THE UNIVERSITY OF CHICAGO.
FOUNDED BY JOHN D. ROCKEFELLER.

Generational Relations for the Abstract Group simply Isomorphic with the Group $LF[2, p^n]$.

A DISSERTATION
SUBMITTED TO THE FACULTY
OF THE
OGDEN GRADUATE SCHOOL OF SCIENCE
IN CANDIDACY FOR THE DEGREE
DOCTOR OF PHILOSOPHY
(DEPARTMENT OF MATHEMATICS).

BY
WILLIAM HENRY BUSSEY.

1904.

AUTOBIOGRAPHY.

I WAS born in Chicago on the twenty-fourth day of October, 1879 After completing the course in the primary and secondary schools of the City of Chicago, I entered the College of Liberal Arts of Northwestern University in September, 1896. I was graduated in June, 1900, receiving the degree Bachelor of Arts. The next two years I spent in graduate work in Mathematics and Physics at Harvard University, and received the degree Master of Arts in June, 1902. I continued my work for two years in the Graduate School of the University of Chicago as a Fellow in Mathematics.

I wish to acknowledge my indebtedness to all of the instructors under whose direction I have worked as a graduate student, and to express my appreciation of the kindly interest manifested by Professor Dickson, under whose direction this investigation has been carried out.

WILLIAM HENRY BUSSEY.

GENERATIONAL RELATIONS FOR THE ABSTRACT GROUP SIMPLY ISOMORPHIC WITH THE GROUP $LF[2, p^n]$

By W. H. Bussey.

Communicated by Prof. L. E. Dickson.

[Received December 10th, 1904.—Read January 12th, 1905.]

[*Extracted from the Proceedings of the London Mathematical Society, Ser. 2, Vol. 3, Part 4.*]

Introduction.

1. The object of this paper is the proof of the following six theorems concerning sets of generational relations for the abstract group G, simply isomorphic with the group $LF[2, p^n]$ of all linear fractional transformations, on one variable, having determinant unity and coefficients belonging to the $GF(p^n)$.

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

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

Theorem II.—*The abstract group $G_{\frac{1}{2}p^n(p^{2n}-1)}$, simply isomorphic with the group $LF[2, p^n]$, $p > 2$, $n > 1$, may be generated by (p^n+1) operators T and S_λ, λ running through the marks of the $GF(p^n)$, subject to the generational relations*

$$\text{(B)} \quad \begin{cases} (1) & S_0 = I, \quad S_\lambda S_\mu = S_{\lambda+\mu} \quad (\lambda, \mu \text{ any marks}), \\ (2) & T^2 = I, \quad (S_1 T)^3 = I, \\ (3) & (S_\tau T S_{2/\tau} T)^2 = I \quad (\tau \text{ any mark} \neq 0), \\ (4) & [1/a, a^2], \ [1/a, ia^2], \ [i, a], \ [1/i, a] \quad (a \neq 0), \end{cases}$$

where i is a primitive root of the $GF(p^n)$, and a is any mark subject to a restriction implied in the notation $[\lambda, \mu]$.

* For the special cases in which $p^n \leqslant 47$, this theorem has been proved by Prof. Dickson, *Proc. London Math. Soc.*, Vol. xxxv., pp. 292–305; *Bull. Amer. Math. Soc.*, Vol. ix., p. 297.

Note.—The symbol $[\lambda, \mu]$ is used to denote the relation*

$$S_\lambda T S_\mu T S_{(\lambda-1)/(\lambda\mu-1)} T S_{1-\lambda\mu} T S_{(\mu-1)/(\lambda\mu-1)} T = I,$$

where λ, μ are marks such that $\lambda\mu \neq 1$.

THEOREM III.†—*For the special cases in which* $p^n = 49, 81, 121$ *relations* (1), (2), (3) *form a set of generational relations for* $G_{\frac{1}{2}p^n(p^n-1)}$, $p > 2$.

THEOREM IV.‡—*The abstract group* $G_{2^n(2^{2n}-1)}$, *simply isomorphic with the group* $LF[2, 2^n]$, *may be generated by three operators* a, b, c, *subject to the generational relations*

$$\text{(C)} \quad \begin{cases} (5) & a^{2^n-1} = I, \quad b^2 = I, \quad ba^\xi b = a^\eta b a^\zeta, \\ (6) & c^2 = I, \quad (ca)^2 = I, \quad (cb)^3 = I, \end{cases}$$

where $\xi = 1, 2, 3, \ldots, (2^n-2)$, *and* η, ζ *are determined by the relations* $i^\zeta = 1+i^\xi$, $\eta \equiv \xi-\zeta$, *mod* (2^n-1), i *being a primitive root of the* $GF(2^n)$.

THEOREM V.—*The abstract group* $G_{2^n(2^{2n}-1)}$, *simply isomorphic with the group* $LF[2, 2^n]$, *may be generated by two operators* a *and* d *subject to the generational relations*

$$\text{(D)} \qquad a^{2^n-1} = I, \quad d^3 = I, \quad (da^\xi d^{-1} a^\xi)^2 = I, \quad (da^\xi da^\zeta)^e = I,$$

where $\xi = 1, 2, 3, \ldots, (2^n-2)$, *and* ζ *is determined by the relation* $i^\zeta = 1+i^\xi$, i *being a primitive root of the* $GF(2^n)$.

THEOREM VI.§—*In the special cases in which* $n = 2, 3, 4, 5, 6$, *the abstract group* $G_{2^n(2^{2n}-1)}$, *simply isomorphic with the group* $LF[2, 2^n]$,

---

* Relations (1), $T^2 = I$, $[\lambda, \mu]$, λ, μ any marks such that $\lambda\mu \neq 1$, constitute a set of generational relations for G. This is a special case of a more general theorem valid for any field due to Moore. See *Proc. London Math. Soc.*, Vol. XXXV., p. 293, and Dickson's *Linear Groups*, p. 300.

Note that, when $\lambda = 0$ or 1, $[\lambda, \mu]$ reduces to $(S_1 T)^3 = I$, and, when $\lambda = -1$, $[\lambda, \mu]$ reduces to (3).

† For the special cases in which $p^n = 9, 25, 27, 125, 243$, Prof. Dickson has proved that (1), (2), (3) constitute a set of generational relations for $G_{\frac{1}{2}p^n(p^{2n}-1)}$, $p > 2$, *loc. cit.* The proofs for the cases in which $p^n = 125, 243$ have not been published.

‡ This theorem is due to de Seguier, *Journal de Mathématiques*, Tome VIII., p. 253.

§ The set of generational relations (E) is due to Prof. Dickson. He has proved Theorem VI. for $n = 2, 3, 4$. See *Proc. London Math. Soc.*, Vol. XXXV., p. 306 and p. 443; *Bull. Amer. Math. Soc.*, Vol. IX., pp. 194–204.

For $n = 2$, the set (E) reduces to $A^5 = I$, $B^2 = I$, $(AB)^3 = I$.

may be generated by two operators A and B subject to the generational relations

(E) $$A^{2^n+1} = I, \quad B^2 = I, \quad (AB)^3 = I, \quad (BA^rBA^s)^2 = I,$$

where $r = 1, 2, 3, \ldots, 2^n$, *and the value of s is determined by the relation* $\xi^s(\xi^r+i^2+1) = \xi^r(i^2+1)+1$, ξ *being defined by the relation* $\xi^2 = i^2\xi+1$, i *being a primitive root of the* $GF(2^n)$.

THE GROUP G SIMPLY ISOMORPHIC WITH $LF[2, p^n]$, $p > 2$.

2. LEMMA.—*The abstract group* $G_{\frac{1}{2}p^n(p^{2n}-1)}$, *simply isomorphic with the group* $LF[2, p^n]$, $p > 2$, *may be generated by* (p^n+2) *operators R, T, and* S_λ, λ *running through the marks of* $GF(p^n)$, *subject to relations* (1) *and*

(7) $$R^{\frac{1}{2}(p^n-1)} = I,$$

(8) $$S_\lambda R^\sigma = R^\sigma S_{\lambda i^{2\sigma}} \qquad (\lambda \text{ any mark}, \ \sigma = 0 \text{ or any integer}),$$

(9) $$(TR^\sigma)^2 = I \qquad (\sigma = 0 \text{ or any integer}),$$

(10) $$TS_\gamma T = R^\rho S_{-\gamma} T S_{-1/\gamma} \ (\gamma \text{ any mark} \neq 0, \ i^\rho = -\gamma),$$

i being a primitive root of the $GF(p^n)$.

Proof. — The group $LF[2, p^n]$, $p > 2$, may be generated by the p^n+1 transformations

$$T : z' = \frac{-1}{z}, \qquad S_\lambda : z' = z+\lambda \qquad (\lambda \text{ any mark}),$$

while the sub-group K of the transformations

$$S_{\alpha,\beta} : z' = \frac{\alpha z+\beta}{\alpha^{-1}}$$

may be generated by the transformations

$$S_{1,\lambda} \equiv S_\lambda : z' = z+\lambda, \qquad R : z' = iz/i^{-1},$$

i being a primitive root of the $GF(p^n)$.

These generators of K satisfy relations (1), (7), and (8). Since the group $LF[2, p^n]$, $p > 2$, when represented as a permutation group on (p^n+1) letters, is doubly transitive while the sub-group K, being then a permutation group on p^n letters, is simply transitive, it follows from the work of Jordan* that it is possible to determine γ, δ, η, ζ, and μ such that

---

* *Traité des Substitutions*, p. 32.

the following relations are true :—

(11) $$TS_{\alpha,\beta}T = S_{\gamma,\delta}TS_{\eta,\zeta} \quad (\alpha, \beta \text{ any marks} \neq 0),$$

(12) $$(TR^{\sigma})^2 = R^{\mu} \qquad (\sigma = 0 \text{ or any integer}).$$

The concrete expressions for $TS_{\alpha,\beta}T$ and $S_{\gamma,\delta}TS_{\eta,\zeta}$ are respectively

$$z' = \frac{\alpha^{-1}z}{-\beta z+\alpha}, \qquad z' = \frac{\gamma\xi . z+\delta\xi-\eta\gamma^{-1}}{\eta^{-1}\gamma . z+\eta^{-1}\delta}.$$

A comparison of these expressions shows that a determination of $\gamma, \delta, \eta, \xi$ is $\gamma = -\beta$, $\delta = \alpha$, $\eta = 1$, $\xi = -\alpha^{-1}\beta^{-1}$. The concrete expression for $TR^{\sigma}T$ is $z' = i^{-2\sigma}z$. Therefore $TR^{\sigma}T = R^{-\sigma}$ and a determination of μ is $\mu = 0$. With these values of $\gamma, \delta, \eta, \xi, \mu$, relations (12) and (11) become, respectively, (9) and

(13) $$TS_{\alpha,\beta}T = S_{-\beta,\alpha}TS_{1,-\alpha^{-1}\beta^{-1}} \quad (\alpha, \beta \text{ any marks} \neq 0).$$

A comparison of the concrete expressions for $S_{\alpha,\beta}$ and $R^{\lambda}S_{1,\alpha\beta}$ shows that $S_{\alpha,\beta} = R^{\lambda}S_{1,\alpha\beta}$ if λ be determined by the relation $i^{\lambda} = \alpha$. Therefore (13) may be written in the form

(14) $$TR^{\lambda}S_{1,\alpha\beta}T = R^{\mu}S_{1,-\alpha\beta}TS_{1,-\alpha^{-1}\beta^{-1}},$$

where λ, μ are determined by the relations $i^{\lambda} = \alpha$, $i^{\mu} = -\beta$.

In view of (9), relation (14) may be written

$$R^{-\lambda}TS_{1,\alpha\beta}T = R^{\mu}S_{1,-\alpha\beta}TS_{1,-\alpha^{-1}\beta^{-1}},$$

or, if we write $\alpha\beta = \gamma$, and use the notation $S_{1,\gamma} \equiv S_{\gamma}$, in the form (10).

This completes the first part of the proof, namely, that the generators T, R, S_{λ} of the group $LF[2, p^n]$, $p > 2$, satisfy relations (1), (7), (8), (9), (10). From this fact it follows that the abstract group G' defined by relations (1), (7), (8), (9), (10) is either the group $G_{\frac{1}{2}p^n(p^{2n}-1)}$ or a larger group. That it cannot be a larger group is seen as follows :—Every element g' of the group G' is a product whose constituents are T, R, S_{λ}. Every such product that does not involve T may be reduced by means of (1), (7), (8) to the form $R^{\sigma}S_{\lambda}$, where λ is a mark of the $GF(p^n)$, and $\sigma = 1, 2, 3, \ldots$, or $\frac{1}{2}(p^n-1)$. The maximum number of distinct products of this type is $\frac{1}{2}p^n(p^n-1)$. Every product that does involve T may be written in the form

$$g' = R^{\sigma_1}S_{\lambda_1}TR^{\sigma_2}S_{\lambda_2}TR^{\sigma_3}S_{\lambda_3}TR^{\sigma_4}S_{\lambda_4}T\ldots,$$

a product containing n T's. If $\lambda_2 = 0$, then $S_{\lambda_2} = I$ and $TR^{\sigma_2}T = R^{-\sigma_2}$, by (9). In this case g' reduces to

$$g' = R^{\sigma_1}S_{\lambda_1}R^{-\sigma_2}R^{\sigma_3}S_{\lambda_3}TR^{\sigma_4}S_{\lambda_4}T\ldots,$$

which, by (1), (7), (8), may be reduced to

$$g' = R^{\sigma'} S_{\lambda'} T R^{\sigma_4} S_{\lambda_4} T \ldots,$$

a product containing $(n-2)$ T's. If $\lambda_2 \neq 0$, we have

$$T R^{\sigma_2} S_{\lambda_2} T = R^{-\sigma_2} T S_{\lambda_2} T$$

by (9). Also, by (10), $T S_{\lambda_2} T = R^{\rho} S_{-\lambda_2} T S_{-1/\lambda_2}$.

Therefore g' becomes

$$g' = R^{\sigma_1} S_{\lambda_1} R^{-\sigma_2} R^{\rho} S_{-\lambda_2} T S_{-1/\lambda_2} R^{\sigma_3} S_{\lambda_3} T R^{\sigma_4} S_{\lambda_4} T \ldots,$$

which, by means of (1), (7), (8), may be reduced to

$$g' = R^{\sigma''} S_{\lambda''} T R^{\sigma'''} S_{\lambda'''} T R^{\sigma_4} S_{\lambda_4} T \ldots,$$

a product containing $(n-1)$ T's.

The process indicated reduces the number of T's in the expression for g' by one or two at each step. A finite number of steps will reduce the expression for g' to a product containing one T or no T's. In the latter case g' may be reduced to the form $R^{\sigma} S_{\lambda}$, as above. In the former case $g' = R^{\sigma} S_{\lambda} T R^{\sigma'} S_{\lambda'}$. In view of (9) this becomes $g' = R^{\sigma} S_{\lambda} R^{-\sigma'} T S_{\lambda'}$, which may be reduced by means of (1), (7), (8) to the type form $g' = R^{\sigma_1} S_{\lambda_1} T S_{\lambda'}$.

The maximum number of distinct products of this type is $\frac{1}{2} p^{2n} (p^n - 1)$. The maximum order of the group G' is

$$\tfrac{1}{2} p^n (p^n - 1) + \tfrac{1}{2} p^{2n} (p^n - 1) = \tfrac{1}{2} p^n (p^{2n} - 1),$$

which is precisely the order of the group $G_{\frac{1}{2} p^n (p^{2n}-1)}$. Therefore the two groups are identical, and relations (1), (7), (8), (9), (10) constitute a set of generational relations for the group $G_{\frac{1}{2} p^n (p^{2n}-1)}$.

3. *Proof of Theorem II.*

Relations (1) and (2) are those of relations (1), (7), (8), (9), (10) which do not involve R. $T^2 = I$ comes from (9) when $\sigma = 0$, and $(S_1 T)^3 = I$ comes from (10) when $\gamma = \pm 1$. When $\gamma = -i$, relation (10) becomes

$$R = T S_{-i} T S_{-1/i} T S_{-i}. \tag{15}$$

The rest of relations (10), viz., $R^{\rho} = T S_{\gamma} T S_{1/\gamma} T S_{\gamma}$, $\gamma = -i^{\rho}$, $\rho \neq 0$ or 1, follow from (1), (2), (4), and (15). To prove this it will be sufficient to show that the relation

$$T S_{\gamma} T S_{1/\gamma} T S_{\gamma} T S_{-i} T S_{-1/i} T S_{-i} = T S_{i\gamma} T S_{1/i\gamma} T S_{i\gamma} \tag{16}$$

(where $\gamma = -i^{\rho}$, $\rho \neq 0$ or 1) follows from (1), (2), and (4). By means of (1) and (2) relation (16) may be written

$$(T S_{i\gamma - \gamma} T S_{1/i\gamma} T) S_{i\gamma + i} T S_{1/i} (T S_i T S_{-\gamma} T) S_{-1/\gamma} = I.$$

But, by (4), $TS_iTS_{-\gamma}T = S_{(-\gamma-1)/(i\gamma+1)}TS_{-i\gamma-1}TS_{(i-1)/(i\gamma+1)}$,

and $TS_{i\gamma-\gamma}TS_{1/i\gamma}T = S_{(1-i\gamma)/\gamma}TS_{-1/i}TS_{i^2\gamma-i\gamma-i}$.

Therefore (16) becomes

$$S_{(1-i\gamma)/\gamma}TS_{-1/i}TS_{i^2\gamma-i\gamma-i}S_{i\gamma+i}TS_{1/i}S_{(-\gamma-1)/(i\gamma+1)}TS_{-i\gamma-1}TS_{(i-1)/(i\gamma+1)}S_{-1/\gamma} = I,$$

or, by (1) and (2),

$$TS_{-1/i}TS_{i^2\gamma}TS_{(1-i)/(i+i^2\gamma)}TS_{-i\gamma-1}TS_{(-1-i^2\gamma)/(1+i\gamma)} = I,$$

which is the inverse of $\left[\frac{1}{i}, \frac{1+i^2\gamma}{1+i\gamma}\right]$, one of relations (4).

To complete the proof of the theorem it will be sufficient to show that relations (7), (8), and (9), expressed in terms of T and S_λ by means of (10), follow from (1), (2), (3), and (4).

The substitution in (7) of the value of $R^{\frac{1}{2}(p^n-1)}$ given by (10) results in $(S_1T)^3 = I$, one of relations (2).

The substitution in (9) of the value of R^σ given by (10) results in $(S_{-i^\sigma}TS_{-i^{-\sigma}}TS_{-i^\sigma})^2 = I$, which follows from (1) and (3).

Relations (8) are seen to be equivalent to the relations

$$(17) \qquad S_{i^{2k}} = R^{-k}S_1R^k, \qquad (18) \qquad S_{i^{2k+1}} = R^{-k}S_iR^k,$$

the range for k being 1, 2, 3, ..., $\frac{1}{2}(p^n-3)$.

The substitution in (17) of the value of R^k given by (10) results in the relations $[-1/i^{2k}, i^{2k}]$ which follow from (4). The same substitution in (18) results in

$$(19) \qquad S_{-ia^2}TS_{-1/a}TS_{-a}TS_iTS_aTS_{1/a}T = I, \qquad a = -i^k.$$

When $ia \neq 1$, relation (19) follows from (1), (2), and $[i, a]$, $[1/a, ia^2]$, as may be seen by substituting in (19) the value of TS_iTS_aT given by $[i, a]$. When $ia = 1$, relation (19) follows from (1), (2), and $[i, -1/i]$, $[1/i, \frac{1}{2}(i+1)]$, as may be seen by substituting in (19) the value of $TS_iTS_{-1/i}T$ given by $[i, -1/i]$. This substitution is made after replacing a by $1/i$ in (19).

This completes the elimination of R from the set of generational relations (1), (7), (8), (9), (10), the result being the set of relations (B).

4. LEMMA.—*The abstract group* $G_{\frac{1}{2}p(p-1)}$, *simply isomorphic with the group* $LF[2, p^n]$, *may be generated by two operators* T *and* S *subject to the generational relations* (A) *and* (20) $[1/i, i^2]$, i *being a primitive root of* p.

Proof.—For the group $LF[2, p]$, $p > 2$, only two generators, T and S, are necessary, and in relations (1), (7), (8), (9), (10) we may write S^λ in place of S_λ. Some simplifications result from the fact that the marks

of the $GI(p)$ are all integers. Relations (17) and (18), which were seen to be equivalent to (8), now become

$$S^{i^{2k}} = R^{-k}SR^k, \quad S^{i^{2k+1}} = R^{-k}S^iR^k. \tag{21}$$

Relations (21) all follow from $S_{i^2} = R^{-1}SR$, as may be proved easily by induction. Relations (9) all follow from $T^2 = I$ and $(TR)^2 = I$, and the set of relations (1), (7), (8), (9), (10) becomes the following:—

$$S^p = I, \quad T^2 = 1, \quad (ST)^3 = I; \tag{22}$$

$$R^{\frac{1}{2}(p-1)} = I; \tag{23}$$

$$S^{i^2} = R^{-1}SR; \tag{24}$$

$$(TR)^2 = I; \tag{25}$$

$$R^\rho = TS^\gamma TS^{1/\gamma}TS^\gamma, \quad \text{where} \quad \gamma = -i^\rho, \ \rho \neq 0. \tag{26}$$

When $\rho = 1$, (26) gives R in terms of S and T, viz.,

$$R = TS^{-i}TS^{-1/i}TS^{-i}. \tag{27}$$

When $\rho = 2k$, an even number, (26) becomes

$$R^{2k} = TS^{-i^{2k}}TS^{-i^{-2k}}TS^{-i^{2k}}.$$

This follows from (22), (24), (25), and (27), for

$$\begin{aligned}
TS^{-i^{2k}}TS^{-i^{-2k}}TS^{-i^{2k}} &= T(R^{-k}S^{-1}R^k)T(R^kS^{-1}R^{-k})T(R^{-k}S^{-1}R^k), && \text{by (24)}\\
&= TR^{-k}S^{-1}(R^kTR^k)S^{-1}(R^{-k}TR^{-k})S^{-1}R^k\\
&= TR^{-k}(S^{-1}TS^{-1}TS^{-1})R^k, && \text{by (25)},\\
&= TR^{-k}TR^k, && \text{by (22)},\\
&= R^kT^2R^k, && \text{by (25)},\\
&= R^{2k}, && \text{by (22)}.
\end{aligned}$$

When $\rho = 2k+1$, an odd number, (26) becomes

$$R^{2k+1} = TS^{-i^{2k+1}}TS^{-i^{2k+1}}TS^{-i^{2k+1}}.$$

This follows from (22), (24), (25), and (27), for

$$\begin{aligned}
TS^{-i^{2k+1}}TS^{-i^{-(2k+1)}}TS^{-i^{2k+1}} &= T(R^{-k}S^{-i}R^k)T(R^{k+1}S^{-i}R^{-k-1})T(R^{-k}S^{-i}R^k), \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{by (24)},\\
&= (TR^{-k})S^{-i}(R^kTR^k)RS^{-i}R^{-1}(R^{-k}TR^{-k})S^{-i}R^k,\\
&= R^kTS^{-i}T(RS^{-i}R^{-1})TS^{-i}R^k, && \text{by (25)},\\
&= R^k(TS^{-i}TS^{-1/i}TS^{-i})R^k, && \text{by (24)},\\
&= R^kRR^k, && \text{by (27)},\\
&= R^{2k+1}.
\end{aligned}$$

To complete the proof of the theorem it will be sufficient to show that relations (23), (24), and (25), expressed in terms of S and T by means of (26), follow from relations (A) and (20).

The substitution in (23) of the value of $R^{\frac{1}{2}(p-1)}$ given by (26) results in the relation $(ST)^3 = I$. The substitution in (24) of the value of R given by (26) results in a relation which reduces to (20) by means of relations (A). The same substitution in (25) results in the relation $(S^{-i}TS^{-1/i}TS^{-i})^2 = I$, which follows from relations (A).

This completes the elimination of R from the set of generational relations (22), (23), (24), (25), (26), the result being the set of generational relations (A) and (20).

5. *Proof of Theorem I.*

The proof of Theorem I. consists in showing that (20) is a consequence of relations (A). (20) may be written in the form

$$(TS^{1/i}TS^{2i})S^{i^2-2i}TS^{-1/i}T^{1-i}TS^{1+i} = I.$$

Replace the expression in parentheses by its inverse, as may be done by (A), and invert. The relation becomes

$$TS^{i-1}TS^{1/i}TS^{2i-i^2}TS^{1/i}TS^{i-1} = I. \tag{28}$$

Conversely, (20) follows from (A) and (28). Consider the relation

$$TS^{i-k}TS^{1/(i-k+1)}TS^{-(i-k-1)(i-k+1)}TS^{1/(i-k+1)}TS^{i-k} = I, \tag{29}$$

where k is an odd integer. It may be written

$$TS^{i-k}TS^{1/(i-k+1)}(TS^{-(i-k+1)(i-k-1)}TS^{-2/(i-k+1)(i-k-1)})S^{1/(i-k-1)}TS^{i-k} = I.$$

Replace the expression in parentheses by its inverse, as may be done by (A), and it becomes

$$TS^{-i+k+2}(S^{2i-2k-2}TS^{1/(1-k-1)}T)S^{(i-k-1)(i-k+1)}(TS^{1/(i-k-1)}TS^{2i-2k-2})S^{-i+k+2} = I.$$

Replace the expression in each pair of paren ses by its inverse, as may be done by (A), and then invert. The relation becomes

$$TS^{i-k'}TS^{1/(i-k'+1)}TS^{-(i-k'-1)(i-k'+1)}TS^{1/(i-k'+1)}TS^{i-k'} = I, \tag{30}$$

where $k' = k+2$.

Relation (30) is a consequence of (A) and (29), and, conversely, (29) is a consequence of (A) and (30). But, for $k = 1$, (29) becomes (28). Therefore, for any value of k, k being an odd integer, relation (29) is a consequence of (A) and (28), and, conversely, (28) is a consequence of (A) and (29). But, for $k = i$ or $k = i+1$, according as i is an odd or even integer, relation (29) reduces to $(ST)^3 = I$. Therefore (28) is a consequence of the relations (A).

6. *Theorem III.—Outline of Proof.*

By making use of the method used by Prof. Dickson* for other special cases, the writer has made the computations which prove that, for the special cases in which $p^n = 49, 81, 121$, relations (4) are a consequence of relations (1), (2), (3). The method was proved to fail for $p^n = 169$. For this computation it was found convenient to have the marks of the $GF(p^n)$ arranged in two tables. In each table every mark is expressed as a power of a primitive root i, and as a polynomial in i of degree $k \leqslant n-1$. The coefficients in this polynomial are integers reduced modulo p. The mark $\alpha i^k+\beta i^{k-1}+\gamma i^{k-2}+\ldots+\delta i+\epsilon$ is denoted by the symbol $(\alpha\beta\gamma\ldots\delta\epsilon)$. This symbol is the usual symbol for a positive integer in the notation of the number system whose base is p. In the first table the marks are arranged according to ascending powers of i. In the second table the marks are arranged so that the symbols $(\alpha\beta\gamma\ldots\delta\epsilon)$ represent the positive integers in their natural order. These two tables make it possible to perform with ease the operations of addition, subtraction, multiplication, and division within the field $GF(p^n)$. For $p^n \leqslant 169$, these tables have been computed by the writer and have been deposited in the mathematical library of the University of Chicago.

THE GROUP G SIMPLY ISOMORPHIC WITH $LF[2, 2^n]$.

7. *Proof of Theorem IV.*

Relations (5) and (6) are found to be satisfied when a, b, c are identified with the transformations $z' = iz$, $z' = z+1$, $z' = 1/z$ of the group $LF[2, 2^n]$. Therefore the abstract group G' defined by (5) and (6) must be either the group $G_{2^n(2^{2n}-1)}$ or a larger group. That it cannot be a larger group is seen as follows.

Let H' be the sub-group of G' that is defined by (5). Every element g' of the group G' can be reduced by means of (5) and (6) to one of the two type forms h_1', $h_1'ch_2'$, where h_1' and h_2' are elements of the group H'. Every element h' of H' can be reduced by means of (5) to one of the two type forms a^λ, $a^\lambda ba^\mu$. Therefore every element g' of G' can be reduced by means of (5) and (6) to one of the six type forms

$$a^\lambda, \quad a^\lambda ba^\mu, \quad a^\lambda ca^\mu, \quad a^\lambda ca^\mu ba^\nu, \quad a^\lambda ba^\mu ca^\nu, \quad a^\lambda ba^\mu ca^\nu ba^\sigma.$$

The last four of these can be further reduced by means of (5) and (6), so

---

* *Proc. London Math. Soc.*, Vol. XXXV., pp. 292–305.

that the six type forms are

$$a^\lambda, \quad a^\lambda b a^\mu, \quad a^\lambda c, \quad a^\lambda c b a^\mu, \quad a^\lambda b c a^\mu, \quad a^\lambda b c a^\mu b a^\nu.$$

The maximum numbers of distinct elements of the six types are respectively (2^n-1), $(2^n-1)^2$, (2^n-1), $(2^n-1)^2$, $(2^n-1)^2$, $(2^n-1)^3$. Therefore the maximum number of distinct elements g' is

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

which is precisely the order of the group $G_{2^n(2^{2n}-1)}$.

8. The relations $ba^\xi b = a^\eta b a^\zeta$ are highly redundant. If they be denoted symbolically by (ξ, η, ζ), it appears that the relations $(-\xi, -\zeta, -\eta)$, $(\eta, \xi, -\zeta)$, $(-\eta, \zeta, -\xi)$, $(\zeta, -\eta, \xi)$, $(-\zeta, -\xi, \eta)$, and $(2^k\xi, 2^k\eta, 2^k\zeta)$ follow from (ξ, η, ζ), and the two relations $a^{2^n-1} = I$, $b^2 = I$. In the special case in which $x = 3$, de Seguier has reduced the system (C) to the system (D) of Theorem V. The attempt to do this in general has resulted in Theorem V.

9. *Proof of Theorem V.*

The proof consists in expressing relations (5) and (6) in terms of $d = cb$, and in simplifying the set of relations thus obtained. Since $(ca)^2 = I$, and consequently $ca^\zeta c = a^{-\zeta}$, the relation $(-\xi, -\zeta, -\eta)$ may be written $ba^{-\xi}b = ca^\zeta cba^{-\eta}$, whence

$$b = a^\xi d^{-1} a^\zeta d a^{-\eta}, \tag{31}$$

$$c = d a^\xi d^{-1} a^\zeta d a^{-\eta}. \tag{32}$$

The relation $b^2 = I$, expressed in terms of a and d, is, since $\xi - \eta \equiv \zeta \pmod{2^n-1}$,

$$(d^{-1}a^\zeta d a^\zeta)^2 = I. \tag{33}$$

The relation $(ca)^2 = I$ may be replaced by the relation $(ca^\eta)^2 = I$, since the latter includes the former and follows from it. Expressed in terms of a and d, this relation is

$$(d^{-1}a^\xi d^{-1}a^\zeta)^2 = I. \tag{34}$$

The relation $c^2 = I$, expressed in terms of a and d, is

$$(a^{-\xi}da^{\xi-\zeta}d^{-1}a^{-\zeta}d)^2 = I$$

or

$$[(a^{-\xi}da^{\xi-\zeta})d^{-1}a^{-\zeta}da^{-\xi}da^{\xi-\zeta}(a^{-\xi}da^{\xi-\zeta})]^2 = I,$$

which is equivalent to $(d^{-1}a^{-\zeta}da^{-\xi}da^{\xi-\zeta})^2 = I$.

If $da^{-\xi}da^{-\zeta}$ be replaced by its inverse, as may be done by (34), this becomes

$$(da^{\xi}d^{-1}a^{\zeta})^2 = I, \tag{35}$$

which is equivalent to (33).

The relation $ba^{\xi}b = a^{\eta}ba^{\zeta}$, expressed in terms of a and d, is

$$(d^{-1}a^{\zeta}da^{\zeta})\,a^{\xi}d^{-1}a^{\zeta}(da^{-\zeta}d^{-1}a^{-\zeta})\,da^{-\eta} = I. \tag{36}$$

Replace each of the expressions in parentheses by its inverse, as may be done by (33), transform by a^{ζ}, and (36) becomes

$$\begin{aligned}
&d\,(da^{-\zeta}da^{-\xi})\,(a^{2\xi}d^{-1}a^{2\zeta}d^{-1})\,d^{-1}a^{-\eta}\\
&= d\,(a^{\xi}d^{-1}a^{\zeta}d^{-1})\,(da^{-2\zeta}da^{-2\xi})\,d^{-1}a^{-\eta}\\
&= da^{\xi}d^{-1}a^{-\zeta}da^{-\xi}\,(a^{-\xi}d^{-1}a^{-\eta}d^{-1})\,d\\
&= da^{\xi}d^{-1}\,(a^{-\zeta}da^{-\xi}d)\,a^{\eta}da^{\xi}d\\
&= d\,(a^{\xi}da^{\xi}d^{-1})\,a^{\zeta}a^{\eta}da^{\xi}d\\
&= d^{-1}a^{-\xi}d^{-1}a^{-\xi+\zeta+\eta}da^{\xi}d\\
&= d^{-1}a^{-\xi}d^{-1}da^{\xi}d \qquad\qquad \text{(since } \zeta+\eta-\xi = 0\text{)}\\
&= d^3 = I.
\end{aligned}$$

The relation $(cb)^3 = I$, expressed in terms of d, is $d^3 = I$. Relations (5) and (6) have now been expressed in terms of a and d, and the resulting set of relations has been proved to follow from (5) and (6).

10. In proving Theorem VI. for $n = 2, 3, 4$, Prof. Dickson's point of departure was Prof. Moore's set of relations for $G_{2^n(2^{2n}-1)}$ (see note to Theorem II. in the Introduction). He defined T and S_λ in terms of A and B by means of certain relations which express T and S_λ in terms of A and B when T, S_λ, A, B are identified with certain concrete transformations of the group $LF[2, 2^n]$. He then proved that T and S_λ, thus defined, satisfy Moore's relations in view of relations (E).

The same method of proof was applied successfully by the writer to the case in which $n = 5$, but the computation was so excessive as to render it unadvisable to try it for higher cases. The proof for the case $n = 5$ was much simplified by using the same method with relations (C) as the point of departure. Finally, a simpler proof was made for the cases in which $n = 2, 3, 4, 5, 6$, by applying the same method to the set of relations (D).

11. To obtain relations with which to define a and d of the set (D) in terms of A and B, the generators A, B, d, a were identified with the transformations S_iT, S_{1+i}, TS_1, $z' = iz$, where T and S_λ denote the transformations $z' = 1/z$ and $z' = z+\lambda$. Among these concrete transformations exist the relations

$$d = A^{-1}B, \qquad a = S_{i^{2^{n-1}}-1}TS_{i^{2^{n-1}}}TS_{i^{2^{n-1}}-1}T.$$

For any particular value of n, T and S_λ can be expressed in terms of A and B, as is indicated by Prof. Dickson,* and therefore a can be expressed in terms of A and B. This expression can be reduced by means of relations (E), which are satisfied by the concrete transformations A and B.

The result obtained in the special cases in which $n = 2, 3, 4, 5, 6$ is

$$a = A^{-1}BA^{2^{n-1}}B = (BA)\,BA^{2^{n-1}+2}(BA)^{-1}. \tag{41}$$

12. *Proof of Theorem VI. for* $n = 3$.

The $GF[2^3]$ is defined by the primitive irreducible congruence $i^3 \equiv i+1 \pmod 2$. The pairs of values (r, s) of (E) are (1, 2), (2, 1), (3, 5), (4, 6), (5, 3), (6, 4), (7, 8), (8, 7). The set (D) reduces to

$$a^7 = I,\ d^8 = I,\ (d^{-1}ada)^2 = I,\ (d^{-1}a^3da^3) = I,\ (d^{-1}ad^{-1}a^3)^2 = I. \tag{38}$$

Define $d = A^{-1}B$ and $a = (BA)\,BA^6(BA)^{-1}$ and substitute in (38). The relation $a^7 = I$ becomes

$$\begin{aligned}
&BA^6BA^6\,(BA^6BA^4)\,A^2BA^6\,(BA^6BA^4)\,A^2\\
&= BA^6BA^6\,(A^5BA^3B)\,A^2BA^6\,(A^5BA^3B)\,A^2\\
&= BA^6BA^2BA^3\,(BA^3BA)\,ABA^3BA^2\\
&= BA^6BA^2BA^3A^{-1}BA^{-2}\,(BAB)\,A^3BA^2\\
&= BA^6\,(BA^2BA)\,ABA^{-2}\,(A^{-1}BA^{-1})\,A^3BA^2\\
&= BA^6\,(A^{-1}BA^{-2}B)\,ABA^{-3}\,(BA^2BA)\,A\\
&= BA^5BA^7\,(A^{-1}BA^{-1})\,A^{-3}\,(A^{-1}BA^{-2}B)A\\
&= BA^5\,(BA^6BA^4)\,BA^7BA\\
&= BA^5\,(A^{-4}BA^{-6}B)\,BA^7BA\\
&= (BA)^8 = I,
\end{aligned}$$

which is one of relations (E).

* *Proc. London Math. Soc.*, Vol. xxxv., pp. 306 and 443.

The relation $d^3 = I$ becomes $(A^{-1}B)^3 = I$, which is the inverse of one of relations (E).

The relation $(d^{-1}a\,da)^2 = I$ becomes $(A^9B)^2 = I$, which follows from $A^9 = I$ and $B^2 = I$.

The relation $(d^{-1}a^3\,da^3)^2 = I$ becomes

$$\begin{aligned}
&[A(A^4BA^6B)A^2(BA^6BA^4)AB]^2 \\
&= [A(BA^3BA^5)A^2(A^5BA^3B)AB]^2 \\
&= [ABA^3BA^3BA^3(BAB)]^2 \\
&= [ABA^3BA^3BA^2BA^{-1}]^2 \\
&= ABA^3(BA^3BA^5)BA^3BA^2BA^{-1} \\
&= ABA^3(A^4BA^6B)\,BA^3BA^2BA^{-1} \\
&= ABA^7BA^9BA^2BA^{-1} = I,
\end{aligned}$$

which follows from relations (E).

The relation $(d^{-1}a\,d^{-1}a^3)^2 = I$ becomes

$$\begin{aligned}
&[A^5(BAB)A^6BA^6BA^5B]^2 \\
&= [A^4BA^5(BA^6BA^4)AB]^2 \\
&= [A^4BA^5(A^5BA^3B)AB]^2 \\
&= [A^4(BAB)A^3(BAB)]^2 \\
&= [A^4(A^{-1}BA^{-1})A^3(A^{-1}BA^{-1})]^2 \\
&= [A^3(BAB)A^{-1}]^2 \\
&= [A^2BA^{-2}]^2 = I,
\end{aligned}$$

which follows from $B^2 = I$.

This completes the proof of Theorem VI. for $n = 3$.

13. *Proof of Theorem VI. for* $n = 4$.

The $GF(2^4)$ is defined by the primitive irreducible congruence $i^4 \equiv i+1 \pmod 2$. The pairs of values (r, s) of (E) are (1, 2), (2, 1), (3, 7), (4, 12), (5, 13), (6, 9), (7, 3), (8, 11), (9, 6), (10, 14), (11, 8), (12, 4), (13, 5), (14, 10), (15, 16), (16, 15).

The set of relations (D) reduces to

$$(39) \qquad \begin{cases} a^{15} = I, \quad d^3 = I, \quad (d^{-1}a^\xi\,da^\xi)^2 = I, \quad \xi = 1, 4, 5, 10, \\ (d^{-1}a\,d^{-1}a^4)^2 = I, \quad (d^{-1}a^5\,d^{-1}a^{10})^2 = I. \end{cases}$$

Define $d = A^{-1}B$, $a = (BA)BA^{10}(BA)^{-1}$, and substitute in (39). Ex-

pressions for various powers of BA^{10} reduced by means of (E) are as follows :—

$$(BA^{10})^5 = A^{12}BA^{14}BA^{18}BA^{12}, \quad (BA^{10})^{10} = A^{14}BA^{18}BA^{14}B, \quad (BA^{10})^{15} = A^{34}.$$

The relation $a^{15} = I$ becomes $A^{34} = I$, which follows from (E).

The relation $(d^{-1}a\,da)^2 = I$ becomes $(A^{17}B)^2 = I$, which follows from $A^{17} = I$ and $B^2 = I$.

The relation $(d^{-1}a^4\,da^4)^2 = I$ becomes

$$[A^{-1}B(BA^{10})^4A^{-1}B(BA^{10})^4A^{-1}B]^2 = I,$$

which reduces, by means of (E), to $(BA^9BA^6)^2 = I$.

The relation $(d^{-1}a^5\,da^5)^2 = I$ becomes

$$[A^{-1}B(BA^{10})^5A^{-1}B(BA^{10})^5A^{-1}B]^2 = I,$$

which reduces, by means of (E), to $(BA^7BA^8)^2 = I$.

The relation $(d^{-1}a^{10}\,da^{10})^2 = I$ becomes

$$[A^{-1}B(BA^{10})^{10}A^{-1}B(BA^{10})^{10}A^{-1}B]^2 = I,$$

which reduces, by means of (E), to $(BA^6BA^9)^2 = I$.

The relation $(d^{-1}a\,d^{-1}a^4)^2 = I$ becomes

$$[A^8BA^9BA^{10}BA^{10}BA^9B]^2 = I,$$

which reduces, by means of (E), to $A^{17} = I$.

The relation $(d^{-1}a^5\,d^{-1}a^{10})^2 = I$ becomes

$$[A^{-1}BA^{12}BA^{14}BA^{18}BA^{12}BA^{15}BA^{18}BA^{14}BA^{-1}B]^2 = I,$$

which reduces, by means of (E), to $(BA^5BA^{13})^2 = I$.

This completes the proof of Theorem VI. for $n = 4$.

14. *Proof of Theorem VI. for* $n = 5$.

The $GF[2^5]$ is defined by the primitive irreducible congruence $i^5 \equiv i^3+i^2+i+1 \pmod 2$. The pairs of values (r, s) of (E) are (1, 2), (2, 1), (3, 25), (4, 10), (5, 17), (6, 15), (7, 11), (8, 30), (9, 14), (10, 4), (11, 7), (12, 20), (13, 21), (14, 9), (15, 6), (16, 28), (17, 5), (18, 27), (19, 24), (20, 12), (21, 13), (22, 26), (23, 29), (24, 19), (25, 3), (26, 22), (27, 18), (28, 16), (29, 23), (30, 8), (31, 32), (32, 31).

The set of relations (D) reduces to

$$(40) \quad \begin{cases} a^{31} = I, \quad d^3 = I, \quad (d^{-1}a^\xi\,da^\xi)^2 = I, \quad \xi = 1, 3, 8, 12, \\ (d^{-1}a\,d^{-1}a^{12})^2 = I, \quad (d^{-1}a^3\,d^{-1}a^3)^2 = I. \end{cases}$$

Define $d = A^{-1}B$, $a = (BA)BA^{18}(BA)^{-1}$, and substitute in (40). The relation $a^{31} = I$ becomes $(BA^{18})^{31} = I$. Before proceeding further it will be necessary to simplify the expressions for various powers of (BA^{18}) by means of (E).

$$\begin{aligned}(BA^{18})^7 &= BA^{18}BA^{18}BA^{18}(BA^{18}BA^{27})A^{24}BA^{18}BA^{18}\\ &= BA^{18}BA^{-1}(A^{19}BA^{24}B)A^{15}(BA^{24}BA^{19})A^{-1}BA^{18}\\ &= BA^{18}(ABA)A^9BA^{14}A^{15}A^{14}BA^9(ABA)A^{18}\\ &= BA^{19}BA^{10}BA^{10}BA^{10}BA^{19}.\end{aligned}$$

$$\begin{aligned}(BA^{18})^{15} &= (BA^{18})^4(BA^{18})^7(BA^{18})^4\\ &= (BA^{18})^2(BA^{18}BA^{27})(A^{24}BA^{19}B)A^{10}BA^{10}BA^{10}(BA^{19}BA^{24})\\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\times(A^{27}BA^{18}B)A^{18}BA^{18}\\ &= BA^{18}BA(A^{28}BA^{29}B)A^{19}BA^{10}BA^{19}(BA^{29}BA^{28})ABA^{18}\\ &= BA^{18}(BAB)A^4BA^{29}BA^{10}BA^{29}BA^4(BAB)A^{18}\\ &= BA^{17}(BA^3BA^{25})A^4(BA^{10}BA^4)(A^{25}BA^3B)A^{17}\\ &= BA^{25}BA^{17}BA^{25}.\end{aligned}$$

$$\begin{aligned}(BA^{18})^{31} &= (BA^{18})^{15}(BA^{18})^{15}(BA^{18})\\ &= BA^{25}BA^{17}BA^{25}(BA^{25}BA^3)A^{14}BA^{25}BA^{18}\\ &= BA^{25}BA^{17}BA^{22}BA^{-1}(A^9BA^{14}B)A^{25}BA^{18}\\ &= BA^{25}BA^{17}BA^{23}BA^{20}(BA^{16}BA^{23})A^{23}\\ &= BA^{25}BA^{17}BA^{23}(BA^{25}BA^3)A^{14}BA^{23}\\ &= BA^{25}BA^{17}BA^{20}BA^{-1}(A^9BA^{14}B)A^{23}\\ &= BA^{25}BA^{17}BA^{21}(BA^{20}BA^{12})A^2\\ &= BA^{25}BA^{17}(BA^9BA^{14})A^{-1}BA^2\\ &= (BA^{25}BA^3)^2.\end{aligned}$$

The relation $(BA^{18})^{31} = I$ becomes $(BA^{25}BA^3)^2 = I$, which is one of relations (E).

The relation $(d^{-1}a\,da)^2 = I$ becomes $(A^{33}B^2)^2 = I$, which follows from $A^{33} = I$ and $B^2 = I$.

The relation $(d^{-1}a^3\,da^3)^2 = I$ becomes

$$[A^{17}BA^{18}BA^2BA^{18}BA^{17}B]^2 = I$$

$$\begin{aligned}
\text{or}\quad & A^{17}BA^{18}BA^{2}BA^{18}(BA^{17}BA^{5})A^{12}BA^{18}BA^{2}(BA^{18}BA^{27})A^{23}B \\
&= A^{17}BA^{18}BA^{2}(BA^{18}BA^{21})A^{28}BA^{12}(BA^{18}BA^{27})A^{14}BA^{15}BA^{23}B \\
&= A^{17}BA^{18}BA^{14}BA^{20}BA\,(A^{27}BA^{18}B)A^{15}BA^{14}BA^{15}BA^{23}B \\
&= A^{17}BA^{18}BA^{14}BA^{19}BA^{14}\,(BA^{21}BA^{18})ABA^{15}BA^{23}B \\
&= A^{17}BA^{18}BA^{14}BA^{19}(BAB)A^{12}(BAB)A^{15}BA^{23}B \\
&= A^{17}BA^{18}BA^{14}BA^{18}BA\,(A^{9}BA^{14}B)A^{23}B \\
&= A^{17}BA^{18}BA^{14}(BA^{17}BA^{5})A^{13}BA^{14}B \\
&= A^{17}BA^{4}(A^{14}BA^{9}B)A^{16}BA^{13}BA^{14}B \\
&= B(BA^{17}BA^{5})A^{-1}BA^{24}BA^{2}BA^{13}BA^{14}B \\
&= BA^{-5}BA^{17}(BA^{25}BA^{5})A^{-1}BA^{13}BA^{14}B \\
&= BA^{-5}(BA^{14}BA^{9})^{2}A^{5}B = I,
\end{aligned}$$

which follows from relations (E).

The relation $(d^{-1}a^{8}da^{8})^{2} = I$ becomes

$$[A^{17}(BA^{18})^{7}A^{17}(BA^{18})^{7}A^{-1}B]^{2} = I$$

$$\begin{aligned}
\text{or}\quad & [A^{17}(BA^{19}BA^{24})A^{19}BA^{10}\,(BA^{10}BA^{4})A^{-1}BA^{19}(BA^{10}BA^{4})A^{6}BA^{10}BA^{18}B]^{2} \\
&= [A^{26}BA^{14}BA^{19}BA^{6}(BA^{24}BA^{19})A^{30}(BA^{23}BA^{29})A^{10}BA^{10}BA^{18}B]^{2} \\
&= [A^{26}BA^{14}(BA^{19}BA^{24})A^{29}BA^{9}(BAB)A^{10}BA^{10}BA^{10}BA^{18}B]^{2} \\
&= [A^{26}BA^{23}BA^{14}BA^{-1}\,(A^{30}BA^{8}B)\,A^{9}BA^{10}BA^{10}BA^{18}B]^{2} \\
&= [A^{26}BA^{23}(BA^{15}BA^{6})(A^{20}BA^{12}B)A^{10}BA^{10}BA^{18}B]^{2} \\
&= [A^{26}(BA^{17}BA^{5})ABA^{23}BA^{10}BA^{18}B]^{2} \\
&= [A^{21}BA^{15}BA^{22}BA^{10}BA^{18}B]^{2} \\
&= A^{21}BA^{15}BA^{22}(BA^{10}BA^{4})A\,(A^{13}BA^{21}B)A^{15}BA^{22}(BA^{10}BA^{4})A^{14}B \\
&= A^{21}BA^{15}BA^{18}BA^{22}(BA^{11}BA^{7})A\,(A^{27}BA^{18}B)A^{23}BA^{14}B \\
&= A^{21}BA^{15}BA^{18}BA^{15}(BA^{21}BA^{18})ABA^{29}BA^{14}B \\
&= A^{21}BA^{15}BA^{18}BA^{2}(BA^{11}BA^{7})A^{21}BA^{14}B \\
&= A^{21}BA^{15}(BA^{18}BA^{27})ABA^{22}(BA^{21}BA^{18})AB \\
&= A^{21}BA^{21}BA^{15}(BAB)A^{8}BA^{12}BAB \\
&= A^{21}(BA^{21}BA^{18})ABA^{8}BA^{12}BAB \\
&= A^{8}BA^{12}(BAB)A^{8}BA^{12}(BAB) \\
&= A\,(A^{7}BA^{11}B)^{2}A^{-1} = I,
\end{aligned}$$

which follows from relations (E).

The relation $(d^{-1}a^{12}da^{12})^2 = I$ becomes

$$[A^{-1}B(BA^{18})^{12}A^{-1}B(BA^{18})^{12}A^{-1}B]^2 = I$$

or
$$[A^{-1}B\{BA^{25}BA^{17}BA(A^6BA^{15}B)A^{16}BA\}^2]^2$$
$$= [A^{-1}B(BA^{25}BA^{16}BA^{17}BA^{10}BA)^2]^2$$
$$= [A^{24}(BA^{16}BA^{28})A^{22}BA^9BA^{24}BA^{16}BA^{17}BA^{10}BA]^2$$
$$= [A^{29}BA^{17}(BA^{22}BA^{26})A^{16}BA^{24}BA^{16}BA^{17}BA^{10}BA]^2$$
$$= [A^{29}BA^{24}BA^{11}(BA^{16}BA^{28})A(A^{28}BA^{16}B)A^{17}BA^{10}BA]^2$$
$$= [A^{29}BA^{24}B(A^{16}BA^{16}BA^{28})A^{21}BA^{22}BA^{10}BA]^2$$
$$= [A^{29}BA^{24}BA^{21}BA^{17}(BA^{21}BA^{13})A^9BA^{10}BA]^2$$
$$= [A^{29}BA^{24}BA^{21}BA^4BA^{12}(BA^9BA^{14})A^{-4}BA]^2$$
$$= [A^{29}BA^{24}BA^{21}BA^4BA^{31}BA(A^{23}BA^{29}B)A]^2$$
$$= [A^{29}BA^{11}(A^{13}BA^{21}B)A^4BA^{30}BA^3BA^{11}]^2$$
$$= [A^{29}(BA^{11}BA^7)A^5BA^{24}BA^{30}BA^3BA^{11}]^2$$
$$= [A^{22}BA^{22}(BA^5BA^{17})A^{-1}(A^8BA^{30}B)A^3BA^{11}]^2$$
$$= [A^{22}BA^5BA^{29}BA^4BA^{28}BA^{11}]^2 = I,$$

which follows from relations (E).

The relation $(d^{-1}ad^{-1}a^{12})^2 = I$ becomes

$$[A^{17}BA(BA^{18})^{12}A^{-1}B]^2 = I$$

or
$$[A^{17}(BAB)A^{25}BA^{17}BA(A^6BA^{15}B)A^{16}BA]^2$$
$$= [A^{16}BA^{24}BA^{16}(BA^{17}B^5A)A^5BA]^2$$
$$= [A^{16}BA^{24}BA^{11}BA^{-1}(A^{17}BA^5B)A]^2$$
$$= [A^{16}BA^{24}BA^{12}BA^{29}BA^{17}]^2$$
$$= (A^{16}BA^{24})(BA^{12}BA^{20})^2(A^{16}BA^{24})^{-1} = I,$$

which follows from relations (E).

The relation $(d^{-1}a^8d^{-1}a^6)^2 = I$ becomes

$$[A^{-1}B(BA^{18})^8BA(BA^{18})^8A^{-1}B]^2 = I$$

or $$[A^{17}BA^{18}BA^{17}(BA^{18}BA^{27})A^{16}BA^{10}BA^{10}(BA^{19}BA^{24})A^{26}B]^2$$

$$= [A^{17}BA^{18}BA^{23}BA^{15}(BA^{16}BA^{23})A^{15}BA^{19}(BA^{14}BA^{9})A^{17}B]^2$$

$$= [A^{17}BA^{18}BA^{23}(BA^{20}BA^{12})A^{-1}(A^{6}BA^{15}B)A^{10}BA^{19}BA^{17}B]^2$$

$$= [A^{17}BA^{18}BA^{11}(BA^{14}BA^{9})(A^{10}BA^{4}B)A^{19}BA^{17}B]^2$$

$$= [A^{17}BA^{18}BA^{2}BA(A^{14}BA^{9}B)A^{17}B]^2$$

$$= [A^{17}BA^{18}(BAB)A^{23}BA^{3}B]^2$$

$$= A^{17}BA^{17}BA^{22}BA^{3}(BA^{17}BA^{5})A^{12}BA^{22}BA^{3}B$$

$$= A^{17}BA^{17}(BA^{22}BA^{26})A^{5}BA^{16}BA^{12}BA^{22}BA^{3}B$$

$$= A^{17}BA^{24}BA^{11}(BA^{5}BA^{17})A^{-1}BA^{12}BA^{22}BA^{3}B$$

$$= A^{17}BA^{24}BA^{27}BA^{29}(BA^{18}BA^{21})ABA^{3}B$$

$$= A^{17}BA^{24}BA^{27}BA^{8}(BA^{19}BA^{24})A^{11}B$$

$$= A^{17}BA^{24}(BA^{27}BA^{18})A^{-1}BA^{14}BA^{11}B$$

$$= A^{17}BA^{6}BA(A^{6}BA^{15}B)A^{11}B$$

$$= [A^{17}BA^{5}B]^2 = I,$$

which follows from relations (E). This completes the proof of Theorem VI. for $n = 5$.

15. *Proof of Theorem VI. for* $n = 6$.

The $GF(2^6)$ is defined by the primitive irreducible congruence $i^6 \equiv i+1 \pmod 2$. The pairs of values (r, s) of (E) are (1, 2), (2, 1), (3, 50), (4, 17), (5, 30), (6, 10), (7, 43), (8, 46), (9, 16), (10, 6), (11, 25), (12, 21), (13, 28), (14, 20), (15, 62), (16, 9), (17, 4), (18, 42), (19, 57), (20, 14), (21, 12), (22, 58), (23, 47), (24, 32), (25, 11), (26, 38), (27, 39), (28, 13), (29, 34), (30, 5), (31, 36), (32, 24), (33, 41), (34, 29), (35, 60), (36, 31), (37, 52), (38, 26), (39, 27), (40, 54), (41, 33), (42, 18), (43, 7), (44, 53), (45, 51), (46, 8), (47, 23), (48, 61), (49, 56), (50, 3), (51, 45), (52, 37), (53, 44), (54, 40), (55, 59), (56, 49), (57, 19), (58, 22), (59, 55), (60, 35), (61, 48), (62, 15), (63, 64), (64, 63).

The set of relations (D) reduces to

$$(41)\quad \begin{cases} a^{63} = I, \quad d^3 = I, \quad (d^{-1}a^{\xi}da^{\xi})^2 = I, \quad \xi = 1, 6, 7, 9, 21, 26, 42, 45, \\ (d^{-1}a^{\xi}d^{-1}a^{\zeta})^2 = I, \text{ the pairs } (\xi, \zeta) \text{ being } (1,6), (7,26), (9,45), (21,42). \end{cases}$$

Define $d = A^{-1}B$, $a = (BA)BA^{34}(BA)^{-1}$, and substitute in (41). The expressions for various powers of (BA^{34}) reduced by means of (E) are

$$(BA^{34})^3 = A^{35}BA^{59}BA^4, \qquad (BA^{34})^9 = A^{20}BA^2BA^{35}BA^{53}BA^{26}BA^{45},$$

$$(BA^{34})^{18} = A^{42}BA^{25}BA^{50}BA^9, \qquad (BA^{34})^{21} = A^{31}BA^{41}BA^{12}BA^{31}BA^{14},$$

$$(BA^{34})^{26} = A^{58}BA^{58}BA^{14}BA^{39}BA^{17}, \quad (BA^{34})^{42} = A^{63}BA^{60}BA^{46}BA^{19}BA^{22}BA^{24},$$

$$(BA^{34})^{45} = A^{63}BA^{52}BA^{42}BA^{40}BA^4, \quad (BA^{34})^{63} = A^2(BA^{23}BA^{47})^2A^{-2}.$$

The relation $a^{63} = I$ becomes

$$(BA)A^2(BA^{23}BA^{47})^2A^{-2}(BA)^{-1} = I,$$

which follows from relations (E).

The relation $(d^{-1}a\,da)^2 = I$ becomes

$$(A^{65}B)^2 = I,$$

which follows from $A^{65} = I$ and $B^2 = I$.

The relation $(d^{-1}a^6\,da^6)^2 = I$ becomes

$$[A^{-1}B(A^{35}BA^{59}BA^{39}BA^{59}BA^3B)^2]^2 = I,$$

which reduces, by means of (E), to $(BA^{19}BA^{57})^2 = I$.

The relation $(d^{-1}a^7\,da^7)^2 = I$ becomes

$$[A^3(BA^{59}BA^{39}BA^{59}BA^7)^2A^{61}B]^2 = I,$$

which reduces, by means of (E), to $(BA^{52}BA^{37})^2 = I$.

The relation $(d^{-1}a^9\,da^9)^2 = I$ becomes

$$[A^{-1}B(A^{20}BA^2BA^{35}BA^{53}BA^{26}BA^{44}B)^2]^2 = I,$$

which reduces, by means of (E), to $(BA^{13}BA^{28})^2 = I$.

The relation $(d^{-1}a^{21}\,da^{21})^2 = I$ becomes

$$[A^{-1}B(A^{31}BA^{41}BA^{12}BA^{31}BA^{13}B)^2]^2 = I,$$

which reduces, by means of (E), to $(BA^{18}BA^{42})^2 = I$.

The relation $(d^{-1}a^{26}\,da^{26})^2 = I$ becomes

$$[A^{-1}B(A^{53}BA^{58}BA^{14}BA^{39}BA^{16}B)^2]^2 = I,$$

which reduces, by means of (E), to $(BA^4BA^{17})^2 = I$.

The relation $(d^{-1}a^{42}\,da^{42})^2 = I$ becomes

$$[A^{-1}B(A^{63}BA^{60}BA^{46}BA^{19}BA^{22}BA^{23}B)^2]^2 = I,$$

which reduces, by means of (E), to $(BA^{22}BA^{58})^2 = I$.

The relation $(d^{-1}a^{45}da^{45})^2 = I$ becomes

$$[A^{-1}B(A^{68}BA^{52}BA^{42}BA^{40}BA^{3}B)^2]^2 = I,$$

which reduces, by means of (E), to $(BA^{3}BA^{50})^2 = I$.

The relation $(d^{-1}ad^{-1}a^{6})^2 = I$ becomes

$$[A^{33}BA^{36}BA^{59}BA^{39}BA^{59}BA^{3}B]^2 = I,$$

which reduces, by means of (E), to $(BA^{64}BA^{63})^2 = I$.

The relation $(d^{-1}a^{7}d^{-1}a^{26})^2 = I$ becomes

$$[A^{3}BA^{59}BA^{39}BA^{59}BA^{4}BA^{54}BA^{58}BA^{14}BA^{39}BA^{16}B]^2 = I,$$

which reduces, by means of (E), to $(BA^{24}BA^{32})^2 = I$.

The relation $(d^{-1}a^{9}d^{-1}a^{45})^2 = I$ becomes

$$[A^{-1}BA^{20}BA^{2}BA^{35}BA^{53}BA^{26}BA^{45}BA^{-1}BA^{52}BA^{42}BA^{40}BA^{8}B]^2 = I,$$

which reduces, by means of (E), to $(BA^{17}BA^{4})^2 = I$.

The relation $(d^{-1}a^{21}d^{-1}a^{42})^2 = I$ becomes

$$[A^{-1}BA^{31}BA^{41}BA^{12}BA^{31}BA^{14}BA^{-1}BA^{60}BA^{46}BA^{19}BA^{22}BA^{23}B]^2 = I,$$

which reduces, by means of (E), to $(BA^{32}BA^{24})^2 = I$. This completes the proof of Theorem VI. for $n = 6$.

Printed by C. F. Hodgson & Son, 2 Newton Street, High Holborn, W.C.