NOTES

Edited by: **John Duncan**

$PSL_2(\mathbf{Z}) = \mathbf{Z}_2 * \mathbf{Z}_3$

Roger C. Alperin

We shall prove that the modular group $\Gamma = PSL_2(\mathbf{Z})$ has the structure of a free product of a cyclic group of order 2 and a cyclic group of order 3. Usually this result is obtained by finding a fundamental domain for the action on the upper half-plane. Here the result is proved in a quite surprising manner using only the action on the irrational numbers. The proof uses the characterization of a free product as the set of alternating words (cf. [L-S, Proposition 12.2]): viz., G is the free product of its subgroups A and B, denoted, $G = A * B$, if and only if it is generated by these subgroups and if $w = a_1b_1a_2b_2 \cdots a_nb_n$ for $a_i \in A$, $b_j \in B$, $1 \leq i, j \leq n$ and a_i, b_j are different from the identity except possibly for $i = 1$ or $j = n$, then w is not the identity element of G.

The group Γ is the quotient group $SL_2(\mathbf{Z})/\{\pm I\}$ where $SL_2(\mathbf{Z})$ is the group of 2×2 integer matrices of determinant 1. It is easy to see using row and column operations and the Euclidean algorithm that the matrices

$$\mu = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \alpha = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

generate $SL_2(\mathbf{Z})$ and hence their images generate Γ. Now let $\beta = \mu\alpha$ and denote similarly their images in Γ. It is clear now that Γ is generated by $A = \langle\alpha\rangle$ and $B = \langle\beta\rangle$. The subgroup A is cyclic of order 2 and the subgroup B is cyclic of order 3.

The group Γ acts via linear fractional transformations on the extended complex numbers and hence also on the set of $\mathscr{I}$ of real irrational numbers. Explicitly if $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in $SL_2(\mathbf{Z})$ then the action on the irrationals is given by

$$z \to \frac{az + b}{cz + d}.$$

The action of the generators is given by

$$\alpha\colon z \to \frac{-1}{z}$$

$$\beta\colon z \to -\frac{1}{z}$$

and

$$\beta^{-1}\colon z \to \frac{1}{1 - z}.$$

To obtain the theorem of the title we prove the alternating word characterization of free products; for this we make some observations about the action. Let $\mathscr{P}$ denote the set of positive irrationals and $\mathscr{N}$ denote the set of negative irrationals.

It is clear that

$$\alpha(\mathscr{P}) \subset \mathscr{N}$$

and

$$\beta^{\pm}(\mathscr{N}) \subset \mathscr{P}.$$

We are now ready to verify the alternating word property. Given a word w which is alternating from A to B, if it is of odd length as a word in $\alpha, \beta^{\pm}$ then either $w(\mathscr{P}) \subset \mathscr{N}$ or $w(\mathscr{N}) \subset \mathscr{P}$ depending on whether the rightmost letter is α or not. If the word is of even length, we can conjugate by α if necessary to obtain a new word w which begins with a power of β and ends with an α. Now, if $w = \beta \cdots \alpha$ then $w(\mathscr{P}) \subset \beta(\mathscr{N})$ is a subset of irrationals greater than 1; similarly, if $w = \beta^{-1} \cdots \alpha$ then $w(\mathscr{P}) \subset \beta^{-1}(\mathscr{N})$ is a subset of positive irrationals less than 1. In any case then $w(z) \neq z$ for some irrational z and thus it is not the identity; since this is a conjugate of the given word we have verified that it too is not the identity element.

REFERENCES

[L-S] Lyndon, Roger C. and Schupp, Paul E., Combinatorial Group Theory, Springer-Verlag, New York, 1971.

Department of Mathematics and Computer Science
San Jose State University
San Jose, CA 95192

Generators for the Algebra of Symmetric Polynomials

D. G. Mead

With n a fixed positive integer, let Σ denote the ring of symmetric polynomials in the variables $x_1, x_2, \ldots, x_n$ with rational coefficients. As is well known, this ring is generated by the elementary symmetric functions in $x_1, x_2, \ldots, x_n$ and also by the first n power symmetric functions $p_i = x_1^i + x_2^i + \cdots + x_n^i$, $1 \leq i \leq n$. In response to a question raised by S. K. Stein in a conversation, we show that these facts are two cases of a more general theorem concerning families that generate Σ.

First, a few definitions. Let $Q[x_1, x_2, \ldots, x_n]$ be the ring of polynomials in the variables $x_1, x_2, \ldots, x_n$ with rational coefficients. Let $k \leq n$ be a positive integer and let $a_1 \geq a_2 \geq \cdots \geq a_k$ be positive integers. We denote by $\langle a_1, a_2, \ldots, a_k \rangle$ the symmetric polynomial $\Sigma x_{i_1}^{a_1} x_{i_2}^{a_2} \ldots x_{i_k}^{a_k}$, where the sum is over all permutations of $\{1, 2, \ldots, n\}$ that yield distinct monomials. Note that the degree of $\langle a_1, a_2, \ldots, a_k \rangle$ is $a_1 + a_2 + \cdots + a_k$. For example, when $n = 3$, $\langle 1 \rangle = x_1 + x_2 + x_3$, $\langle 2 \rangle = x_1^2 + x_2^2 + x_3^2$, $\langle 1, 1 \rangle = x_1x_2 + x_1x_3 + x_2x_3$, and $\langle 2, 1 \rangle = x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2$. The notation $\langle a_1, a_2, \ldots, a_k \rangle$ appears in [2] (p. 82, Ex. 5) and such a polynomial is called (see [1]) a monomial symmetric