ORTHOGONAL GROUP IN A GALOIS FIELD.

BY DR. L. E. DICKSON.

(Read before the American Mathematical Society at the Meeting of December 29, 1897.)

1. A linear substitution S on the marks of a Galois Field of order p^n (in notation $GF[p^n]$)

$$\xi_i' = \sum_{j=1}^{m} a_{ij}\,\xi_j \qquad (i = 1, 2, \cdots m)$$

will be called *orthogonal* if it leaves absolutely invariant

$$\xi_1^{\,2} + \xi_2^{\,2} + \cdots + \xi_m^{\,2}.$$

The conditions on the coefficients of S are seen to be

$$a_{1j}^{\,2} + a_{2j}^{\,2} + \cdots + a_{mj}^{\,2} = 1 \qquad (j = 1, \cdots m),$$

$$a_{1j}\,a_{1k} + a_{2j}\,a_{2k} + \cdots + a_{mj}\,a_{mk} = 0 \quad (j, k = 1, \cdots m, j \neq k),$$

the latter not occurring* if $p = 2$. Replacing a_{ij} by a_{ji} we get the reciprocal of S, with a set of conditions equivalent to the above. Thus the determinant of S^{-1} equals the determinant A of S, so that $A^2 = 1$, being the determinant of $S^{-1}S$.

2. For the case $p = 2$, an orthogonal substitution S leaves invariant the square root of $\xi_1^{\,2} + \cdots + \xi_m^{\,2}$ in the $GF[2^n]$, viz.,

$$X \equiv \xi_1 + \xi_2 + \cdots + \xi_m.$$

Taking as independent indices $X, \xi_2, \cdots \xi_m$, S takes the form (with unaltered determinant $A = 1$):

$$X' = X, \quad \xi_i' = \sum_{j=2}^{m} \beta_{ij}\,\xi_j + a_{i1}\,X \qquad (i = 2, \cdots m),$$

where the a_{i1} are arbitrary and the $\beta_{ij} \equiv a_{ij} + a_{i1}$ satisfy the condition

$$A = |\,\beta_{ij}\,| = 1 \quad (i, j = 2, \cdots m).$$

The order of the orthogonal group G on m indices in the $GF\,[2^n]$ is thus

$$2^{n(m-1)} \left(\frac{(2^{n(m-1)} - 1)\,(2^{n(m-1)} - 2^n) \cdots (2^{n(m-1)} - 2^{n(m-2)})}{2^n - 1} \right),$$

* The remark of Jordan, Traité des Substitutions, p. 169, ll. 18–21, is thus not exact.