THE EUCLIDEAN ALGORITHM

TH. MOTZKIN

In this note a constructive criterion for the existence of a Euclidean algorithm within a given integral domain is derived, and from among the different possible Euclidean algorithms in an integral domain one is singled out. The same is done for "transfinite" Euclidean algorithms. The criterion obtained is applied to some special rings, in particular rings of quadratic integers. By an example it is shown that there exist principal ideal rings with no Euclidean algorithm. Finally, different sets of axioms for the Euclidean algorithm and related notions are compared, and the possible implications for the classification of principal ideal rings, and other integral domains, indicated.

The question of the relationship between different Euclidean algorithms in the same integral domain was raised (orally) by O. Zariski.

1. **The derived sets.** Let Q be an integral domain. A subset P of $Q-0$ (Q except zero) shall be called a *product ideal* if $P(Q-0)\subseteq P$.

For any subset S of Q, the set B of all b in Q for which there exists an a in Q such that $a+bQ\subseteq S$ is called the *total derived set* of S, and the intersection $B\cap S$ is called the *derived set* S'. With S also S' is a product ideal. If $S_1\subseteq S$, then $S_1'\subseteq S'$.

A *Euclidean algorithm* (or process) is given by a norm $|a|$ defined in $Q-0$, with positive integral (or zero) values and such that $|a|\geqq|b|$ for b dividing a and that for any b in $Q-0$ and any a not divisible by b there exist q and r in Q satisfying $a=qb+r$, $|r|<|b|$.

Let P_i, $i=0, 1, 2, \cdots$, be the set of all b in Q with $|b|\geqq i$. Obviously P_i is a product ideal. For any b in P_i', let a be an element with $a+bQ\subseteq P_i$, whence $a-bq\neq 0$ and (for any $r=a-bq$ with $|r|<|b|$) $|r|\geqq i$, $|b|\geqq i+1$; we see that $P_i'\subseteq P_{i+1}$. Conversely, given a sequence $Q-0=P_0\supseteq P_1\supseteq\cdots$ of product ideals with empty intersection $\bigcap P_i$ such that $P_i'\subseteq P_{i+1}$, the norm defined by $|b|=i$ for every b in P_i-P_{i+1} will fulfil the conditions for a Euclidean algorithm. Hence *there is a one-one correspondence between sequences of this kind and Euclidean algorithms.*

If for another Euclidean algorithm, with the sequence $\overline{P}_i$, always $P_i\subseteq\overline{P}_i$, we say that the first algorithm is the *faster* one (under cer-

Presented to the Society, October 30, 1948; received by the editors September 28, 1948.