

TWO-VARIABLE LAWS FOR $PSL(2, 5)$

R. M. BRYANT¹ and M. B. POWELL

(Received 29 April 1969)

To Bernhard Hermann Neumann on his 60th birthday

Communicated by G. E. Wall

1. Introduction

In [2], John Cossey and Sheila Oates Macdonald give a basis for the set of laws of $PSL(2, 5)$ — the simple group of order 60 — and with one extreme exception the laws of their basis involve at most two variables. They raise the problem of finding a basis in which all of the laws involve only a small number of variables, and remark that they have shown that five variables will suffice. Here we give a basis consisting entirely of two-variable laws.

In notation and terminology we follow [2].

We use a set of two-variable laws including (1)–(6) of [2], and the fact proved there that this set will be a basis for the laws of $PSL(2, 5)$ so long as $PSL(2, 5)$ is the only non-abelian simple group in the variety \mathfrak{B} that the set defines. Consequently we prove

THEOREM. *The only non-abelian simple group in \mathfrak{B} is $PSL(2, 5)$.*

The method used to establish the structure of the simple group is based upon an idea introduced in [1]. If $\{w_i\}_{i=1}^n$ is a set of words of the free group F , we shall say that a group G satisfies the *disjunction* $w_1 \vee w_2 \vee \cdots \vee w_n$ if for every homomorphism $\phi : F \rightarrow G$, $w_i \phi = 1$ for at least one value of i . From a disjunction we may construct words which are laws of every group satisfying the disjunction, and, what is more important, which allow us to recover the disjunction in certain groups — for example non-abelian simple groups — having these words as laws.²

For example, in $PSL(2, 5)$ every element has order 1, 2, 3 or 5; therefore $PSL(2, 5)$ satisfies the disjunctions

$$(7') \quad x^3 \vee x^{10}, \text{ and}$$

$$(8') \quad x^5 \vee x^6,$$

¹ Research supported by a Science Research Council Research Studentship.

² A particular case is that of the *chief centralizer law* and its application in [4] of L. G. Kovács and M. F. Newman, which in fact suggested the more general idea.

giving rise to the two-variable laws

(7) $[x^3, (x^{10})^y]$, and

(8) $[x^5, (x^6)^y]$.

Now if G is a non-abelian simple group, no non-identity element of G can commute with a complete set of conjugates of any other non-identity element. Thus if G satisfies (7) and (8), any element of G is of order dividing 3 or 10, and again of order dividing 5 or 6. Consequently we retrieve in G the fact that every element has order 1, 2, 3 or 5.

The other disjunctions we use are

(9') $[x^6, y^6] \vee (xy)^3 \vee (xy^{-1})^3$, and

(10') $[x^6, y^6] \vee (xy)^2 \vee (xy^2)^2 \vee (xy^3)^2 \vee (xy^4)^2$,

which are easily checked to be satisfied by $PSL(2, 5)$. Essentially they express the fact that two non-commuting elements of order 5 generate the whole group. From these disjunctions we construct the sets of laws under (9) and (10) below. The choice of the conjugating words u_1, u_2, u_3 and u_4 is determined by the need to restrict to two-variable laws, but as a consequence the recovery of the corresponding disjunctions is more difficult. (See Lemma 1.)

2. The basis

\mathfrak{B} is the variety defined by the following set of two-variable laws.

(1) x^{30}

(2) $\{(x^{10}y^{10})^6[x^{10}, y^{10}]^2\}^5$

(3) $\{((x^6y^{12})^5(x^6y^{18})^5)^3[x^6, y^6]^6\}^6$

(4) $[x^3, y^3]^{15}$

(5) $\{[x^6y^{10}x^{-6}, y^{-10}][y^{10}, x^6]\}^{10}$

(6) $\{[y^{10}x^6y^{-10}, x^{-6}][y^{10}, x^6]^2\}^6$

(7) $[x^3, (x^{10})^y]$

(8) $[x^5, (x^6)^y]$

(9) The set of words

$$[x^6, y^6, (xy)^{3u_1}, (xy^{-1})^{3u_2}]$$

with u_1, u_2 , taken from the set $\{1, x, y\}$.

(10) The set of words

$$[x^6, y^6, (xy)^{2u_1}, (xy^2)^{2u_2}, (xy^3)^{2u_3}, (xy^4)^{2u_4}]$$

with u_1, u_2, u_3, u_4 from $\{1, x, y\}$.

3. Proof of the theorem

We have included as (1)–(6) the laws (1)–(6) of [2], and so we have all the results of § 3 of that paper. Thus

- (i) p -groups in \mathfrak{B} are elementary abelian, and
- (ii) an element of order p which belongs to the normalizer of a q -subgroup of a group in \mathfrak{B} belongs to its centralizer if p and q take the values 5 and 2, 5 and 3, or 3 and 5.

We let G be a non-abelian simple group in \mathfrak{B} . Then as remarked above, (7) and (8) give

- (iii) every element of G has order 1, 2, 3 or 5.

(i) and (iii) put us in a familiar situation where we can deduce

- (iv) the Sylow (i.e. maximal) p -subgroups of G are the centralizers of each of their non-identity elements,
- (v) each Sylow subgroup has trivial intersection with any distinct conjugate, and
- (vi) two elements of a Sylow p -subgroup P of G are conjugate in G if and only if they are conjugate in the normalizer $N_G(P)$.

If P is a non-trivial Sylow p -subgroup we see from (iv) that $N_G(P)/P$ acts fixed point freely on P by conjugation, and from (ii) that it is a q -group, where $q = 3, 2$ or 2 according as $p = 2, 3$ or 5 . By a well-known theorem of Frobenius, any subgroup of $N_G(P)/P$ of order q^2 is cyclic: and using (i) we have

- (vii) $[N_G(P) : P]$ divides 3, 2 or 2 according as $p = 2, 3$ or 5 .

We are now able to make our deductions from (9) and (10).

LEMMA 1. G satisfies (9') and (10').

PROOF. Suppose otherwise that, say, (9') is not satisfied for $x = a$ and $y = b$. Let $c_0 = [a^6, b^6]$, $c_1 = (ab)^3$ and $c_2 = (ab^{-1})^3$, so that c_0, c_1 and c_2 are all non-trivial. Let $H = \langle a, b \rangle$, the group generated by a and b .

From (9) we have the relations $[c_0, c_1^{u_1}, c_2^{u_2}] = 1$ for $u_i = 1, a$ or b , $i = 1, 2$. Suppose that $[c_0, c_1^{u_1}] = c \neq 1$ for some choice of u_1 , and let P be the centralizer of c in G . Since $c_2^{u_2} \in P$ for $u_2 = 1, a$ or b , it follows by (iv) and (v) that $H \leq N_G(P)$. Thus $c_0 = [a^6, b^6] = 1$ by (vii), which is a contradiction. Consequently $[c_0, c_1^{u_1}] = 1$ for $u_1 = 1, a$ or b , and arguing in the same way again we deduce that $c_0 = 1$, a final contradiction.

In a similar way we can prove that (10') is satisfied.

LEMMA 2. Any two non-commuting elements of G of order 5 generate a subgroup isomorphic to $PSL(2, 5)$.

PROOF. Suppose that $[a^6, b^6] \neq 1$. Then from (10') we have $(ab^j)^2 = 1$ for $j = 1, 2, 3$ or 4 , and putting $x = a, y = b^j$ in (9') gives $(ab^{-j})^3 = 1$ and so $(b^{-j}a)^3 = 1$. Thus if $H = \langle a, b \rangle$, H is also generated by $c = ab^j$ and $d = b^{-j}a$ with relations $c^2 = d^3 = (cd)^5 = 1$. Since these are defining relations for $PSL(2, 5)$, H is isomorphic to a factor group of $PSL(2, 5)$, and so actually to $PSL(2, 5)$; which proves the lemma.

G contains elements of order 5, for otherwise it would have exponent 6. But a group of exponent 6 is soluble: its finitely generated subgroups are finite and consequently soluble of bounded derived length by the results of [3]. Since G is simple it contains elements of order 5 which do not commute and so

(viii) G contains a subgroup H isomorphic to $PSL(2, 5)$.

Let a and b be elements of order 5 which are in distinct Sylow 5-subgroups of G . Then $\langle a, b \rangle \cong PSL(2, 5)$ by Lemma 2 and so a is conjugate to b or to b^2 . Thus G contains at most two conjugacy classes of elements of order 5. Applying (vi) and (vii) we obtain

(ix) the Sylow 5-subgroups of G have order 5.

If a and b are elements of G of order 2 which are in distinct Sylow 2-subgroups of G , then $\langle a, b \rangle$ cannot be a four-group by (iv). Thus by (iii) $\langle a, b \rangle$ must have twice odd order and a and b are conjugate. Consequently G contains only one conjugacy class of elements of order 2 and so by (vi) and (vii) a Sylow 2-subgroup of G has order not greater than 4. Therefore by (viii)

(x) the Sylow 2-subgroups of G have order 4.

Now let a be any element of G of order 5. Then there is some element b of H of order 5 such that $[a, b] \neq 1$, and so $K = \langle a, b \rangle \cong PSL(2, 5)$ by Lemma 2. $N_H \langle b \rangle = N_K \langle b \rangle = N_G \langle b \rangle$ by (vii) and (ix). By (x), H and K contain complete Sylow 2-subgroups of G and each of these intersects $N_H \langle b \rangle = N_K \langle b \rangle$. Thus H and K contain the same elements of order 2 and, since they are generated by these elements, we have $H = K$ and so $a \in H$. Thus H contains every element of G of order 5. Since G is generated by these elements we have $G = H$ and the proof of the theorem is complete.

References

- [1] R. M. Bryant, D. Phil. thesis, to appear.
- [2] John Cossey and Sheila Oates Macdonald, 'A basis for the laws of $PSL(2, 5)$ ', *Bull. Amer. Math. Soc.* 74 (1968), 602—606.
- [3] Marshall Hall, Jr., 'Solution of the Burnside problem for exponent six', *Illinois J. Math.* 2 (1958), 764—786.
- [4] L. G. Kovács and M. F. Newman, 'Cross varieties of groups', *Proc. Roy. Soc. Ser. A* 292 (1966), 530—536.

Mathematical Institute, Oxford

Mathematical Institute and St. Peter's College, Oxford