A NOTE ON THE SPECIAL LINEAR HOMOGENEOUS GROUP $SLH(2, p^n)$

F. A. LEWIS

1. **Introduction.** The following theorem is due to E. H. Moore.

The special linear homogeneous group $SLH(2, p^n)$ of binary linear substitutions of determinant unity in the $GF[p^n]$ is simply isomorphic with the abstract group L generated by the operators T and S_λ, where λ runs through the series of p^n marks of the field, subject to the generational relations

(a) $S_0 = I$, $S_\lambda S_\mu = S_{\lambda+\mu}$ (λ, μ *any marks*),

(b) $T^4 = I$, $S_\lambda T^2 = T^2 S_\lambda$,

(c) $S_\lambda T S_\mu T S_{(1-\lambda)/(1-\lambda\mu)} T S_{1-\lambda\mu} T S_{(1-\mu)/(1-\lambda\mu)} T = I$ (λ, μ *any marks*, $\lambda\mu \neq 1$).

For $\lambda = 1$, $\mu \neq 1$, (c) gives

(d) $(S_1 T^3)^3 = I$.

Other relations employed by Dickson[1] in a proof of this theorem are

(e) $TS_\alpha TS_{2\alpha^{-1}} TS_\alpha TS_{2\alpha^{-1}} T^2 = I$ ($\alpha \neq 0$),

(f) $TS_\alpha TS_{\alpha^{-1}} TS_\rho = S_{\alpha^{-2}\rho} TS_\alpha TS_{\alpha^{-1}} T$ (ρ any mark).

It is the purpose of this paper to prove that (a), (b), (d), and (e) define an abstract group simply isomorphic with $SLH(2, p^n)$ when $p > 2$. If $p = 2$, relation (e) reduces to an identity and must be replaced by (f).

2. **Preliminary relations.** We first prove that (f) is a consequence of (a), (b), (d), and (e) when $p > 2$, so that in what follows we may use (f) for any p. We write (e) in the form

(e′) $TS_\alpha T = S_{-2\alpha^{-1}} TS_{-\alpha} TS_{-2\alpha^{-1}} T^2$

and make an even number of applications of this formula to the right member of (f) as follows:

$$S_{\alpha^{-2}\rho} \cdot TS_\alpha T \cdot S_{\alpha^{-1}} T = S_{\alpha^{-2}\rho - 2\alpha^{-1}} TS_{-\alpha} \cdot TS_{-\alpha^{-1}} T \cdot T^2$$
$$= S_{\alpha^{-2}\rho - 2\alpha^{-1}} \cdot TS_\alpha T \cdot S_{\alpha^{-1}} TS_{2\alpha} = S_{\alpha^{-2}\rho - 4\alpha^{-1}} TS_{-\alpha} \cdot TS_{-\alpha^{-1}} T \cdot S_{2\alpha} T^2$$
$$= S_{\alpha^{-2}\rho - 4\alpha^{-1}} \cdot TS_\alpha T \cdot S_{\alpha^{-1}} TS_{4\alpha} = S_{\alpha^{-2}\rho - 6\alpha^{-1}} TS_{-\alpha} \cdot TS_{-\alpha^{-1}} T \cdot S_{4\alpha} T^2$$
$$= S_{\alpha^{-2}\rho - 6\alpha^{-1}} \cdot TS_\alpha T \cdot S_{\alpha^{-1}} TS_{6\alpha} = \cdots = S_{\alpha^{-2}\rho - 2m\alpha^{-1}} \cdot TS_\alpha T \cdot S_{\alpha^{-1}} TS_{2m\alpha}.$$

Relation (f) is established by taking $m = \rho/2\alpha$. It will be convenient to write (f) in the equivalent form

(f′) $S_\rho TS_\alpha TS_{\alpha^{-1}} T = TS_\alpha TS_{\alpha^{-1}} TS_{\rho\alpha^2}$.

[1] *Linear Groups*, Leipzig, 1901. The notation is that employed by Dickson.

Now let e be a primitive root of the field and define

$$R = T^3 S_e T^3 S_{e^{-1}} T^3 S_e. \tag{1}$$

Since

$$R^k = T^3 S_{e^k} T^3 S_{e^{-k}} T^3 S_{e^k} \tag{2}$$

is true by definition when $k=1$, by induction (2) holds for any k if

$$T^3 S_{e^k} T^3 S_{e^{-k}} T^3 S_{e^k} T^3 S_e T^3 S_{e^{-1}} T^3 S_e = T^3 S_{e^{k+1}} T^3 S_{e^{-k-1}} T^3 S_{e^{k+1}}$$

or

$$T^3 S_{e^k} T^3 S_{e^{-k}} T^3 S_{e^k} T^3 S_e T^3 S_{e^{-1}} T^3 S_e S_{-e^{k+1}} T S_{-e^{-k-1}} T S_{-e^{k+1}} T = I.$$

Upon making obvious reductions this last relation becomes

$$S_{e^k - e^{k+1}} T S_{e^{-k}} T S_{e^k} \cdot T S_e T S_{e^{-1}} T \cdot S_{e - e^{k+1}} T S_{-e^{-k-1}} T = T^2.$$

If we apply (f) as indicated, this becomes

$$S_{e^k - e^{k+1}} T S_{e^{-k}} T S_{e^k - e^{k-1} + e^{-1}} T S_e T S_{e^{-1} - e^{-k-1}} T = I,$$

which may be written

$$S_{e^k - e^{k-1} + e^{-1}} T S_e T S_{e^{-1} - e^{-k-1}} T S_{e^k - e^{k+1}} T S_{e^{-k}} T = I. \tag{3.1}$$

We next apply (f′) repeatedly as illustrated in the following sample computation.

$$S_{e^k - e^{k-1} + e^{-1}} \cdot T S_e T S_{e^{-1}} T \cdot T^3 S_{-e^{-k-1}} T S_{e^k - e^{k+1}} T S_{e^{-k}} T = I,$$

$$T S_e T S_{e^{-1}} T S_{e^{k+2} - e^{k+1} + e} T S_{-e^{-k-1}} T S_{e^k - e^{k+1}} T S_{e^{-k}} T^3 = I,$$

$$S_{e + e^{-k}} T S_{e^{-1}} T S_{e^{k+2} - e^{k+1} + e} T S_{-e^{-k-1}} T S_{e^k - e^{k+1}} T = I, \tag{3.2}$$

$$S_{e^k - e^{k+1} + e^{-1}} T S_e T S_{e^{-1} + e^{-k-2}} T S_{e^{k+2} - e^{k+1}} T S_{-e^{-k-1}} T = I, \tag{3.3}$$

$$S_{e - e^{-k-1}} T S_{e^{-1}} T S_{e^{k+2} - e^{k+3} + e} T S_{e^{-k-2}} T S_{e^{k+2} - e^{k+1}} T = I, \tag{3.4}$$

$$S_{e^{k+2} - e^{k+1} + e^{-1}} T S_e T S_{e^{-1} - e^{-k-3}} T S_{e^{k+2} - e^{k+3}} T S_{e^{-k-2}} T = I, \tag{3.5}$$

$$S_{e + e^{-k-2}} T S_{e^{-1}} T S_{e^{k+4} - e^{k+3} + e} T S_{-e^{-k-3}} T S_{e^{k+2} - e^{k+3}} T = I, \tag{3.6}$$

$$S_{e^{k+2} - e^{k+3} + e^{-1}} T S_e T S_{e^{-1} + e^{-k-4}} T S_{e^{k+4} - e^{k+3}} T S_{-e^{-k-3}} T = I, \tag{3.7}$$

$$S_{e - e^{-k-3}} T S_{e^{-1}} T S_{e^{k+4} - e^{k+5} + e} T S_{e^{-k-4}} T S_{e^{k+4} - e^{k+3}} T = I. \tag{3.8}$$

These relations illustrate the four types that arise if the process is repeated indefinitely. It is evident that $S_{e^{p^n-1}} = S_1$ must appear. Suppose, for example, that $S_{e^{p^n-1}}$ appears in the following generalization of (3.4), say $(3.2 \cdot u)$, where u is even. That is, we assume $u = p^n - k - 1$ in

$$S_{e - e^{1-k-u}} T S_{e^{-1}} T S_{e^{k+u} - e^{k+u+1} + e} T S_{e^{-k-u}} T S_{e^{k+u} - e^{k+u-1}} T = I \tag{3.2·u}$$

and easily reduce the left member to $S_0TS_{e^{-1}}(TS_1)^3S_{-e^{-1}}T=I$ by means of (b) and (d).

3. **Proof of theorem.** Relations (a), (b), (d), and (f) are satisfied by

$$t = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad s_\lambda = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

which generate[2] $SLH(2, p^n)$. The corresponding form of R is

$$r = \begin{pmatrix} e^{-1} & 0 \\ 0 & e \end{pmatrix}$$

of period p^n-1. The order l of L is not less than the order of $SLH(2, p^n)$. That is, $l \geqq p^n(p^{2n}-1)$. Now

$$R^{-1}S_\lambda R = S_{-e}TS_{-e^{-1}}TS_{-e}TS_\lambda TS_eTS_{e^{-1}}T^3S_e = S_{\lambda e^2}$$

by (b) and (f'). Further, $R^{p^n-1}=I$ by (2) and (d). We conclude that $K=\{R, S_\lambda\}$ is of order $p^n(p^n-1)$ and all of its elements may be represented in either of the forms R^aS_b, S_cR^d. Now consider the p^n+1 sets of $p^n(p^n-1)$ elements represented by K, KTS_λ (λ arbitrary). There are at most $p^n(p^{2n}-1)$ distinct elements. It is evident that the sets are permuted among themselves on multiplication on the right by S_ρ. If $\lambda \neq 0$,

$$KTS_\lambda T = K(S_{-\lambda}TS_{-\lambda^{-1}}TS_{-\lambda}T)TS_\lambda T$$

by (2). Making obvious simplifications we obtain $KTS_\lambda T=KTS_{-\lambda^{-1}}$. Now $KTS_0T=KT^2=K$, since $T^2=(T^3S_{-1})^3$. Also $KT=KTS_0$. Hence the sets are also permuted among themselves on multiplication on the right by T. It follows that all the elements of L are in the sets and $l \leqq p^n(p^{2n}-1)$. Hence L and $SLH(2, p^n)$ are of equal orders and simply isomorphic.

THEOREM 1. *The special linear homogeneous group $SLH(2, p^n)$, $p>2$, of binary linear substitutions of determinant unity in the $GF[p^n]$ is simply isomorphic with the abstract group generated by the operators T and S_λ, where λ runs through the series of p^n marks of the field, subject to the generation relations*

(a)[3] $S_\lambda S_\mu=S_{\lambda+\mu}$ (λ, μ *any marks*),

(b) $T^4=I$, $S_\lambda T^2=T^2S_\lambda$,

(d) $(S_1T^3)^3=I$,

(e) $TS_\alpha TS_{2\alpha^{-1}}TS_\alpha TS_{2\alpha^{-1}}T^2=I$ (α *any mark* $\neq 0$).

[2] Dickson, loc. cit., p. 80.

[3] A referee has pointed out that $S_0=I$ follows from $S_\lambda S_\mu=S_{\lambda+\mu}$.

THEOREM 2. *The special linear homogeneous group $SLH(2, 2^n)$ of binary linear substitutions of determinant unity in the $GF[2^n]$ is simply isomorphic with the abstract group generated by the operators T and S_λ, where λ runs through the series of 2^n marks of the field subject to the generational relations*

(a) $S_\lambda S_\mu = S_{\lambda+\mu}$ (λ, μ *any marks*),

(b) $T^4 = I$, $S_\lambda T^2 = T^2 S_\lambda$,

(d) $(S_1 T^3)^3 = I$,

(f) $TS_\alpha TS_{\alpha^{-1}} TS_\rho = S_{\alpha^{-2}\rho} TS_\alpha TS_{\alpha^{-1}} T$ (ρ *arbitrary*; $\alpha \neq 0$).

COROLLARY 1.[4] *The linear fractional group $LF(2, p^n)$, $p > 2$, of linear fractional transformations in the $GF[p^n]$ is simply isomorphic with the abstract group generated by the operators T and S_λ, where λ runs through the series of p^n marks of the field, subject to the generational relations*

(a) $S_\lambda S_\mu = S_{\lambda+\mu}$ (λ, μ *any marks*),

(b′) $T^2 = I$,

(d′) $(S_1 T)^3 = I$,

(e′) $(S_\alpha T S_{2/\alpha} T)^2 = I$ (α *any mark* $\neq 0$).

COROLLARY 2. *The linear fractional group $LF(2, 2^n)$ of linear fractional transformations in the $GF[2^n]$ is simply isomorphic with the abstract group generated by the operators T and S_λ, where λ runs through the series of p^n marks of the field, subject to the generational relations*

(a) $S_\lambda S_\mu = S_{\lambda+\mu}$ (λ, μ *any marks*),

(b′) $T^2 = I$,

(d′) $(S_1 T)^3 = I$,

(f) $TS_\alpha TS_{\alpha^{-1}} TS_\rho = S_{\alpha^{-2}\rho} TS_\alpha TS_{\alpha^{-1}} T$ (ρ *arbitrary*; $\alpha \neq 0$).

COROLLARY 3.[5] *The abstract group $G_{p(p^2-1)/2}$, simply isomorphic with the group $LF(2, p)$, $p > 2$, may be generated by two operators T and S subject to the generational relations*

$$S^p = T^2 = (ST)^3 = (S^\tau T S^{2/\tau})^2 = I, \qquad \tau \neq 0.$$

UNIVERSITY OF ALABAMA

---

[4] Special cases of this corollary have been proved by Dickson and Bussey. See the latter's dissertation, Proceedings of the London Mathematical Society, (2), vol. 3 (1905), pp. 296–315.

[5] Due to W. H. Bussey, loc. cit., p. 303.