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 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

$$O_{ij}^{\alpha\beta}: \begin{cases} \xi_i' = a_{ij}^2 + \beta_{ij}^2 \\ \xi_j' = -\beta_{ij} + a_{ij}^2 \end{cases} \quad (\alpha^2 + \beta^2 = 1).$$

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 $G$

* The fact that $p^n = 3$ is an exception was not pointed out in the Bulletin. In fact Jordan had not proven case 2 of § 211 when $-1 = a^2 = b^2 = c^2 = \ldots = 1$ 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.,

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

† A preliminary account was presented before the Mathematical Conference at Chicago, December 30, 1897.
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 \(O_{m,2}^\beta\) form a commutative group of order \(p^n \pm 1\). A subgroup of index 2 is formed by the substitutions

\[
Q_{i,1}^{a,\beta} : \xi_1' = (a^2 - \beta^2)\xi_1 - 2a\beta \xi_2, \\
\xi_2' = 2a\beta \xi_1 + (a^2 - \beta^2)\xi_2.
\]

Indeed,

\[
Q_{i,1}^{a,\beta} Q_{i,2}^{a,\beta} = Q_{i,1}^{a,\beta - \beta, \alpha + \beta \gamma}.
\]

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

If \(C_i\) denotes the substitution affecting only the index \(i\), whose sign it changes, \(C_i\) is always contained among the substitutions \(Q_{i,1}^{a,\beta}\).

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 \(T_{1,2}\) denotes the transposition \((\xi_1, \xi_2)\), \(T_{1,2} C_i\) is not of the form \(Q_{i,1}^{a,\beta}\) but serves to extend the group of the latter to the group of the \(Q_{i,1}^{a,\beta}\). Furthermore, if \(j > 2, T_{1,2} C_i\) transforms \(Q_{i,1}^{a,\beta}\) into \(Q_{i,1}^{a,\beta}\) and \(Q_{1,2}^{a,\beta}\) into \(Q_{1,1}^{a,\beta}\). Hence if we extend the alternating group on the \(m\) letters \(\xi_i\) by the substitutions \(Q_{i,1}^{a,\beta}\) 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

\[
N : \xi_i' = -\xi_i \quad (i = 1, \ldots, m).
\]

Suppose \(H\) has an invariant subgroup \(I\) containing a substitution

---

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

neither the identity nor $N$. By suitably transforming $S$, we can suppose that $a_i^2 + a_j^2 = 1$. Then $S$ is not commutative with $C_i C_j$; for, if so, it would be merely a product of a substitution affecting only $\xi_1$ and $\xi_2$ by a substitution affecting only $\xi_3, \ldots, \xi_m$. 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

$$\xi_i' = \xi_i - 2a_{ai} \sum_{j=1}^{m} a_{aj} \xi_j - 2a_{ai} \sum_{j=1}^{m} a_{aj} \xi_j \quad (i = 1, \ldots, m).$$

4. Lemma: The orthogonal substitution

$$O_{\psi} : \begin{cases} \xi_i' = \lambda \xi_i + \mu \xi_j + \nu \xi_k, \\ \xi_j' = \lambda' \xi_i + \mu' \xi_j + \nu' \xi_k, \\ \xi_k' = \lambda'' \xi_i + \mu'' \xi_j + \nu'' \xi_k, \end{cases}$$

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

$$\begin{align*}
a_{ai}' &= \lambda a_{ai} + \mu a_{aj} + \nu a_{ak}, \\
a_{aj}' &= \lambda' a_{ai} + \mu' a_{aj} + \nu' a_{ak}, \\
a_{ak}' &= \lambda'' a_{ai} + \mu'' a_{aj} + \nu'' a_{ak}, \\
a_{as}' &= a_{as} \\
(a_s = 1, \ldots, m, s = i, j, k).
\end{align*}$$

If $a_{ai} = 0$, we can choose $\lambda$, $\mu$, $\nu$ such that $a_{ai}' = 0$. For if $a_{ai} + a_{aj} = 0$ and therefore $a_{ai} = 0$, we may take

$$\begin{align*}
\lambda &= \frac{-a_{ai}}{2a_{ai}}, \\
\mu &= \frac{-a_{ai}}{2a_{aj}}, \\
\nu &= 1.
\end{align*}$$

If $a_{ai} + a_{aj} = 0$, we derive the equivalent condition,

$$\mu (a_{ai} + a_{aj}) + \nu a_{aj} a_{ai} \lambda^2 + \nu^2 a_{ai}^2 (a_{ai} + a_{aj} + a_{ak}) = a_{ai}^2 (a_{ai} + a_{aj}),$$

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

$$a_{ai}^2 = -(\mu a_{ai} - \nu a_{aj})^2,$$

having solutions if and only if $-1$ is a square.

* Bulletin, l.c. § 3.
5. Lemma: $O_{a_i}$ transforms $S_a$ into $S_{a'}$, where

$$a_{i}' = \lambda a_{i} + \mu a_{j} + \nu a_{k} + a a_{i}.$$  

If $a_{i}^2 + a_{j}^2 + a_{k}^2 = 0$, the values

$$\lambda = \frac{-a_{i}}{a_{i}^2}, \quad \mu = \frac{a_{j}}{a_{i}^2}, \quad \nu = \frac{-a_{k}}{a_{i}^2}, \quad \sigma = 1$$

make

$$a_{i}' = 0, \quad \mu^2 + \nu^2 + \sigma^2 = 1$$

6. The invariant subgroup $I$ of $H$ was shown to contain the substitution $S' = S_a C_1 C_2$ not the identity. Transforming $S'$ successively by

$$O_{a_45} \text{ or } T_{12} C_1 O_{a_45} \quad (i = m, m - 1, \ldots, 6),$$

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 $I$ and having $a_{a_1} = a_{a_1} - 1 = \cdots = a_{a_1} = 0$. Also, by § 4, we may make $a_{a_1} = 0$; for we have

$$a_{a_1}^2 + a_{a_1}^2 = a_{a_1}^2 + a_{a_1}^2 = 1,$$

so that

$$a_{a_1}^2 + a_{a_1}^2 + a_{a_1}^2 = 0.$$  

Next we transform $S_{a'} C_1 C_2$ successively by

$$O_{a_57} \quad (j = m, m - 1, \ldots, 8)$$

and obtain in $I$ a substitution $S_{a''} C_1 C_2$ having

$$a_{a''} = 0, \quad a_{a''} = 0 \quad (j = m, \ldots, 8).$$

The group $I$ thus contains a substitution

$$S: \quad \xi_i = \sum_{j=1}^{7} \beta_j \xi_j \quad (i = 1, \ldots, 7)$$

neither the identity nor $N = C_1 C_2 \cdots C_m$.

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 $C_i$ are lacking. But if

$$S = C_i C_j C_k C_l \cdots,$$

the group $I$ contains

$$T_{a}^ST_{a}^ST_{a}^S = C_k C_l$$

and hence, by transforming by suitable even substitutions, every product of two $C_i$'s. But $H$ contains either $O_{a_45}^b$ or $O_{a_45}^b T_{12} C_1$, which transform $C_1 C_2$ into $Q_{a_4}^b C_1 C_2$ and $Q_{a_4}^b C_2 C_1$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
respectively. Hence the group \( I \) contains every \( Q^\alpha_1, \beta \), among which, if \( p^n > 5 \), occurs one different from the identity and from \( C_1 C_2 \).

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

\[
S^{-1} C_i C_S C_i C_S = R \beta C_1,
\]

where \( R \beta \equiv S^{-1} C_i S \) is seen to be

\[
R \beta : \xi_i' = \xi_i - 2\beta_i \sum_{j=1}^{7} \beta_j \xi_j \quad (i = 1, \ldots, 7).
\]

Transforming \( R \beta C_1 \) by \( Q_{12} \), for \( i = 7, 6, 5 \) successively, we may suppose that \( \beta_{71} = \beta_{61} = \beta_{51} = 0 \).

It is readily seen that a substitution \( R \) affecting only \( \xi_1, \ldots, \xi_4 \) is not commutative with every \( T_{ij} (i, j = 1, \ldots, 5) \) for example not with \( T_{12} \). Then \( I \) contains the substitution, not the identity,

\[
R^{-1} T_{12} T_{67} R T_{67} T_{12} = T_8 T_{12},
\]

where \( T_8 \equiv R^{-1} T_{12} R \) has the form

\[
T_8: \xi_i' = \xi_i - \delta_i \sum_{j=1}^{4} \delta_j \xi_j \quad (i = 1 \ldots 4),
\]

where

\[
\delta_1^2 + \delta_2^2 + \delta_3^2 + \delta_4^2 = 2.
\]

9. If \( \delta_3 = \delta_4 = 0 \), \( T_8 T_{12} \) becomes \( Q^\alpha_1, \beta \) if we set

\[
a = \frac{1}{2}(\delta_1 - \delta_2), \quad \beta = \frac{1}{2}(\delta_1 + \delta_2).
\]

Having \( Q^\alpha_2, \beta \), \( I \) contains also \( Q^\alpha_3, \beta \) and \( Q^\alpha_4, \beta \) and thus the product of the two, which reduces to \( T_8 T_{12} \) having

\[
\sigma_1 = -1, \quad \sigma_2 = a_2 - \beta, \quad \sigma_3 = 2a_2 \beta.
\]

If \( a \cdot \beta = 0 \), \( Q^\alpha_{1, \beta} = C_1 C_2 \); not being the identity. Then, by §7, \( I \) contains every \( Q^\alpha_{1, \beta} \) and therefore, if \( p^n > 5 \), a substitution \( Q^\alpha_2, \beta Q^\alpha_3, \beta = T_8 T_{12} \) in which \( a \beta = 0 \).

10. Thus \( I \) contains a substitution \( T_8 T_{12} \) having \( \delta_3 \) and \( \delta_4 \) not both zero, say \( \delta_3 \neq 0 \). Transforming it by \( Q_{12} \), we can make the resulting substitution \( T_8 T_{12} \) commutative with \( T_{12} \). Indeed, the conditions

\[
\delta_4' = \alpha \delta_3 + \beta \delta_4 = \delta_1, \quad \alpha^2 + \beta^2 + \gamma^2 = 1,
\]

combine into the single condition
For \( \delta_2^2 + \delta_2^1 = 0 \), a solution is given by \( \gamma = 0 \) when \( \delta_1 + 0 \), and by \( \gamma = 1 \) when \( \delta_1 = 0 \). For \( \delta_2^2 + \delta_2^1 = 0 \), there exist solutions \( a, \gamma \) in the \( GF[p^n] \) of the equivalent equation of condition

\[
\{ a(\delta_2^3 + \delta_2^1) - \delta_1 \delta_3^3 + \delta_1^2(\delta_2^1 + \delta_2^1)\gamma^2 = \delta_1^2(\delta_2^1 + \delta_2^2 - \delta_1^1). \]

Hence \( I \) contains the substitution, not the identity,

\[
(T_6^1 T_1^2) = T_{26} T_{29} (T_6^1 T_1^2)^{-1} T_{29} T_{26} = T_{3} T_{16} T_{30} = T_{5} T_{26}.
\]

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 \( T_{16} T_{26} C_1 C_2 \), so that \( I \) contains \( C_1 C_2 \) and therefore every \( C_1 C_2 \). Hence, by § 7, \( I \) contains every \( Q_{i}^m \). 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 \( 2^5 3^2 \), and its factors of composition are all primes.

12. Suppose \( p^n = 8l \pm 1 \), so that 2 is a square. Let \( O_{i}^a \) denote a definite orthogonal substitution not in \( H \), so that \( 1 \pm a \) are not-squares. Denote by \( H \), the group obtained by extending the group of the \( Q_i \) by all the products \( O_{i}^a O_{i}^b \).

**Theorem:** \( H \) contains half of the substitutions of \( G \). For every substitution of \( G \) is of the form

\[
S = h_1 O_{i,j}^a h_2 O_{i,i}^a \ldots ,
\]

\( h_1, h_2, \ldots, h \) denoting substitutions of \( H \). Now \( O_{i,j}^a \) can be carried to the right of every \( Q_{i}^m \) and every \( Q_{i}^m \) (\( k, l \rightarrow i, j \)). Further, since \( (O_{i,j}^a)^2 = Q_{i}^a \),

\[
O_{i,j}^a Q_{i,i}^m = O_{i,j}^a (O_{i,i}^a)^2 Q_{i,i}^m \cdot Q_{i,i}^m = O_{i,j}^a Q_{i,i}^m \cdot Q_{i,i}^m \cdot Q_{i,i}^m = h O_{i,i}^a.
\]

*BULLETIN, 1, 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

$$h' \ O_{\gamma_i}^\alpha = h' \ O_{\gamma_i}^\alpha \ O_{\gamma_i}^\beta \ O_{\gamma_i}^\beta = h' \ O_{\gamma_i}^\beta.$$ 

13. **Theorem:** For $m > 4$, $p = 2$, the maximal invariant subgroup of $H_i$ 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 $T_{12} C_{1} O_{1345}$ by $O_{12}^\beta$. 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 $H_i$.

Indeed, $O_{12}^\beta$ transforms $C_i C_j$ into $O_{13}^\beta C_i C_j$, so that $I$ contains every $Q_{1,2}^\beta$. Having $T_{23} C_3$, $I$ contains every $O_{1j}^\beta O_{1j}^\beta$. Thus, for example,

$$(T_{23} C_3) \ (O_{12}^\beta O_{13}^\beta) \ (T_{23} C_3)^{-1} \ (O_{12}^\beta O_{13}^\beta)^{-1} = O_{12}^\beta O_{12}^\beta.$$

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

$$\gamma_1 = -i\xi_1, \quad \gamma_2 = \xi_2 - i\xi_3, \quad \gamma_3 = \xi_2 + i\xi_3,$$

leaves $\gamma_1^2 - \gamma_2 \gamma_3$ invariant and has the form

$$S_i: \begin{cases} a_{11} \frac{1}{2} (a_{13} - ia_{12}) - \frac{1}{2} (a_{13} + ia_{12}) \\ -a_{31} - ia_{31} \frac{1}{2} (a_{23} + ia_{23} + ia_{23} + a_{23}) + \frac{1}{2} (a_{23} + ia_{23} - ia_{23} - a_{23}) \\ -a_{31} - ia_{31} \frac{1}{2} (a_{23} + ia_{23} + ia_{23} - a_{23}) + \frac{1}{2} (a_{23} + ia_{23} - ia_{23} + a_{23}) \end{cases}$$

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

$$S_i: \begin{cases} a \alpha^2 + b \beta \gamma \gamma^2 + \beta \beta \alpha^2 \\ 2a \beta \gamma \gamma^2 + \beta \beta \alpha^2 \end{cases} \quad [a \beta - \beta \gamma = 1]$$

where $a$ is conjugate to $\alpha$, $\beta$ to $\gamma$. Further two such ternary

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

$$O_{i, 2}^{n, \beta}, \quad O_{i, 2}^{n, \alpha} T_{13} C_1 C_2 C_3, \quad O_{i, 2}^{n, \beta} T_{13} T_{24}$$

are respectively $Q_{i, 2}^{n, -\beta}, \quad O_{i, 2}^{n, \alpha} O_{i, 2}^{n, \beta}, \quad O_{i, 2}^{n, \beta} O_{i, 2}^{n, \beta}$,
we may unite our results into the following

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

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

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

$$\frac{1}{2} [p^{2n} - (\pm 1)^k] p^{2n} \cdots (p^{2n-2k} - 1) p^n,$$

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

**UNIVERSITY OF CALIFORNIA,**

February 10, 1898.

---

**A PROOF OF THE THEOREM:**

$$\frac{\partial^2 u}{\partial x \partial y} = \frac{\partial^2 u}{\partial y \partial x}$$

**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 derivatives and the two second derivatives in question, is continuous in the neighborhood of the point $(x, y)$; then

$$\frac{\partial^2 u}{\partial y \partial x} = \frac{\partial^2 u}{\partial y \partial x}$$

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