THE SUBGROUPS OF ORDER A POWER OF 2 OF THE SIMPLE QUINARY ORTHOGONAL GROUP IN THE GALOIS FIELD OF ORDER $p^n = 8l \pm 3$*

BY

LEONARD EUGENE DICKSON

1. The group of all quinary orthogonal substitutions of determinant unity in the $GF[p^n]$, $p > 2$, has a subgroup O_Ω of index 2 which is simple. The latter is simply isomorphic with the quotient-group Q of the quaternary abelian group and the group composed of the identity and the substitution which merely changes the sign of each variable. The difficulty in the employment of Q is apparent, while for O_Ω there is unfortunately no known practical† criterion to distinguish its substitutions from the remaining quinary orthogonal substitutions. While the abelian form seems best adapted to the determination‡ of the subgroups of order a power of p, the orthogonal form is found to possess advantages in the study of the subgroups of order a power of 2.

The case $p^n = 8l \pm 3$, namely, that in which 2 is a not-square in the $GF[p^n]$, is here treated on account of its simplicity (compare in particular §§ 2, 4, 5, 22) and in view of the applications to be made in subsequent papers in these Transactions to the determination of all the subgroups when $p^n = 3$ and $p^n = 5$.

There is established the remarkable result that, independent of the values of p and n (such that p^n is of the form $8l \pm 3$), the group O_Ω contains the same number of distinct sets of conjugate subgroups of order each power of 2, one set of representatives serving for every O_Ω (compare the diagrammatic summary in § 21, the group notations being given in earlier sections in display formulæ separately numbered). Moreover, except for the subgroups of orders 2, 4, and certain types of order 8, the order of the largest subgroup of O_Ω in which a group of order a power of 2 is self-conjugate is independent of p and n.

* Presented to the Society at the Boston meeting, August 31–September 1, 1903. Received for publication, July 28, 1903.

† In the theory we have recourse to the generators (see § 2). When this becomes impracticable, we resort to the isomorphism with the abelian group by means of the "second-compound" theory (compare §§ 11, 40, 44).

‡ Transactions, vol. 4 (1903), pp. 371–386.

By way of check, it may be stated that the results of §§ 10, 11 and all after § 21 were first established by other methods in the case $p^n = 3$ and in part for $p^n = 5$.

Orientation of the case $p^n = 8l \pm 3$, §§ 2–5.

2. The simple quinary orthogonal group O_Ω in the $GF[p^n]$, $p > 2$, has the order

$$\Omega_{n,p} = \tfrac{1}{2}p^{4n}(p^{4n}-1)(p^{2n}-1). \tag{1}$$

We observe the following lowest orders:

$\Omega_{1,3} = 2^6 \cdot 3^4 \cdot 5$, $\Omega_{1,5} = 2^6 \cdot 3^2 \cdot 5^4 \cdot 13$, $\Omega_{1,7} = 2^8 \cdot 3^2 \cdot 5^2 \cdot 7^4$,

$\Omega_{1,11} = 2^6 \cdot 3^2 \cdot 5^2 \cdot 11^4 \cdot 61$, $\Omega_{1,13} = 2^6 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 13^4 \cdot 17$,

$\Omega_{1,17} = 2^{10} \cdot 3^4 \cdot 5 \cdot 17^4 \cdot 29$, $\Omega_{1,19} = 2^6 \cdot 3^4 \cdot 5^2 \cdot 19^4 \cdot 181$, $\Omega_{2,3} = 2^8 \cdot 3^8 \cdot 5^2 \cdot 41$,

$\Omega_{2,5} = 2^8 \cdot 3^2 \cdot 5^8 \cdot 13 \cdot 313$, $\Omega_{2,7} = 2^{10} \cdot 3^2 \cdot 5^4 \cdot 7^8 \cdot 1201$, $\Omega_{3,3} = 2^6 \cdot 3^{12} \cdot 5 \cdot 7^2 \cdot 13^2 \cdot 73$.

Let $p^n = 2k+1$. Then $\frac{1}{2}(p^{2n}+1)$ is odd, while

$$(p^{2n}-1)^2 = 2^6\left[\tfrac{1}{2}k(k+1)\right]^2.$$

Hence $\Omega_{n,p}$ is always divisible by 2^6. The condition that 2^6 shall be the highest power of 2 occurring as a factor is that $\frac{1}{2}k(k+1)$ shall be odd. According as $k = 2t$ or $k = 2t-1$, we have $k = 4j+2$ or $k = 4j+1$, upon replacing the odd number t by $2j+1$. Hence $p^n = 8j+5$ or $8j+3$, respectively.

Theorem. *The highest power of* 2 *occurring as a factor of* $\Omega_{n,p}$ *is* 2^6 *if and only if* $p^n = 8l \pm 3$.

3. By *Linear Groups*, §§ 181, 182, 189, O_Ω is generated by

$$Q_{i,j}^{\alpha,\beta} \equiv (O_{i,j}^{\alpha,\beta})^2, \qquad O_{i,j}^{\rho,\sigma} O_{k,l}^{\rho,\sigma} \qquad (i, j, k, l = 1, \cdots, 5), \tag{2}$$

where α and β are arbitrary solutions of $x^2+y^2=1$, ρ and σ fixed solutions,

$$O_{i,j}^{\alpha,\beta}: \qquad \xi_i' = \alpha\xi_i + \beta\xi_j, \qquad \xi_j' = -\beta\xi_i + \alpha\xi_j \qquad (\alpha^2+\beta^2=1),$$

the cases $p^n = 3$ and $p^n = 5$ alone being exceptional. Let

$$(\xi_i\xi_j): \qquad \xi_i' = \xi_j, \qquad \xi_j' = \xi_i,$$

noting that these *linear* substitutions do not compound as *literal* substitutions; for example, $(\xi_1\xi_3)(\xi_1\xi_2) = (\xi_1\xi_2\xi_3)$. Let

$$C_i: \qquad \xi_i' = -\xi_i, \qquad \xi_j' = \xi_j \qquad (j = 1, \cdots, 5;\ j \neq i).$$

Then for $p^n = 3$, the generators are the C_iC_j, $(\xi_i\xi_j)(\xi_k\xi_l)$, and

$$W = W^{-2}: \quad \begin{aligned} &\xi_1' = \xi_1 - \xi_2 - \xi_3 - \xi_4, \qquad \xi_2' = \xi_1 - \xi_2 + \xi_3 + \xi_4, \\ &\xi_3' = \xi_1 + \xi_2 - \xi_3 + \xi_4, \qquad \xi_4' = \xi_1 + \xi_2 + \xi_3 - \xi_4. \end{aligned}$$

For $p^n = 5$, the generators are the $C_i C_j, (\xi_i \xi_j)(\xi_k \xi_l)$, and

$R = R^{-1}$: $\qquad \xi_1' = \xi_1 + \xi_2 + 2\xi_3, \quad \xi_2' = \xi_1 + 2\xi_2 + \xi_3, \quad \xi_3' = 2\xi_1 + \xi_2 + \xi_3.$

4. The conditions that $Q_{i,j}^{\alpha,\beta}$ shall reduce to $(\xi_i \xi_j) C_i$ are

$$2\alpha^2 = 1, \qquad 2\alpha\beta = -1,$$

solutions of which exist in the $GF[p^n]$, $p > 2$, if and only if 2 is a square. Now 2 is a quadratic residue of all primes of the form $8k \pm 1$ and a quadratic non-residue of all primes $8k \pm 3$. Hence (*Linear Groups*, § 62), 2 is a not square in the $GF[p^n]$, $p > 2$, if and only if p^n is of the form $8l \pm 3$.

THEOREM. *The second type of generators* (2) *may be replaced by* $(\xi_i \xi_j)(\xi_k \xi_l)$ *if and only if* $p^n = 8l \pm 3$.

5. We are therefore led to the group * merely permuting $\xi_1^2, \cdots, \xi_5^2$; viz.,

(3) $\qquad G_{960} = \{$ group generated by all the $C_i C_j$ and $(\xi_i \xi_j)(\xi_k \xi_l)\}$.

For brevity set $C_0 = C_1 C_2 C_3 C_4 C_5$. Then G_{960} has the commutative subgroup

(4) $\qquad G_{16} = \{I,\ C_i C_j\ (i, j = 0, 1, 2, 3, 4, 5; j > i)\}$.

The alternating group on 5 letters is simply isomorphic with the subgroup

(5) $\qquad G_{60} = \{$ group generated by all the $(\xi_i \xi_j)(\xi_k \xi_l)\}$.

Extending the group G_{16} by the substitutions

$B_1 =$ identity, $\quad B_2 = (\xi_1 \xi_2)(\xi_3 \xi_4), \quad B_3 = (\xi_1 \xi_3)(\xi_2 \xi_4), \quad B_4 = (\xi_1 \xi_4)(\xi_2 \xi_3)$,

we obtain a subgroup of G_{960} whose substitutions are given uniquely thus:

(6) $\quad G_{64} = \{B_k,\ B_k C_i C_j\ (k = 1, 2, 3, 4; i, j = 0, 1, \cdots, 5; j > i)\}$.

THEOREM. *The subgroups of* O_Ω *of order the highest power of* 2 *contained in* Ω *are of order* 2^6 *and conjugate with* G_{64} *if and only if* p^n *is of the form* $8l \pm 3$; *namely, if* 2 *is a not-square in the* $GF[p^n]$, $p > 2$.

REPRESENTATIVES OF THE SETS OF CONJUGATE SUBGROUPS OF ORDER A POWER OF 2 WITHIN O_Ω, §§ 6–21.

Distribution of the substitutions of G_{64} *into sets of conjugates.*

6. The substitutions in the four following sets

$$I,\ C_1C_3,\ C_2C_4,\ C_1C_2C_3C_4; \qquad C_1C_5,\ C_3C_5,\ C_1C_2C_4C_5,\ C_2C_3C_4C_5;$$

$$C_2C_5,\ C_4C_5,\ C_1C_2C_3C_5,\ C_1C_3C_4C_5; \qquad C_1C_2,\ C_1C_4,\ C_2C_3,\ C_3C_4;$$

transform B_3 into B_3, $B_3C_1C_3$, $B_3C_2C_4$, $B_3C_1C_2C_3C_4$, respectively. Further,

* Two sets of generational relations for G_{960} are given in *Linear Groups*, p. 293.

the B_i are commutative. Hence B_3 is conjugate within G_{64} only with B_3, $B_3C_1C_3$, $B_3C_2C_4$ and $B_3C_1C_2C_3C_4$. Now $(\xi_3\xi_k)$ transforms G_{64} into itself if $k=2, 3$ or 4. Hence if l and m denote the two integers left in the set $2, 3, 4$ after the exclusion of k, the substitutions

$$B_k,\ B_kC_1C_k,\ B_kC_lC_m,\ B_kC_1C_2C_3C_4$$

form a complete set of conjugates within G_{64}. Next B_i transforms C_1C_5 into C_iC_5, so that the substitutions $C_iC_5(i=1, 2, 3, 4)$ form a complete set of conjugates. Since B_2, B_3 and B_4 transform C_1C_2 into C_1C_2, C_3C_4 and C_3C_4, respectively, C_1C_2 is conjugate only with itself and C_3C_4. Likewise for C_1C_3 and C_2C_4, for C_1C_4 and C_2C_3. Evidently $C_1C_2C_3C_4$ is self-conjugate. Hence B_2, B_3 and B_4 transform $B_kC_1C_2$ into $B_kC_1C_2$, $B_kC_3C_4$ and $B_kC_3C_4$, respectively; while the substitutions of G_{16} transform $B_3C_1C_2$ into $B_3C_1C_2$, $B_3C_2C_3$, $B_3C_1C_4$, $B_3C_3C_4$ and transform $B_3C_3C_4$ into $B_3C_3C_4$, $B_3C_1C_4$, $B_3C_2C_3$, $B_3C_1C_2$. Hence $B_3C_1C_3$ is conjugate only with itself and $B_3C_1C_4$, $B_3C_3C_2$, $B_3C_3C_4$. Applying the above transformation $(\xi_3\xi_k)$, we obtain the conjugates to $B_kC_1C_l$.

Since B_3 is one of four conjugates and since B_i transforms $B_3C_1C_5$ into $B_3C_iC_5$, it follows that the substitutions of G_{64} transform $B_3C_1C_5$ only into $B_3C_iC_5$, $B_3C_1C_3C_iC_5$, $B_3C_2C_4C_iC_5$, or $B_3C_1C_2C_3C_4C_iC_5\equiv B_3C_iC_0$, where $i=1, 2, 3, 4$. Hence $B_3C_iC_5$ is conjugate only with $B_3C_iC_5$ and $B_3C_iC_0(i=1, 2, 3, 4)$. Applying the transformation $(\xi_3\xi_k)$, we obtain the conjugates to $B_kC_1C_5$.

The substitutions of G_{64} fall into the following 16 distinct sets of conjugates:

$$\{I\};\ \{C_1C_2C_3C_4\};\ \{C_1C_k,\ C_lC_m\};\ \{C_iC_5(i=1, 2, 3, 4)\};$$

$$\{B_k,\ B_kC_1C_k,\ B_kC_lC_m,\ B_kC_1C_2C_3C_4\};\ \{C_iC_0(i=1, 2, 3, 4)\};$$

$$\{B_kC_1C_l,\ B_kC_1C_m,\ B_kC_kC_l,\ B_kC_kC_m\};\ \{B_kC_iC_5,\ B_kC_iC_0(i=1, 2, 3, 4)\};$$

where $k=2, 3, 4$, while l and m denote the two integers left in the set 2, 3, 4 after the exclusion of k, the order of l and m being immaterial.

Determination of all the self-conjugate subgroups of G_{64}.

7. If a self-conjugate subgroup H contains one C_iC_5, it contains them all and hence also every $C_iC_j(i, j=1, 2, 3, 4)$, so that H contains G_{16}. Similarly, if H contains one C_iC_0, it contains G_{16}. If H contains C_1C_k, or B_k, or $B_kC_1C_l$, it contains the respective commutative group

(7) $G_4^k=\{I,\ C_1C_k,\ C_lC_m,\ C_1C_2C_3C_4\}$,

(8) $G_8^k=\{B_i,\ B_iC_1C_k,\ B_iC_lC_m,\ B_iC_1C_2C_3C_4(i=1, k)\}$,

(9) $H_8^k=\{I,\ C_1C_k,\ C_lC_m,\ C_1C_2C_3C_4,\ B_kC_1C_l,\ B_kC_1C_m,\ B_kC_kC_l,\ B_kC_kC_m\}$.

If H contains one $B_k C_i C_5$, it contains the group

(10) $H_{16}^k = \{I,\ C_i C_j,\ C_1 C_2 C_3 C_4,\ B_k C_i C_5,\ B_k C_i C_0 (i, j = 1, 2, 3, 4)\}$.

Hence the self-conjugate subgroups of G_{64} *are given by the series*

(11) $I,\ G_2 = \{I,\ C_1 C_2 C_3 C_4\},\ G_4^k,\ G_8^k,\ H_8^k,\ G_{16},\ H_{16}^k (k = 2, 3, 4)$,

together with the groups resulting from the combination of two or more of them.

Now G_2 is a subgroup* of all of order > 2; while G_4^k is a subgroup of G_8^k, H_8^k, G_{16}, H_{16}^2, H_{16}^3, H_{16}^4. Any two of the groups G_4^k combine into

(12) $$G_8 = \{I,\ C_i C_j,\ C_1 C_2 C_3 C_4 (i, j = 1, 2, 3, 4)\}.$$

Combining H_8^k with either G_4^l or G_4^m, we obtain the group

(13) $J_{16}^k = \{I,\ C_i C_j,\ C_1 C_2 C_3 C_4,\ B_k,\ B_k C_i C_j,\ B_k C_1 C_2 C_3 C_4 (i, j = 1, 2, 3, 4)\}$.

The same group results from the combination of G_8^k with either G_4^l or G_4^m; also from the combination of G_8^k with H_8^k. Combining H_8^k with either G_8^l or G_8^m, we get the group of all the substitutions of G_{64} which leave ξ_5 fixed:

(14) $$G_{32} = \{B_t,\ B_t C_i C_j\ B_t C_1 C_2 C_3 C_4 (t, i, j = 1, 2, 3, 4)\}.$$

Combining any two of the groups G_8^2, G_8^3, G_8^4, or any two of the groups H_8^2, H_8^3, H_8^4, we obtain G_{32}. Combining G_{16} with any one of the groups G_8^k, H_8^k, H_{16}^k, we obtain the group

(15) $J_{32}^k = \{I,\ C_i C_j,\ B_k,\ B_k C_i C_j (i, j = 0, 1, 2, 3, 4, 5; j > i)\}$.

The same group results from the combination of H_{16}^k with either G_8^k or H_8^k. Combining H_{16}^l with either G_8^k or H_8^k, we obtain the group

(16) $H_{32}^k = \{I,\ C_i C_j,\ C_1 C_2 C_3 C_4,\ B_k,\ B_k C_i C_j,\ B_k C_1 C_2 C_3 C_4,\ B_t C_i C_5,\ B_t C_i C_0\}$
$(i, j = 1, 2, 3, 4;\ t = 2, 3, 4;\ t \neq k)$.

We have now combined the groups (11) by pairs in every possible way.

The groups G_4^2, G_4^3, G_4^4, G_8 all lie in each of the five new groups (12)–(16), while G_8 lies also in G_{16} and H_{16}^k. Now G_8^k and H_8^k lie in J_{16}^k, G_{32}, J_{32}^k, H_{32}^k, but neither lies in J_{16}^l, J_{32}^l, H_{32}^l. Also G_{16} lies in every J_{32}^k, but not in G_{32}, nor in any H_{32}^k. Finally, H_{16}^k lies in J_{32}^k, H_{32}^l, H_{32}^m, but not in G_{32}, J_{32}^l, H_{32}^k. We have therefore to consider the following compositions:

$$(G_8^k,\ G_8) = (H_8^k,\ G_8) = J_{16}^k, \qquad (G_8^k,\ J_{16}^l) = (H_8^k,\ J_{16}^l) = G_{32},$$

$$(G_8^k,\ J_{32}^l) = (H_8^k,\ J_{32}^l) = G_{64}, \qquad (G_8^k,\ H_{32}^l) = (H_8^k,\ H_{32}^l) = G_{64},$$

* Hence the self-conjugate subgroups may also be determined from a study of the quotient-group G_{64}/G_2.

$$(G_{16}, J^k_{16}) = J^k_{32}, \qquad (G_{16}, G_{32}) = (G_{16}, H^k_{32}) = (H^k_{16}, G_{32}) = G_{64},$$

$$(H^k_{16}, J^k_{16}) = J^k_{32}, \quad (H^k_{16}, J^l_{16}) = H^l_{32}, \quad (H^k_{16}, J^l_{32}) = (H^k_{16}, H^k_{32}) = G_{64},$$

noting finally that any two of the groups G_{32}, J^k_{32}, H^k_{32}, H^l_{32} combine into G_{64}.

THEOREM. *The group G_{64} contains, in addition to itself, exactly the* 26 *self-conjugate subgroups given by formulæ* (11)–(16).

COROLLARY. *The only subgroups of order* 32 *of G_{64} are*

$$G_{32},\ J^k_{32},\ H^k_{32} \qquad (k=2, 3, 4).$$

REMARK. Any three groups marked with the affix $k\,(k = 2, 3, 4)$ are conjugate in O_Ω. No two of the groups J^3_{32}, H^3_{32}, G_{32} are conjugate in O in view of the number of sets of conjugate substitutions in each (§§ 8–10).

Determination of all the self-conjugate subgroups of J^3_{32}.

8. Proceeding as in § 6, we readily find that the substitutions of J^3_{32} fall into the following 14 distinct sets of conjugates:

$$\{I\};\ \{C_1C_2C_3C_4\};\ \{C_1C_3\};\ \{C_2C_4\};\ \{C_1C_2,\ C_3C_4\};\ \{C_1C_4,\ C_2C_3\};$$

$$\{C_1C_5, C_3C_5\}; \{C_2C_5, C_4C_5\}; \{C_1C_2C_3C_5, C_1C_3C_4C_5\}; \{C_1C_2C_4C_5, C_2C_3C_4C_5\};$$

$$\{B_3, B_3C_1C_3, B_3C_2C_4, B_3C_1C_2C_3C_4\};\ \{B_3C_1C_2, B_3C_2C_3, B_3C_1C_4, B_3C_3C_4\};$$

$$\{B_3C_1C_5, B_3C_3C_5, B_3C_1C_0, B_3C_3C_0\};\ \{B_3C_2C_5, B_3C_4C_5, B_3C_2C_0, B_3C_4C_0\}.$$

If a self-conjugate subgroup H contains C_1C_2 or C_1C_4, it contains the group G^2_4 or the group G^4_4, respectively. If H contains C_1C_5 or C_2C_5, it contains one or the other of the commutative groups

(17) $\quad K_4 = \{I,\ C_1C_5,\ C_3C_5,\ C_1C_3\}, \qquad K'_4 = \{I,\ C_2C_5,\ C_4C_5,\ C_2C_4\}.$

If H contains $C_1C_2C_3C_5$ or $C_1C_2C_4C_5$, it contains one or the other of

(18)
$$K''_4 = \{I,\ C_1C_2C_3C_5,\ C_1C_3C_4C_5,\ C_2C_4\},$$
$$K'''_4 = \{I,\ C_1C_2C_4C_5,\ C_2C_3C_4C_5,\ C_1C_3\}.$$

If H contains B_3, it contains G^3_8. If H contains $B_3C_1C_2$, it contains H^3_8. If H contains $B_3C_1C_5$ or $B_3C_2C_5$, it contains the respective commutative group:

(19) $K_8 = \{I,\ C_1C_3,\ C_2C_4,\ C_1C_2C_3C_4, B_3C_1C_5,\ B_3C_3C_5,\ B_3C_1C_0,\ B_3C_3C_0\},$

(20) $K'_8 = \{I,\ C_1C_3,\ C_2C_4,\ C_1C_2C_3C_4, B_3C_2C_5,\ B_3C_4C_5,\ B_3C_2C_0,\ B_3C_4C_0\}.$

Hence the self-conjugate subgroups of J^3_{32} are given by the series

(21)
$$I,\ G_2,\ G'_2 = \{I,\ C_1C_3\},\ G''_2 = \{I,\ C_2C_4\},\ G^2_4,\ G^4_4,$$
$$K_4,\ K'_4,\ K''_4,\ K'''_4,\ G^3_8,\ H^3_8,\ K_8,\ K'_8,$$

together with the groups resulting from their composition. Now

$$(G_2,\ G_2') = (G_2,\ G_2'') = (G_2',\ G_2'') = G_4^3.$$

Also, G_2 lies in every G_4^k, G_8^k, H_8^k, K_8, K_8'; $(G_2,\ K_4)$ and $(G_2,\ K_4')$ give

(22) $$G_8' = \{I,\ C_1C_3,\ C_2C_4,\ C_1C_2C_3C_4,\ C_1C_5,\ C_3C_5,\ C_1C_0,\ C_3C_0\},$$

(23) $$G_8'' = \{I,\ C_1C_3,\ C_2C_4,\ C_1C_2C_3C_4,\ C_2C_5,\ C_4C_5,\ C_2C_0,\ C_4C_0\},$$

respectively. Also,

$$(G_2,\ K_4'') = G_8'',\ (G_2,\ K_4''') = G_8',\ (G_2',\ G_4^2) = (G_2',\ G_4^4) = G_8,$$
$$(G_2',\ K_4') = G_8'',\ (G_2',\ K_4'') = G_8'',$$

while G_2' lies in K_4, K_4''', G_8^3, H_8^3, K_8, K_8', G_8', G_8'', G_8. Since

$$C_2C_4 = C_1C_3 \cdot C_1C_2C_3C_4,$$

nothing new results from a combination by G_2'', By § 9, the groups G_4^2, G_4^3, G_4^4, G_8^3, H_8^3 and G_8 combine to give only the additional group J_{16}^3. Now G_4^2, G_4^4 or G_8 combine with any of the groups K_4, K_4', K_4'', K_4''', G_8', G_8'' to give G_{16}. Combining G_4^2 or G_4^4 with either K_8 or K_8', we get H_{16}^3. Combining G_4^3 with either K_4 or K_4''', we get G_8'; G_4^3 with either K_4' or K_4'', we get G_8''. Now G_4^3 is a subgroup of K_8, K_8', G_8, G_8' and G_8''. Next, K_4 with K_4' or K_4'' gives G_{16}, K_4' or K_4'' with K_4''' gives G_{16}, K_4 with K_4''' gives G_8', K_4' with K_4'' gives G_8''. Next, $(K_4,\ G_8^3)$ and $(K_4',\ G_8^3)$ are respectively

(24) $$G_{16}' = \left\{\begin{matrix} B_i,\ B_iC_1C_3,\ B_iC_2C_4,\ B_iC_1C_2C_3C_4, \\ B_iC_1C_5,\ B_iC_3C_5,\ B_iC_1C_0,\ B_iC_3C_0 (i = 1,\ 3) \end{matrix}\right\},$$

(25) $$G_{16}'' = B_2^{-1} G_{16}' B_2.$$

Also, K_4'' with G_8^3 gives G_{16}'', K_4''' with G_8^3 gives G_{16}', K_4 and K_4' with H_8^3 give

(26) $$\begin{aligned} H_{16}' = \{&I,\ C_1C_3,\ C_2C_4,\ C_1C_2C_3C_4,\ C_1C_5,\ C_3C_5,\ C_1C_0,\ C_3C_0,\ B_3C_1C_2, \\ &B_3C_1C_4,\ B_3C_2C_3,\ B_3C_3C_4,\ B_3C_2C_5,\ B_3C_4C_5,\ B_3C_2C_0,\ B_3C_4C_0\}, \end{aligned}$$

(27) $$H_{16}'' = B_2^{-1} H_{16}' B_2,$$

respectively. Next, K_4'' with H_8^3 gives H_{16}'', K_4''' with H_8^3 gives H_{16}',

$$(K_4,\ K_8) = (K_4''',\ K_8) = G_{16}',\ (K_4',\ K_8) = (K_4'',\ K_8) = H_{16}''.$$

Interchanging the subscripts 1 with 2 and 3 with 4, we obtain as the compounds of K_8' with K_4, K_4', K_4'', K_4''', the groups H_{16}' and H_{16}''. Next,

$$(G_8^3,\ K_8) = G_{16}',\ (G_8^3,\ K_8') = G_{16}'',\ (H_8^3,\ K_8) = H_{16}'',\ (H_8^3,\ K_8') = H_{16}',$$
$$(K_8,\ K_8') = H_{16}^3,\ (G_8',\ G_8^3) = G_{16}',\ (G_8',\ H_8^3) = H_{16}',\ (G_8'',\ G_8^3) = G_{16}'',$$

and $(G_8'', H_8^3) = H_{16}''$. Finally, a combination of a group of order 16 with a group not a subgroup of it evidently gives J_{32}^3.

THEOREM. *The group J_{32}^3 contains exactly 26 self-conjugate subgroups:*

$$I,\ G_2,\ G_2',\ G_2'',\ G_4^2,\ G_4^3,\ G_4^4,\ K_4,\ K_4',\ K_4'',\ K_4''',\ G_8^3,\ H_8^3,$$

$$K_8,\ K_8',\ G_8,\ G_8',\ G_8'',\ G_{16},\ G_{16}',\ G_{16}'',\ H_{16}',\ H_{16}'',\ J_{16}^3,\ H_{16}^3,\ J_{32}^3.$$

COROLLARY. *There are exactly 7 subgroups of order 16 of J_{32}^3.*

Determination of all the self-conjugate subgroups of H_{32}^3.

9. Its substitutions fall into the following 11 distinct sets of conjugates:

$\{I\}$; $\{C_1C_2C_3C_4\}$; $\{C_1C_2,\ C_3C_4\}$; $\{C_1C_3,\ C_2C_4\}$; $\{C_1C_4,\ C_2C_3\}$; $\{B_3, B_3C_1C_3, B_3C_2C_4, B_3C_1C_2C_3C_4\}$; $\{B_3C_1C_2, B_3C_1C_4, B_3C_2C_3, B_3C_3C_4\}$; $\{B_2C_1C_5, B_2C_3C_5, B_2C_1C_0, B_2C_3C_0\}$; $\{B_2C_2C_5, B_2C_4C_5, B_2C_2C_0, B_2C_4C_0\}$; $\{B_4C_1C_5, B_4C_3C_5, B_4C_1C_0; B_4C_3C_0\}$; $\{B_4C_2C_5, B_4C_4C_5, B_4C_2C_0, B_4C_4C_0\}$.

Forming the group generated by each substitution and its conjugates, we get

$$I,\ G_2,\ G_4^2,\ G_4^3,\ G_4^4,\ G_8^3,\ H_8^3,\ H_{16}^2,\ H_{16}^2,\ H_{16}^4,\ H_{16}^4,$$

respectively. Combining two or more of them, we obtain the additional groups

$$G_8,\ J_{16}^3,\ H_{32}^3.$$

THEOREM. *The only self-conjugate subgroups of H_{32}^3, aside from itself and the identity, are G_2, G_4^2, G_4^3, G_4^4, G_8^3, H_8^3, G_8, H_{16}^2, H_{16}^4, J_{16}^3.*

COROLLARY. *There are exactly 3 subgroups of order 16 in H_{32}^3.*

The self-conjugate subgroups of G_{32}.

10. Its substitutions fall into exactly 17 distinct sets of conjugates. Indeed, aside from the self-conjugate substitutions I and $C_1C_2C_3C_4$, any substitution S is conjugate only with itself and $SC_1C_2C_3C_4$. Now every substitution of G_{32} is of period 2 except identity and the following 12:

$$B_kC_1C_l, \qquad B_kC_kC_l \qquad (k, l = 2, 3, 4;\ k \neq l),$$

the square of any one of which is $C_1C_2C_3C_4$. It follows that, if S ranges over a set of 15 substitutions obtained by taking one and only one of each pair of conjugates within G_{32}, the groups

(28) I, $G_2 = \{I,\ C_1C_2C_3C_4\}$; $K_4^S = \{I,\ C_1C_2C_3C_4,\ S,\ SC_1C_2C_3C_4\}$,

together with the groups resulting from their composition, give all the self-conjugate subgroups of G_{32}.

It is more convenient to proceed by a different method. From what precedes, the quotient-group $Q_{16} = G_{32}/G_2$ is a commutative group all of whose operators, aside from the identity, are of period 2. The quotient of

$$(16-1)(16-2)(16-4) \quad \text{by} \quad (8-1)(8-2)(8-4)$$

gives 15 as the number of subgroups of order 8 of Q_{16}. Likewise, it contains 35 subgroups of order 4 and 15 of order 2. To every self-conjugate subgroup of G_{32}, necessarily containing $C_1C_2C_3C_4$ (as shown above), there corresponds an unique subgroup of Q_{16}, and inversely. We may thus readily obtain all the self-conjugate subgroups of G_{32}. Those of orders 1, 2, 4 are given by (28). We desire in particular those of order 16.

Denote by a, b, c, d a set of generators of Q_{16}. As generators of its 15 subgroups of order 8, we may take

$$(a, b, c);\ (a, b, d);\ (a, c, d);\ (b, c, d);\ (a, b, cd);$$

$$(a, c, bd);\ (a, d, bc);\ (b, c, ad);\ (b, d, ac);\ (c, d, ab);$$

$$(a, bd, cd);\ (b, ad, cd);\ (c, ad, bd);\ (d, ac, bc);\ (ad, bd, cd).$$

For the generators of Q_{16} we may take

$$a = C_1C_2, \qquad b = C_1C_3, \qquad c = B_3, \qquad d = B_2,$$

understanding in this section that S and $SC_1C_2C_3C_4$ are identical operators.

The *analytic* substitution $(\xi_1\xi_3\xi_2)$ transforms the group (a, b, c) into

$$(C_2C_3,\ C_1C_2,\ B_2) = (ab, a, d) = (a, b, d).$$

Likewise, $(\xi_1\xi_3\xi_4)$ transforms (a, b, c) into

$$(C_4C_2,\ C_4C_1,\ B_4) = (b, ab, cd) = a, b, cd).$$

As shown in § 11, G_Ω contains a substitution Σ which transforms

$$C_1C_2,\ C_1C_4,\ B_2,\ B_3C_1C_4 \quad \text{into} \quad B_4C_2C_3,\ B_3C_2C_4,\ C_2C_3,\ B_3C_1C_4,$$

respectively. Hence Σ transforms a into $abcd$, b into ad, c into a, d into ab.

It follows that Σ transforms (a, b, d) into $(abcd, ad, ab)$, identical with (ad, bd, cd), and transforms the latter into $(cd, bd, b) = (b, c, d)$. Again, Σ transforms (a, b, c) into (a, d, bc), and the latter into (c, d, ab). Also, Σ transforms (a, b, cd) into (b, c, ad), and the latter into (a, c, d).

Hence the following 9 groups are conjugate within G_Ω:

$$(a, b, c), (a, b, d), (a, b, cd), (ad, bd, cd), (b, c, d),$$

$$(a, d, bc), (c, d, ab), (b, c, ad), (a, c, d).$$

It is next shown that the remaining 6 subgroups are conjugate. Now C_1C_5, which transforms B_i into $B_iC_1C_i$, transforms

$$(a,\ c,\ bd) \qquad \text{into} \qquad (a,\ cb,\ bda) = (a,\ bd,\ cd).$$

But Σ transforms (a, bd, cd) into (b, d, ac), and the latter into (c, ad, bd). Again, C_1C_5 transforms (c, ad, bd) and (b, d, ac) into respectively

$$(B_3C_1C_3,\ B_2,\ B_2C_2C_3) = (d,\ ac,\ bc),$$

$$(C_1C_3,\ B_2C_1C_3,\ B_3C_1C_4) = (b,\ ad,\ cd).$$

To the representatives (a, b, c) and (a, c, bd) of the two sets of conjugate subgroups of G_{16}, we adjoin $C_1C_2C_3C_4$ and obtain respectively

$$(C_1C_2,\ C_1C_3,\ B_3,\ C_1C_2C_3C_4)$$
$$= \{B_t,\ B_tC_iC_j,\ B_tC_1C_2C_3C_4\ (i, j = 1, 2, 3, 4;\ t = 1, 3)\},$$

$$(C_1C_2,\ B_3,\ C_1C_3B_2,\ C_1C_2C_3C_4) = F_{16},$$

the former being J_{16}^3 and the latter defined as follows:

$$(29) \qquad F_{16} = \left\{\begin{matrix} B_t,\ B_tC_1C_2,\ B_tC_3C_4,\ B_tC_1C_2C_3C_4, \\ B_iC_1C_3,\ B_iC_2C_3,\ B_iC_1C_4,\ B_iC_2C_4\ (t = 1, 3;\ i = 2, 4) \end{matrix}\right\}.$$

THEOREM. *Within O_Ω the 15 subgroups of order 16 of G_{32} are conjugate with the groups J_{16}^3 and F_{16}, the latter being not conjugate* (§ 13).

11. THEOREM. *The group O_Ω contains one and but one substitution of period* 3 *which transforms $B_3C_1C_4$ into itself and transforms C_1C_4, C_1C_2, B_2 into $B_3C_2C_4$, $B_4C_2C_3$, C_2C_3, respectively.*

If S is commutative with $(B_3C_1C_4)^2 = C_1C_2C_3C_4$, it replaces ξ_5 by $\pm\xi_5$ (§ 25). Denoting the matrix of S by (α_{ij}), we find that $B_3C_1C_4S = SB_3C_1C_4$ leads to the conditions:

$$\alpha_{31} = -\alpha_{13},\ \alpha_{32} = \alpha_{14},\ \alpha_{33} = \alpha_{11},\ \alpha_{34} = -\alpha_{12},\ \alpha_{41} = \alpha_{23},\ \alpha_{42} = -\alpha_{24},$$
$$\alpha_{43} = -\alpha_{21},\ \alpha_{44} = \alpha_{22}.$$

Hence S is commutative with $B_3C_1C_4$ if and only if it has the form

$$S' = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{14} & 0 \\ \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & 0 \\ -\alpha_{13} & \alpha_{14} & \alpha_{11} & -\alpha_{12} & 0 \\ \alpha_{23} & -\alpha_{24} & -\alpha_{21} & \alpha_{22} & 0 \\ 0 & 0 & 0 & 0 & \pm 1 \end{vmatrix}.$$

The conditions for $C_1C_4S' = S'B_3C_2C_4$ are

$$\alpha_{13} = \alpha_{11}, \qquad \alpha_{14} = \alpha_{12}, \qquad \alpha_{23} = \alpha_{21}, \qquad \alpha_{24} = \alpha_{22}.$$

The conditions for $C_1C_2S' = S'B_4C_2C_3$ and $B_2S' = S'C_2C_3$ then reduce to

$$\alpha_{12} = \alpha_{11}, \qquad \alpha_{21} = -\alpha_{11}, \qquad \alpha_{22} = \alpha_{11}.$$

The resulting substitution is orthogonal if and only if $4\alpha_{11}^2 = 1$. Its determinant is $\pm 16\alpha_{11}^4$. Hence must ± 1 equal $+1$. With these conditions satisfied, $S' = S'^{-2}$ if and only if $\alpha_{11} = -\frac{1}{2}$. Then S' becomes

$$\Sigma = \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & 0 \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

It has been shown that Σ belongs to the group of all orthogonal substitutions of determinant unity. It remains to show that Σ belongs to O_Ω. For $p^n = 3$, $\Sigma = W^2(\xi_2\xi_3\xi_4)$ and hence is in O_Ω. For $p^n = 5$,

$$\Sigma = C_3C_4(\xi_2\xi_4\xi_3)R_{234}C_3C_5R_{124}R_{312}C_2C_5(\xi_1\xi_4\xi_2),$$

and hence belongs to O_Ω. For $p^n = 11$, we find that

$$\Sigma = O_{1,3}^{5,-3}O_{1,2}^{5,-3}(\xi_1\xi_3\xi_4)O_{1,4}^{5,-3}O_{1,3}^{5,-3}(\xi_1\xi_3\xi_4)C_3C_4(O_{2,3}^{5,3}O_{2,4}^{5,3})^2(\xi_2\xi_4\xi_3)C_2C_4,$$

and hence belongs to G_Ω.

We next treat the general case in which -1 is the square of a mark i of the $GF[p^n]$, proceeding as in *Linear Groups*, pp. 179–180. Making the transformation of variables there defined, we find that Σ becomes

	Y_{12}	Y_{13}	Y_{14}	Y_{23}	Y_{24}	Y_{34}
$Y'_{12} =$	$1/4$	$(1+i)/4$	$-i/4$	$-i/4$	$(1-i)/4$	$3/4$
$Y'_{13} =$	$(-1+i)/4$	$(-1-i)/2$	$(1-i)/4$	$(1-i)/4$	0	$(1-i)/4$
$Y'_{14} =$	$-i/4$	$(-1-i)/4$	$1/4$	$-3/4$	$(1-i)/4$	$i/4$
$Y'_{23} =$	$-i/4$	$(-1-i)/4$	$-3/4$	$1/4$	$(1-i)/4$	$i/4$
$Y'_{24} =$	$(-1-i)/4$	0	$(-1-i)/4$	$(-1-i)/4$	$(-1+i)/2$	$(1+i)/4$
$Y'_{34} =$	$3/4$	$(-1-i)/4$	$i/4$	$i/4$	$(-1+i)/4$	$1/4$

This substitution is found to be the second compound of

$$\begin{bmatrix} (1-i)/4 & (1-i)/4 & (3+i)/4 & (-1+i)/4 \\ (-1-i)/4 & (1+i)/4 & (1+i)/4 & (3-i)/4 \\ (3+i)/4 & (-1+i)/4 & (1-i)/4 & (1-i)/4 \\ (1+i)/4 & (3-i)/4 & (-1-i)/4 & (1+i)/4 \end{bmatrix},$$

which is a special abelian substitution. Hence Σ belongs to G_Ω.

Determination of all the self-conjugate subgroups of J_{16}^3.

12. Its substitutions fall into the following 10 distinct sets of conjugates:

$$\{I\};\ \{C_1C_2C_3C_4\};\ \{C_1C_3\};\ \{C_2C_4\};\ \{C_1C_2,\ C_3C_4\};\ \{C_1C_4,\ C_2C_3\};$$
$$\{B_3, B_3C_1C_2C_3C_4\}; \{B_3C_1C_2, B_3C_3C_4\}; \{B_3C_1C_3, B_3C_2C_4\}; \{B_3C_1C_4, B_3C_2C_3\}.$$

The only substitutions of period 4 are $B_3C_1C_2$, $B_3C_3C_4$, $B_3C_1C_4$, $B_3C_2C_3$.

The self-conjugate subgroups of J_{16}^3 are

(30) $$I,\ G_2,\ G_2',\ G_2'',\ G_4^4,\ G_4^S \qquad (S = B_3,\ B_3C_1C_2,\ B_3C_1C_3,\ B_3C_1C_4)$$

together with all their combinations. Now G_2 lies in all these groups of order >2. As shown in §§ 7–8, the groups G_2, G_2', G_2'', G_4^2, G_4^4 combine to give only the additional groups G_4^3 and G_8. Either G_2' or G_2'' combines with K_4^S for $S = B_3$ or $B_3C_1C_3$ to give G_8^3. Either G_2' or G_2'' combines with K_4^S for $S = B_3C_1C_2$ or $B_3C_1C_4$ to give H_8^3. Combining K_4^S and $K_4^{S'}$ for the following pairs

$$(S,\ S') = (B_3,\ B_3C_1C_3),\ (B_3C_1C_2,\ B_3C_1C_4),\ (B_3,\ B_3C_1C_2),$$
$$(B_3,\ B_3C_1C_4),\ (B_3C_1C_2,\ B_3C_1C_3),\ (B_3C_1C_3,\ B_3C_1C_4),$$

we get the respective groups G_8^3, H_8^3, J_8, J_8', J_8'', J_8''', where

(31) $$J_8 = \{I,\ C_1C_2,\ C_3C_4,\ C_1C_2C_3C_4,\ B_3,\ B_3C_1C_2,\ B_3C_3C_4,\ B_3C_1C_2C_3C_4\},$$

(32) $$J_8' = \{I,\ C_1C_4,\ C_2C_3,\ C_1C_2C_3C_4,\ B_3,\ B_3C_1C_4,\ B_3C_2C_3,\ B_3C_1C_2C_3C_4\},$$

(33) $$J_8'' = \{I,\ C_1C_4,\ C_2C_3,\ C_1C_2C_3C_4,\ B_3C_1C_2,\ B_3C_1C_3,\ B_3C_2C_4,\ B_3C_3C_4\},$$

(34) $$J_8''' = \{I,\ C_1C_2,\ C_3C_4,\ C_1C_2C_3C_4,\ B_3C_1C_3,\ B_3C_1C_4,\ B_3C_2C_3,\ B_3C_2C_4\},$$

each of the groups J being non-commutative. Finally G_4^2 combines with the four K_4^S, in order, to give J_8, J_8, J_8''', J_8'''; while G_4^4 combines with them to give J_8', J_8'', J_8'', J_8'.

THEOREM. *The self-conjugate subgroups of* J_{16}^3 *are the groups* (30)–(34), *together with* G_4^3, G_8, G_8^3, H_8^3, J_{16}^3.

COROLLARY. *The only subgroups of order* 8 *of* J^3_{16} *are* G_8, G^3_8, H^3_8, J_8, J'_8, J''_8, J'''_8, *of which the first three only are commutative groups.*

Determination of all the self-conjugate subgroups of F_{16}.

13. Its substitutions fall into the 10 distinct sets of conjugates

$$\{I\};\ \{C_1C_2C_3C_4\};\ \{B_2C_1C_3\};\ \{B_2C_2C_4\};\ \{C_1C_2,\ C_3C_4\};\ \{B_2C_2C_3,\ B_2C_1C_4\};$$
$$\{B_3, B_3C_1C_2C_3C_4\};\ \{B_3C_1C_2, B_3C_3C_4\};\ \{B_4C_1C_3, B_4C_2C_4\};\ \{B_4C_1C_4, B_4C_2C_3\}.$$

Since $B_2C_1C_3$ is of period 4, it follows that F_{16} and J^3_{16} are not isomorphic. The self-conjugate subgroups of F_{16} are the groups

$$(35)\qquad I,\ G_2,\ C_4 = (B_2C_1C_3),\ G^2_4,\ K^S_4\quad (S = B_2C_2C_3,\ B_3,\ B_3C_1C_2,\ B_4C_1C_3,\ B_4C_1C_4),$$

together with all their combinations. Now G_2 lies in all those of order 4. Combining C_4 with the last six groups (35) in turn, we get the commutative groups H^2_8, H^2_8, F_8, F'_8, F_8, F'_8, where

$$(36)\ F_8 = \{I,\ C_1C_2C_3C_4,\ B_3,\ B_3C_1C_2C_3C_4,\ B_iC_1C_3,\ B_iC_2C_4\ (i = 2,\ 4)\},$$

$$(37)\ F'_8 = \{I,\ C_1C_2C_3C_4, B_2C_1C_3, B_2C_2C_4, B_3C_1C_2, B_3C_3C_4, B_4C_1C_4, B_4C_2C_3\}.$$

Combining every pair of the K^S_4, we get F_8, F'_8, J_8 and F^*_8 each one, and F''_8 and F'''_8 each three times, where

$$(38)\ F''_8 = \{I,\ C_1C_2C_3C_4,\ B_3,\ B_3C_1C_2C_3C_4,\ B_iC_1C_4,\ B_iC_2C_3\ (i = 2,\ 4)\},$$

$$(39)\ F'''_8 = \{I, C_1C_2C_3C_4, B_2C_1C_4, B_2C_2C_3, B_3C_1C_2, B_3C_3C_4, B_4C_1C_3, B_4C_2C_4\},$$

$$(40)\ F^*_8 = \{I,\ C_1C_2,\ C_3C_4,\ C_1C_2C_3C_4,\ B_4C_1C_3,\ B_4C_1C_4,\ B_4C_2C_3,\ B_4C_2C_4\}.$$

Finally, G^2_4 combines with the K^S_4, in order, to give H^2_8, J_8, J_8, F^*_8, F^*_8.

THEOREM.* *The self-conjugate subgroups of* F_{16} *are the groups* (35)–(40), H^2_8, J_8, F^*_8 *and* F_{16}.

COROLLARY. *The group* F_{16} *has exactly* 7 *subgroups of order* 8. *Of them* H^2_8, F_8 *and* F'_8 *are all commutative groups, while* J_8, F^*_8, F''_8 *and* F'''_8 *are not.*

Determination of all the self-conjugate subgroups of H^3_{16}.

14. Its substitutions fall into the 10 distinct sets of conjugates:

$$\{I\};\ \{C_1C_2C_3C_4\};\ \{C_1C_3\};\ \{C_2C_4\};\ \{C_1C_2,\ C_3C_4\};\ \{C_1C_4,\ C_2C_3\};$$
$$\{B_3C_iC_5,\ B_3C_iC_0\}\qquad (i = 1, 2, 3, 4).$$

It contains exactly 8 substitutions of period 4:

* Another proof may be based on the quotient-group, F_{16}/G_2, which is a commutative group all of whose operators aside from identity are of period 2.

$$B_3C_1C_5,\ B_4C_1C_0,\ B_3C_3C_5,\ B_3C_3C_0 \quad \text{(whose squares are } C_1C_3\text{)},$$

and

$$B_3C_2C_5,\ B_3C_2C_0,\ B_3C_4C_5,\ B_3C_4C_0 \quad \text{(whose squares are } C_2C_4\text{)}.$$

Hence H_{16}^3 is not isomorphic with J_{16}^3. Having its self-conjugate substitutions all of period 1 or 2, it is not isomorphic with F_{16}.

The groups I, G_2, G_2', G_2'', G_4^2, G_4^4, K_8, K_8', together with their combinations, give all the self-conjugate subgroups of H_{16}^3. Proceeding as in § 8, we find that the only additional groups are G_4^3, G_8, H_{16}^3.

THEOREM. *The only self-conjugate subgroups of H_{16}^3, aside from itself and identity, are G_2, G_2', G_2'', G_4^2, G_4^3, G_4^4, K_8, K_8', G_8.*

COROLLARY. *The only subgroups of order 8 of H_{16}^3 are K_8, K_8' and G_8.*

The fifteen subgroups of order 8 of G_{16}.

15. Since all the substitutions, except identity, of the commutative group G_{16} are of period 2, it contains exactly 15 subgroups of order 8 (see § 10). Since there are but 5 products each of 4 of the C_i, any subgroup of order 8 contains at least two C_iC_j. Transforming by a suitable even substitution on $\xi_1, \cdots, \xi_5$, we may take C_1C_3 as the first generator. Suppose first that there is present at least one further C_1C_i or one C_3C_j. Transforming C_1C_i by a suitable power of $(\xi_2\xi_4\xi_5)$, we obtain as first and second generators C_1C_3 and C_1C_2. The only resulting groups are G_8 of § 7 and

$$M_8 = \{ I,\ C_1C_3,\ C_1C_2,\ C_2C_3,\ C_1C_5,\ C_3C_5,\ C_2C_5,\ C_1C_2C_3C_5 \},$$

$$N_8 = \{ I,\ C_1C_3,\ C_1C_2,\ C_2C_3,\ C_4C_5,\ C_1C_3C_4C_5,\ C_1C_2C_4C_5,\ C_2C_3C_4C_5 \}.$$

Suppose, however, that there is present no C_1C_i and no C_3C_j other than C_1C_3. Then there must occur one of the following three: C_2C_4, C_2C_5, C_4C_5. But $(\xi_2\xi_5\xi_4)$ transforms C_2C_5 into C_4C_2 while $(\xi_2\xi_4\xi_5)$ transforms C_4C_5 into C_2C_4. Hence we may take C_1C_3 and C_2C_4 as the first and second generators. The group does not contain $C_1C_2C_4C_5$ or $C_2C_3C_4C_5$, not having C_1C_5 or C_3C_5 by assumption. Hence the group can contain only the 8 substitutions forming G_8'' of § 8.

Now $(\xi_2\xi_4\xi_5)$ transforms G_8 into M_8. Also $(\xi_1\xi_2\xi_5\xi_3\xi_4)$ transforms G_8'' into N_8. Finally, G_8, which contains a single product of four C_i, is not conjugate under linear transformation with G_8'', which contains three products of four C_i, since a product of two C_i and a product of four C_i have different characteristic determinants.

THEOREM. *Within O_Ω every subgroup of order 8 of G_{16} is conjugate with G_8 or else with G_8'', while the latter are not conjugate.*

All the self-conjugate subgroups of G'_{16}.

16. Its substitutions fall into the 10 distinct sets of conjugates:

$$\{I\};\ \{C_1C_2C_3C_4\};\ \{C_1C_3\};\ \{C_2C_4\};\ \{C_1C_5,\ C_3C_5\};\ \{C_1C_0,\ C_3C_0\};$$

$$\{B_3, B_3C_1C_3\}; \{B_3C_2C_4, B_3C_1C_2C_3C_4\}; \{B_3C_1C_5, B_3C_3C_5\}; \{B_3C_1C_0, B_3C_3C_0\}.$$

The only substitutions of period 4 are the four in the last two sets. Hence G'_{16} is not isomorphic with H^3_{16}; also, evidently not with F_{16}. Since $B_3C_1C_0$ has the characteristic determinant $(1-\rho)(1+\rho)^2(1+\rho^2)$, while the four substitutions $B_3C_1C_2$, etc., of period 4 in J^3_{16} have the characteristic determinant $(1-\rho)(1+\rho^2)^2$, the groups G'_{16} and J^3_{16} are not conjugate under linear transformation.

The self-conjugate subgroups of G'_{16} are all given by

(41) $\quad I,\ G_2,\ G'_2,\ G''_2,\ K_4,\ K'''_4,\ C^5_4 = (B_3C_1C_5),\ C^0_4 = (B_3C_1C_0),$

(42) $$\begin{cases} K^*_4 = \{I,\ C_1C_3,\ B_3,\ B_3C_1C_3\}, \\ K^{**}_4 = \{I,\ C_1C_3,\ B_3C_2C_4,\ B_3C_1C_2C_3C_4\}, \end{cases}$$

together with their combinations. Now $G'_2 = \{I,\ C_1C_3\}$ is a subgroup of all of order 4. By § 8, any two of G_2, G'_2, G''_2 generate G^3_4, while G_2 with either K_4 or K'''_4 gives G'_8. Also G''_2 with either K_4 or K'''_4 gives G'_8. Either G_2 or G''_2 with either C^5_4 or C^0_4 gives K_8. Either G_2 or G''_2 with either K^*_4 or K^{**}_4 gives G^3_8. Next, K_4 with either C^5_4 or K^*_4 gives

(43) $\quad L_8 = \{I,\ C_1C_5,\ C_3C_5,\ C_1C_3,\ B_3,\ B_3C_1C_5,\ B_3C_3C_5,\ B_3C_1C_3\}.$

Also, K_4 with either C^0_4 or K^{**}_4 gives

(44) $\quad L'_8 = \{I,\ C_1C_5,\ C_3C_5,\ C_1C_3,\ B_3C_1C_0,\ B_3C_3C_0,\ B_3C_5C_0,\ B_3C_2C_4\}.$

Now K'''_4 with either C^0_4 or K^*_4 gives

(45) $\quad T_8 = \{I,\ C_1C_3,\ C_1C_0,\ C_3C_0,\ B_3,\ B_3C_1C_3,\ B_3C_1C_0,\ B_3C_3C_0\}.$

Again, K'''_4 with either C^5_4 or K^{**}_4 gives

(46) $\quad T'_8 = \{I,\ C_1C_3,\ C_1C_0,\ C_3C_0,\ B_3C_1C_5,\ B_3C_3C_5,\ B_3C_5C_0,\ B_3C_2C_4\}.$

Finally, we have the relations

$$(C^5_4,\ C^0_4) = G'_8, \qquad (C^5_4,\ K^*_4) = L_8, \qquad (C^5_4,\ K^{**}_4) = T'_8,$$

$$(C^0_4,\ K^*_4) = T_8, \qquad (C^0_4,\ K^{**}_4) = L'_8, \qquad (K^*_4,\ K^{**}_4) = G^3_8.$$

THEOREM. *The self-conjugate subgroups of G'_{16} are the groups* (41)–(46) *and G^3_4, G'_8, K_8, G^3_8, G'_{16}.*

COROLLARY. *The subgroups of order* 8 *of G'_{16} are L_8, L'_8, T_8, T'_8, G'_8, K_8, and G^3_8.*

All the self-conjugate subgroups of H'_{16}.

17. Its substitutions fall into the following 10 distinct sets of conjugates:

$$\{I\};\ \{C_1C_2C_3C_4\};\ \{C_1C_3\};\ \{C_2C_4\};\ \{C_1C_5,\ C_3C_5\};\ \{C_1C_0,\ C_3C_0\};$$
$$\{B_3C_1C_2,\ B_3C_2C_3\};\ \{B_3C_1C_4,\ B_3C_3C_4\};\ \{B_3C_2C_5,\ B_3C_4C_0\};$$
$$\{B_3C_4C_5,\ B_3C_2C_0\}.$$

Only the last 8 are of period 4, so that H'_{16} is not isomorphic with G'_{16}, G_{16}, or J^3_{16}. It is not conjugate with F_{16} in view of the periods of their self-conjugate substitutions. Finally, H'_{16} and H^3_{16} are not conjugate * within O_Ω since they are self-conjugate only under J^3_{32} and G_{64}, respectively (§§ 31, 46).

THEOREM. *The only self-conjugate subgroups of* H'_{16} *are* I, G_2, G'_2, G''_2, K_4, K'''_4, H^3_8, K'_8 *and the groups* G^3_4, G'_4, H'_{16}, *resulting from their combination.*

COROLLARY. *The only subgroups of order* 8 *of* H'_{16} *are* H^3_8, K'_8, G'_8.

The non-conjugate subgroups of orders 8, 16, 32 *of* G_{64}.

18. There are 3 distinct sets of conjugate subgroups of order 32 in O_Ω, representatives of which are J^3_{32}, H^3_{32}, G_{32} (end of § 7); 6 distinct sets of order 16, represented by G_{16}, G'_{16}, H'_{16}, J^3_{16}, H^3_{16}, F_{16} (§§ 8–17). These 6 have only the following subgroups of order 8: G_8, G'_8, G''_8, G^3_8, H^3_8, H^2_8, J_8, J'_8, J''_8, J'''_8, F_8, F'_8, F''_8, F'''_8, F^*_8, K_8, K'_8, L_8, L'_8, T_8, T'_8, together with subgroups of G_{16} conjugate with G_8 or G''_8 (§§ 12–17).

Now $B_2 \equiv (\xi_1\xi_2)(\xi_3\xi_4)$ transforms G'_8 into G''_8, and transforms K_8 into K'_8; C_1C_5 transforms J_8 into J'''_8, and J'_8 into J''_8; $(\xi_2\xi_4\xi_3)$ transforms J''_8 into F^*_8; Σ transforms J_8 into F^*_8, F_8 into H^2_8, H^2_8 into F'_8, and F''_8 into J_8. Finally, C_2C_5 transforms L_8 into L'_8, and T_8 into T'_8. Hence the above 21 groups are conjugate within O_Ω with the following:

$$(47)\qquad G_8,\ G'''_8,\ G^3_8,\ J_8,\ L_8,\ T_8,\ H^3_8,\ K_8,\ F'''_8.$$

The numbers of substitutions of period 4 in these groups are respectively

$$0,\ 0,\ 0,\ 2,\ 2,\ 2,\ 4,\ 4,\ 6.$$

In the first place, no two of the groups J_8, L_8, T_8, having exactly 2 substitutions of period 4, are conjugate under O_Ω. Indeed, the two $B_3C_1C_2$ and $B_3C_3C_4$ of J_8 have the characteristic determinant $(1-\rho)(1+\rho^2)^2$, while the two $B_3C_1C_5$ and $B_3C_3C_5$ of L_8 and the two $B_3C_1C_0$ and $B_3C_3C_0$ of T_8 all have

* Another proof follows from Lemma I, § 22, taking $t=5$, since S transforms $C_1C_2C_3C_4$ into a substitution of G_{960} only if it replaces some ξ_r by $\pm\xi_5$. Then $r=5$, since S must transform C_1C_3 and C_2C_4 amongst themselves. Hence S replaces ξ_5 by $\pm\xi_5$ and cannot transform C_1C_2 or C_1C_4 into a substitution involving ξ_5.

the characteristic determinant $(1-\rho)(1+\rho)^2(1+\rho^2)$. Moreover, the five of period 2 in L_8 all have the characteristic determinant $(1+\rho)^2(1-\rho)^3$, while $C_1C_0 \equiv C_2C_3C_4C_5$ of T_8 has $(1+\rho)^4(1-\rho)$.

In the second place, the groups H_8^3 and K_8 are not conjugate, since the four of period 4 in H_8^3 have the characteristic determinant $(1-\rho)(1+\rho^2)^2$, while the four of period 4 in K_8 have $(1-\rho)(1+\rho)^2(1+\rho^2)$.

Finally, no two of the groups G_8, G_8'', G_8^3 are conjugate within O_Ω. Indeed all the substitutions except I and $C_1C_2C_3C_4$, of both G_8 and G_8^3 have the determinant $(1+\rho)^2(1-\rho)^3$, while $C_1C_2C_3C_4$, C_2C_0 and C_4C_0 of G_8'' have the determinant $(1+\rho)^4(1-\rho)$, only four of G_8'' having $(1+\rho)^2(1-\rho)^3$. To show that G_8 and G_8^3 are not conjugate under O_Ω, we note that (§ 34) G_8 is self-conjugate only under G_{192} and (§ 32) G_8^3 only under H_{192}, while G_{192} contains a single subgroup G_{64} of order 64, and H_{192} three subgroups of order 64.

THEOREM. *Within O_Ω every subgroup of order* 8 *is conjugate with one and but one of the nine groups* (47).

The subgroups of order 4.

19. The commutative group G_8 of substitutions of period 2, aside from identity, has exactly 7 subgroups of order 4. Any such subgroup contains at least two C_iC_j. Transforming by a suitable even substitution on $\xi_1, \xi_2, \xi_3, \xi_4$, we may take C_1C_2 as the first generator. It contains a second C_iC_j of the form C_2C_3, C_2C_4, or C_3C_4, so that the groups are G_4^2 or

$$G_4 = \{I,\ C_1C_2,\ C_2C_3,\ C_1C_3\};\quad G_4^* = \{I,\ C_1C_2,\ C_2C_4,\ C_1C_4\}.$$

Now B_2 transforms G_4 into G_4^*, and $(\xi_1\xi_5\xi_4)$ transforms G_4^* into K_4'. But G_4^2 and K_4' are not conjugate in view of the characteristic determinants of their substitutions.

Each of the 7 subgroups of order 4 of G_8'' contains at least one C_iC_j. Now $(\xi_2\xi_4\xi_5)$ transforms C_4C_5 into C_2C_4, while $(\xi_2\xi_5\xi_4)$ transforms C_2C_5 into C_2C_4, each transforming G_8'' into itself. As first generator we may therefore take C_1C_3 or C_2C_4. The resulting groups are G_4^3, K_4', K_4'', and

$$G_4' = \{I,\ C_1C_3,\ C_2C_5,\ C_1C_2C_3C_5\},\ G_4'^* = \{I,\ C_1C_3,\ C_4C_5,\ C_1C_3C_4C_5\},$$

the latter being transformed into the former by B_3. But $(\xi_1\xi_5\xi_4)$ transforms G_4' into G_4^2, while B_2 transforms K_4'' into K_4'''.

The commutative group G_8^3 of substitutions of periods 1 and 2 has exactly 7 subgroups of order 4. Now C_1C_5, C_2C_5, C_1C_2, $\Sigma(\xi_2\xi_4\xi_3)$, $\Sigma(\xi_2\xi_4\xi_3)B_2$ transform G_8^3 into itself and, in particular, transform B_3 into $B_3C_1C_3$, $B_3C_2C_4$, $B_3C_1C_2C_3C_4$, C_2C_4, C_1C_3, respectively. Hence we may take C_1C_3 as the first generator of a subgroup of order 4. The group is therefore G_4^3 or else it contains one of the substitutions B_3, $B_3C_1C_3$, $B_3C_2C_4$, $B_3C_1C_2C_3C_4$. Now

I, C_1C_5, C_2C_5, C_1C_2 transform the preceding four amongst themselves transitively. Hence the resulting groups are conjugate with K_4^* of § 16. Its substitutions, other than identity, have the characteristic determinant $(1-\rho)^3(1+\rho)^2$, so that it is not conjugate with either G_4^2 or K_4'''. But K_4^* is not conjugate with K_4' by §§ 38, 42.

The group J_8 contains a single cyclic group $(B_3C_1C_2)$ of order 4. It remains to determine the groups containing only operators of periods 1 and 2. Since B_3 transforms C_1C_2 into C_3C_4, we may take C_1C_2 or B_3 as the first generator. The resulting groups are G_4^2 and $K_4^{B_3}$ of § 10. The latter is transformed into G_4^2 by Σ.

The group H_8^3 contains only two cyclic groups of order 4: $C_4^3 = (B_3C_1C_4)$ and $(B_3C_1C_2)$, the latter being transformed into the former by C_2C_5. The only further subgroup of order 4 is G_4^3.

The group F_8''' has three cyclic groups of order 4: $(B_3C_1C_2)$, $(B_2C_1C_4)$, and $(B_4C_1C_3)$. Now $(\xi_2\xi_3\xi_4)$ transforms $B_4C_1C_3$ into $B_3C_1C_2$; $(\xi_2\xi_4\xi_3)$ transforms $B_2C_1C_4$ into $B_3C_1C_2$.

The commutative group K_8 contains the cyclic subgroups

$$C_4^5 = (B_3C_1C_5), \qquad C_4^0 = (B_3C_1C_0),$$

and a single further subgroup G_4^3 of order 4. But C_2C_5 transforms C_4^0 into C_4^5. Now C_4^5, whose substitutions of period 4 have the characteristic determinant $(1-\rho)(1+\rho)^2(1+\rho^2)$, is not conjugate with C_4^3, for which the corresponding quantity is $(1-\rho)(1+\rho^2)^2$.

The group L_8 contains a single cyclic group C_4^5 and but two further groups of order 4: K_4^* and K_4. Now B_2 transforms K_4 into K_4'.

Finally, T_8 contains C_4^0, K_4^*, K_4''', but no further groups of order 4.

THEOREM. *Within O_Ω, every subgroup of order 4 is conjugate with one and but one of the six groups G_4^2, K_4', K_4^*, K_4''',*

$$C_4^3 = (B_3C_1C_4), \qquad C_4^5 = (B_3C_1C_5). \tag{48}$$

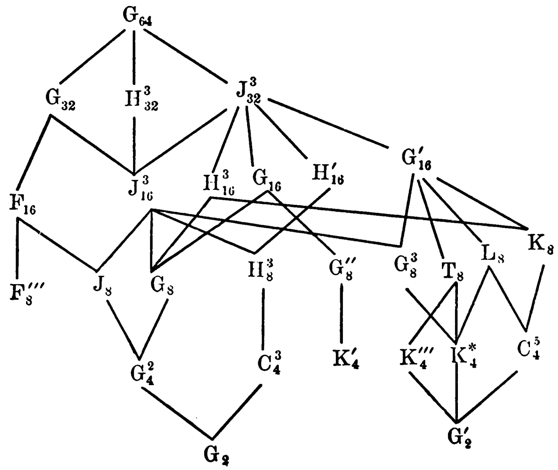
The subgroups of order 2.

20. There are exactly two distinct sets of conjugate operators of period 2 within the simple quaternary abelian group (*Linear Groups*, p. 105). The same consequently holds for O_Ω. As representatives belonging to G_{64}, we may take $C_1C_2C_3C_4$ and C_1C_3, which generate the groups G_2 and G_2', respectively.

THEOREM. *Within O_Ω, every subgroup of order 2 is conjugate with G_2 or G_2'.*

Summary of the subgroups of order a power of 2.

21. Representatives of each distinct set of conjugate subgroups of order a power of 2 within the group O_Ω, together with all their incidences, are exhibited in the following scheme:



LARGEST SUBGROUPS IN WHICH THE GROUPS OF ORDER A POWER OF 2 ARE SELF-CONJUGATE, §§ 22–47.

22. LEMMA I. *If, for $p^n = 8l \pm 3$, a substitution of O_Ω transforms $C_0 C_t$ into a substitution belonging to G_{960}, it replaces one of the variables by $\pm \xi_t$.*

Let S have the matrix (α_{ij}). Then $C_0 C_t$ replaces $\sum_{j=1}^{5} \alpha_{ij} \xi_j$ by

$$-\sum_{\substack{j=1,\ldots,5\\ j\neq t}} \alpha_{ij} \xi_j + \alpha_{it} \xi_t = -\sum_{j=1}^{5} \alpha_{ij} \xi_j + 2\alpha_{it} \xi_t.$$

Since the matrix of S^{-1} is (α_{ji}), it follows that

$$S^{-1} C_0 C_t S: \qquad \xi'_i = -\xi_i + 2\alpha_{it} \sum_{j=1}^{5} \alpha_{jt} \xi_j \qquad (i=1, \cdots, 5).$$

Since 2 is a not-square, no one of the diagonal terms $-1 + 2\alpha^2_{it}$ of the latter is zero. But a substitution of G_{960} has a single non-vanishing coefficient in each row (or column). Hence must

$$\alpha_{it} \alpha_{jt} = 0 \qquad (i, j = 1, \cdots, 5; j \neq i).$$

Hence the product of any two of the five coefficients in the tth column of the matrix of S is zero, so that four are zero. It α_{rt} is the non-vanishing one, all the remaining coefficients in the rth row are zero in view of the orthogonal conditions. Hence S replaces ξ_r by $\alpha_{rt} \xi_t$, where $\alpha^2_{rt} = 1$.

COROLLARY I. *If S transforms each $C_0 C_t (t = 1, 2, 3, 4, 5)$ into a substitution of G_{960}, then S itself belongs to G_{960}.*

COROLLARY II. *If S transforms $C_0 C_t$ into itself, it replaces ξ_t by $\pm \xi_t$:*

Indeed, $-1 + 2\alpha^2_{it} = -1$ gives $\alpha_{it} = 0$ $(i = 1, \cdots, 5;\ i \neq t)$, whence, by the orthogonal conditions, $\alpha_{tj} = 0\,(j \neq t)$.

COROLLARY III. *If S transforms into itself a subgroup of G_{960} which contains a single $C_0 C_t$, then S replaces ξ_t by $\pm \xi_t$.*

Indeed, S transforms $C_0 C_t$ into a substitution in whose matrix each diagonal term is $\neq 0$. Since the latter must belong to G_{960}, it is a product of the C_i. But $C_i C_j$ is not conjugate with $C_0 C_t$, since they have distinct characteristic determinants. Hence $C_0 C_t$ is transformed into itself.

23. LEMMA II. *If a quinary orthogonal substitution S in any $GF[p^n]$, for which $p^n = 8l \pm 3$ or $8l - 1$, transforms each $C_k C_t$ $(k, t = 1, 2, 3, 4)$ into a substitution replacing ξ_5 by $\pm \xi_5$, then S replaces ξ_5 by one of the variables or its negative.*

Taking (α_{ij}) as the matrix of S, we get for $S' = S^{-1} C_k C_t S$:

$$\xi_i' = \xi_i - 2\alpha_{ik} \sum_{j=1}^{5} \alpha_{jk} \xi_j - 2\alpha_{it} \sum_{j=1}^{5} \alpha_{jt} \xi_j \qquad (i = 1, \cdots, 5).$$

The conditions that S' shall replace ξ_5 by $\pm \xi_5$ are

$$1 - 2\alpha_{5k}^2 - 2\alpha_{5t}^2 = \pm 1, \qquad \alpha_{5k}\alpha_{jk} + \alpha_{5t}\alpha_{jt} = 0 \quad (j = 1, 2, 3, 4).$$

According as the upper or lower sign holds, we have

$$\alpha_{5k}^2 + \alpha_{5t}^2 = 0 \qquad \text{or} \qquad \alpha_{5k}^2 + \alpha_{5t}^2 = 1.$$

In the first case, we have the five equations

$$\alpha_{5k}\alpha_{jk} + \alpha_{5t}\alpha_{jt} = 0 \qquad (j = 1, \cdots, 5).$$

But not all the determinants of the second order of the matrix formed of the kth and tth columns of S are zero. Hence $\alpha_{5k} = \alpha_{5t} = 0$. If, in the second case, $\alpha_{5t} = 0$, then $\alpha_{5k} \neq 0$, $\alpha_{jk} = 0$ $(j = 1, 2, 3, 4)$, and $\xi_5' = \alpha_{5k}\xi_k$, in view of the orthogonal conditions.

Now, if every sum of two of the terms α_{51}^2, α_{52}^2, α_{53}^2, α_{54}^2 equals 1, each term equals $\frac{1}{2}$, whence $p^n = 8l \pm 1$. Then $2 + \alpha_{55}^2 = 1$, so that $p^n = 8l + 1$, contrary to assumption. Let next one such sum equal 0; for definiteness, $\alpha_{53}^2 + \alpha_{54}^2 = 0$. Then $\alpha_{53} = \alpha_{54} = 0$. Since $\alpha_{51}^2 + \alpha_{53}^2 = 0$ or 1, $\alpha_{51}^2 = 0$ or 1. Likewise, $\alpha_{52}^2 = 0$ or 1. But $\alpha_{51}^2 + \alpha_{52}^2 = 0$ or 1. Hence at least one of the terms α_{51}^2, α_{52}^2 vanishes. If both vanish, $\xi_5' = \alpha_{55}\xi_5$. If $\alpha_{52} \neq 0$, then $\alpha_{51} = 0$, and $\xi_5' = \alpha_{52}\xi_2$, as shown above.

COROLLARY. *If each transform leaves ξ_5 unaltered, S replaces ξ_5 by $\pm \xi_5$.*

24. Since the $C_0 C_t (t = 1, \cdots, 5)$ generate G_{16}, it follows from Corollary I to Lemma I that *a subgroup of G_{960} containing G_{16} is self-conjugate within O_Ω only under a subgroup of G_{960}.* Now the only even substitutions on $\xi_1, \cdots, \xi_5$ which transform B_k $(k > 1)$ into itself are $B_1 = I$, B_2, B_3, B_4; while the only ones which transform B_2, B_3, B_4 amongst themselves are those of the alternating group on ξ_1, ξ_2, ξ_3, ξ_4.

THEOREM. *Within* O_Ω, G_{16} *is self-conjugate only under* G_{960}, J^k_{32} *is self-conjugate only under* G_{64}, *while* G_{64} *is self-conjugate only under*

$$(49)\quad G_{192} = \left\{ E_t,\ E_t C_i C_j \begin{pmatrix} i, j = 0, 1, 2, 3, 4, 5;\ j > i \\ E_t \text{ ranging over even substitutions on } \xi_1, \cdots, \xi_4 \end{pmatrix} \right\}.$$

25. A substitution S which is commutative with $C_1C_2C_3C_4$ replaces ξ_5 by $\pm\xi_5$ (Corollary II to Lemma I). By *Linear Groups*, p. 160, the number of quaternary orthogonal substitutions of determinant $+1$ is

$$(p^{3n} - p^n)(p^{2n} - 1)p^n.$$

Exactly one half of these belong to O_Ω; for, $S(\xi_1\xi_2)C_1$ is a quaternary orthogonal substitution of determinant $+1$ if S is, while one and but one of the two belongs to O_Ω. Hence the preceding number is the order of the subgroup of O_Ω commutative with $C_1C_2C_3C_4$. Another proof follows from the fact that $C_1C_2C_3C_4$ corresponds (*Linear Groups*, pp. 179–182) to the abelian substitution $T_{1,-1}$. The latter is commutative with exactly $[p^n(p^{2n}-1)]^2$ abelian operators.*

THEOREM. *Within* O_Ω, G_2 *is self-conjugate only under* $G_{p^{2n}(p^{2n}-1)^2}$.

The last group can be given a very simple form when $p^n = 3$. Then

$$\alpha_{i1}^2 + \alpha_{i2}^2 + \alpha_{i3}^2 + \alpha_{i4}^2 \equiv 1 \pmod 3 \qquad (i = 1, 2, 3, 4)$$

requires that one or four of the coefficients in each row of the matrix for S shall $\neq 0$. In the former case, S belongs to G_{192}. In the latter case, $CW^{\pm 1}$ replaces ξ_1 by $\sum_{j=1}^{j=4}\alpha_{1j}\xi_j$, C being a suitably chosen product of an even number of the $C_i\,(i < 5)$. Hence $S = CW^{\pm1}\Gamma$, where Γ leaves ξ_1 unaltered and replaces ξ_5 by $\pm\xi_5$, and therefore belongs to G_{192}. But W transforms C_1C_i into $B_iC_1C_2C_3C_4$, C_1 into WC_1, and C_i into $WB_iC_iC_1C_2C_3C_4$ for $i = 2, 3, 4$. Hence $S = W^{\pm1}\Gamma_1$, where Γ_1 belongs to G_{192}. *Hence, for* $p^n = 3$, *the substitutions commutative with* $C_1C_2C_3C_4$ *form the group*

$$(50)\qquad G_{576} = \{\Gamma,\ W\Gamma,\ W^2\Gamma\ (\Gamma \text{ ranging over } G_{192})\}.$$

26. A substitution is commutative with $B_3C_1C_4$ if and only if it has the form S' of § 11. The orthogonal conditions on S' reduce to the four:

$$(51)\quad \begin{aligned} &\alpha_{11}^2 + \alpha_{12}^2 + \alpha_{13}^2 + \alpha_{14}^2 = 1, \qquad &\alpha_{11}\alpha_{21} + \alpha_{12}\alpha_{22} + \alpha_{13}\alpha_{23} + \alpha_{14}\alpha_{24} = 0, \\ &\alpha_{21}^2 + \alpha_{22}^2 + \alpha_{23}^2 + \alpha_{24}^2 = 1, \qquad &-\alpha_{13}\alpha_{21} + \alpha_{14}\alpha_{22} + \alpha_{11}\alpha_{23} - \alpha_{12}\alpha_{24} = 0. \end{aligned}$$

* Transactions, vol. 2 (1901), bottom of p. 109. The number is the same for the quotient-group of order Ω since P_{12} transforms $T_{1,-1}$ into $T_{2,-1} = T_{1,-1}\cdot T_{1,-1}\,T_{2,-1}$.

If $\alpha_{11}^2 + \alpha_{13}^2 \neq 0$, the equations (51) in the second column give

$$\alpha_{21} = r\alpha_{22} + s\alpha_{24}, \qquad \alpha_{23} = s\alpha_{22} - r\alpha_{24}, \tag{52}$$

where

$$r = \frac{\alpha_{13}\alpha_{14} - \alpha_{11}\alpha_{12}}{\alpha_{11}^2 + \alpha_{13}^2}, \quad s = \frac{-\alpha_{11}\alpha_{14} - \alpha_{12}\alpha_{13}}{\alpha_{11}^2 + \alpha_{13}^2}, \quad r^2 + s^2 = \frac{\alpha_{12}^2 + \alpha_{14}^2}{\alpha_{11}^2 + \alpha_{13}^2}. \tag{53}$$

It follows that

$$\alpha_{21}^2 + \alpha_{23} = (r^2 + s^2)(\alpha_{22}^2 + \alpha_{24}^2), \quad \sum_{j=1}^{4} \alpha_{2j}^2 = \frac{(\alpha_{22}^2 + \alpha_{24}^2)(\alpha_{11}^2 + \alpha_{12}^2 + \alpha_{13}^2 + \alpha_{14}^2)}{\alpha_{11}^2 + \alpha_{13}^2}.$$

The conditions (51) therefore reduce to (52) together with

$$\alpha_{11}^2 + \alpha_{12}^2 + \alpha_{13}^2 + \alpha_{14}^2 = 1, \qquad \alpha_{22}^2 + \alpha_{24}^2 = \alpha_{11}^2 + \alpha_{13}^2. \tag{54}$$

By *Linear Groups*, p. 46, the equation $\alpha_{11}^2 + \alpha_{13}^2 = \kappa$ has $p^n - \nu$ or $p^n + p^n\nu - \nu$ sets of solutions in the $GF[p^n]$, where $\nu = \pm 1$ according as $p^n = 4l \pm 1$. Hence there are $p^{2n} - (2p^n + \nu p^n - 2\nu)$ sets α_{11}, α_{13} for which $\alpha_{11}^2 + \alpha_{13}^2$ is neither 0 nor 1. Each such set furnishes $p^n - \nu$ sets α_{12}, α_{14} satisfying $\alpha_{12}^2 + \alpha_{14}^2 = 1 - (\alpha_{11}^2 + \alpha_{13}^2)$. Next, each of the $p^n - \nu$ sets of solutions of $\alpha_{11}^2 + \alpha_{13}^2 = 1$ furnishes $p^n + p^n\nu - \nu$ sets α_{12}, α_{14}. Hence there are

$$(p^n - \nu)[(p^{2n} - 2p^n - \nu p^n + 2\nu) + (p^n + p^n\nu - \nu)] = (p^n - \nu)(p^{2n} - p^n + \nu)$$

sets $\alpha_{11}, \cdots, \alpha_{14}$ satisfying the first condition * (54) and $\alpha_{11}^2 + \alpha_{13}^2 \neq 0$.

If $\alpha_{11}^2 + \alpha_{13}^2 = 0$, then $\alpha_{12}^2 + \alpha_{14}^2 = 1$. The last equations (51) now give

$$\alpha_{22} = \alpha\alpha_{21} + \beta\alpha_{23}, \qquad \alpha_{24} = \beta\alpha_{21} - \alpha\alpha_{23}, \tag{52'}$$

where

$$\begin{gathered} \alpha = -\alpha_{11}\alpha_{12} + \alpha_{13}\alpha_{14}, \qquad \beta = -\alpha_{12}\alpha_{13} - \alpha_{11}\alpha_{14}, \\ \alpha^2 + \beta^2 = (\alpha_{11}^2 + \alpha_{13}^2)(\alpha_{12}^2 + \alpha_{14}^2) = 0. \end{gathered} \tag{53'}$$

Hence $\alpha_{22}^2 + \alpha_{24}^2 = 0$. The condition (51) therefore reduce to (52′) and

$$\alpha_{11}^2 + \alpha_{13}^2 = 0, \qquad \alpha_{12}^2 + \alpha_{14}^2 = 1, \qquad \alpha_{21}^2 + \alpha_{23}^2 = 1. \tag{54'}$$

and hence have $(p^n - \nu)^2(p^n + p^n\nu - \nu)$ sets of solutions α_{ij}.

The total number of sets of solutions of (51) is thus $(p^n - \nu)^2(p^{2n} + p^n\nu)$.

The determinant of S' is seen to equal

$$\pm\{(\alpha_{11}^2 + \alpha_{12}^2 + \alpha_{13}^2 + \alpha_{14}^2)(\alpha_{21}^2 + \alpha_{22}^2 + \alpha_{23}^2 + \alpha_{24}^2)$$
$$- (\alpha_{11}\alpha_{21} + \alpha_{12}\alpha_{22} + \alpha_{13}\alpha_{23} + \alpha_{14}\alpha_{24})^2 - (-\alpha_{13}\alpha_{21} + \alpha_{14}\alpha_{22} + \alpha_{11}\alpha_{23} - \alpha_{12}\alpha_{24})^2\}$$

and hence by (51) equals ± 1. The sign $\pm$ must therefore be taken $+$.

---

* Since this has $p^{3n} - p^n$ sets of solutions (*Linear Groups*, p. 47), we obtain a second proof.

For $p^n = 3$, only half of the resulting 96 orthogonal substitutions S' of determinant $+1$ belong to O_Ω. These are seen to be

$$(55)\quad B_i,\ B_iC_1C_3,\ B_iC_2C_4,\ B_iC_1C_2C_3C_4,\ B_jC_1C_2,\ B_jC_2C_3,\ B_jC_1C_4,\ B_jC_3C_4 \qquad (i=1,4;\ j=2,3)$$

together with their products on the left by $W(\xi_2\xi_4\xi_3)$ and its inverse $W^2(\xi_2\xi_3\xi_4)$.

For $p^n = 5$, it will be shown that exactly half of the resulting 480 orthogonal substitutions S' of determinant $+1$ belong to O_Ω. Assuming first that 3 of the α_{1j} are zero, we obtain the 16 substitutions (55) and 16 others not in O_Ω. Assume next that exactly one of the α_{1j} is zero. Then two of the α_{1j}^2 are $+1$ and one is -1, so that there are 12 types. For example,* take $\alpha_{11}^2 = \alpha_{12}^2 = +1$, $\alpha_{13}^2 = -1$, $\alpha_{14} = 0$. By (54′), $\alpha_{21}^2 + \alpha_{23}^2 = 1$. Hence either $\alpha_{21} = 0$, whence $\alpha_{22} = -\alpha_{12}\alpha_{13}\alpha_{23}$, $\alpha_{24} = \alpha_{11}\alpha_{12}\alpha_{23}$ by (52′), or else $\alpha_{23} = 0$, whence

$$\alpha_{22} = -\alpha_{11}\alpha_{12}\alpha_{21}, \qquad \alpha_{24} = -\alpha_{12}\alpha_{13}\alpha_{21}.$$

In the respective cases, S' becomes

$$S_1' = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & 0 & 0 \\ 0 & \alpha_{22} & \alpha_{12}\alpha_{13}\alpha_{22} & \alpha_{11}\alpha_{13}\alpha_{22} & 0 \\ -\alpha_{13} & 0 & \alpha_{11} & -\alpha_{12} & 0 \\ \alpha_{12}\alpha_{13}\alpha_{22} & -\alpha_{11}\alpha_{13}\alpha_{22} & 0 & \alpha_{22} & 0 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix} \quad \begin{pmatrix} \alpha_{11}^2 = \alpha_{12}^2 = +1 \\ \alpha_{13}^2 = \alpha_{22}^2 = -1 \end{pmatrix}$$

$$S_2' = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & 0 & 0 \\ -\alpha_{11}\alpha_{12}\alpha_{22} & \alpha_{22} & 0 & \alpha_{11}\alpha_{13}\alpha_{22} & 0 \\ -\alpha_{13} & 0 & \alpha_{11} & -\alpha_{12} & 0 \\ 0 & -\alpha_{11}\alpha_{13}\alpha_{22} & \alpha_{11}\alpha_{12}\alpha_{22} & \alpha_{22} & 0 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix} \quad \begin{pmatrix} \alpha_{11}^2 = \alpha_{12}^2 = \alpha_{22}^2 = +1 \\ \alpha_{13}^2 = -1 \end{pmatrix}.$$

To show that none of the 16 substitutions S_1' belong to O_Ω, denote S_1' by S_1^* when $\alpha_{11} = \alpha_{12} = +1$, $\alpha_{13} = +2$. According as $\alpha_{22} = +2$ or -2, we have for S_1^*

$$R_{123}C_3R_{234}(\xi_2\xi_4)C_2C_3, \qquad \text{or} \qquad R_{123}C_3R_{234}(\xi_2\xi_4)C_3C_4,$$

neither of which belongs to O. Giving to $(\alpha_{11}, \alpha_{12}, \alpha_{13})$ in turn the values $(1, 1, -2)$, $(-1, -1, 2)$, $(-1, -1, -2)$, $(1, -1, 2)$, $(1, -1, -2)$,

* Note that one of the four S', B_4S', $B_3C_1C_2S'$, $B_2C_1C_2S'$ has $\alpha_{14}=0$, while each is commutative with $B_3C_1C_4$. Also, $(\xi_1\xi_2\xi_3)S'$ has $\alpha_{11}^2=-1$, $\alpha_{12}^2=\alpha_{13}^2=+1$, and belongs to O_Ω if and only if S' does.

$-1, 1, 2), (-1, 1, -2)$, we find for S_1': $C_3C_4S_1^*C_3C_4$, $C_3C_4S_1^*C_1C_4$, $S_1^*C_1C_3$, $C_1C_3S_1^*C_1C_3$, $C_1C_4S_1^*C_1C_4$, $C_1C_4S_1^*C_3C_4$, $C_1C_3S_1^*$.

To show that all the 16 substitutions S_2' belong to O_Ω, denote S_2' by S_2^* when $\alpha_{11}=\alpha_{12}=+1$, $\alpha_{13}=+2$. According as $\alpha_{22}=+2$ or -2, we have for S_2^*

$$R_{123}C_2C_5R_{234}C_2C_5, \qquad \text{or} \qquad R_{123}C_3C_4R_{234}C_1C_4.$$

Giving to $(\alpha_{11}, \alpha_{12}, \alpha_{13})$ in turn the values $(1, 1, -2), (-1, -1, 2)$, $-1, -1, -2), (1, -1, 2), (1, -1, -2), (-1, 1, 2), (-1, 1, -2)$, we find for S_2': $C_3C_4S_2^*C_3C_4$, $C_3C_4S_2^*C_1C_4$, $S_2^*C_1C_3$, $C_1C_3S_2C_1C_3$, $C_1C_4S_2C_1C_4$, $C_1C_4S_2^*C_3C_4$, $C_1C_3S_2^*$.

Assume lastly that none of the α_{1j} are zero. Then every $\alpha_{1j}^2 \equiv -1$. By (54), $\alpha_{22}^2+\alpha_{24}^2 \equiv -2$, so that $\alpha_{21}^2+\alpha_{23}^2 \equiv -2 \pmod{5}$. Hence every $\alpha_{2j}^2 \equiv -1$. By (53),

$$r = 2(\alpha_{13}\alpha_{14} - \alpha_{11}\alpha_{12}), \; s = 3(\alpha_{11}\alpha_{14} + \alpha_{12}\alpha_{13}), \; rs \equiv 0.$$

Let first $s \equiv 0$, so that $\alpha_{14} \equiv \alpha_{11}\alpha_{12}\alpha_{13}$, $r \equiv \alpha_{11}\alpha_{12}$. By (52) we find for S':

$$S_3' = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{11}\alpha_{12}\alpha_{13} & 0 \\ \alpha_{11}\alpha_{12}\alpha_{22} & \alpha_{22} & -\alpha_{11}\alpha_{12}\alpha_{24} & \alpha_{24} & 0 \\ -\alpha_{13} & \alpha_{11}\alpha_{12}\alpha_{13} & \alpha_{11} & -\alpha_{12} & 0 \\ -\alpha_{11}\alpha_{12}\alpha_{24} & -\alpha_{24} & -\alpha_{11}\alpha_{12}\alpha_{22} & \alpha_{22} & 0 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

Denote S_3' by S_3^* when $\alpha_{11}=\alpha_{12}=\alpha_{13}=+2$. For $\alpha_{22}=\alpha_{24}=+2$, we have for S_3^*

$$S_3^{**} = C_2C_4(\xi_2\xi_4\xi_3)R_{234}C_2C_4R_{124}(\xi_1\xi_3\xi_2)R_{123}(\xi_1\xi_4\xi_2)C_3C_4.$$

For $\alpha_{22}=\alpha_{24}=-2$, $S_3^*=S_3^{**}C_2C_4$. For $\alpha_{22}=2$, $\alpha_{24}=-2$, S_3^* becomes

$$S_3^{***} = C_2C_4(\xi_2\xi_4\xi_3)R_{234}C_2C_4R_{124}(\xi_1\xi_2\xi_3)R_{123}(\xi_1\xi_4\xi_3\xi_2)C_3.$$

For $\alpha_{22}=-2$, $\alpha_{24}=+2$, S_3^* becomes $S_3^{***}C_2C_4$. Hence S_3^* belongs to O_Ω if and only if $\alpha_{22}=\alpha_{24}$. Next, S_3' becomes $C_2C_4C_3^*C_2C_4$ when $\alpha_{11}=\alpha_{13}=2$, $\alpha_{12}=-2$; hence must $\alpha_{22}=\alpha_{24}$. Again, S_3' becomes $C_2C_4S_3^*C_1C_2C_3C_4$ when $\alpha_{11}=\alpha_{13}=-2$, $\alpha_{12}=+2$, whence must $\alpha_{22}=\alpha_{24}$. Also, $S_3'=S^*C_1C_3$ when $\alpha_{11}=\alpha_{22}=-2$, $\alpha_{13}=-2$, whence must $\alpha_{22}=\alpha_{24}$. Denote S_3' by $[\alpha, \beta]$ when $\alpha_{11}=\alpha_{12}=2$, $\alpha_{13}=-2$. Then $[\alpha, -\beta]=C_3C_4S_3^*C_3C_4$, whence must $\alpha_{22}=-\alpha_{24}$. For $\alpha_{11}=\alpha_{12}=-2$, $\alpha_{13}=+2$, $S_3'=[\alpha,\beta]C_1C_3$, whence must $\alpha_{22}=-\alpha_{24}$. For $\alpha_{11}=2$, $\alpha_{12}=\alpha_{13}=-2$, $S_3'=C_2C_4[-\alpha, -\beta]$, whence must $\alpha_{22}=-\alpha_{24}$. Finally, $S_3'=C_2C_4[-\alpha, -\beta]C_1C_3$, when $\alpha_{11}=-2$, $\alpha_{12}=\alpha_{13}=+2$, whence must $\alpha_{22}=-\alpha_{24}$. To summarize, S_3' belongs to O_Ω only when $\alpha_{22}=+\alpha_{24}$ if $\alpha_{11}=+\alpha_{13}$, and $\alpha_{22}=-\alpha_{24}$ if $\alpha_{11}=-\alpha_{13}$, or briefly, only when $\alpha_{24}=-\alpha_{11}\alpha_{13}\alpha_{22}$.

Let next $r \equiv 0$, so that $\alpha_{14} \equiv -\alpha_{11}\alpha_{12}\alpha_{13}$, $s \equiv \alpha_{12}\alpha_{13}$. Then, by (52),

$$\alpha_{21} = \alpha_{12}\alpha_{13}\alpha_{24}, \qquad \alpha_{23} = \alpha_{12}\alpha_{13}\alpha_{22}.$$

For $\alpha_{11} = \alpha_{12} = \alpha_{13} = \alpha_{22} = \alpha_{24} = +2$, S' becomes* Σ of § 11 and hence belongs to O_Ω. Hence, in view of the preceding case, the general S', with $r = 0$, belongs to O_Ω only when $\alpha_{24} = -\alpha_{11}\alpha_{13}\alpha_{22}$.

We may combine the two preceding cases as follows: An orthogonal substitution S' with every $\alpha_{1j} \neq 0$ belongs to O_Ω if and only if

$$(56) \qquad \alpha_{21} = \alpha_{11}\alpha_{12}\alpha_{22}, \qquad \alpha_{23} = \alpha_{11}\alpha_{14}\alpha_{22}, \qquad \alpha_{24} = -\alpha_{11}\alpha_{13}\alpha_{22}.$$

Hence of the 480 *orthogonal substitutions of determinant unity which are commutative with $B_3C_1C_4$, exactly* 240 *belong to O_Ω for $p^n = 5$.*

In the general case there are exactly $\frac{1}{2}(p^n - \nu)(p^{2n} - 1)p^n$ substitutions of O_Ω commutative with $B_3C_1C_4$, where $\nu = \pm 1$ according as $p^n = 4l \pm 1$. Indeed, $S_1 = (\xi_1\xi_3)C_1S$ is commutative with $B_3C_1C_4$ if S is, while only one of the pair S, S_1 belongs to O_Ω by §§ 3, 4.

Now B_3 transforms $B_3C_1C_4$ into its inverse $B_3C_2C_3$.

THEOREM. *Within O_Ω, the group $C_4^3 = (B_3C_1C_4)$ is self-conjugate only under a group $G_{(p^n-\nu)(p^{2n}-1)p^n}$.*

27. We may now readily determine the largest subgroup transforming G_{32} into itself. The latter has exactly 12 substitutions of period 4: $B_kC_1C_l$, $k, l = 2, 3, 4$; $k \neq l$. They are all conjugate within G_{192}, under which G_{32} is certainly self-conjugate. Indeed, B_3 and C_2C_5 transform $B_3C_1C_4$ into $B_3C_2C_3$ and $B_3C_1C_2$, respectively; $(\xi_2\xi_3\xi_4)$ and $(\xi_2\xi_4\xi_3)$ transform $B_3C_1C_2$ into $B_2C_1C_4$ and $B_4C_1C_3$, respectively: C_2C_5 transforms $B_4C_1C_3$ into $B_4C_1C_2$; B_3 transforms $B_3C_1C_2$ into $B_3C_3C_4$, $B_4C_1C_2$ into $B_4C_3C_4$, and $B_2C_1C_4$ into $B_2C_2C_3$; C_2C_5 transforms $B_2C_2C_3$ into $B_2C_1C_3$; B_2 transforms $B_2C_1C_3$ into $B_2C_2C_4$, and $B_4C_1C_3$ into $B_4C_2C_4$.

We next show that exactly 48 operators of O_Ω transform G_{32} and the substitution $B_3C_1C_4$ each into itself. It will then follow that G_{32} is self-conjugate only under a group of order 12×48.

For $p^n = 3$, this result follows from § 26 since $W^2(\xi_2\xi_3\xi_4)$ transforms G_{32} into itself (§ 11).

For $p^n = 5$ consider in turn the various types of substitutions of O_Ω which are commutative with $B_3C_1C_4$. When 3 of the α_{1j} are zero, there resulted the 16 substitutions (55). Since they belong to G_{192}, they transform G_{32} into itself. When a single α_{1j} is zero, there resulted 12 types of substitutions, one type comprising the 16 substitutions S_2', the substitutions of the remaining types being of the form $\Gamma S_2'$, where Γ belongs to G_{192}. But S_2' transforms C_1C_4 into

* Note that $\Sigma = C_4 S_3^{**} C_4(\xi_2\xi_4\xi_3)$.

$$\begin{bmatrix} -1 & 2\alpha_{12}\alpha_{22} & 2\alpha_{11}\alpha_{13} & 0 & 0 \\ 2\alpha_{12}\alpha_{22} & 1 & 0 & 3\alpha_{11}\alpha_{13} & 0 \\ 2\alpha_{11}\alpha_{13} & 0 & 1 & 2\alpha_{12}\alpha_{22} & 0 \\ 0 & 3\alpha_{11}\alpha_{13} & 2\alpha_{12}\alpha_{22} & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad \left(\begin{matrix} \alpha_{11}^2 = \alpha_{12}^2 = \alpha_{22}^2 = 1 \\ \alpha_{13}^2 = -1 \end{matrix}\right),$$

which does not belong to G_{32} since its non-diagonal terms do not all vanish. Hence the 12 types are all excluded. Finally, when none of the α_{1j} are zero, there resulted the 32 substitutions S of the form S' with every $\alpha_{1j}^2 = \alpha_{2j}^2 = -1$ and satisfying (56). We verify that S transforms $C_1 C_4$ into

$$(57) \qquad \begin{bmatrix} 0 & \lambda & \mu & 0 & 0 \\ \lambda & 0 & 0 & -\mu & 0 \\ \mu & 0 & 0 & \lambda & 0 \\ 0 & -\mu & \lambda & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad \left(\begin{matrix} \lambda = 2\alpha_{12}\alpha_{22} + 2\alpha_{11}\alpha_{13}\alpha_{14}\alpha_{22} \\ \mu = 2\alpha_{11}\alpha_{13} + 2\alpha_{12}\alpha_{14} \end{matrix}\right).$$

Since $\lambda^2 + \mu^2 \equiv 1$, either $\lambda = 0$ or $\mu = 0$. If $\lambda = 0$, then $\alpha_{14} = -\alpha_{11}\alpha_{12}\alpha_{13}$, $\mu = -\alpha_{11}\alpha_{13}$, and (57) is $B_3 C_1 C_3$ or $B_3 C_2 C_4$. If $\mu = 0$, then $\alpha_{14} = \alpha_{11}\alpha_{12}\alpha_{13}$, $\lambda = -\alpha_{11}\alpha_{22}$, and (57) is either B_2 or $B_2 C_1 C_2 C_3 C_4$. Hence (57) belongs to G_{32} in every case.

Next, S transforms $C_1 C_2$ into

$$(58) \qquad \begin{bmatrix} 0 & 0 & \sigma & \rho & 0 \\ 0 & 0 & -\rho & \sigma & 0 \\ \sigma & -\rho & 0 & 0 & 0 \\ \rho & \sigma & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad \left(\begin{matrix} \sigma = 2\alpha_{11}\alpha_{13} - 2\alpha_{12}\alpha_{14} \\ \rho = 2\alpha_{14}\alpha_{22} - 2\alpha_{11}\alpha_{12}\alpha_{13}\alpha_{22} \end{matrix}\right).$$

Since $\rho^2 + \sigma^2 \equiv 1$, either $\rho = 0$ or $\sigma = 0$. If $\rho = 0$, then $\alpha_{14} = \alpha_{11}\alpha_{12}\alpha_{13}$ and (58) is either B_3 or $B_3 C_1 C_2 C_3 C_4$. If $\sigma = 0$, then $\alpha_{14} = -\alpha_{11}\alpha_{12}\alpha_{13}$ and (58) is either $B_4 C_1 C_4$ or $B_4 C_2 C_3$. Hence (58) belongs to G_{32} in every case.

Finally, S transforms B_2 into

$$(59) \qquad \begin{bmatrix} \alpha & 0 & \beta & 0 & 0 \\ 0 & -\alpha & 0 & -\beta & 0 \\ \beta & 0 & -\alpha & 0 & 0 \\ 0 & -\beta & 0 & \alpha & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad \left(\begin{matrix} \alpha = 2\alpha_{11}\alpha_{12} + 2\alpha_{13}\alpha_{14} \\ \beta = 2\alpha_{11}\alpha_{14} - 2\alpha_{12}\alpha_{13} \end{matrix}\right).$$

Then $\alpha^2 + \beta^2 \equiv 1$. If $\alpha = 0$, then $\alpha_{14} = \alpha_{11}\alpha_{12}\alpha_{13}$ and (59) is either $B_3C_1C_3$ or $B_3C_2C_4$. If $\beta = 0$, then $\alpha_{14} = -\alpha_{11}\alpha_{12}\alpha_{13}$ and (59) is either C_1C_4 or C_2C_3. Hence (59) belongs to G_{32} in every case.

The general case will be established indirectly. Of the substitutions transforming $B_3C_1C_4$ into itself and hence also its inverse $B_3C_2C_3$ into itself, B_4 transforms $B_3C_1C_2$ into $B_3C_3C_4$; Σ of § 11 transforms $B_3C_1C_2$ into $B_4C_1C_3$, and the latter into $B_2C_1C_4$; B_4 transforms $B_4C_1C_3$ into $B_4C_2C_4$; $B_2C_1C_2$ transforms $B_2C_1C_4$ into $B_2C_2C_3$. Hence 6 of the 12 substitutions of period 4 in G_{32} are conjugate with $B_3C_1C_2$ by means of substitutions transforming G_{32} and $B_3C_1C_4$ each into itself. We next show that no substitution of O_Ω transforms $B_3C_1C_4$ into itself and $B_3C_1C_2$ into one of the four: $B_4C_1C_2$, $B_4C_3C_4$, $B_2C_1C_3$, $B_2C_2C_4$. The condition $B_3C_1C_2S' = S'B_4C_1C_2$, where S' is given in § 11, requires that every $\alpha_{1j} = \alpha_{2j} = 0$, and hence is impossible. Likewise, $B_3C_1C_2S' = S'B_2C_1C_3$ is impossible. But B_4 transforms $B_4C_1C_2$ into $B_4C_3C_4$, and $B_2C_1C_3$ into $B_2C_2C_4$. Finally, we show that exactly 8 substitutions of O_Ω transform $B_3C_1C_4$ and $B_3C_1C_2$ each into itself. It suffices to find the substitutions which are commutative with both $B_3C_1C_4$ and C_2C_4. Now $C_2C_4S' = S'C_2C_4$ requires that α_{12}, α_{14}, α_{21}, α_{23} all vanish. The resulting special form S'' of S' transforms C_1C_4 into

$$(60)\qquad \begin{vmatrix} \alpha_{13}^2 - \alpha_{11}^2 & 0 & 2\alpha_{11}\alpha_{13} & 0 & 0 \\ 0 & \alpha_{22}^2 - \alpha_{24}^2 & 0 & -2\alpha_{22}\alpha_{24} & 0 \\ 2\alpha_{11}\alpha_{13} & 0 & \alpha_{11}^2 - \alpha_{13}^2 & 0 & 0 \\ 0 & -2\alpha_{22}\alpha_{24} & 0 & \alpha_{24}^2 - \alpha_{22}^2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

This belongs to G_{32}, when 2 is a not-square, if and only if $\alpha_{11}\alpha_{13} = 0$, $\alpha_{22}\alpha_{24} = 0$, since the only conditions on S'' are $\alpha_{11}^2 + \alpha_{13}^2 = 1$, $\alpha_{22}^2 + \alpha_{24}^2 = 1$. For $\alpha_{11} = 0$, S'' belongs to O_Ω if and only if $\alpha_{22} = 0$, whence S'' is $B_3C_1C_2$, $B_3C_1C_4$, $B_3C_2C_3$ or $B_3C_3C_4$, all belonging to G_{32}. For $\alpha_{13} = 0$, then $\alpha_{24} = 0$, whence S'' is I, C_1C_3, C_2C_4, or $C_1C_2C_3C_4$, all belonging to G_{32}.

THEOREM. *Within O_Ω, the group G_{32} is self-conjugate only under*

$$(61)\qquad G_{576} = \{\Gamma,\ \Sigma\Gamma,\ \Sigma^2\Gamma\ (\Gamma \textit{ ranging over } G_{192})\}.$$

28. The group H_{32}^3 is self-conjugate under G_{64} by § 7. Of the 20 substitutions of period 4 in H_{32}^3, the four $B_3C_1C_2$, $B_3C_1C_4$, $B_3C_2C_3$, $B_3C_3C_4$ are conjugate within G_{64}; likewise the eight $B_2C_iC_5$, $B_2C_iC_0$ $(i = 1, 2, 3, 4)$; likewise the eight $B_4C_iC_5$, $B_4C_iC_0$, as follows from the table of conjugate substitutions of G_{64} (§ 6). Now $B_2C_1C_5$ and $B_3C_1C_4$ have the characteristic determinants $(1-\rho)(1+\rho)^2(1+\rho^2)$ and $(1-\rho)(1+\rho^2)^2$, respectively (end of

§ 19). Hence $B_3 C_1 C_4$ is conjugate with only 4 of the substitutions of period 4 of H^3_{32}. We proceed to show that only 16 substitutions of O_Ω transform H^3_{32} and $B_3 C_1 C_4$ each into itself and that the 16 are the substitutions (55) belonging to G_{64}. The proof is similar to that in § 27. Consider first the case $p^n = 5$. Then (57) belongs to H^3_{32} if and only if $\alpha_{14} = -\alpha_{11}\alpha_{12}\alpha_{13}$; (58) belongs to H^3_{32} if and only if $\alpha_{14} = +\alpha_{11}\alpha_{12}\alpha_{13}$. Hence a transformer with each $\alpha_{1j} \neq 0$ is excluded. Those with a single α_{1j} equal zero are excluded as in § 27. For the general case we proceed as at the end of § 27. The only substitutions transforming $B_3 C_1 C_4$ and $B_3 C_1 C_2$ each into itself are 8 substitutions belonging to H^3_{32}. Indeed, (60) belongs to H^3_{32}, when 2 is a not-square, if and only if $\alpha_{11}\alpha_{13} = 0$, $\alpha_{22}\alpha_{24} = 0$.

THEOREM. *Within O_Ω, the group H^3_{32} is self-conjugate only under G_{64}.*

29. The group J^3_{16} is self-conjugate under G_{64} since it is self-conjugate under both G_{32} and J^3_{32} (§§ 8, 10). Within G_{64} the four substitutions of period 4 of J^3_{16} are conjugate with $B_3 C_1 C_4$. It therefore remains only to determine all the substitutions S of O_Ω which transform J^3_{16} and $B_3 C_1 C_4$ each into itself. We proceed as in § 27. For $p^n = 5$, the only substitutions S are the 16 substitutions (55); for, (57) belongs to J^3_{16} if and only if $\alpha_{14} = -\alpha_{11}\alpha_{12}\alpha_{13}$, while (58) belongs J^3_{16} if and only if $\alpha_{14} = +\alpha_{11}\alpha_{12}\alpha_{13}$.

In the general case, S' belongs to G_{64} if it is commutative with $C_2 C_4$ (end of § 27). Within G_{64} the substitutions of period 2 in J^3_{16} fall into sets of conjugates as follows:

$$C_2C_4,\ C_1C_3;\ C_1C_2,\ C_3C_4;\ C_1C_4,\ C_2C_3;\ B_3,\ B_3C_1C_3,\ B_3C_2C_4,\ B_3C_1C_2C_3C_4.$$

The conditions for $C_2 C_4 S' = S' C_1 C_2$ are $\alpha_{1j} = \alpha_{2j} = 0\ (j = 1, 2, 3, 4)$. Likewise, S' cannot transform $C_2 C_4$ into $C_1 C_4$, nor into B_3.

THEOREM. *Within O_Ω, the group J^3_{16} is self-conjugate only under G_{64}.*

30. Since G'_{16} contains $C_1 C_0$, $C_3 C_0$ and $C_5 C_0$, a substitution S commutative with it must replace three variables by $\pm\xi_1$, $\pm\xi_3$, $\pm\xi_5$ (Lemma I, § 22). Since further there exists an even substitution on $\xi_1, \cdots, \xi_5$ which replaces ξ_1, ξ_3, ξ_5 by those three variables, respectively, we may set $S = O^{\lambda,\mu}_{2,4}\Gamma$, where Γ belongs to G_{960}. Now $O^{\lambda,\mu}_{2,4}$ transforms B_3 into $T \equiv (\xi_1\xi_3)T_1$, where T_1 replaces ξ_2 by $2\lambda\mu\xi_2 + (\lambda^2 - \mu^2)\xi_4$. In order that T shall belong to G'_{16}, it is necessary that $T_1 = (\xi_2\xi_4)C$, where C is a product of the C_i. Hence $\lambda\mu = 0$. The case $\lambda = 0$ is excluded if S belongs to O_Ω. Hence $O^{\lambda,\mu}_{2,\mu} = I$ or $C_2 C_4$. Hence S belongs to G_{960}. But the only even substitutions on $\xi_1, \cdots, \xi_5$ which transform B_3 into itself are I, B_2, B_3, B_4. But neither B_2 nor B_4 transforms $C_1 C_0$, $C_3 C_0$, $C_5 C_0$ amongst themselves.

THEOREM. *Within O_Ω, the group G'_{16} is self-conjugate only under J^3_{32}.*

31. By a proof entirely analogous to the preceding, we obtain the

THEOREM. *Within O_Ω, the group H'_{16} is self-conjugate only under J^3_{32}.*

32. A substitution S which transforms G_8^3 into itself must replace ξ_5 by $\pm\xi_5$ (Corollary III of § 22). If S transforms C_1C_3 of G_8^3 into itself, then $S = O_{1,3}O_{2,4}C$, where C is a product of C_i. Now $O_{1,3}^{\lambda,\mu}O_{2,4}^{\rho,\sigma}$ transforms B_3 into a substitution B' which replaces ξ_1 and ξ_2 by

$$2\lambda\mu\xi_1 + (\lambda^2 - \mu^2)\xi_3, \qquad 2\rho\sigma\xi_2 + (\rho^2 - \sigma^2)\xi_4,$$

respectively. Since $\lambda^2 + \mu^2 = 1$ and 2 is a not-square, then $\lambda^2 - \mu^2 \neq 0$. Hence $\lambda\mu = 0$, $\rho\sigma = 0$ if B' belongs to G_8^3, so that S belongs to (G_{16}, B_3). Now G_8^3 is evidently self-conjugate under G_{64}. Within the latter, C_1C_3 and C_2C_4 are conjugate, as also B_3, $B_3C_1C_3$, $B_3C_2C_4$, $B_3B_1C_2C_3C_4$. Hence if O_Ω contains a substitution which transforms C_1C_3 into B_3 and G_8^3 into itself, G_8^3 will be self-conjugate under exactly 6×32 substitutions of O_Ω. Now an orthogonal substitution of period 2 replaces ξ_5 by $\pm\xi_5$ and transforms C_1C_3 into B_3 if and only if it has the form

$$\left|\begin{array}{ccccc} \alpha_{11} & \alpha_{12} & -\alpha_{11} & -\alpha_{12} & 0 \\ \alpha_{12} & \alpha_{22} & \alpha_{12} & \alpha_{22} & 0 \\ -\alpha_{11} & \alpha_{12} & \alpha_{11} & -\alpha_{12} & 0 \\ -\alpha_{12} & \alpha_{22} & -\alpha_{12} & \alpha_{22} & 0 \\ 0 & 0 & 0 & 0 & \pm 1 \end{array}\right| \qquad \left[\begin{array}{l} 4\alpha_{11}^2 = 1 \\ 4\alpha_{12}^2 = 1 \\ 4\alpha_{22}^2 = 1 \end{array}\right].$$

It therefore transforms B_3 into C_1C_3 and $B_3C_1C_3$ and $B_3C_2C_4$ into themselves, and hence G_8^3 into itself. We choose the sign $\pm$ to make the determinant equal $+1$. If S is one such substitution, then $S_1 = S(\xi_1\xi_3)C_5$ is another, since $(\xi_1\xi_3)C_5$ transforms each substitution of G_8^3 into itself. But * either S or S_1 belongs to O_Ω (§ 4).

THEOREM. *Within O_Ω, the group G_8^3 is self-conjugate only under H_{192}.*

33. Since G_8'' contains C_2C_0, C_4C_0 and C_5C_0, a substitution commutative with G_8'' has (as in § 30) the form $O_{1,3}^{\lambda,\mu}\Gamma$, Γ in G_{960}. The first factor is evidently commutative with every substitution of G_8''. It belongs to O_Ω if and only if it is a $Q_{1,3}$ (of § 3), the number of which is $\frac{1}{2}(p^n - \nu)$. But the only even substitutions on $\xi_1, \cdots, \xi_5$ which transforms C_2C_0, C_4C_0 and C_5C_0 amongst themselves are

(62) I, $(\xi_1\xi_3)(\xi_2\xi_4)$, $(\xi_1\xi_3)(\xi_2\xi_5)$, $(\xi_1\xi_3)(\xi_4\xi_5)$, $(\xi_2\xi_4\xi_5)$, $(\xi_2\xi_5\xi_4)$.

THEOREM. *Within O_Ω, the group G_8'' is self-conjugate only under*

(63) $$H_{24(p^n-\nu)} = [\,Q_{1,3}^{\lambda,\mu},\ G_{16},\ (62)\,].$$

For $p^n = 3$ or 5, the only $Q_{1,3}^{\lambda,\mu}$ are I and C_1C_3. Hence $H_{96} = [\,G_{16}, (62)\,]$.

* For $p^n = 5$, the values $\alpha_{11} = \alpha_{12} = \alpha_{22} = 2$, $\pm 1 = -1$, make the transformer equal to
$$C_2C_3C_4C_5(\xi_2\xi_4\xi_3)R_{234}C_2C_4R_{124}(\xi_1\xi_4\xi_3)R_{234}.$$

34. The group G_8 is evidently self-conjugate under G_{192} of § 24. Within the latter C_1C_3 is conjugate with C_1C_2, C_1C_4, C_2C_3, C_2C_4 and C_3C_4. It thus remains to determine the substitutions S which are commutative with both C_1C_3 and G_8. As in § 32, $S = O_{1,3}O_{2,4}C$. But $O_{1,3}^{\lambda,\mu}$ transforms C_1C_2 into a substitution which replaces ξ_1 and ξ_2 by

$$(\mu^2 - \lambda^2)\xi_1 + 2\lambda\mu\xi_3, \qquad (\sigma^2 - \rho^2)\xi_2 + 2\rho\sigma\xi_4,$$

respectively. Hence must $\lambda\mu = 0$, $\rho\sigma = 0$.

THEOREM. *Within O_Ω, the group G_8 is self-conjugate only under G_{192}.*

35. A substitution S commutative with K_8 must replace ξ_5 by $\pm\xi_5$ (Corollary II of § 22), and must transform C_1C_3 into itself or C_2C_4. Hence $S = O_{1,3}O_{2,4}C$ or its product on the right by B_2. Now $O_{1,3}^{\lambda,\mu}O_{2,4}^{\rho,\sigma}$ transforms $B_3C_1C_5$ into

$$\xi_1' = -\xi_3, \qquad \xi_3' = \xi_1, \qquad \xi_2' = 2\rho\sigma\xi_2 + (\rho^2 - \sigma^2)\xi_4,$$

$$\xi_4' = (\rho^2 - \sigma^2)\xi_2 - 2\rho\sigma\xi_4, \qquad \xi_5' = -\xi_5,$$

which belongs to K_8 if and only if $\rho\sigma = 0$. According as $\sigma = 0$ or $\rho = 0$, it becomes $B_3C_1C_5$ or $B_3C_3C_0$, respectively. Hence if $O_{1,3}^{\lambda,\mu}O_{2,4}^{\rho,\sigma}$ belongs to O_Ω it is a $Q_{1,3}$, $Q_{1,3}B_3$, or the product of one of them by C_2C_4. Finally, B_2 does not transform K_8 into itself.

THEOREM. *Within O_Ω, the group K_8 is self-conjugate only under*

$$H_{8(p^n-\nu)} = (Q_{1,3}^{\lambda,\mu},\ B_3,\ G_{16}). \tag{64}$$

For $p^n = 3$ or 5, this group becomes J_{32}^3.

36. A substitution commutative with H_8^3 must be of the type S of § 35. Now $O_{1,3}^{\lambda,\mu}\ O_{2,4}^{\rho,\sigma}$ evidently transforms $B_3C_1C_2 \equiv O_{1,3}^{0,-1}O_{2,4}^{0,-1}$ into itself. Hence it transforms into itself $B_3C_1C_4 \equiv B_3C_1C_2 \cdot C_2C_4$, $B_3C_2C_3 = B_3C_1C_2 \cdot C_1C_3$, $B_3C_3C_4 = B_3C_1C_2 \cdot C_1C_2C_3C_4$. Also, B_2 transforms H_8^3 into itself.

THEOREM. *Within O_Ω, the group H_8^3 is self-conjugate only under*

$$H_{4(p^n-\nu)^2} = (Q_{1,3}^{\lambda,\mu}Q_{2,4}^{\rho,\sigma},\ G_{64}). \tag{65}$$

For $p^n = 3$ or 5, this group becomes G_{64}.

37. A substitution S commutative with G_4^2 must replace ξ_5 by $\pm\xi_5$ (Corollary II of § 22) and transform C_1C_2 into itself or C_2C_4. Hence $S = O_{1,2}O_{3,4}C$ or its product by B_3, respectively.

THEOREM. *Within O_Ω, the group G_4^2 is self-conjugate only under*

$$H'_{4(p^n-\nu)^2} = (Q_{1,2}^{\lambda,\mu}Q_{3,4}^{\rho,\sigma},\ G_{64}). \tag{65'}$$

For $p^n = 3$ or 5, this group becomes G_{64}.

38. The group K_4' is certainly self-conjugate under H_{96} of § 33. Within the latter C_2C_4, C_2C_5 and C_4C_5 are conjugate, and H_{96} has substitutions which transform C_2C_4 into itself and C_2C_5 into C_4C_5. It thus remains to determine the substitutions S commutative with each C_2C_4, C_2C_5, C_4C_5. Now $S = O_{1,\,3}^{\lambda,\,\mu}C$, where C is a product of the C_i.

THEOREM. *Within O_Ω, K_4' is self-conjugate only under $H_{24(p^n-\nu)}$.*

39. A substitution commutative with K_4''' and hence with C_1C_3 is either $S = O_{1,\,3}^{\lambda,\,\mu}O_{2,\,4,\,5}$ or SC_1. Now S transforms $C_1C_2C_4C_5$ into

$$\xi_1' = (\mu^2 - \lambda^2)\xi_1 + 2\lambda\mu\xi_3, \qquad \xi_3' = 2\lambda\mu\xi_1 + (\lambda^2 - \mu^2)\xi_3,$$

$$\xi_2' = -\xi_2, \qquad \xi_4' = -\xi_4, \qquad \xi_5' = -\xi_5.$$

Hence $\lambda\mu = 0$ is the necessary and sufficient condition that the transform shall belong to K_4'''. The substitutions commutative with it are

$$CO_{2,\,4,\,5}, \qquad (\xi_1\xi_3)CO_{2,\,4,\,5} \qquad (C = I,\ C_1,\ C_3,\ C_1C_3).$$

The number of substitutions $O_{2,\,4,\,5}$ of determinant ± 1 is $2(p^{2n}-1)p^n$, by *Linear Groups*, p. 160. Hence $\frac{1}{4}\cdot 8\cdot 2(p^{2n}-1)p^n$ substitutions of O_Ω are commutative with K_4'''.

THEOREM. *Within O_Ω, K_4''' is self-conjugate only under $G_{4p^n(p^{2n}-1)}$.*

COROLLARY. *Exactly $p^n(p^{2n}-1)(p^n-\nu)$ substitutions of O_Ω are commutative with C_1C_3.*

40. A substitution S commutative with J_8 replaces ξ_5 by $\pm\xi_5$. If S is of determinant $+1$ and is commutative with $B_3C_1C_2$ it has the form

$$K = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{14} & 0 \\ \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & 0 \\ -\alpha_{13} & -\alpha_{14} & \alpha_{11} & \alpha_{12} & 0 \\ -\alpha_{23} & -\alpha_{24} & \alpha_{21} & \alpha_{22} & 0 \\ 0 & 0 & 0 & 0 & +1 \end{vmatrix}.$$

If K is commutative with C_1C_2, then $\alpha_{13} = \alpha_{14} = \alpha_{23} = \alpha_{24} = 0$. The resulting $2(p^n-\nu)$ substitutions are commutative with B_3 and hence with J_8 and all belong to O_Ω. If K transforms C_1C_2 into B_3 (and hence B_3 into C_3C_4 and hence J_8 into itself), then $\alpha_{13} = \alpha_{11}$, $\alpha_{14} = \alpha_{12}$, $\alpha_{23} = \alpha_{21}$, $\alpha_{24} = \alpha_{22}$. The orthogonal conditions then reduce to $\alpha_{21} = \pm\alpha_{12}$, $\alpha_{22} = \mp\alpha_{11}$, $\alpha_{11}^2 + \alpha_{12}^2 = \frac{1}{2}$. Denoting the resulting substitution by $K_\pm$, we have $K_- = K_+C_2C_4$. We proceed to show that K_+ (and hence K_-) does not belong to O_Ω. Setting $\alpha_{11} = \alpha$ and $\alpha_{12} = \beta$, we have for K_+

$$[\alpha, \beta] = \begin{bmatrix} \alpha & \beta & \alpha & \beta & 0 \\ \beta & -\alpha & \beta & -\alpha & 0 \\ -\alpha & -\beta & \alpha & \beta & 0 \\ -\beta & \alpha & \beta & -\alpha & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad (\alpha^2 + \beta^2 = \tfrac{1}{2}).$$

For $p^n = 3$, $[1, 1] = W^2(\xi_2\xi_3)C_2$,

$$[-1, -1] = [1, 1]\, C_1C_2C_3C_4, \quad [1, -1] = W^2(\xi_2\xi_3\xi_4)(\xi_1\xi_2)C_1C_2C_4,$$

so that none of the $[\alpha, \beta]$ belong to O_Ω.

For any $GF[p^n]$ in which -1 is the square of a mark i, we make the transformation of variables given in *Linear Groups*, p. 180, and get

	Y_{12}	Y_{13}	Y_{14}	Y_{23}	Y_{24}	Y_{34}
Y'_{12}	$\frac{1}{2}(1+\alpha)$	$-\frac{1}{2}(\alpha+i\beta)$	$\frac{1}{2}i\beta$	$\frac{1}{2}i\beta$	$-\frac{1}{2}(\alpha-i\beta)$	$\frac{1}{2}(1-\alpha)$
Y'_{13}	$\frac{1}{2}(\alpha+i\beta)$	$-i\beta$	$\frac{1}{2}(\alpha-i\beta)$	$\frac{1}{2}(\alpha-i\beta)$	α	$-\frac{1}{2}(\alpha+i\beta)$
Y'_{14}	$\frac{1}{2}i\beta$	$-\frac{1}{2}(\alpha-i\beta)$	$\frac{1}{2}(1-\alpha)$	$-\frac{1}{2}(1+\alpha)$	$\frac{1}{2}(\alpha+i\beta)$	$-\frac{1}{2}i\beta$
Y'_{23}	$\frac{1}{2}i\beta$	$-\frac{1}{2}(\alpha-i\beta)$	$-\frac{1}{2}(1+\alpha)$	$\frac{1}{2}(1-\alpha)$	$\frac{1}{2}(\alpha+i\beta)$	$-\frac{1}{2}i\beta$
Y'_{24}	$\frac{1}{2}(\alpha-i\beta)$	α	$-\frac{1}{2}(\alpha+i\beta)$	$-\frac{1}{2}(\alpha+i\beta)$	$i\beta$	$-\frac{1}{2}(\alpha-i\beta)$
Y'_{34}	$\frac{1}{2}(1-\alpha)$	$\frac{1}{2}(\alpha+i\beta)$	$-\frac{1}{2}i\beta$	$-\frac{1}{2}i\beta$	$\frac{1}{2}(\alpha-i\beta)$	$\frac{1}{2}(1+\alpha)$.

The determinant (141) of *Linear Groups*, p. 154, here equals

$$\tfrac{1}{4}(1 + 2i\beta)(\alpha^2 + i\beta + \beta^2)$$

and must be a square or zero. Applying $\alpha^2 + \beta^2 = \frac{1}{2}$, it reduces to

$$\tfrac{1}{2} \cdot \tfrac{1}{4}(1 + 2i\beta)^2.$$

By proper choice of i as a root of $x^2 = -1$, we can assume that $1 + 2i\beta \neq 0$. But 2 is a not-square. Hence none of the $[\alpha, \beta]$ belong to O_Ω.

Finally, C_1C_2 of J_8 transforms $B_3C_1C_2$ into its inverse $B_3C_3C_4$.

THEOREM. *Within O_Ω, the group J_8 is self-conjugate only under*

$$G_{8(p^n-\nu)} = (G_{32},\ Q^{\lambda,\,\mu}_{1,\,2}\, Q^{\lambda,\,\mu}_{3,\,4}). \tag{66}$$

COROLLARY. For $p^n = 3$ or 5, J_8 is self-conjugate only under G_{32}.

41. A substitution S commutative with F'''_8 replaces ξ_5 by $\pm\xi_5$. Then S is commutative with $B_2C_1C_4$ if and only if it has the form

$$S_1 = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{14} & 0 \\ -\alpha_{12} & \alpha_{11} & \alpha_{14} & -\alpha_{13} & 0 \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \alpha_{34} & 0 \\ \alpha_{32} & -\alpha_{31} & -\alpha_{34} & \alpha_{33} & 0 \\ 0 & 0 & 0 & 0 & \pm 1 \end{bmatrix}.$$

Hence S_1 is commutative with the inverse $B_2C_2C_3$ of $B_2C_1C_4$. There are four further substitutions of period 4 in F_8''': $B_3C_1C_2$, $B_3C_3C_4$, $B_4C_1C_3$, $B_4C_2C_4$. If S_1 is commutative with $B_3C_1C_2$, then $\alpha_{31} = -\alpha_{13}$, $\alpha_{32} = -\alpha_{14}$, $\alpha_{33} = \alpha_{11}$, $\alpha_{34} = \alpha_{12}$. The orthogonal conditions then reduce to $\alpha_{11}^2 + \alpha_{12}^2 + \alpha_{13}^2 + \alpha_{14}^2 = 0$. Hence by *Linear Groups*, p. 47, there are $p^{3n} - p^n$ substitutions S_1' of determinant $+1$ commutative with $B_3C_1C_2$, and consequently commutative with

$$B_2C_1C_4 \cdot B_3C_1C_2 = B_4C_1C_3$$

and hence with the group F_8'''. If S_1 transforms $B_3C_1C_2$ into its inverse, $S_1 = S_1'C_1C_2$. If S_1 transforms $B_3C_1C_2$ into $B_4C_1C_3$, $S_1 = S_1'(\xi_2\xi_4\xi_3)$ and transforms $B_4C_1C_3$ into $B_3C_3C_4$. By symmetry there exist orthogonal substitutions of determinant $+1$ which transform F_8''' into itself and transform $B_2C_1C_4$ into $B_3C_1C_2$ and are commutative with $B_4C_1C_3$. Hence there are $6\cdot 4\cdot(p^{3n} - p^n)$ orthogonal substitutions of determinant $+1$ which are commutative with F_8'''. Exactly half of these belong to O_Ω, since $(\xi_1\xi_2)C_1$ transforms $B_2C_1C_4$, $B_3C_1C_2$ and $B_4C_1C_3$ into $B_2C_1C_4$, $B_4C_2C_4$ and $B_3C_1C_2$, respectively, and hence F_8''' into itself.

THEOREM. *Within O_Ω, F_8''' is self-conjugate only under $G_{12p^n(p^{2n}-1)}$.*

42. The group K_4^* contains I, C_1C_3, B_3 and $B_3C_1C_3$. Now C_1C_5 transforms B_3 into $B_3C_1C_3$, and C_1C_3 into itself. By § 32, O_Ω contains a substitution which transforms C_1C_3 and B_3 into each other. Hence the number of substitutions of O_Ω commutative with K_4^* is 6 times the number commutative with each of its operators. If (α_{ij}) is commutative with C_1C_3, then α_{12}, α_{14}, α_{15}, α_{32}, α_{34}, α_{35}, α_{21}, α_{23}, α_{41}, α_{43}, α_{51}, α_{53} are all zero. If it is also commutative with B_3, then $\alpha_{31} = \alpha_{13}$, $\alpha_{33} = \alpha_{11}$, $\alpha_{42} = \alpha_{24}$, $\alpha_{44} = \alpha_{22}$, $\alpha_{45} = \alpha_{25}$, $\alpha_{54} = \alpha_{52}$. The resulting orthogonal substitutions are

$$(67) \qquad \begin{bmatrix} \alpha_{11} & 0 & \alpha_{13} & 0 & 0 \\ 0 & \alpha_{22} & 0 & \alpha_{24} & \alpha_{25} \\ \alpha_{13} & 0 & \alpha_{11} & 0 & 0 \\ 0 & \alpha_{24} & 0 & \alpha_{22} & \alpha_{25} \\ 0 & \alpha_{52} & 0 & \alpha_{52} & \alpha_{55} \end{bmatrix} \quad \left\{ \begin{array}{l} \alpha_{11}^2 + \alpha_{13}^2 = 1,\ \alpha_{11}\alpha_{13} = 0 \\ \alpha_{22}^2 + \alpha_{24}^2 + \alpha_{25}^2 = 1,\ 2\alpha_{22}\alpha_{24} + \alpha_{25}^2 = 0 \\ 2\alpha_{52}^2 + \alpha_{55}^2 = 2\alpha_{25}^2 + \alpha_{55}^2 = 1 \\ \alpha_{52}(\alpha_{22} + \alpha_{24}) + \alpha_{25}\alpha_{55} = 0 \end{array} \right\}.$$

The condition that the determinant shall equal $+1$ is

$$(68)\qquad (\alpha_{22}-\alpha_{24})[\alpha_{55}(\alpha_{22}+\alpha_{24})-2\alpha_{25}\alpha_{52}]=1.$$

The conditions on $\alpha_{22}, \alpha_{24}, \alpha_{25}, \alpha_{52}, \alpha_{55}$ are seen to reduce to the following:

$$(69)\quad \alpha_{24}=\alpha_{22}\pm 1,\ \alpha_{52}=\pm\alpha_{25},\ \alpha_{55}=\mp 2\alpha_{22}-1,\ 2\alpha_{25}^2+(2\alpha_{22}\pm 1)^2=1.$$

By *Linear Groups*, p. 48, the last condition has $p^n+\nu$ sets of solutions $\alpha_{25}, 2\alpha_{22}\pm 1$, if 2 is a not-square and $\nu=\pm 1$ according as $p^n=4l\pm 1$. There are 4 sets of solutions of $\alpha_{11}^2+\alpha_{13}^2=1$, $\alpha_{11}\alpha_{13}=0$. Of the resulting $2\cdot 4\cdot(p^n+\nu)$ substitutions, half belong to O_Ω, since but one of the pair S and $S(\xi_1\xi_3)C_3$ does.

THEOREM. *Within O_Ω, K_4 is self-conjugate only under $G_{24(p^n+\nu)}$.*

43. The group T_8 contains C_1C_0 and C_3C_0, but no further C_tC_0. Hence, as in the proof of Corollary III of § 22, a substitution S commutative with T_8 must replace the pair ξ_1, ξ_3 by $\pm\xi_1, \pm\xi_3$ in some order. Hence S is commutative with C_1C_3. If S be commutative with B_3, it is of the form (67), of which $4(p^n+\nu)$ belong to O_Ω. Then S is commutative with $B_3C_1C_3$ and transforms $B_3C_1C_0$ into $B_3C_1C_0$ or $B_3C_3C_0$, since it transforms C_1C_0 and C_3C_0 amongst themselves. Next, C_1C_5 transforms T_8 into itself and B_3 into $B_3C_1C_3$, $B_3C_1C_0$ into $B_3C_3C_0$. Finally, B_3 and $B_3C_1C_0$ have different characteristic determinants.

THEOREM. *Within O_Ω, T_8 is self-conjugate only under $G_{8(p^n+\nu)}$.*

44. Every orthogonal substitution commutative with $B_3C_1C_5$ has the form

$$(70)\qquad \begin{vmatrix} \alpha_{11} & 0 & \alpha_{13} & 0 & 0 \\ 0 & \alpha_{22} & 0 & \alpha_{24} & \alpha_{25} \\ -\alpha_{13} & 0 & \alpha_{11} & 0 & 0 \\ 0 & \alpha_{24} & 0 & \alpha_{22} & -\alpha_{25} \\ 0 & \alpha_{52} & 0 & -\alpha_{52} & \alpha_{55} \end{vmatrix} \quad \left\{ \begin{array}{l} \alpha_{11}^2+\alpha_{13}^2=1,\ \alpha_{22}^2+\alpha_{24}^2+\alpha_{25}^2=1 \\ 2\alpha_{22}\alpha_{24}-\alpha_{25}^2=0 \\ 2\alpha_{52}^2+\alpha_{55}^2=2\alpha_{25}^2+\alpha_{55}^2=1 \\ \alpha_{22}\alpha_{52}-\alpha_{24}\alpha_{52}+\alpha_{25}\alpha_{55}=0 \end{array} \right\}.$$

The conditions on $\alpha_{22}, \alpha_{24}, \alpha_{25}, \alpha_{52}, \alpha_{55}$ and that for determinant $+1$ are seen to reduce to (69) if the sign of α_{24} is changed in the latter. Hence these conditions have $2(p^n+\nu)$ sets of solutions. Again, $\alpha_{11}^2+\alpha_{13}^2=1$ has $p^n-\nu$ sets of solutions. Hence exactly* $p^{2n}-1$ of the $2(p^{2n}-1)$ substitutions (70) of determinant $+1$ belong to O_Ω.

Observing that C_1C_5 transforms $B_3C_1C_5$ into its inverse, we may state the

THEOREM. *Within O_Ω, the group $(B_3C_1C_5)$ is self-conjugate only under a group $G_{2(p^{2n}-1)}$.*

---

* To make an explicit determination of them, we proceed as in *Linear Groups*, § 189. When -1 is the square of a mark i, (70) becomes

45. Since L_8 contains a single cyclic subgroup $(B_3C_1C_5)$ of order 4, a substitution which transforms L_8 into itself must be of the form (70) or its product by C_1C_5. Now (70) transforms the substitution C_1C_5 of L_8 into

$$(71)\qquad \begin{bmatrix} \alpha_{13}^2-\alpha_{11}^2 & 0 & 2\alpha_{11}\alpha_{13} & 0 & 0 \\ 0 & 1-2\alpha_{25}^2 & 0 & 2\alpha_{25}^2 & k \\ 2\alpha_{11}\alpha_{13} & 0 & \alpha_{11}^2-\alpha_{13}^2 & 0 & 0 \\ 0 & 2\alpha_{25}^2 & 0 & 1-2\alpha_{25}^2 & -k \\ 0 & k & 0 & -k & 1-2\alpha_{55}^2 \end{bmatrix} \qquad [k=\alpha_{52}(\alpha_{22}-\alpha_{24})-\alpha_{25}\alpha_{55}].$$

If (71) reduces to C_1C_5, then $\alpha_{13}=0$, $\alpha_{25}=0$, $\alpha_{55}=1$, so that (70) becomes I, C_1C_3, C_2C_4 or $C_1C_2C_3C_4$, in case it belongs to O_Ω. If (71) reduces to C_3C_5, then $\alpha_{11}=0$, $\alpha_{25}=0$, $\alpha_{55}=-1$, so that (70) becomes $B_3C_iC_5$ or $B_3C_iC_0$ $(i=1,3)$, in case it belongs to O_Ω. The remaining substitutions of period 2 of L_8, other than $C_1C_3=(B_3C_1C_5)^2$, are B_3 and $B_3C_1C_3$. But (71) cannot reduce to either of these when 2 is a not-square. Now

$$(72)\qquad I,\ C_1C_3,\ C_2C_4,\ C_1C_2C_3C_4,\ B_3C_iC_5,\ B_3C_iC_0 \qquad (i=1,3),$$

together with their products by C_1C_5, give the 16 substitutions of G_{16}'.

$$\begin{bmatrix} \frac{1}{2}(1+\alpha_{11}) & -\frac{1}{2}\alpha_{13} & 0 & 0 & -\frac{1}{2}\alpha_{13} & \frac{1}{2}(1-\alpha_{11}) \\ \frac{1}{2}\alpha_{13} & \frac{1}{2}(\alpha_{11}+\alpha_{22}) & P_+ & P_- & \frac{1}{2}(\alpha_{11}-\alpha_{22}) & -\frac{1}{2}\alpha_{13} \\ 0 & P_\pm & A & B & -P_\pm & 0 \\ 0 & P_\mp & C & D & -P_\mp & 0 \\ \frac{1}{2}\alpha_{13} & \frac{1}{2}(\alpha_{11}-\alpha_{22}) & -P_+ & -P_- & \frac{1}{2}(\alpha_{11}+\alpha_{22}) & -\frac{1}{2}\alpha_{13} \\ \frac{1}{2}(1-\alpha_{11}) & \frac{1}{2}\alpha_{13} & 0 & 0 & \frac{1}{2}\alpha_{13} & \frac{1}{2}(1+\alpha_{11}) \end{bmatrix} \qquad \begin{aligned} P_+ &= \tfrac{1}{2}(a_{22}\mp 1+ia_{25}), \\ P_- &= \tfrac{1}{2}(a_{22}\mp 1-ia_{25}), \\ A &= \tfrac{1}{2}(a_{22}\pm 2a_{22}\pm ia_{25}+ia_{25}-1), \\ B &= \tfrac{1}{2}(a_{22}\mp 2a_{22}\pm ia_{25}-ia_{25}+1), \\ C &= \tfrac{1}{2}(a_{22}\mp 2a_{22}\mp ia_{25}+ia_{25}+1), \\ D &= \tfrac{1}{2}(a_{22}\pm 2a_{22}\mp ia_{25}-ia_{25}-1). \end{aligned}$$

It is seen to be the second compound of

$$\Gamma=\begin{bmatrix} x & y & ry & -rx \\ z & w & rw & -rz \\ -rz & -rw & w & -z \\ rx & ry & -y & x \end{bmatrix} \qquad \left(r=\frac{-a_{13}}{1+a_{11}}=\frac{a_{11}-1}{a_{13}}\right),$$

if and only if the following conditions hold

$$xy=\frac{-P_\pm}{1+r^2},\quad xz=\frac{-P_+}{1+r^2},\quad xw=\frac{\alpha_{22}+1}{2(1+r^2)},\quad x^2=\frac{A}{1+r^2},\quad y^2=\frac{-B}{1+r^2},$$

$$zw=\frac{P_\mp}{1+r^2},\quad yw=\frac{P_-}{1+r^2},\quad yz=\frac{\alpha_{22}-1}{2(1+r^2)},\quad z^2=\frac{-C}{1+r^2},\quad w^2=\frac{D}{1+r^2}.$$

We have $1+r^2=2/(1+\alpha_{11})$. These conditions are seen to be compatible and to determine (except as to sign) marks x, y, z, w of the field if and only if any non vanishing one of the last four fractions is a square. For example, $BC=\frac{1}{4}(1-\alpha_{22})^2$, $AD=\frac{1}{4}(1+\alpha_{22})^2$, $AB=-P_\pm^2$.

If $\alpha_{13}=0$, $\alpha_{11}=+1$, we take $r=0$. If $\alpha_{13}=0$, $\alpha_{11}=-1$, the formulæ fail, but the substitution (70) is then the product of the preceding by C_1C_3, so that one belongs to O_Ω if the other does.

THEOREM. *Within O_Ω, the group L_8 is self-conjugate only under G'_{16}.*

46. The group H^3_{16} contains 8 substitutions of period 4: $B_3C_iC_5$ and $B_3C_iC_0$ $(i = 1, 3)$, all of which are conjugate under G_{64} (§ 6). A substitution which transforms $B_3C_1C_5$ into itself and C_1C_2 into a substitution of H^3_{16} belongs to the set (72). Indeed, the conditions on (70) are

$$\alpha_{25} = 0, \alpha_{11} = 0, \alpha_{22} = 0, \alpha_{55} = -1; \quad \text{or} \quad \alpha_{25} = 0, \alpha_{13} = 0, \alpha_{24} = 0, \alpha_{55} = 1.$$

THEOREM. *Within O_Ω, the group H^3_{16} is self-conjugate only under G_{64}.*

47. The only self-conjugate substitutions of period 4 of F_{16} are $B_2C_1C_3$ and its inverse $B_2C_2C_4$ (§ 13). These must be transformed among themselves by any substitution commutative with F_{16}. Every substitution S commutative with $B_2C_1C_3$ has the form

$$S = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{14} & 0 \\ -\alpha_{12} & \alpha_{11} & -\alpha_{14} & \alpha_{13} & 0 \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \alpha_{34} & 0 \\ -\alpha_{32} & \alpha_{31} & -\alpha_{34} & \alpha_{33} & 0 \\ 0 & 0 & 0 & 0 & \pm 1 \end{vmatrix}.$$

The further substitutions of period 4 of F_{16} are $B_2C_1C_4$ and $B_2C_2C_3$, $B_3C_1C_2$ and $B_3C_3C_4$, $B_4C_1C_3$ and $B_4C_2C_4$, the two of each pair being conjugate within G_{32}, under which F_{16} is self-conjugate (§ 10).

If S is commutative with $B_2C_1C_4$, then $\alpha_{13}, \alpha_{14}, \alpha_{31}, \alpha_{32}$ are zero, so that $S = O^{\alpha_{11}, \alpha_{12}}_{1,2} O^{\alpha_{33}, \alpha_{34}}_{3,4}$ if it is orthogonal and of determinant $+1$. If further S be commutative with $B_3C_1C_2$ and hence with F_{16}, then $\alpha_{33} = \alpha_{11}$, $\alpha_{34} = \alpha_{12}$. But if S transforms $B_3C_1C_2$ into $B_4C_1C_3$, then $\alpha_{33} = \alpha_{12}$, $\alpha_{34} = -\alpha_{11}$, so that $S = O^{\alpha_{11}, \alpha_{12}}_{1,2} O^{\alpha_{11}, \alpha_{12}}_{3,4} (\xi_3\xi_4) C_3$ and hence is not in O_Ω. Hence $O^{\alpha_{11}, \alpha_{12}}_{1,2} O^{\alpha_{11}, \alpha_{12}}_{3,4}$ and its product by C_1C_2 are the only substitutions S of O_Ω which are commutative with F_{16} and $B_2C_1C_4$. Their products by B_3 are the only ones transforming $B_2C_1C_4$ into $B_2C_2C_3$.

If an orthogonal substitution of the form S transforms $B_2C_1C_4$ into $B_3C_1C_2$, it has the form

$$S' = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{14} & 0 \\ -\alpha_{12} & \alpha_{11} & -\alpha_{14} & \alpha_{13} & 0 \\ -\alpha_{12} & \alpha_{11} & \alpha_{14} & -\alpha_{13} & 0 \\ -\alpha_{11} & -\alpha_{12} & \alpha_{13} & \alpha_{14} & 0 \\ 0 & 0 & 0 & 0 & \pm 1 \end{vmatrix} \qquad \left(\begin{matrix} \alpha_{11}^2 + \alpha_{12}^2 = \frac{1}{2} \\ \alpha_{13}^2 + \alpha_{14}^2 = \frac{1}{2} \end{matrix} \right).$$

Its determinant equals $\pm 4(\alpha_{11}^2 + \alpha_{12}^2)(\alpha_{13}^2 + \alpha_{14}^2)$. We therefore take $\pm 1 = +1$. Then S' transforms $B_3C_1C_2$ into

$$\begin{bmatrix} 0 & \rho & 0 & \sigma & 0 \\ -\rho & 0 & -\sigma & 0 & 0 \\ 0 & \sigma & 0 & -\rho & 0 \\ -\sigma & 0 & \rho & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \begin{pmatrix} \rho = 2\alpha_{11}\alpha_{14} - 2\alpha_{12}\alpha_{13} \\ \sigma = -2\alpha_{11}\alpha_{13} - 2\alpha_{12}\alpha_{14} \end{pmatrix}.$$

Then $\rho^2 + \sigma^2 = 1$. This belongs to F_{16} (and consequently S' transforms F_{16} into itself) only when $\rho\sigma = 0$. If $\sigma = 0$, it becomes $B_2 C_1 C_4$ or $B_2 C_2 C_3$. If $\rho = 0$, it becomes $B_4 C_1 C_3$ or $B_4 C_2 C_4$. Since 2 is a not-square, the conditions on S' show that $\alpha_{11}, \alpha_{12}, \alpha_{13}, \alpha_{14}$ all differ from 0. Hence $\rho = 0$ gives $\alpha_{13} = \pm \alpha_{11}$, $\alpha_{14} = \pm \alpha_{12}$, while $\sigma = 0$ gives $\alpha_{13} = \pm \alpha_{12}$, $\alpha_{14} = \mp \alpha_{11}$. From the remark at the end of the section it follows * indirectly that exactly half of the resulting substitutions belong to O_Ω.

If an orthogonal substitution of the form S transforms $B_2 C_1 C_4$ into $B_4 C_1 C_3$ then $S = S'(\xi_3 \xi_4) C_3$.

The total number of orthogonal substitutions S of determinant $+1$ which transforms F_{16} into itself is therefore $6 \cdot 4 \cdot (p^n - \nu)$. These, together with their products by $C_1 C_3$ (which transforms F_{16} into itself and $B_2 C_1 C_3$ into its inverse $B_2 C_2 C_4$), give all of determinant $+1$ which transforms F_{16} into itself. But $(\xi_1 \xi_2) C_1$ transforms F_{16} into itself. Hence exactly $6 \cdot 4 \cdot (p^n - \nu)$ belong to O_Ω.

THEOREM. *Within O_Ω, F_{16} is self-conjugate only under $G_{24(p^n-\nu)}$.*

Another proof follows from the results of § 26. The substitutions of O_Ω commutative with $B_2 C_1 C_3$ are found from those commutative with $B_3 C_1 C_4$ by transformation by $(\xi_2 \xi_3 \xi_4)$. From (55) we thus get

$$(73)\quad B_i,\ B_i C_1 C_2,\ B_i C_3 C_4,\ B_i C_1 C_2 C_3 C_4,\ B_j C_1 C_3,\ B_j C_1 C_4,\ B_j C_2 C_3,\ B_j C_2 C_4 \qquad (i = 1, 3;\ j = 2, 4).$$

Hence, for $p^n = 3$, these and their products by $W(\xi_2 \xi_4 \xi_3)$ and by its inverse give all the substitutions commutative with $B_2 C_1 C_3$. Inversely, they transform F_{16} into itself. For $p^n = 5$, the 12 types S' with a single vanishing α_{1j} are seen to be excluded as in § 27. Consider next Σ^*, the transform of S' by $(\xi_2 \xi_3 \xi_4)$, where S' is the substitution of § 11 subject to the conditions (56). We find that Σ^* transforms $C_1 C_2$ and B_3 into respectively

* To give a direct proof for $p^n = 3$, we note a substitution given by the lower signs is the product of $C_3 C_4$ and that given by the upper signs. For $\alpha_{13} = \alpha_{11} = +1$, $\alpha_{14} = \alpha_{12} = +1$, $S' = W^2(\xi_2 \xi_3 \xi_4)$; for $\alpha_{13} = \alpha_{11} = +1$, $\alpha_{14} = \alpha_{12} = -1$, $S' = W^2(\xi_2 \xi_3 \xi_4) C_2 C_4 B_2$; for $\alpha_{13} = \alpha_{12} = 1$, $\alpha_{14} = -\alpha_{11} = -1$, $S' = C_2 C_3 W(\xi_2 \xi_4 \xi_3)(\xi_3 \xi_4) C_2 C_3 C_4 \equiv S''$; for $\alpha_{13} = \alpha_{12} = 1$, $\alpha_{14} = -\alpha_{11} = 1$, $S' = C_2 C_3 S'' C_1 C_4$. All other cases follow at once from these.

$$\begin{bmatrix} 0 & 0 & \rho & \sigma & 0 \\ 0 & 0 & -\sigma & \rho & 0 \\ \rho & -\sigma & 0 & 0 & 0 \\ \sigma & \rho & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} \lambda & 0 & 0 & \mu & 0 \\ 0 & \lambda & -\mu & 0 & 0 \\ 0 & -\mu & -\lambda & 0 & 0 \\ \mu & 0 & 0 & -\lambda & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \left[\begin{array}{l} \rho = 2\alpha_{12}\alpha_{22} + 2\alpha_{11}\alpha_{13}\alpha_{14}\alpha_{22} \\ \sigma = 2\alpha_{11}\alpha_{13} + 2\alpha_{12}\alpha_{14} \\ \lambda = 2\alpha_{11}\alpha_{12} + 2\alpha_{13}\alpha_{14} \\ \mu = 2\alpha_{11}\alpha_{14} - 2\alpha_{12}\alpha_{13} \end{array} \right].$$

Since $\rho^2 + \sigma^2 \equiv 1$, either $\rho = 0$, whence the first substitution is either $B_4 C_1 C_4$ or $B_4 C_2 C_3$, or $\sigma = 0$, whence it is either B_3 or $B_3 C_1 C_2 C_3 C_4$. Since $\lambda^2 + \mu^2 \equiv 1$, either $\lambda = 0$ and the second substitution is either $B_4 C_1 C_4$ or $B_4 C_2 C_3$, or $\mu = 0$ and it is either $C_1 C_2$ or $C_3 C_4$. The resulting substitutions all belong to F_{16}. But $B_2 C_1 C_3$, $C_1 C_2$ and B_3 generate F_{16}. Hence each of the 32 substitutions Σ^* transforms F_{16} into itself. These together with the 16 substitutions (73) give all the 48 substitutions of O_Ω which transform F_{16} and $B_2 C_1 C_3$ each into itself. But B_2 transforms F_{16} into itself and $B_2 C_1 C_3$ into its inverse. *Hence* F_{16} *is self-conjugate only under the group* (G_{32}, Σ^*) *of order* 96.

THE UNIVERSITY OF CHICAGO,
July 25, 1903.