generators a_i $(1 \leqq i \leqq 6)$ are

* Presented October 20, 1973 by D. S. MITRINOVIĆ.

mapped as indicated in the theorem. We leave to the reader to verify that f is onto.

Let K be the subgroup of H generated by a_1, a_2, a_3 and a_6. A tedious but routine computation using the systematic method of coset enumeration ([1], Ch. 2) shows that $(H:K) \leqq 7$.

From (1) and (2) we obtain $(a_i a_{i+1})^2 = (a_{i-1} a_{i+1})^2 a_{i+1} (a_{i-1} a_{i+1})^2 a_{i+1} = 1$, i. e.,

$$a_i a_{i+1} = a_{i+1} a_i \qquad (1 \leqq i \leqq 6). \tag{4}$$

Every word w in a_1, a_2, a_3 and a_6 can be written in the form $w = w_1 w_2$ where w_1 is a word in a_3, a_6 and w_2 is a word in a_1, a_2. One can obtain such form by using the relations

$$a_1 a_6 = a_6 a_1, \quad a_2 a_6 = a_6 a_2 a_1, \quad a_2 a_3 = a_3 a_2, \quad a_1 a_3 = a_3 a_1 a_2,$$

which follow from (1), (2) and (4). Since $(a_3 a_6)^3 = 1$, $a_3^2 = a_6^2 = 1$ there are at most 6 different words w_1. Since $a_1 a_2 = a_2 a_1$, $a_1^2 = a_2^2 = 1$ there are at most 4 different words w_2. It follows that $|K| \leqq 24$, $|H| \leqq 7 \cdot 24 = 168$. Since $f: H \rightarrow G$ is an epimorphism we have $|H| \geqq |G| = 168$. We infer that $|H| = 168$ and that f is an isomorphism.

The theorem is proved.

Now, it is easy to remove three involutions.

Theorem 2. *The simple group $PSL_2(F_7)$ is isomorphic to the group generated by three elements a, b, c with defining relations*

$$\begin{gathered} a^2 = b^2 = c^2 = (abcbc)^3 = (cabab)^3 = (bcaca)^3 = 1, \\ (abacbc)^2 = b, \ (bcbaca)^2 = c, \ (cacbab)^2 = a. \end{gathered} \tag{5}$$

Proof. Put $a_1 = a$, $a_3 = b$, $a_5 = c$ in (1), (2), (3). The relations (2) for $i = 2, 4, 6$ express a_2, a_4, a_6 in terms of a, b, c. Substituting these expressions for a_2, a_4, a_6 in the remaining relations we obtain (5).

Corollary. *The automorphism $\alpha: a_i \rightarrow a_{i+1} (1 \leqq i \leqq 6)$ of $H \simeq G$ is outer.*

Proof. By Theorem 1 we know that such automorphism exists and it is obviously of order 6. We have a homomorphism $g: H \rightarrow S_7$ such that

$$a_1 \rightarrow (45)(67), \quad a_2 \rightarrow (23)(67), \quad a_3 \rightarrow (27)(36),$$
$$a_4 \rightarrow (14)(36), \quad a_5 \rightarrow (13)(46), \quad a_6 \rightarrow (46)(57).$$

The image of g is doubly transitive and the fixer of 6 and 7 in $\operatorname{Im} g$ has the order $\geqq 4$. Thus $|\operatorname{Im} g| \geqq 4 \cdot 42 = 168$. Therefore g is injective.

If α were inner we would have

$$x^{-1} g(a_1) x = g(a_2), \quad x^{-1} g(a_2) x = g(a_3)$$

for some $x \in S_7$ which is obviously impossible.

Remarks. (i) If we identify H with G as in Theorem 1 then α^2 is the conjugation by $\begin{pmatrix} 3 & -2 \\ 3 & 3 \end{pmatrix}$.

(ii) Note that $\alpha^3 = \beta$ is also an outer automorphism and $\beta^2 = 1$. Thus $\operatorname{Aut}(G)$ is a splitting extension of G.

REFERENCE

1. H. S. M. Coxeter and W. O. J. Moser: *Generators and Relations for Discrete Groups*. New York 1965.