



Title	Multiplicative P-subgroups of simple algebras
Author(s)	Hikari, Michitaka
Citation	Osaka Journal of Mathematics. 1973, 10(2), p. 369-374
Version Type	VoR
URL	https://doi.org/10.18910/11691
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

The University of Osaka

Hikari, M.
Osaka J. Math.
10 (1973), 369-374

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 Δ are division algebras of characteristic 0.

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

Let Δ be a division algebra. We will denote by $M_n(\Delta)$ the full matrix algebra of degree n over Δ . 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 Δ 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 \mathbf{Q} , \mathbf{R} , \mathbf{C} , \mathbf{H} denote respectively the rational number field, the real number field, the complex number field and the quaternion algebra over \mathbf{R} .

If an abelian group G has invariants (e_1, \dots, e_n) , $e_n \neq 1$, $e_{i+1} \mid e_i$, 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 Δ such that $G \subset M_n(\Delta)$ 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 Δ such that $G \subset M_n(\Delta)$. 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

$$1 + p + \dots + p^{m-1}$$

order p^m . We can write $\mathbf{Q}G_0 \cong \mathbf{Q} \oplus \overbrace{\mathbf{Q}(\varepsilon_p) \oplus \dots \oplus \mathbf{Q}(\varepsilon_p)}^m$ where ε_p denotes the primitive p -th root of unity. Since $V_{\mathbf{Q}}(G_0)$ is a direct summand of $\mathbf{Q}G_0$ and

$G_0 \subset V_{\mathbf{Q}}(G_0)$, we have $V_{\mathbf{Q}}(G_0) \cong \overbrace{\mathbf{Q}(\varepsilon_p) \oplus \dots \oplus \mathbf{Q}(\varepsilon_p)}^m$. On the other hand, since

$V_Q(G_0) \subset M_n(\Delta)$, there exist at most n orthogonal idempotents in $V_Q(G_0)$. Thus we have $m \leq n$. The converse is obvious. Q.E.D.

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 Δ such that $P \subset M_n(\Delta)$, then P is abelian.*

Proof. Let $V_Q(P) \cong M_{p^t}(\Delta_1) \oplus \cdots \oplus M_{p^t}(\Delta_t)$ be the decomposition of $V_Q(P)$ into simple algebras where each Δ_i is a division algebra. Then we easily see that $p^{l_1} + \cdots + p^{l_t} \leq n$. Therefore, when $n < p$, we have $l_1 = \cdots = l_t = 0$. Since p is odd, each division algebra Δ_i is commutative ([3]). Hence $V_Q(P)$ 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, \dots, 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 $P'_1^g = P'_2, \dots, P'_{p-1}^g = P'_p, P'_p^g = P'_1$. 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, $P_0 = P', P_1, \dots, P_{n-1}, P_n = P$ such that, for each $0 \leq i \leq n-1$, P_{i+1} is a simple p -extension of P_i .

Now we set

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

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 $M_n(\mathbf{H})$ (resp. $M_n(\mathbf{C})$).*
- (2) *There is a division algebra Δ (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, \dots, m_t with $\sum_{i=0}^t p^i m_i \leq n$ and $P_i^{(1)}, P_i^{(2)}, \dots, P_i^{(m_i)} \in T_p^{(i)}$ (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 χ is a nonlinear irreducible faithful character of P there exists $P_0 \triangleleft P$ and a character ζ 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 Δ be a division algebra such that $P \subset M_n(\Delta)$. Suppose that $V_Q(P) = M_n(\Delta)$.

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

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

Proof. (a) Let M be a simple $M_n(\Delta)$ -module and let E be a splitting field of Δ . Since M is a non-linear faithful QP -module by the assumption that $V_Q(P) = M_n(\Delta)$, there exists a non-linear faithful irreducible EP -module N such that $M \otimes_Q E \cong m_Q(N)(N \oplus N^\sigma \oplus \cdots)$, $\sigma \in Gal(Q(\zeta)/Q)$, where ζ is the character of N and $m_Q(N)$ 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_0 -module N_0 with character ζ_0 such that $N_0^P \cong N$ and $Q(\zeta) = Q(\zeta_0)$. Let χ denote the character of M . Then we have $\chi = m_Q(\zeta)(\zeta + \zeta^\sigma + \cdots) = m_Q(\zeta)(\zeta_0 + \zeta_0^\sigma + \cdots) + m_Q(\zeta)(\zeta_0 + (\zeta_0^\sigma)^\sigma + \cdots)$ where $\{1, g\}$ are representatives of P/P_0 . Since $2 = m_Q(\zeta) \leq m_Q(\zeta_0) \leq 2$, we have $m_Q(\zeta) = m_Q(\zeta_0) = 2$. Let $\chi_0 = m_Q(\zeta_0)(\zeta_0 + \zeta_0^\sigma + \cdots)$. Then χ_0 is a Q -character of P_0 . Further let M_0 be the QP_0 -module corresponding to χ_0 . Then we see that $M_0 \oplus M_0^\sigma \cong QP \otimes_{QP_0} M_0 \cong QP \otimes_{QP_0} M_0^\sigma \cong M$ as QP -module. Since $M_0 \cong M_0^\sigma$ as QP_0 -module, we have

$$\begin{aligned} \Delta &\cong \text{Hom}_{QP}(M, M) \\ &\cong \text{Hom}_{QP}(QP \otimes_{QP_0} M_0, QP \otimes_{QP_0} M_0) \\ &\cong \text{Hom}_{QP_0}(M_0, \text{Hom}_{QP}(QP, QP \otimes_{QP_0} M_0)) \\ &\cong \text{Hom}_{QP_0}(M_0, QP \otimes_{QP_0} M_0) \\ &\cong \text{Hom}_{QP_0}(M_0, M_0), \end{aligned}$$

and, similarly, $\Delta \cong \text{Hom}_{QP_0}(M_0^g, M_0^g)$. Clearly $\dim_Q M_0 = \dim_Q M_0^g = \frac{1}{2} \dim_Q M$, and the semi-simple subalgebra $V_Q(P_0) \subset V_Q(P) = M_n(\Delta)$ has only two simple components corresponding to M_0, M_0^g . Thus we get $V_Q(P_0) \cong M_{n/2}(\Delta) \oplus M_{n/2}(\Delta)$.

(b) Since Δ is commutative by the assumption, we have $C \otimes_{\Delta} V_Q(P) \cong C \otimes_{\Delta} M_n(\Delta) \cong M_n(C)$. From this it follows directly that $V_C(P) = M_n(C)$. Let M be a simple $V_C(P)$ - (CP) -module and let χ 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 $V_C(P_0) \cong \overbrace{M_{n/p}(C) + \cdots + M_{n/p}(C)}^p$.

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 $M_{2^n}(\Delta)$ such that $V_Q(P) = M_{2^n}(\Delta)$ where Δ is a quaternion algebra.

(b) P is a subgroup of $M_{p^n}(C)$ such that $V_C(P) = M_{p^n}(C)$. 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 \tilde{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 $A_i \cong M_{2^{n-1}}(\Delta)$. Let M_i be a simple A_i -module and let $\{1, g\}$ be representatives of P/P_0 . Then $M_2 \cong M_1^g$ as QP_0 -module. Let P_i denote the image of P_0 by the projection on A_i . Then $V_Q(P_i) = M_{2^{n-1}}(\Delta)$. Hence, by induction, each P_i is a subgroup of a 2-group of $(n-1)$ -type. We regard M_i as QP_0 -module by the projection $P_0 \rightarrow P_i$ and so, since $M_2 \cong M_1^g$, we have $P_2 = P_1^g$ and the following commutative diagram:

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

On the other hand, we can find 2-groups \tilde{P}_1, \tilde{P}_2 of $(n-1)$ -type such that $\tilde{P}_1 \cong \tilde{P}_2$. Here we may assume that the restriction of the isomorphism $\tilde{P}_1 \cong \tilde{P}_2$ on P_1 coincides with $g: P_1 \cong P_2$. We denote this isomorphism from \tilde{P}_1 onto \tilde{P}_2 by σ . Put $h = g^2$. Then the map $(1, h): \tilde{P}_2 \times \tilde{P}_1 \rightarrow \tilde{P}_2 \times \tilde{P}_1$ is an isomorphism and so $(\sigma, h\sigma^{-1}): \tilde{P}_1 \times \tilde{P}_2 \rightarrow \tilde{P}_2 \times \tilde{P}_1$ 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:

$$\begin{array}{ccc}
 P_0 & \xrightarrow{g} & P_0 \\
 \downarrow & & \downarrow \\
 P_1 \times P_2 & \xrightarrow{(g, g)} & P_2 \times P_1 \\
 \downarrow & & \downarrow \\
 \tilde{P}_1 \times \tilde{P}_2 & \xrightarrow{(\sigma, h\sigma^{-1})} & \tilde{P}_2 \times \tilde{P}_1
 \end{array}$$

Let $\langle u \rangle$ be a cyclic group of order 2. The automorphism $(\sigma, h\sigma^{-1})$ and the factor set $\{(1, 1) = (u, 1) = (1, u) = 1, (u, u) = h\}$ define a group \tilde{P} with normal subgroup $\tilde{P}_1 \times \tilde{P}_2$ and $\tilde{P}/\tilde{P}_1 \times \tilde{P}_2 \cong \langle u \rangle$, because $(h\sigma^{-1}, \sigma) \cdot (\sigma, h\sigma^{-1}) = (h, \sigma h\sigma^{-1}) = (h, h^{\sigma^{-1}}) = (h, h^{\sigma^{-1}}) = (h, h)$. Then the group \tilde{P} is clearly a 2-group of n -type which contains P . Thus the proof of the lemma is completed.

Lemma 5. *If $P \in T_2^{(n)}$ (resp. $\tilde{T}_p^{(n)}$), P is a subgroup of $M_{2^n}(\mathbf{H})$ (resp. $M_{p^n}(\mathbf{C})$) and $V_R(P) = M_{2^n}(\mathbf{H})$ (resp. $V_C(P) = M_{p^n}(\mathbf{C})$).*

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

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

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

We will omit the proof in the case $P \in \tilde{T}_p^{(n)}$, because we can prove it along the same line as in the case $P \in T_2^{(n)}$. 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 $P \subset M_n(\Delta)$. Let $V_Q(P) \cong M_{p^1}(\Delta_s) \oplus \cdots \oplus M_{p^s}(\Delta_s)$ be the decomposition of $V_Q(P)$ into simple algebras where each Δ_i is a division algebra. Here we easily see that $p^1 + \cdots + p^s \leq n$. Let P_i be the image of P by the projection to $M_{p^i}(\Delta_i)$, 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 $1 \leq i \leq s$, $V_Q(P_i) \cong M_{p^i}(\Delta_i)$. According to the

remark on the Witt-Roquette's theorem, Δ_i is a quaternion algebra or an algebraic number field. Further if Δ_i is a quaternion algebra for some $1 \leq i \leq s$, $p=2$ ([3]). If Δ_i is an algebraic number field, by Lemma 3 (2) $V_C(P_i) \cong M_{p^{l_i}}(\mathbf{C})$. Applying Lemma 4, it follows that each P_i is a subgroup of a p -group of l_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 $L' = \mathbf{C} \cap L$. Since K is commutative, we have $L \otimes_K M_n(K) \cong M_n(L)$. 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 $V_{L'}(P) \cong M_{p^{l_1}}(L') \oplus \cdots \oplus M_{p^{l_s}}(L')$ be the decomposition of $V_{L'}(P)$ into simple algebras. Then $p^{l_1} + \cdots + p^{l_s} \leq n$. If P_i is the image of P by the projection to $M_{p^{l_i}}(L')$, P_i is a subgroup of $M_{p^{l_i}}(\mathbf{C}) \cong M_{p^{l_i}}(L') \otimes_{L'} \mathbf{C}$ and $V_C(P_i) \cong M_{p^{l_i}}(\mathbf{C})$. It follows from Lemma 4 that P_i is a subgroup of \tilde{l}_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 $P_i^{(j)}$ is a p -group of i -type (resp. \tilde{i} -type), by Lemma 5, $P_i^{(j)}$ is a subgroup of $M_{p^i}(\mathbf{H})$ (resp. $M_{p^i}(\mathbf{C})$) and so $\prod_i \prod_{j=1}^{m_i} P_i^{(j)} \subset \sum_{i,j} M_{p^i}(\mathbf{H}) \subset M_n(\mathbf{H})$ (resp. $\prod_i \prod_{j=1}^{m_i} P_i^{(j)} \subset M_n(\mathbf{C})$) by $\sum_{i=0}^t p^i m_i \leq n$. Since P is a subgroup of $\prod_i \prod_{j=1}^{m_i} P_i^{(j)}$, P is a subgroup of $M_n(\mathbf{H})$ (resp. $M_n(\mathbf{C})$). Q.E.D.

TOKYO UNIVERSITY OF EDUCATION

References

- [1] S. Amitsur: *Finite subgroups of division rings*, Trans. Amer. Math. Soc. **80** (1955), 361–386.
- [2] I.N. Herstein: *Finite multiplicative subgroups in division rings*, Pacific J. Math. **1** (1953), 121–126.
- [3] P. Roquette: *Realisierung von Darstellungen endlicher nilpotenter Gruppen*, Arch. Math. **9** (1958), 241–250.
- [4] E. Witt: *Die algebraische Struktur des Gruppenringes einer endlichen Gruppe über einem Zahlenkörper*, J. Reine Angew. Math. **190** (1952), 231–245.