MULTIPlicative p-SUBGROUPS OF SIMPLE ALGEBRAs

MICHITAKA HIKARI

(Received May 1., 1972)

Amitsur ([1]) determined all finite multiplicative subgroups of division algebras. We will try to determine, more generally, multiplicative subgroups of simple algebras. In this paper we will characterize p-groups contained in full matrix algebras $M_n(\Delta)$ of fixed degree $n$, where $\Delta$ are division algebras of characteristic 0.

All division algebras considered in this paper will be of characteristic 0.

Let $\Delta$ be a division algebra. We will denote by $M_n(\Delta)$ the full matrix algebra of degree $n$ over $\Delta$. By a subgroup of $M_n(\Delta)$ we will mean a multiplicative subgroup of $M_n(\Delta)$. Further let $K$ be a subfield of the center of $\Delta$ and let $G$ be a finite subgroup of $M_n(\Delta)$. Now we define $V_K(G) = \{ \sum \alpha_i g_i \mid \alpha_i \in K, g_i \in G \}$. Then $V_K(G)$ is clearly a $K$-subalgebra of $M_n(\Delta)$ and there is a natural epimorphism $KG \rightarrow V_K(G)$ where $KG$ denotes the group algebra of $G$ over $K$. Hence $V_K(G)$ is a semi-simple $K$-subalgebra of $M_n(\Delta)$, which is a direct summand of $KG$. As usual $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ denote respectively the rational number field, the real number field, the complex number field and the quaternion algebra over $\mathbb{R}$.

If an abelian group $G$ has invariants $(e_1, \ldots, e_n)$, $e_n \neq 1$, $e_{i+1} | e_i$, we say briefly that $G$ has invariants of length $n$.

We begin with

**Proposition 1.** Let $n$ be a fixed positive integer and let $G$ be a finite abelian group. Then there is a division algebra $\Delta$ such that $G \subseteq M_n(\Delta)$ if and only if $G$ has invariants of length $\leq n$.

Proof. This may be well known. Here we give a proof. Suppose that there is a division algebra $\Delta$ such that $G \subseteq M_n(\Delta)$. An abelian group $G$ has invariants of length $\leq n$ whenever each Sylow subgroup of $G$ has invariants of length $\leq n$. Hence we may assume that $G$ is a $p$-group ($\neq 1$). Let $m$ be the length of invariants of $G$. Then $G$ contains the elementary abelian group $G_0$ of order $p^m$. We can write $QG_0 \cong \mathbb{Q} \oplus \mathbb{Q}(\varepsilon_p) \oplus \cdots \oplus \mathbb{Q}(\varepsilon_p^m)$ where $\varepsilon_p$ denotes the primitive $p$-th root of unity. Since $V_q(G_0)$ is a direct summand of $QG_0$ and $G_0 \subseteq V_q(G_0)$, we have $V_q(G_0) \cong \mathbb{Q}(\varepsilon_p) \oplus \cdots \oplus \mathbb{Q}(\varepsilon_p^m)$. On the other hand, since
Proposition 2. Let \( p \) be an odd prime and \( 0 < n < p \). Let \( P \) be a finite \( p \)-group. If there exists a division algebra \( \Delta \) such that \( P \subset M_n(\Delta) \), then \( P \) is abelian.

Proof. Let \( V_\mathbb{Q}(P) \approx M_{p^t}(\Delta_1) \oplus \cdots \oplus M_{p^t}(\Delta_t) \) be the decomposition of \( V_\mathbb{Q}(P) \) into simple algebras where each \( \Delta_i \) is a division algebra. Then we easily see that \( p^t + \cdots + p^1 \leq n \). Therefore, when \( n < p \), we have \( l_1 = \cdots = l_t = 0 \). Since \( p \) is odd, each division algebra \( \Delta_i \) is commutative \([3]\). Hence \( V_\mathbb{Q}(P) \) is commutative. This conclude that \( P \) is abelian. Q.E.D.

**Definition.** Let \( P_0 = \langle g \rangle \) be a cyclic group of order \( p \). Let \( P, P' \) be finite \( p \)-groups and let \( P_1, P_2, \ldots, P_p \) be the copies of \( P' \). We will call \( P \) a simple (1-fold) \( p \)-extension of \( P' \) if \( P \) is an extension of \( P_1 \times P_2 \times \cdots \times P_p \) by \( P_0 \) such that \( P^1 = P_1, \ldots, P^p = P_p, P^0 = P_0 \). It should be remarked that this extension does not always split. More generally, a finite \( p \)-group \( P \) will be called an \( n \)-fold \( p \)-extension of a finite \( p \)-group \( P' \), if there exist finite \( p \)-groups, \( P_0 = P', P_1, \ldots, P_{n-1}, P_n = P \) such that, for each \( 0 \leq i \leq n-1 \), \( P_{i+1} \) is a simple \( p \)-extension of \( P_i \).

Now we set

\[
T_p^{(0)} = \begin{cases} 
\{ \text{all cyclic } p \text{-groups} \} & \text{when } p \neq 2 , \\
\{ \text{all generalized quaternion } 2 \text{-groups} \} & \text{when } p = 2 ,
\end{cases}
\]

and \( \tilde{T}_p^{(0)} = \{ \text{all cyclic } p \text{-groups} \} \) for any prime \( p \). An element of \( T_p^{(0)} \) (resp. \( \tilde{T}_p^{(0)} \)) is called a \( p \)-group of 0-type (resp. \( \tilde{0} \)-type).

A finite \( p \)-group \( P \) is said to be of \( n \)-type (resp. \( \tilde{n} \)-type) if \( P \) is an \( n \)-fold \( p \)-extension of a \( p \)-group of 0-type (resp. \( \tilde{0} \)-type). We denote by \( T_p^{(n)} \) (resp. \( \tilde{T}_p^{(n)} \)) the set of all \( p \)-groups of \( n \)-type (resp. \( \tilde{n} \)-type).

Our main result is given the following

**Theorem.** Let \( n \) be a fixed positive integer and let \( P \) be a finite \( p \)-group. Then following conditions are equivalent:

1. \( P \) is a subgroup of \( M_n(H) \) (resp. \( M_n(C) \)).
2. There is a division algebra \( \Delta \) (resp. a commutative field \( K \)) such that \( P \subset M_n(\Delta) \) (resp. \( M_n(K) \)).
3. There exist non-negative integers, \( t, m_0, \ldots, m_t \) with \( \sum_{i=0}^t m_i \leq n \) and \( P_i^{(1)}, P_i^{(2)}, \ldots, P_i^{(m_i)} \in T_p^{(i)} \) (resp. \( \tilde{T}_p^{(i)} \)) for each \( 0 \leq i \leq t \) such that \( P \subset \prod_{i=0}^t \prod_{j=1}^{m_i} P_i^{(j)} \).

The following theorem plays an essential part in the proof of our main theorem.

**Theorem** (Witt-Roquette \([3], [4]\)). Let \( P \) be a \( p \)-group. Let \( K \) be a
commutative field of characteristic 0. Suppose that one of the following hypotheses is satisfied.

(a) $p \neq 2$,
(b) $p = 2$ and $\sqrt{-1} \in K$.
(c) $p = 2$ and $P$ does not contain a cyclic subgroup of index 2.

Then if $\chi$ is a nonlinear irreducible faithful character of $P$ there exists $P_0 \triangleleft P$ and a character $\zeta$ of $P_0$ such that $|P: P_0| = p$, $\chi = \zeta^p$ and $K(\chi) = K(\zeta)$.

From this theorem the following remark follows directly.

REMARK. If $K$ is an algebraic number field in this theorem, each division algebra equivalent to a simple component of $KP$ is an algebraic number field or a quaternion algebra.

Lemma 3. Let $P$ be a finite non-abelian $p$-group and let $\Delta$ be a division algebra such that $P \subset M_n(\Delta)$. Suppose that $V_\sigma(P) = M_n(\Delta)$.

1. Suppose that $P$ is a 2-group which is not of type 0 and that $\Delta$ is noncommutative. Then there exists a subgroup $P_0$ of $P$ of index 2 such that $V_\sigma(P_0) \cong M_{n/2}(\Delta) \oplus M_{n/2}(\Delta)$.

2. Suppose that $\Delta$ is commutative. Then we have $V_\sigma(P) = M_n(C)$ and there exists a normal subgroup $P_0$ of $P$ of index $p$ such that $V_\sigma(P_0) \cong \frac{M_{n/2}(C) \oplus \cdots \oplus M_{n/2}(C)}{M_{n/p}(C)}$.

Proof. (a) Let $M$ be a simple $M_n(\Delta)$-module and let $E$ be a splitting field of $\Delta$. Since $M$ is a non-linear faithful $Q\sigma P$-module by the assumption that $V_\sigma(P) = M_n(\Delta)$, there exists a non-linear faithful irreducible $EP$-module $N$ such that $M \otimes_Q E \cong m_\sigma(N)(N \oplus N^\sigma \oplus \cdots)$, $\sigma \in \text{Gal}(Q(\zeta)/Q)$, where $\zeta$ is the character of $N$ and $m_\sigma(N)$ denotes the Schur index of $N$. Applying the Witt-Roquette’s theorem to $N$, we can find a normal subgroup $P_0$ of $P$ and an irreducible $EP$-module $N_0$ with character $\zeta_0$ such that $N_0^p \cong N$ and $Q(\zeta) = Q(\zeta_0)$. Let $\chi$ denote the character of $M$. Then we have $\chi = m_\sigma(\zeta)(\zeta + \zeta^\sigma + \cdots) = m_\sigma(\zeta_0)(\zeta_0 + \zeta_0^\sigma + \cdots) + m_\sigma(\zeta)(\zeta + \zeta_0^\sigma + \cdots)$ where \{1, $g$\} are representatives of $P/P_0$. Since $2 = m_\sigma(\zeta) \leq m_\sigma(\zeta_0) \leq 2$, we have $m_\sigma(\zeta) = m_\sigma(\zeta_0) = 2$. Let $\chi_0 = m_\sigma(\zeta_0)(\zeta_0 + \zeta_0^\sigma + \cdots)$. Then $\chi_0$ is a $Q$-character of $P_0$. Further let $M_0$ be the $Q\Phi P$-module corresponding to $\chi_0$. Then we see that $M_0 \oplus M_0^\sigma \cong Q\Phi P \otimes_Q Q\Phi P M_0 \cong Q\Phi P \otimes_Q Q\Phi P M_0^\sigma \cong M$ as $Q\Phi P$-module. Since $M_0 \cong M_0^\sigma$ as $Q\Phi P_0$-module, we have

$$\Delta \cong \text{Hom}_{Q\Phi P}(M, M)$$
$$\cong \text{Hom}_{Q\Phi P}(Q\Phi P \otimes_Q Q\Phi P M_0, Q\Phi P \otimes_Q Q\Phi P M_0)$$
$$\cong \text{Hom}_{Q\Phi P_0}(M_0, \text{Hom}_{Q\Phi P}(Q\Phi P, Q\Phi P \otimes_Q Q\Phi P M_0))$$
$$\cong \text{Hom}_{Q\Phi P_0}(M_0, Q\Phi P \otimes_Q Q\Phi P M_0)$$
$$\cong \text{Hom}_{Q\Phi P_0}(M_0, M_0)$$,
372 M. HIKARI

and, similarly, \( \Delta \cong \text{Hom}_{Q(P)}(M^g, M^g) \). Clearly \( \dim_Q M_0 = \dim_Q M^g = \frac{1}{2} \dim_Q M \), and the semi-simple subalgebra \( V_Q(P_0) \subset V_Q(P) = M_\Delta \) has only two simple components corresponding to \( M_0, M^g_0 \). Thus we get \( V_Q(P_0) = M_{\Delta/2} \oplus M_{\Delta/2} \).

(b) Since \( \Delta \) is commutative by the assumption, we have \( C \otimes_a V_Q(P) \cong C \otimes_a M_\Delta \cong M_{\Delta}(C) \). From this it follows directly that \( V_C(P) = M_{\Delta}(C) \). Let \( M \) be a simple \( V_C(P) \)-\((CP)\)-module and let \( \chi \) be the character of \( M \). According to the Witt-Roquette’s theorem, there exists a normal subgroup \( P_0 \) of \( P \) of index \( p \) and an irreducible \( CP_0 \)-module \( M_0 \) such that \( M \cong M_0^p \). Hence, along the same line as in the case (a), we can show that \( V_C(P_0) = M_{\Delta/p}(C) + \cdots + M_{\Delta/p}(C) \).

Q.E.D.

Lemma 4. Let \( P \) be a finite \( p \)-group. Suppose one of the following conditions:

(a) \( p = 2 \) and \( P \) is a subgroup of \( M_{\Delta}(\Delta) \) such that \( V_Q(P) = M_{\Delta}(\Delta) \) where \( \Delta \) is a quaternion algebra.

(b) \( P \) is a subgroup of \( M_{\Delta}(\Delta) \) such that \( V_C(P) = M_{\Delta}(\Delta) \). Then \( P \) is a subgroup of a \( p \)-group of \( n \)-type. Further, in the case (b) \( P \) is a subgroup of a \( p \)-group of \( n \)-type.

Proof. We will give the proof only in the case (a), because the proof in the case (b) can be done similarly. This will be done by induction on \( n \). In case \( n = 0 \) this is obvious. Hence we assume that \( n \geq 1 \). By Lemma 3, there exists a normal subgroup \( P_0 \) of \( P \) of index 2 such that \( V_Q(P_0) = A_1 \oplus A_2 \) where \( A_i \cong M_{\Delta - i}(\Delta) \). Let \( M_i \) be a simple \( A_i \)-module and let \( \{1, g\} \) be representatives of \( P/P_0 \). Then \( M_i \cong M_f^i \) as \( QP_i \)-module. Let \( P_i \) denote the image of \( P_0 \) by the projection on \( A_i \). Then \( V_Q(P_i) = M_{\Delta - i}(\Delta) \). Hence, by induction, each \( P_i \) is a subgroup of a \( 2 \)-group of \( (n-1) \)-type. We regard \( M_i \) as \( QP_i \)-module by the projection \( P_0 \to P_i \) and so, since \( M_i \cong M_f^i \), we have \( P_2 = P_f^2 \) and the following commutative diagram:

\[
\begin{array}{ccc}
P_0 & \xrightarrow{g} & P_0 \\
P_1 \times P_2 & \xrightarrow{(g, g)} & P_2 \times P_1 \\
\end{array}
\]

On the other hand, we can find 2-groups \( P_1, P_2 \) of \((n-1)\)-type such that \( P_1 \cong P_2 \). Here we may assume that the restriction of the isomorphism \( P_1 \cong P_2 \) on \( P \) coincides with \( g: P_1 \to P_2 \). We denote this isomorphism from \( P_1 \) onto \( P_2 \) by \( \sigma \). Put \( h = g^2 \). Then the map \( (1, h): P_2 \times P_1 \to P_2 \times P_1 \) is an isomorphism and so \( (\sigma, h\sigma^{-1}): P_2 \times P_1 \to P_2 \times P_1 \) is an isomorphism, too. Since the restriction of \( h\sigma^{-1} \) on \( P_2 \) coincides with \( hg^{-1} = g \), we get the following commutative diagram:
Let \( \langle u \rangle \) be a cyclic group of order 2. The automorphism \((\sigma, h\sigma^{-1})\) and the factor set \(\{(1, l) \mid (u, y) = (1, u)\} \) define a group \( \bar{P} \) with normal subgroup \( \bar{P}_1 \times \bar{P}_2 \) and \( \bar{P}_1 \times \bar{P}_2 \cong \langle u \rangle \), because \((h\sigma^{-1}, \sigma) \cdot (\sigma, h\sigma^{-1}) = (h, h\sigma^{-1})\). Then the group \( \bar{P} \) is clearly a 2-group of \( n \)-type which contains \( P \). Thus the proof of the lemma is completed.

**Lemma 5.** If \( P \in T_2^{(a)} \) (resp. \( T_2^{(s)} \)), \( P \) is a subgroup of \( M_2(H) \) (resp. \( M_2(C) \)) and \( V_{\mathbb{R}}(P) = M_2(H) \) (resp. \( V_{\mathbb{C}}(P) = M_2(C) \)).

**Proof.** We will prove this in the case \( P \in T_2^{(a)} \).

(a) \( n = 0 \). Since \( P \) is a generalized quaternion group, \( P \) is a subgroup of \( H \) and \( V_{\mathbb{R}}(P) = H \) ([1], [2]).

(b) \( n > 0 \). We proceed by induction on \( n \). By the definition of \( T_2^{(a)} \), there exist 2-groups \( P_1, P_2 \in T_2^{(a-1)} \) such that \( P_1 \times P_2 \) is a subgroup of \( P \) of index 2 and \( P_1 \times P_2 \) is a single \( P \)-module. By the induction hypothesis each \( P_i \) is a subgroup of \( M_2^{-1}(H) \) and \( V_{\mathbb{R}}(P_i) = M_2^{-1}(H) \). Let \( M \) be a simple \( V_{\mathbb{R}}(P_i) \)-module. Put \( M = M_1 \otimes_{\mathbb{R}P_1 \times \mathbb{R}P_2} \mathbb{R}P \). Since \( P_1 = P_2 \), \( M \) is a simple \( \mathbb{R}P \)-module. It follows that \( M \) is a faithful \( \mathbb{R}P \)-module and therefore \( \text{Hom}_{\mathbb{R}P}(M, M) \cong \text{Hom}_{\mathbb{R}P_1 \times \mathbb{R}P_2}(M_1, M_1) \cong \text{Hom}_{\mathbb{R}P_1 \times \mathbb{R}P_2}(M_1, M_1) \cong H \). We see that the simple component of \( \mathbb{R}P \) corresponding to \( M \) is \( M_2(H) \). Because \( M \) is a faithful \( \mathbb{R}P \)-module, \( P \) is a subgroup of \( M_2(H) \) and \( V_{\mathbb{R}}(P) \cong M_2(H) \).

We will omit the proof in the case \( P \in T_2^{(s)} \), because we can prove it along the same line as in the case \( P \in T_2^{(a)} \). Q.E.D.

Now we give the proof of our main theorem.

**Proof of the main theorem.** The implication \((1) \Rightarrow (2)\) is obvious and therefore it suffices to show the implications \((2) \Rightarrow (3) \Rightarrow (1)\).

(a) \( (2) \Rightarrow (3) \). Assume \( P \subset M_2(H) \). Let \( V_q(P) = M_{p_1}(\Delta) \oplus \cdots \oplus M_{p_s}(\Delta) \) be the decomposition of \( V_q(P) \) into simple algebras where each \( \Delta \) is a division algebra. Here we easily see that \( p_1 \leq \cdots \leq p_s \leq n \). Let \( P_i \) be the image of \( P \) by the projection to \( M_{p_i}(\Delta) \), for each \( 1 \leq i \leq s \). Then \( P \) can be identified with a subgroup of \( \prod_{i=1}^s P_i \) and, for each \( 1 \leq i \leq s \), \( V_q(P_i) \cong M_{p_i}(\Delta) \). According to the
remark on the Witt-Roquette's theorem, $\Delta_i$ is a quaternion algebra or an algebraic number field. Further if $\Delta_i$ is a quaternion algebra for some $1 \leq i \leq s$, $p = 2$ ([3]). If $\Delta_i$ is an algebraic number field, by Lemma 3 (2) $V_c(P_i) \approx M_{p^i}(C)$. Applying Lemma 4, it follows that each $P_i$ is a subgroup of a $p$-group of $I_i$-type. Here (3) is concluded in this case.

Assume $P \subset M_n(K)$. Let $L$ be the algebraic closure of $K$ and let $L' = C \cap L$. Since $K$ is commutative, we have $L \otimes_K M_n(K) \approx M_n(L)$. From this it follows directly that $V_{L'}(P) \subset M_n(L)$. In addition, each division algebra equivalent to a simple component of $L'P$ coincides with $L'([3])$. Let $V_{L'}(P) \approx M_{p^i}(L') \oplus \cdots \oplus M_{p^i}(L')$ be the decomposition of $V_{L'}(P)$ into simple algebras. Then $p^i + \cdots + p^i \leq n$. If $P_i$ is the image of $P$ by the projection to $M_{p^i}(L')$, $P_i$ is a subgroup of $M_{p^i}(C) \approx M_{p^i}(L') \otimes L'C$ and $V_c(P_i) \approx M_{p^i}(C)$. It follows from Lemma 4 that $P_i$ is a subgroup of $I_i$-type. On the other hand $P$ can be identified with a subgroup of $\prod_{i=1}^{s} P_i$ and so we conclude (3).

(b) $(3) \Rightarrow (1)$. Since $P^{(p)}_i$ is a $p$-group of $i$-type (resp. $I_i$-type), by Lemma 5, $P^{(p)}_i$ is a subgroup of $M_{p^i}(H)$ (resp. $M_{p^i}(C)$) and $\prod_{i=1}^{s} P^{(p)}_i \subset \prod_{i=1}^{s} M_{p^i}(H) \subset M_n(H)$ (resp. $\prod_{i=1}^{s} P^{(p)}_i \subset M_n(C)$) by $\sum_{i=0}^{s} p^i m_i \leq n$. Since $P$ is a subgroup of $\prod_{i=1}^{s} \prod_{j=1}^{s} P^{(p)}_i$, $P$ is a subgroup of $M_n(H)$ (resp. $M_n(C)$).

Q.E.D.

Tokyo University of Education

References