THE GROUPS OF STEINER IN PROBLEMS OF CONTACT*

BY

LEONARD EUGENE DICKSON

1. The problems of contact discussed by Steiner† and Hesse‡ were investigated from a more general standpoint by Clebsch in his paper on the application of Abelian functions to geometry.‡ A study of the groups of these geometrical problems has been made by Jordan.§ One of the most interesting of these groups was shown by Jordan to be holoedrically isomorphic with the first hypoabelian linear group, which plays so important a rôle in various geometrical questions and in the problem of the construction of all solvable groups. As the proof (Traité, pp. 229–249) is quite complicated, it seemed to the writer worth while to publish the elementary proof given below of the isomorphism in question. No use will be made of the Jordan substitutions \([a_1, \beta_1, \ldots, a_p, \beta_p]\), neither the origin nor the interpretation of which is apparent.

2. The theorem that there are 28 bitangents to a curve of the fourth order has been generalized by Clebsch (l. c., § 8) as follows: Let \(C_n\) be a curve of order \(n\) having no double points and set \(p = \frac{1}{2} (n - 1)(n - 2)\). There are \(2^{p-1}(2^p - 1)\) curves of order \(n - 3\) having simple contact with \(C_n\) at \(\frac{1}{2} n(n - 3)\) points. The determination of these curves depends upon an equation \(E\) of degree \(R_p \equiv 2^{p-1} - 2^{p-1}\), whose roots may be represented by the symbol \((x_1 y_1 \cdots x_p y_p)\), where \(x_1, y_1, \ldots, x_p, y_p\) may be 0 or 1, such that

\[
(1) \quad x_1 y_1 + x_2 y_2 + \cdots + x_p y_p \equiv 1 \pmod{2}.
\]

Let \(\mu\) be any integer, \(\mu \equiv R_p\), such that \(\mu(n - 3)/2\) is also an integer, and consider the \(\mu\) roots

\[
(x_1^{\mu} y_1^{\mu} \cdots x_p^{\mu} y_p^{\mu}), \ldots, (x_1^{(\mu)} y_1^{(\mu)} \cdots x_p^{(\mu)} y_p^{(\mu)}).
\]

Clebsch proved that the points of contact of \(C_n\) with the corresponding \(\mu\)

---

*Presented to the Society (Chicago) April 6, 1901, in connection with a paper entitled "Representation of linear groups as transitive substitution groups." Received for publication May 4, 1901.

†Journal für Mathematik, vol. 49 (1855).
curves all lie on a curve of order \( \mu(n - 3)/2 \), if the following congruences hold simultaneously:

\[
(2) \quad x_i + x_i'' + \cdots + x_i^{(\mu)} \equiv 0, \quad y_i + y_i'' + \cdots + y_i^{(\mu)} \equiv 0 \pmod{2} \quad (i = 1, \ldots, p).
\]

Let \( \phi_\mu \) denote the sum of the products of the \( R_p \) roots taken \( \mu \) at a time. According to a general principle, the substitutions of the group \( G \) of the equation \( E \) will leave the function \( \phi_\mu \) invariant. If \( n \) be even, \( \mu \) can have only even values, so that \( G \) is a subgroup of the group which leaves \( \phi_4, \phi_6, \ldots \) invariant. If \( n \) be odd, \( \mu \) can be any integer such that \( 2 < \mu \leq R_p \), and the group \( G \) is contained in the group \( G' \) defined by the invariants \( \phi_3, \phi_4, \ldots, \phi_{R_p} \). We are to prove that \( G' \) is holoedrically isomorphic with the first hypoabelian group \( G_0 \) on \( 2p \) indices with coefficients taken modulo 2.

3. The first hypoabelian group \( G_0 \) is formed by the substitutions

\[
S: \quad \xi_i = \sum_{j=1}^{p} (a_{ij} \xi_j + \gamma_{ij} \eta_j), \quad \eta_i = \sum_{j=1}^{p} (\beta_{ij} \xi_j + \delta_{ij} \eta_j) \quad (i = 1, \ldots, p),
\]

with coefficients taken modulo 2, which leave formally invariant the function

\[
\theta \equiv \xi_1 \eta_1 + \xi_2 \eta_2 + \cdots + \xi_p \eta_p.
\]

As generators of \( G_0 \), we may take

\[
(3) \quad M_i = (\xi_i, \eta_i), \quad N_{ij} : \xi_j = \xi_i + \eta_i, \quad \xi_j = \xi_j + \eta_i,
\]

where we have written only the indices altered by the substitution.

The substitution \( S \) replaces the function

\[
f = \sum_{i=1}^{p} (x_i \xi_i + y_i \eta_i)
\]

by

\[
f' = \sum_{i=1}^{p} (x_i' \xi_i + y_i' \eta_i), \quad x_i' = \sum_{j=1}^{p} (a_{ij} x_j + \beta_{ij} y_j), \quad y_i' = \sum_{j=1}^{p} (\gamma_{ij} x_j + \delta_{ij} y_j).
\]

The \( x_i', y_i' \) are expressed in terms of \( x_j, y_j \) by formulæ which define a matrix of coefficients identical with the transposed of the matrix of the coefficients of \( S \). Hence these formulæ define a substitution of the group \( G_0 \) (as shown by the explicit conditions on the coefficients of a first hypoabelian substitution).†

Hence

\[
(4) \quad x_1' y_1' + x_2' y_2' + \cdots + x_p' y_p' = x_1 y_1 + x_2 y_2 + \cdots + x_p y_p.
\]

*Compare JORDAN, Traité, no. 421.

†Shown by JORDAN, nos. 319-335, to be holoedrically isomorphic with the Abelian linear group on \( 2p \) indices with coefficients taken modulo 2.

This result may also be shown by considering the generators (3). In fact, $M_1$ and $N_{12}$ replace the function $f$ by, respectively,

$$y_i x_i + x_i y_i + \sum_{i=2}^{p} (x_i x_i + y_i y_i),$$

$$x_i x_i + (y_i + x_i) y_i + x_2 y_2 + (y_2 + x_2) y_2 + \sum_{j=3}^{p} (x_j x_j + y_j y_j).$$

In view of (4), it follows that $S$ permutes amongst themselves the functions $f$ in which $x_1 y_1 + \cdots + x_p y_p = 1$. In place of the functions $f$, we may employ the positional symbols $(x_1 y_1 \cdots x_p y_p)$ of §2. Hence $G_0$ is isomorphic with a substitution-group $\Gamma$ on these $R_p$ symbols. Moreover, the isomorphism is holoedric and the group $\Gamma$ is transitive; these results are readily proved.*

4. We may write the functions $\phi_3$ and $\phi_4$ as follows:

$$\phi_3 = \sum (x_i' y_i' \cdots x_p' y_p') (x_1'' y_1'' \cdots x_p'' y_p'') (x_1 + x_1' + x_1'' + x_2 + x_2'' + \cdots),$$

$$\phi_4 = \sum (x_i' y_i' \cdots) (x_1'' y_1'' \cdots) (x_1'' y_1'' \cdots) (x_1 + x_1'' + x_1'' y_1 + x_2 y_2 + \cdots),$$

the summations extending over all the symbols $(x_i' y_i' \cdots)$, $(x_1'' y_1'' \cdots)$, $(x_1'' y_1'' \cdots)$, such that the final term is, in each case, a symbol. Thus, for $\phi_3$,

$$\sum_{i=1}^{p} x_i' y_i' = 1, \quad \sum_{i=1}^{p} x_i'' y_i'' = 1, \quad \sum_{i=1}^{p} (x_i' + x_i'') (y_i + y_i') = 1 \pmod{2}.$$

Let $G_1$ be the group of Steiner composed of all substitutions on the $R_p$ symbols $(x_1 y_1 \cdots x_p y_p)$ which leave $\phi_3$ and $\phi_4$ invariant.† We first show that $G_1$ contains the group $\Gamma$ as a subgroup. In fact, $M_1$ replaces the general term (written above) of $\phi_3$ by

$$(y_1' x_1' x_2' y_2' \cdots) (y_1'' x_1'' x_2'' y_2'' \cdots) (y_1 + y_1' x_1 + x_1'' x_2 + x_2'' y_2 + y_2'' \cdots),$$

which is also a term of $\phi_3$. Similarly, $M_4$ and $N_{ij}$ leave $\phi_3$ and $\phi_4$ invariant. Hence $G_1$ contains all the generators of $\Gamma$. The next step consists in the proof that every substitution of $G_1$ belongs to $\Gamma$. From the two results we may then conclude that $G_1 \equiv \Gamma$, so that $G_1$ and the first hypoabelian group $G_0$ will be proved holoedrically isomorphic.

5. Let $L$ be an arbitrary substitution of $G_1$ and denote by $f_L$ the symbol which $L$ replaces by $(001100 \cdots 00)$. Then $\Gamma$, being transitive, contains a substitution $L'$ which replaces $f_L$ by $(0011 \cdots 00)$. Hence $M \equiv L'^{-1} L$ will belong to $G_1$ and will leave $(0011 \cdots 00)$ fixed. Since $M$ does not alter $\phi_3$, it

† It appears in the sequel that $G_1 \equiv G_1'$, the latter ($\S2$) leaving $\phi_3, \phi_4, \cdots, \phi_{R_p}$ invariant.
will leave invariant the function $\phi_3'$ given by the sum of those terms in $\phi_3$ which contain the factor $\begin{pmatrix} 0 & 0 & 1 & 1 & \cdots & 0 & 0 \end{pmatrix}$:

$$\phi_3' = \sum (\begin{pmatrix} 0 & 0 & 1 & 1 & \cdots & 0 & 0 \end{pmatrix})(x_1 y_1 x_2 y_2 x_3 y_3 \cdots)(x_1 y_1 x_2 + 1 y_2 + 1 x_3 y_3 \cdots),$$

\hspace{1cm}\text{(5)} \sum x_i y_i = 1, \quad \sum x_i y_i + (x_2 + 1)(y_2 + 1) \equiv 1 \pmod{2},

where the accent denotes that the value $i = 2$ is excluded. Hence $x_2 + y_2 \equiv 1 \pmod{2}$. Note that every set of solutions of (5) makes the three symbols in every triple of $\phi_3'$ all different. Hence $M$ leaves invariant

$$\psi = \sum (x_1 y_1 x_2 y_2 x_3 y_3 \cdots)(x_1 y_1 x_2 + 1 y_2 + 1 x_3 y_3 \cdots).$$

6. Hence $M$ permutes amongst themselves the $N$ symbols* not contained in the function $\psi$ and different from $\begin{pmatrix} 0 & 0 & 1 & 1 & \cdots \end{pmatrix}$, namely, the symbols $(x_1 y_1 x_2 y_2 \cdots)$ for which, in contrast to (5),

$$\sum x_i y_i = 1, \quad \sum x_i y_i + x_2 + y_2 + 1 \equiv 0 \pmod{2}.$$

Hence $x_2 + y_2 \equiv 0 \pmod{2}$. We next prove that the substitutions of $\Gamma$ which leave fixed $\begin{pmatrix} 0 & 0 & 1 & 1 & \cdots \end{pmatrix}$ permute transitively the $N$ symbols defined by (6). Among them occurs $\begin{pmatrix} 1 & 0 & 1 & 1 & \cdots & 0 & 0 \end{pmatrix}$. We are to prove that $\Gamma$ contains a substitution $\Sigma$ leaving fixed the symbol $\begin{pmatrix} 0 & 0 & 1 & 1 & \cdots \end{pmatrix}$ and replacing $\begin{pmatrix} 1 & 0 & 1 & 1 & \cdots & 0 & 0 \end{pmatrix}$ by an arbitrary symbol $(x_1 y_1 \cdots x_p y_p)$ in which

$$\sum x_i y_i = 1, \quad x_2 \equiv y_2 \pmod{2}.$$

In view of §3, we may think of the literal substitutions of $\Gamma$ as linear hypoabelian substitutions on $\xi_1, \eta_1, \cdots \xi_p, \eta_p$. We are therefore to prove that there exists a first hypoabelian substitution $S$ which leaves $\xi_2 + \eta_2$ fixed and replaces $\xi_1 + \xi_2 + \eta_2$ by

$$\sum (x_i \xi_i + y_i \eta_i),$$

subject to (6'). Hence $S$ must leave $\xi_2 + \eta_2$ fixed and replace $\xi_1$ by

$$\sum (x_i \xi_i + y_i \eta_i) - \xi_2 - \eta_2, \quad \sum x_i y_i + (x_2 - 1)(y_2 - 1) \equiv 0, \quad x_2 \equiv y_2 \pmod{2}.$$

\begin{footnote}{* The number $N = R_p - 2R_{p-1} - 1 = 2^{p-2} - 1$. Indeed, the number of sets of solutions of (5) equals the number of sets of solutions of\hspace{1cm} \sum x_i y_i = 1,\hspace{1cm} since $(x_2 + 1)x_2$ is even, which number is evidently $R_{p-1}$.\end{footnote}
7. Changing the notation, we are to prove that \( G_0 \) contains a substitution \( S_1 \) which leaves \( \xi_1 + \eta_1 \) fixed and replaces \( \xi_2 \) by

\[
\sum_{i=1}^{p} (X_i \xi_i + Y_i \eta_i), \quad \sum_{i=1}^{p} X_i Y_i \equiv 0, \quad X_1 \equiv Y_1 \quad \text{(mod 2)}.
\]

If \( X_1 \equiv 0 \), we take as \( S_1 \) a substitution* which leaves \( \xi_1 \) and \( \eta_1 \) fixed and replaces \( \xi_2 \) by

\[
\sum_{i=2}^{p} (X_i \xi_i + Y_i \eta_i), \quad \sum_{i=2}^{p} X_i Y_i \equiv 0 \quad \text{(mod 2)}.
\]

If \( X_1 \equiv 0 \) (mod 2), then \( X_2, X_3, \ldots, X_p, Y_p \) are not all zero. Applying a suitable transformation on \( \xi_2, \ldots, \xi_p \), we may suppose that \( X_2 \neq 0 \). Now \( G_0 \) contains the following substitution leaving \( \xi_1 + \eta_1 \) invariant:

\[
W \equiv Q_{21\alpha} N_{12\alpha}: \left\{ \begin{array}{l}
\xi'_1 = \xi_1 + a \eta_2, \quad \eta'_1 = \eta_1 + a \eta_2, \\
\xi'_2 = \xi_2 + a \xi_1 + a \eta_1 + a^2 \eta_2, \quad \eta'_2 = \eta_2.
\end{array} \right.
\]

Also \( G_0 \) contains the substitution \( V \) which leaves \( \xi_1 \) and \( \eta_1 \) fixed and replaces \( \xi_2 \) by

\[
X_2 \xi_2 + (Y_2 + X_1^2/X_2) \eta_2 + \sum_{i=3}^{p} (X_i \xi_i + Y_i \eta_i),
\]

since, in view of \( X_1 = Y_1 \),

\[
X_2(Y_2 + X_1^2/X_2) + \sum_{i=3}^{p} X_i Y_i = X_1^2 + \sum_{i=2}^{p} X_i Y_i = \sum_{i=1}^{p} X_i Y_i = 0.
\]

If we take \( a = X_1/X_2 \), the required substitution \( S_1 \) is the product \( WV \).

8. It follows that \( M = \Sigma P \), where \( P \) is a substitution of \( G_1 \) which leaves fixed the symbols \((00 11 00 \ldots 00)\) and \((10 11 00 \ldots 00)\). Hence \( P \) leaves invariant the two functions \( \phi'_1 \) and \( \phi'_2 \) formed respectively by those terms of \( \phi_3 \) which contain \((00 11 \ldots)\) and \((10 11 \ldots)\) as a factor. Hence \( P \) leaves invariant the function \( \psi \) of \( \S 5 \) derived from \( \phi'_3 \), and the following function derived from \( \phi'_3 \):

\[
\psi_1 \equiv \sum (x_1 y_2 x_2 y_2 x_3 y_3 \ldots)(x_1 + 1 y_1 x_2 + 1 y_2 + 1 x_3 y_3 \ldots).
\]

Hence \( P \) will permute amongst themselves the symbols occurring in \( \psi_1 \) and not in \( \psi \). These symbols \((x_1 y_2 \ldots)\) are defined by

\[
\sum_{i=1}^{p} x_i y_i \equiv 1, \quad \sum_{i=1}^{p} x_i y_i + (x_2 + 1)(y_2 + 1) \equiv 0,
\]

\[
(x_1 + 1)y_1 + (x_2 + 1)(y_2 + 1) + \sum_{i=3}^{p} x_i y_i \equiv 1 \quad \text{(mod 2)}.
\]

*Bulletin, l. c., p. 498.
Hence there are $2^{2p-3}$ such symbols satisfying the conditions

$$\sum_{i=1}^{p} x_i y_i \equiv 1, \ x_2 \equiv y_2, \ y_1 \equiv 1 \pmod{2}. \quad (7)$$

Among them occurs $\left(01 \ 11 \ 00 \ \ldots \ 00\right)$. We next prove that $T$ contains a substitution $T$ which leaves fixed $\left(00 \ 11 \ \ldots \ \right)$, $\left(10 \ 11 \ \ldots \ \right)$ and replaces $\left(01 \ 11 \ \ldots \ \right)$ by an arbitrary symbol $\left(x_1 y_1 \ x_2 y_2 \ \ldots \ \right)$ satisfying the conditions (7). We are to find a substitution $T$ of the first hypoabelian group $G_0$ which leaves fixed $\xi_1 + \eta_2$ and $\xi_2 + \eta_2$, but replaces $\eta_1 + \xi_2 + \eta_2$ by $x_1 \xi_1 + y_1 \eta_1 + x_2 \xi_2 + y_2 \eta_2 + \ldots$ subject to the relations (7). Then $T$ must leave fixed $\xi_1$ and $\xi_2 + \eta_2$, but replace $\eta_1$ by

$$x_1 \xi_1 + \eta_1 + (x_2 + 1) \xi_2 + (x_2 + 1) \eta_2 + \sum_{i=3}^{p} (x_i \xi_i + y_i \eta_i) \ [x_1 + x_2 + \sum_{i=3}^{p} x_i y_i = 1].$$

Such a substitution belonging to $G_0$ is the following:

<table>
<thead>
<tr>
<th>$\xi_1'$</th>
<th>$\eta_1'$</th>
<th>$\xi_2'$</th>
<th>$\eta_2'$</th>
<th>$\xi_3'$</th>
<th>$\eta_3'$</th>
<th>$\xi_p'$</th>
<th>$\eta_p'$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_1$</td>
<td>1</td>
<td>$x_2 + 1$</td>
<td>$x_3$</td>
<td>$y_3$</td>
<td>$x_p$</td>
<td>$y_p$</td>
<td></td>
</tr>
<tr>
<td>$x_2 + 1$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_2 + 1$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$a_{31}$</td>
<td>$\gamma_{31}$</td>
<td>$a_{32}$</td>
<td>$\gamma_{32}$</td>
<td>$a_{33}$</td>
<td>$\gamma_{33}$</td>
<td>$\ldots$</td>
<td>$a_{3p}$</td>
</tr>
<tr>
<td></td>
<td>$\delta_{p1}$</td>
<td>$\beta_{p2}$</td>
<td>$\delta_{p2}$</td>
<td>$\beta_{p3}$</td>
<td>$\delta_{p3}$</td>
<td>$\ldots$</td>
<td>$\beta_{pp}$</td>
</tr>
</tbody>
</table>

Since the coefficients of the first four rows satisfy the first hypoabelian conditions which affect those rows, there exist values of

$$a_{ij}, \ \gamma_{ij}, \ \beta_{ij}, \ \delta_{ij} \quad (i = 3, \ldots, p; \ j = 1, \ldots, p)$$

for the remaining $2p - 4$ rows which give rise to a first hypoabelian substitution.*

9. It follows that $P = TQ$, where $Q$ is a substitution of $G_1$ which leaves fixed the symbols $\left(00 \ 11 \ 00 \ \ldots \ \right)$, $\left(10 \ 11 \ 00 \ \ldots \ \right)$, and $\left(01 \ 11 \ 00 \ \ldots \ \right)$. Since $Q$ leaves $\phi_3$ fixed, it will leave invariant the functions $\tau$, $\tau_1$, $\tau_2$ which occur in $\phi_3$ each multiplied by the respective factors $\left(00 \ 11 \ \ldots \right)\left(10 \ 11 \ \ldots \right)$, $\left(10 \ 11 \ \ldots \right)\left(01 \ 11 \ \ldots \right)$, $(10 \ 11 \ \ldots)\left(01 \ 11 \ \ldots \right)$, namely,

$$\tau \equiv \sum (x_1 y_1 \ x_2 y_2 \ \ldots \ ) (x_1 + 1 \ y_1 \ x_2 y_2 \ \ldots \ ),$$

$$\tau_1 \equiv \sum (x_1 y_1 \ x_2 y_2 \ \ldots \ ) (x_1 y_1 + 1 \ x_2 y_2 \ \ldots \ ),$$

$$\tau_2 \equiv \sum (x_1 y_1 \ x_2 y_2 \ \ldots \ ) (x_1 + 1 \ y_1 + 1 \ x_2 y_2 \ \ldots \ ).$$

*The successive generality theorem, American Journal, l. c.
Hence $Q$ will permute amongst themselves the $q$ symbols which occur in $\tau$ and $\tau_1$, but not in $\tau_2$, subject therefore to the conditions

$$\sum_{i=1}^{p} x_i y_i = 1, \quad (x_1 + 1)y_1 + \sum_{i=2}^{p} x_i y_i = 1, \quad x_1(y_1 + 1) + \sum_{i=2}^{p} x_i y_i = 1,$$

$$(x_1 + 1)(y_1 + 1) + \sum_{i=2}^{p} x_i y_i \equiv 0 \pmod{2}.$$ 

Hence

$$x_1 \equiv y_1, \quad x_1 y_1 \equiv 0, \quad \sum_{i=2}^{p} x_i y_i \equiv 1 \pmod{2}.$$ 

We obtain the $q$ symbols

$$(00 x_2 y_2 x_3 y_3 \cdots), \quad \sum_{i=2}^{p} x_i y_i \equiv 1. \quad (8)$$

10. The theorem that $G_1 = \Gamma$ may now be proved by induction from $2(p-1)$ to $2p$ indices. We denote by $\phi_3^{(p-1)}, \phi_4^{(p-1)}, \ldots$ the functions composed of those terms of $\phi_3, \phi_4, \ldots$, respectively, which are formed exclusively of the symbols $(00 x_2 y_2 x_3 y_3 \cdots)$. We assume that every substitution which leaves fixed $\phi_3^{(p-1)}, \phi_4^{(p-1)}$ is derived from the substitutions of $\Gamma_{p-1}$, the first hypoabelian group on $p-1$ pairs of indices; and proceed to prove that every substitution which leaves fixed $\phi_3, \phi_4$ is derived from the substitutions of $\Gamma \equiv \Gamma_p$. In view of the earlier sections we need only consider the substitutions of the form $Q$ which permute amongst themselves the $q$ symbols $(8)$. Let $Q'$ be the substitution derived from $Q$ by retaining only the cycles on the $q$ symbols. Since $Q'$ leaves $\phi_3^{(p-1)}$ and $\phi_4^{(p-1)}$ invariant, it belongs to $\Gamma_{p-1}$ by hypothesis. We proceed to show that $K = QQ'$ reduces to the identity, so that the theorem will be proved. Now $K$ leaves fixed every symbol $(00 x_2 y_2 x_3 y_3 \cdots)$, as well as $(011100\cdots)$, and $(101100\cdots)$. Hence it leaves fixed the fourth term of $\phi_4$ in the products

$$(001100\cdots)(101100\cdots)(00 x_2 y_2 x_3 y_3 \cdots),$$

$$(001100\cdots)(011100\cdots)(00 x_2 y_2 x_3 y_3 \cdots),$$

which are $(10 x_2 y_2 x_3 y_3 \cdots)$ and $(01 x_2 y_2 x_3 y_3 \cdots)$, respectively. Hence $K$ leaves fixed the fourth term of $\phi_4$ in the product

$$(101 + x_2 + x_3 y_3 011100\cdots)(0010 y_2 + 111100\cdots)(00 1 + x_3 y_3 1 x_3 y_3 x_4 y_4 \cdots),$$

which is $\sigma \equiv (11 x_2 y_2 x_3 y_3 x_4 y_4 \cdots)$, where $x_4 y_4 + \cdots + x_p y_p \equiv 0, x_2 y_2 + x_3 y_3 \equiv 0$. But, in every symbol $\sigma$, $x_2 y_2 + x_3 y_3 + x_4 y_4 + \cdots + x_p y_p \equiv 0$. If there are any terms $\neq 0$, say $x_r y_r$ and $x_s y_s$, where $r > 1, s > 1, r \neq s$, then $x_r y_r + x_s y_s \equiv 0$

* Evidently, $q = R_{p-1} = 2^{p-3} - 2^{p-2}$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Such a symbol \( \sigma \) may be reached in a manner analogous to that by which was obtained the \( \sigma \) having \( x_2 y_2 + x_3 y_3 \equiv 0 \).

Since \( K \) leaves fixed every symbol of the forms

\[
(00 x_2 y_2 x_3 y_3 \cdots), \quad (10 x_2 y_2 x_3 y_3 \cdots), \quad (01 x_2 y_2 x_3 y_3 \cdots), \quad (11 x_2 y_2 x_3 y_3 \cdots),
\]

it leaves every symbol fixed and is the identity.

11. The order \( \Omega_p \) of the group \( G_1 \equiv \Gamma \) may be derived from the preceding investigation. We have, for \( p > 2 \),

\[
\Omega_p = R_p N 2^{p-3} \Omega_{p-1} \div q \equiv (2^{2p-1} - 2^{p-1})(2^{2p-2} - 1) 2^{p-3} \Omega_{p-1} \div (2^{2p-3} - 2^{p-2}),
\]

upon substituting the values of \( R_p, N \) and \( q \) given in the notes to §6 and §9. The factor \( \Omega_{p-1} \div q \) expresses the number of substitutions on the \( q \) symbols \((00 x_2 y_2 x_3 y_3 \cdots)\) which leave invariant the symbol \((00 11 00 \cdots)\). But \( \Gamma_{p-1} \) is transitive on these \( q \) symbols.

After simplification, we derive the recursion formula

\[
\Omega_p = 2^{p-2}(2^p - 1)(2^{p-1} + 1) \Omega_{p-1} \quad (p > 2).
\]

The formula holds also for \( p = 2 \), if we take \( \Omega_1 = 2 \), as must be done in the case of \( \Gamma \), the hypoabelian substitutions on \( \xi_1 \) and \( \eta_1 \) being \( M_1 \) and the identity. The definition of \( G_1 \) for \( p = 1 \) is delusive since \( R_1 = 1 \); but, for \( p = 2 \), \( G_1 \) is formed of the 36 \( = 2(3!)^2 \) substitutions on \( R_2 = 6 \) symbols which leave invariant

\[
\phi_3 \equiv (00 11)(11 01)(11 10) + (11 00)(10 11)(01 11).
\]

We readily find that *

\[
\Omega_p = (2^p - 1) [(2^{2p-2} - 1) 2^{2p-2}] [(2^{2p-4} - 1) 2^{2p-4}] \cdots [(2^2 - 1) 2^2] 2.
\]

The factors of composition of \( \Gamma \) are known to be 2 and \( \frac{1}{2} \Omega_p \), if \( p > 2 \).

12. The question of the generalization of the results of the paper from the field of integers taken modulo 2 to the Galois Field of order \( 2^m \) will be reserved for a later paper. It may be remarked that the results of §§3, 4, 5, and 7 are true for the \( GF[2^m] \); but that the methods of §§6, 8, 9, and 10 would require essential modifications.

*This result is in accord with that obtained otherwise in the Bulletin, l. c.