CONCERNING JORDAN’S LINEAR GROUPS.

Presented to the American Mathematical Society, August 28, 1895.

BY ELIAKIM HASTINGS MOORE.

Introduction.

I present to the American Mathematical Society to-day a continuation of the paper* presented last November, entitled The group of holoedric transformation into itself of a given group. To recall briefly: The given (abstract) group $G_n$ of order $n$ has the elements $s_1 = \text{identity}, s_2, \ldots s_n$. The substitution-group $I^n$ of transformation of $G_n$ into itself is the substitution-group on the $n$ letters $s_1, \ldots s_n$ which leaves invariant the multiplication-table for $G_n$. Letters $s$ which are conjugate with one another under $I^n$ must as elements of $G_n$ have the same period. Thus, $s_1 = \text{identity}$ is invariant, and $I^n$ is really $I^{n-1}$ on the $n - 1$ letters $s_2, \ldots s_n$.

We are to consider to-day the case that $I^{n-1}$ is transitive on the $n - 1$ letters $s_2, \ldots s_n$. Then the $n - 1$ elements $s_2, \ldots s_n$ of $G_n$ have the same period, which must then be a prime $p$. Hence $G_n$ has the order $n = p^n$. Every group $G_{n^{p^n}}$ has, in accordance with an important (Sylow’s) theorem,† at least one element different from identity commutative with every element of the group. This property of the element may be read out of the multiplication-table for $G_{n^{p^n}}$, and is hence invariant under $I^{n-1}$. But $I^{n-1}$ is transitive on the $n - 1$ letters $s_2, \ldots s_n$. Hence every element of $G_{n^{p^n}}$ is commutative with every other element. Our given group $G_n$ is then the Abelian $G_{p^n}$, or rather, omitting the $I$, $G_{n^{p^n}}$ with $n$ generating elements, each of order $p$, and commutative with one another. It will cause no confusion if we refer to it hereafter simply as the Abelian $G_{p^n}$.


Mr. Hölder explained this notion of the group of holoedric transformations into itself of a given group, for use in his memoir: Die Gruppen der Ordnungen $p^2$, $pq^2$, $pqr$, $p^8$ (Mathematische Annalen, vol. 43, pp. 301-412; see pp. 313, 314), which bears the date March 28, 1893. We, however, hit on the notion independently of each other; see the foot-note (**) of p. 60 of my former paper.

The group $\Gamma_{\Omega(p^n)}^{p^n}$ of holoedric transformation into itself of the
Abelian group $G_{p^n}$ is Jordan's linear homogeneous substitution-
group of degree $p^n$, $\text{LHG}_{\Omega(p^n)}^{p^n}$.

For the Abelian $G_{p^n}$ we take the $n$ generators

$$(1) \quad a_i \quad (i = 1, 2, \ldots n)$$

with the complete system of generating relations.

$$(2) \quad a_i^p = 1, \quad a_i a_j = a_j a_i \quad (i, j = 1, 2, \ldots n)$$

and have as the general element

$$(3) \quad s_K = s_{k_1, k_2, \ldots, k_n} = a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n} = \prod a_i^{k^i} \quad (i = 1, 2, \ldots n)$$

where the suffixes and exponents $k$ are integers taken modulo $p$, and where $K$ is a symbol standing for $(k_1, k_2, \ldots, k_n)$.

The general multiplication equation is

$$(4) \quad s_K s_{K'} = s_{K+K'}, \quad s_{k_1, k_2, \ldots, k_n} s_{k_1', k_2', \ldots, k_n'} = s_{k_1 + k_1', k_2 + k_2', \ldots, k_n + k_n'}$$

where

$$(5) \quad K_1 + K_2 = K_3, \quad k_{1i} + k_{2i} = k_{3i} \quad (i = 1, 2, \ldots n)$$

It turns out that the general substitution $\sigma_G$ of $\Gamma_{\Omega(p^n)}^{p^n}$ replaces $s_x = s_{x_1, x_2, \ldots, x_n}$ by $s_x' = g_{i_1} x_{i_1} \ldots g_{i_n} x_{i_n}$, where

$$(6) \quad X' = G X, \quad x'_i = \sum_{j=1}^{\frac{p^n}{d}} g_{ij} x_j \quad (|g_{ij}| \neq 0) \quad (i, j = 1, 2, \ldots n),$$

where $G$ is a symbol for the matrix

$$(7) \quad G = (g_{ij}) \quad (i, j = 1, 2, \ldots n)$$

whose elements $g_{ij}$ are integers taken modulo $p$. [To follow the customary notation we should write congruences (modulo $p$) everywhere instead of equations. But in group-theoretic applications such as the present, it is much better to breathe the spirit of the congruence once for all into the definitions of the symbols and operations.] Hence, indeed, $\Gamma_{\Omega(p^n)}^{p^n}$ is Jordan's linear homogeneous substitution-group* of degree $p^n$, $\text{LHG}_{\Omega(p^n)}^{p^n}$, of order $\dagger$

$$(8) \quad \Omega(p^n) = (q^n - 1) (q^n - q) (q^n - q^2) \cdots (q^n - q^{n-1}).$$

* Jordan: Traité des substitutions, p. 92, 1870.
\dagger Jordan: loc. cit., p. 97.
This identification of the \( T^\text{LH} G^\text{p} \) of the Abelian \( G^p \) with the \( LHG^\text{p} \) I obtain first by holding the \( G^p \) as an abstract group; I omit the details of this identification. We may however take the \( G^p \) concretely as the regular Abelian substitution-group \( G^p \) on the \( p^n \) letters \( s_x = s_{x_1}, s_{x_2}, \ldots, s_{x_n} \); the general element
\[
s_x = s_{x_1}, s_{x_2}, \ldots, s_{x_n}
\]
then (4, 5) replaces \( s_x \) by \( s_{x'} \), where
\[
X' = X + K, \quad x'_i = x_i + k_i \quad (i = 1, 2, \ldots, n).
\]

We thus win direct contact with Mr. Jordan's work. The \( G^p \) is within the symmetric substitution-group on the \( p^n \) letters \( s_x \) self-conjugate under the linear non-homogeneous group \( LGG^\text{p} \) of degree \( p^n \) and of order \( p^n \), whose general substitution \( \sigma_{G, K} \) replaces \( s_x \) by \( s_{x'} \), where
\[
X' = \sigma_{G, K} X + K, \quad x'_i = \sum_{j=1}^{m} g_{ij} x_j + k_i \quad (i = 1, 2, \ldots, n).
\]
\( \sigma_{G, K} \) replaces \( s_{x_1}, s_{x_2}, \ldots, s_{x_n} \) by \( s_{x'_1}, s_{x'_2}, \ldots, s_{x'_n} \) where
\[
K'_1 = G K_1 + K, \quad K'_2 = G K_2 + K, \quad K'_3 = G K_3 + K,
\]
so that
\[
K'_1 + K'_2 - K'_3 = G (K_1 + K_2 - K_3) + K;
\]

hence under \( \sigma_{G, K} \) of the \( LGG^\text{p} \) (10) a multiplication equation of the \( G^p \) is preserved, that is,
\[
s_{x_1}, s_{x_2}, s_{x_3} = s_{x_1} + s_{x_2} (4, 5)
\]
if and only if \( K = (0) = (k_1, k_2, \ldots, k_n) = (0, 0, \ldots, 0) \), that is, if and only if the substitution \( \sigma_{G, K} \) of the \( LGG^\text{p} \) (10) is a substitution \( \sigma_{G, 0} = \sigma_{G} \) of the \( LHG^\text{p} \) (6). We have then this (second) identification of the \( T^\text{LH} G^\text{p} \) of the Abelian \( G^p \) with the \( LHG^\text{p} \).

The group \( T^\text{LH} G^\text{p} \) is transitive on the \( p^n - 1 \) letters \( s_x (X \neq (0)) \). For \( p = 2 \) it is doubly transitive on the \( p^n - 1 = 2^n - 1 \) letters. For \( p > 2 \) it is simply transitive and imprimitive; the letter \( s_x = s_{x_1}, s_{x_2}, \ldots, s_{x_n} \) belongs to and by the ratios of its \( n \) suffixes \( X = (x_1, x_2, \ldots, x_n) \) determines the system of imprimitivity containing the \( q-1 \) letters * \( s_{x_l}(l = 1, 2, \ldots, p-1) \); in the \( G^p \) the elements \( s_{x_0} \) and the identity \( s_{x_0} = s_{(0)} \) constitute the cyclic group \( G^p \) determined by \( s_{x_0} \) say the \( G_{p, x} \). Thus,

* \( X = (x_1, \ldots, x_n) \), \( LX = (lx_1, \ldots, lx_n) \).
the $G^m_{\Omega(p^n)} = LG^m_{\Omega(p^n)}$ permutes first the $(p^n - 1)/(p - 1) G_p$ of $G_p^m$, and afterwards fixes the elements within the various groups. The self-conjugate sub-group which keeps every $G_p$ fixed is of order $p - 1$:

$$(11) \quad \{X' = lx, \quad x'_i = lx_i (i = 1, 2, \ldots n), \quad (l = 1, 2, \ldots p - 1).$$

The quotient-group, which is a substitution-group on the $(p^n - 1)/(p - 1) G_p$, has the order $\Omega(p^n)/(p - 1)$. Analytically, it is the $LHG^m_{\Omega(p^n)}$ taken fractionally; that is, the linear fractional group $\mathbb{LFG}^m_{\Omega(p^n)/(p - 1)}$, whose general substitution $\sigma_G$ replaces the $G_p, x$ by the $G_p, x'$, where

$$(12) \quad X'_i = G^* X^i,$$

$x'_1; x'_2; \ldots; x'_i; \ldots; x'_n = \sum g_1 x_1 j; \sum g_2 x_2 j; \ldots; \sum g_n x_n j.$

§ 2. Three tactical configurations:

$LCf[p^n], \quad LHCF[p^n - 1], \quad LFCf[(p^n - 1)/(p - 1)]$;

connected with the Abelian $G_p^n$ are defining invariants respectively for the three linear groups:

$LGF^n_{\Omega(p^n)}, \quad LHG^n_{\Omega(p^n)}, \quad \mathbb{LFG}^m_{\Omega(p^n)/(p - 1)}$

The notion configuration I transfer to tactic from geometry $\dagger$; for the proof and ultimate statement of the theorems about to be stated with utmost brevity, this notion must be used to its full content; to-day, however, the term tactical configuration shall be merely a name.

The linear configuration $LCf[p^n]$ in $p^n$ letters.

The $p^n$ letters of the $LCf[p^n]$ are the $p^n$ elements $s_p$ of the Abelian $G_p^n$. The $G_p^n$ contains $(p^n - 1)/(p - 1)$ sub-groups,

---

* JORDAN: loc. cit., p. 228. In my notation the two subscript dots (..) are the ratio dots (;), and are to call to mind that we may without changing anything replace $X = (x_1, \ldots x_n), \quad X' = (x'_1, \ldots x'_n), \quad G = (g_1)$ by $lX = (lx_1, \ldots lx_n), \quad lX' = (lx'_1, \ldots lx'_n), \quad mG = (mg_1),$ respectively, where $l, l'$, $m$ are any integers taken modulo $p$, but $l \neq 0, l' \neq 0, m \neq 0.$

With respect to each sub-group \( G_{pn} \) the \( p^n \) elements \( s_x \) of the \( G_{pn} \) are exhibited as a certain rectangular array of \( p \) lines with \( p^{n-1} \) elements in each line; the order of the lines and the order of the elements in each line are immaterial; one line contains the \( p^{n-1} \) elements of the \( G_{pn} \) itself. We separate every array into its constituent lines, and have before us in the system of (unordered) \( p(p^n - 1)/(p - 1) \) lines or combinations of \( p^{n-1} \) letters each the linear configuration in \( p^n \) letters, \( LCf[p^n] \).

This \( LCf[p^n] \) for \( n \geq 2 \) defines, as the maximum substitution-group on the \( p^n \) letters \( s_x \) leaving it invariant, exactly the \( LG_{p^n(Q)} \) (§ 1 (10)).

The linear homogeneous configuration \( LHCf[p^n - 1] \)

\( p^n - 1 \) letters.

The \( p^n - 1 \) letters of the \( LHCf[p^n - 1] \) are the \( p^n - 1 \) elements \( s_x(X \neq (0)) \) of the Abelian \( G_{pn} \), the identity \( s(0) \) excepted. The \( LHCf[p^n - 1] \) is obtained from the \( LCf[p^n] \) by omitting every line or combination containing the discarded letter \( s(0) \). The \( LHCf[p^n - 1] \) consists, then, of a system of \( p^n - 1 \) lines or combinations of \( p^{n-1} \) letters each. This \( LHCf[p^n - 1] \) is tactically self-reciprocal,\(^*\) that is, we can distribute a notation \( s'_x \) to the \( p^n - 1 \) lines in such a way that the \( LHCf[p^n - 1] \) on the \( p^n - 1 \) letters \( s_x \) as grouped by the \( p^n - 1 \) lines \( s'_x \) differs only in the priming (') from the \( LHCf[p^n - 1] \) on the \( p^n - 1 \) lines \( s'_x \) as grouped by the \( p^n - 1 \) letters \( s_x \).

This \( LHCf[p^n - 1] \) for \( n \geq 2 \) serves as a defining invariant for exactly the \( LHCF[p^n - 1; Q, p^n] \) (§ 1, (6)). The self-reciprocity of the \( LHCf[p^n - 1] \) establishes an holoedric isomorphism of the \( LHCF[p^n - 1; Q, p^n] \) with itself. This isomorphism is (at least for \( n \geq 3 \)) not\(^*\) that arising from a transformation of the \( LHCF[p^n - 1; Q, p^n] \) through one of its own elements.

The linear fractional configuration \( LFCf[(p^n - 1)/(p - 1)] \)

\( p^n - 1 \) letters.

The \( (p^n - 1)/(p - 1) \) letters of the \( LFCf[(p^n - 1)/(p - 1)] \) are the \( (p^n - 1)/(p - 1) \) cyclic groups \( G_{pn} \) of the Abelian \( G_{pn} \). The \( LFCf[(p^n - 1)/(p - 1)] \) is obtained from the \( LCf[p^n] \) by

\(^*\) Notice the particular case \( (q = 2, n = 3) \) in § 2 of my paper cited above. The \( LHCf[2^3 - 1 = 7] \) and the \( A_7 \) are, so to say, complementary. Indeed, for \( q = 2, n = 3 \), the \( LHCf[2^n - 1] \) determines uniquely a \( A_{2^n - 1} \), from which the \( LHCf[2^n - 1] \) is likewise uniquely determined. This \( A_{2^n - 1} \) serves as a defining invariant for the \( LHCF[2^n - 1; Q] \).
omitting every line not containing the identity letter $s_{(0)}$, that is, by retaining the lines corresponding to the $(p^n - 1)/(p - 1)$ sub-groups $G_{p^{n-1}}$, and then in every such line by omitting the $s_{(0)}$ and replacing every set of $p - 1$ letters $s_{lx}$ ($l = 1, 2, \ldots, q - 1$) by the letter $G_q \times x$. The \( LFC[(p^n - 1)/(p - 1)] \) on $(p^n - 1)/(p - 1)$ letters consists then of a system of $(p^n - 1)/(p - 1)$ lines of $(p^{n-1} - 1)/(p - 1)$ letters each. This \( LFC[(p^n - 1)/(p - 1)] \) is tactically self-reciprocal.

This \( LFC[(p^n - 1)/(p - 1)] \) for $n \geq 3$ serves as a defining invariant for exactly the \( LFG_{\varphi(p^n)/(p-1)} \) ($\text{(12)}$). The self-reciprocity of the \( LFC[(p^n - 1)/(p - 1)] \) ($n \geq 3$) establishes an holoedric isomorphism of the \( LFG_{\varphi(p^n)/(p-1)} \) ($n \geq 3$) with itself. This isomorphism is not that arising from a transformation of the \( LFG_{\varphi(p^n)/(p-1)} \) through one of its own elements.

In § 4 I give these various tactical configurations for certain low values of $p$ and $n$.

\section*{3. Utility of the Galois-field theory in the investigation of linear groups.}

The results given in § 2 depend for their proof largely upon the fact that the group \( \Gamma_{\varphi(p^n)} = LHG_{\varphi(p^n)} \) contains a substitution $\sigma_{\varphi}$ which permutes the $p^n - 1$ letters $s_{lx}(X \neq (0))$ in one cycle of period $p^n - 1$. Any such $\sigma_{\varphi}$ answers the purpose. That one such exists we know from the Galois-field theory.\(^*\)

\(^*\) This linear fractional configuration might also be called the sub-group configuration of the Abelian $G_{\varphi}$.


\(\text{JORDAN:} \) Traité des substitutions, pp. 14–18.


Addendum of Oct. 15, 1895. I have found within a week that Mathieu in Chapter III, pp. 275–304, of his Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariantes (Journal de Mathématiques pures et appliquées, vol. 2, 1861), working from the Galois-field standpoint, defines and investigates two substitution-groups, which are (otherwise expressed) the groups \( L\varphi(p^n) \) and \( LHG_{\varphi(p^n)} \). This seems to be the source from which Mr. Jordan's linear groups (1870) were drawn. Mathieu gives two rational integral functions of the $p^n$
Suppose that the $p^n$ marks $\xi$ of the Galois-field $GF[p^n]$ of order $p^n$ are exhibited explicitly in terms of $n$ linearly independent marks $\eta_1, \eta_2, \ldots, \eta_n$ in the form

$$\xi = \sum_{i=1}^{n} x_i \eta_i,$$

where the $x_i$'s are integral marks, or integers taken modulo $p$. We make through the $X = (x_1, \ldots, x_n)$ a 1:1 correspondence between the letters $s_X$ and the marks $\xi$. In fact the $GF[p^n]$ qua additive-group is a concrete Abelian group. Now in the $GF[p^n]$ additions are invariant under the multiplication-substitution $\sigma_y$ on the $p^n - 1$ marks $\xi (\xi \neq 0)$,

$$\xi' = y \xi (y \neq 0),$$

that is, when every mark of the field is multiplied by the same mark $\gamma$. Hence this $\sigma_y$ interpreted on the $s_X$ is a substitution $\sigma_{\gamma}$ of the $I_{p^n - 1}$. If $\gamma$ is a primitive root of the $GF[p^n]$, $\sigma_y$ permutes the $p^n - 1$ marks $\xi (\xi \neq 0)$ in one cycle, and, similarly, $\sigma_\gamma$ permutes the $p^n - 1$ letters $s_X (X \neq (0))$ in one cycle, and is then the substitution sought.

The results of § 2 constitute for the linear groups sweeping generalizations of Mr. Noether's definition* of the group $I_{p^n}$ by the triple system $A^7$ in seven letters.

§ 4.

Tables of the tactical configurations:

$LCf[p^n], LHCf[p^n - 1], LFCf[(p^n - 1)/(p - 1)],$

for cases $p^n = 2^2, 3^2, 5^2, 7^2, 11^2, 2^3, 3^3, 5^3, 7^3; 2^4, 3^4, 5^4, 7^4; 2^5, 2^6$.

The table for a particular case $[p^n]$ gives first a primitive root $\gamma$ of the Galois-field $GF[p^n]$ and its fundamental equation

letters $s_X$, each of which serves as defining invariant for the $LG^{p^n}_{\omega(p^n)}$. These functions are closely related to our $LCf[p^n]$. In explaining my researches in detail in a subsequent paper I shall point out the exact points of contact with Mathieu's results.

It should be added that several weeks ago Mr. Dickson and I came upon a substitution-group on the $p^n$ marks of the $GF[p^n]$ which Mr. Dickson then identified as another expression of Mr. Jordan's $LHG^{p^n}_{\omega(p^n)}$; this was exactly Mathieu's expression of the group.

* See § 2 of my paper cited above.

† The theory of the linear fractional configuration I introduced in my course Groups, during the last spring quarter at the University of Chicago, and in connection with the members of that course, Messrs. Brown, Dickson, Joffe, and Slaught, worked up the linear fractional configurations for the cases given above, except $p^n = 2^6$. I take this opportunity to thank them for their cooperation, and especially Mr. Dickson, who quite recently completed the tables as given above.

§ I add the tables for $p^n = 2^2, 3^2, 5^2, 7^2, 11^2$, whose linear fractional configurations are trivial. Sept. 10, 1895.
of degree \( n \). The \( p^n \) elements of the abstract \( G_{p^n} \) have the index-notation* derived from the \( p^n \) marks of the \( GF[p^n] \) (as a concrete \( G_{p^n} \), § 3): mark \( \xi = 0 \), index *; mark \( \xi \neq 0 \), \( \xi = \gamma^i \), index \( i \) \((i = 0, 1, \ldots, p^n - 1)\); \( i \) is an integer taken modulo \( p^n - 1 \).

The \( LCF[p^n] \) consists (§ 2) of the lines found in certain \((p^n - 1)/(p - 1)\) arrays. Each array has \( p \) lines; each line has \( p^{n-1} \) indices. Only the first array is given; the others are obtained from it by repeated applications of the cyclical substitution

\[
i' = i + 1, \quad (i = 0, 1, \ldots, p^n - 1),
\]

which leaves * fixed. The first line of the first array is the additive sub-group \( G_{p^{n-1}} \) of the \( GF[p^n] \) qua additive \( G_{p^n} \), which contains the \( n - 1 \) marks \( \gamma^0, \gamma^1, \ldots \gamma^{n-2} \). The second line is obtained by adding the mark \( \gamma^{n-1} \) to the marks of the first line. Of course the lines one and two must be expressed in the index-notation. The following lines are derived from the second at once by repeated additions of \((p^n - 1)/(p - 1)\) to the indices of the second line.

The \( LHCf[p^n - 1] \) and the \( LFCf[(p^n - 1)/(p - 1)] \) are easily derived from the \( LCF[p^n] \) (§ 2). The \( LCF[p^n] \) and the \( LHCf[p^n - 1] \) are tabulated together.

### TABLES.

<table>
<thead>
<tr>
<th>([p^n = 2^2])</th>
<th>( GF[2^2] )</th>
<th>Primitive root ( \gamma ) where ( \gamma^2 = 1 + \gamma ).</th>
</tr>
</thead>
<tbody>
<tr>
<td>( LCF[2^2] )</td>
<td>4 indices * 0 1 2.</td>
<td></td>
</tr>
<tr>
<td>( LHCf[2^2-1] )</td>
<td>3 indices 0 1 2.</td>
<td></td>
</tr>
<tr>
<td>([* 0 4]_2)</td>
<td>([1 2]_2)§</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>([p^n = 3^2])</th>
<th>( GF[3^2] )</th>
<th>Primitive root ( \gamma ) where ( \gamma^2 = 1 + 2\gamma ).</th>
</tr>
</thead>
<tbody>
<tr>
<td>( LCF[3^2] )</td>
<td>9 indices * 0 1 2 7.</td>
<td></td>
</tr>
<tr>
<td>( LHCf[3^2-1] )</td>
<td>8 indices 0 1 2 7.</td>
<td></td>
</tr>
<tr>
<td>([* 0 4]_3)</td>
<td>([1 6 7]_3)([2 3 5]_3)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>([p^n = 5^2])</th>
<th>( GF[5^2] )</th>
<th>Primitive root ( \gamma ) where ( \gamma^2 = 2 + 2\gamma ).</th>
</tr>
</thead>
<tbody>
<tr>
<td>( LCF[5^2] )</td>
<td>25 indices * 0 1 2 23.</td>
<td></td>
</tr>
<tr>
<td>( LHCf[5^2-1] )</td>
<td>24 indices 0 1 2 23.</td>
<td></td>
</tr>
<tr>
<td>([* 0 6 12 18]_5)</td>
<td>([1 3 4 8 17]_5) ([7 9 10 14 23]_5) ([5 13 15 16 29]_5) ([2 11 19 21 22]_5)</td>
<td></td>
</tr>
</tbody>
</table>

* The \( s \) notation for the elements can be recovered if necessary.

† The \( LFCf[p^n - 1] \) for \( n = 2 \) is trivial and hence is not tabulated.

§ Every line \([\ ]\) has a suffix indicating the number of indices lying within.
CONCERNING JORDAN'S LINEAR GROUPS.

\[ p^n = 7^2 \]
- \( GF[7^2] \) Primitive root \( \gamma \) where \( \gamma^2 = 2 + 2\gamma \).
- \( LCF[7^2] \) 49 indices: \( 0, 1 \ldots 47 \).
- \( LHCf[7^2 - 1] \) 48 indices: \( 0, 1 \ldots 47 \).

\[
\begin{align*}
0 & \quad 8 & \quad 24 & \quad 32 & \quad 40 \\
1 & \quad 6 & \quad 18 & \quad 20 & \quad 21 & \quad 27 & \quad 31 \\
3 & \quad 7 & \quad 25 & \quad 30 & \quad 42 & \quad 44 & \quad 45 \\
9 & \quad 14 & \quad 22 & \quad 23 & \quad 34 & \quad 36 & \quad 37 & \quad 43 & \quad 47 \\
10 & \quad 12 & \quad 13 & \quad 19 & \quad 23 & \quad 41 & \quad 46 \\
\end{align*}
\]

\[ p^n = 11^2 \]
- \( GF[11^2] \) Primitive root \( \gamma \) where \( \gamma^2 = 9 + 4\gamma \).
- \( LCF[11^2] \) 121 indices: \( 0, 1 \ldots 119 \).
- \( LHCf[11^2 - 1] \) 120 indices: \( 0, 1 \ldots 119 \).

\[
\begin{align*}
0 & \quad 12 & \quad 24 & \quad 36 & \quad 48 & \quad 60 & \quad 72 & \quad 84 & \quad 96 & \quad 108 \\
1 & \quad 27 & \quad 55 & \quad 58 & \quad 65 & \quad 66 & \quad 71 & \quad 80 & \quad 98 & \quad 100 & \quad 117 \\
\end{align*}
\]

\[ p^n = 2^8 \]
- \( GF[2^8] \) Primitive root \( \gamma \) where \( \gamma^2 = 1 + \gamma \).
- \( LCF[2^8] \) 8 indices: \( 0, 1 \ldots 7 \).
- \( LHCf[2^8 - 1] \) 7 indices: \( 0, 1 \ldots 7 \).

\[
\begin{align*}
0 & \quad 13 & \quad 9 & \quad 3 \quad 4 \quad 5 & \quad 6 \\
\end{align*}
\]

\[ p^n = 3^8 \]
- \( GF[3^8] \) Primitive root \( \gamma \) where \( \gamma^2 = 2 + \gamma \).
- \( LCF[3^8] \) 27 indices: \( 0, 1 \ldots 26 \).
- \( LHCf[3^8 - 1] \) 26 indices: \( 0, 1 \ldots 26 \).

\[
\begin{align*}
0 & \quad 13 & \quad 9 & \quad 15 & \quad 14 & \quad 16 & \quad 22 \\
2 & \quad 4 & \quad 6 & \quad 7 & \quad 10 & \quad 11 & \quad 12 & \quad 18 & \quad 21 \\
15 & \quad 17 & \quad 19 & \quad 20 & \quad 23 & \quad 24 & \quad 25 & \quad 5 & \quad 8 \\
\end{align*}
\]

\[ p^n = 5^8 \]
- \( GF[5^8] \) Primitive root \( \gamma \) where \( \gamma^2 = 3 + 2\gamma \).
- \( LCF[5^8] \) 125 indices: \( 0, 1 \ldots 123 \).
- \( LHCf[5^8 - 1] \) 124 indices: \( 0, 1 \ldots 123 \).

\[
\begin{align*}
0 & \quad 13 & \quad 9 & \quad 14 & \quad 26 & \quad 31 & \quad 32 & \quad 34 & \quad 41 & \quad 45 & \quad 57 & \quad 62 & \quad 63 & \quad 65 & \quad 72 & \quad 76 & \quad 88 & \quad 93 & \quad 94 & \quad 96 & \quad 103 & \quad 107 & \quad 119 \\
2 & \quad 9 & \quad 13 & \quad 26 & \quad 33 & \quad 35 & \quad 38 & \quad 39 & \quad 48 & \quad 53 & \quad 56 & \quad 68 & \quad 80 & \quad 82 & \quad 98 & \quad 104 & \quad 105 & \quad 109 & \quad 112 & \quad 114 & \quad 116 & \quad 117 & \quad 120 \\
\end{align*}
\]

\[ p^n = 7^8 \]
- \( GF[7^8] \) Primitive root \( \gamma \) where \( \gamma^2 = 2 + 2\gamma \).
- \( LCF[7^8] \) 125 indices: \( 0, 1 \ldots 123 \).
- \( LHCf[7^8 - 1] \) 124 indices: \( 0, 1 \ldots 123 \).

\[
\begin{align*}
0 & \quad 13 & \quad 9 & \quad 14 & \quad 26 & \quad 31 & \quad 32 & \quad 34 & \quad 41 & \quad 45 & \quad 57 & \quad 62 & \quad 63 & \quad 65 & \quad 72 & \quad 76 & \quad 88 & \quad 93 & \quad 94 & \quad 96 & \quad 103 & \quad 107 & \quad 119 \\
2 & \quad 9 & \quad 13 & \quad 26 & \quad 33 & \quad 35 & \quad 38 & \quad 39 & \quad 48 & \quad 53 & \quad 56 & \quad 68 & \quad 80 & \quad 82 & \quad 98 & \quad 104 & \quad 105 & \quad 109 & \quad 112 & \quad 114 & \quad 116 & \quad 117 & \quad 120 \\
\end{align*}
\]

\[ p^n = 11^8 \]
- \( GF[11^8] \) Primitive root \( \gamma \) where \( \gamma^2 = 9 + 4\gamma \).
- \( LCF[11^8] \) 121 indices: \( 0, 1 \ldots 119 \).
- \( LHCf[11^8 - 1] \) 120 indices: \( 0, 1 \ldots 119 \).

\[
\begin{align*}
0 & \quad 12 & \quad 24 & \quad 36 & \quad 48 & \quad 60 & \quad 72 & \quad 84 & \quad 96 & \quad 108 \\
1 & \quad 27 & \quad 55 & \quad 58 & \quad 65 & \quad 66 & \quad 71 & \quad 80 & \quad 98 & \quad 100 & \quad 117 \\
\end{align*}
\]

\[ p^n = 29 \]
- \( GF[29] \) Primitive root \( \gamma \) where \( \gamma^2 = 1 + \gamma \).
- \( LCF[29] \) 8 indices: \( 0, 1 \ldots 7 \).
- \( LHCf[(29 - 1)/(2 - 1)] \) 7 indices: \( 0, 1 \ldots 7 \).

\[
\begin{align*}
0 & \quad 13 & \quad 9 \\
\end{align*}
\]

\[ p^n = 39 \]
- \( GF[39] \) Primitive root \( \gamma \) where \( \gamma^2 = 2 + \gamma \).
- \( LCF[39] \) 27 indices: \( 0, 1 \ldots 26 \).
- \( LHCf[(39 - 1)/(3 - 1)] \) 13 indices: \( 0, 1 \ldots 12 \).

\[
\begin{align*}
0 & \quad 13 & \quad 9 \\
\end{align*}
\]

\[ p^n = 59 \]
- \( GF[59] \) Primitive root \( \gamma \) where \( \gamma^2 = 3 + 2\gamma \).
- \( LCF[59] \) 125 indices: \( 0, 1 \ldots 123 \).
- \( LHCf[(59 - 1)/(5 - 1)] \) 31 indices: \( 0, 1 \ldots 30 \).

\[
\begin{align*}
0 & \quad 13 & \quad 9 \\
\end{align*}
\]
CONCERNING JORDAN’S LINEAR GROUPS. [Nov.

$p^a = 7^a$

$GF[7^a]$ Primitive root $\gamma$ where $\gamma^2 = 5 + \gamma$.

$LCF[7^a]$ 343 indices *, 0, 1, ... 341.

$LHCf[7^a]$ 342 indices 0, 1, ... 341.

$[\ast 0 1 3 13 32 36 43 32 57 58 60 70 89 93 109 140 160 169 194 203 207 214 223 229 230 241 260 264 271 280 285 286 288 289 317 321 329 337]$\text{a}_9

$[2 4 6 9 14 16 20 23 25 41 44 45 46 50 56 64 75 78 82 86 99 133 134 142 148 169 181 186 194 205 209 212 216 219 222 240 245 246 267 269 277 283 290 293 296 317 321 328 337]$\text{a}_9

$[\ast 0 1 2 4 5 8 10]$\text{a}_7


$[\ast 0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 3 13 36 38 52]$\text{a}_8

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.

$[0 1 2 4 5 8 10]$\text{a}_7

$LFCf[7^a]((7^a - 1)/(7 - 1))] 57$ indices 0, 1, ... 56.
1895]

QUATERNION ASSOCIATIVE PRINCIPLE. 43

\[ p^n = 2^n \]

\begin{align*}
GF[2^n] & \quad \text{Primitive root } \gamma \text{ where } \gamma^5 = 1 + \gamma + \gamma^2 + \gamma^3.
LHCf[2^n] & \quad 32 \text{ indices } 0, 1, \ldots 30.
LHCf[2^n - 1] & \quad 31 \text{ indices } 0, 1, \ldots 30.
\end{align*}

\begin{align*}
[0 1 2 3 5 8 10 12 14 18 24 25 27 28]_{16}
[4 6 7 9 11 15 16 17 20 21 22 23 26 28 30]_{16}
LFCf[(2^n - 1)/(2 - 1)] & \quad 31 \text{ indices } 0, 1, \ldots 30.
[0 1 2 3 5 8 10 12 13 14 18 24 25 27 28]_{16}
\end{align*}

\[ p^n = 2^n \]

\begin{align*}
GF[2^n] & \quad \text{Primitive root } \gamma \text{ where } \gamma^6 = 1 + \gamma + \gamma^2 + \gamma^3 + \gamma^4.
LHCf[2^n] & \quad 64 \text{ indices } 0, 1, \ldots 62.
LHCf[2^n - 1] & \quad 63 \text{ indices } 0, 1, \ldots 62.
\end{align*}

\begin{align*}
[0 1 2 3 4 6 13 14 15 18 20 21 22 23 24 25 26 31 35 37 40 42 43 46 49
50 51 53 54 56 57 58 59]_{32}
[5 7 8 9 10 11 12 15 17 19 23 24 27 28 29 30 32 33 34 36 38 39 41
44 45 47 48 52 55 60 61 62]_{32}
LFCf[(2^n - 1)/(2 - 1)] & \quad 63 \text{ indices } 0, 1, \ldots 62.
[First line above, omitting the \#]_{31}
\end{align*}

The University of Chicago,
August 25, 1895.

ELEMENTARY PROOF OF THE QUATERNION ASSOCIATIVE PRINCIPLE.*

BY PROFESSOR ARTHUR S. HATHAWAY.

The variety of demonstrations that Hamilton has given of the associative principle of quaternion multiplication, and the remarks that he has made upon such demonstrations, show that he considered an elementary proof of this principle as very desirable. Only two of Hamilton’s proofs have been generally employed by subsequent writers—the direct proof by spherical conics, and the indirect one depending upon the assumed laws of i, j, k—and the proof that he considered the most elementary has been entirely ignored, probably because of its deviation from fundamental ideas. On page 297 of the Elements, Hamilton calls attention to another method, as follows: “The associative principle of multiplication may also be proved without the distributive principle, by certain considerations of rotations of a system, on which we cannot enter here.”

It is, of course, easy to see that such a proof is possible; but the details of it could not have presented themselves to Hamilton in an elementary form, or he would have seen that it

* Presented to the American Mathematical Society August 28, 1895.