

FACTOR-SETS OF A GROUP IN ITS ABSTRACT UNIT GROUP

BY

A. H. CLIFFORD AND SAUNDERS MACLANE

The following interesting problem in group extensions arose in an arithmetical study of normal algebraic number fields⁽¹⁾.

Let Γ be any finite group of order n with elements $\rho, \sigma, \tau, \dots$. By the *abstract unit group* of Γ we mean the free abelian group \mathfrak{S} of rank $n-1$ generated by n symbols H^σ (σ ranging over Γ) subject to the single condition that their product is 1:

$$\prod_{\sigma} H^\sigma = 1.$$

Every element of \mathfrak{S} is expressible in the form $H^{\sum a(\sigma)\sigma}$ with integers $a(\sigma)$, and

$$H^{\sum a(\sigma)\sigma} = H^{\sum b(\sigma)\sigma}$$

if and only if there is an integer c such that

$$a(\sigma) - b(\sigma) = c, \quad \text{all } \sigma \text{ in } \Gamma.$$

(\mathfrak{S} is isomorphic with the additive group of the integral group ring of Γ reduced modulo the element $\sum \sigma$.)

For each τ in Γ , the mapping $H^\sigma \rightarrow H^{\sigma\tau}$ generates an automorphism of \mathfrak{S} , namely,

$$H^{\sum a(\sigma)\sigma} \rightarrow H^{\sum a(\sigma)\sigma\tau} = H^{\sum a(\sigma\tau^{-1})\sigma},$$

and to the product $\tau\rho$ evidently corresponds the product of the corresponding automorphisms:

Presented to the Society, February 22, 1941; received by the editors August 24, 1940.

⁽¹⁾ S. MacLane and O. F. G. Schilling, *Normal algebraic number fields*, these Transactions, vol. 50 (1941), pp. 295-384. The present paper is entirely independent thereof.

To indicate briefly what the connection is, let K be a real algebraic field normal of degree n over the rational field k , and let Γ be its Galois group. A theorem of Minkowski (Nachrichten der Gesellschaft der Wissenschaften zu Göttingen, 1900, p. 90) asserts the existence of a unit H in K such that the group \mathfrak{S} generated by H and all its conjugates H^σ is a free abelian group of rank $n-1$, the only relation satisfied by the H^σ being that asserting that the norm of H is 1. This group \mathfrak{S} is of finite index in the group of all units of K . MacLane and Schilling study the class field theory of K by introducing crossed products (K, Γ, F) . (K, Γ, F) is a normal simple algebra over k , determined by K, Γ , and a factor-set F of elements $F_{\sigma,\tau} \neq 0$ of K satisfying (0.3). Under the homomorphism $F_{\sigma,\tau} \rightarrow (F_{\sigma,\tau})$ carrying numerical factor-sets into factor-sets of principal ideals, those mapped into the identity are precisely the factor-sets of units. By further devices they are enabled in some cases to reduce the consideration of the latter to that of factor-sets lying in the Minkowski subgroup \mathfrak{S} .

$$(0.1) \quad A^{\tau\rho} = (A^{\tau})^{\rho}, \quad \text{all } A \text{ in } \mathfrak{S}.$$

This representation of Γ by automorphisms of \mathfrak{S} is effectively the right regular representation of Γ applied to the basis H^{σ} of \mathfrak{S} .

The problem in question is to determine all extensions⁽²⁾ \mathfrak{U} of \mathfrak{S} by Γ realizing this representation, and in particular to compute the number of non-equivalent such extensions, where by \mathfrak{U} equivalent to \mathfrak{U}' we mean the existence of an isomorphism between them leaving \mathfrak{S} and Γ fixed.

We shall think of an extension $\mathfrak{U} = \sum u_{\sigma} \mathfrak{S}$ of \mathfrak{S} by Γ as the set of all symbols $u_{\sigma}A$ (σ in Γ , A in \mathfrak{S}) with the multiplication laws

$$(0.2) \quad Au_{\sigma} = u_{\sigma}A^{\sigma}, \quad u_{\sigma}u_{\tau} = u_{\sigma\tau}F_{\sigma,\tau}.$$

The $F_{\sigma,\tau}$ are elements in \mathfrak{S} satisfying the "associativity conditions"

$$(0.3) \quad F_{\rho,\sigma}^{\tau}F_{\rho\sigma,\tau} = F_{\rho,\sigma\tau}F_{\sigma,\tau}.$$

Such a function $F_{\sigma,\tau}$ on $\Gamma\Gamma$ to \mathfrak{S} is called a factor-set⁽³⁾ (f.s.) of Γ in \mathfrak{S} . Passage to a new set of representatives $u_{\sigma}' = u_{\sigma}C_{\sigma}$ (C_{σ} in \mathfrak{S}) replaces $F_{\sigma,\tau}$ by

$$(0.4) \quad F'_{\sigma,\tau} = \frac{C_{\sigma}^{\tau}C_{\tau}}{C_{\sigma\tau}}F_{\sigma,\tau}.$$

The factor-sets $F_{\sigma,\tau}$ and $F'_{\sigma,\tau}$ are called associate. Two extensions \mathfrak{U} and \mathfrak{U}' are equivalent if and only if the factor-sets of Γ in \mathfrak{S} determined by them are associate.

If $F_{\sigma,\tau}$ and $G_{\sigma,\tau}$ are factor-sets, then so also is the product $F_{\sigma,\tau}G_{\sigma,\tau}$; for \mathfrak{S} is abelian, so that (0.3) is evidently satisfied. Hence the set of all factor-sets of Γ in \mathfrak{S} constitutes an abelian group $F\mathfrak{S}$. The identity element of $F\mathfrak{S}$ is the factor-set each value of which is the identity element 1 of \mathfrak{S} . The factor-sets associate to 1 form a subgroup $T\mathfrak{S}$ of $F\mathfrak{S}$, and the group $M\mathfrak{S} = F\mathfrak{S}/T\mathfrak{S}$ will be called the *multiplicator* of Γ in \mathfrak{S} . The order of $M\mathfrak{S}$ is the desired number of non-equivalent extensions of \mathfrak{S} by Γ .

Let now Ω be any algebraically closed field of characteristic not dividing the order n of Γ . By a factor-set of Γ in Ω we mean a function $\omega_{\sigma,\tau} \neq 0$ on $\Gamma\Gamma$ to Ω satisfying

$$(0.5) \quad \omega_{\rho,\sigma}\omega_{\rho\sigma,\tau} = \omega_{\rho,\sigma\tau}\omega_{\sigma,\tau}.$$

(2) For a description of Schreier's theory of group extensions, see e.g., H. Zassenhaus, *Lehrbuch der Gruppentheorie*, pp. 89–97 (Berlin, 1937). We call \mathfrak{U} an extension of \mathfrak{S} by Γ if it contains \mathfrak{S} as an invariant subgroup and $\mathfrak{U}/\mathfrak{S} \cong \Gamma$.

(3) In Zassenhaus and also in MacLane and Schilling, the representative elements u_{σ} of the cosets of $\mathfrak{S}/\mathfrak{S}$ are written on the right instead of the left. This leads to the composition law $A^{\tau\rho} = (A^{\rho})^{\tau}$ instead of (0.1), and to similar slight changes in (0.3), (0.4), etc. This divergence is regrettable, but the computations are bad enough without having to keep in mind that the composition law runs backwards.

(This differs from (0.3) only in the absence of the superscript τ on the left.) $\omega_{\sigma,\tau}$ and $\omega'_{\sigma,\tau}$ are associate if

$$(0.6) \quad \omega'_{\sigma,\tau} = \frac{c_{\sigma}c_{\tau}}{c_{\sigma\tau}} \omega_{\sigma,\tau}, \quad c_{\sigma} \in \Omega.$$

Schur⁽⁴⁾ defines the multiplier \mathfrak{M} of Γ to be the group of classes of associate factor-sets of Γ in Ω ; it is independent of Ω . *We conjecture that $M\mathfrak{S}$ and \mathfrak{M} are isomorphic*, and it is the purpose of the present paper to prove this conjecture in the case Γ solvable. The structure of \mathfrak{M} is of course much easier to determine than that of $M\mathfrak{S}$, and has already been found by Schur for a considerable number of groups. For example, if Γ is abelian, and is represented as the direct product of cyclic groups of orders m_1, \dots, m_t , then⁽⁵⁾ \mathfrak{M} is the direct product of $\frac{1}{2}t(t-1)$ cyclic groups $\mathfrak{M}_{i,j}$ ($i < j$), where the order of $\mathfrak{M}_{i,j}$ is the G.C.D. of m_i and m_j ; the order of \mathfrak{M} is thus $\prod_{i < j} (m_i, m_j)$.

If one cares to delve into the structure of $T\mathfrak{S}$, the natural thing to do is first to construct the group $V\mathfrak{S}$ of all "vectors" C_{σ} , which is simply the direct product of \mathfrak{S} with itself n times. The mapping

$$C_{\sigma} \rightarrow \frac{C_{\sigma}^{\tau} C_{\tau}}{C_{\sigma\tau}}$$

is a homomorphism of $V\mathfrak{S}$ onto $T\mathfrak{S}$, and hence $T\mathfrak{S} \simeq V\mathfrak{S}/U\mathfrak{S}$ where $U\mathfrak{S}$ is the subgroup of $V\mathfrak{S}$ consisting of those C_{σ} satisfying

$$C_{\sigma}^{\tau} C_{\tau} = C_{\sigma\tau}.$$

We call such a function C_{σ} a *crossed character* (c.c.) of Γ in \mathfrak{S} from the analogy with a crossed representation of Γ by matrices⁽⁶⁾ (i.e., by semi-linear transformations). The study of these is quite fascinating in its own right, in addition to being a necessary preliminary to the main task.

If C is a fixed element of \mathfrak{S} , then $C_{\sigma} = C^{1-\sigma}$ is a crossed character. The totality of these constitutes a subgroup $\mathfrak{S}^{1-\sigma}$ of $U\mathfrak{S}$. We make a second conjecture that the *crossed character group* $C\mathfrak{S} = U\mathfrak{S}/\mathfrak{S}^{1-\sigma}$ of Γ in \mathfrak{S} is isomorphic with the group \mathfrak{C} of linear characters of Γ in the field Ω (functions $\psi(\sigma)$ on Γ to Ω satisfying $\psi(\sigma\tau) = \psi(\sigma)\psi(\tau)$, $\psi(\sigma) \neq 0$), but again we are able to prove this only if Γ is solvable.

The paper is so arranged that all necessary lemmas involving explicit representation $A = H^{\Sigma a(\sigma)\sigma}$ of the elements A of \mathfrak{S} fall in §1. In the remainder of

(4) I. Schur, *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, Journal für die reine und angewandte Mathematik, vol. 127 (1904), pp. 20–50.

(5) Schur, Journal für die reine und angewandte Mathematik, vol. 132 (1907), p. 113.

(6) A. Speiser, *Zahlentheoretische Sätze aus der Gruppentheorie*, Mathematische Zeitschrift, vol. 5 (1919), pp. 1–6; I. Schur, *ibid.*, pp. 7–10.

the paper, only the formal properties expressed by these lemmas are used. In §2 the connection between $M\mathfrak{H}$ and \mathfrak{M} is indicated by means of the notion of trace: $\text{tr } A = \sum a(\sigma)$. The main theorem is stated in this section in two parts (Theorems 1A and 2A). In §3 crossed characters are developed, and the second conjecture proved (Theorems 1B and 2B). Theorem 1A is proved in §4, Theorem 2A in §5. In the final brief section, §6, $M\mathfrak{H}_0$ and $C\mathfrak{H}_0$ are determined, where \mathfrak{H}_0 is the subgroup of \mathfrak{H} of vanishing traces.

Actually we prove these four theorems for any solvable subgroup Γ^* of Γ , and make no restrictions on Γ . Theorem 2B does not even require that Γ^* be solvable. Theorem 1B might be called the "principal genus theorem for crossed characters of Γ^* in \mathfrak{H} ," being in essence just an extension of Lemma 2. O. F. G. Schilling was the first to observe the importance of such a theorem in his work on the class field theory. The authors wish to acknowledge that they profited considerably from discussions with Schilling.

1. Norms, traces, and the principal genus theorem. Let Δ be any subgroup of Γ , the elements of which will be denoted by α, β, \dots . The Δ -norm of an element A of \mathfrak{H} is defined to be

$$N_{\Delta}A = \prod_{\alpha} A^{\alpha} = A^{\sum \alpha}$$

extended over all α in Δ . Evidently

$$N_{\Delta}(AB) = (N_{\Delta}A)(N_{\Delta}B).$$

The Γ -norm of every element of \mathfrak{H} is 1. For if $A = H^{\sum a(\sigma)\sigma}$ then

$$N_{\Gamma}A = A^{\sum \tau} = H^{\sum \sigma a(\sigma)\sigma \sum \tau} = H^{\sum \tau \sum \sigma a(\sigma)\sigma} = 1$$

since $\sum \tau$ is in the center of the integral group ring of Γ , and $H^{\sum \tau} = 1$.

LEMMA 1. *An element A of \mathfrak{H} is invariant under a subgroup Δ of Γ if and only if it is the Δ -norm of an element B of \mathfrak{H} .*

Proof. If $A = N_{\Delta}B = B^{\sum \alpha}$, then since $(\sum \alpha)\beta = \sum \alpha$ for any β in Δ , we have $A^{\beta} = A$.

Suppose conversely that $A^{\alpha} = A$ for all α in Δ , and let $A = H^{\sum a(\sigma)\sigma}$. We then have

$$H^{\sum a(\sigma)\sigma} = A = A^{\alpha} = H^{\sum \sigma a(\sigma\alpha^{-1})\sigma}.$$

Hence to each α in Δ there exists an integer $c(\alpha)$ such that

$$a(\sigma) - a(\sigma\alpha^{-1}) = c(\alpha)$$

for all σ in Γ . Taking the sum of these equations over σ we get $0 = nc(\alpha)$, whence $c(\alpha) = 0$ and

$$(1.1) \quad a(\sigma\alpha) = a(\sigma), \quad \text{all } \sigma \in \Gamma, \alpha \in \Delta.$$

Let

$$\Gamma = \rho_1\Delta + \rho_2\Delta + \cdots + \rho_r\Delta.$$

Then by (1.1)

$$\sum_{\sigma \in \Gamma} a(\sigma)\sigma = \sum_{i=1}^r \sum_{\alpha \in \Delta} a(\rho_i)\rho_i\alpha = \sum_i a(\rho_i)\rho_i \sum_{\alpha} \alpha.$$

Hence if $B = H^{\sum_i a(\rho_i)\rho_i}$ we have

$$N_{\Delta}B = H^{\sum_i a(\rho_i)\rho_i \sum_{\alpha} \alpha} = H^{\sum a(\sigma)\sigma} = A,$$

which completes the proof.

Since $N_{\Gamma}A = 1$ for all A in \mathfrak{S} , it follows from this lemma that *there are no elements $\neq 1$ of \mathfrak{S} invariant under Γ* .

If ρ is any element of Γ and A is in \mathfrak{S} , we define the ρ -norm $N_{\rho}A$ of A to be $N_{\Delta}A$, where Δ is the cyclic group $\{\rho\}$ generated by ρ . If ρ has order r , then

$$N_{\rho}A = A^{1+\rho+\rho^2+\cdots+\rho^{r-1}}.$$

The *trace* of an element $A = H^{\sum a(\sigma)\sigma}$ of \mathfrak{S} is defined by

$$\text{tr } A = \sum a(\sigma).$$

Since for any integer c , $A = H^{\sum (a(\sigma)+c)\sigma}$ we have

$$\text{tr } A = \sum a(\sigma) + nc,$$

and hence $\text{tr } A$ is actually an integer taken modulo n . The coefficients $a(\sigma)$ can be chosen so that $\text{tr } A$ has one of the values $0, 1, 2, \dots, n-1$. It is clear that elements of any preassigned trace exist in \mathfrak{S} , for example, the powers of H . Evidently

$$(1.2) \quad \text{tr } AB \equiv \text{tr } A + \text{tr } B, \quad \text{tr } A^{\sigma} \equiv \text{tr } A, \quad \text{all } A, B \in \mathfrak{S}, \sigma \in \Gamma.$$

All congruences throughout the paper are taken modulo the order n of Γ and the sign (mod n) will be omitted.

The next lemma we might call the "principal genus theorem" for \mathfrak{S} , being analogous to Hilbert's theorem on units in a cyclic field⁽⁷⁾.

LEMMA 2. *Let ρ be any element of Γ , and let Δ^* be any subgroup of Γ invariant under ρ . Then an element A of \mathfrak{S} has the form $A = B^{1-\rho}$ with B invariant under Δ^* if and only if $N_{\rho}A = 1$, $\text{tr } A \equiv 0$, and A is invariant under Δ^* .*

Proof. Let $\Delta = \{\rho, \Delta^*\}$ be the group generated by ρ and Δ^* . Let g be the index of Δ^* in Δ , so that

$$\Delta = \Delta^* + \Delta^*\rho + \Delta^*\rho^2 + \cdots + \Delta^*\rho^{g-1}, \quad \rho^g \in \Delta^*.$$

⁽⁷⁾ D. Hilbert, *Gesammelte Abhandlungen*, vol. 1, Theorem 90, p. 149.

(The lemma is trivial if $\rho \in \Delta^*$; for, since \mathfrak{G} has no elements $\neq 1$ of finite order, each condition is equivalent to $A = 1$.) If $A = B^{1-\rho}$ with B invariant under Δ^* , and r is the order of ρ , then

$$\text{tr } A \equiv \text{tr } B - \text{tr } B^\rho \equiv 0, \quad N_\rho A = B^{1-\rho^r} = B^0 = 1.$$

If α is in Δ^* then so also is $\beta = \rho\alpha\rho^{-1}$, since Δ^* is invariant under ρ . Hence we have

$$B^{\rho\alpha} = B^{\beta\rho} = B^\rho,$$

and

$$A^\alpha = B^{\alpha-\rho\alpha} = B^{1-\rho} = A.$$

Assume conversely that $A = H^{\sum a(\sigma)\sigma}$ is invariant under Δ^* , $N_\rho A = 1$, and $\text{tr } A \equiv 0$. As in the proof of Lemma 1, equation (1.1), the invariance of A under Δ^* is equivalent to

$$(1.3) \quad a(\sigma\alpha) = a(\sigma), \quad \text{all } \sigma \in \Gamma, \alpha \in \Delta^*.$$

Again let r be the order of ρ . Then

$$\sum_{\sigma} a(\sigma)\sigma \sum_{i=0}^{r-1} \rho^i = \sum_i \sum_{\sigma} a(\sigma\rho^{-i})\sigma = \sum_{\sigma} \left(\sum_i a(\sigma\rho^i) \right) \sigma,$$

and hence $N_\rho A = 1$ requires that

$$(1.4) \quad \sum_{i=0}^{r-1} a(\sigma\rho^i) = c, \quad \text{all } \sigma \in \Gamma,$$

where c is an integer independent of σ .

Let $l = n/r$, and let $\lambda_1, \dots, \lambda_l$ be representative elements of the cosets in Γ of the cyclic group $\{\rho\}$ generated by ρ :

$$\Gamma = \lambda_1\{\rho\} + \lambda_2\{\rho\} + \dots + \lambda_l\{\rho\}.$$

We now choose the components $a(\sigma)$ of A so that $\text{tr } A$ is actually zero, not merely divisible by n . Then from (1.4).

$$0 = \text{tr } A = \sum_{j=1}^l \sum_{i=0}^{r-1} a(\lambda_j\rho^i) = \sum_{j=1}^l c = lc,$$

whence $c=0$. Using (1.3) and the fact that ρ^σ is in Δ^* , (1.4) with $c=0$ gives

$$(1.5) \quad \sum_{i=0}^{r-1} a(\sigma\rho^i) = 0, \quad \text{all } \sigma \in \Gamma.$$

Now let

$$\Gamma = \mu_1\Delta + \mu_2\Delta + \dots + \mu_m\Delta.$$

Every element of Γ is then uniquely expressible in the form $\mu_j \alpha \rho^i$ ($j=1, \dots, m; \alpha \in \Delta^*; i=0, \dots, g-1$). We define the element $B = H^{\sum b(\sigma)\sigma}$ as follows:

$$b(\mu_j \alpha \rho^i) = a(\mu_j \alpha) + a(\mu_j \alpha \rho) + \dots + a(\mu_j \alpha \rho^i).$$

(1.5) and $\rho^g \in \Delta^*$ give $b(\mu_j \alpha \rho^{-1}) = 0$, and hence

$$b(\mu_j \alpha \rho^i) - b(\mu_j \alpha \rho^{i-1}) = a(\mu_j \alpha \rho^i).$$

For any element $\sigma = \mu_j \alpha \rho^i$ of Γ this gives

$$b(\sigma) - b(\sigma \rho^{-1}) = a(\sigma),$$

whence $A = B^{1-\rho}$.

From (1.3),

$$a(\mu_j \alpha \rho^i) = a(\mu_j \rho^i \cdot \rho^{-i} \alpha \rho^i) = a(\mu_j \rho^i),$$

whence

$$b(\mu_j \alpha \rho^i) = b(\mu_j \rho^i).$$

Hence for any element $\sigma = \mu_j \alpha \rho^i$ of Γ and any element β of Δ^* ,

$$b(\sigma \beta) = b(\mu_j \cdot \alpha \rho^i \beta \rho^{-i} \cdot \rho^i) = b(\mu_j \rho^i) = b(\sigma),$$

whence $B^\beta = B$, and the proof is complete.

LEMMA 3. *If Δ is a subgroup of index m in Γ , then there exists an element A of \mathfrak{S} such that $\text{tr } A \equiv m$ and $N_\Delta A = 1$.*

Proof. Let

$$\Gamma = \mu_1 \Delta + \mu_2 \Delta + \dots + \mu_m \Delta.$$

Define $A = H^{\sum a(\sigma)\sigma}$ as follows:

$$a(\mu_j \alpha) = \begin{cases} 1 & \text{if } \alpha = 1, \\ 0 & \text{if } \alpha \neq 1, \end{cases} \quad \alpha \in \Delta; j = 1, \dots, m.$$

That $\text{tr } A \equiv m$ is obvious. If $\sigma = \mu_j \beta$ is any element of Γ ,

$$\sum_{\alpha \in \Delta} a(\sigma \alpha^{-1}) = \sum_{\alpha} a(\mu_j \beta \alpha^{-1}) = \sum_{\alpha} a(\mu_j \alpha) = 1.$$

Hence

$$\sum_{\sigma \in \Gamma} a(\sigma) \sigma \sum_{\alpha \in \Delta} \alpha = \sum_{\sigma} \left(\sum_{\alpha} a(\sigma \alpha^{-1}) \right) \sigma = \sum_{\sigma} \sigma,$$

and

$$N_\Delta A = H^{\sum \sigma} = 1.$$

COROLLARY. *An element A of \mathfrak{S} has the form $A = N_\rho B$ with $\text{tr } B \equiv 0$ if and only if $A^\rho = A$ and $\text{tr } A \equiv 0$.*

Proof. If $A = N_\rho B$ with $\text{tr } B \equiv 0$, then $A^\rho = A$ is evident and $\text{tr } A \equiv r \text{tr } B \equiv 0$, where r is the order of ρ . Conversely, from $A^\rho = A$ follows $A = N_\rho B_1$ for some $B_1 \in \mathfrak{S}$ by Lemma 1. Then $r \text{tr } B_1 \equiv \text{tr } A \equiv 0$. Fixing on a definite representation of B_1 , this asserts that $r \text{tr } B_1 = ln$ for some integer l . Applying Lemma 3 to $\Delta = \{\rho\}$, there exists C in \mathfrak{S} such that $\text{tr } C \equiv n/r$, $N_\rho C = 1$. Set $B = B_1 C^{-l}$. Then

$$N_\rho B = (N_\rho B_1)(N_\rho C)^{-l} = N_\rho B_1 = A,$$

$$\text{tr } B \equiv \text{tr } B_1 - l \text{tr } C \equiv \frac{ln}{r} - \frac{ln}{r} \equiv 0.$$

2. Connection with Schur's multiplier. In the brief discussion of factor-sets and group extensions in the introduction, \mathfrak{S} may of course be replaced by any abelian group \mathfrak{A} , and we may take any representation of Γ by automorphisms $A \rightarrow A^\sigma$ of \mathfrak{A} . The two cases with which we shall be chiefly concerned are: (1) Γ replaced by a subgroup Γ^* , without changing \mathfrak{S} , and (2) \mathfrak{A} a cyclic group \mathfrak{Z} of order n , with $z^\sigma = z$ for all $z \in \mathfrak{Z}$, $\sigma \in \Gamma$. (When Γ induces the identical automorphism in \mathfrak{A} we shall speak of *central extensions* \mathfrak{G} of \mathfrak{A} by Γ , since \mathfrak{A} is in the center of \mathfrak{G} .)

We shall call an f.s. $F_{\sigma, \tau}$ *normalized* if, in the extension \mathfrak{G} defined by (0.2),

$$\sigma^s = 1 \text{ implies } u_\sigma^s = 1.$$

From (0.2) one readily sees that this is equivalent to

$$(2.1) \quad F_{\sigma, \sigma} F_{\sigma, \sigma^2} \cdots F_{\sigma, \sigma^{s-1}} = 1 \quad \text{if} \quad \sigma^s = 1.$$

The set of all normalized f.s.'s of Γ in \mathfrak{A} constitutes a subgroup $\overline{F}\mathfrak{A}$ of $F\mathfrak{A}$, and we shall call the corresponding subgroup $\overline{M}\mathfrak{A}$ of $M\mathfrak{A}$ the *normalized multiplier* of Γ in \mathfrak{A} . In general, e.g., in case (2) above, $\overline{M}\mathfrak{A}$ is a proper subgroup of $M\mathfrak{A}$, but in case (1) they coincide:

If $\mathfrak{G}^ = \sum u_\sigma \mathfrak{S}$ ($\sigma \in \Gamma^*$) is any extension of \mathfrak{S} by a subgroup Γ^* of Γ , new representatives v_σ can be found such that if $\sigma^s = 1$ then $v_\sigma^s = 1$.*

In proving this we may evidently assume that s is the order of σ . It is clear that we can first normalize the u_σ so that $u_1 = 1$. Then

$$(2.2) \quad u_\sigma^s = F_{\sigma, \sigma} F_{\sigma, \sigma^2} \cdots F_{\sigma, \sigma^{s-1}} = A_\sigma$$

is an element of \mathfrak{S} . Since

$$A_\sigma^\sigma = u_\sigma^{-1} A_\sigma u_\sigma = u_\sigma^s = A_\sigma$$

there exists by Lemma 1 an element B_σ of \mathfrak{G} such that

$$(2.3) \quad A_\sigma = N_\sigma B_\sigma = B_\sigma^{1+\sigma+\cdots+\sigma^{s-1}}.$$

If we set $u_\sigma = v_\sigma B_\sigma$ then an easy calculation shows that

$$u_\sigma^s = v_\sigma^s B_\sigma^{1+\sigma+\cdots+\sigma^{s-1}} = v_\sigma^s A_\sigma,$$

whence $v_\sigma^s = 1$.

Now Schur has shown⁽⁸⁾ that any f.s. $\omega_{\sigma,\tau}$ of Γ in the field Ω (see introduction, equation (0.5)) is associate to one such that each number $\omega_{\sigma,\tau}$ is an n th root of unity. $\omega_{\sigma,\tau}$ defines a central extension $\sum \bar{u}_\sigma \Omega^*$ of the multiplicative group Ω^* of Ω by Γ :

$$(2.4) \quad \bar{u}_\sigma \bar{u}_\tau = \bar{u}_{\sigma\tau} \omega_{\sigma,\tau}, \quad \omega \bar{u}_\sigma = \bar{u}_\sigma \omega, \quad \text{all } \omega \in \Omega.$$

We proceed to show that $\omega_{\sigma,\tau}$ is associate to a normalized f.s. $\omega'_{\sigma,\tau}$ which likewise has the property $\omega_{\sigma,\tau}^n = 1$. Let

$$\omega_\sigma = \prod_{\tau} \omega_{\sigma,\tau}.$$

Taking the product of (0.5) over τ and using $\omega_{\rho,\sigma}^n = 1$, we get

$$(2.5) \quad \omega_{\rho\sigma} = \omega_\rho \omega_\sigma,$$

i.e., ω_σ is a linear character of Γ in Ω . If σ has order s and τ is arbitrary in Γ , then by successive multiplication of (2.4) on the left by \bar{u}_σ we find

$$a_\sigma = \bar{u}_\sigma^s = \omega_{\sigma,\tau} \omega_{\sigma,\sigma\tau} \cdots \omega_{\sigma,\sigma^{s-1}\tau}.$$

If we think of Γ as decomposed into $\{\sigma\}$ and its cosets, we see from this that $\omega_\sigma = a_\sigma^{n/s}$. Let c_σ be any s th root of a_σ^{-1} in Ω , and let $\bar{v}_\sigma = \bar{u}_\sigma c_\sigma$. Then $\bar{v}_\sigma^s = 1$, so that the new factor-set $\omega'_{\sigma,\tau}$ (given by (0.6)) is normalized. Since $c_\sigma^n = a_\sigma^{-n/s} = \omega_\sigma^{-1}$, raising (0.6) to the n th power and using (2.5) gives $\omega_{\sigma,\tau}^n = 1$.

Since the $\omega_{\sigma,\tau}$ lie in the cyclic group $\mathfrak{Z} = \mathfrak{Z}_n$ of n th roots of unity in Ω , the equations (2.4) also serve to define a central extension $\bar{\mathfrak{G}} = \sum \bar{u}_\sigma \mathfrak{Z}$ of \mathfrak{Z} by Γ . If two normalized f.s.'s of Γ in \mathfrak{Z} are associate relative to \mathfrak{Z} they are plainly associate relative to Ω . But the converse is also true. For if $\bar{v}_\sigma = \bar{u}_\sigma c_\sigma$ ($c_\sigma \in \Omega$), from $\bar{u}_\sigma^n = \bar{v}_\sigma^n = 1$ follows $c_\sigma^n = 1$, i.e., $c_\sigma \in \mathfrak{Z}$. We have therefore shown that *the multiplier \mathfrak{M} of any finite group Γ of order n (as defined by Schur) is isomorphic with the normalized multiplier $\bar{\mathfrak{M}}$ of Γ in a cyclic group \mathfrak{Z} of order n .* (The normalized f.s.'s of Γ in \mathfrak{Z} correspond to those central extensions $\bar{\mathfrak{G}}$ of \mathfrak{Z} by Γ having the property that the order of every element of $\bar{\mathfrak{G}}$ divides n .)

Let ϵ be a primitive n th root of unity in Ω , fixed throughout the rest of

(8) In the 1904 paper, p. 26.

the paper. If $F_{\sigma,\tau}$ is any f.s. of Γ in \mathfrak{S} and we set

$$(2.6) \quad f_{\sigma,\tau} = \text{tr } F_{\sigma,\tau},$$

then from (0.3) and (1.2)

$$(2.7) \quad f_{\rho,\sigma} + f_{\rho\sigma,\tau} \equiv f_{\rho,\sigma\tau} + f_{\sigma,\tau},$$

and hence

$$(2.8) \quad \omega_{\sigma,\tau} = \epsilon^{f_{\sigma,\tau}}$$

is an f.s. of Γ in \mathfrak{Z} . By taking traces of (0.4) it is clear that associate f.s.'s of Γ in \mathfrak{S} give rise to associate f.s.'s of Γ in \mathfrak{Z} :

$$(2.9) \quad f'_{\sigma,\tau} \equiv c_{\sigma} + c_{\tau} - c_{\sigma\tau} + f_{\sigma,\tau}, \quad c_{\sigma} = \text{tr } C_{\sigma}.$$

Again by (1.2) a product FF' maps into the sum $f+f'$ and thence into the product $\omega\omega'$. Finally, by taking the trace of (2.1),

$$(2.10) \quad f_{\sigma,\sigma} + f_{\sigma,\sigma^2} + \cdots + f_{\sigma,\sigma^{s-1}} \equiv 0, \quad \sigma^s = 1,$$

and using (2.8) it is seen that a normalized F maps into a normalized ω .

Since every F has been shown to be associate to a normalized one, the mapping $F \rightarrow f \rightarrow \omega$ given by (2.6) and (2.8) is a homomorphism of $M\mathfrak{S}$ onto a subgroup of $\overline{M}\mathfrak{Z}$. As mentioned in the introduction, our conjecture is that this is actually an isomorphism between $M\mathfrak{S}$ and $\overline{M}\mathfrak{Z}$ ($\simeq \mathfrak{M}$), and we shall prove it for solvable Γ . We must show (1) that distinct elements of $M\mathfrak{S}$ correspond to distinct elements of $\overline{M}\mathfrak{Z}$, and (2) that $\overline{M}\mathfrak{Z}$ is covered by the mapping. We accordingly split the main theorem into two parts. All the foregoing holds as well for any subgroup Γ^* of Γ , and the inductive nature of the proof makes it necessary to consider this more general situation. We are of course rewarded with a correspondingly more general result; only the subgroup Γ^* need be solvable, Γ being perfectly arbitrary.

To avoid circumlocution, we shall identify \mathfrak{Z} with the additive group of integers mod n . An f.s. of Γ in \mathfrak{Z} is then a set of integers $f_{\sigma,\tau}$ satisfying the congruence (2.7). Associate f.s.'s are connected as in (2.9). (2.10) is the normalization condition.

THEOREM 1A. *If Γ^* is a solvable subgroup of Γ , and if $F_{\sigma,\tau}$ is a factor-set of Γ^* in \mathfrak{S} such that the factor-set $\text{tr } F_{\sigma,\tau}$ of Γ^* in \mathfrak{Z} is associate to 1, then $F_{\sigma,\tau}$ is itself associate to 1.*

THEOREM 2A. *If Γ^* is a solvable subgroup of Γ , and if $f_{\sigma,\tau}$ is a normalized factor-set of Γ^* in \mathfrak{Z} , then there exists a normalized factor-set $F_{\sigma,\tau}$ of Γ^* in \mathfrak{S} such that $\text{tr } F_{\sigma,\tau} \equiv f_{\sigma,\tau}$.*

Theorem 1A will be proved in §4, Theorem 2A in §5. It is first necessary to develop the theory of crossed characters.

3. Crossed characters. Let Γ^* be a subgroup of order m of Γ which we regard as fixed throughout this section. There will be no occasion to consider elements of Γ outside of Γ^* .

As mentioned in the introduction, a function A_σ on Γ^* to \mathfrak{S} will be called a crossed character (c.c.) of Γ^* in \mathfrak{S} if

$$(3.1) \quad A_\sigma^\tau A_\tau = A_{\sigma\tau}.$$

If B_σ is another c.c. of Γ^* in \mathfrak{S} , so is $A_\sigma B_\sigma$, and likewise A_σ^{-1} . Hence they form an abelian group $U\mathfrak{S}$.

If A is any element of \mathfrak{S} and we set $A_\sigma = A^{1-\sigma}$ for all σ in Γ^* , then A_σ is a c.c. For

$$A_\sigma^\tau A_\tau = A^{(1-\sigma)\tau + (1-\tau)} = A^{1-\sigma\tau} = A_{\sigma\tau}.$$

$A^{1-\sigma}$ will be called a *unit* c.c. The unit c.c.'s of Γ^* in \mathfrak{S} constitute a subgroup $\mathfrak{S}^{1-\sigma}$ of $U\mathfrak{S}$. (Incidentally⁽⁹⁾, by taking the product of (3.1) over σ we find that the m th power of any c.c. is a unit c.c.)

If $a_\sigma = \text{tr } A_\sigma$ then from (3.1)

$$(3.2) \quad a_\sigma + a_\tau \equiv a_{\sigma\tau}$$

and hence

$$\psi_A(\sigma) = \epsilon^{a_\sigma}$$

is a linear character of Γ^* in the field Ω . Evidently

$$\psi_{AB}(\sigma) = \psi_A(\sigma)\psi_B(\sigma).$$

Moreover, if $A_\sigma = A^{1-\sigma}$ then $\text{tr } A_\sigma \equiv 0$ and $\psi_A(\sigma) = 1$. Hence the mapping $A_\sigma \rightarrow \psi_A(\sigma)$ is a homomorphism of the crossed character group $C\mathfrak{S} = U\mathfrak{S}/\mathfrak{S}^{1-\sigma}$ of Γ^* in \mathfrak{S} onto a subgroup of the group \mathfrak{C} of linear characters of Γ^* in Ω . (\mathfrak{C} is of course identical with the character group $C\mathfrak{Z}$ of Γ^* in \mathfrak{Z} .) We conjecture that this mapping is an isomorphism between $C\mathfrak{S}$ and \mathfrak{C} , and shall prove it for the case Γ^* solvable. Again we split the proof into its two parts. Observe here that *the second part* (Theorem 2B) *does not require the solvability of Γ^** .

THEOREM 1B. *If Γ^* is a solvable subgroup of Γ , and if A_σ is a crossed character of Γ^* in \mathfrak{S} such that $\text{tr } A_\sigma \equiv 0$, then A_σ is a unit crossed character.*

THEOREM 2B. *If Γ^* is any subgroup of Γ , and $\psi(\sigma)$ is a linear character of Γ^* in Ω , then there exists a crossed character A_σ of Γ^* in \mathfrak{S} such that $\epsilon^{\text{tr } A_\sigma} = \psi(\sigma)$.*

If we identify \mathfrak{Z} with the additive group of integers mod n , Theorem 2B is more conveniently expressed as follows. If Γ^* is any subgroup of Γ , and a_σ is a

(⁹) Cf. Zassenhaus, loc. cit., p. 126. Thus every c.c. of a finite group of order m in an abelian group of finite exponent prime to m is a unit c.c.

linear character of Γ^* in \mathfrak{Z} , i.e., the a_σ are integers satisfying (3.2), then there exists a c.c. A_σ of Γ^* in \mathfrak{S} such that $\text{tr } A_\sigma \equiv a_\sigma$.

Proof of 1B. Let A_σ be a c.c. of Γ^* in \mathfrak{S} . Putting $\sigma = \tau = 1$ in (3.1) we find $A_1 = 1$. From (3.1) one readily computes

$$(3.3) \quad A_{\sigma^i} = A_\sigma^{1+\sigma+\sigma^2+\cdots+\sigma^{i-1}}$$

for any σ in Γ^* and any positive integer i . If s is the order of σ , then $i = s$ yields

$$(3.4) \quad N_\sigma A_\sigma = 1.$$

We prove the theorem by showing that A_σ can be reduced to 1 by successive multiplication by unit c.c.'s $B^{1-\sigma}$. The result will be established by an obvious induction on a composition series of Γ^* when we have proved the following statement.

Let $\Delta^* \subset \Delta$ be subgroups of Γ^* such that Δ^* is invariant in Δ , and Δ/Δ^* is cyclic. If $A_\alpha = 1$ for all α in Δ^* , and $\text{tr } A_\sigma \equiv 0$ for all σ in Δ , then there exists B in \mathfrak{S} such that $A_\sigma = B^{1-\sigma}$ for all σ in Δ .

Let

$$\Delta = \Delta^* + \Delta^*\rho + \Delta^*\rho^2 + \cdots + \Delta^*\rho^{s-1}, \quad \rho^s \in \Delta^*.$$

From (3.1) and the condition $A_\alpha = 1$ we have, for every α in Δ^* ,

$$A_{\alpha\rho} = A_\rho, \quad A_{\rho\alpha} = A_\rho^\alpha,$$

and, since $\rho\alpha\rho^{-1}$ is in Δ^* ,

$$A_\rho^\alpha = A_{\rho\alpha} = A_{\rho\alpha\rho^{-1}\cdot\rho} = A_\rho.$$

Hence A_ρ is invariant under Δ^* , $N_\rho A_\rho = 1$ by (3.4), and $\text{tr } A_\rho \equiv 0$ by hypothesis. By Lemma 2 of §1 there exists an element $B = B_\rho$ of \mathfrak{S} (ρ is a fixed element!) such that

$$A_\rho = B^{1-\rho}, \quad B^\alpha = B, \quad \text{all } \alpha \in \Delta^*.$$

By (3.3),

$$A_{\rho^i} = B^{1-\rho^i},$$

and hence for any $\sigma = \alpha\rho^i$ in Δ ,

$$A_\sigma = A_{\alpha\rho^i} = A_{\rho^i} = B^{1-\rho^i} = B^{1-\alpha\rho^i} = B^{1-\sigma}.$$

Proof of 2B. Let Γ' be the commutator subgroup of Γ^* , and let ρ_1, \dots, ρ_t be representative elements of basic classes of the abelian group Γ^*/Γ' (expressed as a direct product of t cyclic groups). Let r_j be the order of ρ_j mod Γ' . Every linear character of Γ^* is a product of the basic characters ψ_j ($j = 1, \dots, t$) defined in the obvious way from

$$\psi_j(\rho_j) = \epsilon^{n/r_j}, \quad \psi_j(\rho_k) = 1 \quad \text{for } k \neq j.$$

(Any linear character of Γ^* must have the value 1 over Γ' .) We need only show that each basic ψ_j can be realized by a c.c. $A_\sigma^{(j)}$ of Γ^* in \mathfrak{S} , for then any linear character ψ can be realized by taking the corresponding product of the $A_\sigma^{(j)}$.

Without loss in generality we may take $j=1$, and for simplicity we write ρ for ρ_1 , r for r_1 , ψ for ψ_1 . $\Delta = \{\Gamma', \rho_2, \dots, \rho_t\}$ is an invariant subgroup of Γ^* ,

$$\Gamma^* = \Delta + \Delta\rho + \Delta\rho^2 + \dots + \Delta\rho^{r-1}, \quad \rho^r \in \Gamma' \subseteq \Delta,$$

and for each $\sigma = \alpha\rho^i$ of Γ^* ($\alpha \in \Delta$; $i=0, 1, \dots, r-1$) we have

$$(3.5) \quad \psi(\alpha\rho^i) = \epsilon^{in/r}.$$

By Lemma 3 of §1 there exists an element B of \mathfrak{S} such that

$$\text{tr } B \equiv \frac{n}{m}, \quad N_{\Gamma^*} B = 1,$$

since n/m is the index of Γ^* in Γ . Let

$$A = N_\Delta B.$$

Since m/r is the order of Δ ,

$$(3.6) \quad \text{tr } A \equiv \frac{m}{r} \text{tr } B \equiv \frac{m}{r} \cdot \frac{n}{m} \equiv \frac{n}{r}.$$

Also, since

$$\sum_{\alpha \in \Delta} \alpha \sum_{i=0}^{r-1} \rho^i = \sum_{\sigma \in \Gamma^*} \sigma,$$

we have

$$(3.7) \quad A^{1+\rho+\dots+\rho^{r-1}} = N_{\Gamma^*} B = 1.$$

For every $\sigma = \alpha\rho^i$ in Γ^* we now define

$$(3.8) \quad A_{\alpha\rho^i} = A^{1+\rho+\dots+\rho^{i-1}}.$$

Since A is a Δ -norm, it is invariant under the element ρ^r of Δ . From this and (3.7) it follows that (3.8) is valid for all integers $i \geq 0$. If β is in Δ so also are $\beta_j = \rho^j \beta \rho^{-j}$ ($j=0, 1, \dots, i-1$), and, since A is invariant under Δ ,

$$A_{\alpha\rho^i}^\beta = A^{\beta_0+\beta_1\rho+\dots+\beta_{i-1}\rho^{i-1}} = A_{\alpha\rho^i}.$$

For any two elements $\sigma = \alpha\rho^i$, $\tau = \beta\rho^j$ of Γ^* we therefore have

$$A_{\sigma\tau} = A_{\alpha\rho^i\beta\rho^{-i}\cdot\rho^{i+j}} = A_{\rho^{i+j}},$$

$$A_\sigma^\tau A_\tau = A_{\alpha\rho^i}^{\beta\rho^j} A_{\beta\rho^j} = A^{(1+\rho+\dots+\rho^{i-1})\rho^j + (1+\rho+\dots+\rho^{j-1})} = A_{\rho^{i+j}}.$$

Hence A_σ defined by (3.8) is a c.c. of Γ^* in \mathfrak{S} . By (3.6) for $\sigma = \alpha\rho^i$,

$$\text{tr } A_\sigma \equiv i \text{ tr } A \equiv \frac{in}{r},$$

whence by (3.5),

$$\epsilon^{\text{tr}} A_\sigma = \psi(\sigma).$$

Hence A_σ realizes the basic character $\psi(\sigma)$.

4. Proof of Theorem 1A. By hypothesis, Γ^* is a fixed solvable subgroup of Γ and $F_{\sigma,\tau}$ is an f.s. of Γ^* in \mathfrak{S} such that

$$(4.1) \quad \text{tr } F_{\sigma,\tau} \equiv c_\sigma + c_\tau - c_{\sigma\tau}, \quad \text{all } \sigma, \tau \in \Gamma^*,$$

where the c_σ are integers. By an obvious induction on a composition series of Γ^* , the theorem will be established when we have proved the following statement.

Let $\Delta^* \subset \Delta$ be subgroups of Γ^* such that Δ^* is invariant in Δ and Δ/Δ^* is cyclic. If the f.s. $F_{\alpha,\beta}$ of Δ^* in \mathfrak{S} is associate to 1 ($\alpha, \beta \in \Delta^*$), then the f.s. $F_{\sigma,\tau}$ of Δ in \mathfrak{S} is likewise associate to 1 ($\sigma, \tau \in \Delta$).

$F_{\sigma,\tau}$ determines an extension $\mathfrak{G} = \sum u_\sigma \mathfrak{S}$ ($\sigma \in \Delta$) of \mathfrak{S} by Δ :

$$u_\sigma u_\tau = u_{\sigma\tau} F_{\sigma,\tau}, \quad A u_\sigma = u_\sigma A^\sigma.$$

By hypothesis for induction we may assume the u_α ($\alpha \in \Delta^*$) so chosen that

$$(4.2) \quad u_\alpha u_\beta = u_{\alpha\beta}, \quad \alpha, \beta \in \Delta^*.$$

(It is hardly necessary to point out that an f.s. $F'_{\alpha,\beta}$ associate to $F_{\alpha,\beta}$ within a subgroup of Γ^* can be extended to an f.s. $F'_{\sigma,\tau}$ of Γ^* associate to $F_{\sigma,\tau}$, and that (4.1) remains valid with new integers c'_σ .)

Let

$$\Delta = \Delta^* + \rho\Delta^* + \cdots + \rho^{g-1}\Delta^*, \quad \rho^g \in \Delta^*.$$

Then

$$(4.3a) \quad u_\rho^{-1} u_\alpha u_\rho = u_{\rho^{-1}\alpha\rho} A_{\rho^{-1}\alpha\rho}, \quad \text{all } \alpha \in \Delta^*,$$

$$(4.3b) \quad u_\rho^g = u_{\rho^g} B,$$

where the elements $A_{\rho^{-1}\alpha\rho}$ and B are in \mathfrak{S} . The proof consists in showing that these elements can be reduced to 1 by successive normalizations of the u_σ . For if, along with (4.2), we have the equations

$$u_\rho^{-1} u_\alpha u_\rho = u_{\rho^{-1}\alpha\rho}, \quad u_\rho^g = u_{\rho^g}$$

and define for any $\sigma = \rho^i \alpha$ of Δ ($\alpha \in \Delta^*$; $i = 0, 1, \dots, g-1$)

$$u_{\rho^i \alpha} = u_\rho^i u_\alpha,$$

it is readily seen this last holds for all integers $i \geq 0$, and for any $\sigma = \rho^i \alpha$, $\tau = \rho^j \beta$ of Δ ,

$$u_\sigma u_\tau = u_\rho^{i+j} u_\rho^{-i} u_\alpha u_\rho^j u_\beta = u_\rho^{i+j} u_{\rho^{-i} \alpha \rho^j} u_\beta = u_{\rho^{i+j} \cdot \rho^{-i} \alpha \rho^j \beta} = u_{\sigma \tau}.$$

This means, of course, that the original $F_{\sigma, \tau}$ is associate to 1.

(4.3a) may also be written

$$u_\rho^{-1} u_{\rho \alpha \rho^{-1}} u_\rho = u_\alpha A_\alpha.$$

Hence for $\alpha, \beta \in \Delta^*$, using (4.2),

$$u_{\alpha \beta} A_{\alpha \beta} = u_\rho^{-1} u_{\rho \alpha \rho^{-1}} u_{\rho \beta \rho^{-1}} u_\rho = u_\alpha A_\alpha u_\beta A_\beta = u_{\alpha \beta} A_\alpha^\beta A_\beta.$$

A_α is thus a crossed character of Δ^* in \mathfrak{S} . We proceed to show that the u_α can be normalized so that $\text{tr } A_\alpha \equiv 0$. From

$$u_\alpha u_\rho = u_{\alpha \rho} F_{\alpha, \rho}, \quad u_\rho u_{\rho^{-1} \alpha \rho} = u_{\alpha \rho} F_{\rho, \rho^{-1} \alpha \rho}$$

and (4.3a) we find that

$$A_{\rho^{-1} \alpha \rho} = \frac{F_{\alpha, \rho}}{F_{\rho, \rho^{-1} \alpha \rho}}.$$

Hence by (4.1)

$$\text{tr } A_{\rho^{-1} \alpha \rho} \equiv c_\alpha - c_{\rho^{-1} \alpha \rho}.$$

Again from (4.1) and $F_{\alpha, \beta} = 1$ we see that c_α is a linear character of Δ^* in \mathfrak{S} , and hence by Theorem 2B there exists a c.c. C_α of Δ^* in \mathfrak{S} with $\text{tr } C_\alpha \equiv c_\alpha$. If we now set $u_\alpha = v_\alpha C_\alpha$, (4.2) remains valid for the v_α and

$$u_\rho^{-1} v_\alpha u_\rho = v_{\rho^{-1} \alpha \rho} A_{\rho^{-1} \alpha \rho}'$$

where

$$A_{\rho^{-1} \alpha \rho}' = C_{\rho^{-1} \alpha \rho} A_{\rho^{-1} \alpha \rho} C_\alpha^{-\rho}.$$

Hence

$$\text{tr } A_{\rho^{-1} \alpha \rho}' \equiv c_{\rho^{-1} \alpha \rho} + \text{tr } A_{\rho^{-1} \alpha \rho} - c_\alpha \equiv 0.$$

We may therefore assume that $\text{tr } A_\alpha \equiv 0$ in (4.3a).

But now A_α is a c.c. of Δ^* in \mathfrak{S} with zero trace, and by Theorem 1B there exists A in \mathfrak{S} such that $A_\alpha = A^{1-\alpha}$. If we now set $u_\rho = v_\rho A$ we find

$$v_\rho^{-1} u_\alpha v_\rho = A u_{\rho^{-1} \alpha \rho} A_{\rho^{-1} \alpha \rho} A^{-1} = u_{\rho^{-1} \alpha \rho} A_{\rho^{-1} \alpha \rho} A^{\rho^{-1} \alpha \rho - 1} = u_{\rho^{-1} \alpha \rho}.$$

Hence we can assume that the u_σ have been normalized so that, along with (4.2),

$$(4.4a) \quad u_\rho^{-1} u_\alpha u_\rho = u_{\rho^{-1} \alpha \rho}, \quad \alpha \in \Delta^*,$$

$$(4.4b) \quad u_\rho^0 = u_{\rho^0} B.$$

For $\alpha = \rho^0$, (4.4a) shows that u_ρ commutes with u_{ρ^0} . Hence by (4.4b) u_ρ must commute with B , so that $B^\rho = B$. By successive application of (4.4a),

$$u_\rho^{-\alpha} u_\alpha u_\rho^0 = u_{\rho^{-\alpha} \alpha \rho^0}.$$

By (4.4b),

$$u_\alpha u_{\rho^0} B = u_{\rho^0} B u_{\rho^{-\alpha} \alpha \rho^0}, \quad u_{\alpha \rho^0} B = u_{\alpha \rho^0} B^{\rho^{-\alpha} \alpha \rho^0}.$$

Replacing α by $\rho^0 \alpha \rho^{-0}$, this gives $B^\alpha = B$ (all $\alpha \in \Delta^*$). Since B is invariant under ρ as well as Δ^* , it is invariant under Δ , and hence by Lemma 1 of §1 there exists C in \mathfrak{S} such that $B = N_\Delta C$. Since

$$\sum_{\sigma \in \Delta} \sigma = \sum_{\alpha \in \Delta^*} \alpha \sum_{i=0}^{\rho-1} \rho^i$$

it follows that if we set $D = N_\Delta C$ then

$$B = D^{1+\rho+\dots+\rho^{\rho-1}}.$$

Hence if we set $u_\rho = v_\rho D$, we have

$$u_\rho^0 = v_\rho^0 B, \quad v_\rho^0 = u_{\rho^0},$$

and (4.4a) remains valid:

$$v_\rho^{-1} u_\alpha v_\rho = D u_{\rho^{-1} \alpha \rho} D^{-1} = u_{\rho^{-1} \alpha \rho}$$

since D (being a Δ^* -norm) is invariant under Δ^* . We have thus achieved the desired normalization.

5. Proof of Theorem 2A. Let us make first a preliminary observation. As stated in §2, Theorem 2A apparently gives more precise information than is really required. Given the normalized f.s. $f_{\sigma, \tau}$ of Γ^* in \mathfrak{Z} , all we require is an f.s. $F'_{\sigma, \tau}$ of Γ^* in \mathfrak{S} such that $\text{tr } F'_{\sigma, \tau}$ is associate to $f_{\sigma, \tau}$:

$$\text{tr } F'_{\sigma, \tau} \equiv f_{\sigma, \tau} + c_\sigma + c_\tau - c_{\sigma\tau}.$$

But if such an $F'_{\sigma, \tau}$ is given, there exists a normalized f.s. $F_{\sigma, \tau}$ associate to it such that $\text{tr } F_{\sigma, \tau} \equiv f_{\sigma, \tau}$. We first pick any elements C_σ in \mathfrak{S} such that $\text{tr } C_\sigma \equiv c_\sigma$. Then the associate f.s. $F_{\sigma, \tau}$ given by (0.4) has the property that $\text{tr } F_{\sigma, \tau} \equiv f_{\sigma, \tau}$. Now taking the trace of (2.2) and using the hypothesis (2.10) that $f_{\sigma, \tau}$ is normalized, we see that the elements A_σ defined by (2.2) have zero trace. By the corollary to Lemma 3 of §1, the elements B_σ in (2.3) can be chosen so as to have zero trace. Hence on setting $u_\sigma = v_\sigma B_\sigma$ the resulting normalized f.s. has the same trace as $F_{\sigma, \tau}$.

Theorem 2A will be established by an obvious induction on a composition series of Γ^* when we have proved the following statement.

Let $\Delta^* \subset \Delta$ be subgroups of Γ^* such that Δ^* is invariant in Δ and Δ/Δ^* is cyclic. If $F_{\alpha, \beta}$ is a normalized f.s. of Δ^* in \mathfrak{S} such that $\text{tr } F_{\alpha, \beta} \equiv f_{\alpha, \beta}$, then it is possible to construct a normalized f.s. $F_{\sigma, \tau}$ of Δ in \mathfrak{S} such that $\text{tr } F_{\sigma, \tau} \equiv f_{\sigma, \tau}$.

By virtue of the preliminary observation (applied to Δ) we need only construct an f.s. $F_{\sigma, \tau}$ of Δ in \mathfrak{S} such that $\text{tr } F_{\sigma, \tau}$ is associate to $f_{\sigma, \tau}$.

Let

$$\Delta = \Delta^* + \rho\Delta^* + \cdots + \rho^{g-1}\Delta^*, \quad \rho^g \in \Delta^*.$$

Let \mathfrak{A} be any abelian group, which we later specialize to be \mathfrak{S} or \mathfrak{Z} , and let $A \rightarrow A^\sigma$ be a representation of Δ by automorphisms of \mathfrak{A} : $(A^\sigma)^\tau = A^{\sigma\tau}$. Let $\mathfrak{G}^* = \sum u_\alpha \mathfrak{A}$ ($\alpha \in \Delta^*$) be a given extension of \mathfrak{A} by Δ^* :

$$u_\alpha u_\beta = u_{\alpha\beta} F_{\alpha, \beta}, \quad Au_\alpha = u_\alpha A^\alpha.$$

Let u_ρ be a new symbol. Then (Zassenhaus, loc. cit., p. 94) the equations

$$(5.1a) \quad u_\rho^{-1} u_\alpha u_\rho = u_{\rho^{-1}\alpha\rho} A_{\rho^{-1}\alpha\rho}, \quad \text{all } \alpha \in \Delta^*,$$

$$(5.1b) \quad u_\rho^{-1} A u_\rho = A^\rho, \quad \text{all } A \in \mathfrak{A},$$

$$(5.1c) \quad u_\rho^g = u_{\rho^g} B$$

with $A_{\rho^{-1}\alpha\rho}$ and B in \mathfrak{A} , will define a cyclic extension

$$\mathfrak{G} = \mathfrak{G}^* + u_\rho \mathfrak{G}^* + u_\rho^2 \mathfrak{G}^* + \cdots + u_\rho^{g-1} \mathfrak{G}^*$$

of \mathfrak{G}^* if and only if the following three conditions are satisfied.

I. The mapping (combining (5.1a) and (5.1b))

$$u_\alpha A \rightarrow P(u_\alpha A) = u_{\rho^{-1}\alpha\rho} A_{\rho^{-1}\alpha\rho} A^\rho$$

is an automorphism of \mathfrak{G}^* ($\alpha \in \Delta^*$, $A \in \mathfrak{A}$).

II. The g th power P^g of P is the inner automorphism defined by $u_{\rho^g} B$:

$$P^g(u_\alpha A) = (u_{\rho^g} B)^{-1} u_\alpha A (u_{\rho^g} B).$$

III. $u_{\rho^g} B$ is invariant under P :

$$P(u_{\rho^g} B) = u_{\rho^g} B.$$

If these conditions are satisfied the group \mathfrak{G} will be an extension of \mathfrak{A} by Δ . For by (5.1b) \mathfrak{A} is invariant in \mathfrak{G} , every element of \mathfrak{G} is uniquely expressible in the form

$$u_\rho^i u_\alpha A, \quad i = 0, 1, \dots, g-1; \alpha \in \Delta^*; A \in \mathfrak{A},$$

and if for each $\sigma = \rho^i \alpha$ in Δ we define u_σ by $u_{\rho^i \alpha} = u_\rho^i u_\alpha$, the product $u_\sigma u_\tau$ will differ from $u_{\sigma\tau}$ by a factor in \mathfrak{A} .

It can be shown⁽¹⁰⁾ by straightforward computation that I, II, III are equivalent respectively to the following conditions on the elements A_α, B of \mathfrak{A} .

$$(Ia) \quad F_{\rho\alpha\rho^{-1}, \rho\beta\rho^{-1}}^\rho = \frac{A_\alpha^\beta A_\beta}{A_{\alpha\beta}} F_{\alpha, \beta}, \quad \alpha, \beta \in \Delta^*.$$

$$(IIa) \quad B^{1-\alpha} = \frac{F_{\rho^\theta, \alpha}}{F_{\rho^\theta\alpha\rho^{-\theta}, \rho^\theta}} A_\alpha A_{\rho\alpha\rho^{-1}}^\rho A_{\rho^2\alpha\rho^{-2}}^{\rho^2} \cdots A_{\rho^{\theta-1}\alpha\rho^{-\theta+1}}^{\rho^{\theta-1}}, \quad \alpha \in \Delta^*,$$

$$(IIIa) \quad B^{1-\rho} = A_{\rho^\theta}.$$

By hypothesis, $\omega_{\sigma, \tau} = \epsilon^{f_{\sigma, \tau}}$ is, with σ and τ ranging over Δ , an f.s. of Δ in \mathfrak{Z} . Let $\bar{\mathfrak{G}} = \sum \bar{u}_\sigma \mathfrak{Z}$ be the corresponding central extension of \mathfrak{Z} by Δ :

$$\bar{u}_\sigma \bar{u}_\tau = \bar{u}_{\sigma\tau} \omega_{\sigma, \tau}, \quad z \bar{u}_\sigma = \bar{u}_\sigma z, \quad \text{all } z \in \mathfrak{Z}.$$

The equations (5.1) for $\mathfrak{A} = \mathfrak{Z}$ have the form

$$(5.2a) \quad \bar{u}_\rho^{-1} \bar{u}_\alpha \bar{u}_\rho = \bar{u}_{\rho^{-1}\alpha\rho} \epsilon^{a_{\rho^{-1}\alpha\rho}}, \quad \text{all } \alpha \in \Delta^*,$$

$$(5.2b) \quad \bar{u}_\rho^{-1} z \bar{u}_\rho = z, \quad \text{all } z \in \mathfrak{Z},$$

$$(5.2c) \quad \bar{u}_\rho^\theta = \bar{u}_{\rho^\theta} \epsilon^b,$$

with integers a_α and b . Since these equations do in fact define an extension $\bar{\mathfrak{G}}$ of $\bar{\mathfrak{G}}^* = \sum \bar{u}_\alpha \mathfrak{Z}$ ($\alpha \in \Delta^*$), the conditions (Ia), (IIa), (IIIa) must hold. Translated into congruences involving the exponents $f_{\alpha, \beta}$, a_α , b of ϵ they are respectively as follows:

$$(Ib) \quad f_{\rho\alpha\rho^{-1}, \rho\beta\rho^{-1}} \equiv a_\alpha + a_\beta - a_{\alpha\beta} + f_{\alpha, \beta}, \quad \alpha, \beta \in \Delta^*,$$

$$(IIb) \quad f_{\rho^\theta\alpha\rho^{-\theta}, \rho^\theta} - f_{\rho^\theta, \alpha} \equiv a_\alpha + a_{\rho\alpha\rho^{-1}} + a_{\rho^2\alpha\rho^{-2}} + \cdots + a_{\rho^{\theta-1}\alpha\rho^{-\theta+1}}, \quad \alpha \in \Delta^*,$$

$$(IIIb) \quad a_{\rho^\theta} \equiv 0.$$

The integer b does not enter into these, but from (5.2c) and the assumption that $f_{\sigma, \tau}$ is normalized we have

$$1 = \bar{u}_\rho^n = (\bar{u}_{\rho^\theta})^{n/\theta} \epsilon^{nb/\theta} = \epsilon^{nb/\theta}.$$

Therefore

$$(IVb) \quad \text{the integer } b \text{ is divisible by the index } g \text{ of } \Delta^* \text{ in } \Delta.$$

By hypothesis for induction, we have already constructed a normalized f.s. $F_{\alpha, \beta}$ of Δ^* in \mathfrak{H} such that $\text{tr } F_{\alpha, \beta} \equiv f_{\alpha, \beta}$, and corresponding thereto we have an extension $\bar{\mathfrak{G}}^* = \sum u_\alpha \mathfrak{H}$ of \mathfrak{H} by Δ^* . The whole proof will consist in showing that we can find elements A_α, B of \mathfrak{H} satisfying (Ia), (IIa), (IIIa) (with $\mathfrak{A} = \mathfrak{H}$) and such that

⁽¹⁰⁾ Due to its rather unwieldy nature, much of the computation in this section will be omitted.

$$(5.3) \quad \text{tr } A_\alpha \equiv a_\alpha, \quad \text{tr } B \equiv b.$$

For, if such elements exist, the equations (5.1) define an extension $\mathfrak{G} = \sum u_\sigma \mathfrak{H}$ of \mathfrak{H} by Δ . We then define, for each $\sigma = \rho^i \alpha$ of Δ ,

$$u_{\rho^i \alpha} = u_\rho^i u_\alpha, \quad i = 0, 1, \dots, g-1,$$

and at the same time make a new choice of representative elements

$$\bar{u}_{\rho^i \alpha} = \bar{u}_\rho^i \bar{u}_\alpha$$

in the extension $\bar{\mathfrak{G}}$ of \mathfrak{H} by Δ . The latter determine an f.s. $f'_{\sigma, \tau}$ of Δ in \mathfrak{H} associate to $f_{\sigma, \tau}$ and coinciding with it within Δ^* . The former determine an f.s. $F_{\sigma, \tau}$ of Δ in \mathfrak{G} coinciding with $F_{\alpha, \beta}$ within Δ^* . But the f.s. $\omega'_{\sigma, \tau} = \epsilon f'_{\sigma, \tau}$ of Δ in \mathfrak{H} is computed from the elements ϵ^a, ϵ^b in formally the same way that $F_{\sigma, \tau}$ is computed from A_α, B . Hence the trace relations (5.3) will carry over into $\text{tr } F_{\sigma, \tau} \equiv f'_{\sigma, \tau}$ for all σ and τ in Δ , which is the desired result.

$F_{\alpha, \beta}$ being an f.s. of Δ^* in \mathfrak{G} , that is,

$$(5.4) \quad F_{\alpha, \beta}^\gamma F_{\alpha \beta, \gamma} = F_{\alpha, \beta \gamma} F_{\beta, \gamma}, \quad \text{all } \alpha, \beta, \gamma \in \Delta^*,$$

one readily verifies by direct substitution in (5.4) that $F_{\rho \alpha \rho^{-1}, \rho \beta \rho^{-1}}^\rho$ (ρ is a fixed element!) is also an f.s. of Δ^* in \mathfrak{G} . (Were the group \mathfrak{G} already constructed, it would belong to the representatives $v_\alpha = u_\rho^{-1} u_{\rho \alpha \rho^{-1}} u_\rho$.) (Ib) asserts that the f.s.

$$\frac{F_{\rho \alpha \rho^{-1}, \rho \beta \rho^{-1}}^\rho}{F_{\alpha, \beta}}$$

has trace $a_\alpha + a_\beta - a_{\alpha \beta}$. It follows from Theorem 1A (applied to Δ) that this f.s. is associate to 1. Hence there exist elements C_α in \mathfrak{H} such that

$$F_{\rho \alpha \rho^{-1}, \rho \beta \rho^{-1}}^\rho = \frac{C_\alpha^\beta C_\beta}{C_{\alpha \beta}} F_{\alpha, \beta}, \quad \alpha, \beta \in \Delta^*.$$

Let $c_\alpha = \text{tr } C_\alpha$. Then, taking traces,

$$f_{\rho \alpha \rho^{-1}, \rho \beta \rho^{-1}} \equiv c_\alpha + c_\beta - c_{\alpha \beta} + f_{\alpha, \beta}.$$

Combining this with (Ib), we see that $d_\alpha = a_\alpha - c_\alpha$ is a linear character of Δ^* in \mathfrak{H} . By Theorem 2B, there exists a c.c. D_α of Δ^* in \mathfrak{H} such that $\text{tr } D_\alpha \equiv d_\alpha$. Set $A_\alpha = C_\alpha D_\alpha$. Then (Ia) holds and $\text{tr } A_\alpha \equiv a_\alpha$.

Now let B_α stand for the expression on the right of (IIa) with the A_α as already determined. Form the expression

$$(5.5) \quad \frac{B_\alpha^\beta B_\beta}{B_{\alpha \beta}}$$

directly from the definition of B_α . Divide (Ia) by $F_{\alpha,\beta}$, solving for the A -expression, so to speak. Using this in (5.5) one replaces each of the g A -expressions by a quotient of two F 's. Each numerator cancels the following denominator, and (5.5) reduces to

$$(5.6) \quad \frac{F_{\rho\theta,\alpha}^\beta F_{\rho\theta,\beta} F_{\rho\theta,\alpha\beta\rho^{-\theta},\rho\theta}}{F_{\rho\theta,\alpha\rho^{-\theta},\rho\theta}^\beta F_{\rho\theta,\beta\rho^{-\theta},\rho\theta} F_{\rho\theta,\alpha\beta}} \cdot \frac{F_{\rho\theta,\alpha\rho^{-\theta},\rho\theta\beta\rho^{-\theta}}^{\rho\theta}}{F_{\alpha,\beta}}.$$

The left factor is the original F -part of (5.5); the right factor is all that remains of the A -part. By means of the f.s. identities (5.4), with (α, β, γ) replaced in turn by $(\rho^\theta, \alpha, \beta)$, $(\rho^\theta\alpha\rho^{-\theta}, \rho^\theta, \beta)$, and $(\rho^\theta\alpha\rho^{-\theta}, \rho^\theta\beta\rho^{-\theta}, \rho^\theta)$, (5.6) is found to reduce to 1. Hence B_α is a c.c. of Δ^* in \mathfrak{S} .

But (IIb) asserts that B_α has zero trace, since we already have $\text{tr } A_\alpha \equiv a_\alpha$. By Theorem 1B, there exists B in \mathfrak{S} such that $B_\alpha = B^{1-\alpha}$. B then satisfies (IIa). It does not necessarily satisfy (IIIa) of course, and our next task is to find B_1 in \mathfrak{S} which satisfies both, i.e.,

$$(5.7) \quad B_1^{1-\alpha} = B^{1-\alpha} \quad (\text{all } \alpha \in \Delta^*), \quad B_1^{1-\rho} = A_{\rho\theta}.$$

For $\alpha = \rho^\theta$, (IIa) gives

$$B^{1-\rho\theta} = A_{\rho\theta}^{1+\rho+\cdots+\rho\theta-1}.$$

Hence

$$(5.8) \quad N_\rho A_{\rho\theta} = N_{\rho\theta} B^{1-\rho^\theta} = 1.$$

By (IIa),

$$B^{(1-\rho)(1-\alpha)} = \frac{B^{1-\alpha}}{B^{(1-\rho\alpha\rho^{-1})\rho}} = \frac{F_{\rho\theta,\alpha}^\rho F_{\rho\theta+1\alpha\rho^{-\theta-1},\rho\theta}}{F_{\rho\theta,\alpha\rho^{-\theta},\rho\theta}^\rho F_{\rho\theta,\rho\alpha\rho^{-1}}^\rho} \cdot \frac{A_\alpha}{A_{\rho\theta,\alpha\rho^{-\theta}}^{\rho\theta}}.$$

By (Ia) with (α, β) replaced by (ρ^θ, α) and $(\rho^\theta\alpha\rho^{-\theta}, \rho^\theta)$ this reduces to

$$B^{(1-\rho)(1-\alpha)} = A_{\rho\theta}^{1-\alpha}.$$

Hence the element $A_{\rho\theta} B^{-1+\rho}$ is invariant under Δ^* . By (5.8) its ρ -norm is 1. By (IIIb) its trace is zero. Hence by Lemma 2 of §1 there exists an element C invariant under Δ^* such that

$$A_{\rho\theta} B^{-1+\rho} = C^{1-\rho}.$$

Then $B_1 = BC$ has the desired property (5.7), and so satisfies (IIa) and (IIIa). We have therefore succeeded in finding elements A_α, B of \mathfrak{S} (we now write B for B_1) satisfying (Ia), (IIa), and (IIIa) and such that $\text{tr } A_\alpha \equiv a_\alpha$. It remains only to show that they can be modified so as to satisfy the second condition of (5.3), $\text{tr } B \equiv b$.

Since A_α and B satisfy (Ia), (IIa), (IIIa), the equations (5.1) define an extension $\mathfrak{G} = \sum u_\sigma \mathfrak{G}$ of \mathfrak{G} by Δ . Let r be the order of ρ ; it is divisible by g , say $r = gh$. Raising (5.1c) to the power h ,

$$u_\rho^r = u_{\rho\sigma}^h N_{\rho\sigma} B.$$

By hypothesis for induction, the f.s. $F_{\alpha,\beta}$ of Δ^* in \mathfrak{G} is normalized, and hence $u_{\rho\sigma}^h = 1$. Since u_ρ commutes with u_ρ^r , the latter is invariant under ρ and by Lemma 1 must be the ρ -norm of an element D of \mathfrak{G} :

$$N_{\rho\sigma} B = N_\rho D.$$

Taking traces,

$$h \operatorname{tr} B \equiv hg \operatorname{tr} D.$$

Since n is divisible by hg it follows that $\operatorname{tr} B$ is divisible by g , say

$$\operatorname{tr} B \equiv gk_1.$$

By (IVb), b is also divisible by g , say

$$b \equiv gk_2.$$

Now let E be any element of \mathfrak{G} such that

$$\operatorname{tr} E \equiv k_2 - k_1,$$

and let

$$A'_\alpha = A_\alpha E^{1-\alpha}.$$

Since $E^{1-\alpha}$ is a c.c., (Ia) will remain valid with A'_α instead of A_α . If we replace A_α by A'_α in the right-hand member of (IIa), the new expression is equal to the old one multiplied by E with the exponent

$$\begin{aligned} (1 - \alpha) + (1 - \rho\alpha\rho^{-1})\rho + \cdots + (1 - \rho^{g-1}\alpha\rho^{-g+1})\rho^{g-1} \\ = (1 + \rho + \cdots + \rho^{g-1})(1 - \alpha). \end{aligned}$$

Hence (IIa) will remain valid if we replace B by

$$B' = E^{1+\rho+\cdots+\rho^{g-1}} B.$$

(IIIa) will also remain valid, since

$$B'^{1-\rho} = E^{1-\rho g} B^{1-\rho} = E^{1-\rho g} A_{\rho\sigma} = A'_{\rho\sigma}.$$

But we now have

$$\operatorname{tr} A'_\alpha \equiv \operatorname{tr} A_\alpha \equiv a_\alpha,$$

$$\operatorname{tr} B' \equiv g \operatorname{tr} E + \operatorname{tr} B \equiv g(k_2 - k_1) + gk_1 \equiv b.$$

Hence the elements A'_α, B' satisfy (Ia), (IIa), (IIIa) and the trace conditions (5.3), which concludes the proof of the theorem.

6. The subgroup of vanishing traces. Let \mathfrak{H}_0 be the subgroup of \mathfrak{H} consisting of all A in \mathfrak{H} with $\text{tr } A \equiv 0$. $\mathfrak{H}/\mathfrak{H}_0$ is evidently a cyclic group of order n . Let Γ^* be a solvable subgroup of Γ of order m . We conclude the paper by proving the following two statements.

(1) *The multiplier of Γ^* in \mathfrak{H}_0 is 1.*

(2) *The crossed character group of Γ^* in \mathfrak{H}_0 is cyclic of order m .*

Let $F_{\sigma, \tau}$ be an f.s. of Γ^* in \mathfrak{H}_0 . Since this means that $\text{tr } F_{\sigma, \tau} \equiv 0$, it follows from Theorem 1A that elements A_σ exist in \mathfrak{H} such that

$$F_{\sigma, \tau} = \frac{A_\sigma^\tau A_\tau}{A_{\sigma\tau}}.$$

Let $a_\sigma = \text{tr } A_\sigma$. Taking traces, we obtain $0 \equiv a_\sigma + a_\tau - a_{\sigma\tau}$. By Theorem 2B, there exists a c.c. B_σ of Γ^* in \mathfrak{H} such that $\text{tr } B_\sigma \equiv a_\sigma$. Setting $C_\sigma = A_\sigma B_\sigma^{-1}$ we have

$$F_{\sigma, \tau} = \frac{C_\sigma^\tau C_\tau}{C_{\sigma\tau}}$$

with $\text{tr } C_\sigma \equiv 0$. Hence $F_{\sigma, \tau}$ is associate to 1 in \mathfrak{H}_0 , proving (1).

Let A_σ be a c.c. of Γ^* in \mathfrak{H} . Since this means that $\text{tr } A_\sigma \equiv 0$, it follows from Theorem 1B that A_σ is a unit c.c. of Γ^* in \mathfrak{H} . Conversely every unit c.c. $A^{1-\sigma}$ of Γ^* in \mathfrak{H} lies in \mathfrak{H}_0 . Hence the group $U\mathfrak{H}_0$ of c.c.'s of Γ^* in \mathfrak{H}_0 coincides with the group $\mathfrak{H}^{1-\sigma}$ of unit c.c.'s of Γ^* in \mathfrak{H} , and the crossed character group $C\mathfrak{H}_0$ of Γ^* in \mathfrak{H}_0 is by definition $\mathfrak{H}^{1-\sigma}/\mathfrak{H}_0^{1-\sigma}$.

Let $N_{\Gamma^*}\mathfrak{H}$ be the subgroup of \mathfrak{H} invariant under Γ^* . Considering the homomorphism $A \rightarrow A^{1-\sigma}$ of \mathfrak{H} onto $\mathfrak{H}^{1-\sigma}$ we see that $\mathfrak{H}^{1-\sigma} \simeq \mathfrak{H}/N_{\Gamma^*}\mathfrak{H}$. The subgroup $N_{\Gamma^*}\mathfrak{H}_0$ of \mathfrak{H}_0 invariant under Γ^* is evidently the intersection $\mathfrak{H}_0 \cap N_{\Gamma^*}\mathfrak{H}$. (That it coincides with the group of Γ^* -norms of elements of \mathfrak{H}_0 follows from the corollary to Lemma 3, but we do not need this.) Hence $\mathfrak{H}_0^{1-\sigma} \simeq \mathfrak{H}_0/N_{\Gamma^*}\mathfrak{H}_0 \simeq \mathfrak{H}_{\Gamma^*}/N_{\Gamma^*}\mathfrak{H}$, where \mathfrak{H}_{Γ^*} is the group generated by \mathfrak{H}_0 and $N_{\Gamma^*}\mathfrak{H}$. Since $N_{\Gamma^*}\mathfrak{H}$ is the group of Γ^* -norms of elements of \mathfrak{H} (Lemma 1), the trace of every element thereof, and hence the trace of every element of \mathfrak{H}_{Γ^*} , is divisible by m . Conversely, if the trace of A in \mathfrak{H} is divisible by m , say $\text{tr } A \equiv lm$, and we select any element B of trace l , then $C = N_{\Gamma^*}B$ has trace lm and $A = AC^{-1} \cdot C$ is in \mathfrak{H}_{Γ^*} ; for AC^{-1} is in \mathfrak{H}_0 and C is in $N_{\Gamma^*}\mathfrak{H}$. Hence \mathfrak{H}_{Γ^*} consists of all elements of \mathfrak{H} whose traces are divisible by m . (2) then follows from $\mathfrak{H}^{1-\sigma}/\mathfrak{H}_0^{1-\sigma} \simeq \mathfrak{H}/\mathfrak{H}_{\Gamma^*}$.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY,
CAMBRIDGE, MASS.
HARVARD UNIVERSITY,
CAMBRIDGE, MASS.