A NOTE ON DIVISION ALGORITHMS IN IMAGINARY QUADRATIC NUMBER FIELDS

D. W. DUBOIS AND A. STEGER

An integral domain E is said to be *Euclidean* if there exists a non-negative, integer-valued function g defined on the non-zero elements of E such that for every non-zero x and y in E,

(1) $g(xy) \geqslant g(x)$;

(2) (division algorithm) if x does not divide y then there exists an element q in E, depending on x and y, with

$$g(y - qx) < g(x).$$

The function g will be called a *Euclidean function.*

The elementary properties of Euclidean domains may be found in Van der Waerden (**4**, p. 56).

The problem of determining all quadratic number fields $K(\sqrt{m})$ in which the norm is a Euclidean function (on the sub-domain of algebraic integers in $K(\sqrt{m})$) has been solved. See (**2**, ch. xiv) for a partial discussion and bibliography. The following is unsolved: are there any Euclidean quadratic fields for which the norm is not a Euclidean function? That is, can the norm be generalized so as to enlarge the class of fields possessing division algorithms? The following theorem asserts that for *imaginary* quadratic fields the answer is no; the proof, based on the scarcity of units in these fields, fails for the real fields. This theorem answers a question of Hasse (**3**) concerning whether the field $K(\sqrt{-19})$, known by Dedekind (**1**, suppl. xi, p. 451) to be a principal ideal domain in which the norm is not a Euclidean function, is Euclidean in the general sense defined above, and appears to be the first proof that a principal ideal domain need not be Euclidean.

THEOREM. *An imaginary quadratic field $K(\sqrt{m})$ is Euclidean if and only if the norm N is a Euclidean function.*

Proof. The norm N is a Euclidean function for imaginary $K(\sqrt{m})$ only when $m = -1, -2, -3, -7, -11$; see (**2**) for a proof. Let $m < 0$ be different from these and suppose that $K(\sqrt{m})$ is Euclidean with Euclidean function g. There exists an integer t in $K(\sqrt{m})$ distinct from zero and units, such that $g(t)$ is a minimum of the set of all $g(x)$ for which x is neither zero nor a unit. Then for every integer b there is an integer q with $b - qt$ either zero or a unit; this means that every integer in $K(\sqrt{m})$ is congruent to zero or to a unit (mod t). But the only units are $\pm\ 1$. It follows that

$$N(t) = N((t)) \leqslant 3.$$

Received May 13, 1957.

https://doi.org/10.4153/CJM-1958-030-3 Published online by Cambridge University Press

But for the m chosen above, this inequality implies that t is zero or a unit, contrary to the choice of t. The contradiction establishes the theorem.

References

1. L. Dirichlet and R. Dedekind, *Vorlesungen über Zahlentheorie* (4 Aufl. Braunschweig, 1894).
2. G. H. Hardy and E. M. Wright, *The Theory of Numbers* (Oxford, 1954).
3. Helmut Hasse, *Ueber eindeutige Zerlegung in Primelemente oder Primhauptideale in Integraetsbereichen*, J. reine angew. Math., *159* (1928), 3–12.
4. B. L. Van der Waerden, *Modern Algebra* (New York, 1949).

University of New Mexico