Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 19 (1973)
Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: FINITE GROUPS AND DIVISION ALGEBRAS
Autor: Ford, Charles
DOI: https://doi.org/10.5169/seals-46295

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 16.10.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

FINITE GROUPS AND DIVISION ALGEBRAS

by Charles FORD

The rational quaternions form a four dimensional division algebra over the rational field. Contained as a multiplicative subgroup is the quaternion group whose eight elements generate the algebra as a rational vector space. The main purpose of our paper is to present, in sections one, two and three, the existence and structure of certain division algebras which are generated over the rational field by a finite multiplicative group. A more general problem, the determination of *all* division algebras which are generated over the rational field by some finite group, was made by Amitsur [2]. We describe some of Amitsur's results in section four. The most general connection between finite groups and division algebras arises in the study of the group algebra. The fifth section of this paper describes several general results relating division algebras and finite groups and concludes with an indication of some recent work in this area.

Usually, a proof of the existence of division algebras, as in Amitsur's paper or in Albert's book [1], assumes a tremendous amount of background material, including the global and local theory of algebras and of algebraic number theory. Some of the most important requisite theorems are not proved in any text written in English. Our proofs are designed for the first or second year graduate algebra student. We assume some familiarity with semi-simple ring theory and the Wedderburn structures theorems. We also assume some knowledge of finite groups, finite field and Galois theory. We have attempted to develop the factorization of ideals which we require. References are given for any results used from ideal theory.

The outline of our proof follows a 1930 paper by Richard Brauer [5] where many of the results presented here were first proved. The existence of the division algebras is first reduced to a question about norms in a cyclotomic field. Our arguments for this are new and elementary. The norm question is answered using the factorization of ideals in the algebraic integers of this field. This use of ideals closely follows Brauer's paper, which was written just as algebraic number theory was being developed. The groups discussed here were first mentioned in a paper by W. Burnside [9, p. 8].

1. Structure of the Algebras. In this section we construct simple algebras, each of which is generated by a finite group. Let p and q be prime numbers and b a positive integer such that q^b is the highest power of q dividing $p - 1$. Let a be a positive integer and let ε and ω be primitive p^a-th and q^b-th roots of unity respectively. If $n = p^a q^b$, then $\rho = \varepsilon\omega$ is a primitive n-th root of unity. Let $\mathbf{Q}$ denote the rational field, and let $\mathbf{E}$ denote the field $\mathbf{Q}(\rho)$. There is an automorphism σ on the field $\mathbf{E}$ of order q which fixes ω. Let $\mathbf{F}$ be the subfield of $\mathbf{E}$ fixed by σ. For α in $\mathbf{E}$ let $\mathscr{R}(\alpha)$ be the $q \times q$ matrix

$$\mathscr{R}(\alpha) = \begin{bmatrix} \alpha & & & & \\ & \alpha^{\sigma} & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & & \alpha^{\sigma^{q-1}} \end{bmatrix}$$

with all entries off the main diagonal equal to zero. For α in $\mathbf{F}$ the matrix $\mathscr{R}(\alpha)$ is scalar. Also define the $q \times q$ matrix

$$\mathscr{T}(\sigma) = \begin{bmatrix} 0 & . & . & . & 0 & \omega \\ 10 & & & & & \\ 1 & & & & & \\ & \cdot & & & & \\ & & \cdot & & & \\ & & & \cdot & & \\ & & & & 1 & 0 \end{bmatrix}$$

with ones immediately below the main diagonal, ω in the upper right corner and zero's elsewhere. Notice $\mathscr{R}(\omega)$ is a scalar matrix since ω is fixed under σ. Notice also $\mathscr{T}(\sigma)^q = \mathscr{R}(\omega)$. The elements $\mathscr{R}(\varepsilon)$ and $\mathscr{T}(\sigma)$ generate a finite group in which the cyclic group generated by $\mathscr{R}(\varepsilon)$ is normalized by the cyclic group generated by $\mathscr{T}(\sigma)$.

The following relation can be verified for any α in $\mathbf{E}$

$$\mathscr{T}(\sigma)^{-1}\,\mathscr{R}(\alpha)\,\mathscr{T}(\sigma) = \mathscr{R}(\alpha^{\sigma}). \tag{1}$$

The collection Δ of matrices of the form $\sum_{i=1}^{q} \mathscr{R}(\alpha_i)\,\mathscr{T}(\sigma)^i$, $\alpha_i \in \mathbf{E}$ is an algebra. The subsets of matrices $\{\mathscr{R}(\alpha) : \alpha \in \mathbf{E}\}$ and $\{\mathscr{R}(\alpha) : \alpha \in \mathbf{F}\}$ form subfields isomorphic to $\mathbf{E}$ and $\mathbf{F}$ respectively, and we will identify these subsets with the fields $\mathbf{E}$ and $\mathbf{F}$.

We wish to prove that Δ is a simple algebra. Let Δ^* be the set of all complex linear combinations of the matrices in Δ. The algebra of matrices commuting with Δ^* consists only of the scalar matrices, since only a scalar matrix can commute with both $\mathscr{R}(\varepsilon)$ and $\mathscr{T}(\sigma)$.

A special case of Wedderburn's theorem concerns an algebra of complex matrices. It assets that if only a scalar matrix commutes with all matrices in the algebra, then the algebra must be the full matrix algebra. Thus Δ^* is the algebra of $q \times q$ matrices, a simple algebra. If Δ had a non-trivial nilpotent ideal, then the complex linear combinations of elements of this ideal would form a non-trivial nilpotent ideal of Δ^*. This proves that Δ has zero radical and is a semi-simple algebra. The Wedderburn structure theorem asserts that Δ is isomorphic to the ring direct sum of simple algebras. If Δ were not simple one could construct a central idempotent e (an element in the center satisfying $e^2 = e$) by choosing an element which corresponds to the identity in one component and zero in all others. This element would be a central idempotent in Δ^*, different from zero or one, and would generate a proper non-zero ideal of Δ^*. This contradiction to the simplicity of Δ^* establishes that Δ is a simple algebra.

The matrix $\mathscr{T}(\sigma)^i$ for any power $i < q$ has the form

$$\left[\begin{array}{c|c} 0 & \omega I_i \\ \hline I_{q-i} & 0 \end{array}\right]$$

where I_i and I_{q-i} are identity matrices of size i and $q - i$ respectively. This matrix has non-zero entries along two diagonals and all other entries zero. The matrix $\mathscr{R}(\alpha_i)$ for any $\alpha_i \in \mathbf{E}$ has non-zero entries only on the main diagonal, so the product $\mathscr{R}(\alpha_i)\,\mathscr{T}(\sigma)^i$ has non-zero entries only on the same diagonals as $\mathscr{T}(\sigma)^i$. Thus any sum $\sum_{i=l}^{q} \mathscr{R}(\alpha_i)\,\mathscr{T}(\sigma)^i$ can equal zero only if $\mathscr{R}(\alpha_i) = 0$ for each of the field elements $\alpha_1, \ldots, \alpha_n$ in $\mathbf{E}$. This shows that the dimension of Δ over $\mathbf{E}$ is q. We also know the dimension of $\mathbf{E}$ over $\mathbf{F}$ is q so that the dimension of Δ over $\mathbf{F}$ is q^2. We can now see that $\mathbf{F}$ must be the center of Δ. Otherwise Δ would contain a central subfield $\mathbf{L}$ of co-dimension q. Then for any element A not in $\mathbf{L}$, Δ would consist of all polynomials in A with coefficients from $\mathbf{L}$ which is commutative.

Our goal is to show that Δ is a division algebra. Part of Wedderburn's Theorem asserts that for some integer k the simple algebra Δ is isomorphic to the algebra of $k \times k$ matrices over some division algebra with center $\mathbf{F}$. The dimension of Δ over $\mathbf{F}$ would then be $k^2 d$, with d the dimension of this division algebra over $\mathbf{F}$. Since the dimension of Δ over $\mathbf{F}$ is q^2 where q is a prime, either $k = 1$ or $d = 1$ and Δ is either a division algebra or isomorphic to the $q \times q$ matrices with entries from $\mathbf{F}$. We assume the latter possibility holds and shall arrive at a contradiction in section three.

Thus we suppose there is an isomorphism under which $\mathscr{T}(\sigma)$ and $\mathscr{R}(\alpha)$ for every α in $\mathbf{E}$ correspond to $q \times q$ matrices $\mathscr{W}(\sigma)$ and $\mathscr{U}(\alpha)$ respectively, with entries in $\mathbf{F}$. The element $\mathscr{R}(\alpha)$ in Δ has as minimum polynomial over $\mathbf{F}$ the minimum polynomial of α when regarded as an element in the extension field $\mathbf{E}$ over $\mathbf{F}$. Under the above isomorphism, $\mathscr{U}(\alpha)$ has the same minimum polynomial. For α not in $\mathbf{F}$ this minimum polynomial has as roots the distinct conjugates of α under the powers of σ. This polynomial has degree q and must also be the characteristic polynomial of $\mathscr{U}(\alpha)$. For α in $\mathbf{F}$ the matrix $\mathscr{U}(\alpha)$ is scalar.

Let V be the underlying vector space on which the matrices $\mathscr{W}(\sigma)$ and $\mathscr{U}(\alpha)$ for α in $\mathbf{E}$ may be regarded as linear transformations. We suppose that the transformations act from the right. We know from the isomorphism with Δ that $\mathscr{U}(\alpha)\,\mathscr{U}(\beta) = \mathscr{U}(\alpha\beta)$ for every α and β in $\mathbf{E}$. Also the $\mathbf{F}$-linear combinations of the powers of $\mathscr{U}(\varepsilon)$ form the ring $\{\mathscr{U}(\alpha) : \alpha \in \mathbf{E}\}$ which is isomorphic to the field $\mathbf{E}$. Since $\mathscr{U}(\varepsilon)$ has an irreducible minimum polynomial of degree q, V is a cyclic module for this ring of polynomials in $\mathscr{U}(\varepsilon)$ over $\mathbf{F}$.

Thus we can find a vector $v \in V$ so that

$$V = \{v\,\mathscr{U}(\alpha) : \alpha \in \mathbf{E}\}$$

In fact each vector w in V has a unique expression as $w = v\,\mathscr{U}(\alpha)$; for if $v\,\mathscr{U}(\alpha) = v\,\mathscr{U}(\beta)$, then v would be an eigen-vector for $\mathscr{U}(\alpha\beta^{-1})$. Thus one would be a root to the characteristic polynomial of $\mathscr{U}(\alpha\beta^{-1})$ which would imply by our remarks on characteristic polynomials that $\alpha\beta^{-1} = 1$.

Since every vector in V has a unique expression as $v\,\mathscr{U}(\alpha)$ for some α in $\mathbf{E}$ the following equation uniquely defines a linear transformation $\mathscr{S}(\sigma)$ on V:

$$v\mathscr{U}(\alpha)\,\mathscr{S}(\sigma) = v\mathscr{U}(\alpha^{\sigma}).$$

An argument similar to that just given shows $\mathscr{S}(\sigma)$ is one-to-one, hence

invertible. By replacing α by $\alpha^{\sigma^{-1}}$ and multiplying by $\mathscr{S}(\sigma)^{-1}$ one arrives at the formula

$$v\mathscr{U}(\alpha)\,\mathscr{S}(\sigma)^{-1} = v\mathscr{U}(\alpha^{\sigma^{-1}}).$$

Therefore for any α and β in $\mathbf{E}$

$$\begin{aligned} v\mathscr{U}(\alpha)\,\mathscr{S}(\sigma)^{-1}\,\mathscr{U}(\beta)\,\mathscr{S}(\sigma) &= v\mathscr{U}(\alpha^{\sigma^{-1}}\beta)\,\mathscr{S}(\sigma) \\ &= v\mathscr{U}\left((\alpha^{\sigma^{-1}}\beta)^{\sigma}\right) \\ &= v\mathscr{U}(\alpha)\,\mathscr{U}(\beta^{\sigma}) \end{aligned}$$

For fixed β, allowing α to vary gives the following equality of transformations on V

$$\mathscr{S}(\sigma)^{-1}\,\mathscr{U}(\beta)\,\mathscr{S}(\sigma) = \mathscr{U}(\beta^{\sigma}).$$

This identity holds for any β in $\mathbf{E}$. Now from identity (1) and the isomorphism between Δ and the $q \times q$ matrix ring over $\mathbf{F}$ we have for any β in $\mathbf{E}$

$$\mathscr{W}(\sigma)^{-1}\,\mathscr{U}(\beta)\,\mathscr{W}(\sigma) = \mathscr{U}(\beta^{\sigma}). \tag{2}$$

Combining these two equations one sees that $\mathscr{W}(\sigma)^{-1}\,\mathscr{S}(\sigma)$ centralizes $\mathscr{U}(\beta)$ for every β in $\mathbf{E}$.

Thus the matrix in Δ which corresponds under the isomorphism to $\mathscr{W}(\sigma)^{-1}\,\mathscr{S}(\sigma)$ must commute with $\mathscr{R}(\varepsilon)$ and must therefore be diagonal. However since the only diagonal matrices in Δ are actually in $\mathbf{E}$, we see that for some γ in $\mathbf{E}$

$$\mathscr{W}(\sigma)^{-1}\,\mathscr{S}(\sigma) = \mathscr{U}(\gamma)$$

or

$$\mathscr{S}(\sigma) = \mathscr{W}(\sigma)\,\mathscr{U}(\gamma).$$

Since σ is an automorphism of order q, we must have $\mathscr{S}(\sigma)^q = 1$. From identity (2) we have

$$\mathscr{U}(\gamma)\,\mathscr{W}(\sigma) = \mathscr{W}(\sigma)\,\mathscr{U}(\gamma^{\sigma}).$$

Therefore

$$\begin{aligned} \left(\mathscr{W}(\sigma)\,\mathscr{U}(\gamma)\right)^q &= \mathscr{W}(\sigma)\,\mathscr{U}(\gamma)\,\mathscr{W}(\sigma)\,\mathscr{U}(\gamma)\cdots\mathscr{W}(\sigma)\,\mathscr{U}(\gamma) \\ &= \mathscr{W}(\sigma)^2\,\mathscr{U}(\gamma^{\sigma})\,\mathscr{U}(\gamma)\cdots\mathscr{W}(\sigma)\,\mathscr{U}(\gamma) \\ &= \mathscr{W}(\sigma)^q\,\mathscr{U}(\gamma^{\sigma^{q-1}})\,\mathscr{U}(\gamma^{\sigma^{q-2}})\cdots\mathscr{U}(\gamma). \end{aligned}$$

Since $\mathscr{W}(\sigma)^q = \mathscr{U}(\omega)$ and $\mathscr{U}$ is multiplicative on elements of $\mathbf{E}$ we conclude

$$1 = \omega\gamma^{\sigma^{q-1}}\gamma^{\sigma^{q-2}}\cdots\gamma\,. \tag{3}$$

We will use this identity, which asserts that ω is a norm under the automorphism σ, to arrive at a contradiction in section three.

2. Factorization of ideals. Our object in this section is to factor the ideal generated by p in the ring of algebraic integers of $\mathbf{E}$ into prime ideals and to show that each prime ideal factor is invariant under σ. Background material can be found in Chapters 18 and 21 of Curtis and Reiner [11]. Let $\mathbf{Z}$ denote the ring of rational integers. The notation of a ring followed by an element in square brackets denotes the polynomial ring in that element. An important result in algebraic number theory [11, Theorem 21.13, p. 140] asserts that $\mathbf{Z}[\rho]$ and $\mathbf{Z}[\omega]$ are the rings of algebraic integers in the fields $\mathbf{Q}(\rho)$ and $\mathbf{Q}(\omega)$ respectively. The major theorem about the ring of algebraic integers asserts that each ideal can be factored uniquely into a product of prime (or maximal) ideals [11, pages 111, 112].

Let $f(x)$ denote the q^b-th cyclotomic polynomial. We shall use round parentheses to denote "ideal generated by." The homomorphism of $\mathbf{Z}[x]$ onto $\mathbf{Z}[\omega]$ induced by mapping x to ω has kernel $(f(x))$. The ideal $(p, f(x))$ is mapped to the ideal $p\,\mathbf{Z}[\omega]$. We have the isomorphisms

$$\frac{\mathbf{Z}[\omega]}{p\mathbf{Z}[\omega]} \approx \frac{\mathbf{Z}[x]}{(p, f(x))} \approx \frac{\overline{\mathbf{Z}}[x]}{(\bar{f}(x))} \tag{4}$$

where $\overline{\mathbf{Z}}$ denotes the field of integers modulo p and $\bar{f}(x)$ is the reduction of $f(x)$ modulo p. Since p and q^b are relatively prime, $x^{q^b} - 1$ has a non zero derivative in $\overline{\mathbf{Z}}[x]$ and must have distinct roots in any splitting field. Therefore the polynomial $\bar{f}(x)$ must have distinct irreducible factors $\bar{f}_1(x), \ldots, \bar{f}_r(x)$ in $\overline{\mathbf{Z}}[x]$.

According to the Chinese remainder theorem [11, Theorem 18.19, p. 113] the last quotient displayed in (4) is isomorphic to the direct sum taken over $i = 1, \ldots, r$ of the fields $\overline{\mathbf{Z}}[x] / (\bar{f}_i(x))$. If P_i is the maximal ideal of $\mathbf{Z}[\omega]$ corresponding under the isomorphism in (4) to $(\bar{f}_i(x))$ then $p\,\mathbf{Z}[\omega]$ is the intersection of the P_i. In our rings the intersection of ideals equals the product of the ideals [11, 18.16, p. 112]. Therefore

$$p\mathbf{Z}[\omega] = P_1 \ldots P_r \tag{5}$$

where the P_i are distinct maximal ideals of $\mathbf{Z}[\omega]$.

For the n-th root of unity ρ there is an isomorphism similar to (4)

$$\frac{\mathbf{Z}[\rho]}{p\mathbf{Z}[\rho]} \approx \frac{\overline{\mathbf{Z}}[x]}{(\bar{\phi}_n(x))}$$

where $\phi_n(x)$ and $\bar{\phi}_n(x)$ represent the n-th cyclotomic polynomial and its reduction modulo p. Since in a field of characteristic p one is the only p-

power root of unity, the polynomial $\bar{\phi}_n(x)$ has repeated roots; in fact each root is repeated e times where $e = \varphi(p^a) = p^{a-1}(p-1)$. Thus $\bar{\phi}_n(x) = \bar{f}(x)^e$ and

$$\frac{\mathbf{Z}[\rho]}{p\mathbf{Z}[\rho]} \approx \frac{\bar{\mathbf{Z}}[x]}{(\bar{f}(x))^e}.$$

Appealing again to the Chinese remainder theorem we conclude that the quotient above is isomorphic to the direct sum over $i = 1, \cdots, r$ of the rings $\bar{\mathbf{Z}}[x] / (\bar{f}_i(x))^e$. Let Q_i be the (maximal) ideal of $\mathbf{Z}[\rho]$ corresponding to $(\bar{f}_i(x))$. We have

$$p\mathbf{Z}[\rho] = Q_l^e \cdots Q_r^e. \tag{6}$$

From the earlier result (5) we deduce that

$$p\mathbf{Z}[\rho] = P_l\mathbf{Z}[\rho] \cdots P_r\mathbf{Z}[\rho].$$

By comparison with (6) we see that each $P_i\mathbf{Z}[\rho]$ must be a product of the Q_i. We assert that

$$P_i\mathbf{Z}[\rho] = Q_i^e. \tag{7}$$

If this were not so, some Q_j would appear in the factorization of two ideals $P_k\mathbf{Z}[\rho]$ and $P_l\mathbf{Z}[\rho]$. Then Q_j would contain both P_k and P_l and also their sum. Since the sum of two distinct maximal ideals of $\mathbf{Z}[\omega]$ would equal $\mathbf{Z}[\omega]$, Q_j would contain one, an impossibility since the Q_j are proper ideals. Since the left side of (7) is invariant under the automorphism σ, we see that $(Q_i^\sigma)^e = (Q_i^e)^\sigma = Q_i^e$. According to unique factorization, we conclude that

$$Q_i^\sigma = Q_i.$$

3. The existence proof. We have assumed Δ is not a division algebra and our object is to arrive at a contradiction using identity (3). Any element in the field $\mathbf{E}$ can be expressed as a quotient of an algebraic integer by an ordinary integer [11, p. 105]. Express $\gamma = \alpha/a$ with α in $\mathbf{Z}[\rho]$ and a in $\mathbf{Z}$. Then from (3) we have

$$\omega\,\alpha\,\alpha^\sigma \cdots \alpha^{\sigma^{q-1}} = a^q. \tag{8}$$

Suppose p^c is the highest power of p dividing a for some non-negative integer c. Then according to (6) the ideal of $\mathbf{Z}[\rho]$ generated by a^q contains in its factorization the product $Q_l^{ecq} \ldots Q_r^{ecq}$. For a fixed i, the multiplicity with which Q_i appears in the factorization of the ideal generated by α^{σ^j} is the

same for each $j = 1, \cdots, q$. This is because Q_i is fixed under σ as was proved at the end of section two. There are q terms on the left side of (8) so the ideal generated by each α^{σ^j} contains the factor Q_i^{ec}. Since this is true for each $i = 1, \cdots, r$ the ideal generated by α contains as a factor the ideal

$$Q_l^{ec} \cdots Q_r^{ec} = p^c \mathbf{Z}[\rho] .$$

Therefore the ideal generated by p^c contains the ideal generated by α and we can write $\alpha = p^c \alpha'$ for some algebraic integer α. By replacing α with α' and a with $a' = a/p^c$, but keeping the unprimed notation, we have $\gamma = \alpha/a$ where α is an algebraic integer and a an ordinary integer relatively prime to p.

Let $Q = Q_i$ for some i. The quotient ring $\mathbf{Z}[\rho]/Q$ is a finite field of characteristic p. Since 1 is the only p-power root of unity in a field of characteristic p, we have $\varepsilon \equiv 1 \pmod{Q}$. Thus $\rho \equiv \omega\varepsilon \equiv \omega \pmod{Q}$ and every element in the quotient field is represented by a polynomial in ω with integral coefficients. Since q^b divides $p - 1$, the field of p elements contains a primitive q^b-th root of unity. Thus ρ is congruent to an integer modulo Q, and the quotient field is the field of p elements.

Any power of ε is congruent to 1 modulo Q and since ω is fixed by σ,

$$\rho^\sigma \equiv \varepsilon^\sigma \omega \equiv \omega \pmod{Q} .$$

The algebraic integer α can be expressed $\alpha = g(\rho)$ as a polynomial in ρ with rational integral coefficients. Thus we have

$$\alpha^\sigma \equiv g(\rho^\sigma) \equiv g(\omega) \pmod{Q} .$$

Therefore (8) yields

$$\omega g(\omega)^q \equiv a^q \pmod{Q} .$$

Raise both sides to the power $s = p - 1/q$

$$\omega^s g(\omega)^{p-1} \equiv a^{p-1} \pmod{Q} .$$

The maximal ideal Q intersects the ring of integers $\mathbf{Z}$ in a maximal ideal which, since Q contains p, must be $p\mathbf{Z}$. Since a is relatively prime to p we conclude that a is not contained in Q. So $a \not\equiv 0 \pmod{Q}$ and consequently $g(\omega) \not\equiv 0 \pmod{Q}$. By Fermat's little theorem

$$g(\omega)^{p-1} \equiv a^{p-1} \equiv 1 \pmod{Q} .$$

Hence

$$\omega^s \equiv 1 \pmod{Q} .$$

The highest power of q dividing s is q^{b-1}, so ω^s is a primitive q-th root of unity and satisfies the q-th cyclotomic polynomial $\phi_q(x)$. In the reduction modulo Q, the residue class $\omega^s + Q = 1 + Q$ will satisfy the reduced polynomial $\bar{\phi}_q(x)$. Since the roots of $\bar{\phi}_q(x)$ are residue classes represented by $q - 1$ integers, not including 1, we must have

$$1 \equiv j \pmod{Q}$$

for some integer j between 2 and $p - 1$. But then Q would contain $j - 1$ which is impossible since Q intersects the rational integers in the ideal $p\,\mathbf{Z}$. This contradiction establishes that Δ is a division ring.

4. Groups which generate a division algebra. A group $\mathfrak{G}$ is called the *semi-direct product* of a normal subgroup $\mathfrak{H}$ with a subgroup $\mathfrak{K}$ provided $\mathfrak{H}$ and $\mathfrak{K}$ intersect in the identity and $\mathfrak{G} = \mathfrak{H}\mathfrak{K}$. Each of the division algebras determined above is generated over the rational field by a finite group. This group is the semi-direct product of the cyclic normal subgroup generated by $\mathscr{R}(\varepsilon)$ with the cyclic subgroup generated by $\mathscr{T}(\sigma)$. The order of this group is $p^a q^{b+1}$ and the scalar matrix $\mathscr{T}(\sigma)^q = \mathscr{R}(\omega)$ of order q^b generates the center of the group. The group of smallest odd order which generates a division algebra over $\mathbf{Q}$ has order 63 and is generated by the matrices

$$\mathscr{R}(\varepsilon) = \begin{bmatrix} \varepsilon & & \\ & \varepsilon^2 & \\ & & \varepsilon^4 \end{bmatrix}$$

and

$$\mathscr{T}(\sigma) = \begin{bmatrix} 0 & 0 & \omega \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

where $\mathscr{R}(\varepsilon)$ has off diagonal equal to zero and ε and ω are primitive 7-th and 3-rd roots of unity respectively. This group was first mentioned by Burnside [9, p. 4] and Schur [21, p. 179]. Their discussion concerns whether a complex matrix S exists for which the matrices $S^{-1}\mathscr{R}(\varepsilon)S$ and $S^{-1}\mathscr{T}(\sigma)S$ have entries in the subfield $\mathbf{F}$ of index three in the field $\mathbf{E} = \mathbf{Q}(\varepsilon, \omega)$. In fact this question is asked as an exercise on page 319 of Burnside's book *The Theory of Groups of Finite Order!* This question is related to whether the algebra Δ generated by these matrices is a division

algebra. Were such a matrix S to exist, the correspondence of $\mathscr{T}(\sigma)$ with $S^{-1}\mathscr{T}(\sigma)S$ and of $\mathscr{R}(\alpha)$ with $S^{-1}\mathscr{R}(\alpha)S$ for every α in $\mathbf{E}$ would induce an isomorphism between Δ and the 3×3 matrices over $\mathbf{F}$.

The dimension of any finite dimensional division algebra over its center is a perfect square. The square root of this dimension is called the *index* of the algebra. The algebras constructed in section one have index q. By a very similar construction division algebras of certain non-prime indices can be produced. Let p be a prime congruent to 1 modulo 4. Let ε be a primitive p^a-th root of unity for some positive integer a. Let ω be a primitive $(p-1)$-st root of unity. The field $\mathbf{E} = \mathbf{Q}(\varepsilon, \omega)$ has an automorphism of order $p-1$ fixing ω. We define two $(p-1) \times (p-1)$ matrices; $\mathscr{R}(\varepsilon)$ has the conjugates of ε under the powers of σ on the main diagonal and all other entries zero, $\mathscr{T}(\sigma)$ has ones just below the main diagonal, ω in the upper right corner and all other entries zero. The group generated by $\mathscr{R}(\varepsilon)$ and $\mathscr{T}(\sigma)$ has order $p^a(p-1)^2$. Then the $\mathbf{Q}$-linear combinations of this group of matrices is a division algebra of index $p-1$ with center isomorphic to the subfield $\mathbf{F}$ of $\mathbf{E}$ fixed by σ.

The proof that the algebras just constructed are division algebras was given by Amitsur [2, Theorem 5.2 *a*, p. 372]. In that paper Amitsur determined all finite groups $\mathfrak{G}$ which generate some rational division algebra Δ over $\mathbf{Q}$. We shall state part of Amitsur's results; but first some preliminary development. The groups involved have a very special form: the Sylow subgroups are either cyclic or generalized quaternion. This will follow from a well known theorem [18, p. 189] once we have proved the following result. For each prime divisor p of the order of $\mathfrak{G}$, a p-Sylow subgroup $\mathfrak{P}$ has only one subgroup of order p. We now prove this.

Multiplication of the elements of Δ on the right by a particular element G of $\mathfrak{G}$ is a linear transformation on Δ. Choose a basis and denote the corresponding matrix by $\mathbf{X}(G)$. The mapping sending G to $\mathbf{X}(G)$ is a homomorphism of $\mathfrak{G}$. We assert that, unless G is the identity, $\mathbf{X}(G)$ cannot have eigenvalue one. For to have a non-zero eigenvector D in Δ of eigenvalue one means that $DG = D$ or $D(G-1) = 0$, which, in a division algebra, implies $G = 1$.

Any finite p-group has a non trivial center, so we may choose a central element Z of order p in $\mathfrak{P}$. We wish to show that the subgroup generated by Z is the only subgroup of order p in $\mathfrak{P}$. Suppose that P also generates a subgroup of order p. Since $\mathbf{X}(Z)$ and $\mathbf{X}(P)$ commute, they can be simultaneously diagonalized. Thus for some complex matrix S, the matrices $S^{-1}\mathbf{X}(Z)S$ and $S^{-1}\mathbf{X}(P)S$ are diagonal. Let ξ_1 and ξ_2 be, respectively,

the first entries in the two diagonal matrices. Since all characteristic roots of $\mathbf{X}(Z)$ and $\mathbf{X}(P)$ are primitive p-th roots of unity, there is an integer i with $\xi_2 = \xi_1{}^1$. The matrix $S^{-1}\mathbf{X}(Z^{-i}P)S$ thus has first entry one and $\mathbf{X}(Z^{-i}P)$ has eigenvalue one. Therefore $Z^{-i}P = 1$ and so $P = Z^i$ generates the same group as Z. This completes the proof that $\mathfrak{P}$ has just one subgroup of order p and is either cyclic or generalized quaternion.

We assume until further notice that $\mathfrak{G}$ has odd order. Thus $\mathfrak{G}$ has no generalized quaternion Sylow subgroups and so all Sylow subgroups of $\mathfrak{G}$ are cyclic. In [18, Theorem 9.4.3, p. 146] such a group is shown to have the following form: $\mathfrak{G}$ is the semi-direct product of a cyclic normal subgroup $\mathfrak{H}$ of order h with a cyclic group $\mathfrak{K}$ of order k, for relatively prime integers h and k. (The assertion that these subgroups have relatively prime order is not stated in the theorem cited above but it is proved at the end of the second last paragraph of the proof.)

For a prime divisor p of h, the p-Sylow subgroup $\mathfrak{P}$ of $\mathfrak{G}$ is a normal subgroup. A necessary condition that $\mathfrak{G}$ generate a division algebra is that $\mathfrak{G}$ be the direct product of subgroups, one for each prime divisor p of h. Specifically, for each prime q dividing k, a q-Sylow subgroup of $\mathfrak{K}$ which does not centralize $\mathfrak{P}$ must centralize all other Sylow subgroups. Let $\mathfrak{D}$ be the product of all the Sylow subgroups of $\mathfrak{K}$ which do not centralize $\mathfrak{P}$. The semi-direct product $\mathfrak{P}\,\mathfrak{D}$ must then be a direct factor of $\mathfrak{G}$.

Assume $\mathfrak{G}$ has the structure of a direct product as described in the previous paragraph. Let the centralizer of $\mathfrak{P}$ in $\mathfrak{D}$ have index x in $\mathfrak{D}$ and order y. The number x divides $p-1$. Let q be a prime divisor of x and suppose q^t is the highest power of q dividing $p-1$. A necessary condition is that q^t divide y. Suppose q^{t+u} is the highest power of q dividing y. Let f be a prime divisor of the order of $\mathfrak{G}$ and l the smallest integer satisfying the equation

$$p^l \equiv 1 \pmod{f}.$$

A necessary and sufficient condition that $\mathfrak{G}$ generate a division algebra over $\mathbf{Q}$ is that for each prime f dividing the order of $\mathfrak{G}$, other than p or q, q^{u+1} must not divide the order l of p modulo f. This condition must hold for every pair of primes p and q for which p divides h and a q-Sylow subgroup of $\mathfrak{K}$ does not centralize the p-Sylow subgroup of $\mathfrak{G}$.

The paper of Amitsur gives necessary and sufficient conditions for any finite group, of odd or even order to generate a division algebra. We have restricted attention to groups of odd order because the statement for

groups of even order is still more complicated! The proofs given by Amitsur are quite difficult and rely on some very advanced algebraic number theory. The construction of the division algebra for a group $\mathfrak{G}$ described in the previous paragraph follows the procedure used in section one. Before describing the construction we need one preliminary result.

We must show that the center of $\mathfrak{G}$ is a subgroup of $\mathfrak{K}$. Every subgroup of $\mathfrak{G}$ is the semi-direct product of a subgroup of $\mathfrak{H}$ with a subgroup of $\mathfrak{K}$. Thus it is sufficient to show that only the identity subgroup of $\mathfrak{H}$ is central. From the third paragraph of the proof cited above [18, p. 147] we see that $\mathfrak{H}$, generated by the element A, is the commutator subgroup of $\mathfrak{G}$. The element B generates $\mathfrak{K}$, and $A^{-1} B^{-1} AB = A^{r-1}$ generates the commutator subgroup of $\mathfrak{G}$. Therefore A^{r-1} generates $\mathfrak{H}$. The equation $B^{-1} AB = A^r$ can be raised to the power j to yield $B^{-1} A^j B = A^{rj}$ or $A^{-j} B^{-1} A^j B = A^{j(r-1)}$. If A^j is central the left side of this last equation equals one. Since A^{r-1} and A have the same order we conclude that $A^j = 1$. Thus the center of $\mathfrak{G}$ is a subgroup of $\mathfrak{K}$. Let z be the order of the center. Notice that z, a divisor of k, is relatively prime to h.

To construct the algebra, choose ε and ω primitive h-th and z-th roots of unity respectively. The field $\mathbf{Q}(\varepsilon)$ has an automorphism sending ε to ε^r which corresponds to the action of $\mathfrak{K}$ on $\mathfrak{H}$. Extend this to the automorphism σ on the field $\mathbf{E} = \mathbf{Q}(\varepsilon, \omega)$. Let $\mathbf{F}$ be the subfield of $\mathbf{E}$ fixed by σ. Then the matrices $\mathscr{R}(\varepsilon)$ and $\mathscr{T}(\sigma)$ defined as in section one generate the division algebra over $\mathbf{Q}$.

There are an infinite number of finite groups which generate the real quaternion algebra. Those with order divisible by eight have a generalized quaternion Sylow subgroup and cannot be expressed as a semi-direct product. All the groups have a center of order two and the quotients modulo these centers include the family of dihedral groups of order $2m$ for every integer $m > 2$. There are exactly three other groups. Their quotients are the rotation groups of the regular tetrahedron, octahedron and icosahedron [2, Theorem 11, p. 385].

5. Division algebras in the group algebra. The group algebra of a finite group over a field of characteristic zero decomposes as the direct sum of simple algebras. Each simple component is a full matrix algebra with entries in some division algebra. We shall call such division algebras coefficient algebras for the group. A very striking theorem, conjectured by the author, was proved by M. Benard and M. Schacher in [4]. It concerns the center $\mathbf{F}$ of a coefficient algebra Δ of index m. The theorem states that $\mathbf{F}$ must contain

a primitive m-th root of unity ζ. Using this result the author [17] has given generators A and B for Δ over $\mathbf{F}$ satisfying the relations

$$\begin{aligned} &1) \quad A^{-1} B^{-1} AB = \zeta \\ &2) \quad A^m \in \mathbf{F} \\ &3) \quad B^m \in \mathbf{F} \end{aligned}$$

For the algebras described in section one, A corresponds to

$$\sum_{j=0}^{q} \mathscr{R}(\zeta^{-j} \varepsilon^{\sigma^j})$$

where $\zeta = \omega^{q^{b-1}}$ is a primitive q-th root of unity. The element B corresponds to $\mathscr{T}(\sigma)$.

In an early paper [8], Brauer and E. Noether proved some major theorems concerning coefficient algebras. Here is a description of their main results. We know that a simple component Γ of the rational group algebra of a finite group is isomorphic to the $k \times k$ matrices over a coefficient algebra Δ, for some integer k. Suppose $\mathbf{F}$ is the center of Δ. Let $d = m\,k$ where m is the index of Δ. Then there exists a finite dimensional extension field $\mathbf{E}$ of $\mathbf{F}$ so that Γ is isomorphic to the $\mathbf{F}$-linear combinations of a finite group of $d \times d$ matrices whose entries belong to $\mathbf{E}$. Furthermore a field $\mathbf{E}$ has this property if and only if $\mathbf{E}$ is isomorphic to a subfield of Δ and has dimension m over $\mathbf{F}$.

This allows us to state a criterion that a group generates a division algebra. Let ε and ω be any roots of unity of relatively prime order and $\mathbf{E} = \mathbf{Q}(\varepsilon, \omega)$. Let σ be an automorphism of $\mathbf{E}$ of order d fixing a subfield $\mathbf{F}$ which contains ω. The $d \times d$ matrices $\mathscr{R}(\varepsilon)$ and $\mathscr{T}(\sigma)$ defined as in section one generate a finite group. The algebra generated over $\mathbf{Q}$ by this group is a division algebra if and only if there exists no matrix S for which the matrices $S^{-1} \mathscr{R}(\varepsilon) S$ and $S^{-1} \mathscr{T}(\sigma) S$ have entries in a field extension of $\mathbf{F}$ of dimension smaller than d.

An important unsolved problem is to characterize the coefficient division algebras in some manner. The most significant general result, proved independently by Brauer [6] and Witt [23], relates the coefficient algebras for a group $\mathfrak{G}$ to coefficient algebras for certain special types of subgroups. To state their conclusion, suppose m is the index of some coefficient division algebra for $\mathfrak{G}$. Let p be a prime divisor of m and p^a the highest power of p dividing m. Then there is a subgroup $\mathfrak{E}$ of $\mathfrak{G}$ which has a coefficient algebra of index p^a. This subgroup $\mathfrak{E}$ is the semi-direct product of a cyclic group $\mathfrak{A}$ of order prime to p with a p-group $\mathfrak{B}$ which normalizes $\mathfrak{A}$. Furthermore there

is a close relationship between the two coefficient algebras. A new proof of this result was given by Solomon [22, Theorem 3]. This proof can be found in [11, p. 475-479).

The theorem was further refined by Brauer [7] and Witt [23]. They showed that for some quotient group $\mathfrak{C}$ of $\mathfrak{B}$, the quotient $\mathfrak{F} = \mathfrak{A}\,\mathfrak{C}$ of $\mathfrak{E}$ has a coefficient algebra of index p^a. The group $\mathfrak{C}$ contains a cyclic normal subgroup $\mathfrak{Z}$ for which $\mathfrak{C}/\mathfrak{Z}$ is Abelian. A proof of this is given in [16, Lemma 1]. Yamada [24], [25] and [26] has investigated coefficient division algebras for certain special types of the groups just described.

The index m of a coefficient algebra must divide the order g of the group. Another bound on the index states that for a prime divisor p of m, the highest power of p dividing m must also divide $q - 1$ for some prime divisor q of g. An exception to this can occur if g is a power of two; we may have $m = 2$ in this case. This theorem is implicit in the work of Witt [23, Satz 12, p. 245] and was stated and proved independently by the author in [16].

Suppose a field **F** is given and the question is asked: which division algebras with center **F** appear as the coefficient algebras in some group algebra. This question has been answered for different fields by several authors in [3], [4], [13], [14], [15], [19] and [27]. Closely related problems have been investigated in [12].

REFERENCES

[1] A. A. Albert. *Structure of Algebras*, Amer. Math. Soc. Colloq. Publ. Vol. 24, Providence R.I., 1939.

[2] S. A. Amitsur. Finite subgroups of division rings, *Tran. Amer. Math. Soc.*, *18* (1955), pp. 361-386.

[3] M. Benard. Quaternion constituents of group algebras, *Proc. Amer. Math. Soc.*, *30* (1971), pp. 217-219.

[4] —— and M. Schacher. The Schur subgroup II, *J. of Alg.*, *22* (1972), pp. 378-385.

[5] Richard Brauer. Unterschungen über die arithmetischen Eigenschaften von Gruppen linearer Substitutionen, *Math. Zeit.*, *31* (1930), pp. 733-747.

[6] —— On the algebraic structure of group rings, *J. Math. Soc. Japan*, *3* (1951), pp. 237-251.

[7] —— On the representations of groups of finite order, *Proc. Internat. Cong. Math., Cambridge*, 1950, Vol. 2 pp. 33-36.

[8] —— and E. Noether. Über minimale Zerfällungskörper irreducibler Darstellungen, *Sitz. Preuss. Akad.*, *32* (1927), pp. 221-226.

[9] W. Burnside. On the arithmetical nature of the coefficients in a group of linear substitutions of finite order II, *Proc. Lond. Math. Soc.*, *4* (1906), pp. 1-9.

[10] —— *The Theory of Groups of Finite Order*, 1911, Dover Publ. Inc., New York.

[11] C. Curtis and I. Reiner. *The Representation Theory of Finite Groups and Associative Algebras*, Interscience, New York, 1962.

[12] B. Fein and M. Schacher. Embedding finite groups in rational division algebras I, *J. Alg.*, *17* (1971), pp. 412-428.
[13] K. Fields. On the Brauer-Speiser theorem, *Bull. Amer. Math. Soc.*, *77* (1971), p. 223.
[14] —— On the Schur subgroup, *Bull. Amer. Math. Soc.*, *77* (1971), pp. 477-478.
[15] —— and I. Herstein, On the Schur subgroup of the Brauer group, *J. Alg.*, *20* (1972), pp. 70-71.
[16] C. Ford. Some results on the Schur index of a representation of a finite group, *Can. J. Math.*, *22* (1970), pp. 626-640.
[17] —— Pure normal maximal subfields for division algebras in the Schur subgroup, *Bull. Amer. Math. Soc.*, *78* (1972), pp. 810-812.
[18] M. Hall. *The Theory of Groups*, Macmillan, New York, 1959.
[19] M. Schacher. More on the Schur subgroup, *Proc. Amer. Math. Soc.*, *31* (1972), pp. 15-17.
[21] I. Schur. Arithmetische Untersuchungen über gruppen endlicher Ordnung, *Sitz. Preuss. Akad.*, (1906), pp. 164-184.
[22] L. Solomon. The representation of finite groups in algebraic number fields, *J. Math. Soc. Japan*, *13* (1961), pp. 144-164.
[23] E. Witt. Die algebraische Struktur des Gruppenringes einer endlichen Gruppe über einem Zahlkörper, *J. Reine. Angew. Math.*, *190* (1952), pp. 231-245.
[24] T. Yamada. The group algebras of metacyclic groups over algebraic number fields, *J. Fac. Univ. Tokyo*, *15* (1968), pp. 179-199.
[25] —— On the group algebras of metabelian groups over algebraic number fields I, *Osaka J. Math.*, *6* (1969), pp. 211-228.
[26] —— On the group algebras of metabelian groups over algebraic number fields II, *J. Fac. Univ. Tokyo*, *16* (1969), pp. 83-90.
[27] —— Characterizations of the simple components of the group algebras over the p-adic number field, *J. Math. Soc. Japan*, *23* (1971), pp. 295-310.

(Reçu le 30 avril 1973)

Charles Ford
Department of Mathematics
Washington University
St. Louis, Missouri 63130

vide-leer-empty