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 \( GF[p^n] \))

\[
\xi'_i = \sum_{j=1}^{m} a_{ij} \xi_j \quad (i = 1, 2, \ldots m)
\]

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

\[
a_{ij}^2 + a_{ij}^2 + \cdots + a_{mj}^2 = 1 \quad (j = 1, \ldots m),
\]

\[
a_{ij}a_{ik} + a_{ij}a_{ik} + \cdots + a_{mj}a_{mk} = 0 \quad (j, k = 1, \ldots m, j \neq k),
\]

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 \( X, \xi_2, \ldots \xi_m \), \( S \) takes the form (with unaltered determinant \( A = 1 \)):

\[
X' = X, \quad \xi'_i = \sum_{j=1}^{m} \beta_{ij} \xi_j + a_{ii} X \quad (i = 2, \ldots m),
\]

where the \( a_{ii} \) are arbitrary and the \( \beta_{ij} = a_{ij} + a_{ii} \) satisfy the condition

\[
A = |\beta_{ij}| = 1 \quad (i, j = 2, \ldots m).
\]

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

\[
2^{n(m-1)} \left( \frac{2^{n(m-1)} - 1}{2^n - 1} \right),
\]

* The remark of Jordan, Traité des Substitutions, p. 169, l. 18-21, is thus not exact.
the quantity in brackets being the order of the group * of substitutions of determinant 1 on \( m - 1 \) indices of the \( GF[2^n] \). \( G \) is obtained by extending \( \Gamma^* \) by the substitutions

\[ \xi'_i = \xi_i + \gamma_i X, \quad X' = X, \]

forming a commutative group self-conjugate under \( G \). Hence the decomposition of \( G \) reduces to that of \( \Gamma^* \) (reference just given). Henceforth I suppose \( p \equiv 2 \).

3. We may readily generalize Jordan, §§ 197–199, thus:

**Theorem:** The number of systems of solutions in the \( GF[p^n] \), \( p \equiv 2 \), of

\[ a_1 \xi_1^2 + a_2 \xi_2^2 + \cdots + a_{2m} \xi_{2m}^2 = x, \]

where every \( a_j \) is a mark \( \equiv 0 \) of the \( GF[p^n] \), is

\[ p^{n(2m-1)} - p^{n(m-1)} \nu \quad (x \equiv 0) \]

\[ p^{n(2m-1)} + (p^{nm} - p^{n(m-1)}) \nu \quad (x \equiv 0), \]

where \( \nu \) is +1 or \(-1\) according as \((-1)^m a_1 a_2 \cdots a_{2m} \) is a square or not square in the \( GF[p^n] \).

Similarly from §200 (where the minus sign is a misprint):

**Theorem:** The number of systems of solutions of

\[ a_1 \xi_1^2 + a_2 \xi_2^2 + \cdots + a_{2m+1} \xi_{2m+1}^2 = x \]

is \( p^{nm} + p^{nm} \nu' \), where \( \nu' \) is +1, \(-1\), or 0 according as \((-1)^n a_1 a_2 \cdots a_{2m+1} x \) is a square, not-square or zero in the \( GF[p^n] \).

4. In view of the succeeding paragraphs, it may be readily seen that the investigation of Jordan, §§ 201–212, affords the following generalization:

The orthogonal group on \( m \) indices in the \( GF[p^n] \), \( p \equiv 2 \) is generated † by the substitutions [only the indices changed being written]:

\[ \xi' = a \xi_i + \beta \xi_j, \quad \xi'_i = -\beta \xi_i + a \xi_j \quad (a^2 + \beta^2 = 1) \]

and

\[ \xi'_i = -\xi_i. \]

---

*Current number of the Annals of Mathematics, article on linear groups.
† Note the correction of Jordan, p. 169, l. 15, in either of the ways:
| \( x, y, z, u, v \) | \( y + z + u, x + z + u, z, u, v \) |
| \( x, y, z, u, v \) | \( y + z + u, x + u + v, x + y + u, y, x \). |
‡ The only exception is \( p^n = 5 \), when other generators are necessary if \( m > 2 \). Thus, for \( m = 3 \), we may choose the additional generator

\[ \xi'_1 = 2\xi_1 + \xi_2 + \xi_3, \quad \xi'_2 = \xi_1 + 2\xi_2 + \xi_3, \quad \xi'_3 = \xi_1 + \xi_2 + 2\xi_3. \]
ORTHOGONAL GROUP IN A GALOIS FIELD. [Feb.,

and its order is \( P_1 \cdot P_{m-1} \cdot P_m \), where \( P_i \) denotes the number of solutions in the \( \mathbb{GF}(p^n) \) of \( z_1^2 + z_2^2 + \cdots + z_t^2 = 1 \), given by § 3.

Hence if \( \varepsilon = +1 \) or \(-1\) according as \(-1\) is square or not-square, we have

\[
P_{4t} = p^{n(4t-1)} - p^{n(3t-1)}; \quad P_{4t+1} = p^{nt} + p^{2nt};
\]

\[
P_{4t+2} = p^{n(4t+1)} - \varepsilon p^{2nt}; \quad P_{4t+3} = p^{2n(2t+1)} + \varepsilon p^{n(2t+1)}.
\]

Thus

\[
P_{4t+2} \cdot P_{4t+3} = p^{n(4t+1)}(p^{n(4t+2)} - 1).
\]

Except when \( m = 4t + 2 \), the order of the orthogonal group on \( m \) indices is independent of the quadratic character of \(-1\).

If \( m = 2k + 1 \) the order is \( 2\omega \), where \( \omega \) is the order of the linear Abelian group on \( 2k \) indices (with the factors of composition 2 and \( \omega/2 \)), viz.:

\[
\omega = (p^{2k} - 1)(p^{n(2k-2)} - 1)p^{n(2k-3)} \cdots (p^n - 1)p^n.
\]

5. To generalize Jordan, §§ 208–9, we need the theorem:

In every \( \mathbb{GF}(p^n) \), except for \( p^n = 3^2 \), 5 or 13, a mark \( \nu \) may be found, such that \( \nu^4 - 1 \) shall be at wish a square or a not-square.

For \( n = 1 \) this theorem was proved by Gauss.* Thus, if \( p^n = 5 \) or 13 (exceptions omitted by Jordan), an integer \( \nu = 1 \) exists, making \( \nu^4 - 1 \) a square in the \( \mathbb{GF}(p^n) \) and hence also a square in the \( \mathbb{GF}(p) \); likewise an integer \( \nu^4 - 1 \) exists which is a not-square in the \( \mathbb{GF}(p^n) \), and hence in the \( \mathbb{GF}(p) \), \( n \) odd. For the case \( n \) even, and thus \( p^n = 8t + 1 \), we may readily generalize Gauss, I. c. 16–18, and obtain the formulæ:

\[
2k = i + l, \quad m = -k + (p^n - 1)/8, \quad p^n = [4(k - m) + 1]^2 + 4(i - l)^2,
\]

from which we are to prove† that (in Gauss’ notation) \( i \equiv 10 \) and \( l \equiv 30 \) are not both zero. But if \( i = l = 0 \), we readily find

\[
(\pm p^n - 1)^2 = 4 \quad \text{or} \quad p^n = 3^2.
\]

The proposition fails for the \( \mathbb{GF}(3^2) \), which we may define by the irreducible congruence \( j^2 \equiv -1 \) (mod 3). Thus \( j + 1 \) is a primitive root and Gauss’ four classes are

\[
1, \quad -1; \quad j + 1, \quad -j - 1; \quad -j, j; \quad -j + 1, j - 1;
\]

*Theoria residuorum biquadraticorum commentatio prima, 16–21.
† If \( p \) be of the form \( 4t + 1 \), so that \( p^n \) may be expressed as the sum of two squares each \( \equiv 0 \), the proof follows as in Gauss, Art. 18, since \( i \equiv 4t \).
the fourth powers are 1, \(-1\) and thus neither is followed (on adding \(+1\)) by a not-square. But for \(p^n = 3^2\), the theorem of Jordan, \(\S\ 208\), follows by \(\S\ 203\) since

\[ 1 - c'^2 = a'^2 + b'^2 = 1 + 1 = -1 = \text{square}. \]

It remains to prove the theorem for \(5'^\) and \(13'^\), \(n'\) odd and \(> 1\). Consider the general case \(p'^n = 8n + 5\). By Gauss, Art. 20 generalized, there exist \(2h\) squares and \(2m\) not-squares each followed by a fourth power. But \(h = 0\) gives \(m = n, i + l = 1, k = 2n\), whence

\[ p'^n = 8n + 5 = (-4n + 1)^2 + 4. \]

Hence \(n = 0\) or \(1\), so that \(p'^n = 5\) or \(13\). Again, \(m = 0\) gives \(h + k = 0, h = n\), so that \(p'^n = 5\). That \(p'^n = 5\) and \(13\) are really exceptions appears at once from the tables of Gauss, Art. 15.

For \(p = 13\) the result of Jordan \(\S\ 208\) may be obtained as follows. We have \(a' = \pm 1, b' = \pm 1, c'' = \pm 5\). Similarly, as in \(\S\ 204\), I take \(\beta b' - \gamma c'' = b''\). Then for \(\beta = \pm 2, \gamma = \pm 6\), the signs to agree with those of \(b'\) and \(c''\) respectively, we have \(b'' = 2 + 30, 1 - b'^2 = 4\), a case solved by \(\S\ 203\).

The proof needed in \(\S\ 209\) follows as a corollary if \(p^n = 3^2\) or \(5\). Thus if \(\nu^4 = 1\) and hence also \(1 - \nu^2\) be a not-square, either at once \(1 - \nu^2\) is a not-square and \(1 + \nu^2\) a square, or vice versa, when we replace \(\nu\) by \(\nu-1, -1\) being a square. But if \(p^n = 3^2\), we cannot proceed as in \(\S\ 209\). Since \(a' = \pm 1, b' = \pm d, 1 - d^2 = \text{not-square}\), we must have

\[ d^2 = \pm j, \quad c'' = \pm (j + 1) \]

Thus \(b' = \pm (j - 1), c'' = \pm (j + 1)\) or vice versa, leading to a similar treatment. As in \(\S\ 204\), I take

\[ b'' = \beta b' - \gamma c'' = \beta [\pm (j - 1)] - \gamma [\pm (j + 1)], \quad (\beta^2 + \gamma^2 = 1). \]

We may take \(\beta = \pm j, \gamma = \pm j\) such that the signs combine to give

\[ b'' = j(j - 1) - j(j + 1) = -2j, \]

whence \(1 - b'' = -1 = \text{square}\), a case solved by \(\S\ 203\).

6. For \(\S\S\ 207\) we need the theorem, proved as in Jordan, \(\S\ 198\) or as in Gauss, l. c. Art. 16:

In the GF\([p^n]\), for which \(1 = \text{square}\), \((p^n - 5)/4\) of the squares are followed by squares, \((p^n - 1)/4\) by not-squares, and one (viz., \(-1\)) by zero.
7. As in § 210, \( p^{2n} + 4p^n - 1 \), being relatively prime to \( p \), must divide \((p^{2n} - 1)(p^{2n} - 1)\) and thus also \( 4p^n(p^{2n} - 1) \) and hence \* \( 4(17p^n - 5) \) and hence divides

\[
20(p^{2n} + 4p^n - 1) - (68p^n - 20) = p^n(20p^n + 12)
\]

Hence \((p^n + 2)^2 - 5\) must divide 304, since

\[
3(68p^n - 20) + 5(20p^n + 12) = 304p^n.
\]

Thus

\[
p^n + 2 < 18 > \sqrt{309}.
\]

But \( p^n = 13, 11, 9, 5, 3 \) are readily excluded; while \( p^n = 7 \) yields 76 a divisor of 304 and indeed of \((7^3 - 1) (7^2 - 1)\), but is excluded since \(-1\) is a non-residue of 7.

8. With the hypothesis of Jordan § 211, that \( a^2 + b^2 + c^2 = 0 \), etc., we have \( a^2 = b^2 = \cdots \). Hence \( 3a^2 = 3b^2 = \cdots = 0 \) and \( ma^2 = 1 \). Thus either \( a^2 = b^2 = \cdots = 1 \) or \( 2a^2 = 2b^2 = \cdots = 1 \), when \( 1 - a^2 = a^2 = \text{square} \).

\[
\text{UNIVERSITY OF CALIFORNIA,}
\text{November 20, 1897.}
\]

WEBER’S ALGEBRA.


For some years the need of a thoroughly modern textbook on algebra has been seriously felt. The great strides that algebra has taken during the last twenty-five years, in almost all directions, have made Serret’s classical work more and more antiquated, while modern books like Petersen’s and Carnoy’s make no claims to give a large and comprehensive survey of the subject. The appearance of any book modelled on the same broad plan as Serret’s Algèbre Supérieure would thus be greeted with a hearty welcome, but when written by such a master as Heinrich Weber, we greet it with expressions of sincerest joy and satisfaction.

As Weber himself tells us, he has cherished for years the plan of this great undertaking; but before deciding to execute it he has traversed in his university lectures many times this vast domain as a whole, and has treated various parts separately with greater detail. No wonder, then, that

\* Jordan has \( 68p - 12 \), thus losing the divisor 76.