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.

the quantity in brackets being the order of the group* Γ of substitutions of determinant 1 on $m-1$ indices of the $GF[2^n]$. G is obtained by extending Γ by the substitutions

$$\xi_i' = \xi_i + \gamma_i X, \; X' = X,$$

forming a commutative group self-conjugate under G. Hence the decomposition of G reduces to that of Γ (reference just given). Henceforth I suppose† $p \neq 2$.

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

THEOREM: *The number of systems of solutions in the* $GF[p^n]$, $p \neq 2$, *of*

$$a_1\xi_1^2 + a_2\xi_2^2 + \cdots + a_{2m}\xi_{2m}^2 = \varkappa,$$

where every a_j *is a mark* $\neq 0$ *of the* $GF[p^n]$, *is*

$$p^{n(2m-1)} - p^{n(m-1)}\nu \qquad (\varkappa \neq 0)$$

$$p^{n(2m-1)} + (p^{nm} - p^{n(m-1)})\nu \qquad (\varkappa = 0),$$

where ν *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*

$$a_1\xi_1^2 + a_2\xi_2^2 + \cdots + a_{2m+1}\xi_{2m+1}^2 = \varkappa$$

is $p^{2nm} + p^{nm}\nu'$, *where* ν' *is* $+1, -1$, *or* 0 *according as* $(-1)^m a_1 a_2 \cdots a_{2m+1}\varkappa$ *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 $GF[p^n]$, $p \neq 2$ *is generated*‡ *by the substitutions* [*only the indices changed being written*]:

$$\xi_i' = \alpha\xi_i + \beta\xi_j, \quad \xi_j' = -\beta\xi_i + \alpha\xi_j \quad (\alpha^2+\beta^2=1)$$

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:

$$|x, y, z, u, v \quad y+z+u, x+z+u, z, u, v|$$

$$|x, y, z, u, v \quad y+z+u, x+u+v, x+y+u, y, x|.$$

‡ 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

$$\xi_1' = 2\xi_1 + \xi_2 + \xi_3, \quad \xi_2' = \xi_1 + 2\xi_2 + \xi_3, \quad \xi_3' = \xi_1 + \xi_2 + 2\xi_3.$$

and its order is $P_m \cdot P_{m-1} \cdots P_1$, *where* P_t *denotes the number of solutions in the* $GF[p^n]$ of $\xi_1^2 + \xi_2^2 + \cdots + \xi_t^2 = 1$, *given by* § 3.

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

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

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 2ω, where ω is the order of the linear Abelian group on $2k$ indices (with the factors of composition 2 and $\omega/2$), viz.:

$$\omega = (p^{2nk} - 1)\,p^{n(2k-1)}(p^{n(2k-2)} - 1)\,p^{n(2k-3)} \cdots (p^{2n} - 1)p^n.$$

5. To generalize Jordan, §§ 208–9, we need the theorem: *In every* $GF[p^n]$, *except for* $p^n = 3^2$, 5 or 13, *a mark* ν *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 $p \neq 5$ or 13 (exceptions omitted by Jordan), an integer $\nu \neq 0$ exists, making $\nu^4 - 1$ a square in the $GF[p^1]$ and hence also a square in the $GF[p^n]$; likewise an integer $\nu^4 - 1$ exists which is a not-square in the $GF[p^1]$ and hence in the $GF[p^n]$, n odd. For the case n even, and thus $p^n = 8t + 1$, we may readily generalize Gauss, l. c. 16–18, and obtain the formulæ:

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

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

$$(\pm p^{\frac{n}{2}} - 1)^2 = 4 \qquad \text{or } p^n = 3^2.$$

The proposition fails for the $GF[3^2]$, which we may define by the irreducible congruence $j^2 \equiv -1 \pmod 3$. Thus $j + 1$ is a primitive root and Gauss' four *classes* are

$$1,\ -1;\ j + 1,\ -j - 1;\ -j, j;\ -j + 1, j - 1;$$

---

* 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 $\neq 0$, the proof follows as in Gauss, Art. 18, since $l \neq i$.

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, § 208, follows by § 203 since

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

It remains to prove the theorem for $5^{n'}$ and $13^{n'}$, 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 § 208 may be obtained as follows. We have $a' = \pm 1$, $b' = \pm 1$, $c'' = \pm 5$. Similarly, as in § 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 § 203.

The proof needed in § 209 follows as a corollary if $p^n \neq 3^2$ or 5. Thus if $\nu^4 - 1$ and hence also $1 - \nu^4$ 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 ν by $\nu\sqrt{-1}$, -1 being a square. But if $p^n = 3^2$, we cannot proceed as in § 209. Since $a' = \pm 1$, $b' = \pm d$, $1 - d^2 =$ not-square, we must have

$$d^2 = \pm j, \quad c''^2 = \mp j$$

Thus $$b' = \pm (j - 1), \quad c'' = \pm (j + 1)$$

or *vice versa*, leading to a similar treatment. As in § 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 $1 - b''^2 = -1 =$ square, a case solved by § 203.

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

In the $GF[p^n]$, *for which* $-1 =$ *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 $(p^{3n} - 1)(p^{2n} - 1)$ and thus also $4p^n(p^{3n} - 1)$ 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 $1 - a^2 = a^2 =$ square.

UNIVERSITY OF CALIFORNIA,
November 20, 1897.

WEBER'S ALGEBRA.

Lehrbuch der Algebra. By HEINRICH WEBER, Professor of Mathematics in the University of Strassburg. Braunschweig, Friedrich Vieweg und Sohn. 1895–96. 8vo. Vol. I., pp. 653; Vol. II., pp. 796.

For some years the need of a thoroughly modern text-book 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.