3. A mark for each face, and a list of the edges and vertices in their order upon the boundary of each face.

Such a notation must contain a mark of distinction for the two sides of an edge; an easy matter if the direction of positive rotation be adopted uniformly in listing arrangements about the vertices and faces respectively.

These processes, and the proved existence of fundamental polygons, open a range of particular problems of considerable interest. But of even superior interest must be, at least until it is solved, the problem of finding a method for constructing, a priori, upon a given surface the exceptional (Davis) special reticulations whose characteristics are given by the restrictive tables.

NORTHWESTERN UNIVERSITY, April, 1898.

SYSTEMS OF SIMPLE GROUPS DERIVED FROM THE ORTHOGONAL GROUP.

BY DR. L. E. DICKSON.

1. In the February number of the BULLETIN I determined the order ω of the group G of orthogonal substitutions of determinant unity on m indices in the $GF[p^n]$ and proved that, for $p^n > 5$, p + 2, the group is generated by the substitutions

$$O_{i,j}^{\alpha,\beta}: \begin{array}{c} \xi_i' = a\xi_i + \beta\xi_j, \\ \xi_j' = -\beta\xi_i + a\xi_j, \end{array} (a^2 + \beta^2 = 1).$$

The structure of G was determined for the case p = 2. I have since proved[†] that for every m > 4 and every $p^n > 5$ of the form 8l + 3 or 8l + 5, the factors of composition of G

$$W = \begin{pmatrix} 1 & 2 & 2 & 2 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}, W^{3} = 1.$$

[†]A preliminary account was presented before the Mathematical Conference at Chicago, December 30, 1897.

^{*} The fact that $p^n = 3$ is an exception was not pointed out in the BULLETIN. In fact Jordan had not proven case 2^o of § 211 when -1 = square, so that the case $a^2 = b^2 = c^2 = \dots = 1$ was unsolved when p = 3, m = 3k + 1. The theorem is readily proven when $p^n = 3^n$, n > 1; but for $p^n = 3$ an additional generator is necessary and sufficient, viz.,

1898.7

are 2 and $\omega/2$ for *m* odd, and 2, 2, $\omega/4$ for *m* even. [For later results on the cases thus excluded see §§ 11–15.]

For m odd, the orthogonal group G had the same order and factors of composition as the linear Abelian group on m-1 indices. Judging from the results for the corresponding continuous groups of Lie, the resulting triply-infinite systems of simple groups of the same order $\omega/2$ are probably isomorphic when m = 3, but not when m > 3. [See § 14.]

Excluding here the cases m = 5, 6, 7, which require lengthy special investigations, I will now give a short, simple proof of the above result. The complete memoir will appear in the *Proceedings of the California Academy of Sciences.**

The substitutions $O_{1,2}^{\alpha,\beta}$ form a commutative group of order† $p^n \pm 1$. A subgroup of index 2 is formed by the substitutions

$$\begin{split} Q^{a,\beta}_{1,2}: \quad & \xi_1' = (a^2 - \beta^2) \; \xi_1 - 2a\beta \xi_2, \\ & \xi_2' = 2a\beta \xi_1 + (a^2 - \beta^2) \xi_2. \end{split}$$

Indeed,

$$Q_{1,2}^{\gamma,\delta} Q_{1,2}^{\alpha,\beta} = Q_{1,2}^{\alpha\gamma-\beta\delta, \alpha\delta+\beta\gamma}.$$

Further, its order is $\frac{1}{2}(p^n \pm 1)$ since $Q_{1,2}^{\alpha,\beta}$ and $Q_{1,2}^{\gamma,\delta}$ are identical if and only if $\alpha = \pm \gamma$, $\beta = \pm \delta$.

If C_i denotes the substitution affecting only the index ξ_i , whose sign it changes, $C_1 C_2$ is always contained among the substitutions $Q_{1, 2}^{\alpha, \beta}$.

Since we suppose that $p^n = 8l \pm 3$, 2 is a not-square. Thus, with $a^2 + \beta^2 = 1$, we cannot have $a^2 - \beta^2 = 0$. Hence if T_{12} denotes the transposition $(\xi_1 \xi_2)$, $T_{12}C_1$ is not of the form $Q_{1,\beta}^{i,\beta}$ but serves to extend the group of the latter to the group of the $O_{1,\beta}^{a,\beta}$. Furthermore, if j > 2, $T_{12}C_1$ transforms $Q_{1,\beta}^{a,\beta}$ into $Q_{2,\beta}^{a,\beta}$ and $Q_{2,\beta}^{a,\beta}$ into $Q_{1,\beta}^{a,\beta-\beta}$. Hence if we extend the alternating group on the *m* letters ξ_i by the substitutions $Q_{1,\beta}^{a,\beta}$ we obtain a group *H* of index 2 under *G*.

3. THEOREM: For $p^n > 5$, m > 7, the maximal invariant subgroup of H is of order 2 or 1 according as m is even or odd.

For m even, H contains an invariant subgroup of order 2 generated by the substitution

$$N: \quad \xi_i' = -\xi_i \quad (i = 1, \cdots, m).$$

Suppose H has an invariant subgroup I containing a substitution

^{*} Third Series, vol. 1, No. 4; the later results in No. 5.

^{† &}quot;Orthogonal Group in a Galois Field," & 3; BULLETIN, February, 1898, pp. 196-200.

$$S: \qquad \xi_i' = \sum_{j=1}^m a_{ij}\xi_j \quad (i=1,\cdots,m),$$

neither the identity nor N. By suitably transforming S, we can suppose that $a_{11}^2 + a_{21}^2 + 1$. Then S is not commutative with C_1C_2 ; for, if so, it would be merely a product of **a** substitution affecting only ξ_1 and ξ_2 by a substitution affecting only ξ_3, \dots, ξ_m . Hence the group I contains the substitution, not the identity,

$$S^{-1} C_1 C_2 S C_1 C_2 = S_a C_1 C_2,$$

where $S_a \equiv S^{-1} C_1 C_2 S$, of period two, is found to be

$$\xi_i' = \xi_i - 2a_0 \sum_{j=1}^m a_{j1} \xi_j - 2a_{i2} \sum_{j=1}^m a_{j2} \xi_j \quad (i = 1, \cdots, m).$$

4. Lemma: The orthogonal substitution

$$\begin{split} \xi_i' &= \lambda \ \xi_i + \mu \ \xi_j + \nu \ \xi_k, \\ O_{ijk}: \ \xi_j' &= \lambda' \ \xi_i + \mu' \ \xi_j + \nu' \ \xi_k, \\ \xi_k' &= \lambda'' \ \xi_i + \mu'' \ \xi_i + \nu'' \ \xi_k, \end{split}$$

where $\lambda^2 + \mu^2 + \nu^2 = 1$, $\lambda\lambda' + \mu\mu' + \nu\nu' = 0$, etc., transforms S_{α} into $S_{\alpha'}$ where

$$\begin{aligned} a_{il}' &= \lambda \ a_{il} + \mu \ a_{jl} + \nu \ a_{kl}, \\ a_{jl}' &= \lambda' \ a_{il} + \mu' \ a_{jl} + \nu' \ a_{kl}, \\ a_{kl}' &= \lambda'' a_{il} + \mu'' \ a_{jl} + \nu'' \ a_{kl}, \\ a_{sl}' &= a_{sl}, \quad (s = 1, \cdots, m, s + i, j, k). \end{aligned}$$

If $a_{i1} \neq 0$, we can choose λ , μ , ν such that $a_{i1}' = 0$. For if $a_{i1}^2 + a_{j1}^2 = 0$ and therefore $a_{j1} \neq 0$, we may take

$$\lambda = \frac{-a_{k1}}{2a_{i1}}, \quad \mu = \frac{-a_{k1}}{2a_{j1}}, \quad \nu = 1.$$

If $a_{i1}^2 + a_{j1}^2 \neq 0$, we derive the equivalent condition,

$$\{\mu(a_{i1}^2+a_{j1}^2)+\nu a_{j1}a_{k1}\}^2+\nu^2 a_{i1}^2(a_{i1}^2+a_{j1}^2+a_{k1}^2)=a_{i1}^2(a_{i1}^2+a_{j1}^2),$$

which has solutions* for μ and ν in the $GF[p^n]$ except when $a_n^2 + a_{j_1}^2 + a_{k_1}^2 = 0$. In the latter case the condition $\lambda^2 + \mu^2 + \nu^2 = 1$ may be written

$$a_{i1}^2 = - (\mu a_{k1} - \nu a_{j1})^2,$$

having solutions if and only if -1 be a square.

 $\mathbf{384}$

^{*} BULLETIN, l.c. § 3.

1898.]

5. Lemma: O_{iikl} transforms S_a into $S_{a'}$, where

$$a_{i1}' = \lambda a_{i1} + \mu a_{j1} + \nu a_{k1} + \sigma a_{i1}.$$

If $a_{i1}^2 + a_{j1}^2 + a_{k1}^2 = 0$, the values

$$\lambda = \frac{-a_n}{a_n}, \quad \mu = \frac{a_{\mu}a_{\mu}}{a_{i1}^2}, \quad \nu = \frac{-a_na_{\mu}}{a_{i1}^2}, \quad \sigma = 1$$
$$a_{i1}' = 0, \quad \lambda^2 + \mu^2 + \nu^2 + \sigma^2 = 1$$

make

6. The invariant subgroup I of H was shown to contain the substitution $S' \equiv S_{\alpha} C_1 C_2$ not the identity. Transforming S' successively by

$$O_{i345}$$
 or $T_{12} C_1 O_{i345} (i=m, m-1, \cdots, 6)$,

according as the one or the other belongs to H, we obtain, by §§ 4-5, a substitution $S_{a'} C_1 C_2$ belonging to I, we obtain, $a_{m1}' = a_{m-1'1} = \cdots = a_{61}' = 0$. Also, by §4, we may make $a_{51}' = 0$; for we have

$$a_{11}{}^{\prime 2} + a_{21}{}^{\prime 2} = a_{11}{}^{2} + a_{21}{}^{2} + 1,$$

$$a_{51}{}^{\prime 2} + a_{41}{}^{\prime 2} + a_{31}{}^{\prime 2} + 0.$$

so that

Next we transform $S_a \cdot C_1 C_2$ successively by

$$O_{j567}$$
 $(j = m, m - 1, \cdots, 8)$

and obtain in I a substitution $S_{\alpha''}C_1C_2$ having

$$a_{j_1}{}'' \equiv a_{j_1}{}' = 0, \quad a_{j_2}{}'' = 0 \quad (j = m, \cdots, 8).$$

The group I thus contains a substitution

S:
$$\xi_{i}' = \sum_{j=1}^{7} \beta_{ij} \xi_{j}$$
 $(i = 1, \dots, 7)$

neither the identity nor $N \equiv C_1 C_2 \cdots C_m$. 7. If S be commutative with every C_i , it is merely **a** product of an even number of the C_i , in which certain ones as C_k are lacking. But if

$$S = C_i C_j C_r C_s C_i \cdots,$$

the group I contains

1

$$T_{ij}T_{ik}ST_{ik}T_{ij}S^{-1} = C_kC_j,$$

and hence, by transforming by suitable even substitutions, every product of two C's. But H contains either $O_{1,2}^{\alpha,\beta}$ or $O_{1,\frac{\beta}{2}}^{\alpha,\beta}T_{12}^{-}C_1$, which transform C_1C_3 into $Q_{1,\frac{\beta}{2}}^{\alpha,\beta}C_1C_3$ and $Q_{1,\frac{\beta}{2}}^{\alpha,\beta}C_2C_3$ respectively. Hence the group I contains every $Q_{1,2}^{a,\beta}$, among which, if $p^n > 5$, occurs one different from the identity and from C_1C_2 . 8. We may thus assume that S is not commutative with

8. We may thus assume that S is not commutative with C_1 , for example. Supposing $m \equiv 8$, S is commutative with C_8 . Hence the group I contains the substitution not the identity

$$S^{-1}C_1C_8SC_1C_8 = R_\beta C_1,$$

where $R_{\beta} \equiv S^{-1}C_1S$ is seen to be

$$R_{\beta}: \quad \xi_{i}' = \xi_{i} - 2\beta_{i1} \sum_{i=1}^{7} \xi_{j1} \xi_{j} \quad (i = 1, \cdots, 7).$$

Transforming $R_{\beta}C_1$ by O_{i234} for i = 7, 6, 5 successively, we may suppose that $\beta_{\tau_1} = \beta_{\epsilon_1} = \beta_{\epsilon_1} = 0$. It is readily seen that a substitution R affecting only

It is readily seen that a substitution R affecting only ξ_1, \dots, ξ_4 , is not commutative with every T_{ij} $(i, j = 1, \dots, 5)$ for example not with T_{12} . Then I contains the substitution, not the identity,

$$R^{-1}T_{12}T_{67}RT_{67}T_{12} = T_{\delta}T_{12},$$

where $T_{\delta} \equiv R^{-1} T_{12} R$ has the form

$$T_{\delta}: \quad \xi_i' = \xi_i - \delta_i \sum_{j=1}^4 \delta_j \xi_j \quad (i = 1 \cdots 4),$$

 $\delta_{1}^{2} + \delta_{2}^{2} + \delta_{3}^{2} + \delta_{4}^{2} = 2.$

where

9. If $\delta_3 = \delta_4 = 0$, $T_{\delta} T_{12}$ becomes $Q_{2,1}^{a,\beta}$ if we set

$$\alpha = \frac{1}{2}(\delta_1 - \delta_2), \quad \beta = \frac{1}{2}(\delta_1 + \delta_2).$$

Having $Q_{2,1}^{a,\beta}$, *I* contains also $Q_{2,3}^{a,\beta}$ and $Q_{3,1}^{a,\beta}$ and thus the product of the two, which reduces to $T_{\sigma}T_{12}$, having

$$\sigma_1 = -1, \quad \sigma_2 = a^2 - \beta^2, \quad \sigma_3 = 2a\beta.$$

If $a \cdot \beta = 0$, $Q_{2,1}^{a,\beta} = C_1 C_2$, not being the identity. Then, by §7, *I* contains every $Q_{i,j}^{a,\beta}$ and therefore, if $p^n > 5$, a substitution $Q_{2,3}^{a,\beta} Q_{3,1}^{a,\beta} = T_{\sigma} T_{12}$ in which $a\beta \neq 0$.

10. Thus I contains a substitution T_{δ} T_{1_2} having $\delta_{\mathfrak{s}}$ and $\delta_{\mathfrak{s}}$ not both zero, say $\delta_{\mathfrak{s}} \neq 0$. Transforming it by $O_{\mathfrak{s}\mathfrak{s}\mathfrak{s}}$, we can make the resulting substitution T_{δ} T_{1_2} commutative with T_{1_6} . Indeed, the conditions

$$\delta_6' \equiv a \delta_3 + \beta \delta_4 = \delta_1, \quad a^2 + \beta^2 + \gamma^2 = 1,$$

combine into the single condition

1898.]

$$a^{2}(\delta_{3}^{2}+\delta_{4}^{2})-2a\delta_{1}\delta_{3}+\delta_{4}^{2}\gamma^{2}=\delta_{4}^{2}-\delta_{1}^{2}$$

For $\delta_s^2 + \delta_4^2 = 0$, a solution is given by $\gamma = 0$ when $\delta_1 \pm 0$, and by $\gamma = 1$ when $\delta_1 = 0$. For $\delta_3^2 + \delta_4^2 \pm 0$, there exist* solutions α , γ in the $GF[p^n]$ of the equivalent equation of condition

$$\{a(\delta_3^2 + \delta_4^2) - \delta_1 \delta_3\}^2 + \delta_4^2(\delta_3^2 + \delta_4^2)\gamma^2 = \delta_4^2(\delta_3^2 + \delta_4^2 - \delta_1^2).$$

Hence I contains the substitution, not the identity,

$$(T_{\delta'} T_{12}) = T_{26} T_{76} (T_{\delta'} T_{12})^{-1} T_{78} T_{26}$$

= $T_{\delta'} T_{16} T_{\delta'}^{-1} T_{26} = T_{16} T_{26}.$

The alternating group on m > 4 letters being simple, the group I, containing T_{16} T_{26} , contains the whole alternating group. Further, C_1 C_2 transforms T_{16} T_{26} into T_{16} T_{26} C_1 C^9 , so that I contains C_1 C_6 and therefore every C_i C_j . Hence, by § 7, I contains every $Q_{1,2}^{a,\beta}$. Thus the group I coincides with H.

ADDENDA † OF APRIL 18.

11. For $p^n = 3$ or 5, the maximal invariant sub-group of H is of order 2 or 1, according as m > 4 is even or odd. For $p^n = 3$, m = 4, the order of H is $2^5 \cdot 3^2$, and its factors of composition are all primes.

12. Suppose $p^n = 8l \pm 1$, so that 2 is a square. Let $O_{1,2}^{\alpha,\beta}$ denote a definite orthogonal substitution not in $Q_{1,2}$, so that $1 \pm a$ are not-squares. Denote by H_1 the group obtained by extending the group of the $Q_{i,j}$ by all the products $O_{i,j}^{\alpha,\beta} = O_{k,j}^{\alpha,\beta}$.

THEOREM: H_1 contains half of the substitutions of G. For every substitution of G is of the form

$$S = h_1 \ O_{i,j}^{\alpha,\beta} \ h_2 \ O_{k,l}^{\alpha,\beta} \cdots,$$

 h_1, h_2, \dots, h denoting substitutions of H_1 . Now $O_{i,j}^{\alpha,\beta}$ can be carried to the right of every $Q_{i,j}^{\lambda,\mu}$ and every $Q_{k,i}^{\lambda,\mu}$ (k, l + i, j). Further, since $(O_{1,2}^{\alpha,\beta})^2 = Q_{1,2}^{\alpha,-\beta}$,

$$O_{i,j}^{\alpha,\beta} Q_{i,k}^{\lambda,\mu} = O_{i,j}^{\alpha,\beta} (O_{i,k}^{\alpha,\beta})^2 Q_{i,k}^{\alpha,\beta} \cdot Q_{i,k}^{\lambda,\mu},$$

= $O_{i,j}^{\alpha,\beta} O_{i,k}^{\alpha,\beta} \cdot Q_{i,k}^{\alpha,\beta} Q_{i,k}^{\lambda,\mu} \cdot O_{i,k}^{\alpha,\beta} = h O_{i,k}^{\alpha,\beta}.$

* BULLETIN, l. c. § 3.

[†] The results here announced will be proven in full in the Proceedings of the California Academy of Sciences, Third Series, vol. 1, No. 5.

Thus S finally takes the form

$$h' O_{r,s}^{a,\beta} = h' O_{r,s}^{a,\beta} O_{2,1}^{a,\beta} O_{1,2}^{a,\beta} = h'' O_{1,2}^{a,\beta}.$$

13. THEOREM: For m > 4, p + 2, the maximal invariant sub group of H_1 is of order 2 or 1 according as m is even or odd.

For m > 7, the group is similar to that for the group H as given above. In §6 we replace $T_{12} C_1 O_{i345}$ by $O_{1,2}^{\alpha,\beta} O_{i345}$. We replace §7 by the

Lemma: If $p^n = 8l \pm 1$, m > 3, an invariant sub-group I containing every $C_i C_j$ coincides with H_1 .

Indeed, $O_{2,4}^{a,\beta}$ $O_{1,2}^{a,\beta}$ transforms $C_1 C_3$ into $Q_{1,2}^{a,\beta} C_1 C_3$, so that *I* contains every $Q_{i,j}^{a,\beta}$. Having $T_{23}C_3$, *I* contains every $O_{i,j}^{a,\beta}$ $O_{k,i}^{a,\beta}$. Thus, for example,

$$(T_{23}C_3) (O_{1,2}^{a,\beta} O_{1,4}^{a,\beta}) (T_{23}C_3)^{-1} (O_{1,2}^{a,\beta} O_{1,4}^{a,\beta})^{-1} = O_{1,3}^{a,\beta} O_{2,1}^{a,\beta}$$

14. THEOREM: For p > 2, the ternary orthogonal group in the $GF[p^n]$ has a sub-group H' of index two and of order $\frac{1}{2}p^n(p^{2n}-1)$ which is simply isomorphic to the group of linear fractional substitutions of determinant unity on a single index.

Indeed, the orthogonal substitution

$$S: \xi_i' = \sum_{j=1}^3 a_{ij} \xi_j \quad (i = 1, 2, 3),$$

expressed in terms of the new indices

$$\eta_1 = - \, i \xi_1, \quad \eta_2 = \xi_2 - i \xi_3, \quad \eta_3 = \xi_2 + \, i \xi_3,$$

leaves $\eta_1^2 - \eta_2 \eta_3$ invariant and has the form

$$S_{1}: \left\{ \begin{array}{c} a_{11} \frac{1}{2}(a_{13}-ia_{12}) & -\frac{1}{2}(a_{13}+ia_{12}) \\ a_{31}+ia_{21} \frac{1}{2}(a_{22}-ia_{32}+ia_{23}+a_{33}) & \frac{1}{2}(a_{22}-ia_{32}-ia_{23}-a_{33}) \\ -a_{31}-ia_{21} \frac{1}{2}(a_{22}+ia_{32}+ia_{23}-a_{33}) & \frac{1}{2}(a_{12}+ia_{32}-ia_{23}+a_{33}) \end{array} \right\}$$

Understanding by H' the group H or H_1 according as $p^n = 8l \pm 3$ or $p^n = 8l \pm 1$, we may verify that for every substitution of H' the coefficient $\frac{1}{2}(a_{22} - ia_{32} + ia_{23} + a_{33})$ is the square of a complex a of the form $\rho + \sigma i$, where ρ and σ are marks of the $GF[p^n]$. It readily follows * that S_1 may be written in the form :

$$S_{1}: \begin{cases} a\delta + \beta\gamma & a\gamma & \beta\delta \\ 2a\beta & a^{2} & \beta^{2} \\ 2\gamma\delta & \gamma^{2} & \delta^{2} \end{cases} \qquad [a\delta - \beta\gamma = 1]$$

where α is conjugate to δ , β to γ . Further two such ternary

 $\mathbf{388}$

^{*}Compare Klein-Fricke : Automorphic Functions I., p. 14; Weber: Algebra, II., p. 190.

substitutions have the same composition formula as linear fractional substitutions. Hence, according as -1 is a square or a not square, H' is simply isomorphic to the "real" or the "imaginary" form * of the group of linear fractional substitutions of determinant unity. Thus, for $p^n > 3, H'$ is simple.

15. Observing that the squares of the substitutions

 $O_{1,2}^{a,\beta}, \quad O_{1,2}^{a,\beta} T_{13}C_1C_2C_3, \quad O_{1,2}^{a,\beta} T_{13}T_{24}$

are respectively $Q_{1,2}^{a,-\beta}$, $O_{1,2}^{a,\beta}$, $O_{3,2}^{a,\beta}$, $O_{1,2}^{a,\beta}$, $O_{3,4}^{a,\beta}$, we may unite our results into the following

THEOREM : The squares of the linear substitutions on m indices in the $GF[p^n]$, $p \neq 2$, which leave invariant the sum of the squares of the m indices, generate a group, which for m = 2k + 1 has the order

$$\frac{1}{2}(p^{2nk}-1) p^{2nk-n} (p^{2nk-2n}-1) p^{2nk-3n} \cdots (p^{2n}-1) p^{n}$$

and is simple except when $p^n = 3$, m = 3; while for m = 2k > 4it has the factors of composition 2 and

$$\frac{1}{4} \left[p^{nk} - (\pm 1)^k \right] p^{nk-n} \left(p^{2nk-2n} - 1 \right) p^{2nk-3n} \cdots \left(p^{2n} - 1 \right) p^n,$$

the sign \pm depending upon the form $4l \pm 1$ of p^n .

UNIVERSITY OF CALIFORNIA,

February 10, 1898.

A PROOF OF THE THEOREM:

$\partial^2 u$		$\partial^2 u$
$\overline{\partial x \partial y}$	-	$\overline{\partial y \partial x}$

BY MR. J. K. WHITTEMORE.

(Read before the American Mathematical Society at the Meeting of April 30, 1898.)

THEOREM: Let u = f(x, y) denote a function of the two independent variables x and y which, together with its first deriva-tives and the two second derivatives in question, is continuous in

the neighborhood of the point (x, y); then $\frac{\partial^2 u}{\partial x \partial y} = \frac{\partial^2 u}{\partial y \partial x}$

Let
$$\frac{\partial^2 f(x, y)}{\partial x \partial y}$$
 denote $\frac{\partial}{\partial x} \left(\frac{\partial f(x, y)}{\partial y} \right)$

* Moore: Mathematical Papers of the Chicago Congress (1893), "A doubly-infinite system of simple groups," 22 5-6.