FINITE SUBGROUPS OF DIVISION RINGS

BY

S. A. AMITSUR

1. **Introduction.** The problem of determining all finite groups which can be embedded in the multiplicative group of the nonzero elements of division rings was first proposed and partially solved in [6] by I. N. Herstein. It was shown there that the only finite subgroup of division rings of finite characteristic are cyclic, and that the subgroups of odd order of division rings of characteristic zero are of a very special type [6, Theorem 5]. In particular, the odd subgroups of the real quaternions are all cyclic. This brought I. N. Herstein to the conjecture that all odd subgroups of division rings are cyclic.

The purpose of the present paper is to determine completely all subgroups (of even and odd order) of division rings. These groups are classified in five classes connected in some way to the finite groups of rotations of the 3-Euclidean sphere. Among others we disprove the conjecture of Herstein and exhibit infinitely many finite subgroups of division rings of odd order. In particular the minimal order of an odd noncyclic group contained in a division ring is 63.

We say that a group G is *without fixed points* if G has a representation $g \to \Gamma_g$ by matrices with the property that 1 is a characteristic root of the matrix Γ_g if and only if g is the identity of G. These groups have been first studied by W. Burnside [4] and later by Vincent [9] and were almost completely determined by Zassenhaus in [8](1). Establishing the fact that the subgroups of division rings are without fixed points, most of the results of [6] are an immediate consequence of [4]. In the present paper, we utilize the classification of the groups without fixed points as developed by Zassenhaus in [8] to determine the minimal algebras containing the respective types of the groups. Thus we are able to reduce our problem to determining conditions of the existence of certain division algebras. The latter is then completely solved by methods of class field theory.

2. **A general result.** Let $\mathfrak{R}^*$ denote the multiplicative group of the nonzero elements of a division ring $\mathfrak{R}$ of characteristic zero. Let Q be the rational field assumed to belong to the center of $\mathfrak{R}$.

Let G be a finite subgroup of $\mathfrak{R}^*$. Put:

$$\mathcal{U} = \mathcal{U}(G) = \left\{ \sum \alpha_i A_i \,\middle|\, \alpha_i \in Q,\ A_i \in G \right\},$$

and denote by $\mathcal{Z}$ the center of $\mathcal{U}$. Clearly, $\mathcal{U}$ is a finite central division algebra

Received by the editors June 15, 1954.

(1) The results of this paper will be quoted here by Z followed by the number of the theorem quoted.

of order u^2 over $\mathfrak{Z}$. Our main purpose is to determine the structure of $\mathcal{U}$ over $\mathfrak{Z}$.

THEOREM 1. *If $G \subseteq \mathfrak{R}^*$, then G is group without fixed points*(2).

Indeed, $\mathcal{U}$ is a finite space over $\mathfrak{Z}$. The mapping $g \to \Gamma_g$, where Γ_g is the linear transformation of $\mathcal{U}$ defined by $\Gamma_g u = gu$, $u \in \mathcal{U}$, is a representation of G, without fixed points. If Γ_g has 1 as characteristic value, then $(\Gamma_g - 1)u = 0$ for some $u \neq 0$ of $\mathcal{U}$. This means that $(g-1)u = 0$. Since $\mathfrak{R}$ is without zero divisors it follows that $g = 1$. q.e.d.

It follows now by [4] (see also [9, p. 123]) that:

THEOREM 2. *If $G \subseteq \mathfrak{R}^*$, then G is one of the following types*:

(2A) *All Sylow subgroups of G are cyclic.*

(2B) *The odd Sylow subgroups of G are cyclic and the even Sylow subgroup of G is a generalized quaternion group of order $2^{\alpha+1}$, $\alpha \geqq 2$.*

The generalized quaternion group of order $2^{\alpha+1}$ is a group generated by two elements P, Q satisfying $P^{2^{\alpha-1}} = Q^2$, $Q^4 = 1$, $QPQ^{-1} = P^{-1}$. The case $\alpha = 2$ is the known quaternion group of order 8. Note that, in the general case, $\{P^{2^{\alpha-2}}, Q\}$ is a quaternion group.

3. $G_{m,r}$ **groups.** Let m, r be two relatively prime integers. Put:

(3A) $s = (r-1, m)$, $t = m/s$; $n =$ the minimal integer satisfying $r^n \equiv 1 \pmod{m}$.

Denote by $G_{m,r}$, a group generated by two elements A, B satisfying the relations

(3B) $A^m = 1$; $B^n = A^t$; $BAB^{-1} = A^r$(3).

REMARK 3.1. The order of the group $G_{m,r}$ is $g = mn$ and, clearly, the commutator $G'_{m,r} = \{A^s\}$ and its center is $\{A^t\}$.

Theorem Z5(1) is restated here in the form:

LEMMA 1. *A group G is of type* (2A) *if and only if $G \cong G_{m,r}$ where the numbers n, t, s satisfy*:

(3C) $(n, t) = 1$; *and then* $(s, t) = 1$.

Theorem Z5 states only that $(n, t) = 1$, but following the proof of that theorem, we show that $(n, t) = 1$ implies $(s, t) = 1$. Indeed, if $p \mid (s, t)$, let p^α be the highest power of p dividing s. Since $p \mid t$ it follows by (3A) that $p^\alpha \mid r-1$, and $p^{\alpha+1} \nmid r-1$. Now $(n, t) = 1$ implies that $p \nmid n$. Consequently, $r^n - 1$ is divisible by p^α but not by $p^{\alpha+1}$. On the other hand $p^{\alpha+1} \mid s \cdot t = m$ and by (3A) $m \mid r^n - 1$. Contradiction.

We remark that t is necessarily an odd number. For, if $t \equiv 0(2)$, then m is even and, therefore, $r \equiv 1(2)$. Thus, by (3A), $s \equiv 0(2)$ which contradicts $(s, t) = 1$.

(2) The definition of groups without fixed points, given in the introduction, has a geometric background. See e.g. [9, p. 117].

(3) For $r = 1$, we put $n = s = 1$ and thus $G_{m,1}$ is a cyclic group of order m.

LEMMA 2. *A group $G_{m,r}$ is of type* (2B) *if and only if the numbers of* (3A) *satisfy*:

(3D) $n=2n'$, $m=2^{\alpha}m'$, $s=2s'$, *where* $\alpha\geqq 2$, m', s', n' *are odd numbers*; $(n, t)=(s, t)=2$, *and* $r\equiv -1(2^{\alpha})$.

Clearly, if G is of type (2B) and $2^{\alpha+1}$ the highest power of 2 dividing $g=mn$, then $\alpha+1\geqq 3$. Hence $\alpha\geqq 2$. Following the proof of Z5, one shows that if $p\mid(n, t)$ then $\{B^{n/p}, A^{t/p}\}$ generates an abelian group of type (p, p) modulo $\{A^{t}\}$. Since $G_{m,r}$ is assumed to be of type (2B), this is possible only if $p=2$. If it were $(n, t)=1$, then by the preceding lemma $G_{m,r}$ is of type (2A) which is impossible. Thus $2^{\beta}=(n, t)$. The only abelian subgroups of $G_{m,r}/\{A^{t}\}$ of order a power of 2 can be either cyclic or of the type (2, 2), hence one readily verifies as before that $4\nmid(n, t)$. Consequently, $2=(n, t)$.

It follows, by Remark 3.1, that $G'_{m,r}=\{A^{s}\}$ is of order t. On the other hand since $G'_{m,r}\supseteq\{P\}^{2}$[4], it follows that $2^{\alpha-1}\mid t$. r is odd since $m=st$ is even. Thus (3A) implies that $s\equiv 0(2)$. n is also even and the highest power of 2 dividing $g=mn=nst$ is $2^{\alpha+1}$. It follows therefore that $n=2n'$, $s=2s'$, $t=2^{\alpha-1}t'$ and hence $m=2^{\alpha}m'$, where n', s', t', m' are odd numbers. In particular, this shows that $2\mid(s, t)$. Following the preceding proof one shows that (s, t) has no odd prime factors. Thus, we conclude that $(s, t)=2$. The elements $B^{ns/4}$, $A^{m2^{-\alpha}}$ clearly generate a 2-Sylow subgroup of $G_{m,r}$, hence $B^{ns/4}A^{m2^{-\alpha}}\cdot B^{-ns/4}=A^{-m2^{-\alpha}}$. This implies that $m2^{-\alpha}(r^{ns/4}+1)\equiv 0(m)$, i.e. $r^{ns/4}\equiv -1(2^{\alpha})$. Since $ns/4$ is odd, $r\equiv -1(2^{\alpha})$.

Conversely, let (3D) hold. Since $g=nm$, it follows as in the proof of Z5 that for primes $p\neq 2$ either $p^{\beta}\mid ns$ or $p^{\beta}\mid t$, where p^{β} is the highest power of p dividing g. In the first case, the cyclic subgroup $\{B\}$ of $G_{m,r}$, which is of order ns, contains a cyclic p-Sylow subgroup; and in the second case, $\{A\}$ contains a cyclic p-Sylow subgroup of $G_{m,r}$. For $p=2$, since $r\equiv -1(2^{\alpha})$ one readily shows that $\{B^{ns/4}, A^{m2^{-\alpha}}\}$ is a generalized quaternion subgroup of order $2^{\alpha+1}$ of $G_{m,r}$. This completes the proof of the lemma.

LEMMA 3. *A necessary and sufficient condition that a group G of type* (2A) *or* (2B) *have generators satisfying* (3B) (*i.e.*, $\cong G_{m,r}$) *is that G contains a normal cyclic subgroup N such that G/N is cyclic.*

If G has generators satisfying (3B) then clearly $N=\{A\}$ satisfies the condition of the theorem.

To prove the converse, let N be a maximal normal cyclic subgroup of G such that G/N is cyclic. Let $N=\{A\}$ and let $G/N=\{BN\}$ be of order n. Since N is normal, $A^{m}=1$, $BAB^{-1}=A^{r}$ and $B^{n}=A^{t}$, for some integers m, n, r, t. n is the minimal integer satisfying $r^{n}\equiv 1(m)$. For, if $r^{\nu}\equiv 1(m)$ and $\nu<n$ then $\{B^{\nu}, A\}=N'$ will form an abelian group and, clearly, a normal subgroup of G. Since N' is also of type (2A) or (2B) and abelian, all its Sylow subgroups are cyclic, hence it follows that N' is cyclic. This contradicts the maximality

[4] In the notations of the definition following Theorem 2.

of N. We may assume that $t \mid m$, since by taking A^α instead of A, where $\alpha t+\beta m=(m, t)$, one obtains another generator of N satisfying the preceding relation with $t=(m, t) \mid m$. (Note, that r remains the same.) To complete the proof of (3A) it remains to show that $st=m$. Indeed $A^t=BA^tB^{-1}=A^{rt}$; hence $t(r-1) \equiv O(m)$ which implies that $m/s=t' \mid t$. On the other hand $BA^{t'}B^{-1}=A^{rt'}=A^{t'} \cdot A^{(r-1)t'}$. So that $A^{t'}$ belongs to the center of G. One readily verifies that $\{A^t\}$ is the center of G, hence $t \mid t'$. Thus $t=t'$. q.e.d.

NOTATIONS. (1) ϵ_m will denote a fixed primitive mth root of unity.

(2) $\mathcal{C}_m$ will denote the cyclotomic field $Q(\epsilon_m)$.

(3) $\sigma=\sigma_r$ will stand for the automorphism of $Q(\epsilon_m)$ determined by the mapping $\epsilon_m \to \epsilon_m^r$.

(4) $\mathcal{Z}=\mathcal{Z}_{m,r}$ will denote the invariant subfield of σ of C_m.

(5) To comply with accepted notation we write $\epsilon_4=i=(-1)^{1/2}$ and for this case $\sigma_{-1}=\sigma_3=j$ is the conjugation in C_m. We shall use the letter j to denote σ_{-1} the conjugation in the general case. In this case $\mathcal{Z}_{m,-1}=\mathcal{R}_m$ is the real subfield of $\mathcal{C}_m$.

(6) Following the notations of [1, Theorem 9, p. 74], $(\mathcal{C}_m, \sigma_r, \epsilon_s)=\mathfrak{A}_{m,r}$ will denote the cyclic algebra determined by the field $\mathcal{C}_m$, the automorphism σ_r and the elements ϵ_s. This algebra is well defined if $\epsilon_s \in \mathcal{Z}_m$ which holds if $s \mid m$ and $s \mid r-1$. In particular, this is valid if s is defined by (3A).

We recall that if n is given by (3A) then $\mathfrak{A}_{m,r}$ is a central simple algebra of order n^2 over $\mathcal{Z}_{m,r}$ and its elements can be uniquely written in the form $\sum_{\nu=0}^{n-1} a_\nu \sigma^\nu$, $a_\nu \in \mathcal{C}_m$, $\sigma=\sigma_r$; and $a\sigma=\sigma a^\sigma$ holds in $\mathfrak{A}_{m,r}$ for every $a \in \mathcal{C}_m$.

LEMMA 4. *If $G_{m,r} \subseteq \mathfrak{R}^*$, then $\mathcal{U}_{m,r}=\mathcal{U}(G_{m,r}) \cong \mathfrak{A}_{m,r}$ and the isomorphism is obtained by the correspondence: $A \leftrightarrow \epsilon_m$, $B \leftrightarrow \sigma$.*

Clearly, the mapping $A \leftrightarrow \epsilon_m$ induces an isomorphism: $f(A) \leftrightarrow f(\epsilon_m)$ between the subfield $Q(A)$ of $\mathfrak{R}^*$ and $\mathcal{C}_m=Q(\epsilon_m)$. One readily observes that the elements of $\mathcal{U}_{m,r}$ are of the form $\sum_{\nu=0}^{n-1} f_\nu(A)B^\nu$, $f_\nu(A) \in Q(A)$. Hence, in view of (3B), the mapping $\sum_{\nu=0}^{n-1} f_\nu(\epsilon_m)\sigma^\nu \to \sum_{\nu=0}^{n-1} f_\nu(A)B^\nu$ determines a homomorphism of $\mathfrak{A}_{m,r}$ onto $\mathcal{U}_{m,r}$. Since $\mathfrak{A}_{m,r}$ is simple and $\mathcal{U}_{m,r} \neq 0$, this homomorphism is actually an isomorphism.

Note that $\mathfrak{A}_{m,r}$ is not uniquely determined, since there is a choice in choosing the primitive roots ϵ_m and ϵ_s. In fact, only ϵ_s affects the construction of $\mathfrak{A}_{m,r}$ and ϵ_m does not play any role in the construction of $\mathfrak{A}_{m,r}$, since only $Q(\epsilon_m)$ is considered. Nevertheless, all these algebras will be isomorphic, but the isomorphisms involved are not over the center as usually dealt with in the theory of central division algebras.

If the converse holds, namely: if $\mathfrak{A}_{m,r}$ is a division algebra, then clearly $\{\epsilon_m, \sigma\}$ generate a $G_{m,r}$ group. Thus:

THEOREM 3. *A group $G_{m,r}$ can be embedded in a division ring, if and only if $\mathfrak{A}_{m,r}$ is a division algebra; and then $\mathcal{U}(G_{m,r}) \cong \mathfrak{A}_{m,r}$.*

REMARK. In the proof of this theorem and of the preceding lemma we

have used only the definition of n and s in (3A) and no use was made of the requirements (3C) and (3D). It follows, therefore, by Theorem 2 that a necessary condition that $\mathfrak{A}_{m,r}$ is a division algebra is that the numbers m, r which yield the numbers n, s and t by (3A) will satisfy (3C) or (3D).

4. **The algebra $\mathfrak{A}_{m,r}$.** The object of this section is to determine the conditions imposed on the numbers m, r so that $\mathfrak{A}_{m,r}$ be a division algebra.

To this we retain the notations of the preceding section and assume that m, r, n, t, s are integers satisfying (3A) and either (3C) or (3D).

LEMMA 5. *If* $\mathfrak{A}_{m,r}=(Q(\epsilon_m), \sigma, \epsilon_s)$ *is a division algebra, then* $n \mid s$.

Proof. It follows by [1, Theorem VI 12, p. 75] that $A^s_{m,r} \cong (Q(\epsilon_m), \sigma, \epsilon_s^s) = (Q(\epsilon_m), \sigma, 1)$. The latter is known to be a matrix ring. On the other hand, since $\mathfrak{A}_{m,r}$ is a division algebra over an algebraic field of index n it follows by the Hasse-Brauer-Noether theorem (e.g. [2, Satz 7, p. 119]) that its exponent is also n. Hence $n \mid s$.

We introduce some additional notations:

$\mathcal{J}=\mathcal{J}_q$, for primes $q \mid n$ will denote the cyclic extension $\mathcal{Z}_{m,r} \subseteq \mathcal{J}_q \subseteq \mathcal{C}_m$ of degree q over $\mathcal{Z}_{m,r}$.

$G(\mathcal{K}/\mathcal{Z})$, the Galois group of a normal extension $\mathcal{K}$ over $\mathcal{Z}$.

Q_p, the p-adic extension of the rational Q.

$\mathcal{K}_1/\mathcal{K}_2$ will be used as a short notation to mean $\mathcal{K}_1$ is an extension of $\mathcal{K}_2$, or "$\mathcal{K}_1$ over $\mathcal{K}_2$," or similar phrases.

$\overline{\mathcal{K}}$, the residue field of a field $\mathcal{K} \supseteq Q_p$, and $a \to \bar{a}$ will denote the residue (p-adic) map of $\mathcal{K}$ onto $\overline{\mathcal{K}}$.

Let p be a fixed prime dividing m. We put:

$\alpha=\alpha_p$, where p^α is the highest power of p dividing m.

n_p, the minimal integer satisfying $r^{n_p} \equiv 1 (mp^{-\alpha})$.

ν_p, the minimal integer satisfying $r^{\nu_p} \equiv 1 (p^\alpha)$.

$\mu=\mu_p$, the minimal integer satisfying $r^{\mu_p} \equiv p^{\mu'} (mp^{-\alpha})$ for some integer μ'.

$\delta=\delta_p$, the minimal integer satisfying $p^{\delta_p} \equiv 1 (mp^{-\alpha})$.

Generally:

$\gamma(m_1, m_2)$ denotes the minimal integer satisfying $m_1^{\gamma(m_1,m_2)} \equiv 1 (m_2)$.

$\beta(m_1, m_2)$ denotes the highest power $m_1^{\beta(m_1,m)}$ dividing m_2.

Before proceeding with the problem we need two lemmas in number theory.

LEMMA 6. *Let q be a prime dividing n, then there exists at most one prime $p \mid m$ for which $q \nmid n_p$; and if*: (1) $p \neq 2$, *then $p \nmid s$ and $q \mid p-1$*; (2) $p=2$, *then $q=p=2$ and* (3D) *holds. Furthermore, if for $q=2$ such a p exists then* (3C) *implies that* (1) *holds and* (3D) *implies that $p=2$ (i.e.,* (2) *is valid).*

Let $m=p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where p_i are the different prime factors of m. Let $\nu_i=\nu_{p_i}$ and $n_i=n_{p_i}$, that is: ν_i is the minimal integer satisfying $r^{\nu_i} \equiv 1 \pmod{p_i^{\alpha_i}}$ and n_i is the minimal integer for which $r^{n_i}=1 \pmod{mp_i^{-\alpha_i}}$. One readily observes that $n_i=[\nu_1, \cdots, \hat{\nu}_i, \cdots, \nu_k]$ is the least common multiple of

$\nu_1, \cdots, \nu_{i-1}, \nu_{i+1}, \cdots, \nu_k$ and that $n=[n_i, \nu_i]$. Hence, if $q \mid n$ and $q \nmid n_i$ it follows that $q \nmid \nu_j$ for $j \neq i$ and $q \mid \nu_i$. Clearly, the last relation implies that $q \mid n_j$ for $j \neq i$ since $\nu_i \mid n_j$ for these j. This proves that there is at most one prime p for which $q \nmid n_p$.

Note that if $p_i \mid s$ and: (1) $p_i \neq 2$ or $p_i=2$ but (3C) holds then $\nu_i=1$, but if (2) $p_i=2$ and (3D) holds then $\nu_i=2$. Indeed, one observes that under condition (1) it follows that if $p_i^{\alpha_i} \mid m$ then $p_i^{\alpha_i} \mid s$. Hence, $r \equiv 1 \pmod{s}$ implies that $r \equiv 1 \pmod{p_i^{\alpha_i}}$, i.e., $\nu_i=1$. In case of (2), (3D) states that $r \equiv -1 \pmod{2_i^{\alpha_i}}$ and $\alpha_i \geqq 2$, hence $\nu_i=2$.

This immediately yields that if $p_i=p \mid m$ for which $q \nmid n_p$ then in case (1) we have $p \nmid s$, since $q \mid \nu_i=1$. This implies $q \mid t$. Now if (2) holds, then from $q \mid \nu_i=2$ it follows that $q=2$. Let $\nu_i=\nu_p$. Clearly $\nu_p \mid \phi(p^\alpha)=p^{\alpha-1}(p-1)$; hence $q \mid \nu_p$ implies that either $q=p$ or $q \mid p-1$. Now in case (1) either $p \nmid (n, t)=2$ or $(n, t)=1$, hence since $q \mid n$ and $p \mid t$ it follows that $q \neq p$. Consequently, $q \mid p-1$. Clearly, this can not be true if $p=2$. This completes the proof of (1) and (2) of the lemma. In fact, this includes the proof of the rest also. Indeed, if $q=2$ and (3C) holds then clearly case (2) of the lemma is impossible; it follows, therefore, that $p \neq 2$, and if (3D) holds then since $\nu_2=2$ it follows by the uniqueness of the prime p for which $2 \nmid n_p$ (equivalently $2 \nmid \nu_{p_j}$ for all $p_j \neq p$) that $p=2$ and, therefore, (2) of the lemma holds. q.e.d.

LEMMA 7. *Let x, y be two integers and let $\beta=\beta(q, x-1) \geqq 1$* (i.e., $x \equiv 1 \pmod{q}$) *and $\beta_y=(q, y) \geqq 0$ for a prime q. Then*: (1) *if $q \neq 2$* or $\beta \geqq 2$ (*i.e.*, $x \equiv 1 \pmod 4$ *in case $q=2$*) *then $\beta(q, x^y-1)=\beta+\beta_y$.* (2) *If $q=2$ and $\beta=1$ then*: $\beta_y=0$ *implies that $\beta(2, x^y-1)=1$, and $\beta_y \geqq 1$ implies that $\beta(2, x^y-1)=\beta_y+i+1$ where $x=1+2+\cdots+2^i+2^{i+2}x_1$, $i \geqq 1$.*

The proof is by induction on β_y. If $\beta_y=0$, let $x=1+q^\beta z$, $(z, q)=1$. Then, $(1+q^\beta z)^y=1+q^\beta yz+$terms with higher powers of q, and this case is proved since $(yz, q)=1$. Let $y=qy'=q^{\beta_y}y''$, $(y'', q)=1$, and $\beta_y \geqq 1$. By induction it follows that $x^{y'}=1+q^{\beta+\beta_y-1}u$, $(u, q)=1$. Hence,

$$x^y = (1+q^{\beta+\beta_y-1}u)^q = 1+q^{\beta+\beta_y}u+\cdots+C_{q,\nu}\,q^{\nu(\beta+\beta_y-1)}u^{q-\nu}+\cdots.$$

The highest power of q dividing

$$C_{q,\nu}\,q^{\nu(\beta+\beta_y-1)}\,u^{q-\nu}$$

is $\nu(\beta+\beta_y-1)+1$ if $1 \leqq \nu < q$ and it is $q(\beta+\beta_y-1)$ if $\nu=q$. Hence, the exceptional case to the proof of this lemma may occur if $q(\beta+\beta_y-1)=1\cdot(\beta+\beta_y-1)+1$. Equivalently, $(q-1)(\beta+\beta_y)=q$. This may happen only if $q=2$ and $\beta+\beta_y=2$. This proves the first part of the lemma.

To prove the second part it suffices to show it only for $y=2$. For, if x is of the form given in the lemma then $x^2=1+2^{i+2}x_2$, $(x_2, 2)=1$, by the case $y=2$, and now one can apply the first part to obtain the general result. If

$y=2$, and x is of the given form, then $x=-1+2^{i+1}(1+2x_1)=-1+2^{i+1}v$, where v is odd. Hence $x^2=1+2^{i+2}(-1+2^iv)v=1+2^{i+2}v_1$ and v_1 is odd. q.e.d.

The case $\beta_y=0$ is evident.

We recall some results of valuations of n cyclotomic fields and the rational field Q. Let p be a prime number, then to p corresponds a valuation of Q with its completion Q_p. Let $\mathcal{C}_m=Q(\epsilon_m)$, then the different extensions of this valuation to correspond to the different embeddings of $\mathcal{C}_m$ into a composition $\mathcal{C}_mQ_p$. Since $\mathcal{C}_m$ is normal the latter is uniquely defined, within the algebraic closure of Q_p. If $m=p^\alpha$, then $\mathcal{C}_mQ_p/Q_p$ is completely ramified with ramification number equal to $\phi(p^\alpha)$. If $(m, p)=1$, $\mathcal{C}_mQ_p/Q_p$ is unramified and $(\mathcal{C}_mQ_p: Q_p)=(\overline{\mathcal{C}_mQ_p}: \overline{Q_p})=f$, where f is defined above as the minimal integer satisfying $p^f\equiv 1(m)$.

LEMMA 8. *Let q, p be primes such that: $q\mid n$. Then:*

(1) *$\mathfrak{J}_q=\mathfrak{J}$ is the unique extension of $\mathfrak{Z}$ of degree q contained in $\mathcal{C}_m$, and $G(\mathcal{C}_m/\mathfrak{J})=\{\sigma^q\}$.*

(2) *$G(\mathcal{C}_mQ_p/\mathfrak{Z}Q_p)=G(\mathcal{C}_m/\mathfrak{Z}Q_p\cap\mathfrak{Z})=\{\sigma^\mu\}$.*

(3) *The inertia field of $\mathcal{C}_mQ_p/\mathfrak{Z}Q_p$ is $\mathfrak{T}=\mathfrak{Z}Q_p(\epsilon_{mp^{-\alpha}})$ if $p\mid m$, and $G(\mathcal{C}_mQ_p/\mathfrak{T})=G(\mathcal{C}_m\mid \mathfrak{T}\cap\mathcal{C}_m)=\{\sigma^{n_p}\}$. If $p\nmid m$, $\mathcal{C}_mQ_p/\mathfrak{Z}Q_p$ is unramified.*

The first part is evident. To prove (2) we first note that $\mathcal{C}_mQ_p/\mathfrak{Z}Q_p$ is also cyclic with generating automorphism which is σ^λ. Since $\mathcal{C}_mQ_p=Q_p(\epsilon_{p^\alpha}, \epsilon_{mp^{-\alpha}})$, σ^λ must be the first power of σ which induces an automorphism of $Q_p(\epsilon_{p^\alpha})$ and $Q_p(\epsilon_{mp^{-\alpha}})$. Now, $(Q_p(\epsilon_{p^\alpha}):Q_p)=(Q(\epsilon_{p^\alpha}):Q)=\phi(p^\alpha)$, hence any automorphism of $Q(\epsilon_{p^\alpha})/Q$ can be raised to an automorphism of $Q_p(\epsilon_{p^\alpha})/Q_p$. Thus one has to consider only the automorphisms of $Q_p(\epsilon_{mp^{-\alpha}})/Q_p$. Since $(p, mp^{-\alpha})=1$, the latter is an unramified extension (see e.g. [2, Theorem IV 3, p. 64]); hence its automorphisms are powers of the Frobenius automorphism S defined by: $\epsilon_{mp^{-\alpha}}\rightarrow\epsilon_{mp^{-\alpha}}^p$. The minimal power $\sigma^\lambda\in\{S\}$ is clearly given by the minimal integer satisfying $r^\lambda\equiv p^{\lambda'}(mp^{-\alpha})$ i.e. $\lambda=\mu_p$. The rest of (2) is well known.

Since $\mathfrak{T}=\mathfrak{Z}Q_p(\epsilon_{mp^{-\alpha}})$ and $(p, mp^{-\alpha})=1$, one concludes as before that $\mathfrak{T}/\mathfrak{Z}Q_p$ is unramified. On the other hand, $\mathcal{C}_mQ_p=\mathfrak{T}(\epsilon_{p^\alpha})$; hence $\mathcal{C}_mQ_p/\mathfrak{T}$ is complete and ramified (the proof of Theorem X 4, p. 217 [2]). From these facts one readily concludes that $\mathfrak{T}$ is the maximal unramified extension of $\mathfrak{Z}Q_p$ in $\mathcal{C}_m$.

The power of σ which leaves $\mathfrak{Z}Q_p(\epsilon_{mp^{-\alpha}})$ invariant is σ^{n_p}, since $\mu\mid n_p$, and as follows immediately by the definition of these numbers. Note that σ^{n_p} is also the minimal power of σ leaving $\epsilon_{mp^{-\alpha}}$ invariant. The rest of (3) is easily established.

LEMMA 9. (1) *The residue class degree $f(\mathfrak{Z}Q_p/Q_p)=\mu_p\delta_p/n_p=\delta'$.*

(2) *$\mathfrak{J}Q_p/\mathfrak{Z}Q_p$ is unramified if and only if $q\mid n_p$. If $q\nmid n_p$, this extension is totally ramified.*

(3) *If $q\nmid n_p$ and it is not the case where $q=p=2$ and* (3D) *holds, then a*

necessary and sufficient condition that $a \in ZQ_p$ *is a* Norm $(\mathfrak{J}Q_p/ZQ_p, x)$ *is that* $a \equiv b^q \pmod{\pi}$ *for some* $b \in \mathfrak{J}Q_p$ *and where* π *is a prime of* $\mathfrak{J}Q_p$.

To prove (1) we observe that $f(Q_p(\epsilon_{mp^{-\alpha}}) : Q_p) = f(\mathcal{C}_m Q_p : Q_p) = \delta$. Hence, applying the lemma of [2, p. 59] we obtain

$$\delta = f(\mathcal{C}_m Q_p : ZQ_p) f(ZQ_p : Q_p) = \frac{n_p}{\mu} \cdot f(ZQ_p : Q_p),$$

since by (3) of the preceding lemma it follows immediately that $(\mathcal{C}_m Q_p : \mathfrak{T}) = n/n_p$ and $(\mathcal{C}_m Q_p : ZQ_p) = n/\mu$ and $(\mathfrak{T} : ZQ_p) = f(\mathcal{C}_m Q_p : ZQ_p)$. This proves (1).

Combining (1) and (3) of the preceding lemma, it follows that $q \mid n_p$ is equivalent to the fact that $\mathfrak{J} \subseteq \mathfrak{T} \cap \mathcal{C}_m$. The latter condition is the same as $\mathfrak{J}Q_p \subseteq \mathfrak{T}$, which holds if and only if $\mathfrak{J}Q_p/Q_p$ is unramified. Since q is prime, it follows that if $q \nmid n_p$ the extension $\mathfrak{J}Q_p/Q_p$ must be totally ramified, and thus (2) is proved.

Note that under the conditions of (3) it follows by Lemma 6 that $q \mid p - 1$. Hence $q \mid p^{\delta'} - 1$. If $q \nmid n_p$, $\mathfrak{J}Q_p/ZQ_p$ is completely ramified and, therefore, if $a = N(\mathfrak{J}Q_p/ZQ_p, b)$ then $a \equiv b^q (\pi)$, which proves the necessity of (3). To prove the sufficiency, let E denote the group of all units of $\mathfrak{J}Q_p$ and $N(E)$ be the group of all Norms $(\mathfrak{J}Q_p/ZQ_p)$ of the elements of E. The residue class mapping maps E homomorphically onto $\overline{E} = \overline{\mathfrak{J}Q}_p$. By the necessity of (3), it follows that $N(E)$ is mapped into $\overline{E}_q$, the group of all qth powers of the elements of $\overline{E}$. Hence the residue mapping induces a homomorphism of $E/N(E)$ onto $\overline{E}/\overline{E}_q$. The latter is of order q since the order of $\overline{E}$ is $p^{\delta'} - 1$ and $q \mid p^{\delta'} - 1$. $E/N(E)$ is by a fundamental result of class field theory, in our case, also of order q. Hence $E/N(E) \cong \overline{E}/\overline{E}_q$ by the residue class mapping. Consequently, $N(E)$ is exactly the set of elements which are mapped by the residue mapping onto qth powers, which proves (3).

With the aid of the preceding lemmas, we are able to show

THEOREM 4. *The algebra* $\mathfrak{A}_{m,r}$ *is a division algebra if and only either* (3C) *or* (3D) *holds and one of the following holds*:

(1) $n = s = 2$ *and* $r \equiv -1 \pmod{m}$.

(2) *For every* $q \mid n$ *there exists a prime* $p \mid m$ *such that* $q \nmid n_p$ *and that either*

(a) $p \neq 2$, and $(q, (p^{\delta'} - 1)/s) = 1$ *or*,

(b) $p = q = 2$, (3D) *holds, and* $m/4 \equiv \delta' \equiv 1 \pmod{2}$.

Proof. By the remark to Theorem 3 it follows that one has to consider only the case where (3C) or (3D) holds.

$\mathfrak{A}_{m,r} = (\mathcal{C}_m, \sigma, \epsilon_s)$ is a cyclic algebra of index n over an algebraic number field. Hence, in view of the Hasse-Brauer-Noether theorem (e.g. [5, Satz 7, p. 119]), $A_{m,r}$ is a division algebra if and only if it is of exponent n. It follows, therefore, by [1, Theorem VII 19, p. 98] that A is a division algebra if and only if, for every $q \mid n$, $\epsilon_s \neq$ Norm $(F_q/Z, x_q)$. To determine the conditions for the element ϵ_s to be a norm we use Hasse's theorem which states, in our cyclic

case, that an element is a norm globally if and only if it is a norm locally everywhere([5]). First consider the finite primes. These rise from primes of the rational field Q. If $\mathfrak{F}Q_p/\mathfrak{Z}Q_p$ is unramified then since ϵ_s is a unit, it is always a norm [2, Theorem VII 2, p. 131]. By (3) of Lemma 8 and (3) of Lemma 9, one has to consider only primes $p \mid m$ and such that $q \nmid n_p$. In view of Lemma 6, we have to consider separately the cases (1) $p \neq 2$ (which implies that (3C) holds) and (2) $p=q=2$ and (3D) holds. Consider first case (1). Here, by (3) of Lemma 9, $\epsilon_s = \text{Norm}\ (\mathfrak{F}Q_p/\mathfrak{Z}Q_p, x)$ if and only if $\epsilon_s \equiv b^q(\pi)$. In this case the nonzero element of the residue field $\overline{\mathfrak{F}Q}_p = \overline{\mathfrak{Z}Q}_p$ is cyclic of degree $p^{\delta'}-1$ and, by Lemma 7, $q \mid p-1$, so that $\epsilon_s^{(p^{\delta'}-1)/q} \equiv 1(\pi)$. By Lemma 7, $(s, p)=1$, hence the last congruence can be replaced by an equality which implies that $s \mid (p^{\delta'}-1)/q$. The converse is also true, i.e. if $s \mid (p^{\delta'}-1)/q$, then $\epsilon_s^{(p^{\delta'}-1)/q} = 1$, which in view of the fact that the multiplicative groups of $\overline{\mathfrak{F}Q}_p$ is cyclic of degree $p^{\delta'}-1$, yields that $\epsilon_s = b^q(\pi)$. Thus, Lemma 9 yields

$$\epsilon_s = \text{Norm}\ (FQ_p/zQ_p, x).$$

This proves that ϵ_s is not a norm if and only if $s \nmid (p^{\delta'}-1)/q$. In the present case $(s, p)=1$, hence the fact $\epsilon_s \in \mathfrak{Z}Q_p$ implies that $s \mid p^{\delta'}-1$. Consequently, the condition $s \nmid (p^{\delta'}-1)/q$ is equivalent to $(q, (p^{\delta'}-1)/s)=1$.

It remains now to consider case (2) where $q=p=2$ and (3D) holds. In this case $\mathfrak{F}Q_2 = \mathfrak{Z}Q_2(i)$, where $i^2+1=0$. Indeed, by (3D), $r \equiv -1(2^\alpha)$, where 2^α is the highest power of 2 dividing m. Since $2 \nmid n_2$ and $\mu = \mu_2$ divides n_2, $r^\mu \equiv -1(2^\alpha)$, so that the effect of σ^μ on ϵ_{2^α} is the mapping $\epsilon_{2^\alpha} \to \epsilon_{2^\alpha}^{-1}$, in particular $i \to -i$. Hence, $i \notin \mathfrak{Z}$. $\mathfrak{F}$ is by Lemma 8 the unique cyclic extension of degree 2 of $\mathfrak{Z}$ contained in $\mathfrak{C}_m$; hence $\mathfrak{F} = \mathfrak{Z}(i)$, and thus $\mathfrak{F}Q_2 = \mathfrak{Z}Q_2(i) = \mathfrak{Z}Q_2 \cup Q_2(i)$. Applying the translation theorem of class field theory one obtains that $\epsilon_s = \text{Norm}\ (\mathfrak{F}Q_2/\mathfrak{Z}Q_2, b)$ if and only if $\text{Norm}\ (\mathfrak{Z}Q_2/Q_2, \epsilon_s) = \text{Norm}\ (Q_2(i)/Q_2, c)$ for some $c \in Q_2(i)$. In view of (3D), it follows that $\epsilon_s = -\epsilon_{s'}$ where $s = 2s'$ and s' is odd. $\text{Norm}\ (Q_2(\epsilon_{s'})/Q_2, \epsilon_{s'}) = \epsilon_{s'}^{1+2+\cdots+2^{l-1}} = \epsilon_{s'}^{2^l-1}$, where $l = (Q_2(\epsilon_{s'}) : Q_2)$, since $Q_2(\epsilon_{s'})/Q_2$ is unramified. Since s' is odd, l is the minimal integer such that $2^l \equiv 1(s')$. Hence $\text{Norm}\ (Q_2(\epsilon_{s'})/Q_2, \epsilon_{s'}) = 1$. Since $\epsilon_{s'} \in \mathfrak{Z}Q_2$, we obtain that $\text{Norm}\ (\mathfrak{Z}Q_2/Q_2, \epsilon_s) = (-1)^{(\mathfrak{Z}Q_2 : Q_2)}$. Here we have to distinguish between two cases one $\alpha = \beta(2, m) = 2$, and the second case $\alpha > 2$, i.e. $m \equiv O(8)$. In the second case, $\mathfrak{Z}$ contains the real subfield $\mathfrak{R}$ of $Q(\epsilon_{2^\alpha})$, since the effect of σ on $Q(\epsilon_{2^\alpha})$ is the conjugation. Furthermore, since $(Q(\epsilon_{2^\alpha}) : Q) = (Q_2(\epsilon_{2^\alpha}) : Q_2) = \phi(2^\alpha)$ it follows that $(\mathfrak{R} : Q) = (\mathfrak{R}Q_2 : Q_2) = \phi(2^\alpha)/2 = 2^{\alpha-2}$. Hence if $\alpha > 2$, $(\mathfrak{Z}Q_2 : Q_2)$ is even and, therefore, $\text{Norm}\ (\mathfrak{Z}Q_2/Q_2, \epsilon_s) = 1$. Consequently $\epsilon_s = \text{Norm}\ (FQ_2/Q_2, x)$. If $\alpha = 2$, the ramification degree of $\mathfrak{C}_m Q_2/Q_2$ is only 2; and since $\mathfrak{F}Q_2/Q_2$ is completely ramified, $\mathfrak{Z}Q_2/Q_2$ is unramified. Hence, $(\mathfrak{Z}Q_2 : Q_2) = (\overline{\mathfrak{Z}Q}_2 : \overline{Q}_2) = \delta'$ by (1) of Lemma 9. Thus, $\text{Norm}\ (\mathfrak{Z}Q_2/Q_2, \epsilon_s) = (-1)^{\delta'}$. If $\delta' \equiv O(2)$, then this proves that $\epsilon_s = \text{Norm}\ (FQ_2/Q_2, x)$. If $\delta' \equiv 1(2)$, $(-1)^{\delta'} = -1$ and -1 is not a $\text{Norm}\ (Q_2(i)/Q_2, c)$ as can be readily proved.

([5]) Quoted e.g. in [1, Lemma IX 9, p. 147].

This proves that $\epsilon_s = \text{Norm}\ (FQ_2/Q_2, x)$ if and only if δ' is even.

Consider now the infinite primes. In this case $\mathcal{C}_m Q_\infty/\mathcal{Z}Q_\infty$ is ramified if and only if $\mathcal{Z}$ is isomorphic with a subfield of Q_∞ i.e. with a real field. In the unramified case ϵ_s is, evidently, a norm. Since $\mathcal{Z}/Q$ is also normal the ramification is equivalent to the fact that $\mathcal{Z}$ should be a real field. This happens if and only if $n=s=2$, and $r\equiv -1(m)$ (and, therefore, (3D) holds). Indeed, since $\epsilon_s \in \mathcal{Z}$ and $\mathcal{Z}$ is a real field, it follows that $\epsilon_s = -1$, i.e., $s=2$. Lemma 5 implies that $n=s=2$. If $r \not\equiv -1(m)$, since $r^2 \equiv 1(m)$ it follows that $r \equiv 1(m_1)$ for some divisor m_1 of m. This implies that ϵ_{m_1} is left invariant under σ, hence $\epsilon_{m_1} \in \mathcal{Z}$. The latter is real. Consequently, $m_1 = 2$. But by (3D) $r \equiv -1(2^\alpha)$. The converse is readily verified. Furthermore, if $n=s=2$ and $r \equiv -1(m)$, then σ is the conjugation of $\mathcal{C}_m$ and one readily observes that $\mathfrak{A}_{m,r}$ is a quaternion algebra over the real field $\mathcal{Z}=\mathfrak{R}$, hence, a division algebra.

Summarizing the preceding results, we see that $\mathfrak{A}_{m,r}$ is a division algebra if and only if either (1) of Theorem (5) holds, or $\epsilon_s \neq \text{Norm}\ (\mathcal{J}_q/\mathcal{Z}, x)$ for every prime $q \mid n$. The latter is equivalent that for some finite prime p,

$$\epsilon_s \neq \text{Norm}\ (\mathcal{J}_q Q_p/\mathcal{Z}Q_p, x_p),$$

and necessary and sufficient conditions for this are, by the preceding result, that $p \mid m$, $q \nmid n_p$, and $(q, (p^{\delta'}-1)/s) = 1$ if $p \neq 2$. In the other case $p=q=2$ of (3D) holds and then we must have $m = 4m'$, where m' and δ' are odd integers, which completes the proof of Theorem 5.

LEMMA 10. *In the conditions of Theorem* 4, *the integer* δ' *can be replaced by* $\delta = \delta_p$, *the minimal integer satisfying* $p^\delta \equiv 1 \pmod{mp^{-\alpha}}$.

Indeed, in all cases $q \nmid n_p$; hence since n_p/μ_p is an integer, $q \nmid n_p/\mu_p$. Thus, the highest power of q dividing $\delta' = \delta_p n_p/\mu_p$ is the same as that dividing δ_p. In our notation this is stated in the form $\beta(q, \delta') = \beta(q, \delta)$. Clearly this implies that in (b) of Theorem 4, δ' can be replaced by δ since this condition is equivalent to $\beta(2, \delta') = \beta(2, \delta) = 0$. To prove the lemma for condition (a) of the preceding theorem, we note first that by Lemma 6 it follows that $q \mid p-1$, i.e., $\beta(q, p-1) \geqq 1$. Hence, if the conditions of case (1) of Lemma 7 holds, we obtain that $\beta(q, p^{\delta'}-1) = \beta(q, p-1) + \beta(q, \delta')$. Thus, the latter is equal to $\beta(q, p-1) + \beta(q, p^\delta - 1) = \beta(q, p^\delta - 1)$. This proves that $\beta(q, p^{\delta'}-1) = \beta(q, p^\delta - 1)$. A similar proof obtained by using the second case of Lemma 7 yields together with the preceding result that $\beta(q, p^{\delta'}-1) = \beta(q, p^\delta - 1)$ always holds. Hence:

$$\beta\left(q, \frac{p^{\delta'}-1}{s}\right) = \beta(q, p^{\delta'}-1) - \beta(q, s) = \beta(q, p^\delta - 1) - \beta(q, s)$$

$$= \beta\left(q, \frac{p^\delta - 1}{s}\right).$$

Condition (a) of Theorem 4 is equivalent to $\beta(q, (p^{\delta'}-1)/s)=0$, which now holds if and only if $\beta(q, (p^{\delta}-1)/s)=0$. In other words this means replacing δ' by δ.

For further applications we state the last condition in another form. It was already observed that (a) of Theorem 4 is equivalent to the fact that $0=\beta(q, (p^{\delta}-1)/s)=\beta(q, p^{\delta}-1)-\beta(q, s)$. Now if $p\neq 2$, it follows by Lemma 6 that we can apply Lemma 7 to compute $\beta(q, p^{\delta}-1)$. Thus, we obtain by the two parts of Lemma 7 that condition (a) of Theorem 4 is equivalent to one of the following conditions:

(I_1) $\beta(q, s)=\beta(q, p-1)+\beta(q, \delta)$ if either $q\neq 2$ or $p\equiv 1 \pmod 4$.

(I_2) $\beta(2, s)=\beta(2, \delta)+i+1$ if $p=1+2+\cdots+2^i \pmod{2^{i+2}}$, $i\geqq 1$ and $\beta(2, \delta)\geqq 1$, and $\beta(2, s)=1$ if $\beta(2, \delta)=0$.

In order to obtain a more applicable condition than these we wish to compute $\beta(q, \delta)$. To this end we consider the factorization of m: $m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}\cdot p^{\alpha}\cdot q^{\beta}$, where q, p, p_i are the different prime factors of m. In our notations we have $\beta=\beta(q, m)$, $\alpha=\beta(p, m)$ and $\alpha_i=\beta(p_i, m)$. Let $\bar{\gamma}_i=(p, p_i^{\alpha_i})$, i.e., $\bar{\gamma}_i$ is the minimal integer satisfying $p^{\bar{\gamma}_i}\equiv 1 \pmod{p_i^{\alpha_i}}$. Let $\gamma_0=\gamma(p, q^{\beta})$. Then clearly, $\delta=[\gamma_0, \bar{\gamma}_1, \cdots, \bar{\gamma}_k]$ is the least common multiple of $\gamma_0, \bar{\gamma}_1, \cdots, \bar{\gamma}_k$. Hence $\beta(q, \delta)=\text{Max}\{\beta(q, \gamma_0), \beta(q, \bar{\gamma}_1), \cdots, \beta(q, \bar{\gamma}_k)\}$. The number $\gamma_i=\gamma(p, p_i)$ is by definition the minimal integer satisfying $p^{\gamma_i}\equiv 1 \pmod{p_i}$. Hence, one readily verifies that $\bar{\gamma}_i=\gamma_i p_i^{\lambda_i}$ for some integer λ_i. Since $q\neq p_i$, the highest power of q dividing $\bar{\gamma}_i$ is a divisor of γ_i. Thus $\beta(q, \bar{\gamma}_i)=\beta(q, \gamma_i)$. This yields that:

(II) $\beta(q, \delta)=\text{Max}\{\beta(q, \gamma_0), \beta(q, \gamma_1), \cdots, \beta(q, \gamma_k)\}$.

The second step towards simplification is to compute $\beta(q, \gamma_0)$ in two cases, namely we show that:

(III_1) If $p\equiv 1 \pmod 4$ or $q\neq 2$ then $\beta(q, \gamma_0)=\text{Max}\{0, \beta(q, m)-\beta(q, p-1)\}$.

(III_2) If $q=2$ and $p\equiv 1+2+\cdots+2^i \pmod{2^{i+2}}$, $i\geqq 1$, then $\beta(2, \gamma_0)=0$ if $\beta(2, m)=1$; and $\beta(2, \gamma_0)=\text{Max}\{1, \beta(2, m)-i-1\}$ if $\beta(2, m)\geqq 2$.

Recall that γ_0 is by definition the minimal integer for which $p^{\gamma_0}\equiv 1 \pmod{q^{\beta}}$. Since $p\neq 2$, it follows by Lemma 6 that $q \mid p-1$. Hence applying Lemma 7, it follows that if $p\equiv 1 \pmod 4$ or $q\neq 2$ then $\beta(q, p^{\gamma_0}-1)=\beta(q, p-1)+\beta(q, \gamma_0)$. Thus one readily verifies that $\gamma_0=q^{\lambda}$, where $\lambda=\beta(q, \gamma_0)$ has to be chosen as the minimal integer satisfying $\lambda+\beta(q, p-1)\geqq\beta$. Since $\beta=\beta(q, m)$ it follows that $\lambda=\text{Max}\{0, \beta(q, m)-\beta(q, p-1)\}$ which proves (III_1). The proof of (III_2) follows the same line with the application of the second part of Lemma 7. Here, $\beta(2, p^{\gamma_0}-1)=\beta(2, \gamma_0)+i+1$ if $\beta(2, \gamma_0)\geqq 1$ and $\beta(2, p^{\gamma_0}-1)=1$ if γ_0 is odd. Under the conditions of (III_2) we have $\beta(2, p-1)=1$ and γ_0 should be minimal with the property that $p^{\gamma_0}-1$ is divisible by 2^{β}; hence one readily verifies that for $\beta=1$, $\gamma_0=1$ is the required integer and if $\beta\geqq 2$ then $\gamma_0=2^{\lambda}$ with λ the minimal integer $\geqq 1$ for which $\lambda+i+1\geqq\beta$. Thus $\lambda=\beta(2, \gamma_0)=\text{Max}\{1, \beta(2, m)-i-1\}$. The proof of ($III_2$) is now completed with the

obvious remark that under the condition of (III_2), $\beta(2, m)=1$ if and only if $\beta(2, \gamma_0)=0$ and thus for $\beta(2, m)\geqq 2$ we have $\beta(2, \gamma_0)\geqq 1$.

The last preparatory remark we need is the fact that:

(IV) If $q\nmid n_p$ and $p\neq 2$ then $\beta(q, m)=\beta(q, s)$.

Indeed by Lemma 6 it follows that if $q=2$ then (3C) holds and, therefore, $(n, t)=1$; hence the highest power of 2 dividing $m=st$ must divide s since $2\mid n$ and $(n, t)=1$ implies $2\nmid t$. If $q\neq 2$ then the same argument holds since $(n, t)=1$ or 2.

With these results we are in position to prove:

THEOREM 5. *A necessary and sufficient condition that $\mathfrak{A}_{m,r}$ is a division algebra is that* (3C) *or* (3D) *holds and either*:

(1) $n=s=2$ *and* $r\equiv -1 \pmod m$ *or*,

(2) *For every prime* $q\mid n$ *there exists a prime* $p\mid m$ *such that* $q\nmid n_p$ *and that one of the following holds*:

(2a) $p\equiv 1 \pmod 4$ *or* $q\neq 2$ *and* $\beta(q, s)\geqq\beta(q, p-1)+\mathrm{Max}_i\,\beta(q, \gamma_i)$.

(2b) $p\equiv 1+2+\cdots+2^i \pmod{2^{i+2}}$, $i\geqq 1$ *and* $q=2$, (3C) *holds; and* $\beta(2, s)\geqq i+1+\mathrm{Max}\{1, \beta(2, \gamma_i)\}$ *if* $s\equiv 0 \pmod 4$, *but if* $s\not\equiv 0 \pmod 4$ *then all* $\beta(2, \gamma_i)=0$; i.e., *all* γ_i *are odd integers.*

(2c) $p=q=2$, (3D) *holds,* $m/4$ *and all* γ_i *are odd integers.*

Proof. Evidently, (1) of Theorem 4 and condition (1) of the present theorem are equivalent. The proof of this theorem will be achieved by showing that the condition (2a) is equivalent to (I_1), (2b) is equivalent to (II_2) and that (2c) and (b) of Theorem 4 are equivalent. This will prove the theorem since it was shown that (I_1) and (I_2) together are equivalent to (a) of Theorem 4.

Substituting (III_1) in (II) we obtain by (IV) that (I_1) is equivalent to the condition that:

$$\beta(q, s)=\beta(q, p-1)+\mathrm{Max}\{0, \beta(q, s)-\beta(q, p-1), \beta(q, \gamma_1), \cdots, \beta(q, \gamma_k)\}$$

or, equivalently, $\beta(q, s)\geqq\beta(q, p-1)+\mathrm{Max}_i\,\beta(q, \gamma_i)$. This proves that ($I_1$) and (2a) are equivalent.

Now (II), (III_2), and (IV) imply that:

$$\beta(2, \delta)=\mathrm{Max}\{1, \beta(2, s)-i-1, \beta(2, \gamma_1), \cdots, \beta(2, \gamma_k)\} \text{ if } \beta(2, m)\geqq 2$$

and

$$\beta(2, \delta)=\mathrm{Max}\{\beta(2, \gamma_1), \cdots, \beta(2, \gamma_k)\} \text{ if } \beta(2, m)=1.$$

In the first case $\beta(2, \delta)\geqq 1$ and in the second case $\beta(2, \delta)=0$ if and only if $\beta(2, \gamma_i)=0$ for $i=1, \cdots, k$. From this we conclude by (III_2) and (IV) that:

(α) If $\beta(2, m)=\beta(2, s)\geqq 2$ then (I_2) is equivalent to

$$\beta(2, s)=i+1+\mathrm{Max}\{1, \beta(2, s)-i-1, \beta(2, \gamma_1), \cdots, \beta(2, \gamma_k)\}.$$

Hence,

$$\beta(2, s)\geqq i+1+\mathrm{Max}\,\beta(2, \gamma_j).$$

(β) If $\beta(2, m)=\beta(2, s)=1$ and all γ_j are odd, i.e., $\beta(2, \gamma_j)=0$, then (I_2) is equivalent to the condition that $\beta(2, s)=1$ which is not an additional restriction at all.

(γ) If $\beta(2, m)=\beta(2, s)=1$ and at least one $\beta(2, \gamma_j)>0$ then $\beta(2, \delta)\geqq 1$ and, therefore, (I_2) is equivalent to $\beta(2, s)=i+1+\beta(2, \delta)$ but the latter is $\geqq 2$ since $i\geqq 1$. Thus, this condition includes a contradiction. Hence noting that $\beta(2, s)\geqq 2$ means that $s\equiv 0 \pmod 4$ and $\beta(2, s)=1$ means that $s\not\equiv 0 \pmod 4$, (α) and (β) prove that (2b) is equivalent to (I_2).

The equivalency of (2c) and (b) of Theorem 4 follows from the fact that since $p=q=2$ one has not to consider γ_0, and δ is odd means that $\beta(2, \delta)=0$ which is equivalent by (II) to the condition that all $\beta(2, \gamma_j)=0$, i.e., all γ_j are odd integers. This concludes the proof of Theorem 5.

In order to construct groups of odd order which can be embedded in division rings we have to find odd integers m, n, s, r, t satisfying (3A), (3C) and which are subjected to condition (2a), since then the group $G_{m,r}$ and the algebra $\mathfrak{A}_{m,r}$ satisfy Theorems 3 and 5. The following is a method of finding such numbers: we choose $t=p$ a prime not of the form $1+2^i$ and $n=q$ any odd prime factor of $p-1$. Then we set $s=q^\lambda$ where $\lambda=\beta(q, p-1)$, i.e., s is the highest power of q dividing $p-1$. Thus, by definition, $\beta(q, p-1)=\beta(q, s)$. Hence $m=st=q^\lambda p$. Note that since no γ_j are to be considered, condition (2a) is valid and evidently (3C) holds. To complete the proof it suffices to exhibit a number r for which $s=(r-1, m)$ and such that r is an nth primitive root modulo m. Since $n=q \mid p-1$, there exists a primitive root modulo p. Now the set of all elements of the form $1+sx$, where x ranges over the numbers $0, 1, \cdots, p-1$, range over all different classes modulo p; hence, for some x, the number $1+sx=r$ is a primitive nth root modulo p. Since $r\equiv 1 \pmod s$ it follows that r is also a primitive nth root modulo $m=sp$. By definition of r and s, one readily verifies that $s=(r-1, m)=(sx, sp)=s(x, p)$. Thus, the existence of an infinite number of primes not of the form $1+2^i$ yields an infinite number of groups of odd order which can be embedded in division rings.

It follows readily, by (3A), that a group $G_{m,r}$ of minimal odd order which can be embedded in a division ring may be obtained by taking $s=q, t=p$ two odd primes. Since we must have $n=q$ (for $n \mid s$) and by Lemma 6 it follows necessarily that since $q \nmid n_p$, $q \mid p-1$. The minimal possible primes are $q=3$ and $p=7=1+3\cdot 2$. In this case we obtain $\beta(3, 3)=\beta(3, 7-1)=1$. Hence condition (2a) of Theorem 5 is valid. Furthermore, the present example of the numbers 3 and 7 falls under the class of the numbers chosen above to construct groups of odd order which are subgroups of division rings, hence the minimal order thus obtained is $mn=7\cdot 3\cdot 3=63$. Following the method suggested above one finds that r can have only the values 16 and 4 but it is not hard to show that $G_{21,4}\cong G_{21,16}$ (here $m=7\cdot 3$). This proves that the

minimal group is uniquely determined up to isomorphism. This completes the proof of

THEOREM 6. *There are an infinite number of groups of odd order which can be embedded in division rings and the group with this property which is of minimal order is uniquely determined and it is of order* 63.

5. **The various types.** The following different types of groups will be shown to contain the groups which can be embedded in division rings.

(5A) *Cyclic groups.*

(5B) *D-groups.* This class contains the set of all groups $G_{m,r}$ which are not cyclic. Important examples of this class is the quaternion group $\mathfrak{Q}^* = \{\pm 1, \pm i, \pm j, \pm k\}$ of order 8 and more generally the *binary dihedral group* $\mathfrak{D}_m^*$ (see [9, §6.1, p. 138]), which are closely related with the dihedral subgroup of order $2m$ of the three dimensional orthogonal group O_3.

(5C) *T-groups.* The simplest group of this type is the *binary tetrahedral group* $\mathfrak{T}^*$ of order 24 (see [9, §6.2, p. 139]). This group $\mathfrak{T}^*$ contains as a 2-Sylow subgroup the quaternion group and an additional element of order 3. Namely: $\mathfrak{T}^* = \{P, Q, R\}$ where the elements P, Q, R satisfy the relations:

(T_1) $P^4 = 1$; $P^2 = Q^2$; $PQP^{-1} = Q^{-1}$,

(T_2) $RPR^{-1} = Q$; $RQR^{-1} = PQ$,

(T_3) $R^3 = 1$.

The element P^2 of $\mathfrak{T}^*$ generates the center of $\mathfrak{T}^*$ and $\mathfrak{T}^*/(P^2)$ is isomorphic with the tetrahedral group. Actually, $\mathfrak{T}^*$ can be uniquely determined by this property (see Z12).

By a general *T-group* we mean a group $G_T \cong \mathfrak{T}^* \times G_{m,r}$, where $G_{m,r}$ is either cyclic (i.e. $r = 1$) of order prime to 6, or a D-group of order prime to 6.

(5D) *O-groups.* The simplest group of this type is the *binary octahedral* group $\mathfrak{O}^*$ (see [9, §6.3, p. 140]). $\mathfrak{O}^*$ is of order 48, its center is group of order 2 and $\mathfrak{O}^*$ modulo the center is isomorphic with the octahedral group. $\mathfrak{O}^*$ has a 2-Sylow subgroup of order 16 generated by T, Q satisfying:

$$(O_1) \qquad T^8 = 1; \qquad T^4 = Q^2; \qquad QTQ^{-1} = T^{-1}$$

and another generator R satisfying among others the relation $R^3 = 1$. Furthermore, $\{T^2, Q, R\}$ is isomorphic with $\mathfrak{T}^*$.

By a general *O-group* we mean a group $G_O \cong \mathfrak{O}^* \times G_{m,r}$, where $G_{m,r}$ is a cyclic group or a D-group of order prime to 6.

(5E) *I-groups.* The basic group of this type is the *binary icosahedral* group $\mathfrak{I}^*$ of order 120 (see [9, §6.4, p. 140]). This group contains a center of order 2 and $\mathfrak{I}^*$ modulo this center is isomorphic with the icosahedral group. By Z12, it follows that $\mathfrak{I}^* \cong M(2, 5)$, where $M(2, 5)$ denotes the homogeneous modular group modulo 5. $\mathfrak{I}^*$ contains a subgroup isomorphic with $\mathfrak{T}^*$ of index 5.

By an *I-group* we shall mean a group $G \cong \mathfrak{I}^* \times G_{m,r}$ where $G_{m,r}$ is either

cyclic or a D-group and its order is relatively prime to 120.

We turn to the possible embeddings of the groups of the preceding types in division rings.

LEMMA 11. *If the quaternion group* $\mathfrak{Q}^* \subseteq \mathfrak{R}^*$ *then* $\mathfrak{U}(\mathfrak{Q}^*) = (Q(i), j, -1) = \mathfrak{A}_2$ *the quaternion algebra over the rational field* Q.

As was pointed out $\mathfrak{Q}^*$ is a $G_{4,3}$ group, hence this lemma is a special case of Lemma 3.

LEMMA 12. *If* $G \subseteq \mathfrak{R}^*$ *contains a group* $G_0 = \{P, Q, R\}$ *where the generator* P, Q, R *satisfy* (T_1) *and* (T_2) *and instead of* (T_3): $R^{3^\beta} = 1$, $\beta \geqq 1$. *Then* $\beta = 1$, *i.e.* $G_0 \cong \mathfrak{Z}^*$. *Furthermore,* $\mathfrak{U}(G_0)$ *is isomorphic with the quaternion algebra* $\mathfrak{A}_2$ *over the rationals and* $R = -(1+P+Q+PQ)/2$ *in* $\mathfrak{R}^*$.

Since $G_1 = \{P, Q\}$ is a quaternion group, it follows by the preceding lemma that $\mathfrak{U}(G_1)$ is the quaternion algebra over Q. One readily verifies by the proof of Lemma 4 that 1, P, Q, PQ are a Q-base of $\mathfrak{U}(G_1)$. Since $P^4 = 1$, $(P^2-1)\cdot(P^2+1) = 0$ in K^*. Hence $P^2 = -1$, and thus $P^{-1} = -P$. Similarly $Q^{-1} = -Q$, and, therefore, $PQ = -QP$. Let $D = -(1+P+Q+PQ)/2$. A straightforward computation shows that $D^3 = 1$ and $DP = QD$, $DQ = (PQ)D$. Put $C = RD^{-1} \in \mathfrak{R}^*$. Then, in view of (T_2) C commutes with P and Q. Hence, $G_0 \subseteq \mathfrak{A}_2 \otimes Q(C) \subseteq \mathfrak{R}^*$. Now $R = CD$, C and D commute; hence $R^3 = C^3D^3 = C^3$. Since $R^{3^\beta} = 1$ it follows that $C^{3^\beta} = 1$. If $C \neq 1$, $Q(C)$ contains a primitive 3rd root of unity ω (which is a power of C). But then $\mathfrak{A}_2 \otimes Q(\omega) \subseteq \mathfrak{R}^*$ contains zero divisor, since $0 = D^3 - 1 = (D-1)(D-\omega)(D-\omega^2)$ and $D \neq 1, \omega, \omega^2$ since D does not commute with P or Q. Consequently, $C = 1$, i.e. $R = D = -(1+P+Q+PQ)/2$ and as a by-result it follows that $R^3 = 1$.

LEMMA 13. *If* $\mathfrak{D}^* \subseteq \mathfrak{R}^*$ *then,* $\mathfrak{U}(\mathfrak{D}^*) \cong (\mathcal{C}_8, j, -1) = \mathfrak{A}_2 \otimes Q(2^{1/2})$. *Furthermore, if* $\{P, Q\}$ *generate the quaternion subgroup of* $\mathfrak{D}^*$ *and* $\mathfrak{D}^* = \{T, Q, R\}$ *satisfying* (O_1) *and* $T^2 = P$, *then*

$$R = -(1 + P + Q + PQ)/2 \quad \text{and} \quad T = \pm(1 + P)/2^{1/2}(6),$$

in $\mathfrak{R}^*$.

The subgroup $\{T, Q\}$ of $\mathfrak{D}^*$ is a $G_{8,-1}$ group. Hence, by Theorem 3, $\mathfrak{U}(\mathfrak{D}^*) \supseteq \mathfrak{U}(G_{8,1}) \cong \mathfrak{A}_{8,-1} = (\mathcal{C}_8, j, -1)$. j is the conjugation of $\mathcal{C}_8$ and its real subfield is $Q(2^{1/2})$, thus $\mathfrak{A}_{8,-1} = \mathfrak{A}_2 \otimes Q(2^{1/2})$. If $T^2 = P$ corresponds to i in $\mathfrak{A}_2$, then in the field $Q(T)$, $T = P^{1/2} = \pm(1+P)/2^{1/2}$. By the previous result, $R = -(1+P+Q+PQ)/2$. Hence $\mathfrak{D}^* = \{T, Q, R\} \subseteq \mathfrak{U}\{P, Q\} \otimes Q(2^{1/2}) \cong \mathfrak{A}_2 \otimes Q(2^{1/2})$.

Actually, in view of the proof of Lemma 5, we have shown:

COROLLARY 1. *If a group* $G \subseteq \mathfrak{R}^*$ *contains a generalized quaternion group of*

(6) $2^{1/2}$ denotes here the real number satisfying $x^2 = 2$ in $Q(T)$.

order 2^4: $G_2=\{T^8=1,\ T^4=Q^2,\ QTQ^{-1}=T^{-1}\}$ *and an element* R *of order* 3^β *satisfying* $RT^2R^{-1}=Q$, $RQR^{-1}=T^2Q$, *then* $\beta=1$ *and* $\{R, T, Q\}\cong\mathfrak{O}^*$.

For by the proof of Lemma 5, $R=-(1+T^2+Q+T^2Q)/2$ and by the proof of the previous lemma $T=\pm(1+T^2)/2^{1/2}$. Thus the relation between T^2, Q completely determine the group $\{R, T, Q\}$. One readily shows that in the quaternion algebra over the reals the element $-(1+i+j+k)/2$, $(1+i)/2^{1/2}$, j generate a group isomorphic with $\mathfrak{O}^*$. Clearly this group is isomorphic with $\{R, T, Q\}$; hence $\{R, T, Q\}\cong\mathfrak{O}^*$.

We turn now to the more complicated group $\mathfrak{J}^*$.

LEMMA 14. *If* $\mathfrak{J}^*\subseteq\mathfrak{R}^*$ *then* $\mathcal{U}(\mathfrak{J}^*)\cong\mathfrak{A}_{10,-1}\cong(\mathcal{C}_5, j, -1)\cong\mathfrak{A}_2\otimes Q(5^{1/2})$ [7] *where* $\mathfrak{A}_2$ *denotes the quaternions over the rationals.*

First we observe that the real subfield of $Q(\epsilon_5)=\mathcal{C}_5$ is $Q(5^{1/2})$. Put $\epsilon=\epsilon_5$. The elements j, $i_1=(1/5^{1/2})(\epsilon^2-\epsilon^3)+(1/5^{1/2})(\epsilon-\epsilon^4)j$ of $\mathfrak{A}_{10,-1}$ form a basis of a quaternion subalgebra $\overline{\mathfrak{A}}_2$ of $\mathfrak{A}_{10,-1}$. This follows by a straightforward computation using the fact that $j\epsilon j^{-1}=\epsilon^{-1}$. Now $(\mathfrak{A}_{10,-1}:Q)=8$ and $5^{1/2}$ belongs to the center, hence one readily shows that 1, i_1, j, i_1j, $5^{1/2}$, $i_15^{1/2}$, $j5^{1/2}$, $i_1j5^{1/2}$ constitute a base of $A_{10,-1}$ over Q. Consequently $\mathfrak{A}_{10,-1}\cong\overline{\mathfrak{A}}_2\otimes Q(5^{1/2})$.

The group $\mathfrak{J}^*$ has generators P, Q with relations: $P^2=Q^3=(PQ)^5$, $P^4=1$. (See Z16 or [9, p. 140]). In $\mathfrak{R}^*$, $P^4=1$ implies, as was seen before, $P^2=-1$. Put $R=-Q=P^2Q=Q^4$, $S=-PQ=PQ^4$. Then $R^3=1$, $S^5=1$, $(SR^{-1})^2=-1$. This yields in $\mathfrak{R}^*$ the relations $R^2+R+1=0$; $S^4+S^3+S^2+S+1=0$; $SR^{-1}=-RS^{-1}$ or equivalently since $R^{-1}=-R-1$, $-S(R+1)=-RS^{-1}$ which yields: $SR=RS^{-1}-S$. $\mathfrak{J}^*$ is already generated by -1, R, S; hence the preceding relation shows that $\mathcal{U}(\mathfrak{J}^*)=Q+SQ+S^2Q+S^3Q+RQ+RSQ+RS^2Q+RS^3Q$. Thus $(\mathcal{U}(\mathfrak{J}^*):Q)\leqq 8$. On the other hand, $\mathcal{U}(\mathfrak{J}^*)$ is a central simple algebra over Q, hence it is of degree u^2r, where r is the degree of its center over Q. Consequently $u^2r\leqq 8$. Note that since $\mathfrak{J}^*$ is not abelian, $u>1$; hence $u=2$. $\mathcal{U}(\mathfrak{J}^*)\supset Q(S)\cong\mathcal{C}_5$ which is a field of degree 4. Hence $4\,|\,ur$. This immediately yields that $u=2$, $r=2$. Consequently, $u^2r=8$ and, therefore, $(\mathcal{U}(\mathfrak{J}^*):Q)=8$. This proves more: the field $Q(S)$, which is of degree 4, must contain the center of $U(\mathfrak{J}^*)$ which is of degree 2. $\mathcal{C}_5\cong Q(S)$ is cyclic over Q and its only subfield of degree 2 is its real subfield which is isomorphic with $Q(5^{1/2})$. Hence, the center of $\mathcal{U}(\mathfrak{J}^*)$ is isomorphic with $Q(5^{1/2})$. The algebra $\mathcal{U}(\mathfrak{J}^*)$ contains a quaternion algebra $\mathfrak{A}_2$ over the rationals, since $\mathfrak{J}^*$ contains a quaternion group and from the fact that $5^{1/2}$ belongs to the center of $\mathcal{U}(\mathfrak{J}^*)$ one deduces as above that $\mathcal{U}(\mathfrak{J}^*)\cong\mathfrak{A}_2\otimes Q(5^{1/2})$. Consequently, $\mathcal{U}(\mathfrak{J}^*)\cong\mathfrak{A}_{5,-1}\cong\mathfrak{A}_{10,-1}$.

This also can be obtained by using the fact that $\mathfrak{J}^*\cong M(2, 5)$. The latter contains the matrices

[7] Note that $Q(\epsilon_5)=Q(\epsilon_{10})$, and therefore $\mathfrak{A}_{10,-1}=\mathfrak{A}_{5,-1}$.

$$S_1 = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, \qquad P_1 = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$$

satisfying $S_1^{10}=1$, $P_1^4=1$, $P_1S_1P_1^{-1}=S_1^{-1}$, $P_1^2=S_1^5$. Namely, P_1, S_1 generate a group $G_{10,-1}$. Hence by Theorem 3a: $\mathfrak{A}_{10,-1}\cong\mathcal{U}(P_1, S_1)\subseteq\mathcal{U}(\mathfrak{J}^*)$. Since $\mathfrak{A}_{10,-1}=\mathfrak{A}_{5,-1}$ is also of degree 8 over Q, $\mathcal{U}(\mathfrak{J}^*)\cong\mathfrak{A}_{5,-1}$.

The converse of the last lemmas is also true. That is: the group $\mathfrak{T}^*$ is in fact a subgroup of the quaternions $\mathfrak{A}_2$ over the rationals, i.e. the element $(i, j, -(1+i+j+k)/2)$ generates a group (isomorphic with) $\mathfrak{T}^*$.

The group $\mathfrak{O}^*$ is a subgroup of $\mathfrak{A}_{8,-1}\cong\mathfrak{A}_2\otimes Q(2^{1/2})$, for a group $\mathfrak{O}^*$ is generated by $\{i, j, -(1+i+j+k)/2, (1+i)/2^{1/2}\}$. The group $\mathfrak{J}^*$ is contained in $\mathfrak{A}_{5,-1}\cong\mathfrak{A}_2\otimes Q(5^{1/2})$. Namely, the elements (ϵ, j, i_1) generate a group $\mathfrak{J}^*$. This can be readily shown by noting that the elements $-\epsilon$, $\rho=(1+i_1+j+i_1j)/2$ satisfy the relations $(-\epsilon)^{10}=1$, $\rho^2=(-\epsilon)^5=(-\rho\epsilon)^2=-1$. A simple proof for the latter is obtained by showing that trace $\rho=-1$, trace $(\rho\epsilon)=0$ and since Norm $\rho=$ Norm $\rho\epsilon=1$, ρ satisfies $\rho^2-\rho+1=0$ and $\rho\epsilon$ satisfies $(\rho\epsilon)^2+1=0$.

With these remarks we are ready to show:

THEOREM 6a. *A T-group $G_T=\mathfrak{T}^*\times G_{m,r}$ can be embedded in a division ring if and only if $\mathfrak{A}_{4m,r_1}$ is a division algebra where r_1 is a number satisfying $r_1\equiv r$ (mod m), $r_1\equiv -1$ (mod 4); and then $\mathcal{U}(G_T)\cong\mathfrak{A}_2\otimes_Q\mathfrak{A}_{m,r}\cong\mathfrak{A}_{4m,r_1}$, and the latter is of order $(2n)^2$ over its center.*

THEOREM 6b. *An O-group, $G_O=\mathfrak{O}^*\times G_{m,r}$ can be embedded in a division ring if and only if $\mathfrak{A}_{8,-1}\otimes_Q\mathfrak{A}_{m,r}\cong\mathfrak{A}_{8m,r_1}$ is a division algebra, where $r_1\equiv r$ (mod m), $r_1\equiv -1$ (mod 8); and then $\mathcal{U}(G_O)\cong A_{8m,r_1}$ and the latter is of order $(2n)^2$ over its center.*

THEOREM 6c. *An I-group $G_O=\mathfrak{J}^*\times G_{m,r}$ can be embedded in a division ring if and only if $\mathfrak{A}_{10m,r_1}\cong\mathfrak{A}_{10,-1}\otimes_Q\mathfrak{A}_{m,r}$ is a division ring, where $r_1\equiv -1(10)$, $r_1\equiv r(m)$; and then $\mathcal{U}(G_I)\cong A_{10m.r_1}$ and the latter is of order $(2n)^2$ over its center.*

We remark that all the Kronecker products mentioned above are products over Q.

To prove our results we need a result on Kronecker products. Let $\mathfrak{A}$ be an algebra over a commutative ring Z[8] possessing the unit of A and let $\mathfrak{B}$ be an algebra over a subring T of Z, then: (*) $\mathfrak{A}\otimes_Z(\mathfrak{B}\otimes_T Z)\cong\mathfrak{A}\otimes_T\mathfrak{B}$. This isomorphism is clearly obtained by mapping $a\otimes(b\otimes z)\to az\otimes b$. We apply this result iteratively to the following situation: $\mathfrak{A}$ be a Z_1 algebra and $\mathfrak{B}$ be a Z_2-algebra and Z_1, Z_2 are $\mathfrak{T}$-algebras. Put $Z_1\otimes_T Z_2=Z$, then we show that (**) $(\mathfrak{A}\otimes_{Z_1}Z)\otimes_Z(\mathfrak{B}\otimes_{Z_2}Z)\cong\mathfrak{A}\otimes_T\mathfrak{B}$. Indeed, applying (*) to the left-hand side we obtain that the latter is isomorphic with $(\mathfrak{A}\otimes_{Z_1}Z)\otimes_{Z_2}\mathfrak{B}$. Now apply (*) to $\mathfrak{A}\otimes_{Z_1}Z=\mathfrak{A}\otimes_{Z_1}(Z_1\otimes_T Z_2)=\mathfrak{A}\otimes_T Z_2$. Applying again (*) to $(\mathfrak{A}\otimes_T Z_2)\otimes_{Z_2}\mathfrak{B}$

[8] Assuming $az=za$, $z\in Z$, $a\in A$.

after interchanging the factors yields that the latter is isomorphic with $A \otimes_T B$.

If Z_1, Z_2 are fields linearly disjoint over a subfield T, then $Z = Z_1 \otimes_T Z_2$ is isomorphic with the composition field $Z_1 Z_2$. We shall apply this to the case $\mathfrak{A}$ which is a central simple algebra over Z_1 and $\mathfrak{B}$ a central simple algebra over Z_2 and $T = Q$. Then $\mathfrak{A} \otimes_{Z_1} Z = \mathfrak{A}_Z$ and $\mathfrak{B} \otimes_{Z_2} Z = \mathfrak{B}_Z$ simply means the algebras obtained from $\mathfrak{A}$ and $\mathfrak{B}$ respectively by extending their center to Z. Thus $\mathfrak{A} \otimes_Q \mathfrak{B} = \mathfrak{A}_Z \otimes_Z \mathfrak{B}_Z$. The latter is well known to be also central simple; hence $\mathfrak{A} \otimes_Q \mathfrak{B}$, in this case, is also simple.

Let $G = H \times G_{m,r}$ where G is a T-group if $H = \mathfrak{T}^*$, an O-group if $H = \mathfrak{O}^*$, etc. If $G \subseteq \mathfrak{R}^*$ then clearly $\mathcal{U}(G)$ is a homomorphic image of $\mathcal{U}(H) \otimes_Q \mathcal{U}(G_{m,r})$ as we shall see in all cases the center Z_H of $\mathcal{U}(H)$ is linearly disjoint from the center $\mathfrak{Z}_{m,r}$ of $\mathcal{U}(G_{m,r})$ over Q; hence the preceding remark yields that $\mathcal{U}(H) \otimes_Q \mathcal{U}(G_{m,r})$ is simple. Consequently $\mathcal{U}(G) \cong \mathcal{U}(H) \otimes_Q \mathcal{U}(G_{m,r})$.

To prove that the centers of $\mathcal{U}(H)$ and $\mathcal{U}(G_{m,r})$ are linearly disjoint over Q we turn to the different cases: If G is a T-group, $H = \mathfrak{T}^*$, the center of $\mathcal{U}(H)$ is Q by Lemma 4, and this case is trivial. If G is an O-group, then $Z_H \subseteq \mathcal{C}_8$, and the center of $\mathcal{U}(G_{m,r})$, $\mathfrak{Z}_{m,r} \subseteq \mathcal{C}_m$. For this group, it was assumed that $(m, 8) = 1$, and then, clearly, $\mathcal{C}_m$ and $\mathcal{C}_8$ are linearly disjoint over Q. For I-groups, $Z_H \subseteq \mathcal{C}_{10}$, $\mathfrak{Z}_{m,r} \subseteq \mathcal{C}_m$ and by assumption $(m, 10) = 1$, and the rest is similar.

The remarks stated before these theorems clearly prove that if $\mathfrak{A}_2 \otimes \mathfrak{A}_{m,r}$ is a division algebra then it contains the group $\mathfrak{T}^* \times G_{m,r}$, and similarly for the other types. The rest of the proof of these parts of the theorem will follow immediately by the following lemma:

LEMMA 15. *If* $(m_1, m_2) = (n_1, n_2) = 1$, *where* n_i *are given by* (3A), *then* $\mathfrak{A}_{m_1,r_1} \otimes_Q \mathfrak{A}_{m_2,r_2} \cong \mathfrak{A}_{m,r}$ *with* $m = m_1 m_2$ *and* $r \equiv r_i \pmod{m_i}$. *Furthermore, the numbers* s, n, t *defined by* (3A) *are* $n = n_1 n_2$, $s = s_1 s_2$ *and* $t = t_1 t_2$.

As in the preceding proof, one readily verifies that (m_1, m_2) implies that the centers of $\mathfrak{A}_{m_i,r_i} (\subseteq \mathcal{C}_{m_i})$ are linearly disjoint over Q, hence the product considered is a simple algebra. The isomorphism of the lemma is readily seen to be obtained by the mapping: $\epsilon_{m_1} \otimes \epsilon_{m_2} \to \epsilon_{m_1 m_2} \in \mathcal{C}_m$ and $\sigma_{r_1} \otimes \sigma_{r_2} \to \sigma_r$. Since $(n_1, n_2) = 1$ it follows readily that σ_r is an automorphism of order $n = n_1 n_2$. The fact that $t = t_1 t_2$ will follow immediately by showing that $s = s_1 s_2$. To prove this, note that since $r - 1 = r_i - 1 \pmod{m_i}$ and $s_i = (r_i - 1, m_i)$ it follows that $s_i \mid s = (r - 1, m)$; hence $s_1 s_2 \mid s$. On the other hand, clearly, $s = s_1' s_2'$ where $s_i' \mid m_i$. Hence, since $r_i - 1 \equiv r - 1 \pmod{m_i}$ it follows that $s_i' \mid (r_i - 1, m_i) = s_i$. This shows that $s = s_1' s_2' \mid s_1 s_2$. Consequently $s = s_1 s_2$. q.e.d.

To complete the proof of the three parts of Theorem 6 it remains now to verify that the algebras considered there satisfy the requirements of the last lemma. This is readily achieved and in particular one observes that $n_1 = 2$ and n_2 is an odd integer. Furthermore, in the first two cases the numbers ob-

gained satisfy (3D) and in the last case they satisfy (3C).

6. The classification.

LEMMA 16. *Let $G\subseteq K^*$. $G\cong G_{m,r}$ if and only if G is either of type* (2A) *or contains a subgroup G_1 of type* (2A) *which is of index 2 in G.*

If G is isomorphic with $G_{m,r}$, then since G is either of type (2A) or (2B) it follows by Lemmas 1 and 2 that either $(n,t)=1$ or $(n,t)=2$. In the first case G is of type (2A) and in the second case, in view of Lemma 2, one can show that $\{B^{n/2}, A\}=G_1$ generates a group of type (2A) and of index 2 in G.

Conversely, if G is of type (2A) it follows by Lemma 1 that $G\cong G_{m,r}$. Let G be not of type (2A) but containing G_1 which is of type (2A) and $(G:G_1)=2$. By Theorem 2 it follows that G is of type (2B), and evidently G is solvable since G_1 is solvable. It follows now by the proof of Z7 (§2, p. 203) that if $G_1\cong G_{m,r}$ of the type satisfying (3A), (3B) and (3C), then $G=\{R, A, B\}$ where $\{A, B\}=G_1$ and either G_1 is cyclic and

$$RAR^{-1}=A^l,\qquad l^2\equiv 1(n),\qquad R^4=1, \tag{6A}$$

or G_1 is not cyclic and:

$$RAR^{-1}=A^l,\qquad RBR^{-1}=B^l,\qquad R^4=1, \tag{6B}$$
$$l^2\equiv 1(m),\qquad l\equiv 1(n).$$

If (6A) holds then $G_1=\{A\}$ and $G/G_1=\{RG_1\}$, hence by Lemma 3 $G\cong G_{m,r}$.

If (6B) holds we distinguish between two cases: (1) n is odd, (2) n is even. Let n be odd, then the quotient $G/\{A\}$ is an abelian group of order $2n$ or $4n$, since, by (6B), $RBR^{-1}B^{-1}=B^{l-1}=A^{t(l-1)/n}\in\{A\}$. Since n is odd, this quotient is, clearly, a cyclic group, hence Lemma 3 implies that $G\cong G_{m,r}$.

Let n be even. As in previous proofs (of Lemma 5) we obtain $R^2=-1$. Thus, in particular, it follows that R^2 belongs to the center of G. Let $\mathcal{U}_1=\mathcal{U}(G_1)\subseteq\mathfrak{K}^*$. Since G_1 is normal in G, the inner automorphism: $X\to RXR^{-1}$ of $\mathfrak{K}^*$ induces an automorphism ρ of order 2 in $\mathcal{U}_1$. It follows by Theorem 3 that $\mathcal{U}_1$ is a central simple algebra of order n^2 over its center $\mathfrak{Z}_1$, from this we assert that ρ must be inner in $\mathcal{U}_1$. If ρ were an outer automorphism, then it follows by [7, Theorem 4] that $\mathcal{U}_1=\mathfrak{A}_1\otimes\mathfrak{Z}_1$ where ρ is an automorphism of $\mathfrak{Z}_1$ with the invariant subfield $\mathfrak{L}_1$ and $\mathfrak{A}_1$ is a division algebra of order n^2 over $\mathfrak{L}_1$, invariant under ρ. The elements of $\mathcal{U}(G)=\mathcal{U}$ have the form $a+bR$, $a, b\in\mathcal{U}_1$, and consider the algebra $\mathfrak{A}_1\otimes(\mathfrak{Z}_1, \rho, -1)=\overline{\mathcal{U}}$, whose elements are readily seen to be of the form $a+b\rho$, $a, b\in\mathfrak{A}_1\otimes\mathfrak{Z}_1$. One readily verifies that the mapping $a+b\rho\to a+bR$ determines a homomorphism of $\overline{\mathcal{U}}$ onto $\mathcal{U}$. Since the first is simple and $\mathcal{U}\neq 0$, this mapping is actually an isomorphism. Consequently, $\mathcal{U}\cong\mathfrak{A}_1\otimes(\mathfrak{Z}_1, \rho, -1)$ is a division algebra of order $(2n)^2$ over $\mathfrak{L}_1$. Since n is even $(\mathfrak{Z}_1, \rho, -1)^n$ is a matrix algebra; hence $\mathcal{U}^n=\mathfrak{A}_1^n\otimes(\mathfrak{Z}_1, \rho, -1)^n$ is also a matrix algebra. This is impossible, since by the Hasse-Brauer-

Noether theorem (e.g. [5, Satz 7, p. 119]) the index of division algebras ($2n$ in our case) over algebraic number fields is equal to their exponent ($\leqq n$ in our case).

Thus ρ is inner in $\mathcal{U}_1$. Let $\overline{R}\in\mathcal{U}_1$ be the element which induces ρ. By the proof of Lemma 4 it follows that $\overline{R}=\sum_{\nu=0}^{n-1} a_\nu B^\nu$, $a_\nu\in Q(A)$. Hence, (6B) yields that $(\sum_{\nu=0}^{n-1} a_\nu B^\nu)A=A^l(\sum_{\nu=0}^{n-1} a_\nu B^\nu)$. This implies, in view of (3B), that $a_\nu A^{r^\nu}=a_\nu A^l$. Hence, $a_\nu=0$ unless $r^\nu\equiv l(m)$. Since $\overline{R}\neq 0$, $r^\nu\equiv l(m)$ for some $0\leqq\nu<n-1$. The facts that $l^2\equiv 1(m)$ and that r generates a cyclic group of order n mod m imply that either $\nu=0$ or $\nu=n/2$.

If $\nu=0$, then it follows that $l\equiv 1(m)$. Thus (5A) implies that A and R commute. Consequently $N=\{A, R\}$ is an abelian subgroup of $\mathfrak{R}^*$ and, therefore, cyclic. Furthermore N is normal in G, since $B^{-1}AB=A^{-r}\in N$ and by (6B), $B^{-1}RB=B^{l-1}R=A^{t(l-1)/n}R\in N$. Clearly $G/N=\{BN\}$ is cyclic, hence by Lemma 3, $G\cong G_{m,r}$.

If $\nu=n/2$ put $Q=RB^\nu$. Then by (6B) it follows that Q and A commute and as this implies that $N=\{Q, A\}$ is cyclic. N is normal in G, for $B^{-1}RB^\nu B=B^{-1}RB\cdot B^\nu=A^{t(l-1)/n}(RB^\nu)\in N$. The rest follows as in the previous case. This concludes the proof of the lemma.

The groups of odd order always satisfy the preceding lemma, hence:

COROLLARY 2. *The groups of odd order which can be embedded in division rings are either cyclic or D-groups.*

LEMMA 17. *The only solvable subgroups of division algebra are either cyclic, D-group, T-groups or O-groups.*

By Theorem 2, it follows that if $G\subseteq\mathfrak{R}^*$, G satisfies the conditions of Z7. We follow the four different possible types of groups as given in the proof of Z7. If G is either of type (2A) or contains a subgroup G_1 of type 2A of index 2 (§1 and §2 of [8, p. 203]) then by the previous lemma it follows that either G is cyclic or a D-group. The other possible cases, in view of §3, §4 of the proof of Z7 [8, pp. 203–204], satisfy either:

(6C) G contains a normal subgroup G_3 of index 3 in G and $G_3=S_2\times G_2$, where $S_2=\{P, Q\}$ is a quaternion group of order 8 (the 2-Sylow subgroup of G) and G_2 is a group of type (2A) of odd order.

(6D) The commutator G' of G is of type (6C) and $(G:G')=2$.

Consider first the case (6C). Since $(G:G_3)=3$, we may assume that G/G_3 is generated by a coset RG_3 where $R^{3^\beta}=1$. The groups S_2 and G_2 are characteristic subgroups of G_3, since S_2 is the only 2-Sylow subgroup of G_3 and G_2 is characterized as the set of elements of G_3 which commute with the elements of S_2. Hence, $RS_2R^{-1}=S_2$ and $RG_2R^{-1}=G_2$. If the inner automorphism $X\to RXR^{-1}$ of G induces the identity in S_2, then $\{R, P, G_2\}$ will then generate a group G_1 of type (2A) and of index 2 in G, which is impossible since G is assumed not to be of the previous cases. Now the only automorphisms of odd order of the quaternion group are σ, σ^2 where σ: $P\to Q$, $Q\to PQ$. Without loss

of generality we may assume that R induces σ. Hence, by Lemma 5, $\beta=1$ and $R=-(1+P+Q+PQ)/2$. This in turn yields that the elements of G_2 which commute with P and Q commute also with R, hence $G=\{P, Q, R\}\times G_2$. As was mentioned before G_2 is of odd order. Furthermore, the order of G_2 is prime to 3, otherwise R and the 3-Sylow subgroup of G_2 would generate an abelian non cyclic subgroup of G which is impossible. This proves that G is a T-group.

Let (6D) hold. Then $(G:G')=2$ and G' is by the preceding case a T-group, i.e. $G'=\mathfrak{T}^*\times G_{m,r}$ and $T^*=\{P, Q, R\}$ satisfying $(T_1)-(T_3)$. Furthermore, $G_{m,r}$ is of odd order. Let $T\in G$, $T\notin G'$ and $T^{2^\gamma}=1$. Then T^2 belongs to the unique 2-Sylow subgroup of G', i.e. to $\{P, Q\}$. This readily implies, in view of the fact that G must be a group of type (2B), that $\gamma=3$, i.e. $T^8=1$. By a suitable change of the symbols P, Q or PQ if necessary, and replacing R by R^2 (if necessary), we can thus obtain that T, P, Q and R will satisfy Corollary 1. Hence, this corollary implies that $\{T, Q, R\}=\{T, \mathfrak{T}^*\}\cong\mathfrak{D}^*$. To prove that $G\cong\mathfrak{D}^*\times G_{m,r}$ it suffices to show that T commutes with $G_{m,r}$. Clearly $\mathfrak{T}^*$ is a characteristic group of G', and $G_{m,r}$ can be characterized as the set of elements which commute with P and Q, hence $G_{m,r}$ is also a characteristic subgroup of G'. Thus $TG_{m,r}T^{-1}=G_{m,r}$. This implies that the mapping $\tau: X\to TXT^{-1}$ induces an automorphism of $\mathfrak{U}(G_{m,r})$. If τ is inner in $U(G_{m,r})$ it must be identity. Since, then τ is induced by an element $\overline{T}$ and $\overline{T}^2=\lambda\in\mathfrak{Z}_{m,r}$ the center of $\mathfrak{U}(G_{m,r})$. τ is the identity if $\lambda^{1/2}\in\mathfrak{Z}_{m,r}$. If it were not then $\mathfrak{Z}_{m,r}(\lambda^{1/2})$ is an extension of order 2 of $\mathfrak{Z}_{m,r}$ contained in the algebra $\mathfrak{U}(G_{m,r})$, which is, by Theorem 3, a division algebra of order n^2 over $\mathfrak{Z}_{m,r}$. Hence $2\mid n$ (e.g. [1, Theorem IV, 21, p. 60], which is impossible since $G_{m,r}$ is of odd order. If τ is not inner in $\mathfrak{U}(G_{m,r})$ it cannot leave the center of $\mathfrak{U}(G_{m,r})$ invariant ([7, Theorem 4]). On the other hand, by Theorem 6b, $\mathfrak{U}(T^*\times G_{mr})\cong\mathfrak{A}_{4m,r_1}$ and, therefore, it is a division algebra of order $(2n)^2$ over its center. Furthermore $\tau: X\to TXT^{-1}$ induces an automorphism of $\mathfrak{U}(T^*\times G_{m,r})$; hence one proves in a similar way to the proof of the second case (6B) (n even) of Lemma 6 that τ must be inner. Thus τ leaves the center of this algebra and, therefore, of $\mathfrak{U}(G_{m,r})$ invariant. This is a contradiction and the proof is thus completed.

LEMMA 18. *The non solvable subgroups of division algebras are I-groups.*

Indeed, in view of Theorem 1, Z16 can be applied to these groups. Hence, if $G\subseteq\mathfrak{R}^*$ is not solvable, either $G\cong\mathfrak{J}^*\times G_{m,r}\cong M(2, 5)\times G_{m,r}$ where the order of $G_{m,r}$ is relatively prime to 120, or G has a subgroup G_1 of this type and $(G:G_1)=2$. In the first case, G is an I-group by definition and we now show that the existence of the second case leads to a contradiction.

Let $G_1=\mathfrak{J}^*\times G_{m,r}$ and $(G:G_1)=2$. Then the 2-Sylow subgroup of G is of order 16, hence by (2B) it follows that there exists an element $T_0\in G$ of order 8. This readily implies that $P_0=T_0^2\in\mathfrak{J}^*$ and P_0 is an element of order 4. Since all elements of order 4 of $\mathfrak{J}^*$ are conjugates (which follows by the existence

of an element $R\in\mathfrak{J}^*$ satisfying (T_2)), in particular conjugate with P_0, it follows that for any $P\in\mathfrak{J}^*$ of order 4 there exists a $T\in G$ such that $T^2=P$ and clearly $T\notin G_1$. Now, $T\mathfrak{J}^*T^{-1}=\mathfrak{J}^*$ since $\mathfrak{J}^*$ contains and it is generated by all Sylow subgroups of G_1 belonging to the primes 2, 3, 5. Hence the mapping: $X\to TXT^{-1}$, $X\in\mathcal{U}(\mathfrak{J}^*)$ induces an automorphism of $\mathcal{U}(\mathfrak{J}^*)$. Following the method of proof of case (6B) of Lemma 16, one shows that since $\mathcal{U}(\mathfrak{J}^*)$ is of even order over its center, this automorphism is necessarily inner. That is, $TXT^{-1}=T_0XT_0^{-1}$ for some $T_0\in\mathcal{U}(\mathfrak{J}^*)$. Hence $T=T_0a$, where $a\in\mathcal{U}(G)$ and commutes with the elements of $\mathcal{U}(\mathfrak{J}^*)$, in particular with T_0. It follows now, in view of Lemma 14 that $\mathcal{U}(\mathfrak{J}^*, T)$ is a quaternion algebra over the field $Z=Q(5^{1/2}, a)$. The proof of Lemma 14 shows that $\mathfrak{J}^*$ contains elements P, S satisfying: $S^5=1$, $P^4=1$, $PSP^{-1}=S^{-1}$. Choose T so that $T^2=P$. Then T commutes with P hence $T\in Z(P)$. Since $P^2+1=0$, one readily observes that $T=\pm(1+P)/2^{1/2}$. Consider the element $ST=\pm(S+SP)/2^{1/2}\in G$. The minimal equation of ST over Z is clearly $x^2\mp((S+S^{-1})/2^{1/2})x+1=0$. Since ST is an element of finite order u in $\mathfrak{R}^*$ it follows that there is a root of unity ϵ_u satisfying $\epsilon_u^2\mp((\epsilon+\bar{\epsilon})/2^{1/2})\epsilon_u+1=0$, where $\epsilon=\epsilon_5$ is a fifth root of unity and $\bar{\epsilon}$ is its conjugate. This implies that the real subfield of $Q(\epsilon_u)$ is $Q((\epsilon+\bar{\epsilon})/2^{1/2})$ which is readily seen to be $Q(5^{1/2}, 2^{1/2})$. Since the latter is of degree 4 over Q it follows that $\phi(u)=(Q(\epsilon_u):Q)=8$, hence, $u=16$, 20 or $u=30$. But in the first case $5^{1/2}\notin Q(\epsilon_{16})$ and in the other cases $2^{1/2}\notin Q(\epsilon_u)$. Contradiction.

We are now in position to complete the proof of our main theorem:

THEOREM 7. *A group G can be embedded in a division ring if and only if G is one of the following types*:

(1) *Cyclic group.*

(2) *A D-group $G_{m,r}$, where the integers m, r etc. satisfy Theorem* 4 *or Theorem* 5.

(3) *A T-group $\mathfrak{T}^*\times G_{m,r}$ where $G_{m,r}$ is either cyclic of order m, or of the preceding type, and in both cases, for all primes $p\mid m$ the minimal integer γ_p satisfying $2^{\gamma_p}\equiv 1(p)$ is odd*(9).

(4) *The groups $\mathfrak{O}^*$, $\mathfrak{J}^*$.*

In view of Lemmas 16, 17 and Theorem 4, it remains only to prove that every T-group satisfying the requirement of the preceding theorem satisfies (3) and the only O-group and I-groups satisfying our requirements are $\mathfrak{O}^*$ and $\mathfrak{J}^*$.

We start with the O-groups. Let G_p be a cyclic group of prime order p, $(p, 6)=1$. Consider the group $G=\mathfrak{O}^*\times G_p$. By Theorem 6b it follows that G can be embedded in a division ring if and only if $\mathfrak{A}_{8p,r}$ is a division algebra when $r\equiv -1(8)$ and $r\equiv 1(p)$. Thus the numbers satisfying (3A) are $n=2$, $s=2$, $t=4p$ and $m=8p$. Applying Theorem 4 (or 5) to this case we see that (2b) never holds. In view of Lemma 6 it follows that if for $q\mid n=2$ there exists

(9) This is equivalent to saying that 2 is a root of one of odd order mod m.

a prime p so that $q \nmid n_p$ then we must have $q=p=2$ and (3D) holds. But here we have $m/4 \equiv 0 \pmod 2$ which contradicts (2c) of Theorem 5. Consequently, the required algebra $\mathfrak{A}_{8p,r}$ is not a division algebra, and clearly this implies that O-groups $\mathfrak{D}^* \times G_{m,r}$ where the latter is not the identity cannot be embedded in division algebra. $\mathfrak{D}^*$ can be embedded, by the remarks preceding Theorem 6a.

Applying again Theorem 6c and Theorem 5 we wish to show that a group $\mathfrak{I}^* \times G_p$, $(p, 120)=1$, cannot be embedded in a division ring. Indeed, by Theorem 6c this is equivalent to proving that $\mathfrak{A}_{10p,r}$ is not a division ring, where $m=10p$, $r \equiv -1(10)$ and $r \equiv 1(p)$. The numbers satisfying (3A) will be in this case $n=2$, $s=2$, $t=5p$. To apply Theorem 5 we observe that (1) and (2a) and (2c) of that theorem are never valid. Furthermore $\beta(2, s)=1$, $\beta(2, m)=1$ and $\beta(2, p_q-1) \geqq 1$ where p_q is the prime required by Theorem 5 which in our case is either p or 5. If $p_q=5$, then $\beta(2, p_q-1)=2$ which contradicts (2a) the only possible condition since $5 \equiv 1 \pmod 4$. If $p_q=p$ then $n_p=2$ so that $2 \mid n_p$ and thus none of the conditions of (2) of Theorem 5 can hold. From this we conclude, as for O-groups before, that the only I-group which can be embedded in a division ring is $\mathfrak{I}^*$. This completes the proof of (4).

To prove (3), we observe that in view of Theorem 6a our problem is equivalent to the condition that the algebra $\mathfrak{A}_{4m,r_1}$ is a division algebra. Assume that $G_{m,r}$ is of odd order and satisfies the requirement (2) of our theorem. The numbers involved in $\mathfrak{A}_{4m,r_1}$ satisfying (3A) and Theorem 6 will be: $\bar{m}=4m$, $\bar{r}=r_1$, where by Theorem 6a $\bar{r} \equiv -1(4)$, $\bar{r} \equiv r(m)$. Furthermore, $\bar{n}=2n$ since $G_{m,r}$ is of odd order, and one readily observes that $\bar{s}=2s$. Clearly, for every prime $p \mid m$, $\bar{n}_p=2n_p$ since n_p is odd, and $\bar{n}_2=n$.

If $q \mid \bar{n}$ and $q \neq 2$, then $q \mid n$ and by assumption that (2) holds for $G_{m,r}$, i.e. by Theorem 6 there exist a prime $p \mid m$ and therefore $p \mid \bar{m}$ such that $q \nmid n_p$, and since $q \neq 2$, $q \nmid \bar{n}_p$ and (2a) of Theorem 5 holds. That is:

$$\beta(q, s) \geqq \beta(q, p-1) + \operatorname{Max} \beta(q, \gamma_j), \quad \text{where} \quad \gamma_j = \gamma(p, p_j)$$

is defined for all primes $p_j \mid m$. In order to show that this condition should hold in our case, one first notices that $\beta(q, s)=\beta(q, \bar{s})$ and the only additional term to appear in the Max is $\beta(q, \gamma')$ where γ' is the minimal integer satisfying $p^{\gamma'} \equiv 1(2)$. Since p is odd, $\gamma'=1$ hence $\beta(q, \gamma')=0$ and this condition is valid also in our case. It remains, therefore, to consider the case $q=2$. Now for every odd prime $\bar{n}_p=2n_p$ hence p must be even, so that (2a) and (2b) Theorem 5 can never hold; and in order that (2c) of that theorem should hold we must require $\gamma_j \equiv 1(2)$ for every prime $p_j \mid m$. This proves (3).

Immediate consequences of the preceding theorem are:

COROLLARY 3. *The subgroups of division algebras of order* $\neq 120, 48$ *are cyclic or D-groups.*

COROLLARY 4. *The only nonsolvable subgroup of division rings is* $\mathfrak{J}^*$.

7. **Subgroups of given division rings.** We utilize the preceding results to obtain some relations between the finite subgroups of a division ring and the algebra itself.

Let $G \subseteq \mathfrak{K}^*$ be of order g. If G is a T-group, $\mathfrak{D}^*$ or $\mathfrak{J}^*$, then $4 \mid g$. If G is a D-group then $g = nm = nst$. It follows by Lemma 5 that $g = n^2(s/n)t$. Hence,

COROLLARY 5. *If* $G \subseteq \mathfrak{K}^*$ *and the order of* G *is square free, then* G *is cyclic.*

Let $\mathfrak{K}$ be a division algebra of order k^2 over its center $\mathfrak{L}$. If $G \subseteq \mathfrak{K}^*$ (of order g) then, by Theorem 3, $\mathfrak{U}(G) = \mathfrak{A}_{m,r}$ and the latter is of order n^2 over its center. It follows, therefore, that $n \mid k$. Hence $n^2 \mid k^2$. In all possible cases, one verifies with the aid of Lemma 10 that $n^2 \mid g$. Hence,

THEOREM 8. *If* $G \subseteq \mathfrak{K}^*$ where $\mathfrak{K}$ *is of order* k^2 *over its center, then if* (g, k^2) *is square free,* G *is necessarily cyclic.*

In particular, this yields Theorem 7 of [6]:

COROLLARY 6. *The odd subgroups of the quaternions are cyclic.*

Another immediate consequence is that

COROLLARY 7. *If* k *is odd then the subgroups of* $\mathfrak{K}^*$ *are* D*-groups, or cyclic.*

Since otherwise $n \mid k$ and $n \equiv 0(2)$ by Theorems 6a–6c. Furthermore:

THEOREM 9. *If* $\mathfrak{K}$ *is a division algebra of order* k^2 *over* $\mathfrak{L}$ *and* $G \subseteq \mathfrak{K}^*$ *where* G *is a group of type* (2B), *then* $\mathfrak{K} = \mathfrak{A}_2 \otimes_Q \mathfrak{A}$ *where* $\mathfrak{A}_2$ *is the quaternion algebra over the rational and* $\mathfrak{A}$ *is an algebra of order* $(k/2)^2$ *over* $\mathfrak{L}$. *If* $\mathfrak{L}$ *is an algebraic number field then* $k/2$ *is odd.*

If G is of type (2B), then G contains a quaternion group $\{P^{2^{\alpha-2}}, Q\}$. Hence $\mathfrak{K} \supseteq \mathfrak{U}(P^{2^{\alpha-2}}, Q) = \mathfrak{A}_2$. By [1, Theorem IV 6, p. 51] it follows that $\mathfrak{K} = (\mathfrak{A}_2 \otimes_Q L) \otimes_L \mathfrak{A} = \mathfrak{A}_2 \otimes_Q \mathfrak{A}$. If $k' = k/2$ is even then $\mathfrak{K}^{k'} \cong \mathfrak{A}_2^{k'} \otimes \mathfrak{A}^{k'}$ is a matrix ring, so that the exponent of $\mathfrak{K}$ is $\leq k' < k$. Since $\mathfrak{L}$ is an algebraic number field it follows by the Hasse-Brauer-Noether theorem [5, Satz 7, p. 119] that $\mathfrak{K}$ is not a division algebra. Contradiction.

With this we are able to show:

THEOREM 10. *If an algebra* $\mathfrak{K}$ *of order* k^2 *over an algebraic number field* $\mathfrak{L}$ *contains an* $\mathfrak{D}^*$ *then* $2^{1/2} \in \mathfrak{L}$. *If* K *contains an* $\mathfrak{J}^*$ *then* $5^{1/2} \in \mathfrak{L}$.

Indeed, if $\mathfrak{D}^* \subseteq \mathfrak{K}^*$, then $\mathfrak{K}$ contains a field $Q(S) \cong Q(\epsilon_8)$ which is of order 4 over Q. If $Q(S) \cap \mathfrak{L} = Q$ then one readily verifies $(\mathfrak{L}(S) : \mathfrak{L}) = 4$ and, therefore, $4 \mid k$ which contradicts the preceding theorem. Furthermore, $Q(S) \not\subset L$ since S does not belong to the center of $\mathfrak{D}^*$. Hence $Q \subset Q(S) \cap L \subset Q(S)$. The unique subfield of $Q(S)$ different from Q or $Q(S)$ is $Q(2^{1/2})$, hence $2^{1/2} \in Q(S)$. A similar proof holds for $\mathfrak{J}^*$.

8. **The real quaternions.** We determine now the subgroups of the real quaternions $\mathfrak{A}_\mathfrak{R} = \mathfrak{A}_2 \otimes \mathfrak{R}$. It follows immediately by Theorem 3 and Theorem 7 that the subgroups of $\mathfrak{A}_\mathfrak{R}$ are either cyclic, D-groups for which $n=2$, T-groups of the form $\mathfrak{T}^* \times G_m$ where G_m is cyclic or the groups $\mathfrak{O}^*$, $\mathfrak{J}^*$. The latter were shown to be contained in $\mathfrak{A}_\mathfrak{R}$. Since $\mathfrak{A}_\mathfrak{R} \supseteq \mathfrak{R}(i)$ which is the complex field, the quaternion contains cyclic groups of any given order. If a D-group $G_{m,r} \subseteq \mathfrak{A}_\mathfrak{R}$, with $n=2$, then we assert that $r \equiv -1(m)$. Indeed, if $r \not\equiv -1(m)$ then $r \equiv 1(m_1)$, $r \equiv -1(m_2)$ for some divisors m_1, m_2 of m satisfying $m = m_1 m_2$. Hence by (3B) it follows that if $G_{m,r} = \{A, B\}$, A^{m_2} belongs to the center of $G_{m,r}$ and hence also to the center of $\mathfrak{A}_\mathfrak{R}$. The latter is the real field $\mathfrak{R}$ and the only roots unity belonging to $\mathfrak{R}$ are ± 1. Hence $A^{m_2} = -1$, and consequently $m_1 = 2$. But $r \equiv 1 \not\equiv -1(2)$, and therefore $r \equiv -1(m)$. These groups $G_{m,-1}$ are known as the *binary dihedral* groups and they are readily seen actually to belong to $\mathfrak{A}_\mathfrak{R}$. The same reasoning yields that if $G = \mathfrak{T}^* \times G_m \subseteq \mathfrak{A}_\mathfrak{R}^*$ then since G_m belongs to the center of G, $G_m \subseteq \mathfrak{R}$, but then the fact that G_m is odd yields that $G_m = 1$. It was shown before that $\mathfrak{T}^* \subseteq \mathfrak{A}_\mathfrak{R}$. This completes the proof of the following:

THEOREM 11. *The finite subgroups of the real quaternions are the cyclic group of any order, the binary dihedral group of order $4m$, the groups $\mathfrak{T}^*$, $\mathfrak{J}^*$, and $\mathfrak{O}^*$.*

REMARK. There is a well known homomorphism of the group N of all quaternions of Norm 1 onto the orthogonal group O_3. This is obtained by considering the set $\mathfrak{S} = \{\zeta;\ \zeta = xi + yj + zk\}$ of $\mathfrak{A}_\mathfrak{R}$ as a Euclidean 3-space S_3 and to each $\eta \in N$ one corresponds the notation L_η of S_3 defined by $L_\eta \zeta = \eta \zeta \eta^{-1}$. The kernel of this homomorphism is the group containing $\{+1, -1\}$. From this one readily concludes that the finite subgroups of O_3 are the images of the finite subgroups of N which are the same as those of $\mathfrak{A}_\mathfrak{R}$. The image of the cyclic groups will be *cyclic*, of the binary dihedral groups will be the *dihedral groups* of order $2m$, and the images of T^*, O^*, and I^* are respectively the *tetrahedral* group, the *octahedral* group, and the *icosahedral* group([10]). This is the well known classification of the finite subgroups of O_3.

BIBLIOGRAPHY

1. A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloquium Publications, vol. 24, 1939.

2. E. Artin, *Algebraic numbers and algebraic functions* I, Princeton, 1951.

3. W. Burnside, *On finite groups in which all Sylow subgroups are cyclic*, Messenger of Mathematics vol. 35 (1905) pp. 46–50.

4. ———, *On a general property of finite irreducible groups of linear substitutions*, Messenger of Mathematics vol. 35 (1905) pp. 51–55.

5. M. Deuring, *Algebren*, New York, Chelsea, 1948.

6. I. N. Herstein, *Finite multiplicative subgroups in division rings*, Pacific Journal of Mathematics vol. 1 (1953) pp. 121–126.

([10]) This was also shown by Sono, Tôhoku Math. J. vol. 4 (1913) pp. 114–119.

7. N. Jacobson, *The fundamental theorem of the Galois theory for quasi-fields*, Ann. of Math. vol. 41 (1940) pp. 1–7.

8. H. Zassenhaus, *Über endliche Fastkörper*, Hamb. Abhand. vol. 11 (1936) pp. 187–220.

9. G. Vincent, *Les groupes linéaires finis sans points fixés*, Comment. Math. Helv. vol. 20 (1947) pp. 117–171.

HEBREW UNIVERSITY,
JERUSALEM, ISRAEL.
THE INSTITUTE FOR ADVANCED STUDY,
PRINCETON, N. J.

ERRATA, VOLUME 78

Summation of bounded divergent sequences, topological methods. By Albert Wilansky and Karl Zeller. Pages 501–509.

Page 502, lines 24–25. The conjecture is now known to be false.

Page 507, lines 24–26. For "For each $n \cdots a_{nk}$ otherwise." read "Let $\{k(n)\}$ be a strictly increasing sequence of indices so chosen that for each n, $|s_n/s_{k(n)}| < \epsilon/n$, $|s_{k(n)}/s_{k(n+1)}| < \epsilon/n$. Let $a_{nn}=1$; then, given n, if $n=k_m$, set $a_{n,k(m+1)} = -s_{k(m)}/s_{k(n+1)}$; while if $n \neq k_m$ for all m, set $a_{n,k(n)} = -s_n/s_{k(n)}$. In either case $a_{nk}=0$ for other k."

ERRATA, VOLUME 79

Arithmetical predicates and function quantifiers. By S. C. Kleene. Pages 312–340.

Page 325, last line of text. For "$z_{(t)O}$" read "$z_{(t)0}$".

Page 327, line 5. For "30" read "29".

Page 330, line 10. For "$R^{H_s Q}$" read "$R^{H_s Q}$".

Page 333, line 11. Insert at the end "a,".

Page 333, line 22. For "$2^{f_1} \cdot 3^{y_1}$" read "$2^{f_1} \cdot 3^{g_1}$".

Page 335. Beside Footnote 24 write "to page 338 line 4", and then interchange footnote numbers "(24)" and "(25)" both in the text (lines 6 and 17) and on the footnotes.

Page 336, formulas (22) and (23). For "R_y^H" read "R^{H_y}".

Page 338, line 4. For "$F_{y^*}^k$" read "F_y^k".