ON THE CLASS NUMBER OF A QUATERNION ALGEBRA WITH A NEGATIVE FUNDAMENTAL NUMBER*

BY

CLAIBORNE G. LATIMER

1. **Introduction.** Let $\mathfrak{A}$ be a rational generalized quaternion algebra and let $\mathfrak{G}$ be a set of integral elements in $\mathfrak{A}$ according to Dickson's definition.† The number h, of classes of left ideals in $\mathfrak{G}$ is independent of the particular $\mathfrak{G}$ in $\mathfrak{A}$ which is considered and is equal to the number of classes of right ideals.‡ We shall show that if $\mathfrak{A}$ contains an element with a negative norm, then every ideal in $\mathfrak{G}$ is principal and hence $h=1$.

From this, we obtain theorems on the existence of a greatest common right divisor, or g.c.r.d., and a g.c.l.d. of two elements and on the factorization of an element in $\mathfrak{G}$. Results equivalent to these have been previously obtained for a number of special cases.§ These theorems are also similar to well known results, due to Hurwitz, for a certain $\mathfrak{G}$ in the classic rational quaternion algebra.

Let G be the set of all integral algebraic numbers in a quadratic field. It will be shown that G is contained in a set $\mathfrak{G}$ as above defined, such that every pair of elements ξ, η in G, not both zero, have a g.c.r.d. δ_1 and a g.c.l.d. δ_2 in $\mathfrak{G}$ which are uniquely determined, apart from unit factors. Moreover, if ξ, η have a g.c.d. δ in G, we may take $\delta_1=\delta_2=\delta$. Hence, while sacrificing commutativity, such an enlargement of G yields a result similar to that obtained by the introduction of ideals.

2. **A special $\mathfrak{G}$.** It is known that $\mathfrak{A}$ has a basis $1, i, j, ij$ such that

$$i^2 = -\tau, \qquad j^2 = -d, \qquad ij = -ji,$$

where d is the fundamental number of $\mathfrak{A}$ and τ is any one of the infinitude of positive primes which satisfy the conditions:

(a) τ is prime to d, $\tau \equiv 3 \pmod 4$ and $-\tau$ is a quadratic non-residue of every odd prime factor of d;

* Presented to the Society, September 13, 1935, received by the editors October 9, 1935.

† *Algebras and their Arithmetics*, pp. 141–142. This definition is equivalent to the definition of a maximal realm of integrity as given by Brandt, *Idealtheorie in Quaternionenalgebren*, Mathematische Annalen, vol. 99 (1928), p. 11.

‡ Brandt, loc. cit., p. 23.

§ E.g., *On ideals in generalized quaternion algebras and Hermitian forms*, these Transactions, vol. 38 (1935), pp. 436–446, where references are given to other special cases. This paper will be referred to hereafter as Tr.

(b) $-d$ is a quadratic residue of τ;

(c) if d is even, $\tau\equiv 3 \pmod 8$.*

Though not necessary for the proofs of the three lemmas to follow, we shall assume without loss of generality that

(d) $$\tau > 4|d| .$$

We shall now prove

LEMMA 1. *Let μ be an integer such that $4\mu^2+d\equiv 0 \pmod \tau$. Then*

$$e_1 = 1, \quad e_2 = \frac{\tau + i}{2}, \quad e_3 = j, \quad e_4 = \frac{(-2\mu + e_3)e_2}{\tau}$$

form a basis of a set of integral elements.†

We shall prove this lemma by showing that the e's may be obtained by an integral transformation of determinant ±1 from known basal elements of a set of integral elements.

For the case where d is odd, basal elements of those sets of integral elements which contain i and j may be obtained by specializing certain results obtained by the writer.‡ In this reference, set $I=i$, $J=j$, $K=ij$, $\alpha=-\tau$, $\beta=d$, take H_1 so that $dH_1\equiv 2\mu \pmod \tau$ and, employing (a) and (b) above, properly specialize the various divisors of $\alpha\beta$ which appear in the expressions for the basal elements 1, P'', Q_1'', R_1 of S_1'', as given on p. 62. It will then be found that the above e's are obtained from these basal elements by an integral transformation of determinant ±1. But by the same reference, S_1'' is a set of integral elements. The lemma follows for the case where d is odd.

Suppose d is even. We employ results due to Darkow,§ setting her e_1, e_2, e_3 equal to ij, j, $-di$, respectively. Then by (c) above, $\mathfrak{A}$ is of type A as defined by Darkow. Take her $H_1=F_1=1$ and E_1 so that $dE_1\equiv 2\mu \pmod \tau$. It will be found, as in the case where d is odd, that the e's of the lemma are obtained from her $A_0, \cdots, A_3$ (p. 267) by an integral transformation of determinant ±1. But the A's form a basis of a set of integral elements. The lemma follows.

* *On the fundamental number of a rational generalized quaternion algebra*, Duke Mathematical Journal, vol. 1 (1935), pp. 433–435. For the definition of d, see Brandt, loc. cit., p. 9.

† For the case where $\mathfrak{A}$ is a division algebra, a similar result was obtained by Albert. See his *Integral domains of rational generalized quaternion algebras*, Bulletin of the American Mathematical Society, vol. 40 (1934), p. 176, Theorem 9. In the paper in the Duke Mathematical Journal cited above, it was shown that Albert's $\sigma=-d$. Albert's τ, the negative of ours, is subject to the restriction that it is represented by a certain binary quadratic form.

‡ *Arithmetics of generalized quaternion algebras*, American Journal of Mathematics, vol. 48 (1926), pp. 57–63.

§ *Determination of a basis for the integral elements of certain generalized quaternion algebras*, Annals of Mathematics, (2), vol. 28 (1926–27), pp. 263–270.

It will be assumed hereafter, unless the contrary is explicitly stated, that $\mathfrak{G}$ is the set of integral elements given by Lemma 1.

Suppose $\mathfrak{A}$ has a basis 1, I, J, IJ, where $I^2=-\alpha$, $J^2=-\beta$, $IJ=-JI$, α and β being rational integers, neither divisible by the square of a prime. It may be shown that if a set of integral elements contains two of I, J, IJ/δ, then it contains the third, δ being the g.c.d. of α and β, for otherwise the set would not be maximal. While not necessary for the sequel, we note that this, together with Lemma 1 and the papers cited in its proof, has an important bearing on certain remarks and results in Albert's paper previously cited.

In the papers cited in the proof of Lemma 1, Darkow and the writer determined those sets of integral elements containing I and J if $\alpha\equiv\beta$ (mod 2), Darkow treating the case where α is even. Albert remarked (loc. cit., p. 165) that these results did not complete the problem, presumably referring to the case where $\alpha\equiv\beta+1$ (mod 2). However this lack of completeness is only apparent since, by a change of notation, this case is seen to be included in Darkow's results. Thus if $\alpha\equiv\beta+1\equiv 1$ (mod 2), the sets containing I and J are identical with the sets containing IJ/δ and J, and the latter are obtained from Darkow's results by setting her e_1, e_2, e_3 equal to IJ/δ, J, $-\beta I/\delta$, respectively.

If d is odd, by the above mentioned results of the writer's, there are exactly two sets of integral elements containing e_2 and e_3 of Lemma 1. If d is even, the same is true by Darkow's results and by the above statement as to a set containing two of I, J, IJ/δ. Albert's Theorem 9 (loc. cit., p. 176) follows at once from Lemma 1 without the restriction that $\mathfrak{A}$ be a division algebra.

3. **On the ideals in a certain ring.** It will be observed that 1 and e_2 form a basis of a set G, equivalent to the set of all integral numbers in the field defined by $(-\tau)^{1/2}$. Let $\mathfrak{G}_1$ be the ring consisting of all elements in the form $x+e_3y$, where x, y are in G. $\mathfrak{G}$ contains $\mathfrak{G}_1$ and an element $\sum u_ie_i$ of $\mathfrak{G}$ is in $\mathfrak{G}_1$ if and only if $u_4\equiv 0$ (mod τ). Hence $\bar{e}_i=e_i$ $(i=1, 2, 3)$, $\bar{e}_4=\tau e_4$ form a basis of $\mathfrak{G}_1$.

We shall use the same definitions of a left ideal in $\mathfrak{G}$, a class of such ideals and the norm of an ideal as given by Brandt.* A left ideal in $\mathfrak{G}_1$, a regular ideal and a class of such ideals are defined as in Tr.† Unless the contrary is explicitly stated, it will be understood that all ideals referred to, in $\mathfrak{G}$ or in $\mathfrak{G}_1$, are left ideals; also, that every element of an ideal in $\mathfrak{G}$ belongs to $\mathfrak{G}$.

Those elements of an ideal $\mathfrak{L}$, in $\mathfrak{G}$ which are in $\mathfrak{G}_1$ form an ideal $\mathfrak{L}_1$, in $\mathfrak{G}_1$ which will be said to correspond to $\mathfrak{L}$. We shall now prove

* Brandt, loc. cit., pp. 16, 14. See also second footnote, p. 21 and p. 3.

† To identify the notation of Tr. with that of this paper, set $E=e_3$, $\alpha=-d$, $\Delta=-\tau$, $\mathfrak{G}=\mathfrak{G}_1$.

LEMMA 2. *If $\mathfrak{L}$ is an ideal in $\mathfrak{G}$ and $\mathfrak{L}_1$ is the corresponding ideal in $\mathfrak{G}_1$, then $\mathfrak{L}_1$ is a regular ideal if and only if $\mathfrak{L}$ contains an element not in $\mathfrak{G}_1$.*

$\mathfrak{L}$ has a basis $\omega_i = \sum_j a_{ij} e_j$ $(i=1, \cdots, 4)$, where the determinant $|a_{ij}| = a^2$, a being a positive integer which, by definition, is the norm $N(\mathfrak{L})$ of $\mathfrak{L}$.[*] We shall assume, without loss of generality, that every $a_{ii} > 0$ and $a_{ij} = 0$ if $i < j$.

$\mathfrak{L}_1$ has as a basis $\bar{\omega}_i = \omega_i$ $(i = 1, 2, 3)$, $\bar{\omega}_4 = \tau\omega_4$ or $\bar{\omega}_i = \omega_i$ $(i = 1, \cdots, 4)$ according as not all or all of the elements of $\mathfrak{L}$ are in $\mathfrak{G}_1$. If we set $\bar{\omega}_i = \sum_j \bar{a}_{ij}\bar{e}_j$, in the first case the determinant $|a_{ij}| = |\bar{a}_{ij}|$ and in the second case, $|a_{ij}| = \tau |\bar{a}_{ij}|$.

There are certain ideals $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{d}$ in G determined by $\mathfrak{L}_1$ and by Lemmas 1, 2 of Tr., $|\bar{a}_{ij}| = N(\mathfrak{a})N(\mathfrak{b}) = a_1^2 N^2(\mathfrak{b})N(\mathfrak{d})$, where a_1 is a rational integer. $-\tau$ is the discriminant of the quadratic field defined by i. Hence by (a) and (c) of §2 and by a well known result,[†] no rational prime factor of d is divisible by a prime ideal in G of the first degree. Then by Lemma 2 of Tr., $N(\mathfrak{d}) = 1$ or $N(\mathfrak{d}) = \tau$. But $|a_{ij}|$ is a square. Therefore in the first case above $N(\mathfrak{d}) = 1$; in the second case, $N(\mathfrak{d}) = \tau$. Since $\mathfrak{L}_1$ is regular by definition if and only if $N(\mathfrak{d}) = 1$, the lemma follows.

We shall assume hereafter that $d < 0$.

LEMMA 3. *Every regular ideal in $\mathfrak{G}_1$ is a principal ideal.*

By Theorem 3 of Tr. there is a one-to-one correspondence between the regular classes of ideals in $\mathfrak{G}_1$ and the classes of Hermitian forms in G of determinant $-d$. By the last sentence in §4 of Tr., every ideal in a regular class is regular. Hence, to prove the lemma, it is sufficient to show that there is a single class of such Hermitian forms. Let $f(x, y) = axx' + bx'y + b'xy' + cyy'$ be such a form. It may be shown that f is equivalent, under a unitary transformation with coefficients in G, to such a form with a odd and b in the ring G_1, consisting of all elements in the form $r + si$ where r, s are rational integers. Assume that a is odd and b is in G_1. Since $bb' - ac = -d$ and d contains no square factor > 1,[‡] if we restrict x, y to G_1, f is a properly primitive form in G_1. By a result due to Humbert,[§] there is a single class of such forms; i.e., any two such forms are equivalent under a unitary transformation with coefficients in G_1. Since G contains G_1, the lemma follows.

4. **Proof of principal theorem.** Let C be a class of ideals in $\mathfrak{G}$. The class

[*] Brandt, loc. cit., pp. 13, 16.

[†] Cf. Hecke, *Vorlesungen über die Theorie der Algebraischen Zahlen*, p. 110, Satz. 90.

[‡] Fueter, *Zur Theorie der Brandtschen Quaternionenalgebren*, Mathematische Annalen, vol. 110 (1934), p. 658.

[§] Comptes Rendus, Paris, vol. 171 (1920), pp. 287–293; Dickson, *History of the Theory of Numbers*, vol. 3, p. 278.

C contains an ideal $\mathfrak{L}$ such that $N(\mathfrak{L}) \leqq 2(-d)^{1/2}$.* Let $\omega_1, \cdots, \omega_4$ be a basis of $\mathfrak{L}$ as used in the proof of Lemma 2. Then by (d) of §2, $N^2(\mathfrak{L}) = a_{11}a_{22}a_{33}a_{44} \leqq -4d < \tau$, a_{44} is prime to τ and $\bar{\omega}_i = \omega_i$ $(i=1, 2, 3)$, $\bar{\omega}_4 = \tau\omega_4$ form a basis of the corresponding ideal $\mathfrak{L}_1$ in $\mathfrak{G}_1$. If we set $\bar{\omega}_i = \sum_j \bar{a}_{ij}\bar{e}_j$, we have $N^2(\mathfrak{L}) = |a_{ij}| = |\bar{a}_{ij}|$.

Since a_{44} is prime to τ, ω_4 is not in $\mathfrak{G}_1$. Then by Lemmas 2, 3, $\mathfrak{L}_1$ is a principal ideal $\{\rho\}$, where ρ is an element in $\mathfrak{G}_1$. Then $\bar{e}_i\rho = \sum_j r_{ij}\bar{e}_j$ $(i=1, \cdots, 4)$ form a basis of $\mathfrak{L}_1$, where the matrix (r_{ij}) is the transpose of the second matrix of ρ, with respect to the basis $\bar{e}_1, \cdots, \bar{e}_4$ of $\mathfrak{A}$.† Hence $|r_{ij}| = N^2(\rho)$. But the $\bar{\omega}_i$ also form a basis of $\mathfrak{L}_1$. Therefore $N^2(\mathfrak{L}) = |\bar{a}_{ij}| = N^2(\rho)$.

Since ρ is in $\mathfrak{L}$, $e_i\rho = \sum t_{ij}\omega_j = \sum_j s_{ij}e_j$, where the t's are rational integers and $(s_{ij}) = (t_{ij})(a_{ij})$ is the transpose of the second matrix of ρ with respect to the basis $e_1, \cdots, e_4$ of $\mathfrak{A}$. Hence $N^2(\rho) = |s_{ij}| = |t_{ij}| N^2(\mathfrak{L})$, $|t_{ij}| = 1$ and the $e_i\rho$ $(i=1, \cdots, 4)$ form a basis of $\mathfrak{L}$. Therefore $\mathfrak{L}$ is the principal ideal defined by ρ.

It follows that every ideal in C is a principal ideal. But C was an arbitrarily chosen class. Hence every ideal in $\mathfrak{G}$ is principal. We have then by the second sentence in §1,

Theorem 1. *Let $\mathfrak{A}$ be a rational generalized quaternion algebra with a negative fundamental number, and let $\mathfrak{G}$ be an arbitrarily chosen set of integral elements in $\mathfrak{A}$. Every one-sided ideal in $\mathfrak{G}$ is a principal ideal.*

It will be observed that in the above proof, the condition $N(\mathfrak{L}) \leqq 2(-d)^{1/2}$ was used only to insure a_{44} being prime to τ, i.e., that $\mathfrak{L}$ contains an element not in $\mathfrak{G}_1$. It follows from the above proof that if η is a non-singular element in the special $\mathfrak{G}$ considered above, there is a unit U in $\mathfrak{G}$, i.e., an element of norm ± 1, such that $U\eta = \rho$ is in $\mathfrak{G}_1$.‡

If we employ narrow equivalence of ideals, as in Tr., it may be shown that the number h_0, of classes of narrowly equivalent ideals in an arbitrary $\mathfrak{G}$ is independent of the particular $\mathfrak{G}$ which is considered; the proof of this being the same as Brandt's proof for the broader case.§ By the proof of Lemma 3, there is a single class of regular ideals in $\mathfrak{G}_1$, narrow equivalence being employed. Hence $\mathfrak{G}_1$ contains an element of norm -1. Therefore the same is true of the special $\mathfrak{G}$ employed in the proof of Theorem 1. Hence $h_0 = 1$ and every $\mathfrak{G}$ contains an element of norm -1.||

* Brandt, loc. cit., p. 23.

† Dickson, *Algebras and their Arithmetics*, p. 95.

‡ Cf. Dickson, *Algebras and their Arithmetics*, p. 153, Lemma 7.

§ Brandt, loc. cit., p. 23.

|| Cf. Brandt, loc. cit., p. 29.

5. **Applications of Theorem 1.** Let $\mathfrak{S}$ be as in Theorem 1 and let η_1, η_2 be elements of $\mathfrak{S}$ such that one of $N(\eta_1)$, $N(\eta_2)$, $\eta_1\eta_2'$ is $\neq 0$. Let $\mathfrak{L}$ be the set of all elements $\xi_1\eta_1+\xi_2\eta_2$, where ξ_1, ξ_2 are in $\mathfrak{S}$. The set $\mathfrak{L}$ is an ideal if it contains a non-singular element. This is obviously the case if either η_1 or η_2 is non-singular. Suppose they are both singular. For a properly chosen rational integer t, $\mathfrak{S}$ contains ti, tj, tij. We have $N(\xi\eta_1+\eta_2)=\xi\eta_1\eta_2'+\eta_2\eta_1'\xi'$, which is the trace of $\xi\eta_1\eta_2'$. Hence if we take $\xi=1$, ti, tj, or tij, $N(\xi\eta_1+\eta_2)\neq 0$ and $\mathfrak{L}$ is an ideal.

Let the g.c.r.d. and the g.c.l.d. of two elements in $\mathfrak{S}$ be defined as in Tr. Employing the above and Theorem 1, the following theorems may be proved by the same methods used in the proof of Theorem 4 of Tr.

THEOREM 2. *Let $\mathfrak{S}$ be as in Theorem* 1, *and let η_1, η_2 be elements of $\mathfrak{S}$ such that one of $N(\eta_1)$, $N(\eta_2)$, $\eta_1\eta_2'$ is $\neq 0$. Then η_1, η_2 have a* g.c.r.d. δ_1, *and a* g.c.l.d. δ_2 *and there are elements μ_1, μ_2, γ_1, γ_2 in $\mathfrak{S}$ such that $\mu_1\eta_1+\mu_2\eta_2=\delta_1$, $\eta_1\nu_1+\eta_2\nu_2=\delta_2$. Furthermore, δ_1 $[\delta_2]$ is uniquely determined, apart from a unit left [right] factor.*

THEOREM 3. *Let $\mathfrak{S}$ be as in Theorem* 1, *let λ be a non-singular element in $\mathfrak{S}$ not divisible by a rational prime, and let $N(\lambda)=\pm p_1\cdot p_2\cdot\,\cdots\,\cdot p_r$, where the p's are rational primes arranged in an arbitrary but fixed order. Then $\lambda=\pi_1\cdot\pi_2\cdot\,\cdots\,\cdot\pi_r$ where $N(\pi_i)=\pm p_i$ $(i=1, 2, \cdots, r)$ and each π_i is an element of $\mathfrak{S}$ which is uniquely determined apart from unit factors.*

We have seen that $\mathfrak{S}$ contains an element of norm -1. Hence, in the above factorization of λ, the sign of each $N(\pi_i)$, except one, may be arbitrarily chosen.

6. **An enlargement of a set of quadratic integers.** Let G be the set of all algebraic integers in the quadratic field defined by $(-\alpha)^{1/2}$, α being a rational integer with no square factor >1. Let β be a negative integer, with no square factor >1, such that $\alpha\equiv\beta \pmod 2$. Let $\mathfrak{A}$ be the rational generalized quaternion algebra with a basis 1, i, j, ij where $i^2=-\alpha$, $j^2=-\beta$, $ij=-ji$. Since $N(j)=\beta<0$, the fundamental number of $\mathfrak{A}$ is negative. By the results of Darkow or of the writer cited in the proof of Lemma 1, there is a set $\mathfrak{S}$ of integral elements in $\mathfrak{A}$ which contains a sub-set equivalent to G. Then the statements made in the last paragraph of §1 follow from Theorem 2.

UNIVERSITY OF KENTUCKY,
LEXINGTON, KY.