A BASIS FOR THE LAWS OF A CLASS OF SIMPLE GROUPS

Dedicated to the memory of Hanna Neumann

BRUCE SOUTHCOTT

Received 30 June 1972, revised 13 April 1973)

Communicated by M. F. Newman

1. Introduction

This paper presents a basis for the laws which hold in each of the finite simple groups, $PSL(2,2^n)$, $n \geqq 2$, thus partially solving a problem raised by Cossey, Macdonald and Street [3]. They considered the more general problem of finding bases for the laws which hold in $PSL(2,p^n)$, and succeded in finding a number of general laws, and in completing bases for $p^n \leqq 11$. The solution of the general problem appears to be very difficult.

In the basis for the laws of $PSL(2,2^n)$ to be given in §4 all laws, except that used to ensure local finiteness, involve two variables. Bryant [1] has shown that two-variable laws suffice to ensure local finiteness in any var $PSL(2,p^n)$, and Bryant and Powell [2] have given a two-variable basis for var $PSL(2,4)$. At this point, at least, the present basis could be improved.

The most important tool in the investigation of laws in $PSL(2,2^n)$ is a systematic use of the character of the natural representation of $SL(2,2^n) \cong PSL(2,2^n)$ as the group of 2×2 unimodular matrices over the field of order 2^n. The relevant properties of this representation are collected in §2. The characterisation of var $PSL(2,2^n)$ also given there enables one to establish quickly whether a given set of laws of $PSL(2,2^n)$ forms a basis for the laws of the variety.

2. Notation, definitions, and preliminary results

The notation and terminology follow [3]. Upper case Roman letters denote groups; lower case letters denote group elements or words. The symbol 1 is used indiscriminately as the multiplicative identity of groups and fields.

The variety generated by the group G is denoted by var G.

2.1 The word u_m is defined recursively by

$$u_3 = \left[\left(x_1^{-1}x_2\right)^{x_{1,2}}, \left(x_1^{-1}x_3\right)^{x_{1,3}}, \left(x_2^{-1}x_3\right)^{x_{2,3}}\right]$$

$$u_m = \left[u_{m-1}, \left(x_1^{-1}x_m\right)^{x_{1,m}}, \cdots, \left(x_{m-1}^{-1}x_m\right)^{x_{m-1,m}}\right].$$

The law $u_m = 1$ has the following properties:

(1) *Every group of order less than m satisfies $u_m = 1$.*

(2) *A group with chief centraliser of index greater than $m-1$ does not satisfy $u_m = 1$.* (Kovács and Newman [4] 1.71, 1.72)

The following result is a simple consequence of the second of these: *A non-abelian simple group which satisfies $u_m = 1$ has order less than m.*

In the next three sub-sections, F denotes an arbitrary field.

2.2 If $x \in SL(2,F)$, then $tr\ x$ denotes the trace of x in the two-dimensional representation. The following properties are used repeatedly without explicit reference:

If $x, y \in SL(2,F)$, then $tr\ x^{-1} = tr\ x$, $tr\ x^y = tr\ x$, and $tr\ xy = tr\ yx$.

2.3 *If $x, y \in SL(2,F)$ then $tr\ xy + tr\ xy^{-1} = tr\ x\ tr\ y$.* ([3] 5.2.1)

2.4 *If $x, y \in SL(2,F)$, then the trace of any word in x and y is a polynomial in $tr\ x$, $tr\ y$, and $tr\ xy$ with integer coefficients.* ([3] 5.2.2)

It follows from this that if $x, y \in SL(2,F)$, then the trace of any word in x and y is uniquely determined by $tr\ x$, $tr\ y$, and $tr\ xy$.

From this point, all fields considered are of characteristic 2. The results in the next four sub-sections are needed for the proof of Theorem 1 (§3).

2.5 *The following identities hold in $PSL(2, 2^n)$*

(1) $tr[x,y] = tr^2x + tr^2y + tr^2xy + tr\ x\ tr\ y\ tr\ xy$.

(2) $tr x^{2^k} = tr^{2^k}x$.

(3) $tr[x,y,x] = tr[x,y]\{tr[x,y] + tr^2x\}$.

([3] 5.2.5 (2), (4), (3).)

(4) $tr[x^{-1},y] = tr[x,y]$.

(5) $tr[x,y]x^{-1} = tr\,x\{1 + tr[x,y]\}$.

(6) $tr[x,y,y] = tr[x,y]\{tr[x,y] + tr^2y\}$.

(7) $tr[x,y,xy] = tr[x,y]\{tr[x,y] + tr^2xy\}$.

(8) $tr[x,y]^{2^k}x^{-1} = tr\,x\{1 + tr^{2^{k-1}}[x,y] + tr^{2^{k-1}+2^{k-2}}[x,y] + \cdots + tr^{2^k-1}[x,y] + tr^{2^k}[x,y]\}$.

(9) $tr[x,y]^{2^k-1}x^{-1} = tr\,x\{1 + tr^{2^{k-1}}[x,y] + tr^{2^{k-1}+2^{k-2}}[x,y] + \cdots + tr^{2^k-1}[x,y]\}$.

([3] 5.2.5 (8) and (9) are special cases of these last two).

https://doi.org/10.1017/S1446788700018097 Published online by Cambridge University Press

PROOFS. (4) $tr[x^{-1}, y] = tr[y, x]^{x^{-1}}$
$= tr[x, y]$

(5) $tr[x,y]x^{-1} = tr\,x\,tr[x, y] + tr\,x[x, y]$
$= tr\,x\{1 + tr[x, y]\}$.

(6) $tr[x, y, y] = tr[y, x, y]$ by (4)
$= tr[x, y]\{tr[x, y] + tr^2 y\}$ by (3).

(7) $tr[x, y, xy] = tr[x, y, y^{-1}x^{-1}]$ by (4)
$tr^2[x,y] + tr^2 xy + tr^2[x, y]y^{-1}x^{-1}$
$+ tr[x, y]tr\,xy\,tr[x, y]y^{-1}x^{-1}$ by (1)
$= tr[x, y]\{tr[x, y] + tr^2 xy\}$.

(8) Proof is by induction on k. From (5) $tr[x, y]x^{-1} = tr\,x\{1 + tr[x, y]\}$, so assume $tr[x, y]^{2^k}x^{-1} = tr\,x\{1 + tr^{2^{k-1}}[x, y] + \cdots + tr^{2^k - 1}[x, y] + tr^{2^k}[x, y]\}$.

Then $tr[x, y]^{2^{k+1}}x^{-1} = tr[x, y]^{2^k} tr[x, y]^{2^k}x^{-1} + tr\,x^{-1}$

$$= tr\,x\{1 + tr^{2^k}[x, y] + tr^{2^k + 2^{k-1}}[x, y] + \cdots + tr^{2^{k+1}-1}[x, y] + tr^{2^{k+1}}[x, y]\}.$$

(9) Proof is by induction on k. Again $tr[x, y]x^{-1} = tr\,x\{1 + tr[x, y]\}$, so assume $tr[x, y]^{2^k - 1}x^{-1} = tr\,x\{1 + tr^{2^{k-1}}[x, y] + \cdots + tr^{2-1^k}[x, y]\}$.

Then $tr[x, y]^{2^{k+1}-1}x^{-1} = tr[x, y]^{2^k} tr[x, y]^{2^k - 1}x^{-1} + tr[x, y]^{-1}x^{-1}$

$$= tr\,x\{1 + tr^{2^k}[x,y] + tr^{2^k + 2^{k-1}}[x,y] + \cdots + tr^{2^{k+1}-1}[x, y]\}.$$

2.6 Any element of $PSL(2, 2^n)$ has order dividing $2, 2^n - 1$ or $2^n + 1$.

If $x \in PSL(2, 2^n)$, then $x^2 = 1$ if and only if $tr\,x = 0$. For elements of odd order, the following identities hold:

(1) $x^{2^n - 1} = 1$, $x \neq 1$ *implies that*

$$1 + tr^{2^{n-2}}x + tr^{2^{n-2}+2^{n-3}}x + \cdots + tr^{2^{n-1}-1}x = 0.$$

(2) $x^{2^n + 1} = 1$, $x \neq 1$ *implies that*

$$1 + tr^{2^{n-2}}x + tr^{2^{n-2}+2^{n-3}}x + \cdots + tr^{2^{n-1}-1}x + tr^{2^{n-1}}x = 0 \qquad ([3]\ 5.2.6).$$

2.7 *If $x, y \in PSL(2,2^n)$ with $[x, y]$ of odd order then $tr[x, y]^{2^{2n-1}-1}x^{-1} = 0$ or, equivalently, $\{[x, y]^{2^{2n-1}-1}x^{-1}\}^2 = 1$.*

PROOF. Suppose $[x, y]$ has order dividing $2^n - 1$. Then

$$[x, y]^{2^{2n-1}-1}x^{-1} = [x, y]^{2^{n-1}-1}x^{-1} \quad \text{and}$$

$$tr[x, y]^{2^{n-1}}x^{-1} = tr\,x\{1 + tr^{2^{n-2}}[x, y] + tr^{2^{n-2}+2^{n-3}}[x, y] + \cdots + tr^{2^{n-1}-1}[x, y]\}$$
$$= 0 \text{ by } 2.6\ (1)$$

Otherwise $[x,y]$ has order dividing 2^n+1.

Then $[x,y]^{2^{2n-1}-1}x^{-1} = [x,y]^{2^{n-1}}x^{-1}$ and

$$\begin{aligned} tr[x,y]^{2^{n-1}}x^{-1} &= tr\,x\{1 + tr^{2^{n-2}}[x,y] + tr^{2^{n-2}+2^{n-3}}[x,y] + \cdots \\ &\qquad + tr^{2^{n-1}-1}[x,y] + tr^{2^{n-1}}[x,y]\} \text{ by 2.5 (8).} \\ &= 0 \text{ by 2.6 (2).} \end{aligned}$$

2.8 *If x and y are elements of a group of exponent dividing some odd number m, which satisfy the relation*

$$[x,y]^{\frac{1}{2}(m-1)}x^{-1} = 1, \quad \text{then } x = 1.$$

PROOF. Suppose $[x,y]^{\frac{1}{2}(m-1)}x^{-1} = 1$.
then

$$[x,y]^{m-1} = x^2$$

and

$$x^{-1}y^{-1}xy = x^{-2}$$

Hence

$$x^y = x^{-1}$$

But this implies that y has even order, or that x has order dividing 2. Hence, $x = 1$, since we are in a group of odd exponent.

The applications of 2.8 in this paper have

$$m = 2^{2n}-1, \ \tfrac{1}{2}(m-1) = 2^{2n-1}-1.$$

The results in the rest of this section are used in the proof of Theorem 2 (§4).

2.9 A characterisation of var $PSL(2,2^n)$.

A group G belongs to var $PSL(2,2^n)$ if and only if it satisfies the following conditions:

(1) *The exponent of G divides $2(2^{2n}-1)$.*

(2) *An element of G of order dividing 2^n+1 which belongs to the normaliser of a 2-subgroup belongs to its centraliser.*

(3) *Subgroups of G of exponent dividing $2^{2n}-1$ are abelian.*

(4) *The law $u_{2^n(2^{2n}-1)+1} = 1$ holds in G.* ([3]).

2.10 *The following laws hold in $PSL(2,2^n)$*:

(1) $x^{2(2^{2n}-1)} = 1$

(2) $[x, y^{2(2^n-1)}]^{2^{2n}-1} = 1$

(3) $u_{2^n(2^{2n}-1)+1=1}$

([3] 3.3 (A) (1), (2), (4).).

A group which satisfies these laws satisfies conditions 2.9 (1), (2) and (4).

https://doi.org/10.1017/S1446788700018097 Published online by Cambridge University Press

3. A new law which holds in *PSL* (2, 2^n)

THEOREM 1. *Let* $p = \left[[x^2, y^2]^{2^{2n}}, x^2\right]^{2^{2n}+2^{2n-1}-2} [y^2, x^2]$,

$$q = \left[p^{-2^{2n}}\, y^2\right]^{2^{2n}+2^{2n-1}-2} p,$$

$$r = \left[q^{-2^{2n}}, x^2y^2\right]^{2^{2n-1}-1} q,$$

then the law $r^2 = 1$ *holds in* $PSL(2, 2^n)$ *and implies that groups of exponent dividing* $2^{2n} - 1$ *which satisfy it are abelian.*

PROOF. The law is trivial unless both x and y are of odd order. First suppose $[x^2, y^2]^2 = 1$. Then $p^2 = q^2, = r^2 = 1$.

Otherwise, $p = [x^2, y^2, x^2]^{2^{2n}+2^{2n-1}-2}[y^2, x^2]$.

Now by 2.7, $p^2 = 1$ if $[x^2, y^2, x^2]$ is of odd order. In this case $p^2 = q^2 = r^2 = 1$.

Otherwise, $q = [x^2, y^2, y^2]^{2^{2n}+2^{2n-1}-2}[y^2, x^2]$, and, in terms of traces $tr[x^2, y^2] = tr^2x^2$, from 2.5 (3), since $tr\,x^2 \neq 0$. Again by 2.7, $q^2 = 1$ if $[x^2, y^2y^2]$ is of odd order.

In this case $q^2 = r^2 = 1$.

Otherwise $r = [x^2, y^2, x^2y^2]^{2^{2n-1}-1}[y^2, x^2]$, and in terms of traces, $tr[x^2, y^2] = tr^2y^2$, from 2.5 (6). If $[x^2, y^2, x^2y^2]$ is of odd order, then $r^2 = 1$.

Now suppose that $tr[x^2, y^2, x^2y^2] = 0$. Then $tr[x^2, y^2] = tr^2x^2y^2$, from 2.5 (7). Hence in this case, we have

$$tr[x^2, y^2] = tr^2x^2 = tr^2y^2 = tr^2x^2y^2.$$

But, from 2.5 (1), $tr[x^2, y^2] = tr^2x^2 + tr^2y^2 + tr^2x^2y^2 + tr\,x^2tr\,y^2tr\,x^2y^2$. Substituting throughout in terms of $tr\,x^2$

$$tr^2x^2 = tr^2x^2 + tr^3x^2,$$

and hence $tr\,x^2 = 0$. This is impossible, so $r^2 = 1$ in all cases.

Now consider a group of exponent dividing $2^{2n} - 1$ in which the law $r^2 = 1$ holds. This implies that $r = 1$ in such a group.

Now $r = [q^{-1}, x^2 y^2]^{2^{2n-1}-1}q = 1$, and applying 2.8, $q = 1$.

In turn, $q = [p^{-1}, y^2]^{2^{2n-1}-1}p = 1$, and again applying 2.8, $p = 1$.

A final application of 2.8 to

$$p = [x^2, y^2, x^2]^{2^{2n-1}-1}[y^2, x^2] \qquad \text{gives} \qquad [x^2, y^2] = 1.$$

Since x^2, y^2 run through all elements of any group of odd exponent as x and y do, any two elements commute.

Hence a group of exponent dividing $2^{2n} - 1$ which satisfies $r^2 = 1$ is abelian.

4. A basis for the laws of $PSL(2, 2^n)$

THEOREM 2. *The following set of laws is a basis for the laws of var* $PSL(2, 2^n)$ $n \geqq 2$

(1) $x^{2(2^{2n}-1)} = 1$.

(2) $[x, y^{2(2^n-1)}]^{2^{2n-1}} = 1$.

(3) $r^2 = 1$.

(4) $u_{2^n(2^{2n}-1)+1} = 1$.

PROOF. All these laws hold in $PSL(2, 2^n)$.
As noted in §2.10, a group which satisfies law (1), (2) and (4) satisfies conditions 2.9 (1), (2) and (4) of the characterisation of var $PSL(2, 2^n)$; and, as proved in Theorem 1, a group which satisfies law (3) satisfies condition 2.9 (3) of that characterisation.

References

[1] Roger M. Bryant, 'On the laws of certain linear groups', *J. London Math. Soc.* (2), 4 (1971), 309–313.

[2] R. M. Bryant and M. B. Powell, 'Two variable laws for *PSL* (2, 5)', *J. Austral. Math. Soc.* 10 (1969), 499–502.

[3] John Cossey, Sheila Oates Macdonald and Anne Penfold Street, 'On the laws of certain finite groups', *J. Austral. Math. Soc.* 11 (1970), 441–489.

[4] L. G. Kovács and M. F. Newman, 'On critical groups', *J. Austral. Math. Soc.* 6 (1966). 237–250.

Department of Mathematics
University of Queensland
St. Lucia, Queensland
Australia

Present address
Department of Mathematics
Queensland Institute of Technology
Australia

https://doi.org/10.1017/S1446788700018097 Published online by Cambridge University Press