University of Nebraska - Lincoln
DigitalCommons@University of Nebraska - Lincoln

Faculty Publications, Department of Mathematics | Mathematics, Department of

1-1-1944

A Theorem on the Unit Groups of Simple Algebras

Ralph Hull
University of Nebraska - Lincoln

Follow this and additional works at: http://digitalcommons.unl.edu/mathfacpub

Part of the Mathematics Commons

Hull, Ralph, "A Theorem on the Unit Groups of Simple Algebras" (1944). *Faculty Publications, Department of Mathematics.* Paper 23.
http://digitalcommons.unl.edu/mathfacpub/23

This Article is brought to you for free and open access by the Mathematics, Department of at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in Faculty Publications, Department of Mathematics by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.

Published in Bull. Amer. Math. Soc. 50 (1944) 405-411.

A THEOREM ON THE UNIT GROUPS OF SIMPLE ALGEBRAS

RALPH HULL

1. Introduction. Let k be an algebraic number field of finite degree m and let A be a normal simple algebra of degree n, order n^2, over k. Our object is to prove the following theorem.

THEOREM. *If A is an R-algebra, that is, if $n>2$ or at least one infinite prime place of k is unramified in A when $n=2$, then any two distinct maximal orders of A have distinct groups of units.*

There are essential arithmetical differences between algebras which satisfy the R-condition (R-algebras) and those which do not, especially with regard to class-number properties (Eichler [1, 2, 3]).[1] The meaning of the R-condition in the case $n=2$ is as follows. Both k and A are simple algebras over the field k_0 of rational numbers, of orders m and $4m$, respectively, over k_0. Suppose k_0 is extended to the field k_1 of real numbers. Then the extended algebra $k\times k_1$ is the direct sum of fields, each of which is isomorphic either to k_1 or to the field k_2 of complex numbers. This decomposition of $k\times k_1$ involves the decomposition of $A\times k_1$ into a direct sum of simple algebras over k_1, the centers of which are the corresponding summands of $k\times k_1$. Each summand of $A\times k_1$ is either (1) a matrix algebra of degree 2 over k_1, (2) a matrix algebra of degree 2 over k_2, or (3) the division algebra of quaternions over k_1. With each summand of $k\times k_1$ is associated an infinite prime place of k which is said to be ramified or unramified in A according as the corresponding summand of $A\times k_1$ is (3) or is either (1) or (2). The R-condition for $n=2$ is thus equivalent to requiring that not all summands of $A\times k_1$ be (3), in other words, that A over k is not a totally definite quaternion algebra. The condition is in general indispensable in our theorem. For example, the unit groups of all maximal orders in certain definite quaternion algebras over k_0 consist of the units ± 1 only.

The proof of the theorem will be based on the following Hilfssatz due to Eichler [3, p. 239, Hilfssatz 9].

Let A be an R-algebra, let $\mathfrak{O}$ be a maximal order of A, and let $\mathfrak{F}$ be a two-sided $\mathfrak{O}$-ideal. If $\mathcal{A}$ is an element of $\mathfrak{O}$ whose reduced norm $N(\mathcal{A})$ is congruent modulo $\mathfrak{F}$ to a unit of k, then $\mathfrak{O}$ contains a unit $\mathcal{E}\equiv\mathcal{A}$ modulo $\mathfrak{F}$.

Presented to the Society, November 27, 1943; received by the editors December 3, 1943.

[1] Numbers in brackets refer to the references cited at the end of the paper.

By local (p-adic) methods we shall first reduce the proof of the theorem to that for a special case. The lemmas proved for this purpose are independent of the R-condition and may be of interest also in another connection not discussed here, namely, in the problem of imbedding non-maximal orders in maximal orders. Next, also by local methods, we prove the theorem in the special case by applying the Hilfssatz. Finally, we indicate briefly an application of the theorem to the determination of the structure of the Brandt groupoid of normal ideals of A.

2. **Reduction to a special case.** Let A' be a normal simple algebra over a p-adic number field k'. Let ν be the index of A', $n=\nu\kappa$. Then A' is the algebra of matrices of degree κ with elements in a division algebra B' of degree ν over k'. If $\kappa=1$, the unique maximal order $\mathfrak{o}'$ in B' is the only maximal order in $A'=B'$. If $\kappa>1$, the set

$$\mathfrak{O}' = \sum e_{ij}\mathfrak{o}' \qquad (i, j = 1, \cdots, \kappa), \tag{1}$$

where the e_{ij} are ordinary matric units in A', is a maximal order in A'. Conversely, every maximal order in A' is of the form (1) with the appropriate e_{ij}.

Let $\mathfrak{p}'$ be the prime ideal of B'. Then $\mathfrak{p}'$ is a principal ideal: $\mathfrak{p}'=\pi\mathfrak{o}'=\mathfrak{o}'\pi$, where π is a prime element in B'. The ideal $\mathfrak{P}'=\mathfrak{O}'\mathfrak{p}'=\mathfrak{p}'\mathfrak{O}'=\sum e_{ij}\mathfrak{p}'$ is the $\mathfrak{O}'$-prime-ideal in A'. If $\mathfrak{L}'$ is any integral $\mathfrak{O}'$-left-ideal in A', the matric units can be further selected (Hasse [1, p. 524]) so that (1) holds and also

$$\mathfrak{L}' = \mathfrak{O}'\Lambda = \sum e_{ii}\pi^{(a_1+\cdots+a_i)}, \tag{2}$$

where the a's are non-negative integers. The right order of $\mathfrak{L}'$ is

$$\Lambda^{-1}\mathfrak{O}'\Lambda = \sum e_{ij}\mathfrak{p}'^{(a_1+\cdots+a_j)-(a_1+\cdots+a_i)}. \tag{3}$$

The intersection of $\mathfrak{O}'$ and $\Lambda^{-1}\mathfrak{O}'\Lambda$ is

$$\mathfrak{O}' \cap \Lambda^{-1}\mathfrak{O}'\Lambda = \sum_{i\geqq j} e_{ij}\mathfrak{o}' + \sum_{i<j} e_{ij}\mathfrak{p}'^{(a_{i+1}+\cdots+a_j)}. \tag{4}$$

Equations (3) and (4) are readily verified by displaying matrices in the usual way.

With these preliminaries we are ready to prove the following lemma.

LEMMA 1. *Let A' be a normal simple algebra over a p-adic number field k', and let $\mathfrak{O}_1'$ and $\mathfrak{O}_2'$ be any two distinct maximal orders in A', whose distance is $\mathfrak{D}_{12}'=(\mathfrak{O}_2'\mathfrak{O}_1')^{-1}$. Then, either $\mathfrak{D}_{12}'$ is irreducible, or there exists a maximal order $\mathfrak{O}_3'$ in A' such that $\mathfrak{O}_1'\cap\mathfrak{O}_3'\supset\mathfrak{O}_1'\cap\mathfrak{O}_2'$ and such that $\mathfrak{D}_{13}'=(\mathfrak{O}_3'\mathfrak{O}_1')^{-1}$ is irreducible and divides $\mathfrak{D}_{12}'=\mathfrak{D}_{13}'\mathfrak{D}_{32}'$.*

By a remark above $\kappa > 1$, since otherwise A' would have only one maximal order. Let $\mathfrak{O}_1' = \mathfrak{O}'$ in (1) and $\mathfrak{D}_{12}' = \mathfrak{L}'$ in (3). Then $\mathfrak{L}' \neq \mathfrak{O}'$, since $\mathfrak{O}_2' \neq \mathfrak{O}'$, and hence at least one a_i in (2) is not zero. If a_1 were not zero, $\mathfrak{L}'$ would be divisible by the two-sided ideal $\mathfrak{P}'$, contrary to the properties of a distance ideal.[2] It follows that there is a fixed $r \geqq 2$ for which $a_1 = a_2 = \cdots = a_{r-1} = 0$, $a_r \neq 0$. If $r = \kappa$, $a_r = 1$, $\mathfrak{D}_{12}' = \mathfrak{L}'$ is irreducible and the first alternative in Lemma 1 holds.

Assume that $r < \kappa$ or $a_r > 1$ if $r = \kappa$. Then $\mathfrak{L}'$ has the irreducible left divisor

$$\mathfrak{J}_r' = \mathfrak{O}'\Lambda_r, \qquad \Lambda_r = 1 + (\pi - 1)e_{rr}. \tag{5}$$

For, $\Lambda = \Lambda_r\Lambda_0$, where Λ_0 is in $\mathfrak{O}'$. Writing $\mathfrak{O}_3' = \Lambda_r^{-1}\mathfrak{O}\Lambda_r$, $\mathfrak{O}_3'\Lambda_0 = \mathfrak{D}'$, we have $\mathfrak{L}' = \mathfrak{J}_r'\mathfrak{D}'$, $\mathfrak{D}' = \mathfrak{O}_3'\Lambda_0$. Since $\mathfrak{J}_r'$ is irreducible and has $\mathfrak{O}'$ and $\mathfrak{O}_3'$ as its left and right orders, $\mathfrak{J}_r'$ is the distance $\mathfrak{D}_{13}'$. It can be shown easily, but is not required in what follows, that $\mathfrak{D}' = (\mathfrak{O}_2'\mathfrak{O}_3')^{-1} = \mathfrak{D}_{32}'$. By a simple computation, we obtain

$$\mathfrak{O}_3' = \Lambda_r^{-1}\mathfrak{O}'\Lambda_r = \sum_{i,j\neq r} e_{ij}\mathfrak{o}' + \sum_{j<r} e_{rj}\mathfrak{p}'^{-1} + \sum_{i<r} e_{ir}\mathfrak{p}' + e_{rr}\mathfrak{o}', \tag{6}$$

and

$$\mathfrak{O}' \cap \mathfrak{O}_3' = \sum_{j\neq r} e_{ij}\mathfrak{o}' + e_{rr}\mathfrak{o}' + \sum_{i\neq r} e_{ir}\mathfrak{p}'. \tag{7}$$

Comparison of (4) and (7) shows that $\mathfrak{O}' \cap \mathfrak{O}_3' \supset \mathfrak{O}' \cap \mathfrak{O}_2'$. This completes the proof of Lemma 1.

The reduction in the large, corresponding to that in Lemma 1, is based on the following lemma.

LEMMA 2. *Let A be a normal simple algebra over an algebraic number field k and let $\mathfrak{O}_1$ and $\mathfrak{O}_2$ be any two distinct maximal orders in A, whose distance is $\mathfrak{D}_{12} = (\mathfrak{O}_2\mathfrak{O}_1)^{-1}$. Let p be a prime ideal of k which divides the reduced norm $N(\mathfrak{D}_{12})$. Then, either $\mathfrak{D}_{12}$ is irreducible, in which case $N(\mathfrak{D}_{12}) = p$, or there exists a maximal order $\mathfrak{O}_3$ in A such that $\mathfrak{O}_1 \cap \mathfrak{O}_3 \supset \mathfrak{O}_1 \cap \mathfrak{O}_2$ and such that $\mathfrak{D}_{13} = (\mathfrak{O}_3\mathfrak{O}_1)^{-1}$ is irreducible, has norm p, and divides $\mathfrak{D}_{12} = \mathfrak{D}_{13}\mathfrak{D}_{32}$.*

In proving Lemma 2, we write $\mathfrak{O}$ for $\mathfrak{O}_1$ and use primed symbols, without subscripts, to refer to p-components for a fixed p which divides $N(\mathfrak{D}_{12})$.

The ideal $\mathfrak{O}p$ is a power of a two-sided $\mathfrak{O}$-prime-ideal P:

$$\mathfrak{O}p = p\mathfrak{O} = P^\nu, \qquad n = \nu\kappa, \qquad N(P) = p^\kappa, \tag{8}$$

[2] See Deuring [1, chap. VI, VII] for definitions and properties when explicit reference elsewhere is not made.

where $\nu=\nu_p$ and $\kappa=\kappa_p$ are the order of ramification and the capacity, respectively, of p or of P in A. In A, P decomposes into a product of κ irreducible ideals, each of norm p. In accord with (8), the index of A', over k', is ν. The p-component $\mathfrak{D}'_{12}$ is the distance $(\mathfrak{O}'_2\mathfrak{O}'_1)$ (Hasse [1, p. 529]; cf. Deuring [1, p. 104]). Moreover, $\mathfrak{D}'_{12}\neq\mathfrak{O}'$, since $p\mid N(\mathfrak{D}_{12})$. Hence $\mathfrak{O}'_2\neq\mathfrak{O}'$, from which it follows that $\kappa\geqq 2$, $\nu<n$. If $\mathfrak{D}_{12}$ is irreducible its norm is necessarily p, and we have nothing to prove. We now assume that $\mathfrak{D}_{12}$ is not irreducible and obtain $\mathfrak{D}_{13}$ and $\mathfrak{O}_3$ of the lemma by the usual method of specifying their components at all finite prime places of k.

Let q_1 denote any prime ideal of k, other than p, which divides $N(\mathfrak{D}_{12})$. If there is no q_1 we omit (10) and the q_1-components in (13), $\cdots$, (16), below, but the argument is not essentially altered. Let q_2 be any prime ideal of k which does not divide $N(\mathfrak{D}_{12})$. By Lemma 1, we have

$$\mathfrak{D}'_{12}=\mathfrak{D}'_{13}\mathfrak{D}'_{32},\qquad \mathfrak{O}'_1\cap\mathfrak{O}'_3\supset\mathfrak{O}'\cap\mathfrak{O}'_2, \tag{9}$$

where $\mathfrak{D}'_{13}$ is the distance $(\mathfrak{O}'_3\mathfrak{O}'_1)^{-1}$ and is irreducible. Also, for any q_1 and any q_2,

$$\mathfrak{D}'_{12q_1}=\mathfrak{O}'_{q_1}\mathfrak{D}'_{12q_1},\qquad \mathfrak{O}'_{q_1}\cap\mathfrak{O}'_{q_1}\supset\mathfrak{O}'_{q_1}\cap\mathfrak{O}'_{2q_1}, \tag{10}$$

and

$$\mathfrak{D}'_{12q_2}=\mathfrak{O}'_{q_2}\mathfrak{O}'_{q_2},\qquad \mathfrak{O}'_{q_2}\cap\mathfrak{O}'_{q_2}=\mathfrak{O}'_{q_2}\cap\mathfrak{O}'_{q_2}, \tag{11}$$

where the first statement in (11) follows from

$$\mathfrak{O}'_{q_2}=\mathfrak{O}'_{2q_2}=\mathfrak{D}'_{12q_2},\qquad q_2\nmid N(\mathfrak{D}_{12}). \tag{12}$$

Consider the sets

$$\mathfrak{D}'_{13},\ \mathfrak{O}'_{q_1},\ \mathfrak{O}'_{q_2},\ \textit{for all } q_1 \textit{ and all } q_2, \tag{13}$$

$$\mathfrak{O}',\ \mathfrak{O}'_{q_1},\ \mathfrak{O}'_{q_2},\ \textit{for all } q_1 \textit{ and all } q_2, \tag{14}$$

$$\mathfrak{O}'_2,\ \mathfrak{O}'_{2q_1},\ \mathfrak{O}'_{2q_2},\ \textit{for all } q_1 \textit{ and all } q_2, \tag{15}$$

and

$$\mathfrak{O}'_3,\ \mathfrak{O}'_{q_1},\ \mathfrak{O}'_{q_2},\ \textit{for all } q_1 \textit{ and all } q_2. \tag{16}$$

The intersection of (13) and A is an irreducible left divisor $\mathfrak{D}_{13}$ of $\mathfrak{D}_{12}$, that of (14) and A is $\mathfrak{O}$, that of (15) and A is $\mathfrak{O}_2$, and that of (16) and A is $\mathfrak{O}_3$, the right order of $\mathfrak{D}_{13}$. The irreducibility of $\mathfrak{D}_{13}$ follows at once from its definition by (13) and the irreducibility of $\mathfrak{D}'_{13}$. That $\mathfrak{D}_{13}$ divides $\mathfrak{D}_{12}$ follows from the first statements in (9), (10) and (11).

The statements concerning (14), (15) and (16) are evident. Moreover, $\mathfrak{D}_{13}=(\mathfrak{O}_3\mathfrak{O}_1)^{-1}$ since $\mathfrak{D}_{13}$ is irreducible and $\mathfrak{O}_1$ and $\mathfrak{O}_3$ are its left and right orders, respectively. We write $\mathfrak{D}_{12}=\mathfrak{D}_{13}\mathfrak{D}_{32}$ but omit the proof that $\mathfrak{D}_{32}=(\mathfrak{O}_2\mathfrak{O}_3)^{-1}$.

Let $\mathcal{A}$ be any element of $\mathfrak{O}\cap\mathfrak{O}_2$. Then $\mathcal{A}$ is in the p-, q_1-, and q_2-components of both $\mathfrak{O}$ and $\mathfrak{O}_2$, for all q_1 and all q_2. By the second statements in (9), (10) and (11), $\mathcal{A}$ is in the corresponding components of $\mathfrak{O}_3$. Hence $\mathcal{A}$ is in $\mathfrak{O}_3$ and $\mathfrak{O}\cap\mathfrak{O}_3$, since $\mathcal{A}$ is in A. This proves that $\mathfrak{O}\cap\mathfrak{O}_3\supset\mathfrak{O}\cap\mathfrak{O}_2$, and completes the proof of Lemma 2.

3. **Proof of the theorem.** By virtue of Lemma 2, in order to prove the theorem it evidently suffices to prove that *if* $\mathfrak{D}_{13}=(\mathfrak{O}_3\mathfrak{O}_1)^{-1}$ *is irreducible, there is a unit in* $\mathfrak{O}_1$ *which is not in* $\mathfrak{O}_3$.

Let $N(\mathfrak{D}_{13})=p$, and take p to be the fixed prime ideal of k in §2. As before, we use primed symbols, without subscripts, to refer to p-components, and we write $\mathfrak{O}$ for $\mathfrak{O}_1$. We employ the representation (1) of $\mathfrak{O}'$, and have $\kappa\geqq 2$ by an argument used in the proof of Lemma 2. The "canonical" form of $\mathfrak{D}'_{13}$, corresponding to (2), is

$$\mathfrak{D}'_{13}=\mathfrak{O}'\Delta,\qquad \Delta=1+(\pi-1)e_{\kappa\kappa}, \tag{17}$$

and we assume that the e_{ij} are chosen so that (17) holds. The ideal $\mathfrak{D}'_{13}$ divides the two-sided ideal $\mathfrak{O}'P=\mathfrak{P}'$, where P is defined in (8).

Consider the element $\mathcal{A}_p=1+e_{\kappa-1,\kappa}$ of $\mathfrak{O}'$. The reduced norm of an element of $\mathfrak{O}'$ is the determinant of the matrix representing it in (1), with the understanding[3] that the coefficients, in B', are replaced by their corresponding matrices in a reduced representation of B'. It follows that $N(\mathcal{A}_p)=1\equiv 1 \pmod{\mathfrak{O}'P}$. Since $\mathfrak{O}/P$ and $\mathfrak{O}'/\mathfrak{O}'P$ are isomorphic, there exists an element $\mathcal{A}$ in $\mathfrak{O}$ such that $\mathcal{A}\equiv\mathcal{A}_p \pmod{\mathfrak{O}'P}$ and $N(\mathcal{A})\equiv 1 \pmod{P}$. Using, at last, the assumption that A *is an* R*-algebra*, by Eichler's Hilfssatz, $\mathfrak{O}$ contains a unit $\mathcal{E}\equiv\mathcal{A} \pmod{P}$. We shall prove that $\mathcal{E}$ is not in $\mathfrak{O}_3$.

Using (17), we get

$$\mathfrak{O}'_3=\Delta^{-1}\mathfrak{O}'\Delta=\sum_{i,j<\kappa}e_{ij}\mathfrak{o}'+e_{\kappa\kappa}\mathfrak{o}'+\sum_{j<\kappa}e_{\kappa j}\mathfrak{p}'^{-1}+\sum_{i<\kappa}e_{i\kappa}\mathfrak{p}'. \tag{18}$$

Comparison of (1) and (18) shows that $\mathcal{A}_p$ is not in $\mathfrak{O}'_3$. Since $\mathcal{E}\equiv\mathcal{A}_p \pmod{\mathfrak{O}'P}$, $\mathcal{E}$ is not in $\mathfrak{O}'_3$ and hence $\mathcal{E}$ is not in $\mathfrak{O}_3$.

4. **An application of the theorem.** The author was led to the theorem in attempting to answer the following question proposed to him some time ago by Professor R. Baer. The normal ideals of an algebra

[3] This is essential if $\nu>1$, since then B is noncommutative.

A form an infinite groupoid (Brandt [1]) with respect to proper multiplication. The normal ideals having the same left order form, similarly, a *Mischgruppe* (Loewy [1]). Baer [1] has shown that the theory of the latter, and hence the closely related theory of groupoids, is essentially subordinate to the theory of a group G and a non-invariant subgroup H. Indeed, with one trivial exception, every Mischgruppe is isomorphic to the factor-Mischgruppe $(G\|H)_L$ of cosets $H\mathcal{G}$, $\mathcal{G}\in G$, for suitable G and H. Similarly, every Brandt groupoid, with the corresponding exception, is a factor-groupoid $(G\|H)_B$ of cosets $\mathcal{G}_1^{-1}H\mathcal{G}_2$, $\mathcal{G}_i\in G$. The question is: *Are there groups G and H in an algebra A such that $(G\|H)_B$ and $(G\|H)_L$ are isomorphic to the groupoid and Mischgruppe, respectively, of normal ideals, described above?*

By means of our theorem a partial answer to this question can be given. Let $\mathfrak{O}$ be any order of A, U the unit group of $\mathfrak{O}$, A^* the multiplicative group of nonsingular elements of A. Then *if A is an R-algebra, the Mischgruppe of principal $\mathfrak{O}$-left-ideals $\mathfrak{O}\mathcal{A}$, $\mathcal{A}\in A^*$, and the groupoid of ideals $\mathcal{A}_1^{-1}\mathfrak{O}\mathcal{A}_2$, $\mathcal{A}_i\in A^*$ are isomorphic to $(A^*\|U)_L$ and $(A^*\|U)_B$, respectively.*

The Mischgruppe and groupoid described are natural generalizations of the group of principal ideals of k, and hence the above isomorphism, for R-algebras, is a natural generalization of the isomorphism of the group of principal ideals of k with the factor group k^*/u, where u is the group of units of k. However, Baer's formal subordination of the theory of the Brandt groupoid to the theory of groups does not seem to make the concept of a groupoid, as such, any less essential to a satisfactory arithmetical theory of simple algebras. The above isomorphism for R-algebras evidently fails for the rational definite quaternion algebras cited in the introduction since $(A^*\|U)_L$ and $(A^*\|U)_B$ are both groups if U consists of ± 1 only.

References

R. Baer

1. *Zur Einordnung der Theorie der Mischgruppen in die Gruppentheorie*, Sitzungsberichte der Heidelberger Akademie der Wissenschaften, Math.-Naturw. Klasse vol. 4 (1928) pp. 1–18.

H. Brandt

1. *Über eine Verallgemeinerung des Gruppenbegriffes*. Math. Ann. vol. 96 (1927) pp. 360–366.

M. Deuring

1. *Algebren*, Ergebnisse der Mathematik, vol. 4 (1935).

M. Eichler

1. *Bestimmung der Idealklassenzahl in gewissen normalen einfachen Algebren*, Journal für Mathematik vol. 176 (1937) pp. 192–202.

2. *Über die Idealklassenzahl hyperkomplexer Systeme*, Math. Zeit. vol. 43 (1938) pp. 481–494.
3. *Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraische Zahlkörpern und ihre L-Reihen*, Journal für Mathematik vol. 179 (1938) pp. 227–251.

H. Hasse
1. *Über p-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme*, Math. Ann. vol. 104 (1931) pp. 495–534.

A. Loewy
1. *Über abstrakt definierte Transmutationssysteme oder Mischgruppen*, Journal für Mathematik vol. 157 (1927) pp. 239–254.

The University of Nebraska