ON THE FACTORIZATION OF GENERALIZED QUATERNIONS

By Gordon Pall

1. A fundamental theorem in the arithmetic of Lipschitz[1] integral quaternions

$$v = v_0 + i_1v_1 + i_2v_2 + i_3v_3 , \tag{1}$$

where the v_i are rational integers and the i_α are the familiar Hamilton units ($i_\alpha^2 = -1$, etc.), is that any proper v (i.e., one in which $v_0 , \cdots , v_3$ are coprime), whose norm $\sum v_i^2$ is divisible by an odd positive integer m, has exactly eight right-divisors t of norm m, these forming a class of left-associates

$$\pm t, \qquad \pm i_1t, \qquad \pm i_2t, \qquad \pm i_3t. \tag{2}$$

In this article a connection is set up between the problems of factoring "generalized quaternions" (defined in §3) and of representing the number 1 in a certain quaternary quadratic form S. Hence the problem is reduced to that of equivalence of quaternary quadratic forms. However, the order and genus of S is readily identified. Hence in all cases where there is but one class in this quaternary genus, a theorem of the type quoted above will follow; and when several classes occur in that genus, some similar theorem may be deducible.

Our definition of generalized quaternion, based on Hermite's identity,[2] connects the theory with ternary and quaternary quadratic forms, rather than with binary Hermitian forms as in Dickson's definition. For results similar to ours in Dickson's generalized quaternions, perhaps the best reference is *Ideals in generalized quaternion algebras*, Trans. Amer. Math. Soc., vol. 38(1935), pp. 436–446, by C. G. Latimer.

2. Our method is based on a process of Hermite's,[3] who in turn was guided by Gauss's algorithm for reducing the representation of numbers in a binary quadratic form to the solution of a quadratic congruence and to identifying the class of a form constructed from the solution. We shall introduce the method by exhibiting a similar device for quadratic fields. We shall confine ourselves, however, to fields in which the integers are of the form

$$v = v_0 + v_1\omega, \qquad v_0 \text{ and } v_1 \text{ rational integers}, \tag{3}$$

where $\omega^2 = -D$ is a non-square rational integer. There is no difficulty in extending the theory to $\omega^2 + \omega + \frac{1}{4}(1 - \Delta) = 0$. Similarly, in this article we

Received May 18, 1938.

[1] R. Lipschitz, Jour. de Math., (4), vol. 2(1886), French translation by J. Molk.

[2] C. Hermite, Jour. für Math., vol. 47(1854), pp. 313–330; *Oeuvres*, vol. 1, 1905, pp. 200–220, especially p. 212.

[3] Hermite, Jour. für Math., vol. 47(1854), pp. 343–345; *Oeuvres*, vol. 1, pp. 234–237.