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 $|\mathrm{a}|$ 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.

tain additional conditions, indeed less algorithm steps are needed).

If there exists at all a Euclidean algorithm in Q, then *there exists a fastest Euclidean algorithm* defined by the sequence $P_0, P_0', P_0'', \cdots$. Hence *the emptiness of the intersection* $\bigcap P_0^{(i)}$ *is a criterion* (n.a.s.c.) *for the existence of a Euclidean algorithm in* Q.

Any sequence (P_i) as above may be changed to a new sequence $P_1, \cdots, P_{i-1}, \bar{P}_i, \bar{P}_i', \bar{P}_i'', \cdots$, where $\bar{P}_i$ is a product ideal with $P_{i-1} \supseteq \bar{P}_i \supseteq (P_{i-1})'$, so (besides the trivial repetition of identical product ideals) there always exist, if any, different Euclidean algorithms except if there are no product ideals between any $P_0^{(i)}$ and $P_0^{(i+1)}$.

2. **Generalization.** These considerations may be generalized as follows. Let a *tea* (*transfinite Euclidean algorithm*) be an algorithm as before but where (1) we allow $|b|$ to take any ordinal numbers as values; (2) we do not require $|a| \geqq |b|$ for b dividing a. Then it is seen in the usual way that the existence of a *tea* implies that Q is a principal ideal ring.

Further, such a *tea* determines, and is determined by, a transfinite sequence S_λ, $0 \leqq \lambda \leqq \mu$, of subsets of $Q-0$ with (1) $S_\lambda' \subseteq S_{\lambda+1}$, (2) $S_\lambda \subseteq S_{\lambda-1}$, but $S_\lambda = \bigcap S_i$, $i < \lambda$, if $\lambda - 1$ does not exist, (3) empty S_μ.

Defining "faster" as before there is again a *fastest tea* given by $P_0^{(\lambda)}$, where $S^{(\lambda)}$ is defined as $(S^{(\lambda-1)})'$ or $\bigcap S^{(i)}$, $i < \lambda$.

Hence *the criterion for the existence of a tea is the emptiness of some* $P_0^{(\mu)}$.

For the fastest *tea* the sequence consists of product ideals, so that the monotonity condition $|a| \geqq |b|$ for b dividing a is automatically fulfilled.

If no $P_0^{(\lambda)}$ vanishes then there is no *tea*. If Q is not a principal ideal ring this is certainly so, but even for a principal ideal ring the constant $P_0^{(\mu)}$ (which is the largest subset S of Q with $S = S'$, and therefore never a principal ideal) may not be empty, as shown by some of the following examples.

3. **Examples.** The derived set S' of a given set S may also be defined as the set obtained from S by exemption of all b such that for every a, b divides some $a+c$ with c not in S. In particular P_0' is the set of all non-units except 0. Now call a non-unit $b \neq 0$ a *side divisor* of a if b divides some $a+e$, where e is a unit or 0. Then P_0'' is obtained from P_0' by exemption of the *universal side divisors*, that is, of those elements b which are side divisors of every a in Q, or equivalently for which there is a unit, or 0, in every residue class mod b. Such an element is obviously prime; the principal ideal (b) must even be

maximal. If no universal side divisors exist, then $P_0''=P_0'$, and there is, except for the trivial case of a field, no *tea* in Q.

For the ring of rational integers, $Q-P_0'$ has three elements 0, ±1. Hence the universal side divisors are ±2 and ±3, and $Q-P_0''$ contains all c with $|c|<2^2$. By induction, b is in $P_0^{(i)}$ if and only if $|b|\geqq 2^i$. The fastest Euclidean algorithm is given by $a=bq+r$ with minimal $|r|$ (in a fixed algorithm q and r need not be unique).

$P_0''=P_0'$ holds for the algebraic integers of every quadratic number field with negative discriminant d except -1, -2, -3, -7, -11. This can be seen as follows. It is well known that the above integers are the numbers $f+gd^{1/2}$, where f and g denote arbitrary rational integers, and in addition, if 4 divides $d-1$, the numbers $f+1/2+(g+1/2)d^{1/2}$. It follows easily that, except for the five stated values of d, 2 and 3 are irreducible and ±1 the only units, so that the only side divisors of 2 are ±2, ±3; but these are not side divisors of $(1+d^{1/2})/2$, and if this is not an integer, of $d^{1/2}$. Hence there are no universal side divisors. For the excepted values of d there are respectively 12, 4, 24, 4, 4 universal side divisors, among which all the 22 non-real quadratic integers b with $1<b\bar{b}\leqq 3$ occur. (Dedekind [2, Supplement XI, §159 (4th ed., 1894, p. 451)][1] stated that the usual norm gives no Euclidean algorithm for the principal ideal ring belonging to $d=-19$. Hasse [4, p. 11] asked whether a Euclidean algorithm might be obtained by another norm, retaining the multiplicativity condition $|ab|=|a|\,|b|$. We see that this is not the case, even without this condition and allowing ordinal numbers as norm values. Hence we have an example of a principal ideal ring with no Euclidean algorithm. The given result for arbitrary negative discriminant generalizes, and contains a new proof of, the similar result of Dickson [3, pp. 150–151] for the usual norm. For this norm and positive discriminant the question is not entirely solved, see Chatland [1], with further references.)

We have also $P_0''=P_0'$ for the ring of all polynomials, or power series, of one variable over an integral domain that is not a field. Likewise, for a valuation ring with no smallest positive value, $P_0''=P_0'$. If a smallest positive value v exists, then $P_0^{(i)}$ is the set of all elements whose value is at least i, and $P_0^{(\omega)}=P_0^{(\omega+1)}$. In particular for the power series of one variable over a field, $P_0^{(\omega)}=0$. Similarly for the polynomials of one variable over a field, $P_0^{(i)}$ is the set of all polynomials of degree not less than i. This is a special case of the next example.

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

4. **Quotient rings.** If, within the affine space over an algebraically closed field K of arbitrary characteristic, C is a rational curve with no singular point at finite distance, then the ring of all rational functions on C with no poles at finite distance is a principal ideal ring (for example, since we shall see that it has a Euclidean algorithm). The ring consists of all those rational functions with coefficients in K, of a parameter t of the curve, whose poles belong to a given finite set $(t_1, \cdots, t_k)$. Subjecting t, if necessary, to a broken linear transformation, we may suppose $t_1=\infty$. In this case $P^{(i)}$ is the set of all the functions in the ring that have at least i zeros (with due counting of multiplicities) outside $(t_1, \cdots, t_k)$. Indeed, define $|a|$ accordingly as the number of zeros of a outside $(t_1, \cdots, t_k)$; to prove that $|a-bq|<|b|$ can be solved we may (multiplying both by a polynomial c with $|c|=0$) suppose that a and b are polynomials and (shifting other factors of b to q) that b has no zero in $(t_1, \cdots, t_k)$, in which case the usual polynomial q will do. And obviously, since for $|a_1|<|b|$, $|a_2|<|b|$, $a_1\neq a_2$, never $a_1-a_2=bq$, no faster Euclidean algorithm exists.

Similarly a *tea* may be defined in any quotient ring of an integral domain with a given *tea* by letting $|a|$ be the smallest value of $|am/n|$ in the original ring, where m and n are elements of a fixed multiplicatively closed set of denominators that yields the quotient ring considered.

5. **Related notions.** If we modify the definition of the derived set by demanding the existence of an a (not divisible by b) such that $aM+bN\subseteq(S, 0)$, where M and N are given subsets of Q (for instance, the set $0, \pm 1, \pm 2, \cdots$), we obtain sequences of subsets quite similar to those obtained before, which contract the faster the larger the sets M and N are. Here too P_0 is the set of non-units except 0. For $M=N=Q$ and if Q is a principal ideal ring, $P_0^{(i)}$ is the set of all elements that are products of at least i primes, so $P_0^{(\omega)}=0$; the corresponding (multiplicative) norm being γ^i with fixed $\gamma>1$.

Comparing the strength of different notions similar to the usual Euclidean algorithm, we may consider an algorithm (j, k, l), where $j=1$ means that the norm shall be a positive integer, $j=2$ that it be within a set of real positive numbers with no limit point except ∞, $j=3$ that it be an ordinal number; $k=1$ that $|ab|=|a||b|$, $k=2$ that $|a|\geqq|b|$ for b dividing a, $k=3$ no such condition; $l=1$ that, for any $b\neq 0$ and a not divisible by b, there exists some q with $|a-bq|<|b|$, $l=2$ that, in the only relevant case $|a|\geqq|b|$, there only need exist m and q with $|am-bq|<|b|$ and m prime to b (that is, b shall divide

mn only if it divides n), $l=3$ the same, demanding only $|am-bq| < |a|$, $l=4$ again demanding that $|am-bq| < |b|$, but with no restriction for m. So l determines the stepping down condition characteristic for the "descente infinie" application of Euclidean algorithms. We exclude the case $j=3$, $k=1$.

Then the existence of any algorithm (j, k, l) clearly implies that the integral domain Q is a principal ideal ring. It is easily seen that in every principal ideal ring the before mentioned norm γ^i fulfils (1, 1, 2) (see, for example, [4, pp. 7–8]), so that every combination with $l>1$ gives a n.a.s.c. for principal ideal rings. On the other hand, even the weakest condition with $l=1$, which is (3, 3, 1), is not always fulfilled in principal ideal rings, as we have shown; and (3, 3, 1) is equivalent to (3, 2, 1), (2, 3, 1) is equivalent to (2, 2, 1), (1, 3, 1), and (1, 2, 1), and finally (2, 1, 1) to (1, 1, 1), while it remains open whether these three sets of conditions are really of different strength.

A further classification of integral domains may be made according to the number μ of §2, or by (M, N)-stepping down conditions. Thus the fact that (1, 1, 3) is fulfilled for $M=(1)$, $N=(\pm 1)$ in the ring of rational integers is the essence of the simple Kronecker-Zermelo proof [4, p. 3] of unique decomposition into primes. For a similar, still weaker condition than $l=4$ characterizing integral domains with unique decomposition into primes, see Krull [5, pp. 107–108]; also with respect to that condition derived sets may be defined and integral domains grouped according to whether the constant $P^{(\mu)}$ is or is not empty, and according to μ.

References

1. H. Chatland, *On the Euclidean Algorithm in quadratic number fields*, Bull. Amer. Math. Soc. vol. 55 (1949) pp. 948–953.

2. L. Dickson, *Algebren und ihre Zahlentheorie*, Zürich and Leipzig, 1927.

3. P. G. Lejeune Dirichlet, *Vorlesungen über Zahlentheorie*, ed. by R. Dedekind.

4. H. Hasse, *Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen*, J. Reine Angew. Math. vol. 159 (1928) pp. 3–12.

5. W. Krull, *Idealtheorie*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vols. 4, no. 3, 1935.

Hebrew University and
Harvard University