MODULAR THEORY OF GROUP-MATRICES*

BY

LEONARD EUGENE DICKSON

1. The importance of the concept group-matrix in the theory of finite groups was recognized by DEDEKIND as early as 1880. The development of a general theory of group-matrices is due, however, to FROBENIUS, (Berliner Sitzungsberichte, from 1896 to the present). In particular, FROBENIUS has applied the theory to the representation of a finite group as a (non-modular) linear group. Since linear congruence groups are of importance in the theory of groups, particularly in questions of isomorphisms, and play a fundamental rôle in the applications of groups to the theory of functions and to geometry, the study of the representations of a finite group as a linear congruence group is of decided importance.

It is here proved that, if p^π is the highest power of the prime p dividing the order g of a group G, the group-matrix of G can be transformed, by a matrix whose elements are integers taken modulo p, into a compound matrix in which the submatrices to the right of the main diagonal have zero elements throughout, while the p^π submatrices in the diagonal are identical. Let D denote one of the diagonal submatrices, so that D is a square matrix of order g/p^π. Then the group-determinant Δ of G is congruent to $|D|^{p^\pi}$ modulo p. This result is in marked contrast to the non-modular theory, in which each algebraically irreducible factor of Δ enters to a power exactly equal to its degree.

It is shown in § 8 that the group-matrices of all groups of order p^π can be reduced to their canonical form modulo p by one and the same transformation.

An interesting theorem on group-characters is obtained in § 11.

Just as simplicity is attained in the algebraic theory only when certain algebraic irrationalities are introduced to permit of the complete factoring of the group-determinant into algebraically irreducible factors, so corresponding simplicity in the modular theory can be attained only by the use of Galois imaginaries (roots of irreducible congruences) in order to normalize completely the diagonal matrices D (§ 10). It is therefore proposed to take as the field of reference the field F_p defined as the aggregate of the Galois fields $GF[p^n]$,

* To be presented to the Society, September 5, 1907. Received for publication May 10, 1907.

$n = 1, 2, 3, \cdots$. Every equation with coefficients in F_p is completely solvable within F_p.

When the modulus p does not divide the order of G, the fundamental theorems of the algebraic theory are also true in the field F_p, as was first pointed out in the writer's paper in these Transactions, vol. 3 (1902), pp. 285–301. For the same case, the exposition of the algebraic theory by SCHUR (Berliner Sitzungsberichte, 1905, pp. 406–432) is valid in the field F_p.

When the modulus divides the order of G, the problem presents marked contrasts to the algebraic theory. It is to this outstanding case that the present paper is directed, as also the companion paper, "Modular theory of group-characters" (Bulletin of the American Mathematical Society, July, 1907).

2. Let G be a group of finite order g; let H be a subgroup,

$$H: \qquad s_1 = I, s_2, \cdots, s_h,$$

of order h and index $q = g/h$. Let $e_1 = I, e_2, \cdots, e_q$ be right-hand extenders of H to G, so that

$$G = H + He_2 + \cdots + He_q.$$

Form the left-hand multiplication-table of G with the operations

$$I, e_2, \cdots, e_q; \; s_2, s_2e_2, \cdots, s_2e_q; \; s_3, s_3e_2, \cdots, s_3e_q; \; \cdots$$

in the first row, and their inverses, in this order, in the first column. The body of the table is a compound matrix M with h^2 matrices $M_{i,j}$ as its elements. The matrix in the ith row of matrices and jth column of matrices is

$$(1) \qquad M_{i,j} = M_k, \qquad \text{if} \qquad s_i^{-1}s_j = s_k.$$

We have

$$(2) \qquad M_k = (e_r^{-1}s_ke_c) = \begin{pmatrix} s_k & s_ke_2 & \cdots & s_ke_q \\ e_2^{-1}s_k & e_2^{-1}s_ke_2 & \cdots & e_2^{-1}s_ke_q \\ \cdot & \cdot & \cdot & \cdot \\ e_q^{-1}s_k & e_q^{-1}s_ke_2 & \cdots & e_q^{-1}s_ke_q \end{pmatrix}.$$

If H is a subgroup of order h of a group G, the body of the multiplication-table of G may be exhibited as a compound matrix whose h^2 submatrices M_k have the same relative arrangement as the elements s_k in the multiplication-table $(s_i^{-1}s_j)$ of H.

To the h elements s_i of a group H we make correspond h independent variables x_{s_i}. Then the group-matrix of H is

$$(3) \qquad (x_{s_i^{-1}s_j}) \qquad (i, j = 1, \cdots, h).$$

3. Let p^π be the highest power of p dividing the order $p^\pi q$ of a group G, and let H be a Sylow subgroup of order p^π.

It will be shown in § 5 that there exists a matrix (b_{ij}) which transforms the group-matrix (3) of H into a matrix whose diagonal elements are congruent, modulo p, to $\sum x_{s_i}$, and whose elements to the right of the diagonal are congruent to zero. Then, if I denotes the unit matrix of order q, the compound matrix $(b_{ij}I)$ transforms the group-matrix of G, arranged as in § 2, into a compound matrix, each of the p^π submatrices in the main diagonal being congruent to

$$\left(\sum_{k=1}^{p^\pi} x_{e_r^{-1}s_k e_c}\right) \qquad (r, c = 1, \cdots, q), \tag{4}$$

while each submatrix to the right of the main diagonal has all its elements congruent to zero modulo p. Hence we may state the following

THEOREM. *If p^π is the highest power of p dividing the order of a group G, the group-determinant of G is congruent modulo p to D^{p^π}, where D is the determinant of the matrix* (4).

Consider the linear transformation T on ξ_i $(i = 0, 1, \cdots, p^\pi - 1)$ whose matrix is the group matrix of H_{p^π} with a convenient order for the elements x_{s_i} in the first row (§ 5). When T is expressed in terms of the new variables

$$\eta_i = \sum_{j=i}^{p^\pi-1} \binom{j}{i} \xi_j \qquad (i = 0, 1, \cdots, p^\pi - 1), \tag{5}$$

the coefficients being binomial coefficients, it takes the canonical form (modulo p) given above. The corresponding normalization of the transformation whose matrix is the group-matrix of G is accomplished by the introduction of the new variables

$$\eta_{iq+s} = \sum_{j=i}^{p^\pi-1} \binom{j}{i} \xi_{jq+s} \qquad (i = 0, 1, \cdots, p^\pi - 1;\ s = 1, \cdots, q). \tag{6}$$

4. Matrix (4) has the important property that, in the terminology of FROBENIUS, it is *a matrix belonging to the group G*. Removing the restriction that H is a Sylow subgroup, we obtain the matrix

$$X = \left(\sum_{k=1}^{h} x_{e_r^{-1}s_k e_c}\right) \qquad (r, c = 1, \cdots, q). \tag{7}$$

We prove that matrix X belongs to the group G, viz., that

$$XY = Z \quad \text{if} \quad \sum_R x_R y_{R^{-1}A} = z_A \qquad (R \text{ ranging over } G). \tag{8}$$

The element in the rth row and cth column of XY is

$$\sum_{j=1}^{q}\left(\sum_{m=1}^{h} x_{e_r^{-1}s_m e_j}\right)\left(\sum_{l=1}^{h} y_{e_j^{-1}s_l e_c}\right) = \sum_{k=1}^{h}\sum_R x_R y_{R^{-1}e_r^{-1}s_k e_c} = \sum_{k=1}^{h} z_{e_r^{-1}s_k e_c},$$

where $R = e_r^{-1}s_m e_j$, $s_k = s_m s_l$.

A second proof that matrix X belongs to the group G results incidentally from the following discussion which gives a (partial) normalization of the group-matrix of G by an algebraic transformation, in contrast to the (more complete) normalization in § 3 by a modular transformation. The transformation on $\xi_1, \cdots, \xi_{qh}$ whose matrix is the group-matrix of G (§ 2) is

$$\xi'_{(i-1)q+r} = \sum_{j,t} x_{e_r^{-1}s_i^{-1}s_je_t}\, \xi_{(j-1)q+t} \qquad (i, j = 1, \cdots, h;\ r, t = 1, \cdots, q). \tag{9}$$

Consider the functions analogous to (6) with $i = 0$:

$$\eta_s = \sum_{j=1}^{h} \xi_{(j-1)q+s} \qquad (s = 1, \cdots, q).$$

Then

$$\eta'_r = \sum_{j,t}\left(\sum_{i=1}^{h} x_{e_r^{-1}s_i^{-1}s_je_t}\right)\xi_{(j-1)q+t} = \sum_t\left(\sum_{k=1}^{h} x_{e_r^{-1}s_ke_t}\right)\xi_{(j-1)q+t} = \sum_{t=1}^{g}\left(\sum_{k=1}^{h} x_{e_r^{-1}s_ke_t}\right)\eta_t.$$

Hence the variables $\eta_1, \cdots, \eta_q$ undergo a transformation whose matrix is (7). In particular, $|X|$ is an algebraic factor of the group determinant of G.

5. THEOREM. *If G is a group of order p^π, p a prime, with the operations g_i, the group-matrix of G can be transformed* into one whose diagonal elements are congruent to $\sum x_{g_i}$ modulo p, while the elements to the right of the main diagonal are congruent to zero.*

The proof is by induction from $\pi - 1$ to π. It proved in § 7 for $\pi = 1$.

To apply § 2, let H be a subgroup of order $p^{\pi-1}$. Then $q = p$, and we may set $e_i = e^{i-1}$ $(i = 2, \cdots, p)$. By the hypothesis for the induction, the group matrix (x_{s_k}) of H can be transformed into a matrix whose diagonal elements are congruent to $\sum x_{s_k}$ modulo p, while those to the right of the main diagonal are congruent to zero. Let the transforming matrix be (a_{ij}), $i, j = 1, \cdots, p^{\pi-1}$. Then, if I is the unit matrix of order p, the compound matrix $(a_{ij}I)$ will transform the group-matrix (x_{g_i}) of G_{p^π} into a compound matrix, each of whose diagonal matrices D_i is (7) for $h = p^{\pi-1}$, while the elements of the matrices to the right of the diagonal are zero. Now $H_{p^{\pi-1}}$ is invariant in G_{p^π}. Hence $e^{-1}s_ke$ ranges over the operations of H where s_k does, so that

$$\sum_{k=1}^{p^{\pi-1}} x_{e_r^{-1}s_ke_c} = \sum x_{e^{-(r-1)}s_ke^{c-1}} = \sum x_{s_ke^{c-r}}.$$

We introduce the abbreviation

$$\sigma_t = \sum_{k=1}^{p^{\pi-1}} x_{s_kt}. \tag{10}$$

Since e^p belongs to H, we have

$$\sigma_{te^p} = \sigma_t. \tag{11}$$

* The transforming matrix is given in § 8.

Hence each diagonal matrix D_i is the cyclic matrix

$$(12)\qquad (\sigma_{e^{c-r}}) = \begin{pmatrix} \sigma_I & \sigma_e & \sigma_{e^2} & \cdots & \sigma_{e^{p-1}} \\ \sigma_{e^{p-1}} & \sigma_I & \sigma_e & \cdots & \sigma_{e^{p-2}} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \sigma_e & \sigma_{e^2} & \sigma_{e^3} & \cdots & \sigma_I \end{pmatrix}.$$

By § 7, this matrix of the cyclic group of order p can be transformed into a matrix whose diagonal elements are congruent to

$$\sum_{i=0}^{p-1} \sigma_{e^i} = \sum_{j=1}^{p^\pi} x_{g_j},$$

modulo p, while the elements to right of the diagonal are $\equiv 0$.

6. It remains to normalize the group-matrix of the cyclic group of order p by a transformation modulo p. Without increasing the difficulty of the problem, we treat the cyclic group of order p^π. We shall need two algebraic lemmas.

The transformation, with binomial coefficients,

$$(13)\qquad \eta_i = \sum_{j=i}^{g-1} \binom{j}{i} \xi_j \qquad (i = 0, 1, \cdots, g-1),$$

has, algebraically, the following inverse:

$$(14)\qquad \xi_i = \sum_{j=i}^{g-1} (-1)^{i+j} \binom{j}{i} \eta_j \qquad (i = 0, 1, \cdots, g-1).$$

This will be the case if, and only if,

$$(15)\qquad \sum_{j=i}^{l} (-1)^{l+j} \binom{l}{j} \binom{j}{i} = \delta_{il} \qquad (\delta_{ii} = 1,\ \delta_{il} = 0 \text{ if } i \neq l).$$

This well known formula (cf. NETTO, *Combinatorik*, p. 255, formula 43) is a special case of the following one, which is needed later:

$$(16)\qquad E_{mrs} \equiv \sum_{i=0}^{r} (-1)^i \binom{r}{i} \binom{i+m}{s} = \begin{cases} 0 & (r > s) \\ (-1)^r \binom{m}{s-r} & (r \leqq s). \end{cases}$$

To evaluate E, we apply

$$\binom{r}{i} = \binom{r-1}{i} + \binom{r-1}{i-1}$$

and obtain two sums P and Q. Making a similar replacement for $\binom{i+m}{s}$ in Q, we get

$$Q = -\sum_{i-1=0}^{r-1} (-1)^{i-1} \binom{r-1}{i-1} \binom{i-1+m}{s} - \sum_{i-1=0}^{r-1} (-1)^{i-1} \binom{r-1}{i-1} \binom{i-1+m}{s-1}$$
$$= -P - E_{m,\, r-1,\, s-1}.$$

Hence we have the recursion formula

$$E_{mrs} = -E_{m,\,r-1,\,s-1}.$$

Thus for $r \leqq s$, $E_{mrs} = (-1)^r E_{m0s-r}$ and (16) follows. For $r - s = \rho > 0$,

$$E_{mrs} = (-1)^s E_{m\rho 0} = (-1)^s \sum_{i=0}^{\rho} (-1)^i \binom{\rho}{i} = (-1)^s (1-1)^\rho = 0.$$

For the case $m \leqq s$, formula (16) may be obtained from formula (41), (NETTO, loc. cit., p. 255), by replacing m, n, q, s by r, s, $s-m$, $i-s+m$, respectively.

7. THEOREM. *The group-matrix of the cyclic group of order p^π can be transformed into a matrix, given by* (22), *having congruent elements, modulo p, in every parallel to the main diagonal, the elements to the right of the latter being congruent to zero.*

The group-matrix of the cyclic group of order g is

$$(17) \qquad A = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{g-2} & \alpha_{g-1} \\ \alpha_{g-1} & \alpha_0 & \alpha_1 & \cdots & \alpha_{g-3} & \alpha_{g-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{g-1} & \alpha_0 \end{pmatrix}.$$

Let $\alpha_{-k} = \alpha_{g-k}$. Then A is the matrix of the transformation

$$(18) \qquad \xi_i' = \sum_{j=0}^{g-1} \alpha_{j-i}\, \xi_j \qquad (i = 0, 1, \cdots, g-1).$$

Introducing the variables η by means of (13) and (14), we get

$$(19) \qquad \eta_s' = \sum_{r=0}^{g-1} \gamma_{sr}\eta_r, \qquad \gamma_{sr} = (-1)^r \sum_{i=0}^{r} \sum_{j=s}^{g-1} (-1)^i \binom{r}{i}\binom{j}{s} \alpha_{i-j}.$$

The value of γ_{sr} will be determined modulo p, for the case $g = p^\pi$.

For $0 \leqq m \leqq g-1$, the coefficient of α_{-m} in $(-1)^r\gamma_{sr}$ is $c + c'$, where c is the sum of the terms with $j = i + m$, c' the sum with $j = i + m - g$.

Let first $j = i + m$. The minimum value of i is the greater of 0 and $s - m$. But, for $m < s$ and $i < s - m$, $\binom{j}{s} = 0$. Hence in c we may allow i to begin with the value zero. The maximum value of i is the lesser of r and $g - 1 - m$. Hence if $m < g - r$, c is given by (16). Next, let $m \geqq g - r$, so that $i \leqq g - 1 - m$. Now c will be unaltered modulo p if we allow i to take the additional values $g - m + t$ $(t = 0, 1, \cdots, s-1)$, since

$$\binom{p^\pi + t}{s} \equiv 0 \pmod{p} \qquad (t < s < p^\pi).$$

Indeed, there is no term z^s in

$$(20) \qquad (1 + z^{p^\pi})(1+z)^t \equiv (1+z)^{p^\pi + t} \pmod{p}.$$

Thus, if $g-r \leqq m < g-r+s$, then $g-m+s-1 \geqq r$ and c is congruent to (16). Finally, for $m \geqq g-r+s$, $c+c'$ is congruent to (16) in view of (21).

Let next $j = i+m-g$. Then i ranges from $g-m+s$ to r, so that terms c' occur only for $m \geqq g-r+s$. For $s < p^\pi = g$, $t < g$,

$$\binom{t}{s} \equiv \binom{g+t}{s}, \qquad \binom{i+m-g}{s} \equiv \binom{i+m}{s} \pmod{p},$$

by (20). Hence $c' = 0$ if $m < g-r+s$; while for $m \geqq g-r+s$,

$$c' \equiv \sum_{i=g-m+s}^{r} (-1)^i \binom{r}{i}\binom{i+m}{s} \pmod{p}. \tag{21}$$

Therefore in every case the coefficient of α_{-m} in $(-1)^r\gamma_{sr}$ is congruent modulo p to the sum (16). Thus

$$\gamma_{rs} \equiv 0 \text{ (if } r > s), \qquad \gamma_{sr} \equiv \sum_{m=0}^{g-1} \binom{m}{s-r} \alpha_{-m} \text{ (if } r \leqq s).$$

Hence $\gamma_{sr} \equiv \gamma_{s-r0}$ $(r \leqq s)$. Set $a_t = \gamma_{t0}$. Then (19) becomes

$$\eta_s' = \sum_{t=0}^{s} a_t \eta_{s-t}, \qquad a_t \equiv \sum_{m=0}^{g-1} \binom{m}{t} \alpha_{-m} \pmod{p}. \tag{22}$$

8. THEOREM. *The group-matrices of all groups of order p^π, with a suitable order for the elements of the first row, can be transformed simultaneously into their canonical forms modulo p by the same transforming matrix.*

Employing the notations of § 5, we prove that the transformation T on the variables ξ_i, whose matrix is the group-matrix (y) of a given group G of order p^π, can be reduced to its canonical form modulo p by the introduction of the new variables (5), viz., that transformation (5) transforms T into its canonical form. Then the matrix of (14), i. e., the inverse of the matrix of (5), will transform the group-matrix (y) into its canonical form modulo p. The proof is by induction from $\pi-1$ to π. We therefore assume that the transformation whose matrix is the group-matrix (x) of the subgroup H of order $p^{\pi-1}$ can be reduced to its canonical form by the introduction of the new variables

$$\eta_i = \sum_{j=i}^{a} \binom{j}{i} \xi_j \qquad (i=0, 1, \cdots, a=p^{\pi-1}-1). \tag{23}$$

The matrix (a_{ij}) of § 5 is thus the inverse of the matrix of (23). Hence $(a_{ij}I)$ is the inverse of the matrix of

$$\eta_{ip+s} = \sum_{j=i}^{a} \binom{j}{i} \xi_{jp+s} \qquad (i=0, 1, \cdots, a;\ s=0, 1, \cdots, p-1). \tag{24}$$

It remains to normalize the diagonal matrices D_k $(k=0, 1, \cdots, a)$, each of

which is of the form (12). Hence by § 6 we introduce the new variables

$$\zeta_{kp+i} = \sum_{j=1}^{p-1} \binom{j}{i} \eta_{kp+j} \quad (k=0, 1, \cdots, a;\ i=0, 1, \cdots, p-1). \tag{25}$$

Eliminating the η's from (24) and (25), we get

$$\zeta_{lp+r} = \sum_{s=r}^{p-1} \sum_{m=l}^{a} \binom{s}{r} \binom{m}{l} \xi_{mp+s} \quad (l=0, 1, \cdots, a;\ r=0, 1, \cdots, p-1). \tag{26}$$

To prove that (26) is equivalent modulo p to transformation (5), set

$$i = lp + r, \qquad j = mp + s.$$

In view of the limits of the summation indices in (26), we have

$$0 \leqq r \leqq s \leqq p-1, \qquad 0 \leqq l \leqq m \leqq a \qquad (a = p^{\pi-1} - 1).$$

It therefore follows from the writer's Dissertation (Annals of Mathematics, ser. 1, vol. 11 (1896–7), pp. 75, 76), that

$$\binom{j}{i} \equiv \binom{s}{r} \binom{m}{l} \qquad (\bmod p). \tag{27}$$

The induction is therefore complete.

9. We have now established the lemmas employed in the proof of the general theorem of § 3. The problem of the ultimate canonical form modulo p of the group-matrix of a given group G of order $p^\pi q$ is therefore reduced to the problem of normalizing the diagonal matrices (4). One step of this normalization is readily effected in § 10, the resulting matrix (34) having the desirable property that the elements of the non-diagonal submatrices are all zero. In particular, this normalization is complete if a Sylow subgroup of order p^π is invariant in G.

10. Let H_{p^π} be invariant in $K_{p^\pi m}$, but in no larger subgroup of the given group $G_{p^\pi q}$. Set

$$K = H + He_2 + \cdots + He_m, \qquad G = K + Kf_2 + \cdots + Kf_n \quad (n = q/m). \tag{28}$$

Then (4) may be exhibited as a compound matrix (E_{ij}) whose n^2 elements E_{ij} are square matrices of order m:

$$E_{ij} = \left(\sum_{k=1}^{p^\pi} x_{f_i^{-1} e_r^{-1} s_k e_c f_j} \right) \qquad (r, c = 1, \cdots, m).$$

For r fixed, $e_r^{-1} s_k$ and $s_k e_r^{-1}$ range over the same set of elements. Set

$$\sigma_t^{ij} = \sum_{k=1}^{p^\pi} x_{f_i^{-1} s_k t f} \qquad (t = I, e_2, \cdots, e_m), \tag{29}$$

the m functions with i and j fixed being independent. Hence

$$E_{ij} = (\sigma^{ij}_{e_r^{-1}e_c}) \qquad (r, c = 1, \cdots, m). \tag{30}$$

Now $e_r^{-1}e_c$ may be given the form se_v with s in H. Then

$$\sigma^{ij}_{e_r^{-1}e_c} = \sigma^{ij}_{e_v}, \qquad (He_r)^{-1}(He_c) = He_v. \tag{31}$$

Hence, *for each i and j, E_{ij} is the group-matrix of the quotient-group K/H.* The order, m, of the latter is relatively prime to the modulus p. Hence by § 1 there exists a matrix μ, of order m and with elements in the field F_p, which transforms E_{11} into its ultimate canonical form C_{11}. Then the compound matrix

$$\begin{pmatrix} \mu & 0 & 0 & \cdots \\ 0 & \mu & 0 & \cdots \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} \tag{32}$$

transforms the compound matrix (E_{ij}) into $(\mu^{-1}E_{ij}\mu) = (C_{ij})$. Here the C_i have simultaneously their canonical forms:

$$C_{ij} = \begin{pmatrix} c_1^{ij} & 0 & 0 & \cdots \\ 0 & c_2^{ij} & 0 & \cdots \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix}, \tag{33}$$

where c_s^{ij} is a square matrix, whose determinant is irreducible in F_p, and whose elements are linear functions of $\sigma_1^{ij}, \cdots, \sigma_m^{ij}$, with coefficients independent of i, j. Applying to (C_{ij}) a certain transformation which merely permutes the variables, we get

$$\begin{pmatrix} C_1 & 0 & 0 & \cdots \\ 0 & C_2 & 0 & \cdots \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix}, \qquad C_s = (c_s^{ij}) \qquad (i, j = 1, \cdots, n). \tag{34}$$

The problem has therefore been reduced to the normalization of certain matrices C_s ("belonging" to the group G) of order n, the index of H_{p^π} in the largest subgroup (of the given group G) in which H_{p^π} is invariant.

If the Sylow subgroup H_{p^π} is invariant in G, then $n = 1$ and the normalization is complete.

11. From the theorem in § 5 we readily derive an interesting result on group-characters. Let H be a group with the h elements s_i and group-determinant Δ, defined as the determinant of matrix (3). Let G_{p^π} be any Sylow subgroup with the elements g_i and group-determinant D. If we set

$$x_s = 0 \text{ for every element } s \text{ of } H \text{ not in } G_{p^\pi}, \tag{35}$$

Δ becomes equal to an exact power of D. By § 5,

$$D \equiv L^{p^\pi} \pmod{p}, \qquad L = \sum_{i=0}^{p^\pi - 1} x_{g_i}.$$

In our field F_p, let Φ be an irreducible factor of degree f of Δ. Hence, under the assumption (35), Φ becomes a function congruent to L^f modulo p. The coefficient of

$$x_I^{f-1} x_{g_i} \qquad (g_i \neq I) \tag{36}$$

in L^f is f. By definition the coefficient of (36) in Φ is the character $\chi(g_i)$, while $\chi(I) = f$. We may therefore state the

THEOREM. *If χ is the group-character defined by a factor, of degree f and irreducible in the field F_p, of the group-determinant of a finite group H, then*

$$\chi(g) \equiv f \pmod{p} \tag{37}$$

for every element g of period a power of p in H.

The definition of characters is employed also for reducible factors. But

$$\Phi = \Phi'\Phi'' \text{ implies } \chi(g) = \chi'(g) + \chi''(g).$$

Hence (37) *is true also of algebraic group-characters.*

THE UNIVERSITY OF CHICAGO,
May 8, 1907.