MODULAR THEORY OF GROUP CHARACTERS.

BY PROFESSOR L. E. DICKSON.

1. THE problem of the representation of a given finite group as a linear homogeneous group with real or complex coefficients has been fully treated by Frobenius * by means of his theory of group characters. The present paper and the companion paper to appear simultaneously in the *Transactions* give a first attack on the corresponding problem for linear congruence groups, and in general for finite linear groups in any field F having a prime modulus p. To obtain simple results, it is in general necessary to introduce certain irrationalities, viz., roots of equations with coefficients in F. As our reference field we shall take the field F_p composed of the totality of integral rational functions with integral coefficients of all Galois imaginaries of all degrees, *i. e.*, the roots of congruences irreducible modulo p. In other words, F_p is the aggregate of the Galois fields $GF[p^n]$, $n = 1, 2, 3, \cdots$. Hence every equation with coefficients in F_p is completely solvable in F_p.

The paper also gives a report on the various expositions of the algebraic theory from the standpoint of their availability in the treatment of the modular theory (cf. §§ 3, 5, but particularly § 13).

2. *Definitions.* Given a finite group H with the h elements $H_0, H_1, \cdots, H_{h-1}$, we shall say that the h matrices of degree f (or linear substitutions)

$$A_{H_i} = (a_{\alpha\beta}^{H_i})_{\alpha,\beta=1,\cdots,f} \quad (i = 0, 1, \cdots, h-1), \tag{1}$$

whose elements a are marks of the field F_p, define a representation of the group H if the matrices satisfy the h^2 relations

$$A_R A_S = A_{RS} \quad (R, S = H_0, \cdots, H_{h-1}). \tag{2}$$

The matrices need not be distinct, so that the isomorphism may be multiple. Let $\mathrm{x}_{H_i} (i = 0, \cdots, h-1)$ be independent variables. Then

$$X = \sum_R A_R \mathrm{x}_R \quad (R = H_0, \cdots, H_{h-1}) \tag{3}$$

is called the group matrix corresponding to the representation.

* *Berliner Sitzungsberichte*, from 1896 to date.

If B is a matrix of degree f whose elements are marks of F_p and of determinant not zero, then $B^{-1}XB$ is also a group matrix, called equivalent to X. A group matrix X is called reducible or irreducible (in F_p), according as it is or is not equivalent to a matrix $\left(\begin{smallmatrix} Y & 0 \\ W & Z \end{smallmatrix}\right)$, where Y and Z are square matrices, W a rectangular matrix.

The system of h marks $\chi(H_0), \cdots, \chi(H_{h-1})$, defined by

$$\chi(R) = \sum_{a=1}^{f} a_{aa}^{R} \qquad (R = H_0, \cdots, H_{h-1}), \tag{4}$$

is called a character of the group H for the field F_p, corresponding to the particular representation (1) or group matrix (3). If the latter is irreducible, the character is called simple.

Analogous to the multiplication table of H, the matrix

$$(x_{PQ^{-1}}) \qquad (P, Q = H_0, \cdots, H_{h-1}), \tag{5}$$

in which P indicates the row and Q the column, is called the regular group matrix.

3. For the reasons to be pointed out in § 13, the only one of the various expositions of Frobenius's theory which may be utilized in the construction of a corresponding general modular theory is that by I. Schur, "Neue Begründung der Theorie der Gruppencharaktere," *Berliner Sitzungsberichte*, March 23, 1905. In Frobenius's theory, matrix (5) is completely reducible (with zero matrices to the right and left of the irreducible diagonal matrices), and each irreducible factor occurs to a power equal to its degree; in the modular theory these theorems do not hold true when p divides the order h of the group. In the latter case, only the earlier part of Schur's work can be utilized for the modular theory and then only after essential modifications.

The developments by Schur, pages 409–411, as well as the auxiliary theorems from the general theory of matrices, are valid for our field F_p. His theorem I is valid in any field; his theorem II, however, is valid only in a field F which, like F_p or the field of all real and complex numbers, has the property that every equation with coefficients in F is solvable in F. Instead of his fundamental theorem IV, we have the following (valid whether or not p divides f):

THEOREM. *If in the field F_p X and X' are non-equivalent irreducible group matrices of degrees f and f',*

(6) $X=(x_{\alpha\beta}), x_{\alpha\beta}=\sum_R a^R_{\alpha\beta}x_R(\alpha,\beta=1,\cdots,f;\ R=H_0,\cdots,H_{h-1}),$

(7) $X'=(x'_{\alpha\beta}),x'_{\alpha\beta}=\sum_R b^R_{\alpha\beta}x_R(\alpha,\beta=1,\cdots,f';\ R=H_0,\cdots,H_{h-1}),$

then the following relations hold:

(I) $$\sum_R a^{R^{-1}}_{\alpha\beta}a^R_{\gamma\delta}=ce_{\alpha\delta}e_{\beta\gamma} \qquad (\alpha,\beta,\gamma,\delta=1,\cdots,f),$$

(II) $$\sum_R a^{R^{-1}}_{\alpha\beta}b^R_{\gamma\delta}=0 \qquad (\alpha,\beta=1,\cdots,f;\ \gamma,\delta=1,\cdots,f'),$$

in which $e_{\alpha\delta}=0$ *if* $\alpha\neq\delta$, $e_{\alpha\alpha}=1$, *while* c *is a constant for a given group matrix* X, *equal to that for any equivalent group matrix, and*

(8) $$fc=h.$$

In view of Schur's proof we have (II) and

(I_1) $$\sum_R a^{R^{-1}}_{\alpha\beta}a^R_{\gamma\delta}=c_{\beta\gamma}e_{\alpha\delta},$$

in which the $c_{\beta\gamma}$ are constants to be determined. In view of (1), relations (2) are equivalent to

(9) $$\sum_{\beta=1}^{f}a^R_{\alpha\beta}a^S_{\beta\delta}=a^{RS}_{\alpha\delta} \quad (\alpha,\delta=1,\cdots,f;\ R,S=H,\cdots,H_{h-1}).$$

In (I_1), replace α by ρ, γ by σ; then multiply by $a^S_{\alpha\rho}a^T_{\gamma\sigma}$ and sum for $\rho,\sigma=1,\cdots,f$. We get

$$\sum_R\Big(\sum_\rho a^S_{\alpha\rho}a^{R^{-1}}_{\rho\beta}\Big)\Big(\sum_\sigma a^T_{\gamma\sigma}a^R_{\sigma\delta}\Big)=\sum_{\rho,\sigma}e_{\rho\delta}c_{\beta\sigma}a^S_{\alpha\rho}a^T_{\gamma\sigma}.$$

Applying (9) we get

(10) $$\sum_R a^{SR^{-1}}_{\alpha\beta}a^{TR}_{\gamma\delta}=a^S_{\alpha\delta}\sum_\sigma c_{\beta\sigma}a^T_{\gamma\sigma}.$$

For $T=E=$ identity, we get, since $a^E_{\gamma\sigma}=e_{\gamma\sigma}$ by Schur's proof,

(11) $$\sum_R a^{SR^{-1}}_{\alpha\beta}a^R_{\gamma\delta}=a^S_{\alpha\delta}c_{\beta\gamma}.$$

In (10) replace $c_{\beta\sigma}$ by its value from (I_1) for $\alpha=\delta$, $\gamma=\sigma$. The right member of (10) becomes

$$a^S_{\alpha\delta}\sum_\sigma a^T_{\gamma\sigma}\Big(\sum_R a^{R^{-1}}_{\alpha\beta}a^R_{\sigma\alpha}\Big)=a^S_{\alpha\delta}\sum_R a^{R^{-1}}_{\alpha\beta}a^{TR}_{\gamma\alpha},$$

in view of (9). In (11) replace R by R^{-1}, S by T, γ by α, δ by β, α by γ, β by α. We get

$$\sum_R a^{R^{-1}}_{\alpha\beta} a^{TR}_{\gamma\alpha} = a^T_{\gamma\beta} c_{\alpha\alpha}.$$

We have now shown that (10) becomes

$$\text{(III)} \qquad \sum_R a^{SR^{-1}}_{\alpha\beta} a^{TR}_{\gamma\delta} = a^S_{\alpha\delta} a^T_{\gamma\beta} c_{\alpha\alpha}.$$

In (III) set $T = E$ and compare the result with (11). We get

$$\text{(12)} \qquad a^S_{\alpha\delta} e_{\gamma\beta} c_{\alpha\alpha} = a^S_{\alpha\delta} c_{\beta\gamma} \quad (\alpha, \beta, \gamma, \delta = 1, \cdots, f).$$

If for α fixed, the $a^S_{\alpha\delta}$ were all zero, then by (6) every $x_{\alpha\beta} = 0$, *i. e.*, all the elements of the αth row of X would vanish. But $|X|$ is not identically zero. Hence, by (12),

$$c_{\beta\gamma} = e_{\beta\gamma} c_{\alpha\alpha} \qquad (\alpha, \beta, \gamma = 1, \cdots, f).$$

In particular, the $c_{\alpha\alpha}$ are all equal. Call their common value c. Then

$$\text{(13)} \qquad c_{\beta\gamma} = c e_{\beta\gamma}.$$

Hence (I_1) becomes (I). In (II) replace α by ρ, γ by σ; then multiply by $a^S_{\alpha\rho} b^T_{\gamma\sigma}$ and sum for ρ, σ. We get

$$\text{(IV)} \qquad \sum_R a^{SR^{-1}}_{\alpha\beta} b'^{TR}_{\gamma\delta} = 0.$$

Now (I), for $\delta = \alpha$, $\gamma = \beta$, becomes

$$\text{(14)} \qquad c = \sum_R a^{R^{-1}}_{\alpha\beta} a^R_{\beta\alpha}.$$

Summing for β, applying (9) and $a^E_{\alpha\alpha} = 1$, we obtain (8).

Finally, we prove that $c = d$, d being the constant for

$$P^{-1}XP = \sum_R (d^R_{\alpha\beta}) \mathrm{x}_R.$$

Let $P = (p_{\alpha\beta})$, $P^{-1} = (q_{\alpha\beta})$, so that

$$S_\delta \equiv \sum_\sigma q_{\delta\sigma} p_{\sigma\delta} = 1.$$

Then

$$d^R_{\gamma\delta} = \sum_{\rho,\sigma} q_{\gamma\rho} a^R_{\rho\sigma} p_{\sigma\delta},$$

$$d \equiv \sum_R d^{R^{-1}}_{\gamma\delta} d^R_{\delta\gamma} = \sum_{\rho,\sigma,r,s} q_{\gamma\rho} p_{\sigma\delta} q_{\delta r} p_{s\gamma} \Big(\sum_R a^{R^{-1}}_{\rho\sigma} a^R_{rs} \Big).$$

The final term equals $ce_{\rho\delta}e_{\sigma r}$ by (I). Hence

$$d = c\Big(\sum_{\rho} q_{\gamma\rho}p_{\rho\gamma}\Big)\Big(\sum_{\sigma} q_{\delta\sigma}p_{\sigma\delta}\Big) = cS_\gamma S_\delta = c.$$

4. Certains relations between the simple characters (4) follow readily from (I)–(IV) and (9). In (III) take $\beta = \alpha$, $\delta = \gamma$, and sum for α, γ. Hence

$$\text{(V)} \qquad \sum_R \chi(SR^{-1})\chi(TR) = c\chi(ST).$$

For $T =$ identity, (V) becomes

$$\text{(VI)} \qquad \sum_R \chi(SR^{-1})\chi(R) = c\chi(S).$$

Conversely, replacing S by ST and R by RT in (VI), we get (V). In fact, by (4) and (9), we find that

$$\text{(VII)} \qquad \chi(RT) = \chi(TR), \quad \chi(E) = f \quad (E = \text{identity}).$$

For $S =$ identity, (VI) becomes, by (8),

$$\text{(VIII)} \qquad \sum_R \chi(R^{-1})\chi(R) = h.$$

In (III) take $\gamma = \beta$, $\delta = \alpha$, sum for α, β and apply (9). Hence

$$\text{(IX)} \qquad c\chi(S)\chi(T) = \sum_R \chi(SR^{-1}TR).$$

Let χ' be the character corresponding to the irreducible group matrix X' not equivalent to X. In (IV) set $\beta = \alpha$, $\delta = \gamma$, and sum for α, γ. Hence

$$\text{(X)} \qquad \sum_R \chi(SR^{-1})\chi'(TR) = 0.$$

If the modulus p does not divide h, relations (VI) and (X) follow* from (VII), (VIII), (IX) (the latter three with $c = h/f$ serve in the algebraic theory to determine completely the characters).

Further, when p is prime to h, the entire exposition by Schur is valid in the field F_p. In particular the algebraically irreducible factors of the regular group determinant have integral

* Cf. Weber, Algebra, 2d ed., II, p. 194.

algebraic numbers as coefficients and hence are functions interpretable in F_p and are irreducible in F_p. The fact that the modular theory for p prime to h is identical with the algebraic theory was first stated in the writer's paper, *Transactions*, volume 3 (1902), page 285.

5. For a given group H of order h, let $X, X', \cdots$ be group matrices of degrees $f, f', \cdots$, irreducible in the field F_p, and no two equivalent. Give them the notation (6), (7), etc. Then the $f^2+f'^2+\cdots$ linear functions $x_{\alpha\beta}, x'_{\alpha\beta}, \cdots$ are linearly independent in F_p.

In case p does not divide h, the proof follows at once from relations (I) and (II) (cf. Schur, page 412). In the contrary case the proof fails, since c vanishes for certain group matrices. We may, however, make use of theorem I in the paper by Frobenius and Schur on the equivalence of linear groups, *Berliner Sitzungsberichte*, 1906, page 209, the proof being valid in our field F_p.

It follows that the determinant of an irreducible group matrix X is an irreducible function of the variables x_R; and that two irreducible group matrices are equivalent if and only if their determinants are identically equal.

Let Φ denote the determinant $|X|$ of the irreducible group matrix (3) of degree f. If E is the identity element of the group, and $R \neq E$, the coefficient of $x_E^{f-1}x_R$ in Φ is $\chi(R)$, in view of (4) and $a^E_{\alpha\beta} = e_{\alpha\beta}$. Also $\chi(E) = f$ by (VII). Hence for every element R, $\chi(R)$ is the coefficient of x_E^{f-1} in $\partial\Phi/\partial x_R$. This property is taken as the definition of $\chi(R)$ in Frobenius's second exposition, *Sitzungsberichte*, 1896, page 1349. The latter paper gives a method of determining all the coefficients of Φ in terms of the characters $\chi(R)$. The method must be modified in the case of a modular field. If u is a new independent variable, set

$$(15) \quad \Phi(x_E + u, x_A, x_B, \cdots) = u^f + \Phi_1 u^{f-1} + \cdots + \Phi_f,$$

where Φ_n is an integral homogeneous function of the nth degree of $x_E, x_A, \cdots$, and $\Phi_f = \Phi$. Let S_n denote the sum of the nth powers of the negatives of the quantities $u_1, \cdots, u_f$ for which (15) vanishes. By Frobenius's proof,

$$S_1 = \Phi_1 = \sum_R \chi(R)x_R, \quad S_n = \sum_{R_1, \cdots, R_n} \chi(R_1 \cdots R_n)x_{R_1} \cdots x_{R_n},$$

where $R_1, \cdots, R_n$ range independently over the h elements of

H. By Waring's formula each Φ_i is expressed as a polynomial in the S_n. For a modular field, this formula is not always applicable in view of the denominators. We shall illustrate for small values of f a valid method of determining in F_p the function

$$\Phi = \sum C_{R_{i_1},\cdots,R_{i_f}} x_{R_{i_1}} \cdots x_{R_{i_f}} \qquad (i_1 \leqq i_2 \leqq \cdots \leqq i_f). \tag{16}$$

For $f = 2$, Φ is determined by

$$2\Phi_2 = S_1^2 - S_2, \tag{17}$$

unless $p = 2$. By comparing the coefficients of $x_E y_L x_R y_S$ $(R \neq E,\ S \neq E)$ in

$$\Phi(z) = \Phi(x)\Phi(y), \quad z_T = \sum_R x_R y_{R^{-1}T}, \tag{18}$$

we obtain,* according as $R \neq S$ or $R = S$,

$$C_{RS} = \chi(R)\chi(S) - \chi(RS), \quad 2C_{RR} = \chi(R)\chi(R) - \chi(R^2). \tag{19}$$

For modulus $p = 2$, it remains to determine C_{RR}. Now

$$-S_3 + \Phi_1 S_2 - \Phi_2 S_1 = 0,$$

by Newton's identities. The coefficients of

$$x_R^3,\ x_R^2 x_S \quad (R \neq S \neq E),$$

give

$$C_{RR}\chi(R) = \chi(R)\chi(R^2) - \chi(R^3),$$

$$C_{RR}\chi(S) = -C_{RS}\chi(R) - 3\chi(R^2S) + \chi(R^2)\chi(S) + 2\chi(RS)\chi(R).$$

But C_{RS} is given by (19_1). Hence C_{RR} is determined by the characters unless the latter all vanish. But in that case Φ involves only the squares of the variables x_R and hence is reducible in F_2, contrary to hypothesis.

For $f = 3$, Φ is determined by

$$6\Phi_3 = S_1^3 - 3S_1S_2 + 2S_3 \tag{20}$$

unless $p = 2$ or 3. For $p = 3$, we treat (20) as an algebraic identity and find that the terms in $x_R^2 x_S$ and $x_R x_S x_T$ are multiples of 3; we thus obtain C_{RRS} and C_{RST} algebraically in terms of the characters. In

*Or directly, by treating (17) as an algebraic identity, one half the coefficients of $x_R x_S (R \neq S)$ are given by (19_1).

$$(21) \qquad S_4 - \Phi_1 S_3 + \Phi_2 S_2 - \Phi_3 S_1 = 0,$$

we select the terms x_R^4 and $x_R^3 x_S$, using (17), and obtain $C_{RRR}\chi(R)$ and $C_{RRR}\chi(S)$ as functions of the characters. But if every character vanishes, Φ involves only the cubes of the variables and is reducible modulo 3.

For $f = 3$, $p = 2$, Newton's identities give

$$(22) \quad S_3 + S_1^3 = \Phi_3 + \Phi_2 S_1, \quad \Phi_2(S_3 + S_1^3) = S_5 + S_1^2 S_3.$$

In Φ_2, C_{RS} is given by (19_1); to find C_{RR} we examine the coefficients of $x_R^i x_S^{5-i}$ $(i = 5, \cdots, 2)$ in (22_2). If in each the factor of C_{RR} vanishes then $S_3 + S_1^3 = 0$, identically. But Φ_3 would then be reducible by (22_1). Hence Φ_2 and then Φ_3 can be expressed in terms of the characters.

6. THEOREM. *In the field F_p any commutative group H of order $h = p^\pi q$ (q not divisible by the prime p) has exactly q distinct characters.*

If A is an element of period p^t of H, and we set $\chi(A) = W$, then in the field F_p we have

$$W^{p^t} = 1, \quad (W-1)^{p^t} = 1, \quad W = 1.$$

Proceeding as in Weber's Algebra, II, Chapter 2, we conclude that H has at most $h/p^\pi = q$ different characters. But at least this number occur, since there exist in F_p primitive roots of $x^k = 1$ for k prime to p. In fact, $x^k = 1$ has no double root aud hence k distinct roots in F_p.

7. THEOREM. *If C denotes the commutator group of H, the number of distinct linear factors in F_p of the group determinant of H is obtained by dividing the order of the quotient group $Q = H/C$ by the highest power of p dividing the order of Q.*

The proof follows from §6 and the argument in Frobenius's paper, *Sitzungsberichte*, 1896, pages 1347–1349. As there shown the linear factors occur to the same power. But the argument showing that this power is the first is not valid in F_p (cf. §8).

8. THEOREM. *If p^π is the highest power of p which divides the order of a group H, every irreducible factor, in the field F_p, of the regular group determinant of H enters to a power which is an exact multiple of p^π. For any character of degree f, $\chi(P) = f$ if P is an element of period a power of p.*

The proof is given in the July number of the *Transactions*.

9. The characters in the field F_p of a group H whose order

h is prime to p may be taken to be the algebraic characters given by Frobenius's theory. We shall consider examples in which h is divisible by p. If H is abelian or if h is a power of p, the characters follow from §§ 6, 8.

The relations obtained in § 4 do not in general completely determine the simple characters in F_p. Relation (IX) is equivalent to that obtained by replacing S and T by any elements conjugate to them or by interchanging S and T. Similarly for (VI) and (X); in the latter it suffices to set $T =$ identity. Not all the values of a simple character are zero (§ 5). If $\Phi = \Phi'\Phi''$ then $\chi(R) = \chi'(R) + \chi''(R)$ for every R.

10. Let H be the symmetric group on three letters. Let E, A, B be elements of period 1, 3, 2, and set $\chi(E) = f$, $\chi(A) = a$, $\chi(B) = b$. Then, by § 4,

$$f^2 + 2a^2 + 3b^2 = 6, \quad a^2 + 2af + 3b^2 = ca, \quad 4ab + 2fb = cb,$$

$$ca^2 = 3a + 3f, \quad cab = 6b, \quad cb^2 = 2f + 4a.$$

For modulus 2, the solutions (other than $f = a = b = 0$) are

$$(23) \quad f_1 = a_1 = b_1 = 1, \quad c_1 = 0; \quad f_2 = b_2 = 0, \quad a_2 = c_2 = 1.$$

Hence by § 8, $|H| = \Phi_1^2\Phi_2^2$. Here Φ_2 is irreducible (end of § 9).

For modulus 3, the conditions reduce to $f = a$, $c = 0$. But by §§ 7, 8, $|H| = \Phi_1^3\Phi_1'^3$.

11. Let H be the alternating group on four letters. Let f, x, y, z be the values of a character when the arguments are non-conjugate elements of period 1, 2, 3, 3. Then, by § 4,

$$(24) \quad f^2 + 3x^2 + 8yz = 12, \quad 2fx + 2x^2 + 8yz = cx,$$

$$(25) \quad 2fy + 6xy + 4z^2 = cy, \quad 2fz + 6xz + 4y^2 = cz,$$

$$(26) \quad 4f + 8x = cx^2, \quad 12y = cxy, \quad 12z = cxz,$$

$$(27) \quad 3f + 9x = cyz, \quad 12z = cy^2, \quad 12y = cz^2.$$

Let first the modulus p be 3. The solutions are

$$(28) \quad f = y = z = 0, \ x = \pm 1, \ c = \mp 1; \quad f = x = y = z \neq 0, \ c = 0.$$

By § 5 or § 8, $f = 1$ for the second, $f = 3$ for the first. Further, the lower signs must be taken. Thus $|H| = \Phi_1^3\Phi_3^3$.

For $p = 2$, the relations reduce to $c = 0$, $x = f$. By §§ 7, χ, we have $|H| = \Phi_1^4\Phi_1'^4\Phi_1''^4$. It follows from (17) that $8^2(R) \equiv \chi(R^2)$, whence $x = f$, $y^2 = z$, $z^2 = y$.

12. Finally, let H be the alternating group on five letters. There are five sets of conjugate elements, of periods 1, 3, 2, 5, 5. Denote the corresponding values of $\chi(R)$ by f, A, B, C, D. By § 4,

$$f^2 + 20A^2 + 15B^2 + 12C^2 + 12D^2 = 60, \tag{29}$$

$$2fA + 7A^2 + 12AB + 6AC + 6AD + 3B^2 + 6BC + 6BD + 3C^2 + 6CD + 3D^2 = cA, \tag{30}$$

$$2fC + 5A^2 + 10AB + 10AC + 10AD + 5B^2 + 10BD + 5C^2 + 2CD + D^2 = cC, \tag{31}$$

$$2(fB + 4A^2 + 4AB + 4AC + 4AD + 4BC + 4BD + B^2 + 4CD) = cB, \tag{32}$$

$$3(f + 7A + 6B + 3C + 3D) = cA^2, \tag{33}$$

$$15(A + B + C + D) = cAC, \tag{34}$$

$$3(8A + 4B + 4C + 4D) = cAB, \tag{35}$$

$$20(A + B + D) = cBC, \quad 5(f + 5A + 5C + D) = cC^2, \tag{36}$$

$$4(f + 4A + 2B + 4C + 4D) = cB^2, \quad 5(5A + 5B + C + D) = cCD, \tag{37}$$

together with the relations derived from (31), (34) and (36) by interchanging C with D. Now Φ_f must equal, or be an irreducible factor in F_p, of one of the algebraically irreducible factors of the group determinant

$$|H| = \Phi_1\Phi_3^3\Phi_3'^3\Phi_4^4\Phi_5^5.$$

Let $p = 5$. If $c \neq 0$, we obtain

$$f = C = D = 0, \quad A = \pm 1, \quad B = \mp 1, \quad c = \pm 3. \tag{38}$$

For $c = 0$, the conditions (29)–(37) reduce to

$$f = C = D, \quad B = 3f + 3A, \quad c = 0. \tag{39}$$

In (38) $f = 5$, since $f < 10$ by § 5. The only algebraically irreducible factor of degree $\geqq 5$ has $f = 5$, $C = D = 0$, $A = -1$, $B = 1$. Hence the lower signs must hold in (38). If the resulting function Φ_5 were reducible, $\Phi_5 = \Pi\Phi_i$, the characters

of the irreducible factors would satisfy (39) and $\sum A_i = A$, etc. As this is seen to be impossible, Φ_5 is irreducible in F_5. The remaining irreducible factors of $|H|$ satisfy (39) and have $f \leqq 4$. But the algebraically irreducible factor Φ_4 occurs only to the fourth power; hence by § 8 it is reducible in F_5. Now $\chi_4(R) \equiv \chi_1(R) + \chi_3(R)$. Hence $\Phi_4 = \Phi_1\Phi_3$ in F_5. Finally, there is no factor Φ_2, since H cannot be represented as a binary linear group in F_5, the only binary transformation of period 2 being $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Hence the algebraic factor Φ_3 remains irreducible in F_5. Hence

$$|H| = \Phi_1^5\Phi_3^{10}\Phi_5^5 \text{ in } F_5. \tag{40}$$

Let next $p = 3$. If $c \neq 0$, we obtain

$$f = A = 0,\ c = B = \pm 1,\ C \text{ and } D \text{ roots of } y^2 \pm y - 1 = 0. \tag{41}$$

If $c = 0$, the conditions (29)–(37) reduce to

$$f = A,\ D = C,\ A + B + C = 0,\ c = 0. \tag{42}$$

Proceeding as for $p = 5$, we find that the lower signs must hold in (41) and that the resulting functions Φ_3 and Φ_3' are irreducible in F_3; also that $\Phi_5 = \Phi_1\Phi_4$. Thus

$$|H| = \Phi_1^6\Phi_3^3\Phi_3'^3\Phi_4^9 \text{ in } F_3. \tag{43}$$

Finally, let $p = 2$. If $c \neq 0$, we obtain

$$f = B = 0,\ A = C = D = 1,\ c = 1. \tag{44}$$

If $c = 0$, conditions (29)–(37) reduce to

$$f = B,\quad A + B + C + D = 0. \tag{45}$$

By the argument employed when $p = 5$, we find that the algebraically irreducible function Φ_4, whose characters are congruent to those in (44), remains irreducible in F_2. Since H is simply isomorphic with the group of all binary transformations of determinant unity in the $GF[2^2]$, there exist factors Φ_2 irreducible in F_2. Their characters are

$$f = B = 2,\quad A = 1,\quad C \text{ and } D \text{ roots of } y^2 + y + 1 = 0. \tag{46}$$

We find that in F_2,

$$\Phi_5 = \Phi_1\Phi_2\Phi_2',\quad \Phi_3 = \Phi_1\Phi_2,\quad \Phi_3' = \Phi_1\Phi_2'.$$

Hence

$$|H| = \Phi_1^{12}\Phi_2^8\Phi_2'^8\Phi_4^4 \text{ in } F_2. \tag{47}$$

13. Frobenius's first method of introducing group characters (*Sitzungsberichte*, 1896, page 985) relates primarily to the factorization, into linear factors, of the special group determinant $|x_{PQ^{-1}}|$, in which $x_A = x_B$ if A and B are conjugate elements of the group H. This method is not suitable for the foundation of the modular theory; in fact, two distinct irreducible factors of the general group determinant G may correspond in the field F_p to the same linear factor of the special group determinant S. Thus if H is the symmetric group on three letters, and $p = 3$, $S = (x_E - x_A)^6$, while G has two distinct factors (§ 7 or § 10). It may be argued indirectly (cf. end of § 4) that the prime factors of Frobenius's fundamental determinant $|p_{\alpha\beta}|$ are all divisors of the order of H.

Frobenius's second method (l. c., page 1343) relates initially to the general group determinant G. With the exceptions noted in §§ 5, 7, the developments in his first three sections are valid in the field F_p. But his derivation in § 5 of the relations between the characters is not valid in F_p, when p divides the order h of the group. In fact, the power e to which any irreducible factor occurs in G is a multiple of p (§ 7), so that $\partial\Phi^e/\partial x_R$ vanishes identically in F_p. His method, when applied to F_p, gives rise only to relations all of whose coefficients vanish.

Burnside's first treatment, *Proceedings London Mathematical Society*, volume 29 (1898), pages 207–224, 546–565, depends upon the special group determinant. Although his auxiliary theorems were established by purely rational processes by the writer in the *Transactions*, volume 3 (1902), page 285, it was indicated in the last paper, that the method is limited to fields whose modulus does not divide the order of the group.

Burnside's second treatment, *Acta Mathematica*, volume 28 (1904), page 369, and *Proceedings London Mathematical Society*, volume 1 (1901), page 117, depends upon the existence of an invariant Hermitian form, and hence is not applicable in the construction of a general theory of modular groups.

The exposition by Schur has the advantage that after the modifications noted in § 3, it yields important results in the modular theory.

THE UNIVERSITY OF CHICAGO,
May, 1907.