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 $s_1 =$ identity, $s_2, \ldots s_n$. The substitution-group Γ^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 Γ^n must as elements of G_n have the same period. Thus, $s_1 =$ identity is invariant, and Γ^n is really Γ^{n-1} on the $n-1$ letters $s_2, \ldots s_n$.

We are to consider to-day the case that *Γ^{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 Γ^{n-1}. But Γ^{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 ′, *G_{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}*.

---

* *Bulletin of the American Mathematical Society*, ser. 2, vol. 1, pp. 61–66, Dec. 1894.

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^3, pq^2, pqr, p^4* (*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. 66 of my former paper.

† SYLOW: *Mathematische Annalen*, vol. 5, p. 588.

§ 1.

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

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

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

with the complete system of generating relations.

$$(2)\qquad a_i^p=1, \qquad a_ia_j=a_ja_i \qquad (i,j=1,2,\ldots n)$$

and have as the general element

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

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

$$(4)\qquad s_{K_1}s_{K_2}=s_{K_3}, \quad s_{k_{11},k_{12},\ldots k_{1n}}\cdot s_{k_{21},k_{22},\ldots k_{2n}}=s_{k_{31},k_{32},\ldots k_{3n}},$$

where

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

It turns out that the general substitution σ_G of $\Gamma^{p^n}_{\Omega(p^n)}$ rereplaces $s_X=s_{x_1,x_2,\ldots x_n}$ by $s_{X'}=s_{x'_1,x'_2,\ldots x'_n}$, where

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

where $\boldsymbol{G}$ is a symbol for the matrix

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

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, $\Gamma^{p^n}_{\Omega(p^n)}$ is *Jordan's* linear homogeneous substitution-group * of degree p^n, $LHG^{p^n}_{\Omega(p^n)}$, of order †

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

---

* JORDAN: *Traité des substitutions*, p. 92, 1870.
† JORDAN: loc. cit., p. 97.

This identification of the $\Gamma^{p^n}_{\Omega(p^n)}$ of the Abelian G_{p^n} with the $LHG^{p^n}_{\Omega(p^n)}$ I obtain first by holding the G_{p^n} as an *abstract* group; I omit the details of this identification. We may however take the G_{p^n} *concretely* as the *regular* Abelian substitution-group $G^{p^n}_{p^n}$ on the p^n letters $s_X = s_{x_1, x_2, \ldots x_n}$; the general element (3) $s_K = s_{k_1, k_2, \ldots k_n}$ then (4, 5) replaces s_X by $s_{X'}$, where

$$(9) \qquad X' = X + K, \quad x'_i = x_i + k_i \qquad (i = 1, 2, \ldots n).$$

We thus win direct contact with Mr. *Jordan's* work. The $G^{p^n}_{p^n}$ (9) is within the symmetric substitution-group on the p^n letters s_X self-conjugate under the linear non-homogeneous group $LG^{p^n}_{p^n\Omega(p^n)}$ of degree p^n and of order $p^n\Omega(p^n)$, whose general substitution $\sigma_{G, K}$ replaces s_X by $s_{X'}$, where

$$(10) \quad X' = GX + K, \quad x'_i = \sum_{j=1}^{j=n} g_{ij}x_j + k_i \quad (|g_{ij}| \neq 0) \quad (i, j = 1, 2, \ldots n).$$

$\sigma_{G, K}$ replaces $s_{K_1}, s_{K_2}, s_{K_3}$ by $s_{K'_1}, s_{K'_2}, s_{K'_3}$, where

$$K'_1 = GK_1 + K, \quad K'_2 = GK_2 + K, \quad K'_3 = GK_3 + K,$$

so that

$$K'_1 + K'_2 - K'_3 = G(K_1 + K_2 - K_3) + K;$$

hence under $\sigma_{G, K}$ of the $LG^{p^n}_{p^n\Omega(p^n)}$ (10) a multiplication equation of the G_{p^n} $s_{K_1}s_{K_2} = s_{K_3} = s_{K_1+K_2}$ (4, 5) is preserved, that is,

$$s_{K'_1}s_{K'_2} = s_{K'_3} = s_{K'_1+K'_2},$$

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 $LG^{p^n}_{p^n\Omega(p^n)}$ (10) is a substitution $\sigma_{G, 0} = \sigma_G$ of the $LHG^{p^n}_{\Omega(p^n)}$ (6). We have then this (second) identification of the $\Gamma^{p^n}_{\Omega(p^n)}$ of the Abelian G_{p^n} with the $LHG^{p^n}_{\Omega(p^n)}$.

The group $\Gamma^{p^n}_{\Omega(p^n)} \equiv LHG^{p^n}_{\Omega(p^n)}$ (6) 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 $s_X = s_{x_1, x_2, \ldots x_n}$ belongs to and by the ratios of its n suffixes $\underset{\cdot\cdot}{X} = (x_1 : x_2 : \cdots : x_n)$ determines the system of imprimitivity containing the $q-1$ letters* $s_{lX} (l = 1, 2, \cdots \overline{p-1})$; in the G_{p^n} the elements s_{lX} and the identity $s_{0X} = s_{(0)}$ constitute the cyclic group $G_p\{s_X\}$ determined by s_X, say the $G_{p, \underset{\cdot\cdot}{X}}$. Thus,

* $X = (x_1, \cdots x_n), \ lX = (lx_1, \cdots lx_n)$.

the $\Gamma^{p^n}_{\Omega(p^n)} \equiv LHG^{p^n}_{\Omega(p^n)}$ permutes first the $(p^n-1)/(p-1)$ G_p of G_{p^n}, and afterwards fixes the elements within the various groups. The self-conjugate sub-group which keeps every G_p fixed is of order $p-1$:

$$(11) \qquad \{X' = lX, \quad x'_i = lx_i \, (i = 1, 2, \cdots n)\}, \qquad (l = 1, 2, \cdots \overline{p-1}).$$

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 $LHG^{p^n}_{\Omega(p^n)}$ taken fractionally; that is, the linear fractional group† $LFG^{(p^n-1)/(p-1)}_{\Omega(p^n)/(p-1)}$, whose general substitution $\sigma_{\ddot{G}}$ replaces the $G_{p,\ddot{X}}$ by the $G_{p,\ddot{X}'}$, where

$$(12) \qquad \ddot{X}' = \ddot{G}\ddot{X},^*$$

$$x'_1 : x'_2 : \cdots : x'_i : \cdots : x'_n = \sum_{j=1}^{j=n} g_{1j}x_j : \sum_{j=1}^{j=n} g_{2j}x_j : \cdots : \sum_{j=1}^{j=n} g_{ij}x_j : \cdots : \sum_{j=1}^{j=n} g_{nj}x_j.$$

§ 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:

$$LG^{p^n}_{p^n\Omega(p^n)}, \quad LHG^{p^n \text{ or } p^n-1}_{\Omega(p^n)}, \quad LFG^{(p^n-1)/(p-1)}_{\Omega(p^n)/(p-1)}$$

The notion *configuration* I transfer to tactic from geometry†; 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_X 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 $X = (x_1, \cdots x_n)$, $X' = (x'_1, \cdots x'_n)$, $G = (g_{ij})$ by $lX = (lx_1, \cdots lx_n)$, $l'X' = (l'x'_1, \cdots l'x'_n)$, $mG = (mg_{ij})$, respectively, where l, l', m are any integers taken modulo p, but $l \neq 0$, $l' \neq 0$, $m \neq 0$.

† See, for instance, Reye: *Das Problem der Configurationen* (*Acta Mathematica*, vol. 1, pp. 92–96, 1882).

$G_{p^{n-1}}$. With respect to each sub-group $G_{p^{n-1}}$ the p^n elements s_X of the G_{p^n} 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 $G_{p^{n-1}}$ 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 $n \geqq 2$ defines, as the maximum substitution-group on the p^n letters s_X leaving it invariant, exactly the $LG^{p^n}_{p^n\Omega(p^n)}$ (§ 1 (10)).

The linear homogeneous configuration $LHCf[p^n-1]$ in 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_{p^n}, 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 $n \geqq 2$ serves as a defining invariant for exactly the $LHG^{p^n \text{ or } p^n-1}_{\Omega(p^n)}$ (§ 1, (6)). The self-reciprocity of the $LHCf[p^n-1]$ establishes an holoedric isomorphism of the $LHG^{p^n-1}_{\Omega(p^n)}$ with itself. This isomorphism is (at least for $n \geqq 3$) *not** that arising from a transformation of the $LHG^{p^n-1}_{\Omega(p^n)}$ through one of its own elements.

The linear fractional configuration $LFCf[(p^n-1)/(p-1)]$ on $(p^n-1)/(p-1)$ 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 $G_{q;\,X}$ of the Abelian G_{p^n}. 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 Δ_7 are, so to say, complementary. Indeed, for $q=2$, $n=$ any, the $LHCf[2^n-1]$ determines uniquely a Δ_{2^n-1}, from which the $LHCf[2^n-1]$ is likewise uniquely determined. This Δ_{2^n-1} serves as a defining invariant for the $LHG^{2^n-1}_{\Omega(2^n)}$.

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 $\overline{p-1}$ letters s_{lX} $(l=1, 2, \ldots \overline{q-1})$ by the letter $G_{q;\,X}$. The $LFCf[(p^n-1)/(p-1)]$ 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 $LFCf[(p^n-1)/(p-1)]$ is tactically self-reciprocal.

This $LFCf[(p^n-1)/(p-1)]$ for $n \geqq 3$ serves as a defining invariant for exactly the $LFG^{(p^n-1)/(p-1)}_{\Omega(p^n)/(p-1)}$ (§ 1, (12)). The self-reciprocity of the $LFCf[(p^n-1)/(p-1)]$ $(n \geqq 3)$ establishes an holoedric isomorphism of the $LFG^{(p^n-1)/(p-1)}_{\Omega(p^n)/(p-1)}(n \geqq 3)$ with itself. This isomorphism is *not* that arising from a transformation of the $LFG^{(p^n-1)/(p-1)}_{\Omega(p^n)/(p-1)}$ through one of its own elements.

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

§ 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* $\Gamma^{p^n-1}_{\Omega(p^n)} \equiv LHG^{p^n-1}_{\Omega(p^n)}$ *contains a substitution* σ_G *which permutes the* p^n-1 *letters* $s_X (X \neq (0))$ *in one cycle of period* p^n-1. Any such σ_G 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_{p^n}.

† GALOIS: *Sur la théorie des nombres* (*Bulletin des Sciences Mathématiques* de M. Ferussac, vol. 13, p. 428, 1830; reprinted, *Journal de Mathématiques pures et appliquées*, vol. 11, pp. 398–407, 1846.)

SERRET: *Algèbre supérieure*, fifth edition, vol. 2, pp. 122–189.

JORDAN: *Traité des substitutions*, pp. 14–18.

MOORE: *A doubly infinite system of simple groups* (§ 3 is an abstract formulation of the Galois-field theory). (*Proceedings of the Chicago Congress of Mathematics*; in abstract, *Bulletin of the New York Mathematical Society*, vol. 3, Dec. 1893.)

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 invariables* (*Journal de Mathématiques pures et appliquées*, ser. 2, vol. 6, pp. 241–323, 1861), working from the Galois-field standpoint, defines and investigates two substitution-groups, which are (otherwise expressed) the groups $LG^{p^n}_{p^n\Omega(p^n)}$ and $LHG^{p^n}_{\Omega(p^n)}$. 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 ξ of the Galois-field $GF[p^n]$ of order p^n are exhibited explicitly in terms of n linearly independent marks $\eta_1, \eta_2, \cdot \cdot \eta_n$ in the form

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

where the x_i's are integral marks, or integers taken modulo p. We make through the $X = (x_1, \cdot \cdot x_n)$ a 1.1 correspondence between the letters s_X and the marks ξ. In fact the $GF[p^n]$ quâ additive-group is a concrete Abelian G_{p^n}. Now in the $GF[p^n]$ additions are invariant under the multiplication-substitution σ_γ on the $p^n - 1$ marks ξ $(\xi \neq 0)$,

$$(2) \qquad \xi' = \gamma \xi, \quad (\gamma \neq 0),$$

that is, when every mark of the field is multiplied by the same mark γ. Hence this σ_γ interpreted on the s_X is a substitution σ_G of the $\Gamma^{p^n-1}_{\Omega(p^n)} \equiv LHG^{p^n-1}_{\Omega(p^n)}$. If γ is a primitive root of the $GF[p^n]$, σ_γ permutes the $p^n - 1$ marks $\xi (\xi \neq 0)$ in one cycle, and, similarly, σ_G 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 Γ^7_{168} by the triple system Δ_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 $p^n = 2^2, 3^2, 5^2, 7^2, 11^2;\ 2^3, 3^3, 5^3, 7^3;\ 2^4, 3^4, 5^4;\ 2^5;\ 2^6$.

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

---

letters s_X, each of which serves as defining invariant for the $LG^{p^n}_{p^n(p\Omega^n)}$. 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 coöperation, 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 ($i=0, 1, \ldots \overline{p^n-1}$); 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

$$i'=i+1, \qquad (i=0, 1, \cdot\cdot \overline{p^n-1}),$$

which leaves $*$ fixed. The first line of the first array is the additive sub-group $G_{p^{n-1}}$ of the $GF[p^n]$ quâ additive G_{p^n}, which contains the $n-1$ marks $\gamma^0, \gamma^1, \cdot\cdot \gamma^{n-2}$. The second line is obtained by adding the *mark* γ^{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.†

$[p^n=2^2]$	$GF[2^2]$	Primitive root γ where $\gamma^2=1+\gamma$.
	$LCf[2^2]$	4 indices $*$ 0 1 2.
	$LHCf[2^2-1]$	3 indices 0 1 2.

$[*\ 0]_2 \quad [1\ 2]_2$ §

$[p^n=3^2]$	$GF[3^2]$	Primitive root γ where $\gamma^2=1+2\gamma$.
	$LCf[3^2]$	9 indices $*$ 0 1 . . 7.
	$LHCf[3^2-1]$	8 indices 0 1 . . 7.

$[*\ 0\ 4]_3 \quad [1\ 6\ 7]_3 \quad [2\ 3\ 5]_3$

$[p^n=5^2]$	$GF[5^2]$	Primitive root γ where $\gamma^2=2+2\gamma$.
	$LCf[5^2]$	25 indices $*$ 0 1 . . 23.
	$LHCf[5^2-1]$	24 indices 0 1 . . 23.

$[*\ 0\ 6\ 12\ 18]_5 \quad [1\ 3\ 4\ 8\ 17]_5 \quad [7\ 9\ 10\ 14\ 23]_5 \quad [5\ 13\ 15\ 16\ 20]_5$
$[2\ 11\ 19\ 21\ 22]_5$

---

* The s_X notation for the elements can be recovered if necessary.

† The $LFCf\left[\frac{p^n-1}{p-1}\right]$ for $n=2$ is trivial and hence is not tabulated.

§ Every *line* [ ] has a suffix indicating the number of *indices* lying within.

$[p^n = 7^2]$ $GF[7^2]$ Primitive root γ where $\gamma^2 = 2 + 2\gamma$.
$LCf[7^2]$ 49 indices * 0 1 . . 47.
$LHCf[7^2 - 1]$ 48 indices 0 1 . . 47.

$[* \ 0\ 8\ 16\ 24\ 32\ 40]_7$
$[1\ 6\ 18\ 20\ 21\ 27\ 31]_7$ $[9\ 14\ 26\ 28\ 29\ 35\ 39]_7$ $[17\ 22\ 34\ 36\ 37\ 43\ 47]_7$
$[3\ 7\ 25\ 30\ 42\ 44\ 45]_7$ $[2\ 4\ 5\ 11\ 15\ 33\ 38]_7$ $[10\ 12\ 13\ 19\ 23\ 41\ 46]_7$

$[p^n = 11^2]$ $GF[11^2]$ Primitive root γ where $\gamma^2 = 9 + 4\gamma$.
$LCf[11^2]$ 121 indices * 0 1 . . 119.
$LHCf[11^2 - 1]$ 120 indices 0 1 . . 119.

$[* \ 0\ 12\ 24\ 36\ 48\ 60\ 72\ 84\ 96\ 108]_{11}$
$[1\ 27\ 55\ 58\ 65\ 66\ 71\ 80\ 98\ 100\ 117]_{11}$
[Second line] + 12; 24; 36; 48; 60; 72; 84; 96; 108 = the respective remaining lines.

$[p^n = 2^3]$ $GF[2^3]$ Primitive root γ where $\gamma^3 = 1 + \gamma$.
$LCf[2^3]$ 8 indices *, 0, 1, . . 7.
$LHCf[2^3 - 1]$ 7 indices 0, 1, . . 7.

$[* \ 0\ 1\ 3]_4$ $[2\ 4\ 5\ 6]_4$

$LFCf[(2^3 - 1)/(2 - 1)]$ 7 indices 0, 1, . . 7.

$[0\ 1\ 3]_3$

$[p^n = 3^3]$ $GF[3^3]$ Primitive root γ where $\gamma^3 = 2 + \gamma$.
$LCf[3^3]$ 27 indices *, 0, 1, . . 25.
$LHCf[3^3 - 1]$ 26 indices 0, 1, . . 25.

$[* \ 0\ 1\ 3\ 9\ 13\ 14\ 16\ 22]_9$
$[2\ 4\ 6\ 7\ 10\ 11\ 12\ 18\ 21]_9$
$[15\ 17\ 19\ 20\ 23\ 24\ 25\ 5\ 8]_9$

$LFCf[(3^3 - 1)/(3 - 1)]$ 13 indices 0, 1, . . 12.

$[0\ 1\ 3\ 9]_4$

$[p^n = 5^3]$ $GF[5^3]$ Primitive root γ where $\gamma^3 = 3 + 2\gamma$.
$LCf[5^3]$ 125 indices *, 0, 1, . . 123.
$LHCf[5^3 - 1]$ 124 indices 0, 1, . . 123.

$[* \ 0\ 1\ 3\ 10\ 14\ 26\ 31\ 32\ 34\ 41\ 45\ 57\ 62\ 63\ 65\ 72\ 76\ 88\ 93\ 94\ 96\ 103\ 107\ 119]_{25}$
$[2\ 9\ 13\ 15\ 28\ 29\ 30\ 35\ 38\ 39\ 48\ 53\ 56\ 68\ 80\ 82\ 98\ 104\ 105\ 109\ 112\ 114\ 116\ 117\ 120]_{25}$
[Second line] + 31; 62; 93 = the respective remaining lines.

$LFCf[(5^3 - 1)/(5 - 1)]$ 31 indices 0, 1, . . 30.

$[0\ 1\ 3\ 10\ 14\ 26]_6$

$[p^n = 7^3]$ $GF[7^3]$ Primitive root γ where $\gamma^3 = 5 + \gamma$.
$LCf[7^3]$ 343 indices $*$, 0, 1, . . 341.
$LHCf[7^3 - 1]$ 342 indices 0, 1, . . 341.

[* 0 1 3 13 32 36 43 52 57 58 60 70 89 93 100 109 114 115 117 127 146 150 157 166 171 172 174 184 203 207 214 223 228 229 231 241 260 264 271 280 285 286 288 298 317 321 328 337]$_{49}$

[2 4 6 9 14 16 26 33 35 41 44 45 46 50 56 64 75 78 82 86 99 133 134 142 148 168 181 186 194 195 201 202 218 219 222 240 245 265 267 268 277 281 283 290 293 296 307 312 323]$_{49}$

[Second line] + 57; 114; 171; 228; 285 = the respective remaining lines.

$LFCf[(7^3 - 1)/(7 - 1)]$ 57 indices 0, 1, . . 56.

[0 1 3 13 32 36 43 52]$_8$

$[p^n = 2^4]$ $GF[2^4]$ Primitive root γ where $\gamma^4 = 1 + \gamma$.
$LCf[2^4]$ 16 indices $*$, 0, 1, . . 14.
$LHCf[2^4 - 1]$ 15 indices 0, 1, . . 14.

[* 0 1 2 4 5 8 10]$_8$ [3 6 7 9 11 12 13 14]$_8$

$LFCf[(2^4 - 1)/(2 - 1)]$ 15 indices 0, 1, . . 14.

[0 1 2 4 5 8 10]$_7$

$[p^n = 3^4]$ $GF[3^4]$ Primitive root γ where $\gamma^4 = 1 + \gamma + 2\gamma^2 + 2\gamma^3$.
$LCf[3^4]$ 81 indices $*$, 0, 1, . . 79.
$LHCf[3^4 - 1]$ 80 indices 0, 1, . . 79.

[* 0 1 2 5 12 18 22 24 26 27 29 32 33 40 41 42 45 52 58 62 64 66 67 69 72 73]$_{27}$

[3 7 15 17 20 21 30 31 37 38 44 46 48 49 50 51 53 54 56 59 63 65 68 74 75 76 79]$_{27}$

[Second line] + 40.

$LFCf[(3^4 - 1)/(3 - 1)]$ 40 indices 0, 1, . . 39.

[0 1 2 5 12 18 22 24 26 27 29 32 33]$_{13}$

$[p^n = 5^4]$ $GF[5^4]$ Primitive root γ where $\gamma^4 = 2 + \gamma + \gamma^2$.
$LCf[5^4]$ 625 indices $*$, 0, 1, . . 623.
$LHCf[5^4 - 1]$ 624 indices 0, 1, . . 623.

[* {0 1 2 7 18 19 23 36 43 44 46 47 55 57 61 64 70 76 77 84 86 89 92 94 96 108 119 122 143 148 152} + 0, 156, 312, 468]$_{125}$

[3 4 5 10 17 21 22 29 31 37 39 41 42 59 63 68 74 88 95 99 104 107 109 110 127 130 134 141 146 153 162 165 168 169 181 186 189 190 191 194 196 207 208 216 218 221 222 225 229 231 237 239 241 261 262 269 270 271 272 276 277 279 281 285 287 288 289 291 294 300 305 306 323 328 332 336 338 361 362 365 366 379 383 390 399 402 405 410 412 413 415 424 430 438 440 451 454 467 476 482 483 495 496 500 513 516 524 526 540 547 548 550 559 565 570 579 585 592 604 605 608 613 615 619 622]$_{125}$

[Second line] + 156; 312; 468 = the respective remaining lines.

$LFCf[(5^4 - 1)/(5 - 1)]$ 156 indices 0, 1, . . 155.

[The { } of first line above]$_{31}$

$[p^n = 2^5]$ $GF[2^5]$ Primitive root γ where $\gamma^5 = 1 + \gamma + \gamma^2 + \gamma^3$.
$LCf[2^5]$ 32 indices $*$, 0, 1, . . 30.
$LHCf[2^5 - 1]$ 31 indices 0, 1, . . 30.

[* 0 1 2 3 5 8 10 12 13 14 18 24 25 27 28]$_{16}$
[4 6 7 9 11 15 16 17 19 20 21 22 23 26 29 30]$_{16}$

$LFCf[(2^5 - 1)/(2 - 1)]$ 31 indices 0, 1, . . 30.

[0 1 2 3 5 8 10 12 13 14 18 24 25 27 28]$_{15}$

$[p^n = 2^6]$ $GF[2^6]$ Primitive root γ where $\gamma^6 = 1 + \gamma + \gamma^3 + \gamma^4$.
$LCf[2^6]$ 64 indices $*$, 0, 1, . . 62.
$LHCf[2^6 - 1]$ 63 indices 0, 1, . . 62.

[* 0 1 2 3 4 6 13 14 16 18 20 21 22 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]$_{32}$

$LFCf[(2^6 - 1)/(2 - 1)]$ 63 indices 0, 1, . . 62.

[First line above, omitting the *]$_{31}$

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.