

# ON THE LAWS OF CERTAIN FINITE GROUPS

JOHN COSSEY, SHEILA OATES MACDONALD and ANNE PENFOLD STREET

(Received 12 February 1969)

To Bernhard Hermann Neumann on his 60th birthday

Communicated by G. E. Wall

## 1. Introduction

In recent years a great deal of attention has been devoted to the study of finite simple groups, but one aspect which seems to have been little considered is that of the laws they satisfy. In a recent paper [3], the first two of the present authors gave a basis for the laws of  $PSL(2, 5)$ . The techniques of [3] can be used to show that (modulo certain classification problems) a basis for the laws of  $PSL(2, p^n)$  can be made up from laws of the following types:

- (1) an exponent law,
- (2) laws which determine the Sylow subgroups,
- (3) laws which determine the normalisers of the Sylow subgroups,
- (4) in certain special cases, laws which determine subvarieties of smaller exponent, e.g. the subvariety of exponent 12 for those  $PSL(2, p^n)$  which contain  $S_4$ ,
- (5) a law implying local finiteness.

Laws (1) and (5) are easily obtained and this paper reports on an attempt to make a systematic investigation of laws of types (2) and (3) which hold in  $PSL(2, p^n)$ . In general we have most success with  $PSL(2, 2^n)$  and it seems quite likely that it will be possible to find the requisite set of laws. For  $PSL(2, 2^3)$  we have been able to complete the basis. For  $PSL(2, p^n)$  we have not been as successful, though some progress has been made. The laws in these cases are found by a systematic use of the (two-valued) two-dimensional representation and its character; the proofs can be found in § 5. In the cases  $p^n = 7, 9, 11$  we have also been able to complete the bases; the proofs are in § 6. An important feature of the proofs in § 6 is the use of a 2-variable basis for the laws of  $S_4$ ; this can be found in § 4. In § 7 we show how the laws of certain  $SL(2, p^n)$  can be derived from those of the corresponding  $PSL(2, p^n)$ . Finally we state bases for the laws of  $S_5$ , for the variety of proper factors of  $PSL(2, 7)$ , and the variety of soluble factors of  $PSL(2, 2^n)$ , an outline of the proofs being given in § 8.

The results are fairly technical in nature and we defer precise statement of them until we have established our notation.

Parts of Theorems 3.1, 3.2 and 3.4, and Theorem 3.5 have already been announced, [4]. We note that we have changed the fifth law given there in the basis for  $PSL(2, 9)$  in order to have one which conforms with the general type of such laws given in theorem 3.2. (B). Clearly either law serves the same purpose.

**2. Notation, definitions and preliminary results**

The reader is referred to the book of Hanna Neumann [17] for the basic concepts of the theory of varieties; as there we use upper case Gothic letters for varieties and upper case Roman letters for groups. However we differ in using 1 indiscriminately for the identity element and the trivial subgroup. Finally we note that ‘group’ means ‘finite group’ and ‘simple’ means ‘non-abelian simple’ throughout.

**2.1 NOTATION AND DEFINITIONS**

2.1.1.  $Q$  denotes the quaternion group of order 8 and  $\mathfrak{Q}$  the variety which it generates.

2.1.2.  $C_m$  denotes the cyclic group of order  $m$  and  $D_m$  the dihedral group of order  $2m$ .

2.1.3.  $S_m$  and  $A_m$  denote, respectively, the symmetric and alternating groups of degree  $m$ .

2.1.4.  $\mathfrak{A}_m$  denotes the abelian variety of exponent  $m$ .

2.1.5. The terms of the lower central series are denoted by  $\gamma_i G$ , where  $\gamma_1 G = G$  and  $\gamma_{i+1} G = [\gamma_i G, G]$ ;  $Z(G)$  denotes the centre of  $G$ ,  $\Phi G$  the Frattini subgroup of  $G$  and  $\sigma G$  the socle of  $G$ .

2.1.6. A finite group with a unique minimal subgroup,  $M$ , is said to be monolithic with monolith  $M$ . Then  $M = \sigma G$  and we denote the centraliser in  $G$  of  $M$  by  $\sigma^* G$ .

2.1.7. The word  $u_m$  is defined recursively by

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

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

(Note that this corresponds to the word  $v_{m-1}$  as defined in [17] 52.31.)

2.1.8.  $C(e, m, c)$  denotes the class of all groups of exponent dividing  $e$ , whose chief factors have order at most  $m$ , and the class of whose nilpotent factors does not exceed  $c$ .

2.1.9.  $C(\lambda^t, m)$ , where  $\lambda$  is prime and  $\lambda \nmid m$ , denotes the critical group with a normal subgroup which is a direct product of  $t$  copies of  $C_{\lambda^t}$  and whose factor group is cyclic of order  $m$  where  $t$  is the least integer such that  $m | \lambda^t - 1$ .

2.1.10. If  $H, K$  are groups with isomorphic non-trivial central subgroups  $Z_1$  and  $Z_2$  respectively, then  $\langle HcpK : Z_1 = Z_2 \rangle$  denotes the direct product of  $H$  and  $K$  with  $Z_1$  and  $Z_2$  amalgamated. When there is no ambiguity we write  $\langle HcpK \rangle$ .

2.1.11.  $\text{Var } G$  will denote the variety generated by the group  $G$  and  $\text{var}(w_1, \dots, w_r)$  the variety defined by the laws  $w_1 = 1, \dots, w_r = 1$ .

2.1.12. If  $\pi$  is a set of primes then a  $\pi$ -element, or  $\pi$ -group, will denote an element, or group, whose order is divisible only by primes in  $\pi$ .  $\pi'$  will denote the complementary set of primes. When  $\pi = \{p\}$ , we write  $p$ -element etc.

2.1.13. The upper  $\pi$ -series of a group  $G$ :

$$1 = P_0 \leq N_0 < P_1 < N_1 < \dots \leq G$$

is defined by  $N_i/P_i$  being the greatest normal  $\pi'$ -subgroup of  $G/P_i$ , and  $P_{i+1}/N_i$  being the greatest normal  $\pi$ -subgroup of  $G/N_i$ . If for some  $l$ ,  $N_l = G$ ,  $G$  is said to be  $\pi$ -soluble of  $\pi$ -length  $l$ .

2.1.14. If  $x \in SL(2, p^n)$  then  $\text{tr } x$  denotes the trace of  $x$ . If  $x \in PSL(2, p^n)$  then  $\text{tr } x$  denotes the traces of the two elements of  $SL(2, p^n)$  mapped onto  $x$  in the natural homomorphism. Thus we shall write  $\text{tr } x = \pm s$ .

## 2.2 PRELIMINARY RESULTS

We list in this section various results to which we wish to make frequent reference.

2.2.1.  $\mathfrak{D} = \text{var } D_4 = \text{var}(x^4, [x^2, y])$ . (P.M. Weichsel [23], Theorem 1.1, [24] Lemma 5.1.)

2.2.2. The law  $u_m$  has the following properties:

- (i) every group of order less than  $m$  satisfies  $u_m = 1$ ;
- (ii) a group with a chief centraliser of index greater than  $m-1$  does not satisfy  $u_m = 1$ ;
- (iii) a group with a normal abelian subgroup of index less than  $m-1$  satisfies  $u_m = 1$ . (L. G. Kovács and M. F. Newman [16], 1.71, 1.72, 1.73.)

2.2.3.

- (i)  $C(e, m, c)$  is a Cross variety;
- (ii) if  $\mathfrak{B}$  is a variety of exponent  $e$ , whose nilpotent groups have class at most  $c$  and which satisfies  $u_m = 1$  then  $\mathfrak{B} \leq C(e, e^m, c)$ . (L. G. Kovacs and M. F. Newman [15].)

2.2.4.  $\mathfrak{X}_{\lambda^*} \mathfrak{X}_m = \text{var } C(\lambda^*, m)$  (John Cossey [2], Lemma 4.3.1)

2.2.5. If  $G$  is  $\pi$ -soluble with upper  $\pi$ -series

$$1 = P_0 \leq N_0 < P_1 < \dots \leq N_l = G \quad \text{then}$$

- (i)  $C_{G/N_0}(P_1/N_0) \leq P_1/N_0$ ;

- (ii) if the  $\pi$ -subgroups of  $G$  are abelian then  $G$  has  $\pi$ -length 1;
- (iii) if the 2-subgroups of  $G \in \mathfrak{D}$ , then  $G$  has 2-length  $\leq 2$ . (P. Hall and G. Higman [11], Lemma 1.2.3, Theorem 1.2.6.)

2.2.6. LEMMA. *Let  $G$  be a finite group, and suppose that  $N$  is minimal normal in  $G$  such that  $G/N$  is an abelian  $p$ -group. If  $G/N$  is cyclic, then  $|M_p(G)| \leq |M_p(N)|$ , where  $M(G)$  denotes the multiplier of  $G$  and  $M_p(G)$  its Sylow  $p$ -subgroup.*

PROOF. Let  $H$  be a representing group for  $G$ , with  $K/M(G) = N$ . Then  $K/\gamma_2 K$  has nontrivial Sylow  $p$ -subgroup if  $|M_p(G)| > |M_p(N)|$ . Let  $L/\gamma_2 K$  be the Hall  $p'$ -subgroup of  $K/\gamma_2 K$ ; then  $H/L$  is a  $p$ -group. If  $D/L = \gamma_2(H/L)$ ,  $D < K$ , for a  $p$ -group has cyclic factor derived group if and only if it is itself cyclic. But this gives a contradiction, for  $H/K$  is also the largest abelian  $p$ -quotient of  $H$ .

2.2.7.  $PSL(2, p^n)$  possesses subgroups isomorphic to the following groups only:

- (1)  $C_p \times \dots \times C_p$  ( $\leq n$  factors),
  - (2)  $C_f$  where  $f \mid \frac{p^n \pm 1}{k}$  and  $k = (p^n - 1, 2)$ ,
  - (3)  $D_f$  with  $f$  as in (2),
  - (4)  $A_4$  for  $p > 2$  or  $p = 2$  and  $n \equiv 0(2)$ ,
  - (5)  $S_4$  for  $p^{2n} - 1 \equiv 0(16)$ ,
  - (6)  $A_5$  for  $p = 5$  or  $p^{2n} - 1 \equiv 0(5)$ ,
  - (7) subgroups of  $C(p, t)$  where  $t \mid p^n - 1$ ,
  - (8)  $PSL(2, p^m)$  for  $m \mid n$  and  $PGL(2, p^m)$  for  $2m \mid n$ .
- (B. Huppert [13], Hauptsatz II 8.27, L. E. Dickson [6], § 260.)

### 3. Statement of results

THEOREM 3.1.

(A) *The following set of laws forms a basis for the laws of var  $S_4$ :*

- (1)  $x^{12} = 1$ ,
- (2)  $\{(x^3 y^3)^4 [x^3, y^6]^3\}^3 = 1$ ,
- (3)  $[x^2, y^2]^2 = 1$ ,
- (4)  $[x, y]^6 = 1$ ,
- (5)  $[x^6, y^6] = 1$ ,
- (6)  $[[x, y]^3, y^3, y^2] = 1$ .

(B) *The following set of laws forms a basis for the laws of  $\mathfrak{A}_3 \mathfrak{A}_4 \cup \text{var } S_4$ :*

- (1)  $x^{12} = 1$ ,

- (2)  $\{(x^3 y^3)^4 [x^3, y^6]^3\}^3 = 1,$
- (3)  $[x^4, y^4]^2 = 1,$
- (4)  $[x, y]^6 = 1,$
- (5)  $[x^6, y^6]^3 = 1,$
- (6)  $[[x, y]^3, y^3, y^2] = 1,$
- (7)  $u_8 = 1.$

(C) *Let  $G$  be a finite group of exponent 12, whose Sylow 2-subgroups and Sylow 3-subgroups belong respectively to  $\mathfrak{S}_4$  and  $\mathfrak{A}_3$ . If, in addition,  $G$  satisfies the laws  $[x, y]^6 = 1$ ,  $[x^6, y^6]^3 = 1$ , and  $[[x, y]^3, y^3, y^2] = 1$ ,  $G$  belongs to  $\mathfrak{A}_3 \mathfrak{A}_4 \cup \text{var } S_4$ , and if  $[x^6, y^6]^3 = 1$  is replaced by  $[x^6, y^6] = 1$ , then  $G$  belongs to  $\text{var } S_4$ .*

**THEOREM 3.2.**

(A) *The following laws hold in  $PSL(2, p^n)$ ,  $p \neq 2$ :*

- $p^n \equiv 3(4) : [x^s, y^s]^s = 1;$
- $p^n \equiv 1(4), p \neq 5 : \{(x^s y^s)^\phi [x^s, y^s]^\psi\}^s = 1;$
- $p = 5 : \{(x^s y^s (x^s y^{4s})^{10})^{10} [x^s, y^s]^\chi\}^s = 1;$
- where  $s = \frac{1}{2}(p^{2n} - 1);$
- $\phi \equiv 0(p)$  and  $1(s);$
- $\psi \equiv -1(ps)$  or  $-1(p)$  and  $0(s);$
- $\chi \equiv 0(s)$  and  $4(5).$

(B) *The following laws hold in  $PSL(2, p^n)$ ,  $p \neq 2$ :*

- $p^n \equiv 3(4) : [x^s, y^t]^s = 1;$
- $p^n \equiv 1(4), p \neq 3 : \{[[x^s, y^t]^{\phi s}, x^s]^{-1} [x^s, y^t]^{\phi s}\}^s = 1;$
- $p = 3, n \text{ even} : \{[[x^s, y^t]^{\chi s}, x^s][x^s, y^{-t}]^{\chi s}\}^s = 1;$
- where  $s = \frac{1}{2}(p^{2n} - 1),$
- $t = \frac{p}{2}(p^n - 1),$
- $\phi s \equiv 1(p), \chi s \equiv 1(3).$

*The laws in (A) imply that Sylow  $p$ -subgroups are abelian, and the laws in (B) fail to hold in  $C(p, r)$  where  $r$  is a divisor of  $\frac{1}{2}(p^n + 1)$ .*

**THEOREM 3.3.**

(A)  *$PSL(2, 2^n)$  satisfies the following laws:*

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

$$(3) \{ [x^{2(2^n-1)}, y^2, x^{2(2^n-1)}]^{2^{2^n-1}-1} [y^2, x^{2(2^n-1)}]^2 = 1,$$

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

(B) *A basis for PSL(2, 2<sup>3</sup>) is given by the above laws (with n = 3) together with:*

$$(5) \{ [[x^{18}, y^{112}]^{36}, x^{36}]^{63} [[x^{18}, y^{14}]^{36}, x^{18}]^{94} [y^{14}, x^{18}] \}^{18} = 1,$$

or

$$(5') \{ [[[x^{18}, y^{14}]^{36}, y^{14}]^{36}, y^{28}]^9 = 1,$$

$$(6) \{ \{ (x^{18}y^{18})^{112}(x^{18}y^{108})^{112} \}^k [x^{54}, y^{54}]^l \}^{18} = 1,$$

where  $k = 49$  or  $112$ ,  $l = 18$  or  $81$ .

**THEOREM 3.4.**

(A) *The following set of laws forms a basis for the laws of var PSL(2, 7):*

$$(1) x^{84} = 1,$$

$$(2) \{ (x^{21}y^{21})^{52}(x^{21}y^{63})^4 [x^{21}, y^{42}]^9 \}^{21} = 1,$$

$$(3) \{ (x^{28}y^{28})^{57} [x^{28}, y^{28}]^{14} \}^{28} = 1,$$

$$(4) [x^3, y^{12}]^{12} = 1,$$

$$(5) \{ [[y^{-24}x^{21}y^{24}, y^{-12}x^{21}y^{12}]^{37}, x^{21}]^{13} y^{-48} [x^{21}, y^{48}]^7 y^{48} \}^{21} = 1,$$

$$(6) \{ [x^{28}, y^{12}, x^{28}]^6 [x^{28}, y^{36}]^2 \}^{28} = 1,$$

$$(7) \{ (x^7y^7)^{12}(x^7y^{49})^{12} [x^{35}, y^{49}]^{11} \}^{42} = 1,$$

$$(8) \{ \{ (x^{77}y^{77})^{72} [x^7, y^7]^{15} [x^7, y^{77}]^3 \}^{36} [x^{42}, y^{42}]^5 \}^7 = 1,$$

$$(9) \{ (x^{21}y^{63})^{72}(x^{28}y^{21})^{24} [[[x^7, y^7]^{21}, y^{21}]^7, y^{14}] \}^7 = 1,$$

$$(10) u_{169} = 1.$$

(B) *The following set of laws forms a basis for the laws of var PSL(2, 9):*

$$(1) x^{60} = 1,$$

$$(2) \{ (x^{15}y^{15})^{16}(x^{15}y^{45})^{16} [x^{15}, y^{30}]^{37} \}^{15} = 1,$$

$$(3) \{ (x^{20}y^{20})^{21} [x^{20}, y^{20}]^{29} \}^{20} = 1,$$

$$(4) \{ \{ (x^{12}y^{12})^5 (x^{12}y^{48})^5 \}^{19} [x^{12}, y^{12}]^{16} \}^{36} = 1,$$

$$(5) \{ [[x^{20}, y^{12}]^{40}, x^{20}] [x^{20}, y^{48}]^{40} \}^{20} = 1,$$

$$(6) \{ [y^{40}, x^{12}]^{15} [x^{36}, y^{20}, x^{12}]^5 [y^{40}, x^{36}]^4 \}^{12} = 1.$$

$$(7) \{ x^{48} [x^{12}, y^{15}, x^{24}]^5 x^{12} [x^{12}, y^{30}]^{18} \}^{12} = 1,$$

$$(8) \{ \{ [x^{30}, y^{36}]^{45} (x^{15}y^{12})^{21} (x^{15}y^{48})^{57} \}^{10} [x^{15}, y^{12}]^{45} \}^{15} = 1,$$

$$(9) \{ (x^5y^5)^{12} [x^5, y^5]^{30} \}^5 = 1,$$

$$(10) \{ (x^5y^5)^{12} [x^{30}, y^{30}]^5 \}^{15} = 1,$$

$$(11) \{ (x^5y^5)^{12} [[[x^5, y^5]^{15}, y^{15}]^{25}, y^{10}]^{25} \}^5 = 1,$$

$$(12) u_{361} = 1.$$

(C) *The following set of laws forms a basis for the laws of var PSL(2, 11):*

- (1)  $x^{330} = 1$ ,
- (2)  $\{(x^{110}y^{110})^{111}[x^{110}, y^{110}]^{275}\}^{110} = 1$ ,
- (3)  $\{(x^{66}y^{66})^{180}[[x^{66}, y^{264}]^{66}, x^{66}]^{67}(x^{66}y^{66})^{150}[x^{66}, y^{66}]\}^{66} = 1$ ,
- (4)  $[x^{30}, y^5]^{30} = 1$ ,
- (5)  $\{[x^{165}, y^{90}, x^{165}][x^{165}, y^{30}]^{41}\}^{15} = 1$ ,
- (6)  $\{[x^{110}, y^{30}, x^{110}]^{111}[x^{110}, y^{30}]^5\}^{110} = 1$ ,
- (7)  $\{((x^{30}y^{30})^{55}(x^{30}y^{300})^{55})^{220}[x^{30}, y^{30}]^{264}\}^{66} = 1$ ,
- (8)  $\{[[x^{66}, y^{264}]^{165}, x^{66}]^6[x^{66}, y^{66}]\}^{165} = 1$ ,
- (9)  $\{[x^{110}, y^{66}, y^{220}]^{177}[x^{110}, y^{264}]^{110}\}^{10} = 1$ ,
- (10)  $\{(x^{110}y^{110})^{15}[x^{110}, y^{110}]^{132}\}^{66} = 1$ ,
- (11)  $u_{661} = 1$ .

**THEOREM 3.5.** *Let  $w(x_1, \dots, x_r) = 1$  be a basis for the laws of var PSL(2,  $p^n$ ). Then, for  $n$  odd and  $p^n = 8h \pm 1$ ,  $h$  odd, or  $p^n = 8h \pm 3$ , or for  $p^n = 9$ , a basis for the laws of var SL(2,  $p^n$ ) is:*

- (1)  $[w(x_1, \dots, x_r), y] = 1$ ,
- (2)  $(w(x_1, \dots, x_r))^2 = 1$ .

**THEOREM 3.6.** *The following set of laws forms a basis for the laws of var  $S_5$ :*

- (1)  $x^{60} = 1$ ,
- (2)  $\{(x^{15}y^{15})^4[x^{15}, y^{30}]^{15}\}^{15} = 1$ ,
- (3)  $\{(x^{20}y^{20})^6[x^{20}, y^{20}]^2\}^5 = 1$ ,
- (4)  $\{((x^{36}y^{12})^5(x^{36}y^{48})^5)^3[x^{36}, y^{36}]^6\}^6 = 1$ ,
- (5)  $[x^6, y^6]^{15} = 1$ ,
- (6)  $\{[y^{20}, x^{48}, y^{40}][y^{20}, x^{12}]\}^{10} = 1$ ,
- (7)  $\{[x^{12}, y^{40}, x^{48}][y^{20}, x^{12}]^2\}^6 = 1$ ,
- (8)  $[x, y]^{30} = 1$ ,
- (9)  $\{((x^5y^5)^{36}(x^5y^{15})^{36})^{36}[x^{30}, y^{30}]\}^5 = 1$ ,
- (10)  $\{((x^{25}y^{25})^{36}((x^{35}y^{25})^{50}(x^{25}y^{35})^{50})^{36})^{36}[[x^{25}, y^{25}]^{15}, y^{15}]^{25}, y^{50}\}^5 = 1$ ,
- (11)  $\{((x^{21}y^{45})^{40}(x^{21}y^{15})^{20})^{40}[[x^{21}, y^{21}]^{45}, y^{15}]^{21}, y^{42}\}^{12} = 1$ ,
- (12)  $u_{121} = 1$ .

**THEOREM 3.7.**

(A) *The following set of laws forms a basis for the laws of the variety generated by the proper subgroups of PSL(2, 7):*

- (1)  $x^{84} = 1$ ,
- (2)  $\{(x^{21}y^{21})^4[x^{21}, y^{42}]^3\}^3 = 1$ ,

- (3)  $[x^2, y^2]^{14} = 1,$
- (4)  $[x^3, y^{12}] = 1,$
- (5)  $[x, y]^{42} = 1,$
- (6)  $[x^6, y^6] = 1,$
- (7)  $[[x, y]^{63}, y^3, y^2] = 1.$

(B) *The following set of laws forms a basis for the laws of the variety generated by the soluble subgroups of  $PSL(2, 2^n)$ :*

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

### 4. The proof of Theorem 3.1

#### 4.1 PRELIMINARIES

In this section, we collect a number of results which we will need in the proof of Theorem 3.1.

The following result is due to W. Gaschütz [7] theorem 8: we will use it and its corollary often, usually without explicit reference.

4.1.1. LEMMA. *Let  $G$  be a finite group all of whose Sylow subgroups are elementary abelian. Then every normal subgroup of  $G$  is complemented in  $G$ .*

4.1.2. COROLLARY. *Let  $G$  be a finite group all of whose Sylow subgroups are elementary abelian. Then  $G = G_1 \times Z(G)$ , with  $Z(G_1) = 1$ .*

4.1.3. LEMMA.  $\mathfrak{A}_2\mathfrak{A}_3 \cup \mathfrak{A}_3\mathfrak{A}_2 \cup \mathfrak{D} \leq \text{var } S_4.$

PROOF. This follows immediately from the fact that  $\mathfrak{A}_2\mathfrak{A}_3, \mathfrak{A}_3\mathfrak{A}_2, \mathfrak{D}$  are generated by  $A_4, S_3, D_4$  respectively (2.2.4 and 2.2.1.).

4.1.4. LEMMA. *Let  $G \in \mathfrak{A}_3\mathfrak{A}_2$ . If  $N$  is a normal 2-subgroup,  $N \leq Z(G)$ .*

PROOF. Let  $S$  be a Sylow 3-subgroup of  $G$ ,  $T$  a Sylow 2-subgroup. Then  $N \leq T$ ,  $S \triangleleft G$ , and  $G = ST$ . But  $[S, N] \leq S \cap N = 1$ , and so  $[G, N] = 1$ . That is,  $N \leq Z(G)$ .

The next result can be extracted from Köchendorffer [14].

4.1.5. LEMMA. *Let  $G$  be a finite soluble group, and let  $K$  be a field of characteristic  $p$ . Then  $G$  has a faithful irreducible representation over  $K$  if and only if  $(|\sigma G|, p) = 1$ , and  $\sigma G$  is the normal closure of a single element.*

4.1.6. LEMMA. *Let  $1 \neq G \in \mathfrak{A}_3\mathfrak{A}_2$ , and suppose that the order of a Sylow 2-subgroup of  $G$  is at most 2, and that  $G$  has a faithful irreducible representation over  $GF(2)$ . Then  $G$  is isomorphic to one of the following 3 groups:  $C_3, S_3, S_3 \times C_3$ .*



PROOF. It follows from Lemma 4.1.5 that  $\sigma G$  is the Sylow 3-subgroup of  $G$ , and  $|G/\sigma G| \leq 2$ . Since  $\sigma G$  is the normal closure of a single element, if  $G$  is abelian,  $G \cong C_3$ . If  $G$  is non-abelian, then  $|G/\sigma G| = 2$ , and we may regard  $\sigma G$  as a quotient of the regular  $GF(3)C_2$ -module. From this the result follows easily.

4.1.7. COROLLARY. *If  $G$  satisfies the conditions of the lemma, and in addition,  $G$  contains no elements of order 6, then  $G$  is isomorphic to either  $C_3$  or  $S_3$ .*

4.1.8. LEMMA. *Let  $G$  be isomorphic to a subgroup of  $S_3 \times S_3$ , and suppose that  $G$  contains no normal 2-subgroup. Let  $M$  be an indecomposable quotient of the regular  $GF(2)G$ -module. Then if  $M$  is faithful,  $M$  is irreducible.*

The proof of this lemma involves a case by case examination of the regular representations of the possible choices for  $G$ , and we shall leave it for an appendix (§ 10).

4.2 A BASIS FOR THE LAWS OF  $\mathfrak{A}_2\mathfrak{A}_3\mathfrak{A}_2$

The main result of this section is

4.2.1. LEMMA. *The following subset of the laws given in Theorem 3.1. (A) forms a basis for the laws of  $\mathfrak{A}_2\mathfrak{A}_3\mathfrak{A}_2$ .*

- (1)  $x^{12} = 1$ ,
- (3)  $[x^2, y^2]^2 = 1$ ,
- (4)  $[x, y]^6 = 1$ ,
- (5)  $[x^6, y^6] = 1$ .

PROOF. Let  $\mathfrak{B}$  be the variety defined by these laws. A quick check shows that  $\mathfrak{A}_2\mathfrak{A}_3\mathfrak{A}_2$  satisfies these, and so  $\mathfrak{A}_2\mathfrak{A}_3\mathfrak{A}_2 \leq \mathfrak{B}$ .

In the other direction, we first show that  $\mathfrak{B}$  is locally finite. Let  $G$  be a finitely generated group in  $\mathfrak{B}$ . The laws (1) and (5) tell us that the subgroup  $N$  of  $G$  generated by sixth powers of the elements of  $G$  is an abelian normal subgroup of  $G$  of exponent 2. Then  $G/N$  is a finitely generated group of exponent 6, and so is finite ([9] Theorem 3.1.). It follows that  $N$  is also finitely generated, and hence finite, giving that  $G$  is finite.

Observe that the law (3) ensures that the Sylow 3-subgroups of any finite group in  $\mathfrak{B}$  are abelian.

Now, let  $G$  be a finite group in  $\mathfrak{B}$ , and let  $N$  be the subgroup of  $G$  generated by sixth powers of the elements of  $G$ . Put  $G/N = H$ . Since  $H$  has exponent 6, it is soluble ([10] Theorem 16.8.7), and has abelian Sylow 2-subgroups. Since it also has abelian Sylow 3-subgroups,  $H$  is an  $A$ -group, and so, by [21] Theorem 8.3,  $H$  is metabelian. It follows from [2] Theorem 4.2.2 and Lemma 4.3.1 that  $H \in \mathfrak{A}_3\mathfrak{A}_2 \cup \mathfrak{A}_2\mathfrak{A}_3$ .

All the Sylow subgroups of  $H$  are elementary abelian, and so by Corollary 4.1.2,  $H = L \times Z(H)$ , where  $Z(L) = 1$ . Also  $\sigma L = N_1 \times N_2$ , where  $N_1$  is an

elementary abelian 2-group, and  $N_2$  is an elementary abelian 3-group. Note that  $\sigma L = \gamma_2 L$ . Let  $K$  be a complement for  $\sigma L$  in  $L$ . Then  $K = K_1 \times K_2$ , where  $K_1$  is an elementary abelian 3-group, and  $K_2$  is an elementary abelian 2-group. Since all Sylow subgroups of  $L$  are abelian, we have  $[K_1, N_2] = [K_2, N_1] = 1$ , and so we may conclude that  $L = N_1 K_1 \times N_2 K_2$ , and that  $Z(N_1 K_1) = Z(N_2 K_2) = 1$ . Suppose  $N_1 = S/N$ ; then  $S$  is a normal subgroup of  $G$ , and has exponent 2 or 4. If  $S$  has exponent 2, it is elementary abelian, and since  $G/S \in \mathfrak{U}_3 \mathfrak{U}_2$ , we get  $G \in \mathfrak{U}_2 \mathfrak{U}_3 \mathfrak{U}_2$ . We will prove  $S$  cannot have exponent 4. Suppose  $S$  has exponent 4. Then so does  $S/\gamma_3 S$ , and  $\gamma_3 S < N$ ,  $\gamma_3 S \triangleleft G$ . Thus it is enough to prove it for the case  $\gamma_3 S = 1$ .

The proof divides into two cases. Firstly, suppose that  $S/\gamma_2 S$  has exponent 4. Now the centraliser of  $S/\gamma_2 S$  in  $G$  has index a power of 3, and so by Lemma 6.4 of D. R. Taunt [21],  $S/\gamma_2 S$  can be written as a direct product of indecomposable homocyclic normal subgroups of  $G/\gamma_2 S$ . Since  $S/\gamma_2 S$  has exponent 4, at least one of these subgroups will have exponent 4; let  $M/\gamma_2 S$  be such a subgroup. By the way  $S$  was chosen, the centraliser of  $M/\gamma_2 S$  is not the whole of  $G$ . Now let  $x\gamma_2 S \in M/\gamma_2 S$ , and  $y \in G$ , and  $y$  not in the centraliser of  $M/\gamma_2 S$ . Then  $x \neq x^y$ , and  $x^2 \neq x^{2y}$ , whence  $x^{-1}x^y$  has order 4 modulo  $\gamma_2 S$ , contradicting the fact that  $x^{-1}x^y$  has order dividing 6, by the law (4). Hence, suppose  $S/\gamma_2 S$  has exponent 2.

Then  $S/\gamma_3 S$  has exponent 4, and also  $S/\gamma_3 S \in \mathfrak{D}$ . Then there is an element  $y$  of order 3 in  $G$  such that  $x \neq x^y$ , and also  $xx^y x^{y^2} \in \gamma_2 S$ . Put  $z = xx^y$ . Then

$$\begin{aligned} z^{-1}z^{y^2} &= z^{-2}zz^{y^2} \\ &= z^{-2}xx^y x^{y^2}x, \end{aligned}$$

and since  $z^{-2}xx^y x^{y^2} \in \gamma_2 S \leq Z(S)$ , we get  $z^{-1}z^{y^2}$  has order 4, again giving a contradiction.

Thus every finite group in  $\mathfrak{B}$  is in  $\mathfrak{U}_2 \mathfrak{U}_3 \mathfrak{U}_2$ , and so, since  $\mathfrak{B}$  is generated by its finite groups, we have  $\mathfrak{B} \leq \mathfrak{U}_2 \mathfrak{U}_3 \mathfrak{U}_2$ , completing the proof of the lemma.

### 4.3 AN IMPORTANT LEMMA

4.3.1. LEMMA. *Let  $G$  be a non-nilpotent monolithic group in  $\mathfrak{U}_2 \mathfrak{U}_3 \mathfrak{U}_2$ . Suppose further that the Sylow 2-subgroups of  $G$  are in  $\mathfrak{D}$ , and that  $G$  satisfies the law  $[[x, y]^3, y^3, y^2]$ . Then  $G$  is isomorphic to one of  $S_4, A_4, S_3$ .*

The proof is broken up into a number of steps.

If  $G$  contains no non-trivial normal 2-subgroup, then  $G \in \mathfrak{U}_3 \mathfrak{U}_2$ , and the assertion is easily checked. Hence we may suppose that  $\sigma G$  is a 2-group.

4.3.2.  $G/\sigma^*G$  contains no elements of order 6.

Put  $\sigma^*G = K$ . Then  $G/K \in \mathfrak{U}_3 \mathfrak{U}_2$ , and is faithfully and irreducibly represented on  $\sigma G$ . If  $G/K$  contains elements of order 6, from Lemmas 5.2.1 and 5.2.5 of [2] and Lemma 4.1.6, we may conclude that  $G/K \cong H_1/K \times H_2/K$  where  $H_1/K \cong C_2$ ,  $H_2/K \cong C_3$  and  $H_2/K \triangleleft G/K$ . Regarding  $\sigma G$  as an irreducible

$GF(2)G$ -module, it follows from Clifford's theorem ([5] Theorem 49.2) that if  $yK$  is a non-trivial element of  $H_2/K$ , and  $x$  is any non-trivial element of  $\sigma G$ , we have  $x^y \neq x$ . Also if  $zK$  is a non-trivial element of  $H_1/K$  such that  $z$  has order a power of 2, then there is a non-trivial  $x$  in  $\sigma G$  such that  $[x, z] \neq 1$ . Note that  $xx^y x^{y^2}$  is fixed by  $y$ , and so  $xx^y x^{y^2} = 1$ . Also,  $x, x^y, z$  all lie in the same Sylow 2-subgroup, which, by assumption, has class at most 2, and  $\sigma G$  has exponent 2. Now

$$\begin{aligned} [[x^y, yz]^3, (yz)^3, (yz)^2] &= [[x^y, z][x^y, y]^z, (yz)^3, (yz)^2] \\ &= [[x^y, z](x^y x^{y^2})z, (yz)^3, (yz)^2] \\ &= [[x^y, z]x^z, z, y^2] \\ &= [[[x^y, z][x, z], x, z], y^2] \\ &= [[[x^y, z][x, z], z]^x [x, z], y^2] \\ &= [x, z, y^2] \\ &\neq 1. \end{aligned}$$

Thus if  $G/\sigma^*G$  contains elements of order 6,  $G$  does not satisfy the hypotheses of Lemma 4.3.1, a contradiction.

Since  $G \in \mathfrak{A}_2 \mathfrak{A}_3 \mathfrak{A}_2$ ,  $G$  has a series  $1 \leq N \leq H \leq G$ , where  $N$  is a maximal elementary abelian normal 2-subgroup of  $G$ ,  $H/N$  is an elementary abelian normal 3-subgroup of  $G/N$ , and  $G/H$  is an elementary abelian 2-group.

If either  $H$  is abelian, or  $G = H$ , it follows from the fact that  $G$  is a non-nilpotent critical group that  $G \in \mathfrak{A}_3 \mathfrak{A}_2$  or  $G \in \mathfrak{A}_2 \mathfrak{A}_3$ , and so  $G \in \text{var } S_4$ , by Lemma 4.1.3. Thus we may suppose  $G \neq H$ , and  $\gamma_2 H \neq 1$ .

### 4.3.3. $Z(H) = 1$ .

For  $H \in \mathfrak{A}_2 \mathfrak{A}_3$ , and so  $H = H_1 \times Z(H)$ . Since  $1 \neq \gamma_2 H \leq H_1$ , and  $G$  is monolithic, we must have  $Z(H) = 1$ .

### 4.3.4. Let $F$ be the Fitting subgroup of $G$ . Then $F = N$ .

Since  $G/N \in \mathfrak{A}_3 \mathfrak{A}_2$ , we may conclude from Lemma 4.1.4. that  $F/N$  is the Sylow 2-subgroup of  $Z(G/N)$ . Suppose that  $F > N$ .

If  $N \leq Z(F)$ , and  $x \in F, x \notin N, x$  has order 4, by the choice of  $N$ , and  $x^2 \in N$ . Let  $y \in H$ . Since  $xN \in Z(G/N)$ , we have  $x^y = xz$ , where  $z \in N$ . But then  $(x^2)^y = x^2$ , and since  $y$  was arbitrary, we have  $x^2 \in Z(H)$ , a contradiction to 4.3.3.

If  $N \neq Z(F)$ , then  $N \cap Z(F) \neq 1$  ([17] Theorem 31.26), and  $N \cap Z(F) \triangleleft G$ . If  $N$  is regarded as a  $GF(2)H$ -module,  $N \cap Z(F)$  has a non-trivial complement by Maschke's theorem. Let  $M$  be an irreducible component of this complement. Since  $Z(H) = 1$ , there is an element  $z$  in  $H$  of order 3 such that if  $1 \neq x \in M, x^z \neq x$ , and so  $x^{-1} x^z = x x^z = x^{z^2}$ . Also, since  $M \cap Z(F) = 1$ , there is an element  $y \in F$  such that  $[x, y] \neq 1$  (note that  $y \notin N$ ). Now, consider the elements  $x$  and  $yz$ . We have, since  $[x, yz] \in N$ ,

$$\begin{aligned}
 [x, yz]^3 &= [x, yz] \\
 &= [x, z][x, y]^2.
 \end{aligned}$$

Also  $[x, y]^z \in \gamma_2 F \leq Z(F)$ , since  $F \in \mathfrak{S}$ , and so

$$\begin{aligned}
 [[x, yz]^3, (yz)^3] &= [[x, z][x, y]^z, y] \\
 &= [x, z, y] \\
 &= [x^{z^2}, y] \\
 &= [x, y[y, z^{-2}]]^{z^2} \\
 &= [x, y]^{z^2},
 \end{aligned}$$

since  $y \in Z(G/N)$ , and therefore  $[y, z^{-2}] \in N$ .

$$\begin{aligned}
 [[x, yz]^3, (yz)^3, (yz)^2] &= [x, y, z^2]^{z^2} = [z^2, x, y^{-1}]^{xyz^2} \\
 &= [x^z, y^{-1}]^{xyz^2} = [x, y^{-1}[y^{-1}, z^{-1}]]^{zxyz^2} = [x, y^{-1}]^{zxyz^2} \neq 1.
 \end{aligned}$$

Hence  $G$  does not satisfy the hypotheses of the lemma.

In either case, the assumption that  $F > N$  leads to a contradiction, and so  $F = N$ .

4.3.5. *Regarded as a  $GF(2)(G/N)$ -module,  $N$  is faithful and indecomposable.*

The indecomposability of  $N$  comes from the fact that  $G$  is critical, while the faithfulness comes from 4.3.3 and 4.3.4.

4.3.6. *If  $K$  is a Sylow 3-subgroup of  $H$ , and  $N_0 \leq N, N_0 \triangleleft G$  such that  $N_0 K \triangleleft G$ , then  $N_0 = N$ .*

From the fact that  $Z(H) = 1$ , it is readily deduced that the normal closure of  $K$  in  $H$  is precisely  $H$ , and 4.3.6 follows immediately.

By 4.3.6 and [12] Theorem 1, we have:

4.3.7.  *$N$  is complemented in  $G$ , by  $L$  say.*

4.3.8.  $\sigma G = N$ .

If  $K$  is a Sylow 3-subgroup of  $L, N$ , regarded as a  $GF(2)K$ -module, contains no trivial submodules (since  $Z(H) = 1$ ).

Now, suppose that  $\sigma G < N$ . Let  $M/\sigma G$  be an irreducible submodule of  $N/\sigma G$ . Since  $M \triangleleft G, C_L(M) \triangleleft L$ , and hence it has a complement,  $T$  say. Then  $T$  is faithfully and indecomposably represented on  $M$ .

Let  $D_1 = C_T(\sigma G), D_2 = C_T(M/\sigma G)$ . Then  $D_1 \cap D_2$  is a normal 2-subgroup of  $T$ , and so is a direct factor of  $T$ . Put  $D_1 \cap D_2 = P$ : then  $T = R \times P$ . Now  $\sigma G(T/D_1)$  is critical ([16] Theorem 1.6), and satisfies the hypotheses of Lemma 4.3.1, and since  $\sigma^*(\sigma G(T/D_1)) = \sigma G, T/D_1$  contains no elements of order 6. Also  $T/D_1$  is faithfully and irreducibly represented on  $\sigma G$ , and so, by Corollary 4.1.4,

$T/D_1$  is isomorphic to  $S_3$  or  $C_3$ . Similarly,  $T/D_2$  is isomorphic to  $S_3$  or  $C_3$ . Thus  $R(\cong T/P)$  is isomorphic to a subgroup of  $S_3 \times S_3$ . Also,  $R$  contains no normal 2-subgroups: if it did, it is not difficult to see, using Clifford's theorem ([5] Theorem 49.2), that such a normal subgroup is contained in  $P$ , and  $R \cap P = 1$ , a contradiction. We must first show that  $P = 1$ . Note that  $|\sigma G| = 4 = |M/\sigma G|$ . If  $K$  is the Sylow 3-subgroup of  $T$ , then  $M$ , as a  $GF(2)K$ -module, is completely reducible, by Maschke's theorem, and so  $M = \sigma G \times M_0$ . Now, there exists an element  $y \in K$  such that no non-trivial element of  $M$  is left fixed by  $y$ . Also, if  $1 \neq x \in M_0$ , we have  $x = x^y x^{y^2}$ . Since  $P$  centralises  $\sigma G$  and  $M/\sigma G$ , but not  $M$ , then for  $1 \neq x \in M_0$ , we have an element  $z \in P$  such that  $[x, z] \neq 1$  and  $[x, z] \in \sigma G$ . Now consider the elements  $x^y, yz$ .

$$\begin{aligned} [x^y, yz]^3 &= [x^y, yz] \\ &= [x^y, y]^z [x^y, z] \\ &= x^z [x^y, z] \\ [[x^y, yz]^3, (yz)^3] &= [x^z [x^y, z], z] \\ &= [x^z, z]^{[x^y, z]} [x^y, z, z] \\ &= [x, z] \\ [[x^y, yz]^3, (yz)^3, (yz)^2] &= [[x, z], y^2] \\ &\neq 1. \end{aligned}$$

Thus  $MT$  and so  $G$  does not satisfy the requirements of Lemma 4.3.1, a contradiction. Thus we must have  $P = 1$ .

Hence  $T$  is isomorphic to a subgroup of  $S_3 \times S_3$  and  $T$  contains no normal 2-subgroups. But any faithful indecomposable  $GF(2)T$ -module is irreducible (Lemma 4.1.8), contradicting the assumption that  $M$  was indecomposable. But this means that the assumption that  $N > \sigma G$  leads to a contradiction, and so  $N = \sigma G$ .

To complete the proof of Lemma 4.3.1., note that since  $N = \sigma G$ , and  $G/N$  contains no non-trivial normal 2-subgroups,  $\sigma G = \sigma^*G$ . Thus by Corollary 4.1.7,  $G/\sigma G$  is isomorphic to  $S_3$  or  $C_3$ . In the first case,  $G \cong S_4$ , in the second  $G \cong A_4$ , and so  $G \in \text{var } S_4$ .

#### 4.4 THE PROOF OF THEOREM 3.1(A)

Let  $\mathfrak{B}$  be the variety defined by the laws (1)–(6) of Theorem 3.1(A). By Lemma 4.2.1, the laws (1), (3), (4), (5) form a basis for the laws of  $\mathfrak{A}_2\mathfrak{A}_3\mathfrak{A}_2$ , and so  $\mathfrak{B} \leq \mathfrak{A}_2\mathfrak{A}_3\mathfrak{A}_2$ . Thus  $\mathfrak{B}$  is locally finite, and so is generated by its critical groups ([17] Theorem 51.41).

Let  $G$  be a nilpotent group in  $\mathfrak{B}$ . Then either  $G \in \mathfrak{A}_3$  or  $G$  satisfies  $x^4 = 1$ ,  $[x, y^2] = 1$  and so  $G \in \mathfrak{D}$ .

Thus any critical group in  $\mathfrak{B}$  satisfies the requirements of Lemma 4.3.1, and so is in  $\text{var } S_4$ .

In the other direction, note that  $S_4$  has a chief series  $1 < N < A_4 < S_4$ , where  $N$  is an elementary abelian normal 2-subgroup, and  $G/N \cong S_3$ . In particular then,  $S_4 \in \mathfrak{A}_2\mathfrak{A}_3\mathfrak{A}_2$ , and so satisfies the laws (1), (3), (4), (5) by Lemma 4.2.1. Note also that  $S_4$  contains no elements of order 6.

Let  $x, y \in S_4$ ; then they satisfy law (2) trivially unless  $x$  has order 2 or 4 and  $y$  has order 4. If  $xN = N$ , or  $xN = yN$  then  $x$  and  $y$  belong to the same Sylow 2-subgroup of  $S_4$  and so certainly satisfy (2). Thus we may assume that  $xN$  and  $yN$  are distinct elements of order 2 in  $S_4/N$  and hence  $(x^3Ny^3N)^3 = 1$  and thus  $(x^3y^3)^3 = 1$ . Also, since  $y^2 \in N$ ,  $[x^3, y^6]$  has order 2 or 1 and thus the product  $(x^3y^3)[x^3, y^6]$  has order 3 (being the product of an element of order 3 and one of order 2 or 1 both belonging to  $A_4$ ).

Finally, it follows from the fact that if  $x, y \in S_4$ ,  $[x, y]^3 \in N$ , and either  $y^3 \in N$  or  $y^2 \in N$ , that  $S_4$  satisfies (6). Hence  $S_4 \in \mathfrak{B}$ , and the proof is finished.

Since  $SL(2, 3)$  does not satisfy  $[x^2, y^2]^2 = 1$  we have:

4.4.2. COROLLARY.  $SL(2, 3) \notin \text{var } S_4$ .

4.5 THE PROOF OF THEOREM 3.1(B)

Let  $\mathfrak{B}$  denote the variety defined by the laws (1)–(7). It is easy to check that  $S_4$  and  $C(3, 4)$  satisfy the laws (1)–(7), and so  $\mathfrak{A}_3\mathfrak{A}_4 \cup \text{var } S_4 \subseteq \mathfrak{B}$ .

We shall prove:

4.5.1. LEMMA. *Let  $G$  be a finite critical group satisfying the laws (1) and (4)–(6) of Theorem 3.1(B) and suppose that Sylow 3-subgroups of  $G$  are abelian, and Sylow 2-subgroups of  $G$  are in  $\mathfrak{D}$ . Then  $G \in \mathfrak{A}_3\mathfrak{A}_4 \cup \text{var } S_4$ .*

PROOF. The law (1) and Theorem 16.8.7 of [10] ensure that  $G$  is soluble. If  $G$  is nilpotent, then  $G \in \mathfrak{A}_3 \cup \mathfrak{D} \subseteq \text{var } S_4$  (Lemma 4.1.3).

Since  $G$  is soluble, and has abelian Sylow 3-subgroups,  $G$  has 3-length 1 (2.2.5). That is,  $G$  has a series  $1 \subseteq N_0 \subseteq N_1 \subseteq G$  such that  $N_0$  is a maximal normal 2-subgroup of  $G$ ,  $N_1/N_0$  is a normal 3-subgroup of  $G/N_0$ , and  $G/N_1$  is a 2-group.

Suppose first that  $N_0 = 1$ . Then, regarding  $N_1$  as a  $GF(3)(G/N_1)$ -module, we get from Maschke’s theorem and the criticality of  $G$  that  $\sigma G = \sigma^*G = N_1$ . Also, by the Schur-Zassenhaus theorem,  $\sigma G$  is complemented in  $G$ , by  $L$  say. Suppose if possible that  $L$  is nonabelian. Then by Lemma 4.1.5,  $L$  has cyclic centre; also  $L$  is in  $\mathfrak{D}$ . Thus  $\gamma_2 L$  is cyclic of order 2, and by Clifford’s theorem ([5] Theorem 49.2),  $\sigma G$ , regarded as  $GF(3) \gamma_2 L$ -module, contains no trivial submodules. Now let  $x$  be an element of order 4,  $x \notin Z(L)$ , and  $y \in L$  any element such that  $[x, y] \neq 1$ . Then  $[x, y] = x^2 \in \gamma_2 L$  and  $\sigma G \gamma_2 L$  does not contain any elements of order 6. Also, since  $y$  does not centralise  $\sigma G$ , there is an element  $z \in \sigma G$  such that  $[y, z] \neq 1$ .

Consider the elements  $[y, z]y, x$ .

$$\begin{aligned} [[y, z]y, x]^3 &= [[y, z], y, x] \\ &= [y, z, x]^y[y, x] \\ [[[y, z]y, x]^3, x^3] &= [[y, z, x]^y[y, x], x^3] \\ &= [[y, z, x]^y, x^3]^{[y, x]}[y, x, x^3] \\ &= [[y, z, x]^y, x^3]^{[y, x]} \\ &\neq 1. \end{aligned}$$

Put  $d = [[x, z, x]^y, x^3]^{[y, x]}$ . Then  $1 \neq d \in \sigma G$ .

$$\begin{aligned} [[[y, z]y, x]^3, x^3, x^2] &= [d, x^2] \\ &\neq 1. \end{aligned}$$

Thus  $G$  does not satisfy the law (6), a contradiction. Thus  $L$  is abelian, and  $G \in \mathfrak{A}_3\mathfrak{A}_4$ .

Hence suppose that  $N_0 \neq 1$ . Note that  $N_0$  is the Fitting subgroup of  $G$ .

Suppose that  $G/N_0$  has elements of order 4; let  $xN_0$  be one. Since a Sylow 2-subgroup of  $G$  is in  $\mathfrak{D}$ , it follows that  $x$  also has order 4, and  $x^2$  centralises  $N_0$ . But then so does the normal closure of  $x^2$  in  $G$ , and so, since  $G/N_0$  contains no non-trivial normal 2-subgroups, there is a normal 3-subgroup  $M/N_0$  of  $G/N_0$  which centralises  $N_0$ . Then  $M = N_0 \times M_0$ , where  $M_0 \cong M/N_0$ , contradicting the criticality of  $G$ . Hence  $G/N_0 \in \mathfrak{A}_3\mathfrak{A}_2$ .

Now let  $M$  be a maximal elementary abelian normal 2-subgroup of  $G$ . Then suppose  $G/M$  contains elements of order 4. Let  $xM$  be of order 4. Since a Sylow 2-subgroup of  $G$  is in  $\mathfrak{D}$ ,  $x^{2y}$  centralises  $M$  for all  $y \in G$ . Also, from the previous paragraph,  $x^2 \in N_0$ . Let  $M_1 = \langle gp(x^{2y} : y \in G) \rangle$ . Then  $M_1 \leq N_0$ , and if  $M_1$  is abelian, we obtain  $gp(M_1, M)$  is an elementary abelian normal 2-subgroup of  $G$ , and since  $x^2 \notin M$ , we get a contradiction to the maximality of  $M$ . Thus, for some  $y \in G$ ,  $[x^2, x^{2y}] \neq 1$ . But then  $[x^6, (x^y)^6]^3 = [x^2, x^{2y}]^3 \neq 1$ , since  $M_1 \leq N_0$ . Thus  $G$  does not satisfy the law (3), a contradiction.

Thus  $G/M \in \mathfrak{A}_3\mathfrak{A}_2 \cup \mathfrak{A}_2\mathfrak{A}_3$ . However, as we saw in the proof of Lemma 4.2.1, a group  $G$  in  $\mathfrak{A}_2(\mathfrak{A}_3\mathfrak{A}_2 \cup \mathfrak{A}_2\mathfrak{A}_3)$  which satisfies  $[x, y]^6$  lies in  $\mathfrak{A}_2\mathfrak{A}_3\mathfrak{A}_2$ . Therefore,  $G$  is in  $\mathfrak{A}_2\mathfrak{A}_3\mathfrak{A}_2$ , and so satisfies the requirements of Lemma 4.3.1, giving  $G \in \text{var } S_4$ .

From laws (1) and (7) and Theorem  $D$  of P. Hall and G. Higman [11], we have that  $\mathfrak{B}$  is locally finite, and so is generated by its finite critical groups. From law (4) we deduce that 3-groups in  $\mathfrak{B}$  are abelian, and from the laws (2) and (5) we deduce 2-groups lie in  $\mathfrak{D}$ . Thus finite critical groups in  $\mathfrak{B}$  satisfy the requirements of Lemma 4.5.1, and so  $\mathfrak{B} \leq \mathfrak{A}_3\mathfrak{A}_4 \cup \text{var } S_4$ , and Theorem 3.1 (B) is proved.

**4.6 THE PROOF OF THEOREM 3.1 (C)**

We have already proved the first part of the statement (Lemma 4.5.1) so let  $G$  be a critical group satisfying the hypothesis of the second part. Then  $G \in \mathfrak{U}_3 \mathfrak{U}_4 \cup \text{var } S_4$ . Since all the proper subvarieties of  $\mathfrak{U}_3 \mathfrak{U}_4$  lie in  $\text{var } S_4$ , it is enough to show that  $G$  is not isomorphic to  $C(3,4)$ . Suppose  $G \cong C(3,4)$ . Then let  $y$  be an element of order 4 in  $G$ ,  $x$  an element of order 3. Note that  $G$  has a normal Sylow 3-subgroup, and that  $y^2$  does not leave any element of order 3 fixed. Also note that  $y^x$  has order 4. Hence  $[y^6, (y^x)^6] = [y^2, y^{2x}] = [y^2, [y^2, x]] \neq 1$  (since  $[y^2, x] \neq 1$  is an element of order 3), and so  $G$  does not satisfy the hypotheses of Theorem 3.1(C), a contradiction. Hence  $G \in \text{var } S_4$ .

**5. Laws in  $PSL(2, p^n)$**

In this section we prove Theorems 3.2 and 3.3.

**5.1 ELEMENTARY PROPERTIES OF  $PSL(2, p^n)$**

The following properties can be deduced either from the definition of  $PSL(2, p^n)$  or from the list of subgroups given in 2.2.7.

- 5.1.1. The exponent is  $\frac{1}{2}p(p^{2n}-1)$ ,  $p$  odd,  $2(2^{2n}-1)$ ,  $p = 2$ ; ( $= ps$ , say).
- 5.1.2. The Sylow  $p$ -subgroups are elementary abelian.
- 5.1.3. Every element has order  $p$  or  $p'$ .
- 5.1.4. The elements of order  $p$  have canonical form

$$\pm \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}.$$

These are all conjugate for  $p = 2$ , and fall into two conjugacy classes for odd  $p$ ;

$$\pm \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}$$

is conjugate to

$$\pm \begin{pmatrix} 1 & 0 \\ \nu & 1 \end{pmatrix}$$

if and only if  $\mu\nu$  is a square in  $GF(p^n)$ .

- 5.1.5. (1)  $x$  has order  $p$  or 1 if and only if  $\text{tr } x = \pm 2$ ;
- (2) for  $p \neq 2$   $x$  has order 2 if and only if  $\text{tr } x = 0$ ;
- (3) for  $p \neq 3$   $x$  has order 3 if and only if  $\text{tr } x = \pm 1$ .

**5.2 PROPERTIES OF THE TRACE FUNCTION**

Throughout this section,  $F$  will denote an arbitrary field.



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

PROOF.

$$\text{Let } x = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}, \quad y = \begin{pmatrix} A & \Gamma \\ B & \Delta \end{pmatrix}$$

where  $\alpha\delta - \beta\gamma = 1 = A\Delta - B\Gamma$ .

$$\text{Then } \text{tr } xy = \alpha A + \gamma B + \beta \Gamma + \delta \Delta$$

$$\text{tr } xy^{-1} = \alpha \Delta - \gamma B - \beta \Gamma + \delta A.$$

$$\text{Thus } \text{tr } xy + \text{tr } xy^{-1} = \alpha A + \delta \Delta + \alpha \Delta + \delta A = \text{tr } x \text{tr } y.$$

5.2.2. THEOREM. *If  $x, y \in SL(2, F)$  and  $\text{tr } x = s, \text{tr } y = t, \text{tr } xy = u$ , then the trace of any word in  $x$  and  $y$  is a polynomial in  $s, t$  and  $u$  with integer coefficients. This polynomial belongs to one of four classes of polynomials in 3 variables defined as follows:*

$$f(s, t, u) \in E_0 \Leftrightarrow f(-s, -t, u) = f(s, -t, -u) = f(-s, t, -u) = f(s, t, u);$$

$$f(s, t, u) \in E_s \Leftrightarrow -f(-s, -t, u) = f(s, -t, -u) = -f(-s, t, -u) = f(s, t, u);$$

$$f(s, t, u) \in E_t \Leftrightarrow -f(-s, -t, u) = -f(s, -t, -u) = f(-s, t, -u) = f(s, t, u);$$

$$f(s, t, u) \in E_u \Leftrightarrow f(-s, -t, u) = -f(s, -t, -u) = -f(-s, t, -u) = f(s, t, u).$$

The words in  $x$  and  $y$  also may be divided into four classes, where, if  $w = x^{\alpha_1} y^{\beta_1} \dots x^{\alpha_k} y^{\beta_k}$  then

$$w \in W_0 \Leftrightarrow \Sigma \alpha_i \text{ is even, } \Sigma \beta_i \text{ is even;}$$

$$w \in W_s \Leftrightarrow \Sigma \alpha_i \text{ is odd, } \Sigma \beta_i \text{ is even;}$$

$$w \in W_t \Leftrightarrow \Sigma \alpha_i \text{ is even, } \Sigma \beta_i \text{ is odd;}$$

$$w \in W_u \Leftrightarrow \Sigma \alpha_i \text{ is odd, } \Sigma \beta_i \text{ is odd.}$$

Moreover,  $w \in W_\lambda$  if and only if  $\text{tr } w \in E_\lambda$ .

PROOF. We define binary operations on  $\{E_\lambda\}$  and  $\{W_\lambda\}$  as follows:

$$E_\lambda E_\mu = \{fg | f \in E_\lambda, g \in E_\mu\},$$

$$W_\lambda W_\mu = \{w_1 w_2 | w_1 \in W_\lambda, w_2 \in W_\mu\}.$$

It is easy to see that these operations are well-defined and that under them the sets form groups each isomorphic to  $C_2 \times C_2$ , with  $E_0$  and  $W_0$  as identity elements and that the correspondence  $W_\lambda \leftrightarrow E_\lambda$  is an isomorphism. The theorem implies that this isomorphism is induced by  $w \rightarrow \text{tr } w$ . We note also that the sum of two polynomials in  $E_\lambda$  is also in  $E_\lambda$  and that  $s \in E_s, t \in E_t, u \in E_u$  and  $\text{tr } 1 = 2 \in E_0$ .

We prove by induction on word length that  $w \in W_\lambda$  implies that  $\text{tr } w \in E_\lambda$ . The converse implication follows by reductio ad absurdum. We have already seen the statement to be true for words of lengths 0 and 1, so let  $w = x^{\alpha_1} y^{\beta_1} \dots x^{\alpha_k} y^{\beta_k}$

be a word of length  $n > 1$ , and assume true for all words of length less than  $n$ . There are several cases to consider:

1) Some  $|\alpha_i|$  or  $|\beta_i| > 1$ . Since  $\text{tr } w = \text{tr } w^{-1}$ , and  $\text{tr } w_1 w_2 = \text{tr } w_2 w_1$ , we can assume that  $w$  ends in a term  $y^{\beta_k} c r x^{\alpha_k}$  with  $\beta_k > 1$  or  $\alpha_k > 1$ . We will consider in detail the former case, the argument in the latter being analogous. Thus  $w = x^{\alpha_1} y^{\beta_1} \dots x^{\alpha_k} y^{\beta_k}$  with  $\beta_k > 1$  and so both  $w_1 = w y^{-1}$  and  $w_2 = w_1 y^{-1}$  have length less than  $n$ . Moreover, if  $w \in W_\lambda$ , then  $w_1 \in W_\lambda W_t$  and  $w_2 \in W_\lambda$ , and so, by the induction hypothesis

$$\text{tr } w_1 \in E_\lambda E_t, \quad \text{tr } w_2 \in E_\lambda.$$

By the previous lemma:

$$\text{tr } w_1 y + \text{tr } w_1 y^{-1} = \text{tr } w_1 \text{tr } y$$

i.e. 
$$\text{tr } w = \text{tr } w_1 \text{tr } y - \text{tr } w_2.$$

Now  $\text{tr } w_1 \text{tr } y \in E_\lambda E_t E_t = E_\lambda$  and so  $\text{tr } w \in E_\lambda$ , as required.

2)  $|\alpha_i| = |\beta_i| = 1$  for all  $i$ . Since  $w$  is not of length 1 we can assume that it ends in a term  $y^\beta x^\alpha y$  where  $\beta = 0, 1, -1; \alpha = \pm 1$ .

(a)  $\beta = 1$ . Then  $w_1 = w y^{-1} x^{-\alpha}$ ,  $w_2 = w_1 y^{-1} x^{-\alpha}$  and  $x^\alpha y$  all have length less than  $n$ , and, if  $w \in W_\lambda$  then  $w_1 \in W_\lambda W_t W_s$ ,  $w_2 \in W_\lambda$ ,  $x^\alpha y \in W_u$ . Again

$$\text{tr } w = \text{tr } w_1 \text{tr } x^\alpha y - \text{tr } w_2 \in E_\lambda E_t E_s E_u - E_\lambda = E_\lambda.$$

(b)  $\beta = -1$ . Then  $w = w y^{-1} x^{-\alpha}$  and  $x^\alpha y$  both have length less than  $n$ , but  $w_2 = w_1 y^{-1} x^{-\alpha}$  has length  $n$ . However, it ends in  $y^{-2} x^{-\alpha}$  and so by (1)  $\text{tr } w_2 \in E_\lambda$ . Thus again we have  $\text{tr } w \in E_\lambda$ .

(c)  $\beta = 0$ . Then  $w = x^{-1} y$  or  $xy$  and

$$\text{tr } x^{-1} y = \text{tr } y^{-1} x = \text{tr } xy^{-1} = st - u \in E_u$$

and  $\text{tr } xy = u \in E_u$ .

The truth of the theorem follows.

**5.2.3. COROLLARY.** *If  $x, y \in PSL(2, F)$  ( $\text{char } F \neq 2$ ) and  $\text{tr } x = \pm s, \text{tr } y = \pm t, \text{tr } xy = \pm u$ , then  $\text{tr } xy^{-1}$  takes at most two values, namely  $\pm(st \pm u)$  and selection of one of these uniquely determines the trace of any word in  $x$  and  $y$ .*

**PROOF.** Let  $X$  and  $Y$  be elements of  $SL(2, F)$  which are mapped onto  $x$  and  $y$  in the natural homomorphism. Then  $\text{tr } X = \pm s, \text{tr } Y = \pm t, \text{tr } XY = \pm u$  and, from the theorem we see that  $\text{tr } X^{\alpha_1} Y^{\beta_1} \dots X^{\alpha_k} Y^{\beta_k}$  takes (up to sign) at most two values, and thus, since  $\text{tr } x^{\alpha_1} \dots y^{\beta_k}$  is determined only up to sign, this takes at most two values. In particular

$$\text{tr } xy^{-1} = \pm(st \pm u)$$

and selection of  $\pm(st - u)$  or  $\pm(st + u)$  determines the parity of the number of sign changes and hence  $\text{tr } x^{\alpha_1} \dots y^{\beta_k}$ .

(Note that if one of  $s, t, u$  is zero all sign changes have the same effect, and the traces are then determined uniquely.)

5.2.4. LEMMA. *Let  $x$  and  $y$  be elements of  $SL(2, p^n)$  with  $\text{tr } x = s, \text{tr } y = t, \text{tr } xy = u$  then*

- (1)  $\text{tr } [x, y] = s^2 + t^2 + u^2 - stu - 2,$
- (2)  $\text{tr } xyxy^{-1} = stu - u^2 - t^2 + 2,$
- (3)  $\text{tr } xyxy^{-1}[x, y]^{-1} = (su - t)(u^2 t - st^2 u + s^2 t + t^3 - 4t) + s^2 - 2,$
- (4)  $\text{tr } [x, y, x] = \text{tr}^2 [x, y] + 2 \text{tr}^2 x - \text{tr}^2 x \text{tr } [x, y] - 2,$
- (5)  $\text{tr } [x, y, x]^{-1} [x, y] = \text{tr } [x, y, x] \text{tr } [x, y] - \text{tr } [x, y].$

PROOF. We use Lemma 5.2.1.

- (1)  $\text{tr } x^{-1} y^{-1} xy = \text{tr } xy \text{tr } xy - \text{tr } x^2 y^2$   
 $= u^2 - (s(tu - s) - t^2 + 2)$   
 $= s^2 + t^2 + u^2 - stu - 2.$
- (2)  $\text{tr } xy xy^{-1} = \text{tr } xy \text{tr } xy^{-1} - \text{tr } y^2 = u(st - u) - t^2 + 2$   
 $= stu - u^2 - t^2 + 2.$
- (3)  $\text{tr } xy xy^{-1} [x, y]^{-1} = \text{tr } xyxy^{-1} y^{-1} x^{-1} yx = \text{tr } x^2 y xy^{-2} x^{-1} y$   
 $= \text{tr } x^2 y \text{tr } xy^{-2} x^{-1} y - \text{tr } x^2 y^2$   
 $= (su - t)(\text{tr } xy^{-2} \text{tr } x^{-1} y - \text{tr } x^2 y^{-3}) - stu + s^2 + t^2 - 2$   
 $= (su - t)((st - u)t - s)(st - u) - (s(st - u) - t)(t - 2) + su - t$   
 $- t(su - t) + s^2 - 2$   
 $= (su - t)(-ut(st - u) + s(st - u) + t^3 - 2t + su - t - t) + s^2 - 2$   
 $= (su - t)(u^2 t - ut^2 s + s^2 t + t^3 - 4t) + s^2 - 2.$

(4) and (5) are immediate consequences of (1) and Lemma 5.2.1 once it is observed that  $\text{tr } x [x, y] = \text{tr } x.$

5.2.5. LEMMA. *The following identities hold in  $PSL(2, 2^n).$*

- (1)  $\text{tr } x^k + \text{tr } x^{k-2} = \text{tr } x \text{tr } x^{k-1},$
- (2)  $\text{tr } [x, y] = \text{tr}^2 x + \text{tr}^2 y + \text{tr}^2 xy + \text{tr } x \text{tr } y \text{tr } xy,$
- (3)  $\text{tr } [x, y, x] = \text{tr } [x, y] \{ \text{tr } [x, y] + \text{tr}^2 x \},$
- (4)  $\text{tr } x^{2^k} = \text{tr}^{2^k} x,$
- (5)  $\text{tr } x^{2^{k-1}} + \text{tr } x^{2^{k+1}} = \text{tr}^{2^{k+1}} x,$
- (6)  $\text{tr } x^{2^{k-1}} = \text{tr } x + \text{tr}^{2^{k-1}+1} x + \text{tr}^{2^{k-1}+2^{k-2}+1} x + \dots + \text{tr}^{2^{k-1}} x,$
- (7)  $\text{tr } x^{2^{k+1}} = \text{tr } x + \text{tr}^{2^{k-1}+1} x + \text{tr}^{2^{k-1}+2^{k-2}+1} x +$   
 $\dots + \text{tr}^{2^{k-1}} x + \text{tr}^{2^{k+1}} x,$

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

PROOF. (1), (2) and (3) follow from Lemmas 5.2.1 and 5.2.4.

(4) we prove by induction. Certainly  $\text{tr} x^2 = \text{tr}^2 x$ , so assume

$$\text{tr} x^{2k-1} = \text{tr}^{2k-1} x,$$

then

$$\text{tr} x^{2k} = \text{tr}(x^{2k-1})^2 = \text{tr}^2 x^{2k-1} = \text{tr}^{2k} x.$$

(5) This is an immediate consequence of Lemma 5.2.1 and (4).

(6)  $\text{tr} x^3 = \text{tr}^3 x + \text{tr} x$ , so assume

$$\text{tr} x^{2k-1} = \text{tr} x + \text{tr}^{2k-1+1} x + \text{tr}^{2k-1+2k-2+1} x + \dots + \text{tr}^{2k-1} x.$$

Then

$$\text{tr} x^{2k+1-1} = \text{tr}^{2k} x \text{tr} x^{2k-1} + \text{tr} x$$

$$= \text{tr} x + \text{tr}^{2k+1} x + \text{tr}^{2k+2k-1+1} x + \dots + \text{tr}^{2k+1-1} x.$$

(7) This is an immediate consequence of (5) and (6).

(8) From 5.2.4 (5)

$$\text{tr} \{[x, y, x][y, x]\} = \text{tr} [x, y] \text{tr} [x, y, x] + \text{tr} [x, y]$$

so assume

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

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

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

$$+ \text{tr}^{2k} [x, y, x]\}.$$

Then

$$\text{tr} \{[x, y, x]^{2k+1}[y, x]\}$$

$$= \text{tr} [x, y, x]^{2k} \text{tr} \{[x, y, x]^{2k}[y, x]\} + \text{tr} [y, x]$$

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

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

(9) Again  $\text{tr} \{ [x, y, x][y, x] \} = \text{tr} [x, y] \text{tr} [x, y, x] + \text{tr} [x, y]$  so assume

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

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

$$\begin{aligned} &= \text{tr} \{ [x, y, x]^{2k-1} [y, x] \} \text{tr} [x, y, x]^{2k} + \text{tr} [x, y, x]^{-1} [y, x] \\ &= \text{tr} [x, y] \{ 1 + \text{tr}^{2k} [x, y, x] + \text{tr}^{2k+2k-1} [x, y, x] + \dots + \text{tr}^{2k+1-1} [x, y, x] \} \end{aligned}$$

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

(10)  $\text{tr} [x, y^2] = \text{tr} x^{-1} y^{-2} x y^2$

$$\begin{aligned} &= \text{tr} x y^2 \text{tr} x y^2 + \text{tr} x^2 y^4 \\ &= \{ \text{tr} x y \text{tr} y + \text{tr} x \}^2 + \text{tr} y^2 \text{tr} x^2 y^2 + \text{tr} x^2 \\ &= \text{tr}^2 x y \text{tr}^2 y + \text{tr}^2 x + \text{tr}^2 y \{ \text{tr} [x, y] + \text{tr}^2 x y \} + \text{tr}^2 x \\ &= \text{tr}^2 y \text{tr} [x, y]. \end{aligned}$$

Now assume

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

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

$$\begin{aligned} &= \text{tr}^{2k+1} y \text{tr}^{2(2k-1)} y \text{tr} [x, y] \\ &= \text{tr}^{2(2k+1-1)} y \text{tr} [x, y]. \end{aligned}$$

5.2.6. COROLLARY.

- (1)  $x^{2^n-1} = 1, x \neq 1$  implies that  $1 + \text{tr}^{2^{n-2}} x + \text{tr}^{2^{n-2}+2^{n-3}} x + \dots + \text{tr}^{2^{n-1}-1} x = 0$ ;
- (2)  $x^{2^n+1} = 1, x \neq 1$  implies that  $1 + \text{tr}^{2^{n-2}} x + \text{tr}^{2^{n-2}+2^{n-3}} x + \dots + \text{tr}^{2^{n-1}-1} x + \text{tr}^{2^{n-1}} x = 0$ .

5.3 THE *p*-LAW IN  $PSL(2, p^n), p \neq 2$

Let  $x$  and  $y$  be a pair of elements of order  $p$ . Without loss of generality we may assume them to have the form:

$$\begin{aligned} x &= \pm \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}, \quad y = \pm \begin{pmatrix} \delta & -\gamma \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \\ &= \pm \begin{pmatrix} 1-\alpha\gamma v & -\gamma^2 v \\ \alpha^2 v & 1+\alpha\gamma v \end{pmatrix} \end{aligned}$$

(where  $\alpha\delta - \beta\gamma = 1$ ).

5.3.1. LEMMA.  $(xy)^p = 1$  if and only if either

- (i)  $\mu\nu\gamma^2 = 0$  (which implies  $x$  and  $y$  belong to the same Sylow subgroup); or
- (ii)  $\mu\nu\gamma^2 = 4$  (which implies  $x$  and  $y$  are conjugate).

PROOF.  $\text{tr } xy = \pm(1 - \alpha\gamma\nu - \gamma^2\mu\nu + 1 + \alpha\gamma\nu) = \pm(2 - \gamma^2\nu\mu) = \pm 2$  if and only if either

- (i)  $\gamma^2\mu\nu = 0$  or
- (ii)  $\gamma^2\mu\nu = 4$ .

But (i) implies  $\gamma = 0$  and so  $x$  and  $y$  belong to the same Sylow  $p$ -subgroup, and (ii) implies  $\mu\nu$  is a square and so  $x$  and  $y$  are conjugate.

5.3.2. LEMMA.  $[x, y]^p = 1$  if and only if

- either (i)  $\mu^2\nu^2\gamma^4 = 0$  (when  $[x, y] = 1$ )
- or (ii)  $\mu^2\nu^2\gamma^4 = -4$ .

PROOF.

$$[x, y] = \pm \begin{pmatrix} 1 & 0 \\ -\mu & 1 \end{pmatrix} \begin{pmatrix} 1 + \gamma^2\nu\mu(1 - \alpha\gamma\nu) & -\gamma^4\nu^2\mu \\ (1 - \alpha\gamma\nu)^2\mu & 1 - \gamma^2\nu\mu(1 - \alpha\gamma\nu) \end{pmatrix}$$

and so

$$\begin{aligned} \text{tr } [x, y] &= \pm(1 + \gamma^2\nu\mu(1 - \alpha\gamma\nu) + \gamma^4\nu^2\mu^2 + 1 - \gamma^2\nu\mu(1 - \alpha\gamma\nu)) \\ &= \pm(2 + \gamma^4\nu^2\mu^2) = \pm 2 \end{aligned}$$

if and only if

- either (i)  $\gamma^4\nu^2\mu^2 = 0$
- or (ii)  $\gamma^4\nu^2\mu^2 = -4$ .

But, as in 5.3.1, (i) implies that  $x$  and  $y$  are in the same Sylow subgroup and so  $[x, y] = 1$ .

5.3.3. PROOF OF THEOREM 3.2 (A),  $p \neq 5$ .

From 5.3.2 we see that  $[x, y]$  can have order  $p$  only if  $-1$  is a square in  $GF(p^n)$ , hence, if  $p^n \equiv 3(4)$ ,  $[x, y]$  always has order prime to  $p$  and we have the law

$$[x^s, y^s]^s = 1.$$

If  $p^n \equiv 1(4)$ ,  $xy$  and  $[x, y]$  can have order  $p$  simultaneously only if

$$4^2 \equiv -4 \text{ in } GF(p^n)$$

i.e. only if  $p = 5$ .

Hence, for  $p \neq 5$  we have the law

$$\{(x^s y^s)^\phi [x^s, y^s]^\psi\}^s = 1$$

where  $\phi \equiv 0(p)$  and  $1(s)$ ,  $\psi \equiv -1(ps)$  or  $-1(p)$  and  $0(s)$ .

5.3.4. PROOF OF THEOREM 3.2 (A),  $p = 5$ .

We have  $\text{tr } x = \pm 2 = \text{tr } y$

$$\text{tr } xy = \pm(2 - \gamma^2 \mu \nu), \text{tr } xy^{-1} = \pm(2 + \gamma^2 \mu \nu).$$

From 5.3.2,  $[x, y]$  has order 5 only if  $\gamma^4 \nu^2 \mu^2 = -4 = 1$ , i.e.  $\gamma^2 \nu \mu = \pm 1$ .

Now  $\gamma^2 \nu \mu = 1$  implies  $\text{tr } xy = \pm 1, \text{tr } xy^{-1} = \pm 2$  and  $\gamma^2 \nu \mu = -1$  implies  $\text{tr } xy = \pm 2, \text{tr } xy^{-1} = \pm 1$ . Consider the word

$$\{(xy(xy^{-1})^{10})^{10}[x, y]^{\chi}\}^s$$

where  $\chi \equiv 0(s)$  and  $4(5)$ .

This is clearly 1 if  $[x, y]$  does not have order 5. Now  $\text{tr } z = \pm 1$  implies  $z^3 = 1$  so if  $\gamma^2 \nu \mu = 1$  it reduces to

$$(xy y^{-1} x^{-1} yx)^s = (yx)^s = 1,$$

and if  $\gamma^2 \nu \mu = -1$  it becomes

$$\{(xy xy^{-1})^{10}[x, y]^{-1}\}^s.$$

Writing  $s = t = 2, u = 3$  we have  $\text{tr } xy^{-1} = \pm 1 = \pm(st - u)$ . Hence applying 5.2.4.(2)

$$\text{tr } (xy xy^{-1}) = \pm(2 - 4 - 4 + 2) = \pm 1.$$

Thus  $xyxy^{-1}$  also has order 3 and the above expression becomes

$$(xy xy^{-1}[x, y]^{-1})^s.$$

Now, from 5.2.4. (3)

$$\begin{aligned} \text{tr } ((xy xy^{-1})[x, y]^{-1}) &= \pm \{4(3 - 4 + 3 + 3 - 3) + 4 - 2\} \\ &= 0. \end{aligned}$$

Thus  $xy xy^{-1}[x, y]^{-1}$  has order 2, and the above expression vanishes. Hence, we have the law

$$\{((x^s y^s)(x^s y^{4s})^{10})^{10}[x^s, y^s]^{\chi}\}^s = 1$$

where  $\chi \equiv 0(s)$  and  $4(5)$ .

5.4 THE LAW FORBIDDING  $C(p, r), p \neq 2$

Let  $r = (p^n + 1)/2,$

$t = p(p^n - 1)/2$  (so that  $rt = ps$ ).

From 2.2.7 we see that  $r$  does not divide the order of the normaliser of a Sylow  $p$ -subgroup. Thus if

$$y = \pm \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$$

has order dividing  $r$ ,  $\gamma \neq 0$ . Let

$$x = \pm \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}.$$

5.4.1 LEMMA. *If  $p^n \equiv 3(4)$ ,  $[x, y]$  does not have order  $p$ .*

PROOF.  $[x, y] = x^{-1}x^y$  and  $x^{-1}$  and  $x^y$  do not belong to the same Sylow  $p$ -subgroup. Hence, for  $[x, y]$  to have order  $p$ , we require  $x^{-1}$  conjugate to  $x$  (from 5.3.1). But, since  $p^n \equiv 3(4)$ ,  $-1$  is not a square in  $GF(p^n)$  and so this is impossible.

5.4.2. LEMMA. *If  $p^n \equiv 1(4)$  and  $[x, y]$  has order  $p$ , then  $[x, y, x]^{-1}[x, y]$  has order  $p$  only if  $p = 3$ .*

PROOF.  $\text{tr } x = \pm 2$ ,  $\text{tr } y = \pm(\alpha + \delta)$ ,  $\text{tr } xy = \pm(\alpha + \delta + \gamma\mu)$ ,  
 $\text{tr } xy^{-1} = \pm(\alpha + \delta - \gamma\mu)$ , so let  $s = 2$ ,  $t = \alpha + \delta$ ,  $u = \alpha + \delta + \gamma\mu$ . Then

$$\begin{aligned} \text{tr } [x, y] &= \pm(4 + (\alpha + \delta)^2 + (\alpha + \delta + \gamma\mu)^2 - 2(\alpha + \delta)(\alpha + \delta + \gamma\mu) - 2) \\ &= \pm(2 + \gamma^2\mu^2) \\ &= \pm 2 \text{ only if } \gamma^2\mu^2 = -4 \text{ (since } \gamma \neq 0). \end{aligned}$$

$$\text{tr } [x, y, x] = \pm(8 + (2 + \gamma^2\mu^2)^2 - 4(2 + \gamma^2\mu^2) - 2) = \pm(2 + \gamma^4\mu^4).$$

$$\begin{aligned} \text{tr } [x, y, x]^{-1}[x, y] &= \pm\{(2 + \gamma^4\mu^4)(2 + \gamma^2\mu^2) - (2 + \gamma^2\mu^2)\} \\ &= \pm 34 \text{ when } \gamma^2\mu^2 = -4. \end{aligned}$$

Hence  $[x, y, x]^{-1}[x, y]$  has order  $p$  when  $[x, y]$  has order  $p$  only if  $\pm 34 = \pm 2$  in  $GF(p^n)$ , i.e.  $p = 3$ .

5.4.3. LEMMA. *If  $p = 3$  and  $n$  is even then  $[x, y, x][x, y^{-1}]$  has order prime to 3 when  $[x, y]$  has order 3.*

PROOF.

$$[x, y] = \pm \begin{pmatrix} 1 - \mu\alpha\gamma & -\mu\gamma^2 \\ \mu\alpha^2 - \mu + \mu^2\alpha\gamma & 1 + \mu\alpha\gamma + \mu^2\gamma^2 \end{pmatrix}$$

and from the previous lemma we see that this has order 3 only if  $(\mu\gamma)^2 = -1$ . In this case

$$\begin{aligned} [x, y^{-1}] &= \pm \begin{pmatrix} 1 + \mu\gamma\delta & -\mu\gamma^2 \\ -\mu - \mu^2\gamma\delta + \mu\delta^2 & 1 - \mu\gamma\delta + \mu^2\gamma^2 \end{pmatrix} \\ &= \pm \begin{pmatrix} 1 + \mu\gamma\delta & -\mu\gamma^2 \\ -\mu - \mu^2\gamma\delta + \mu\delta^2 & -\mu\gamma\delta \end{pmatrix} \end{aligned}$$

and

$$[x, y, x] = \pm \begin{pmatrix} -\mu\alpha\gamma & -\mu\gamma^2 \\ \mu\alpha^2 - \mu & \mu\alpha\gamma \end{pmatrix} \text{ has order 2.}$$



Then

$$[x, y, x][x, y^{-1}] = \pm \begin{pmatrix} -1 + \delta^2 + \alpha\delta - \mu\alpha\delta - \mu\gamma\delta & -\alpha\gamma - \gamma\delta \\ * & -1 + \alpha\delta + \alpha^2 \end{pmatrix}.$$

If this has order 3 then

$$-2 + \alpha^2 + \delta^2 + 2\alpha\delta - \mu\alpha\gamma - \mu\gamma\delta = \pm 1$$

i.e.

$$(\alpha + \delta)^2 - \mu\gamma(\alpha + \delta) = 0 \text{ or } 1.$$

In the former case we have  $\text{tr } y = 0$  or  $\pm \mu\gamma$ . Now  $\text{tr } y = 0$  implies that  $y$  has order 2, which is impossible since  $r$  is odd, and  $\text{tr } y = \pm \mu\gamma$  implies that  $\text{tr}^2 y = -1$ . But  $\text{tr } y^2 = \pm(\text{tr}^2 y - 2) = \pm(-1 - 2) = 0$ , giving that  $y^2$  has order 2, which again is impossible. In the latter case we have

$$(\pm \text{tr } y + \mu\gamma)^2 = 0 \quad (\text{since } (\mu\gamma)^2 = -1)$$

and so again we have a contradiction and the truth of the lemma follows.

#### 5.4.4. THE PROOF OF THEOREM 3.2(B).

From Lemma 5.4.1 we have

$$[x^s, y^t]^s = 1 \quad \text{if } p^n \equiv 3(4).$$

If  $p^n \equiv 1(4)$  consider the word

$$[[x^s, y^t]^{\phi s}, x^s]^{-1} [x^s, y^t]^{\phi s}$$

where  $\phi s \equiv 1(p)$ . This certainly vanishes if  $[x^s, y^t]$  has order prime to  $p$ , and if  $[x^s, y^t]$  has order  $p$ , it reduces to

$$[x^s, y^t, x^s]^{-1} [x^s, y^t]$$

which, by Lemma 5.4.2 has order prime to  $p$  if  $p \neq 3$ . Hence we have the law

$$\{[[x^s, y^t]^{\phi s}, x^s]^{-1} [x^s, y^t]^{\phi s}\}^s = 1.$$

Similarly, from 5.4.3 we obtain the law

$$\{[[x^s, y^t]^{\chi s}, x^s][x^s, y^{-t}]^{\chi s}\}^s = 1$$

where  $\chi s \equiv 1(3)$ , when  $p = 3$  and  $n$  is even.

### 5.5 A CHARACTERISATION OF VAR $PSL(2, 2^n)$

5.5.1 THEOREM. *A finite soluble group belongs to var  $PSL(2, 2^n)$  if and only if it satisfies the following conditions:*

- (1) *the exponent divides  $2(2^{2^n} - 1)$ ;*
- (2)  *$(\pi_1 \cup \pi_2)$ -subgroups are abelian, where  $\pi_1$  and  $\pi_2$  denote the sets of prime divisors of  $2^n - 1$  and  $2^n + 1$  respectively;*
- (3) *a  $\pi_2$ -element which belongs to the normaliser of a 2-subgroup belongs to its centraliser.*

PROOF. The only if follows immediately from the list of subgroups of  $PSL(2, 2^n)$  given in 2.2.7.

Let  $G$  be a critical soluble group satisfying the above conditions. Then, by 2.2.5,  $G$  has  $\pi_2$ -length one, and so has the structure

$$1 \leq N \leq P \leq G,$$

where  $N$  and  $G/P$  are  $\pi_2'$ -groups and  $P/N$  is a  $\pi_2$ -group. Let  $S$  be the Hall  $\pi_2$ -subgroup of  $P$ . Then by (2) and (3)  $S$  stabilises any chief series of  $N$  and so centralises  $N$ . Thus  $P \cong S \times N$  and each factor is normal in  $G$ . It follows that  $S = 1$  or  $N = 1$ .

- (i) If  $N = 1$ , then, since  $C_G(P) \leq P$ , by (2)  $G/P$  is a 2-group. Moreover, since  $P$  is abelian and  $G$  is critical,  $P$  must be a homocyclic  $\lambda$ -group of exponent  $\lambda^\beta$  where  $\lambda^\beta | 2^n + 1$ , and  $\lambda$  is prime, and hence  $G = C(\lambda^\beta, 2) \in \text{var } PSL(2, 2^n)$ .
- (ii) If  $P = 1$ ,  $G$  is a  $(\pi_1 \cup \{2\})$ -group and has  $\pi_1$ -length one and 2-length one. It follows that  $G$  has the structure

$$1 \leq P \leq G$$

where either  $P$  is a 2-group and  $G/P$  a  $\pi_1$ -group  
 or  $P$  is a  $\pi_1$ -group and  $G/P$  a 2-group.

Again the criticality of  $G$  gives us that  $G = C(\lambda^\beta, 2)$  or  $C(2, m)$  where  $\lambda^\beta$  and  $m$  divide  $2^n - 1$  and  $\lambda$  is a prime. Thus  $G \in \text{var } PSL(2, 2^n)$ .

5.5.2. REMARK. Similar theorems could be stated for  $PSL(2, p^n)$  where  $p$  is odd, but the enunciation is made difficult by the proliferation of cases which occur, so it seems preferable to treat each case on its own merits. Examples of this occur in § 6.

5.5.3. LEMMA. *A simple group belongs to  $\text{var } PSL(2, 2^n)$  if and only if it satisfies the law  $u_{2^n(2^{2n}-1)+1} = 1$  and conditions (1), (2) and (3) of Theorem 5.5.1.*

PROOF. Again, the only if part follows immediately from the list of subgroups of  $PSL(2, 2^n)$ , since the only non-soluble subgroups are the  $PSL(2, 2^m)$  for  $m|n$ , and these clearly satisfy the given conditions. The converse follows from J. H. Walter's classification of simple groups with abelian Sylow 2-subgroups [22].

5.5.4 THEOREM. *Var  $PSL(2, 2^n)$  is characterised by the law  $u_{2^n(2^{2n}-1)+1} = 1$  together with conditions (1), (2) and (3) of theorem 5.5.1.*

PROOF. The class of groups satisfying the given conditions clearly forms a variety, and it is contained in  $C(e, e^m, 1)$  where  $e = 2(2^{2n} - 1)$ ,  $m = 2^n(2^{2n} - 1) + 1$ , and so (by 2.2.3) is a Cross variety. Thus it is sufficient to prove that a finite group satisfying these conditions has the structure:

$$B_1 \times \cdots \times B_k \times S$$

where  $B_i \cong PSL(2, 2^{m_i})$ ,  $m_i|n$  and  $S$  is soluble, since, by Theorem 5.5.1 and

Lemma 3.2. of Sheila Oates [18] we know that the set of all groups of the above type is precisely the set of finite groups in  $\text{var } PSL(2, 2^n)$ .

If  $G$  is a minimal counterexample, then  $G$  is critical. We have two cases to consider:

- (i)  $\sigma G$  non-abelian. Then  $\sigma G$  is a direct product of groups all isomorphic to  $PSL(2, 2^m)$ , for  $m|n$  (by Lemma 5.5.3). Now the automorphism group of  $PSL(2, 2^m)$  is  $P\Gamma L(2, 2^m)$  (the projective semi-linear group), Huppert [13] II §8. Thus  $G$  has a normal subgroup  $N$  which is a direct product of groups each isomorphic to a subgroup of  $P\Gamma L(2, 2^m)$  containing  $PSL(2, 2^m)$  and  $G/N$  acts transitively on the factors. We show first that no subgroup of  $P\Gamma L(2, 2^m)$  properly containing  $PSL(2, 2^m)$  can occur. Such a group would consist of  $PSL(2, 2^m)$  extended by a cyclic group of automorphisms induced by a field automorphism  $x \rightarrow x^{2^\beta}$ , and the order,  $\beta$ , of this, must divide  $m$ . We consider the effect of these automorphisms on two particular subgroups of  $PSL(2, 2^m)$ .

$$(a) \quad S = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a^2 + b^2 = 1 \right\}.$$

This is a Sylow 2-subgroup of  $PSL(2, 2^m)$  and is clearly invariant under the given automorphism, but is not centralised by it. It follows from (1) and (3) that  $(\beta, 2(2^n + 1)) = 1$ .

$$(b) \quad Q = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \mid a \neq 0 \right\}.$$

This is a cyclic subgroup of  $PSL(2, 2^m)$  of order  $2^m - 1$  and is invariant under the given automorphism. Since  $2^m - 1 | 2^n - 1$  we see from (2) that  $(\beta, 2^n - 1) = 1$ . Hence  $\beta = 1$ .

It follows that  $N = \sigma G$ . If  $G/N \neq 1$  there is an element of prime order acting non-trivially on  $\sigma G$  implying that the corresponding Sylow subgroups of  $G$  are non-abelian. Hence  $G \cong PSL(2, 2^m)$ .

- (ii)  $\sigma G$  abelian. By the minimality of  $G$ ,  $G/\sigma G$  is a direct product in which at least one factor is isomorphic to  $PSL(2, 2^m)$  (since  $G$  is not soluble). Suppose  $G \cong H_1/\sigma G \times H_2/\sigma G$ , where  $H_1/\sigma G \cong PSL(2, 2^m)$  and  $H_2 > \sigma G$ . Then  $H_1 < G$  and so is of the form  $K_1 \times \sigma G$  where  $K_1 \cong PSL(2, 2^m)$ . Thus  $K_1$  stabilises the series  $H_2 \geq \sigma G \geq 1$  and so its factor group by the centraliser of  $H_2$  is abelian. Since  $K_1$  is simple we have that  $K_1$  centralises  $H_2$ . Hence  $G = K_1 \times H_2$  is not critical. Hence  $G/\sigma G \cong PSL(2, 2^m)$ . Since  $\sigma G$  is a  $p$ -group where  $p \in \pi_1 \cup \pi_2 \cup \{2\}$  it will be centralised by the  $\pi_2$ -subgroups of  $PSL(2, 2^m)$  by (2) and (3). Since these generate  $G$ , we have  $\sigma G \leq Z(G)$ . But  $\sigma G \leq \gamma_2 G$  (since  $\gamma_2 G \neq 1$ ) and so  $\sigma G$  is a subgroup of the multiplier of  $PSL(2, 2^m)$ . But, by Huppert [13] V Satz 25.7, this is trivial, and we have  $G \cong PSL(2, 2^m)$ .

5.5.5. COROLLARY. *A group satisfying the laws given in Theorem 3.3(B) belongs to var  $PSL(2, 2^3)$ .*

5.6 THE LAWS OF  $PSL(2, 2^n)$

5.6.1. LEMMA. *If  $x, y \in PSL(2, 2^n)$  and  $[x, y]^2 = 1$ , then  $[x^k, y^l]^2 = 1$  for all  $k$  and  $l$ . Moreover  $[x, y]$  and  $[x^k, y^l]$  belong to the same Sylow 2-subgroup.*

PROOF. Note that  $\text{tr } z = 0$  if and only if  $z^2 = 1$ . We define  $[x, ky]$  by

$$[x, 1y] = [x, y]$$

$$[x, ky] = [x, (k-1)y, y] \quad (k > 1).$$

We prove by induction on  $k$  that

$$[x, y], [x, 2y], \dots, [x, ky]$$

all belong to the same Sylow 2-subgroup.

This is certainly true for  $k = 1$ , so assume true for  $k-1$ , then

$$\begin{aligned} \text{tr } [x, ky] &= \text{tr } [x, (k-1)y, y] = \text{tr } [y, [x, (k-2)y], y] \\ &= \text{tr}^2 [x, (k-1)y] \{ \text{tr } [x, (k-1)y] + \text{tr}^2 y \} = 0. \end{aligned}$$

Hence  $[x, ky]^2 = 1$ .

Also  $\{ [x, (k-1)y][x, ky] \}^2 = \{ [x, (k-1)y]^p \}^2 = 1$ .

Hence  $[x, (k-1)y]$  and  $[x, ky]$  belong to the same Sylow 2-subgroup, and thus, since these are disjoint,  $[x, ky]$  belongs to the same Sylow 2-subgroup as  $[x, y], \dots, [x, (k-1)y]$ . It follows that, if

$$f = f([x, y], \dots, [x, ky])$$

is any word in the above commutators then

$$[f, y] = f([x, y, y], \dots, [x, (k+1)y])$$

is also a word in these. We now prove by induction that  $[x, y^k]$  is a word in these commutators. This is certainly true for  $[x, y]$  so suppose

$$[x, y^{k-1}] = f([x, y], \dots, [x, (k-1)y])$$

then 
$$\begin{aligned} [x, y^k] &= [x, y][x, y^{k-1}][x, y^{k-1}, y] \\ &= [x, y]f([x, y], \dots, [x, (k-1)y])f([x, y, y], \dots, [x, ky]). \end{aligned}$$

Thus  $[x, y^k]$  belongs to the same Sylow 2-subgroups as  $[x, y]$ .

Since  $[x, y^k] = [y^k, x]^{-1} = [y^k, x]$ , we may repeat the above process to obtain that  $[x^k, y^l]$  belongs to the same Sylow 2-subgroup as does  $[x, y]$ .

5.6.2. LEMMA.  $PSL(2, 2^n)$  satisfies the law

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

PROOF. Let

$$\begin{aligned} x &= \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}, \quad y = \begin{pmatrix} \delta & -\gamma \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \\ &= \begin{pmatrix} 1-\alpha\gamma v & -\gamma^2 v \\ \alpha^2 v & 1+\alpha\gamma v \end{pmatrix} \end{aligned}$$

be two elements of order 2. Then  $\text{tr } xy = 1 - \alpha\gamma v - \gamma^2 v \mu + 1 + \alpha\gamma v = \gamma^2 v \mu$ . Hence  $xy$  has order two only if  $\gamma = 0$ , i.e. only if  $x$  and  $y$  belong to the same Sylow 2-subgroup. It follows that if  $z$  is an element of order dividing  $2^n + 1$  (so that  $z$  belongs to the normaliser of no Sylow 2-subgroup) then  $[x, z]^2 \neq 1$ . Hence we have the law

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

as required.

5.6.3. LEMMA. Let  $y \in PSL(2, 2^n)$  have order dividing  $2^n + 1$ . Then for any  $z \in PSL(2, 2^n)$  there exists an element  $x$  of order 2 such that

$$z^{-1}yz = xyx.$$

PROOF. It suffices to prove that the number of distinct conjugates of  $y$  in  $PSL(2, 2^n)$  is equal to the number of distinct conjugates under elements of order 2, where  $y$  has order  $2^n + 1$ . Now the cyclic subgroup generated by  $y$  is self-centralising (by 2.2.7) and hence  $y$  has  $2^n(2^n - 1)$  distinct conjugates. Since  $y$  and  $y^{-1}$  are conjugate, these occur in pairs, two in each of the  $(2^n - 1)2^{n-1}$  cyclic groups of order  $2^n + 1$ . Now the normaliser of  $\langle y \rangle$  in  $PSL(2, 2^n)$  is dihedral of order  $2(2^n + 1)$  and so contains  $2^n + 1$  involutions, one in each of the  $2^n + 1$  Sylow 2-subgroups. Let  $z_1$  be such an involution and  $S$  the Sylow 2-subgroup to which it belongs.

Let  $z_i, z_j$ , and  $z_k, z_l$  be two distinct pairs of elements of  $S$  such that

$$z_i z_j = z_1 = z_k z_l.$$

Then

$$y^{z_i} = y^{z_1 z_j} = y^{-z_j},$$

$$y^{z_k} = y^{z_1 z_l} = y^{-z_l}.$$

Suppose now that

$$y^{z_i} = y^{z_k},$$

then

$$y^{z_i z_k} = y^{z_k^2} = y$$

which implies that  $z_i z_k$  (an involution) centralises  $y$ , a contradiction.

Thus  $y^{z_i} \neq y^{z_k}$  and similarly

$$y^{z_i} \neq y^{z_l}.$$

Now let  $z_m$  be an involution not in  $S$  and suppose

$$y^{z_i} = y^{z_m}.$$

Then  $y^{z_j} = y^{-z_m}$  and so  $y^{z_j z_m} = y^{-1}$ . Thus  $z_j z_m$  belongs to the normaliser of  $y$ , but not to the centraliser. Hence  $(z_j z_m)^2 = 1$  and  $z_j, z_m$  belong to the same Sylow 2-subgroup, a contradiction. Now, there are  $\frac{1}{2}(2^n - 2)$  distinct pairs  $z_i, z_j$  in  $S$ , and there are  $2^n + 1$  Sylow 2-subgroups so, under involutions,  $y$  has (besides itself and  $y^{-1}$ )

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

distinct pairs of conjugates, and hence has altogether  $2^n(2^n - 1)$  distinct conjugates, as required.

5.6.4. COROLLARY.  $PSL(2, 2^n)$  satisfies the law  $[x, y^{2(2^n-1)}]^{(2^{2n-1})} = 1$ .

PROOF. Let  $y$  be an element of order dividing  $2^n + 1$ , and let  $z$  be an arbitrary element of  $PSL(2, 2^n)$ . Then by 5.6.3 there is an element  $x$  of order two such that  $y^z = y^x$ . Hence  $[y, z] = [y, x] = [x, y]^{-1}$  and, from 5.6.2,

$$[y, z]^{2^{2n-1}} = 1$$

so we have the law

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

5.6.5. LEMMA. The following law holds in  $PSL(2, 2^n)$ :

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

PROOF. Let  $x$  be an element of order  $r$ , and  $y$  any element of odd order. If  $y \in N(gp(x))$  then  $[x, y, x] = 1 = [x, y]$ . Otherwise  $[x, y, x] \neq 1$  and, by the previous lemma, it has order dividing either  $2^n + 1$  or  $2^n - 1$ .

(a) Suppose its order is  $2^n + 1$ , then, since

$$\begin{aligned} 2^{2n-1} - 1 &= (2^{n-1} - 1)(2^n + 1) + 2^{n-1} \\ [x, y, x]^{2^{2n-1}-1} &= [x, y, x]^{2^{n-1}}. \end{aligned}$$

Now, by 5.2.5 (8)

$$\begin{aligned} \text{tr } [x, y, x]^{2^{n-1}} [y, x] &= \text{tr } [x, y] \{1 + \text{tr}^{2^{n-2}} [x, y, x] \\ &\quad + \text{tr}^{2^{n-2} + 2^{n-3}} [x, y, x] + \dots \\ &\quad + \text{tr}^{2^{n-2} + 2^{n-3} + \dots + 2} [x, y, x] \\ &\quad + \text{tr}^{2^{n-2} + 2^{n-3} + \dots + 2 + 1} [x, y, x] + \text{tr}^{2^{n-1}} [x, y, x]\} \end{aligned}$$

which, by 5.2.6 (2) is zero.

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

(b) Suppose  $[x, y, x]$  has order  $2^n - 1$  then

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

and, by 5.2.5 (9)

$$\begin{aligned} \text{tr } [x, y, x]^{2^{n-1}-1} [y, x] &= \text{tr } [x, y] \{1 + \text{tr}^{2^{n-2}} [x, y, x] \\ &\quad + \text{tr}^{2^{n-2}+2^{n-3}} [x, y, x] + \dots + \text{tr}^{2^{n-1}-1} [x, y, x]\} \end{aligned}$$

which, by 5.2.6 (1) is zero.

Hence  $\{[x, y, x]^{2^{n-1}-1} [y, x]\}^2 = 1$ .

Combining these results we have the law

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

We have now completed the proof of Theorem 3.3(A) (since laws (1) and (4) are trivial to verify). To complete the characterisation of  $\text{var } PSL(2, 2^n)$  given in 5.5.4 we require laws that make  $\pi_1$ -subgroups abelian, and forbid  $C(q, r)$  where  $q|2^n - 1, r|2^n + 1$ . So far we have been unable to get general laws of this type, though we have the laws in the special case  $n = 3$  given in Theorem 3.3(B). The derivation of these is given in the following section together with an indication of the difficulties involved in generalising them. One major hazard seems to be the lack of a general formula for irreducible polynomials over an arbitrary finite field.

### 5.7 LAWS IN $PSL(2, 8)$

In this section we consider how the laws 5 and 5' given in Theorem 3.3(B) were obtained. Law 6 was found by the sort of process indicated in § 6.4.

#### 5.7.1. THEOREM.

$$\{[[x^{18}, y^{112}]^{36}, x^{36}]^{63} [[x^{18}, y^{14}]^{36}, x^{18}]^{94} [y^{14}, x^{18}]\}^{18} = 1$$

is a law in  $PSL(2, 8)$ .

PROOF. If  $[x^{18}, y^{112}]$  has order dividing 18 the law is trivial, so we have only to consider the case where this has order 7, when the left hand side reduces to

$$\{[x^{18}, y^{112}, x^{36}]^{63} [x^{18}, y^{14}, x^{18}]^{94} [y^{14}, x^{18}]\}^{18}.$$

From now on we use  $x$  and  $y$  instead of  $x^{18}$  and  $y^{14}$ . Now

$$\begin{aligned} \text{tr } [x, y, x] &= \text{tr } [x, y] \{ \text{tr } [x, y] + \text{tr}^2 x \} \\ &= \text{tr } [x, y^{-1}, x], \end{aligned}$$

and so, by Lemma 5.6.1,  $[x, y^{-1}, x^2]$  and  $[x, y, x]$  either both have order dividing 63 or both have order 2.

In the former case the left hand side becomes

$$\{[x, y, x]^{31}[y, x]\}^{18}$$

which, by the same argument as that used in Lemma 5.6.5, is 1.

Hence we may assume both have even order, when the expression becomes

$$\{[x, y^{-1}, x^2][y, x]\}^{18}.$$

Now, since

$$0 = \text{tr } [x, y, x] = \text{tr } [x, y]\{\text{tr } [x, y] + \text{tr}^2 x\}$$

and  $\text{tr } [x, y] \neq 0$ , we have

$$\text{tr } [x, y] = \text{tr}^2 x.$$

Also

$$\begin{aligned} \text{tr } xy^{-1}xy &= \text{tr } x^{-1}x^y + \text{tr } x \text{tr } x^y \\ &= \text{tr } [x, y] + \text{tr}^2 x \\ &= 0. \end{aligned}$$

Now  $\text{tr } [x, y^{-1}, x^2][y, x] = \text{tr } [x, y^{-1}, x^2][x, y]$  and using the fact that

$$(xy^{-1}xy)^2 = (y^{-1}xyx)^2 = 1$$

and 5.2.5 (10), we may reduce this to

$$\{\text{tr } x\{1 + \text{tr } x \text{tr } y\}\}^2.$$

The proof is now completed by computing the last expression for all possible pairs of values chosen from

$$\text{tr } x = \alpha + 1, \alpha^2 + 1, \alpha^2 + \alpha + 1$$

$$\text{tr } y = \alpha, \alpha^2, \alpha^2 + \alpha, 1$$

(where  $\alpha^3 = \alpha + 1$ ).

Unfortunately, both the obvious generalisations of the above law, viz:

$$\{[[x^{34}, y^{480}]^{136}, x^{68}]^{255} [[x^{34}, y^{30}]^{136}, x^{34}]^{382} [y^{30}, x^{34}]\}^{34}$$

and

$$\{[[x^{34}, y^{480}]^{136}, x^{136}]^{255} [[x^{34}, y^{30}]^{136}, x^{34}]^{382} [y^{30}, x^{34}]\}^{34}$$

fail to hold in  $PSL(2, 16)$ , so it seems unlikely that this type of law will yield anything useful for  $PSL(2, 2^n)$  in general, so instead we turn our attention to Engel type laws as exemplified in Theorem 3.3(B) 5'.

5.7.2. THEOREM.  $[[[x^{18}, y^{14}]^{36}, y^{14}]^{36}, y^{28}]^9 = 1$  is a law in  $PSL(2, 8)$ .

PROOF. This is clearly satisfied unless  $[x^{18}, y^{14}]$  has order 7 (and thus trace  $\alpha + 1, \alpha^2 + 1$  or  $\alpha^2 + \alpha + 1$ ). In this case we obtain table A (again replacing  $x^{18}$  and  $y^{14}$  by  $x$  and  $y$ ).



TABLE A

$\text{tr } [x, y]$	$\text{tr } y$	$\text{tr } [x, y] + \text{tr}^2 y$	$\text{tr } [x, y, y]$	$\text{tr } [x, y, y, y]$	$\text{tr } [x, y, y, y^2]$
$\alpha + 1$	1	$\alpha$	$\alpha^2 + \alpha$		
	$\alpha$	$\alpha^2 + \alpha + 1$	$\alpha$		
	$\alpha^2$	$\alpha^2 + 1$	$\alpha^2$		
	$\alpha^2 + \alpha$	1	$\alpha + 1$	$\alpha + 1$	$\alpha^2 + \alpha$
$\alpha^2 + 1$	1	$\alpha^2$	$\alpha$		
	$\alpha$	1	$\alpha^2 + 1$	$\alpha^2 + 1$	$\alpha$
	$\alpha^2$	$\alpha + 1$	$\alpha^2$		
	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + \alpha$		
$\alpha^2 + \alpha + 1$	1	$\alpha^2 + \alpha$	$\alpha^2$		
	$\alpha$	$\alpha + 1$	$\alpha$		
	$\alpha^2$	1	$\alpha^2 + \alpha + 1$	$\alpha^2 + \alpha + 1$	$\alpha^2$
	$\alpha^2 + \alpha$	$\alpha^2 + 1$	$\alpha^2 + \alpha$		

From this table we see that there are only three cases in which  $[x, y, y]$  has order 7, and that in these  $\text{tr } [x, ky]$  is a constant. Accordingly we evaluate  $\text{tr } [x, y, y, y^2]$  and find in these cases this has order 9 and the truth of the theorem follows.

This type of law does generalise to  $PSL(2, 16)$  yielding

$$[[[[[[[x^{34}, y^{30}]^{136}, y^{30}]^{136}, y^{30}]^{136}, y^{60}]^{136}, y^{60}]^{136}, y^{60}]^{136}, y^{60}]^{17} = 1$$

but so far we have not been able to extend it further.

### 6. Bases for $PSL(2, 7)$ , $PSL(2, 9)$ and $PSL(2, 11)$

In this section we prove Theorem 3.4. Let  $\mathfrak{B}_7, \mathfrak{B}_9, \mathfrak{B}_{11}$  be the varieties determined by the sets of laws  $A, B$  and  $C$  listed in Theorem 3.4 and  $\mathfrak{U}_7, \mathfrak{U}_9, \mathfrak{U}_{11}$  the varieties generated by  $PSL(2, 7), PSL(2, 9)$  and  $PSL(2, 11)$  respectively; then our aim is to prove that  $\mathfrak{B}_i = \mathfrak{U}_i$ . In sections 6.1–6.3 we prove that  $\mathfrak{B}_i \leq \mathfrak{U}_i$ ; the reverse inequality may be proved by checking that the appropriate set of laws holds in each of the above groups. In section 6.4 we indicate the methods by which the laws were obtained.

#### 6.1 CONSEQUENCES OF THE LAWS

6.1.1. LEMMA.  *$p$ -groups in  $\mathfrak{B}_i$  for odd primes  $p$  are abelian, and so are 2-groups in  $\mathfrak{B}_{11}$ .*

PROOF. The second result follows from the exponent law in  $\mathfrak{B}_{11}$ , and the first from the laws A 3, 4; C 2, 3, 4; together with the appropriate exponent law. These laws are of two types; we consider an example of each.

A.3. 
$$\{(x^{28} y^{28})^{57} [x^{28}, y^{28}]^{14}\}^{28} = 1.$$

Let  $x$  and  $y$  be elements of order 3 belonging to a 3-group of exponent 3 which

satisfies this law. Then the first term vanishes and we have  $[x, y]^{3^{92}} = 1$ . But  $[x, y]^3 = 1$  and so  $[x, y] = 1$ .

C.3.  $\{(x^{66}y^{66})^{180}[[x^{66}, y^{264}]^{66}, x^{66}]^{67}(x^{66}y^{66})^{150}[x^{66}, y^{66}]\}^{66} = 1$ .

Let  $G$  be a finite group of exponent 5 which satisfies this law, and let  $N$  be a maximal abelian normal subgroup. If  $G \neq N$  then  $N \not\leq Z(G)$  and there exist  $x \in N, y \in G$  such that  $[x, y] \neq 1$ , but, since  $N$  is abelian,  $[x, y, x] = 1$ . Thus the above law reduces to  $[y, x]^{66} = 1$ , and thus  $[x, y] = 1$ , giving a contradiction. It follows that  $G$  is abelian.

6.1.2. LEMMA. 2-groups in  $\mathfrak{B}_7$  and  $\mathfrak{B}_9$  belong to  $\mathfrak{D}$ .

PROOF. Laws A 1,2 and B 1,2 reduce in a 2-group to  $x^4 = 1$  and  $[x, y^2] = 1$ . By 2.2.1 these determine  $\mathfrak{D}$ .

Thus each  $\mathfrak{B}_i$  satisfies the conditions of 2.2.3 (i) and so we have:

6.1.3. COROLLARY.  $\mathfrak{B}_i$  is a Cross variety.

6.1.4. LEMMA. The groups  $C(\lambda^\alpha, m)$  do not belong to  $\mathfrak{B}_i$  for the following pairs  $(\lambda^\alpha, m)$ :

- $i = 7 : (7,2), (7,4), (2,7), (4,7), (3,7);$
- $i = 9 : (3,5), (5,3), (5,4), (2,5), (4,5);$
- $i = 11 : (11,2), (11,3), (2,11), (3,11), (5,11), (2,5), (3,5), (5,3).$

PROOF. We note that, since  $\text{var } C(\lambda^\beta, m_1) \leq \text{var } C(\lambda^\alpha, m)$  for  $\beta \leq \alpha, m_1|m$ , forbidding  $C(\lambda^\beta, m_1)$  automatically forbids  $C(\lambda^\alpha, m)$ .

Now,  $C(\lambda^\alpha, m)$  has exponent  $m\lambda^\alpha$  and its derived group is abelian of exponent  $\lambda^\alpha$ . Also it contains elements  $x$  of order  $\lambda^\alpha$  and  $y$  and  $z$  of order  $m$  such that  $[x, y^{m_1}] \neq 1$ , and  $[y^{m_1}, z^{m_2}] \neq 1$ , for any proper divisors  $m_1, m_2$  of  $m$ . Using these facts together with the laws A 4,5,6, B 5,6,7,8 and C 4,5,6,7,8,9,10 we obtain the required result.

6.1.5. COROLLARY.  $\mathfrak{D}\mathfrak{A}_7 \cap \mathfrak{B}_7 = \mathfrak{D} \cup \mathfrak{A}_7 = \mathfrak{A}_7\mathfrak{D} \cap \mathfrak{B}_7;$   
 $\mathfrak{D}\mathfrak{A}_5 \cap \mathfrak{B}_9 = \mathfrak{D} \cup \mathfrak{A}_5;$   
 $\mathfrak{A}_5\mathfrak{D} \cap \mathfrak{B}_9 = \mathfrak{A}_5\mathfrak{A}_2.$

6.2 FINITE SOLUBLE GROUPS IN  $\mathfrak{B}_i$

As an immediate consequence of 2.2.5 and 6.1.1 and 6.1.2 we have:

6.2.1. LEMMA. A finite soluble group in  $\mathfrak{B}_i$  has  $p$ -length one for all odd primes  $p$ , 2-length one for  $i = 11$ , and 2-length 2 for  $i = 7, 9$ .

6.2.2. LEMMA. A finite group of exponent 12 in  $\mathfrak{B}_7$  or  $\mathfrak{B}_9$  belongs to  $\mathfrak{U}_7, \mathfrak{U}_9$  respectively.

PROOF. In  $\mathfrak{B}_7$  the laws A 7,8,9 reduce, modulo  $x^{12} = 1$  to  $[x, y]^6 = 1$ ,  $[x^6, y^6] = 1$  and  $[[x, y]^3, y^3, y^2] = 1$  and in  $\mathfrak{B}_9$  the laws B 9,10,11 reduce to  $[x, y]^6 = 1$ ,  $[x^6, y^6]^3 = 1$  and  $[[x, y]^3, y^3, y^2] = 1$ . Using Theorem 3.1 and Lemmas 6.1.1 and 6.1.2 we have that groups of exponent 12 in  $\mathfrak{B}_7$  belong to  $\text{var } S_4 \leq \mathfrak{U}_7$  and groups of exponent 12 in  $\mathfrak{B}_9$  belong to  $\text{var } S_4 \cup \mathfrak{A}_3\mathfrak{A}_4 \leq \mathfrak{U}_9$ .

6.2.3. LEMMA. *A critical soluble group in*

- (i)  $\mathfrak{B}_7$  has exponent 12 or belongs to  $\mathfrak{A}_7\mathfrak{A}_3$ ,
- (ii)  $\mathfrak{B}_9$  has exponent 12 or belongs to  $\mathfrak{A}_5\mathfrak{A}_2$ ,
- (iii)  $\mathfrak{B}_{11}$  belongs to  $\mathfrak{A}_3\mathfrak{A}_2$ ,  $\mathfrak{A}_2\mathfrak{A}_3$ ,  $\mathfrak{A}_{11}\mathfrak{A}_5$  or  $\mathfrak{A}_5\mathfrak{A}_2$ .

PROOF. Let  $G$  be a critical soluble group in  $\mathfrak{B}_i$ . Consider the upper  $\tilde{p}$ -series of  $G$  where  $\tilde{p} = 7, 5, 11$  for  $i = 7, 9, 11$  respectively. By 6.2.1. this has the form

$$1 \leq N_0 \leq P_1 \leq N_1 = G,$$

where  $N_0$  and  $N_1/P_1$  are  $\tilde{p}'$ -groups and  $P_1/N_0$  is a  $\tilde{p}$ -group. Let  $S$  be the Sylow  $\tilde{p}$ -subgroup of  $P_1$ , then  $P_1 = SN_0$ . But  $N_0$  is a soluble  $\tilde{p}'$ -group, and  $S$  stabilises the chief factors (by 6.1.3). Hence  $S$  centralises  $N_0$  and so  $P_1 = S \times N_0$ . Since  $S$  and  $N_0$  are both characteristic in  $P_1$ , and  $G$  is critical, we have  $S = 1$  or  $N_0 = 1$ .

(i)  $S = 1$ . In  $\mathfrak{B}_7$  and  $\mathfrak{B}_9$  this means that  $G$  has exponent 12 and there is nothing further to prove.

In  $\mathfrak{B}_{11}$   $G$  has exponent 30, and we have to repeat the argument above, considering now the upper 5-series to obtain that  $G$  either belongs to  $\mathfrak{A}_2\mathfrak{A}_3$  or  $\mathfrak{A}_3\mathfrak{A}_2$  or has a normal Sylow 5-subgroup. In the latter case, since this is necessarily centralised by elements of order 3, from 2.2.5 we see that the factor group has exponent 2 and so  $G \in \mathfrak{A}_5\mathfrak{A}_2$ .

(ii)  $N_0 = 1$ . Then  $G$  has a normal Sylow  $\tilde{p}$ -subgroup,  $S$ , and  $C_G(S) \leq S$  (2.2.5). It follows from 6.1.3 that  $|G|$  cannot be divisible by 2 if  $i = 7$ , by 3 if  $i = 9$ , and by 2 nor 3 if  $i = 11$ .

Hence

$$\begin{aligned} G &\in \mathfrak{A}_7\mathfrak{A}_3 \text{ if } i = 7, \\ G &\in \mathfrak{A}_5\mathfrak{A}_2 \text{ if } i = 9, \\ G &\in \mathfrak{A}_{11}\mathfrak{A}_5 \text{ if } i = 11. \end{aligned}$$

Since  $\mathfrak{A}_5\mathfrak{A}_2 \cap \mathfrak{B}_9 = \mathfrak{A}_5\mathfrak{A}_2$  (6.1.4) the proof of the lemma is complete.

6.2.4. THEOREM. *A soluble group in  $\mathfrak{B}_i$  belongs to  $\mathfrak{U}_i$ .*

PROOF. This follows immediately from 6.2.2, 6.2.3 and the list of subgroups of  $PSL(2, i)$  ( $i = 7, 9, 11$ ) given in 2.2.7.

6.3 FINITE NON-SOLUBLE GROUPS IN  $\mathfrak{B}_i$

Since  $\mathfrak{B}_i$  is by 6.1.3 a Cross variety, in order to complete the proof that  $\mathfrak{B}_i \leq \mathfrak{U}_i$  we have only to prove that finite non-soluble groups in  $\mathfrak{B}_i$  are in  $\mathfrak{U}_i$ .

6.3.1. LEMMA. *The only simple groups in  $\mathfrak{X}_i$  are  $PSL(2, i)$ , and, for  $i = 9$  and  $11$ ,  $PSL(2, 5)$ .*

PROOF. The laws  $u_{169}, u_{361}, u_{661}$  tell us that the maximal order of a simple group in  $\mathfrak{X}_i$  is, respectively, 168, 360, 660. This, together with the exponent law and a consideration of the list of simple groups of order less than 1000 (e.g. Burnside [1] Note  $N$ ) gives the required result.

6.3.2. THEOREM. *A finite non-soluble group in  $V_i$  has the form*

$$S \times T_1 \times \cdots \times T_k$$

where  $S$  is soluble and  $T_i$  is simple.

PROOF. Let  $G$  be a minimal counterexample. Since the set of all such groups (for each  $i$ ) is precisely the set of finite groups in  $\mathfrak{U}_i$  (by 6.2.4 and Oates [18] Lemma3.2)  $G$  is necessarily critical. We consider separately the cases in which  $\sigma G$  is non-abelian and abelian.

(i)  $\sigma G$  non-abelian. Then  $\sigma G$  is a direct product of simple groups and  $|G| = |G/\sigma^*G| \leq 168, 360, 660$  for  $i = 7, 9, 11$  respectively. In  $\mathfrak{X}_7$ ,  $G$  must be  $PSL(2, 7)$ ; in  $\mathfrak{X}_9$  and  $\mathfrak{X}_{11}$  we can have either  $G$  is  $PSL(2, 9)$ ,  $PSL(2, 11)$ , or that  $\sigma G$  is  $PSL(2, 5)$ . In the latter case  $G$  is a subgroup of  $S_5$ . As  $S_5$  itself does not satisfy B 7 or C 1,  $G$  can only be  $PSL(2, 5)$ .

(ii)  $\sigma G$  abelian. By the argument used in 5.5.4 (ii) we have that  $G/\sigma G = T$ , a simple group. Now, if  $T$  is  $PSL(2, 7)$ ,  $PSL(2, 9)$ ,  $PSL(2, 11)$ , or  $PSL(2, 5)$  in  $\mathfrak{X}_9$  it is generated by its  $\tilde{p}$ -groups (where  $\tilde{p}$  has the same meaning as in 6.2.3), and these must centralise  $\sigma G$  (by 6.1.1 and 6.1.4), so in all these cases  $\sigma G \leq Z(G)$ . The one remaining case is  $G \in \mathfrak{X}_{11}$  and  $G/\sigma G = PSL(2, 5)$ . If  $\sigma G$  is not an 11-group, then consideration of the 5-subgroups of  $PSL(2, 5)$  gives  $\sigma G \leq Z(G)$ . If it is an 11-group then we may obtain the same result by considering the 3-subgroups. Hence, in all cases,  $\sigma G \leq Z(G)$ . Since  $G$  is critical,  $\sigma G \leq \gamma_2 G$ , and so  $\sigma G$  is isomorphic to a subgroup of the multiplier of  $G/\sigma G$ . This is  $C_2, C_6, C_2, C_2$  for  $PSL(2, 7)$ ,  $PSL(2, 9)$ ,  $PSL(2, 11)$  and  $PSL(2, 5)$  respectively, and  $G$  has the possible values  $PSL(2, 7)$ ,  $SL(2, 7)$  ( $i = 7$ );  $PSL(2, 9)$ ,  $SL(2, 9)$ , a group with centre  $C_3$  and factor group isomorphic to  $PSL(2, 9)$ ,  $PSL(2, 5)$ ,  $SL(2, 5)$  ( $i = 9$ );  $PSL(2, 11)$ ,  $SL(2, 11)$ ,  $PSL(2, 5)$ ,  $SL(2, 5)$  ( $i = 11$ ). The class of the Sylow 2-subgroups of  $SL(2, 7)$ ,  $SL(2, 9)$  and  $SL(2, 11)$  prevents them from belonging to  $\mathfrak{X}_7, \mathfrak{X}_9, \mathfrak{X}_{11}$ , and also prevents  $SL(2, 5)$  from belonging to  $\mathfrak{X}_{11}$ . Similarly the Sylow 3-subgroup of the group with centre  $C_3$  is not elementary abelian and so this group is not in  $\mathfrak{X}_9$ .  $SL(2, 5)$  has  $SL(2, 3)$  as a subgroup, and, by 4.4.2 this does not belong to  $\mathfrak{X}_9$ . We are left with  $G$  being one of our simple groups, and the truth of the theorem follows.

### 6.4 DETERMINATION OF THE TWO VARIABLE LAWS IN $PSL(2, 7)$

In this section we indicate how the two-variable laws for  $PSL(2, 7)$  were obtained. Similar methods were used for  $PSL(2, 9)$  and  $PSL(2, 11)$ .

From § 6.1 it is clear that we require laws which imply that Sylow 2-subgroups are in  $\mathfrak{Q}$  and Sylow 3- and 7-subgroups in  $\mathfrak{A}_3$  and  $\mathfrak{A}_7$  respectively; laws to forbid  $C(7, 2)$ ,  $C(7, 4)$ ,  $C(2, 7)$ ,  $C(4, 7)$ , and  $C(3, 7)$ , and finally, laws which imply that groups of exponent 12 are in  $\text{var } S_4$ . From Theorem 3.2 we see that the law  $[x^3, y^{12}]^{12} = 1$  holds in  $PSL(2, 7)$ , which deals with the Sylow 7-subgroups,  $C(7, 2)$  and  $C(7, 4)$ . Before determining the remaining laws we must find out how many essentially distinct ways there are of choosing pairs of elements of prescribed orders, and, to do this, we use Corollary 5.2.3 which tells us that the trace of any word in  $x$  and  $y$  is determined by the traces of  $x, y, xy$  and  $xy^{-1}$ . Now, the possible traces are  $0, \pm 1, \pm 2, \pm 3$ , which correspond to elements of orders 2, 3, 7 or 1, and 4 respectively. Thus, except for  $\text{tr } x = \pm 2$ , the trace determines the order uniquely.

Using 5.2.3 we construct Table 1 (given in Appendix II). From this we obtain immediately the Sylow 3-law, for the commutator of two elements of order 3 has order 3 only when the order of the product is prime to 3. Thus (vide 5.3.3) we have the law

$$\{(x^{28}y^{28})^{57}[x^{28}, y^{28}]^{14}\}^{28} = 1.$$

For the remaining laws we have to work a little harder. Consider, for example, the Sylow 2-law. Here we require a law that reduces to  $[x, y^2] = 1$  in a group of exponent 4, so we look at  $[x^{2^1}, y^{4^2}]$ . This is clearly trivial unless  $x$  has order 2 or 4 and  $y$  has order 4. Calculating the trace of  $[x, y^2]$  in these cases we obtain table B.

TABLE B

Tr.	$x$	$y$	$xy$	$xy^{-1}$	$[x, y^2]$
	0	$\pm 3$	0	0	$\pm 2$
			$\pm 1$	$\pm 1$	$\pm 3$
			$\pm 2$	$\pm 2$	$\pm 1$
			$\pm 3$	$\pm 3$	$\pm 2$
	$\pm 3$	$\pm 3$	0	$\pm 2$	$\pm 2$
			$\pm 1$	$\pm 1$	0
				$\pm 3$	$\pm 1$
			$\pm 2$	0	$\pm 2$
				$\pm 3$	$\pm 3$
			$\pm 3$	$\pm 1$	$\pm 1$
				$\pm 2$	$\pm 3$

From this table we see that we have four cases in which  $[x, y^2]$  has order divisible by 2, and that in one of these  $xy$  also has order 4, but that then  $xy^{-1}$  has order 7 (it obviously cannot have order 1 since  $[x, y^2] \neq 1$ ). Hence we consider an expression of the form

$$\{(x^{2^1}y^{2^1})^{4\alpha}(x^{2^1}y^{6^3})^{4\beta}[x^{2^1}, y^{4^2}]^\gamma\}^{2^1} \quad (\gamma \text{ odd})$$

and endeavour to choose  $\alpha$  and  $\beta$  so that this vanishes everywhere. A possible selection is  $\alpha = 13, \beta = 1, \gamma = 9$ .

All the necessary calculations can be performed working with traces, but, for lengthy words, these become somewhat tedious, and it seems easier to select elements of  $PSL(2, 7)$  having the required orders for  $x, y, xy$  and  $xy^{-1}$  and work with these. Such elements are given in table 2 (Appendix II), expressed in the permutation representation of  $PSL(2, 7)$  on seven letters, generated by (12)(36) and (1234567).

Note that by Theorem 5.2.2 the trace of a word in  $x$  and  $y$  will be independent of the choice of  $x$  and  $y$  (for each case) and so the orders of these words are uniquely determined up to the ambiguity between elements of orders 1 and 7. However, all our 2-variable laws in  $PSL(2, 7)$ , save  $[x^3, y^{12}]^{12} = 1$  (which was determined by other means) are raised to a power divisible by 7, so that this ambiguity is irrelevant. (A little more care has to be exercised in  $PSL(2, 9)$  and  $PSL(2, 11)$  where we have laws other than the standard ones which are not raised to a power divisible by 3 or 11, respectively.)

### 7. Laws in $SL(2, q)$

#### 7.1 INTRODUCTION

Let  $w(x_1, \dots, x_r)$  be a law defining var  $PSL(2, q)$ ,  $q = p^n$ ,  $p$  an odd prime. We denote by  $\mathfrak{R}_q$  the variety defined by the laws  $[w(x_1, \dots, x_r), y] = 1$  and  $w(x_1, \dots, x_r)^2 = 1$ , and by  $\mathfrak{U}_q$  the variety generated by  $SL(2, q)$ .

We want to show that, for  $q = 8h \pm 1$ , with  $h$  odd, or  $q = 8h \pm 3$ , and  $n$  an odd integer or for  $q = 9$ ,  $\mathfrak{R}_q = \mathfrak{U}_q$ . For arbitrary  $q$ , it is easy to see  $\mathfrak{U}_q \subseteq \mathfrak{R}_q$ , and easy to show that  $\mathfrak{R}_q$  is a Cross variety. It is easy to show that the non-soluble critical groups in  $\mathfrak{R}_q$  are the same as the non-soluble critical groups in  $\mathfrak{U}_q$ , provided  $GL(2, p^m)$  does not occur as a subgroup of  $SL(2, q)$  ( $p^m > 3$ ), that is, whenever  $n$  is odd, by 2.2.7, or  $q = 9$ . The other cases we cannot deal with at present. The soluble critical groups of  $\mathfrak{R}_q$  can be shown to be the same as the soluble critical groups of  $\mathfrak{U}_q$  if  $q = 8h \pm 3$ , or  $q = 8h \pm 1$ , with  $h$  odd. Combining these two results gives Theorem 3.5. For  $q = 8h \pm 1$ , with  $h$  even, M. F. Newman has pointed out that  $Q$  wr  $C_2$  is in  $\mathfrak{R}_q$ , while 2-groups in  $\mathfrak{U}_q$  are metabelian, giving  $\mathfrak{U}_q \neq \mathfrak{R}_q$ .

We start by proving:

7.1.1 LEMMA.  $\mathfrak{R}_q$  is a Cross variety.

PROOF. Let  $G$  be a finitely generated group in  $\mathfrak{R}_q$ . Then  $G/w(G) \in \text{var } PSL(2, q)$  and  $w(G)$  is central and of exponent 2. If  $PSL(2, q) \in C(e, m, c)$ , then  $G \in C(2e, m, c + 1)$ , and so  $\mathfrak{R}_q$  is a Cross variety by 2.2.3.

#### 7.2 NON-SOLUBLE CRITICAL GROUPS IN $\mathfrak{R}_q$ , $q = p^n$ , $n$ ODD OR $q = 9$

For such  $q$ , we claim that a non-soluble critical group in  $\mathfrak{R}_q$  is in var  $SL(2, q)$ . An examination of the subgroups of  $SL(2, q)$  will convince the reader that it suffices to prove the following lemma.

7.2.1. LEMMA. (a) *If  $q \equiv \pm 1 \pmod{10}$ , then a non-soluble critical group in  $\mathfrak{B}_q$  is isomorphic to  $SL(2, p^m)$  or  $PSL(2, p^m)$ , where  $m$  divides  $n$ .*

(b) *If  $q \equiv \pm 1 \pmod{10}$ , then a non-soluble critical group in  $\mathfrak{B}_q$  is isomorphic to  $SL(2, p^m)$ ,  $PSL(2, p^m)$ , where  $m$  divides  $n$ , or  $SL(2, 5)$ , or  $PSL(2, 5)$ .*

PROOF. Let  $G$  be a non-soluble critical group in  $\mathfrak{B}_q$ . If  $w(G) = 1$ , then  $G \in \text{var } PSL(2, q)$ , and the result follows. If  $w(G) \neq 1$ , then  $w(G)$  is central in  $G$ , and is an elementary abelian 2-group. Since  $G$  is critical, it follows that  $w(G)$  is cyclic of order 2.

By Lemma 3.2 of Oates [18],  $G/w(G) = H_1/w(G) \times H_2/w(G) \times \cdots \times H_t/w(G)$ , where each  $H_i/w(G)$  is either non-abelian simple or soluble. If  $t > 1$ ,  $G$  is not critical, by Theorem 2.1 of Weichsel [23]. Hence  $t = 1$ , and since  $G$  is non-soluble,  $G/w(G)$  is non-abelian simple. The result now follows from Satz 25.7 of Huppert [13].

### 7.3 THE SOLUBLE CRITICAL GROUPS OF $\mathfrak{B}_q$ , $q = 8h \pm 3$

Firstly, note that for  $q = 8h \pm 3$ , the Sylow 2-subgroup of  $PSL(2, q)$  is elementary abelian of order 4, and the Sylow 2-subgroup of  $SL(2, q)$  is the quaternion group  $Q$ . With this in mind, we prove:

7.3.1. LEMMA. *A nilpotent critical group in  $\mathfrak{B}_q$  is in  $\mathfrak{U}_q$ .*

PROOF. Let  $G$  be a critical 2-group in  $\mathfrak{B}_q$ . If  $w(G) = 1$ , then  $G \in \text{var } PSL(2, q) < \mathfrak{U}_q$ . Hence suppose  $w(G) \neq 1$ : as before, we see that  $w(G)$  is cyclic of order 2. Also,  $G/w(G)$  is elementary abelian, and so  $G$  has class at most 2. It now follows from Lemma 5.1 of Weichsel [24] that  $G$  is in the variety generated by the Sylow 2-subgroup of  $SL(2, q)$ .

If  $G$  is a nilpotent critical group of order prime to 2, then  $w(G) = 1$ , and so  $G \in \text{var } PSL(2, q) < \mathfrak{U}_q$ , and the proof is complete.

We now turn to the soluble non-nilpotent critical groups in  $\mathfrak{B}_q$  which are not in  $\text{var } PSL(2, q)$ . If  $G$  is such a group, then as before  $w(G)$  is cyclic of order 2. Since  $w(G)$  is central, and  $G$  is critical,  $G/w(G)$  cannot contain any normal subgroups of order prime to 2. Thus, putting  $H = G/w(G)$ , we have that  $\sigma H$  is a 2-group. It follows that  $H \in \mathfrak{U}_2\mathfrak{U}_3$ , and from Lemma 5.2.5 of Cossey [2], that  $H = H_1 \times H_2$ , where  $Z(H_1) = 1$ , and  $H_2$  is an elementary abelian 2-group. If  $H_1 = 1$ , then  $G$  is nilpotent, and so we have that  $H_1 \neq 1$ , for  $G$  was assumed non-nilpotent. Also, if  $H_2 \neq 1$ ,  $G$  is not critical by Theorem 2.1 of Weichsel [23], and so we have  $H = H_1$ .

Now let  $F$  be the Sylow 2-subgroup of  $G$ : we have  $F < G$ . Further,  $G/w(G)$  is an elementary abelian 2-group and, regarded as a  $GF(2)G$ -module, is completely reducible by Maschke's theorem. From Lemma 7.3.1, we may conclude that  $F$  has class 2, and then from Lemma 2.4.3 of Sheila Oates and M. B. Powell [19] it follows that there are at most 2 irreducible components in a decomposition of  $F/w(G)$ .

Suppose that  $F/w(G)$  is irreducible. Since an abelian group with a faithful irreducible representation is cyclic,  $|G/F| = 3$ . Hence  $|F/w(G)| = 4$ , and  $G/w(G) = PSL(2, 3)$ . From Satz V 25.7 of Huppert [13] it follows that  $G = SL(2, 3)$ .

Suppose that  $F/w(G)$  has 2 irreducible components in a decomposition. Then  $F$  is either  $QcpQ$  or  $QcpD_4$ . It is not difficult to see that a 3-group of automorphisms of  $QcpD_4$  has a non-trivial fixed point modulo the derived group of  $QcpD_4$  (for example, by using 5.4, p. 206 of D. Gorenstein [8]), and so  $F$  cannot be  $QcpD_4$ . If  $F$  is  $QcpQ$ , then it is not difficult to see that  $G$  must be isomorphic to a subgroup of  $SL(2, 3)cpSL(2, 3)$ , and that any such subgroup must contain a copy of  $SL(2, 3)$ . But then  $G$  is not critical.

Thus if  $G$  is a soluble critical group in  $\mathfrak{B}_q$ ,  $q = 8h \pm 3$ ,  $G \in \mathfrak{U}_q$ .

**7.4 THE SOLUBLE CRITICAL GROUPS IN  $\mathfrak{B}_q$ ,  $q = 8h \pm 1$ ,  $h$  ODD**

We start by proving:

7.4.1. LEMMA. *A nilpotent critical group in  $\mathfrak{B}_q$  is also in  $\mathfrak{U}_q$ .*

PROOF. Let  $G$  be a critical 2-group in  $\mathfrak{B}_q$ . If  $w(G) = 1$ , then  $G \in \text{var } PSL(2, q) < \mathfrak{U}_q$ , and so we may suppose that  $w(G) \neq 1$ . As usual,  $w(G)$  is central and of order 2. Also  $G/w(G) \in \mathfrak{D}$ , for the Sylow 2-subgroup of  $PSL(2, q)$  is  $D_4$ . Thus  $G$  is a 2-group of class 3 such that  $G$  has exponent dividing 8,  $\gamma_2 G$  has exponent dividing 4, and  $\gamma_3 G$  has exponent dividing 2. It follows from Lemma 5.1 of Weichsel [24] that  $G$  is in the variety generated by the Sylow 2-subgroup of  $SL(2, q)$ .

If  $G$  has order prime to 2, then  $w(G) = 1$ , and  $G \in \text{var } PSL(2, q) < \mathfrak{U}_q$ , and the proof is complete.

Now, let  $G$  be a non-nilpotent soluble critical group in  $\mathfrak{B}_q$  which is not in  $\text{var } PSL(2, q)$ . As in 7.3,  $w(G)$  is cyclic of order 2, and, putting  $H = G/w(G)$ ,  $\sigma H$  is a 2-group. It follows that  $H \in \text{var } S_4$ .

7.4.2. LEMMA. *Let  $K \in \text{var } S_4$ , and let  $\sigma K$  be a 2-group. If  $F$  is the Fitting subgroup of  $K$ , and  $F \neq K$ , then  $F = F_1 \times \dots \times F_k \times T$ , where each  $F_i$  is a minimal normal subgroup of  $K$ , and is non-trivial, regarded as a  $GF(2)K$ -module,  $T \triangleleft K$ , and all the chief factors of  $K$  contained in  $T$  are trivial, regarded as  $GF(2)K$ -modules.*

PROOF. We first note that  $S_4 \in \mathfrak{A}_2 \mathfrak{A}_3 \mathfrak{A}_2$ , and so  $K$  has an elementary abelian normal 2-subgroup  $N$  with  $K/N \in \mathfrak{A}_3 \mathfrak{A}_2$ . From this it follows that any non-trivial chief factor of 2-power order lies in  $N$ , and from Lemma 4.3.1 that any non-trivial chief factor of  $K$  is complemented in  $N$ . Thus  $N = F_1 \times \dots \times F_k \times T_0$ , where the chief factors of  $K$  in  $T_0$  are all trivial.

Now, consider  $\Phi F$ . Not all of  $F_1, \dots, F_k$  lie in  $\Phi F$ , for if they did, every element of order 3 would centralise all of  $F$ , and there would be no non-trivial chief factors of 2-power order. Suppose that  $F_1 \cap \Phi F = 1$ . Then  $F/\Phi F = F_1 \Phi F/\Phi F \times T_1/\Phi F$ , where  $T_1 \triangleleft K$ , by Lemma 4.3.1. Thus  $F = F_1 \times T_1$ , and the result follows by induction.



From Lemma 7.4.2, we have that if  $F$  is the Fitting subgroup of  $H$ , then  $F = F_1 \times \cdots \times F_k \times T$ , with  $k \geq 1$ , each  $F_i$  a non-trivial minimal normal subgroup of  $H$ ,  $T < H$ , and each chief factor of  $H$  in  $T$  trivial. It follows from Theorem 1 of Higman [12] that  $F_1 \times \cdots \times F_k$  is complemented in  $H$ , and then from Lemma 2.4.3 of Oates and Powell [19] that  $G$  is not critical if  $k > 2$ . Suppose  $k = 2$ . Let  $P/w(G) = F_1 \times F_2$ . Then  $P$  is either  $QcpQ$  or  $QcpD_4$ . As in 7.3, we see that  $P$  cannot be  $QcpD_4$ . If  $P$  is  $QcpQ$ , and  $P_i/w(G) = F_i$ ,  $i = 1, 2$ , then  $P_i \cong Q$ ,  $i = 1, 2$ . But there are only 2 subgroups of  $QcpQ$  isomorphic to  $Q$ , and so  $[P_1, P_2] = 1$ . Again by Lemma 2.4.3 of Oates and Powell [19],  $G$  is not critical. Thus  $k = 1$ , and by Lemma 4.3.1 we conclude that  $H/F = S_3$  or  $C_3$ .

If  $H/F = C_3$ , then  $H = A_4 \times T$ , and by Theorem 2.1 of Weichsel [23],  $G$  is not critical unless  $T = 1$ . But then it follows from V Satz 25.7 of Huppert [13] that  $G$  is isomorphic to  $SL(2,3)$ .

Hence we suppose that  $H/F = S_3$ . We have seen that  $F_1$  is complemented in  $H$ ; let  $B$  be such a complement. Then if  $S$  is a Sylow 2-subgroup of  $B$ ,  $T \leq S$ , and any subgroup of  $T$  normal in  $S$  is normal in  $H$ . Let  $A = \Phi S$ : then  $A \triangleleft H$ , for  $A \leq T$ . Suppose  $A \neq T$ . Then  $S/A = R/A \times T/A$ . Put  $E = RD$ , where  $D$  is a Sylow 3-subgroup of  $B$  (note that  $D \triangleleft B$ ),  $F_0/w(G) = F_1$ ,  $T_0/w(G) = T$ ,  $E_0/w(G) = E$ . Then we have  $G = gp(F_0, T_0, E_0)$ ,  $G \neq gp(F_0, E_0)$ ,  $G \neq gp(T_0, E_0)$ . Let  $x \in F_0$ ,  $x \notin \sigma G$ , and let  $z$  be an element of order 3 in  $G$ . Then  $F_0$  is generated by  $[x, z]$  and its conjugates. Let  $y \in T_0$ : it follows from the Witt identity that  $[x, z, y] = 1$ . We conclude that  $[F_0, T_0] = 1$ , and so  $G$  is not critical. Thus  $A = T$ , and since  $S/T$  is of order 2, we see that  $S$  is cyclic of order 2 or 4.

Now let  $S_4 = gp(x, y | x^2 = y^3 = (xy)^4 = 1)$ , and  $C_4 = gp(z | z^4 = 1)$ . Then  $H$  is isomorphic to the subgroup of  $S_4 \times C_4$  generated by  $xz$  and  $y$ . From 2.2.7 we have that the order of the Schur multiplier of  $H$  is at most that of the Schur multiplier of  $\gamma_2 H = A_4$ . The Schur multiplier of  $A_4$  is  $C_2$ , and, as we shall see below, the Schur multiplier of  $H$  is non-trivial, and so is just  $C_2$ . Hence  $G$  is a representing group of  $H$ . Also, by Theorem I of I. Schur [20], there are at most 2 non-isomorphic representing groups for  $H$ . We show by construction that there are in fact precisely 2 non-isomorphic representing groups for  $H$ .

Let  $GL(2, 3)$  be generated by elements  $x$  (of order 4) and  $y$  (of order 3), and let  $C_4$  be generated by  $u$ ,  $C_8$  by  $v$ . The 2 representing groups are:

- (1) the subgroup of  $GL(2, 3) \times C_4$  generated by  $xu$  and  $y$ , and
- (2)  $B/N$ , where  $B$  is the subgroup of  $GL(2, 3) \times C_8$  generated by  $xv$  and  $y$ , and  $N = gp(w^{-1}v^4)$ , with  $1 \neq w \in Z(GL(2, 3))$ .

Since both these groups are in  $\mathcal{U}_q$ , we have that  $G \in \mathcal{U}_q$ .

Finally, suppose that  $T = 1$ . Then  $H = S_4$ , and we see that  $G$  is isomorphic to  $GL(2, 3)$  or  $A$ , where  $A$  is the splitting extension of  $SL(2, 3)$  by  $C_2 = gp(z)$ , with  $z$  acting on  $SL(2, 3)$  as the inner automorphism induced by  $x$  above. In either case,  $G \in \mathcal{U}_q$ , and the proof is complete.

**8. Theorems 3.6 and 3.7**

**8.1** The proof of Theorem 3.6 follows so closely that of Theorem 3.4 (B) that we give no details except to remark that the law (ii) is needed to eliminate  $\mathfrak{A}_5\mathfrak{Q}$ , since  $\text{var } S_4 \supseteq \mathfrak{A}_5\mathfrak{A}_4$ , but not  $\mathfrak{A}_5\mathfrak{Q}$ .

**8.2** The proof of 3.7 is also akin to that given in §§ 6.1 and 5.5 once it has been established that a finitely generated group in the relevant variety is finite and soluble, so we consider this point only.

8.2.1. THEOREM. *A finitely generated group in the variety defined by the laws given in Theorem 3.7 (A) is finite and soluble.*

PROOF. By law 4 any two elements of order 7 commute, so if  $N = gp(g^{12} | g \in G)$  then  $N$  is abelian of exponent 7 and  $G/N$  has exponent 12, and hence satisfies the laws  $x^{12} = 1$ ,  $\{(x^3 y^3)^4 [x^3, y^4]^3\}^3 = 1$ ,  $[x^2, y^2]^2 = 1$ ,  $[x, y]^6 = 1$ .  $[x^6, y^6] = 1$ ,  $[[x, y]^3, y^3, y^2] = 1$  and so belongs to  $\text{var } S_4$  by Theorem 3.1. Hence  $G/N$  is finite and soluble and so  $N$  is finitely-generated and thus finite (and abelian). It follows that  $G$  is a finite soluble group as required.

8.2.2. THEOREM. *A finitely generated group in*

$$\mathfrak{B} = \text{var} (x^{2(2^{2n}-1)}, [x^2, y^2]^2, [x^2, y^{2(2^n-1)}])$$

*is finite and soluble.*

PROOF. Let  $r = 2^n - 1$ ,  $s = 2^n + 1$ ; then  $r$ -subgroups are abelian and any two elements of order  $s$  commute. Let  $G$  be a finitely generated group in  $\mathfrak{B}$ , and let  $N = gp(g^{2r} | g \in G)$ ; then  $N$  is an abelian group of exponent dividing  $s$  and  $G/N \in \mathfrak{U} = \text{var} (x^{2r}, [x^2, y^2]^2)$ . Hence it is sufficient to prove that finitely generated groups in  $\mathfrak{U}$  are finite and soluble. We do this by a sequence of lemmas akin to (but much simpler than) those used in the proof of the Burnside problem for exponent 6 (M. Hall [9]).

8.2.3. LEMMA. *If  $G \in \mathfrak{U}$  and*

$$G = gp(a, x, y | a^2 = x^r = y^r = 1, x^a = x^{-1}, y^a = y^{-1})$$

*then  $[x, y] = 1$ .*

PROOF. Since  $G$  has exponent dividing  $2r$

$$(axy)^{2r} = 1,$$

i.e.  $(axyaxy)^r = 1,$

i.e.  $(x^{-1}y^{-1}xy)^r = 1.$

But  $[x, y]^2 = 1;$

thus  $[x, y] = 1.$

8.2.4. LEMMA. *Let  $H \in \mathfrak{U}$  and  $H = gp(a, b, c | a^2 = b^2 = c^2 = 1)$ , then  $\gamma_2 H$  is abelian (and of exponent dividing  $r$ ).*

PROOF. The following table shows that  $\gamma_2 H$  is generated by  $\alpha_1, \dots, \alpha_5$ .

	$a\alpha_i a$	$b\alpha_i b$	$c\alpha_i c$
$\alpha_1 = abab$	$\alpha_1^{-1}$	$\alpha_1^{-1}$	$\alpha_2^{-1}\alpha_5^{-1}\alpha_4\alpha_3$
$\alpha_2 = acac$	$\alpha_2^{-1}$	$\alpha_1^{-1}\alpha_4$	$\alpha_2^{-1}$
$\alpha_3 = bcbc$	$\alpha_5$	$\alpha_3^{-1}$	$\alpha_3^{-1}$
$\alpha_4 = abcacb$	$\alpha_4^{-1}$	$\alpha_1^{-1}\alpha_2$	$\alpha_2^{-1}\alpha_5^{-1}\alpha_1\alpha_3$
$\alpha_5 = abebca$	$\alpha_3$	$\alpha_1^{-1}\alpha_5^{-1}\alpha_1$	$\alpha_2^{-1}\alpha_5^{-1}\alpha_2$

All of these, save possibly  $\alpha_4$ , have order dividing  $r$  and, by Lemma 8.2.3,  $[\alpha_1, \alpha_2] = 1, [\alpha_2, \alpha_3] = 1, [\alpha_1, \alpha_3] = 1$ . Thus  $gp(\alpha_1, \alpha_2)$  is abelian of exponent dividing  $r$ , and hence so also is  $b^{-1}gp(\alpha_1, \alpha_2)b = gp(\alpha_1^{-1}, \alpha_1^{-1}\alpha_4)$ . It follows that  $\alpha_4^r = 1$  and also  $[\alpha_1, \alpha_4] = 1, [\alpha_2, \alpha_4] = 1$ .

Now

$$1 = [\alpha_1, \alpha_3]^a = [\alpha_1^{-1}, \alpha_5],$$

$$1 = [\alpha_2, \alpha_3]^b = [\alpha_2^{-1}, \alpha_5],$$

and

$$[\alpha_5, \alpha_4]^b = [\alpha_1^{-1}\alpha_5^{-1}\alpha_1, \alpha_1^{-1}\alpha_2] = 1,$$

$$[\alpha_3, \alpha_4]^a = [\alpha_5, \alpha_4^{-1}] = 1,$$

$$1 = [\alpha_1, \alpha_3]^c = [\alpha_2^{-1}\alpha_5^{-1}\alpha_4, \alpha_3^{-1}] = [\alpha_5^{-1}, \alpha_3^{-1}].$$

Thus  $\gamma_2 H$  is abelian of exponent dividing  $r$ .

8.2.5. LEMMA. *If  $H \in \mathfrak{U}$  and  $H = gp(a, b, c, d | a^2 = b^2 = c^2 = d^2 = 1)$  then  $[(ab)^2, (cd)^2] = 1$ .*

PROOF. Let  $\alpha = abab, \beta_1 = cdcd, \beta_2 = acdca$ ; then, since  $\beta_1$  and  $\beta_2$  belong to the derived group of  $gp(a, c, d)$  by the previous lemma we have  $\beta_1^r = \beta_2^r = [\beta_1, \beta_2] = 1$ . Also  $\alpha^a = \alpha^{-1}(\beta_1\beta_2^{-1})^a = \beta_2\beta_1^{-1} = (\beta_1\beta_2^{-1})^{-1}$  and so  $gp(\alpha, \beta_1\beta_2^{-1})$  is abelian of exponent dividing  $r$ . Hence  $(\alpha\beta_1^i\beta_2^{-i})^r = 1$  and so  $(\beta_2^{-i}\alpha\beta_1^i)^r = 1$ . Also  $(\beta_2^{-i}\alpha\beta_1^i)^a = (\beta_2^{-i}\alpha\beta_1^i)^{-1}$  and so  $K = gp(\alpha, \beta_1\beta_2^{-1}, \beta_2^{-i}\alpha\beta_1^i, (i = 1, \dots, r-1))$  is abelian of exponent dividing  $r$ . But it is clearly a normal subgroup of  $L = gp(\alpha, \beta_1, \beta_2)$  and  $L/K$  is generated by  $K\beta_1$  and so is cyclic of order dividing  $r$ . Thus  $L$  has exponent dividing  $r$  and so, using the law  $[x^2, y^2]^2 = 1$ ,  $L$  is abelian; in particular  $[(ab)^2, (cd)^2] = 1$ .

8.2.6. THEOREM. *Let  $G$  be a finitely generated group in  $\mathfrak{U}$ . Then  $G$  is finite and soluble.*

PROOF. If  $M = gp(g^r | g \in G)$ , then  $G/M$  has exponent  $r$ , so  $G$  is abelian and thus finite. Hence  $M$  is finitely generated, and so, since it is generated by elements of order 2, is generated by finitely many such elements. Thus  $M/\gamma_2 M$  is finite, and  $\gamma_2 M$  is generated by finitely many elements of the form  $abab$  where  $a^2 = b^2 = 1$

(since it is generated by the commutators in the generators of  $M$  and their conjugates). From the previous lemma any two such elements commute and so  $\gamma_2 M$  is finite and abelian. It follows that  $G$  is finite and soluble.

## 9. Conclusion

The arguments in §§ 6.1–6.3 can be extended (along the lines of § 5.5) to larger  $PSL(2, q)$ , but the calculations involved in actually finding the laws will rapidly become impossibly lengthy unless a computer is employed or the results of § 5 can be extended to give all types of laws needed.

As the reader has undoubtedly observed, apart from  $u_n$ , the laws given in Theorem 3.4 involve at most two variables, whereas  $u_n$  itself involves  $\frac{1}{2}n(n+1)$ , so is anomalous. In fact, using § 3.3 of Oates and Powell [19] and Theorem 3.7 we can prove that the laws of  $PSL(2, 7)$  (and  $PSL(2, 8)$ ) possess a basis involving at most 5 variables. In these cases, too, it should be possible to avoid all uses of  $u_n$  (as was done for  $PSL(2, 5)$  in [3]) except in proving local finiteness, and this is the stumbling block. What we need is a two-variable replacement for  $u_n$ .

*Conjecture:* For each  $n$  there is a two-variable law which holds in every group of order not greater than  $n$  and which implies that a simple group satisfying it has order not greater than  $f(n)$ .

## 10. Appendix I: The proof of Lemma 4.1.8

Let  $G$  be a non-trivial subgroup of  $S_3 \times S_3$ , such that  $G$  contains no non-trivial normal 2-subgroups, and let  $M$  be a faithful indecomposable quotient of the regular representation module of  $G$  over  $GF(2)$ . Then we have to show that  $M$  is irreducible.

We will use the notation of Curtis and Reiner [5] and will assume familiarity with Chapters 4, 5, 6 of this book. In particular, § 43, and Theorem 61.16 will be used extensively.

Also, from Theorems 56.6 and 58.14 of [5], we obtain immediately:

10.1 LEMMA. *Let  $G$  be a finite group,  $K$  a field,  $P$  a principal indecomposable component of  $KG$ . If  $P$  is also irreducible, then any  $KG$ -module  $M$  which has a composition factor isomorphic to  $P$  has the form  $M = M_1 \oplus M_2$ , with  $M_2 \cong P$ .*

The following lemma is an easy consequence of the definition of blocks ([5] definition 55.1), and their elementary properties (Theorem 55.2).

10.2 LEMMA. *Let  $G$  be a finite group, and  $K$  a field. If  $M$  is a submodule of  $KG$ , then  $KG/M \cong B_1 M/M \oplus \cdots \oplus B_r M/M$ , when  $B_1, \dots, B_r$  are the blocks of  $KG$ .*

We start the proof by observing that if  $G$  is a 3-group, the result follows from Maschke's theorem. Thus we may suppose that  $G$  is not a 3-group. Note that the

Sylow 3-subgroup  $N$  of  $G$  is normal. By regarding  $N$  as a  $GF(3)(G/N)$ -module, for example, it is easy to see that  $G$  is isomorphic to one of the following four groups.

- (1)  $S_3$ ,
- (2)  $S_3 \times C_3$ ,
- (3)  $gp(a, b, c | a^3 = b^3 = [a, b] = c^2 = 1, a^c = a^{-1}, b^c = b^{-1})$ ,
- (4)  $S_3 \times S_3$ .

We deal with each of these groups separately.

(1) Note that  $S_3 \cong SL(2, 2) = GL(2, 2)$ . Hence  $S_3$  has a faithful irreducible representation over  $GF(2)$ , of degree 2. Let  $P$  be a principal indecomposable component of  $GF(2)S_3$ , let  $N$  be its radical, and suppose  $P/N$  is a faithful irreducible  $GF(2)S_3$ -module. Then  $GF(2)S_3$  acts on  $P/N$  as the algebra of all linear transformations of  $P/N$ : but then the only linear transformations which commute with every element of  $GF(2)S_3$  are those which correspond to multiplication by an element of  $GF(2)$ . That is,  $\text{Hom}_{GF(2)S_3}(P/N, P/N) = K \cong GF(2)$ , and  $(K : GF(2)) = 1$ . Now suppose  $N \neq 0$ . Then, by [5] Theorem 65.16,  $(P : GF(2)) \geq 4$ , and so [5] Theorem 61.16 gives us that  $P/N$  occurs at least 4 times as composition factor of  $GF(2)S_3$ , which it clearly cannot. Hence  $N = 0$ . Also [5] Theorem 61.16 gives that there are two principal indecomposable components of  $GF(2)S_3$  isomorphic to  $P$ . It follows that there is just one other principal indecomposable component of  $GF(2)S_3$ , and that this one is isomorphic to  $GF(2)(S_3/A_3)$ .

Now, suppose  $M$  is a faithful indecomposable quotient of  $GF(2)S_3$ . Then  $M$  contains a composition factor isomorphic to  $P$ , and from Lemma 10.1 we conclude  $M$  is irreducible.

(2) Put  $E = GF(2)(S_3 \times C_3)$ ,  $E_1 = GF(2)S_3$ ,  $E_2 = GF(2)C_3$ . It is convenient at this stage to identify  $E$  and  $E_1 \otimes_{GF(2)} E_2$ . Then  $E$  (qua  $E$ -module) is isomorphic to the outer tensor product of  $E_1$  and  $E_2$  (qua  $E$ -module). Let  $E_1 = P_1 \oplus P_2 \oplus P_3$  be the decomposition of  $E_1$  into principal indecomposables, with  $P_2, P_3$  irreducible, and let  $E_2 = T_1 \oplus T_2$  be the decomposition of  $E_2$  into principal indecomposables, with  $T_2$  non-trivial. From Lemma 4.1.5, we have that  $S_3 \times C_3$  has a faithful irreducible representation over  $GF(2)$ . Clearly, such a representation must have degree at least 4.

From this information, we may conclude that  $E$  has the following principal indecomposable components:  $R_{ij} \cong P_i \# T_j$ , with  $i \in \{2, 3\}, j \in \{1, 2\}$ , all of which are irreducible, and  $R_{11} \cong P_1 \# T_1$ . Using Theorem 61.16 of [5], we see that  $R_{12} \cong P_1 \# T_2$  is also a principal indecomposable, and so we have accounted for all the principal indecomposable components of  $E$ .

Now, suppose that  $M$  is a faithful indecomposable quotient of  $E$ . If  $M$  contains a composition factor isomorphic to  $R_{ij}$  for some  $i \in \{2, 3\}, j \in \{1, 2\}$ , then we may conclude from Lemma 10.1 that  $M \cong R_{ij}$ , and so is irreducible. If  $M$  contains no such composition factor, then  $\gamma_2 S_3$  acts trivially on every composition factor, and so  $M$  is not faithful.

(3) Put  $G = gp(a, b, c)$ , and let  $E = GF(2)G$ . It follows from Lemma 4.1.5 that  $G$  does not have any faithful irreducible representations over  $GF(2)$ .

If  $N \triangleleft G$  such that  $G/N \cong S_3$ , the techniques of (1) give us that there are two principal indecomposable components of  $E$  which are irreducible of degree 2, and which have kernel precisely  $N$ .

Now  $gp(a)$ ,  $gp(b)$ ,  $gp(ab)$ ,  $gp(ab^2)$  are distinct normal subgroups of  $G$  satisfying the conditions of the previous paragraph, and so each gives rise to two irreducible principal indecomposable components of degree 2. We have one more principal indecomposable component to account for, and this is clearly isomorphic to the regular  $GF(2)(G/\gamma_2 G)$ -module.

Thus any faithful indecomposable module  $M$  will contain a non-trivial composition factor, and from Lemma 10.1, we get that  $M$  is irreducible.

(4) Put  $E = GF(2)(S_3 \times S_3)$ , and let  $E_1 \cong E_2 \cong GF(2)S_3$ . As in (2) we identify  $E$  and  $E_1 \otimes_{GF(2)} E_2$ . Let  $E_1 = P_1 \oplus P_2 \oplus P_3$ ,  $E_2 = T_1 \oplus T_2 \oplus T_3$  be the decompositions of  $E_1$  and  $E_2$  into principal indecomposable components, with  $P_2 \cong P_3$  and  $T_2 \cong T_3$  all irreducible. Again from Lemma 4.1.5, we have that  $S_3 \times S_3$  has a faithful irreducible representation over  $GF(2)$ , and such a representation must clearly have degree at least 4.

This information, together with Theorem 61.16, allows us to conclude that  $R_{ij} \cong P_i \not\cong T_j$ ,  $i, j \in \{1, 2, 3\}$  are all the principal indecomposable components of  $E$ . The blocks of  $E$  are  $R_{11}$ ,  $R_{21} \oplus R_{31}$ ,  $R_{12} \oplus R_{13}$ ,  $R_{22} \oplus R_{23} \oplus R_{32} \oplus R_{33}$ .

If  $M$  is a faithful indecomposable quotient of  $E$ , by Lemma 10.2,  $M$  is isomorphic to a quotient of some block. It follows that either  $M$  is irreducible, or  $M$  is not faithful.

11. Appendix II

TABLE 1  
Traces of elements in  $PSL(2, 7)$

$x$	$y$	$xy$	$xy^{-1}$	$[x, y]$	$x$	$y$	$xy$	$xy^{-1}$	$[x, y]$	
0	0	0	0	$\pm 2$	$\pm 1$	$\pm 3$	0	$\pm 3$	$\pm 1$	
		$\pm 1$	$\pm 1$	$\pm 1$			$\pm 1$	$\pm 2$	$\pm 1$	
		$\pm 2$	$\pm 2$	$\pm 2$			$\pm 3$	$\pm 3$	$\pm 2$	
		$\pm 3$	$\pm 3$	0			$\pm 2$	$\pm 1$	$\pm 1$	
	$\pm 1$	0	0	0	$\pm 1$	$\pm 2$	$\pm 2$	$\pm 3$	0	$\pm 1$
			$\pm 1$	$\pm 1$	0			$\pm 3$	$\pm 1$	$\pm 2$
			$\pm 2$	$\pm 2$	$\pm 3$			0	$\pm 3$	$\pm 1$
			$\pm 3$	$\pm 3$	$\pm 1$			$\pm 1$	$\pm 2$	$\pm 3$
	$\pm 2$	0	0	0	$\pm 2$	$\pm 3$	$\pm 3$	0	$\pm 3$	$\pm 1$
			$\pm 1$	$\pm 1$	$\pm 3$			$\pm 1$	$\pm 2$	$\pm 3$
			$\pm 2$	$\pm 2$	$\pm 1$			$\pm 2$	$\pm 2$	$\pm 2$
			$\pm 3$	$\pm 3$	$\pm 3$			$\pm 3$	$\pm 1$	$\pm 3$
$\pm 3$	0	0	0	0	$\pm 2$	$\pm 3$	0	$\pm 1$	$\pm 3$	
		$\pm 1$	$\pm 1$	$\pm 1$			$\pm 1$	$\pm 2$	$\pm 1$	
		$\pm 2$	$\pm 2$	$\pm 3$			$\pm 1$	0	$\pm 3$	
		$\pm 3$	$\pm 3$	$\pm 2$			$\pm 2$	$\pm 3$	$\pm 3$	
$\pm 1$	$\pm 1$	0	$\pm 1$	0	$\pm 3$	$\pm 3$	0	$\pm 2$	$\pm 2$	
		$\pm 1$	0	0			$\pm 1$	$\pm 1$	$\pm 1$	
		$\pm 2$	$\pm 2$	$\pm 2$			$\pm 3$	$\pm 3$	$\pm 2$	
		$\pm 3$	$\pm 1$	$\pm 2$			0	$\pm 2$	$\pm 2$	
	$\pm 2$	$\pm 1$	0	$\pm 2$	$\pm 3$	$\pm 3$	$\pm 3$	0	$\pm 2$	$\pm 2$
			$\pm 1$	$\pm 1$	$\pm 2$			$\pm 1$	$\pm 1$	$\pm 1$
			$\pm 3$	$\pm 3$	$\pm 1$			$\pm 1$	$\pm 3$	$\pm 2$
			$\pm 2$	0	$\pm 3$			$\pm 2$	0	$\pm 2$
	$\pm 3$	$\pm 1$	0	$\pm 3$	$\pm 3$	$\pm 3$	$\pm 3$	0	$\pm 2$	$\pm 2$
			$\pm 1$	$\pm 1$	$\pm 2$			$\pm 1$	$\pm 1$	$\pm 3$
			$\pm 2$	$\pm 3$	$\pm 3$			$\pm 3$	$\pm 3$	$\pm 3$
			$\pm 3$	$\pm 1$	$\pm 1$			$\pm 2$	$\pm 2$	$\pm 3$

TABLE 2  
Typical pairs of elements in  $PSL(2, 7)$

$x$	$y$	$x$	$y$	$x$	$y$
(12)(36)	(36)(57)	(236)(475)	(137)(456)	(1546732)	(1234567)
(35)(67)	(13)(26)	(236)(475)	(173)(465)	(1365274)	(1234567)
(12)(36)	(12)(36)	(236)(475)	(142)(367)	(1753426)	(1234567)
(35)(67)	(24)(37)	(236)(475)	(124)(376)	(1234567)	(1234567)
		(267)(345)	(126)(475)	(1365274)	(1765432)
(12)(36)	(124)(365)			(1753426)	(1765432)
(13)(45)	(124)(365)	(172)(367)	(1234567)	(1546732)	(1765432)
(12)(36)	(137)(254)	(137)(254)	(1234567)		
(36)(57)	(123)(457)	(236)(475)	(1234567)	(1234567)	(12)(3765)
		(172)(364)	(1765432)	(1234567)	(24)(3576)
(12)(36)	(1)	(164)(253)	(1765432)	(1234567)	(12)(3567)
(37)(56)	(1234567)	(236)(475)	(1765432)	(1234567)	(14)(3756)
(36)(57)	(1234567)	(164)(253)	(1234567)	(1234567)	(24)(3675)
(35)(67)	(1234567)			(1)	(12)(3765)
		(236)(475)	(24)(3576)	(1234567)	(14)(3657)
(36)(57)	(24)(3576)	(236)(475)	(1345)(67)		
(35)(67)	(2645)(37)	(236)(475)	(14)(3756)	(24)(3576)	(24)(3576)
(35)(67)	(1263)(47)	(236)(475)	(1543)(67)	(24)(3576)	(2645)(37)
(37)(56)	(24)(3576)	(236)(475)	(12)(3567)	(24)(3576)	(1543)(67)
		(236)(475)	(24)(3675)	(24)(3576)	(24)(3675)
(236)(475)	(267)(345)	(236)(475)	(14)(3657)	(2645)(37)	(1345)(67)
(236)(475)	(276)(354)			(24)(3576)	(1345)(67)
				(2645)(37)	(1543)(67)

## References

- [1] W. Burnside, *Theory of Groups* (2nd edition, 1911, Dover, New York, 1955).
- [2] John Cossey, *On varieties of  $A$ -groups* (Ph. D. dissertation, Australian National University, 1966).
- [3] John Cossey and Sheila Oates Macdonald, 'A basis for the laws of  $PSL(2, 5)$ ', *Bull. Amer. Math. Soc.* 74 (1968), 602–606.
- [4] John Cossey, Sheila Oates Macdonald and Anne Penfold Street, 'On the laws of certain linear groups', *Bull. Amer. Math. Soc.* 75 (1969), 361–363.
- [5] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras* (Interscience, New York, 1962).
- [6] L. E. Dickson, *Linear groups*, (1900, Dover, New York 1958).
- [7] W. Gaschütz, 'Zur Erweiterungstheorie der Endlichen Gruppen', *J. reine angew. Math.* 190 (1952), 93–107.
- [8] D. Gorenstein, *Finite groups* (Harper and Row, New York, 1968).
- [9] M. Hall, 'Solution of the Burnside problem for exponent 6', *Illinois J. of Math.* 2 (1958) 764–786.
- [10] M. Hall, *The theory of groups* (Macmillan, New York, 1959).
- [11] P. Hall and G. Higman, 'On the  $p$ -length of  $p$ -soluble groups and reduction theorems for Burnside's problem', *Proc. London Math. Soc.* (3) 6 (1956), 1–43.
- [12] G. Higman, 'Complementation of abelian normal subgroups', *Publ. Math. Debrecen*, 4 (1956), 455–458.
- [13] B. Huppert, *Endliche Gruppen I* (Die Grundlehrender mathematischen Wissenschaften, Bd. 134. Springer-Verlag, Berlin, 1967).



- [14] R. Köchendorffer, 'Über treue irreduzible Darstellungen endlicher Gruppen', *Math. Nachr.* (1948), 25–39.
- [15] L. G. Kovács and M. F. Newman, 'Cross varieties of groups', *Proc. Roy. Soc. (London)* A, 292 (1966), 530–536.
- [16] L. G. Kovács and M. F. Newman, 'On critical groups', *J. Austral. Math. Soc.* 6 (1966), 237–250.
- [17] Hanna Neumann, *Varieties of groups* (Ergebnisse der Mathematik und ihrer Grenzgebiete, Bd. 37, Springer-Verlag, Berlin, 1967).
- [18] Sheila Oates, 'Identical relations in groups', *J. London Math. Soc.* 38 (1963) 71–78.
- [19] Sheila Oates and M. B. Powell, 'Identical relations in finite groups', *J. Algebra* 1 (1964), 11–39.
- [20] I. Schur, 'Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen', *J. reine angew. Math.* 132 (1907), 85–137.
- [21] D. R. Taunt, 'On  $A$ -groups', *Proc. Cambridge Phil. Soc.* 45 (1949), 24–42.
- [22] J. H. Walter, 'The characterisation of finite groups with abelian Sylow 2-subgroups', (to appear).
- [23] P. M. Weichsel, 'A decomposition theory for finite groups with applications to  $p$ -groups', *Trans. Amer. Math. Soc.* 102 (1962), 218–226.
- [24] P. M. Weichsel, 'On critical  $p$ -groups', *Proc. London Math. Soc.* (3) 14 (1964), 83–100.

Department of Pure Mathematics  
School of General Studies  
Australian National University  
Canberra

Department of Mathematics  
University of Queensland  
Brisbane

Department of Mathematics  
University of Queensland  
Brisbane