ON K-STAGE EUCLIDEAN DOMAINS

KENNETH H. KEPPEN

ABSTRACT. In this paper, k-stage Euclidean Domains, a notion conceived by George Cooke, are defined and characterized. Following the work of Motzkin, a necessary and sufficient condition for an integral domain to be a k-stage Euclidean Domain is given, and from this the minimum k-stage Euclidean Norm is constructed.

1. DIVISIBILITY IN INTEGRAL DOMAINS

In this paper, let D denote an integral domain, D^* the nonzero elements of D, and $D^\times$ the multiplicative group of units of D. While many of the results herein apply to arbitrary commutative rings, we will focus on integral domains. The following definitions will be used throughout.

Definition 1. An element u in D is called a *unit* if $uv = vu = 1$ for some v in D. Elements a and b in D are called *associate* if $a = ub$ for some unit u in D. a and b are called *relatively prime* if their only common divisors are the units of D.

Definition 2. A nonzero nonunit element r in D is called *irreducible* if whenever a and b are elements in D and $r = ab$, then a or b is a unit. A nonzero nonunit element p in D is called *prime* if $p \mid ab$ implies $p \mid a$ or $p \mid b$.

The following facts are easily derived from the above definitions. i) u is a unit if and only if $\langle u \rangle = D$. ii) a and b are associates if and only if $\langle a \rangle = \langle b \rangle$. iii) A nonzero nonunit element p is prime if and only if $\langle p \rangle$ is a prime ideal.

In some integral domains the set of primes differs from the set of irreducibles. However, we always have

Proposition 1. *If p is prime in D, then p is irreducible.*

PROOF. Suppose that $p = ab$ and $p \mid a$. Then $a = px$ and so $p = (px)b$. By the cancellation law, $1 = xb$, which shows that b is a unit. Hence p is irreducible. Note: The converse is true in case D is a PID or UFD. □

The notion of a greatest common divisor plays a central role throughout this paper.

Definition 3. Let $a_1, \cdots, a_n$ be nonzero elements in D. A *greatest common divisor (gcd)* of $a_1, \cdots, a_n$ is a nonzero element d such that $d \mid a_i$ for all $i = 1, \cdots, n$, and if $d' \mid a_i$ for all $i = 1, \cdots, n$, then $d' \mid d$.

Note that in a general integral domain neither existence nor uniqueness of gcds is guaranteed. Propositions 2 and 3 provide some basic facts about gcds of two elements. Although not explicitly shown, by an easy induction, these propositions hold for any finite number of elements.

Completed during the 1993 NSF REU Program at Oregon State University. Special thanks to Professor Robby Robson for his guidance and enthusiasm during this work.

Proposition 2. *Let a and b be nonzero elements in D and let d be a gcd of a and b. Then the gcds of a and b are precisely the associates of d.*

PROOF. If d' is a gcd of a and b, then $d \mid d'$ and $d' \mid d$. Hence $d = ud', d' = vd$, and so $d = uvd$. By the cancellation law, $1 = uv$. Hence u and v are units which shows that d and d' are associates. Conversely, suppose that d and d' are associates. Then $d = ud'$ and $d' = vd$ for some units u and v. Since $d \mid a, d \mid b$, then $d' \mid a, d' \mid b$. Moreover, whenever $c \mid a, c \mid b$, then $c \mid d$, so $c \mid d'$. Hence d' is a gcd of a and b. □

Proposition 3. *Let a and b be nonzero elements in D. If $\langle a, b\rangle = \langle d\rangle$, then d is a gcd of a and b.*

PROOF. Note first that $d \mid a, d \mid b$ if and only if $a, b \in \langle d\rangle$ if and only if $\langle a, b\rangle \subseteq \langle d\rangle$. Thus $d \in D^*$ is a gcd of a and b if and only if $\langle a, b\rangle \subseteq \langle d\rangle$ and if $\langle a, b\rangle \subseteq \langle d'\rangle$ implies $\langle d\rangle \subseteq \langle d'\rangle$. The proposition follows if $\langle a, b\rangle = \langle d\rangle$. □

We now show that in a PID existence of gcds is guaranteed. Specifically,

Corollary 1. *If D is a PID, then a and b possess a gcd d and there exists elements x and y in D with $d = ax + by$.*

PROOF. Since every ideal in D is principal, then $\langle a, b\rangle = \langle d\rangle$ for some $d \in D$. From the proposition, d is a gcd of a and b, and since $d \in \langle a, b\rangle$, then $d = ax + by$ for some $x, y \in D$.

Corollary 2. *If D is a PID, then c is a gcd of a and b if and only if $\langle a, b\rangle = \langle c\rangle$.*

PROOF. By the proposition, if $\langle a, b\rangle = \langle c\rangle$, then c is a gcd of a and b. Conversely, suppose that c is a gcd of a and b. By Corollary 1, a and b possess a gcd d, where $\langle d\rangle = \langle a, b\rangle$. From Proposition 2 it follows that c and d are associates. Hence $\langle c\rangle = \langle d\rangle = \langle a, b\rangle$.

EXAMPLE 1. In $\mathbb{Z}$, the gcds of 18 and 48 are $\pm$ 6. For any D, $D[x]^\times = D^\times$. Thus in $\mathbb{Q}[x]$, the gcds of $x^2 - 2x + 1$ and $x^2 + x - 2$ are all polynomials $q(x - 1)$ with $q \in \mathbb{Q}^*$. However, in $\mathbb{Z}[x]$, the gcds of $x^2 - 2x + 1$ and $x^2 + x - 2$ are $\pm(x - 1)$.

2. k-STAGE EUCLIDEAN DOMAINS

Next we consider Euclidean Domains in tandem with k-stage Euclidean Domains; essentially domains possessing a weakened Division Algorithm. We first define the notion of a norm on an integral domain D. This is a measure of "size" in D.

Definition 4. Any function $N : D^* \longrightarrow \mathbb{Z}^+ \cup \{0\}$ is called a *norm* on D. N is called *semi multiplicative* if $N(ab) \geq N(a)$ for all nonzero a and b in D.

Note that it is permissible for $N(0)$ to be undefined. Some authors define $N(0) = 0$ or $N(0) = -\infty$, while others define $N(a) > 0$ for all nonzero a. These conventions lack necessity for our purpose, however, and consequently will not be adopted here. The following definition of a Euclidean Domain is not standard, but it will be the definition employed throughout this paper.

Definition 5. An integral domain D is a *Euclidean Domain* (ED) if there is a norm N on D such that D admits an *N-Division Algorithm.* That is, for each pair a, b in D with $b \neq 0$, there exists elements q and r in D with $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$. The element q is called the *quotient* and the element r the *remainder.* Any such norm on D is called a *Euclidean Norm.*

Notation: The following statements will be used synonymously; D is Euclidean for N, N is a Euclidean Norm on D, and $(D, +, \cdot, N)$ is a Euclidean Domain. Note that q and r need not be unique in the N-Division Algorithm. Note also that since D is a ring, additive inverses exist in D. We can therefore write the N-Division Algorithm on D as follows: for each pair a, b in D with $b \neq 0$, there exists elements q and r in D with $a + bq = r$ and either $r = 0$ or $N(r) < N(b)$. This

rephrasing will bear its fruit in sections 3 and 4.

Definition 5 is not standard in that most authors additionally require N to be semi multiplicative. A semi multiplicative Euclidean Norm, as we will see, is useful in characterizing the units and associates in D. However, the main interest in a Euclidean Domain D for N is that the N-Division Algorithm shows that D is a PID and that gcds can always be calculated algorithmically (using the Euclidean Algorithm). To show that D is a PID, given any nonzero ideal I in D, take any nonzero element $b \in I$ with minimal N value. By closure, $\langle b \rangle \subseteq I$. For any $a \in I$, $a = bq + r$ with either $r = 0$ or $N(r) < N(b)$. Since $r = a - bq \in I$, we must have $r = 0$. Thus $a = bq$, and so $I \subseteq \langle b \rangle$. In this proof the semi multiplicative property of N has not been used, and any well-ordered set W could be used for the codomain of N. Employment of the later enlarges the class of Euclidean Domains. Additionally, it is unnecessary for D to be an integral domain to possess a Division Algorithm. Samuel [1] therefore gives the following definition. Given a ring R, a *Euclidean Norm* on R is a map N of R into a well-ordered set W such that R admits an N-Division Algorithm. We will not utilize this definition, however. Definition 5 was chosen in the generality needed to coherently discuss subsequent implications.

EXAMPLE 2. a) A field F is trivially a Euclidean Domain with $N(a) = 0$ for all $a \in F$. Take any pair a, b in F with $b \neq 0$. Then $a = bq + 0$ where $q = b^{-1}a$.

b) $\mathbb{Z}$ is a Euclidean Domain for $N(n) = |n|$.

c) For any field $F, F[x]$ is a Euclidean Domain for $N(f) = \deg(f)$. Here, q and r are unique.

d) $\mathbb{Z}[\sqrt{-2}]$, the ring of algebraic integers of $\mathbb{Q}(\sqrt{-2})$, is a Euclidean Domain for the norm N given by $N(\alpha) = \alpha\overline{\alpha}$. To see this first note that $\alpha + \beta, -\alpha, \alpha\beta$, and 1 are elements of $\mathbb{Z}[\sqrt{-2}]$ whenever α, β are elements of $\mathbb{Z}[\sqrt{-2}]$. Additionally this ring is commutative and has no zero divisors; both properties are inherited from $\mathbb{C}$. Next, take any pair α, β in $\mathbb{Z}[\sqrt{-2}]$ with $\beta \neq 0$. We must show there exists elements τ, ρ in $\mathbb{Z}[\sqrt{-2}]$ with $\alpha = \beta\tau + \rho$, and either $\rho = 0$ or $N(\rho) < N(\beta)$. Let $\xi = \frac{\alpha}{\beta} = x + y\sqrt{-2} \in \mathbb{Q}(\sqrt{-2})$. Choose $\tau = a + b\sqrt{-2}$ in $\mathbb{Z}[\sqrt{-2}]$ with $a \in \mathbb{Z}$ chosen closest to $x \in \mathbb{R}$ and $b \in \mathbb{Z}$ chosen closest to $y \in \mathbb{R}$. Clearly $|x - a| \leq \frac{1}{2}$ and $|y - b| \leq \frac{1}{2}$. It follows that $N(\xi - \tau) = N((x - a) + (y - b)\sqrt{-2}) = (x - a)^2 + 2(y - b)^2 \leq \frac{1}{4} + 2\frac{1}{4} = \frac{3}{4}$. Now if $a = x$ and $b = y$, then $\tau = \frac{\alpha}{\beta}$ and $\alpha = \beta\tau$, which shows that $\rho = 0$. If not, let $\rho = \alpha - \beta\tau = (\frac{\alpha}{\beta} - \tau)\beta = (\xi - \tau)\beta$. We then have $N(\rho) = N(\xi - \tau)N(\beta) \leq \frac{3}{4}N(\beta) < N(\beta)$. This shows that $\mathbb{Z}[\sqrt{-2}]$ admits an N-Division Algorithm. Moreover, let α, β be nonzero elements in $\mathbb{Z}[\sqrt{-2}]$. It follows that $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = N(\alpha)N(\beta) \geq N(\alpha)$, since $N(\alpha), N(\beta) \geq 1$. Whence N is a semi multiplicative Euclidean Norm. Note: Similarly one can show that $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{2}]$ are Euclidean for the norm N given by $N(\alpha) = |\alpha\overline{\alpha}|$.

All of the norms given in EXAMPLE 2 are semi multiplicative. Although hard to find, the next example provides a Euclidean Norm which is not semi multiplicative.

EXAMPLE 3. In $\mathbb{Z}$, let $N(n) = |n|$ for $n \neq 7$ and $N(7) = 15$. We claim that N is a Euclidean Norm on $\mathbb{Z}$ which is not semi multiplicative. To see this take integers a and b with $b \neq 0$ and $b \nmid a$. By the usual Division Algorithm on $\mathbb{Z}$, there exists elements $q, r \in \mathbb{Z}$ with $a = bq + r$ and $|r| < |b|$. If $|b| \leq 7$ or $|b| \geq 16$, then $N(r) < N(b)$. If $8 \leq |b| \leq 15$ and $r \neq 7$, then $N(r) < N(b)$. However, if $8 \leq |b| \leq 15$ and $r = 7$, then $a = qb + 7$ for some q. Rewrite this equation as $a = b(q + 1) + (7 - b) = bq' + r'$. Now if $8 \leq b \leq 15$, then $-8 \leq r' \leq -1$, which shows that $N(r') < N(b)$. And if $-15 \leq b \leq -8$, then $11 \leq r' \leq 18$, which shows that $N(r') < N(b)$. We conclude that $\mathbb{Z}$ is Euclidean for N. However, $N(2 \cdot 7) = 14 < 15 = N(7)$, and so N is not semi multiplicative.

Before introducing k-stage Euclidean Domains we need the following definition.

Definition 6. Let a and b be elements in D. An *n-stage division chain* starting from the pair a, b is a sequence of equations

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1} \\ r_{n-2} &= r_{n-1}q_n + r_n. \end{aligned}$$

Such a division chain is called *terminating* if the last remainder r_n is 0.

Remark: A division chain is completely determined by the sequence of quotients $q_1, \cdots, q_n$. Any sequence $q_1, \cdots, q_n$ of elements in D defines an n-stage division chain starting from the pair a, b.

We now consider a weakening of the Division Algorithm and define a notion conceived by George Cooke [2]. The principal definition is

Definition 7. Let k be a natural number. An integral domain D is a *k-stage Euclidean Domain* if there is a norm N on D such that D admits a *k-stage N-Division Algorithm.* That is, for each pair a, b in D with $b \neq 0$ there exists an n-stage division chain starting from the pair a, b for some $n \leq k$ such that the last remainder r_n satisfies either $r_n = 0$ or $N(r_n) < N(b)$. Any such norm on D is called a *k-stage Euclidean Norm.*

Notice that in a k-stage Euclidean Domain after at most k "divisions" (these are actually divisions in the field of quotients of D) a "smaller" remainder is produced, while a "smaller" remainder is achieved after one "division" in a Euclidean Domain. Note also that the k-stage condition implies the m-stage condition if $m > k$, and that the 1-stage condition is the usual Euclidean property. From this definition, an integral domain D is a *2-stage Euclidean Domain* if there is a norm N on D such that for each pair a, b in D with $b \neq 0$, either i) there exists elements $q, r \in D$ with $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$, or ii) there exists elements $q_1, q_2, r_1, r_2 \in D$ with $a = bq_1 + r_1$, $b = r_1q_2 + r_2$ and either $r_2 = 0$ or $N(r_2) < N(b)$. In section 4 we will consider 2-stage Euclidean Domains in detail.

For k-stage Euclidean Domains, as well as Euclidean Domains, we will show why the semi multiplicative property of a norm is auxillary. More precisely, in sections 3 and 4 we will show that every k-stage Euclidean Domain ($k \geq 1$) has a semi multiplicative k-stage Euclidean Norm.

By further weakening the Division Algorithm we have

Definition 8. An integral domain D is an *ω-stage Euclidean Domain* if there is a norm N on D such that D admits an *ω-stage N-Division Algorithm.* That is, for each pair a, b in D with $b \neq 0$ there exists an n-stage division chain starting from the pair a, b for some natural number n such that the last remainder r_n satisfies either $r_n = 0$ or $N(r_n) < N(b)$.

Note that for every k, the k-stage condition implies the ω-stage condition. k-stage Euclidean Domains will be our primary concern.

The following strict inclusions among classes of integral domains is well known.

$$\text{fields} \subset \text{EDs} \subset \text{PIDs} \subset \text{UFDs} \subset \text{integral domains}$$

What can we say about the intrinsic algebraic properties of k-stage Euclidean Domains? Where do k-stage Euclidean Domains ($k \geq 2$) fit into this chain? The remainder of the paper addresses these questions. Dummit [3] states that there are examples of 2-stage Euclidean Domains which are not PIDs, which as we will show, must contain an infinitely generated ideal; and that there are

examples of domains which are 2-stage Euclidean but are not Euclidean. There are also examples of domains which are not Euclidean for a given norm but which are k-stage Euclidean for the norm. For example, the ring $\mathbb{Z}[\sqrt{14}]$ is not Euclidean for the usual norm N given by $N(\alpha) = |\alpha\overline{\alpha}|$, but is 2-stage Euclidean for this norm (see [2]). Cooke showed that $\mathbb{Z}[\sqrt{d}]$ is 2-stage Euclidean for this N in case d is equal to 14, 22, 23, 31, 38, 43, 46, 53, 61, 69, 77, 89, 93, 97, 113, 129, 133, 137, 181, and 253.

EXAMPLE 4. This example shows that choosing q and r in the Division Algorithm is not a trivial matter. Let $\alpha = 21 + 4\sqrt{14}$, $\beta = -3 + \sqrt{14} \in \mathbb{Z}[\sqrt{14}]$, and $N(\alpha) = |\alpha\overline{\alpha}|$. Using the proof given for $\mathbb{Z}[\sqrt{-2}]$ in Example 2d, we apply the N-Division Algorithm to the pair α, β to get: Step 1 Let $\xi_1 = \frac{\alpha}{\beta} = \frac{116}{5} - \frac{33}{3}\sqrt{14}$ and choose $\tau_1 = 23 + 7\sqrt{14}$. Then $\rho_1 = \alpha - \beta\tau_1 = -8 + 2\sqrt{14}$, and $N(\rho_1) = 8 > 5 = N(\beta)$. Step 2 Let $\xi_2 = \frac{\beta}{\rho_1} = -\frac{1}{2} - \frac{1}{4}\sqrt{14}$. Choosing $\tau_2 = 0$ yields $\rho_2 = \beta - \rho_1\tau_2 = \beta$, so $N(\rho_2) = 5 = N(\beta)$. Choosing $\tau_2 = -1$ yields $\rho_2 = -11 + 3\sqrt{14}$ and $N(\rho_2) = 5 = N(\beta)$. Hence $N(\rho_2) \not< N(\beta)$. Is this a counterexample to the "fact" that $\mathbb{Z}[\sqrt{14}]$ is known to be a 2-stage Euclidean for this norm? The answer is no. Cooke's proof uses continued fractions and the geometry of numbers and does *not* employ the method used to prove that $\mathbb{Z}[\sqrt{-2}]$ is Euclidean. Consequently, a completely different procedure must be used to choose quotients and remainders in the Division Algorithm in $\mathbb{Z}[\sqrt{14}]$.

The existence of a k-stage Division Algorithm has important implications. We now reveal a significant advantage of k-stage Euclidean Domains over PIDs; namely, although gcds exist in both settings, in k-stage Euclidean Domains one has an algorithm for computing them.

Lemma. *Let a and b be elements in an integral domain D with $b \neq 0$ and $a = bq + r$. Then i) d is a gcd of a and b if and only if d is a gcd of b and r, and ii) $\langle a, b\rangle = \langle b, r\rangle$.*

PROOF. i) Suppose d is a gcd of a and b. Then $d \mid a, d \mid b$ and so $d \mid r = a - bq$, which shows that d is a gcd of b and r. The converse is similar. ii) Take $c \in \langle a, b\rangle$, then $c = ax + by = (bq + r)x + by = b(qx + y) + r \in \langle b, r\rangle$. Conversely, take $e \in \langle b, r\rangle$, then $e = bu + rv = bu + (a - bq)v = av + b(u - qv) \in \langle a, b\rangle$. This shows that $\langle a, b\rangle \subseteq \langle b, r\rangle \subseteq \langle a, b\rangle$, and so $\langle a, b\rangle = \langle b, r\rangle$. □

Proposition 4. The Euclidean Algorithm. *Let $(D, +, \cdot, N)$ be a k-stage Euclidean Domain for $k \geq 1$. Let a and b be elements in D with $b \neq 0$. Then the pair a, b has a terminating m-stage division chain for some natural number m, and the last nonzero remainder r_{m-1} is a gcd of a and b. Moreover, $r_{m-1} = ax + by$ for some elements x and y in D.*

PROOF. It follows from the Division Algorithm that there is an n-stage division chain starting from the pair a, b for some $n \leq k$ such that $r_n = 0$ or $N(r_n) < N(b)$. If $r_n = 0$, the chain terminates. If not, it follows from the Division Algorithm that there is a j-stage division chain starting from the pair r_{n-1}, r_n for some $j \leq k$ such that $r_{n+j} = 0$ or $N(r_{n+j}) < N(r_n)$. If $r_{n+j} = 0$, the chain terminates. If not, continue this process. Since $N(r_i)$ is nonnegative for all i, this decreasing sequence of normed remainders must end; say $r_m = 0$. By induction and repeated use of Lemma i) we find that d is a gcd of a and b if and only if d is a gcd of r_{m-1} and 0. Since r_{m-1} is a gcd of r_{m-1} and 0, then r_{m-1} is a gcd of a and b. Alternatively, by induction and repeated use of Lemma ii) we find that $\langle a, b\rangle = \langle r_{m-1}, 0\rangle = \langle r_{m-1}\rangle$. Hence r_{m-1} is a gcd of a and b. To find $x, y \in D$ such that $r_{m-1} = ax + by$, first write $r_{m-1} = r_{m-3} - r_{m-2}q_{m-1}$. Upon successively back solving the equations in the terminating m-stage division chain we find that $r_{m-1} = ax + by$ for some $x, y \in D$. □

It is easy to see that if D is an ω-stage Euclidean Domain then every pair a, b with $b \neq 0$ has a terminating m-stage division chain for some $m \in \mathbb{N}$. Consequently, every ω-stage Euclidean Domain admits a Euclidean Algorithm. As a consequence, although not explicitly stated, every subsequent result from this section applies verbatim to ω-stage as well as k-stage Euclidean Domains.

If D is a k-stage Euclidean Domain ($k \geq 1$) and $a_1, \cdots, a_n \in D^*$, an easy induction shows that $\langle a_1, \cdots, a_n \rangle = \langle d \rangle$ for some nonzero d, d is a gcd of $a_1, \cdots, a_n$, and $d = a_1x_1 + \cdots + a_nx_n$ for elements $x_i \in D$. In particular, we have the following corollary.

Corollary 1. *Every finitely generated ideal in a k-stage Euclidean Domain is principal. Moreover, every Noetherian k-stage Euclidean Domain is a PID.*

The next corollary follows immediately from our work thus far.

Corollary 2. *In a k-stage Euclidean Domain D the following are equivalent: i) a and b are relatively prime, ii) the units of D are precisely the gcds of a and b, iii) $\langle a, b \rangle = D$, and iv) $1 = ax + by$ for some elements x and y in D.*

EXAMPLE 5. The proof that $F[x]$ is Euclidean uses long division to obtain unique elements q and r in the Division Algorithm for $N(f) = \deg(f)$. To find the gcds of $f = x^5 + 2x^4 + 2x^2 + x + 2$ and $g = 2x^3 + 2x^2 + x + 1$ in $\mathbb{Z}_3[x]$ we employ this tactic successively at each step in the Euclidean Algorithm.
Step-1 $f = gq_1 + r_1$ where $q_1 = 2x^2 + 2x$, $r_1 = x^2 + 2x + 2$, and $\deg(r_1) < \deg(g)$.
Step-2 $g = r_1q_2 + r_2$ where $q_2 = 2x + 1$, $r_2 = x + 2$, and $\deg(r_2) < \deg(r_1)$.
Step-3 $r_1 = r_2q_3 + r_3$ where $q_3 = x$, $r_3 = 2$, and $\deg(r_3) < \deg(r_2)$.
Step-4 $r_2 = r_3q_4 + r_4$ where $q_4 = \frac{1}{2}x + 1$, $r_4 = 0$.
Hence a gcd of f and g is 2; the other gcd is 1. This shows that f and g are relatively prime in $\mathbb{Z}_3[x]$.

EXAMPLE 6. To find a gcd of $\alpha = 22 + 4\sqrt{-2}$ and $\beta = 6 + 7\sqrt{-2}$ in $\mathbb{Z}[\sqrt{-2}]$ for the norm $N(a+b\sqrt{-2}) = a^2+2b^2$, we use the proof given in Example 2d in conjuction with the N-Euclidean Algorithm.
Step-1 $\alpha = \beta\tau_1+\rho_1$. Let $\xi_1 = \frac{\alpha}{\beta} = \frac{94}{67} - \frac{65}{67}\sqrt{-2}$ and choose $\tau_1 = 1-\sqrt{-2}$, $\rho_1 = \alpha-\beta\tau_1 = 2-5\sqrt{-2}$. Thus $N(\rho_1) = 54 < 134 = N(\beta)$.
Step-2 $\beta = \rho_1\tau_2+\rho_2$. Let $\xi_2 = \frac{\beta}{\rho_1} = -\frac{29}{27} + \frac{22}{27}\sqrt{-2}$ and choose $\tau_2 = -1+\sqrt{-2}$, $\rho_2 = \beta-\rho_1\tau_2 = -2$. Thus $N(\rho_2) = 4 < N(\rho_1) = 54$.
Step-3 $\rho_1 = \rho_2\tau_3 + \rho_3$. Let $\xi_3 = \frac{\rho_1}{\rho_2} = -1 + \frac{5}{2}\sqrt{-2}$ and choose $\tau_3 = -1 + 2\sqrt{-2}$, $\rho_3 = \rho_1 - \rho_2\tau_3 = -\sqrt{-2}$. Thus $N(\rho_3) = 2 < 4 = N(\rho_2)$.
Step-4 $\rho_2 = \rho_3\tau_4 + \rho_4$. Let $\xi_4 = \frac{\rho_2}{\rho_3} = -\sqrt{-2}$. Hence $\rho_4 = 0$.
It follows from the Euclidean Algorithm that $\rho_3 = -\sqrt{-2}$ is a gcd of α and β; $\sqrt{-2}$ is the other gcd.

EXAMPLE 7. Continuing from EXAMPLE 4, if we apply the Euclidean Algorithm to $\alpha = 21+4\sqrt{14}$ and $\beta = -3 + \sqrt{14}$ in $\mathbb{Z}[\sqrt{14}]$ borrowing the technique used in EXAMPLE 6 to obtain quotients τ_i and remainders ρ_i, we get the following:

$$\begin{array}{lll}
\alpha = \beta\tau_1 + \rho_1 & \rho_1 = -8 + 2\sqrt{14} & N(\rho_1) = 8 > 5 = N(\beta) \\
\beta = \rho_1\tau_2 + \rho_2 & \rho_2 = -11 + 3\sqrt{14} & N(\rho_2) = 5 \\
\rho_1 = \rho_2\tau_3 + \rho_3 & \rho_3 = -19 + 5\sqrt{14} & N(\rho_3) = 11 \\
\rho_2 = \rho_3\tau_4 + \rho_4 & \rho_4 = -11 + 3\sqrt{14} & N(\rho_4) = 5 \\
\rho_3 = \rho_4\tau_5 + \rho_5 & \rho_5 = -19 + 5\sqrt{14} & N(\rho_5) = 11.
\end{array}$$

In general, $\rho_{2k} = -11 + 3\sqrt{14}$ and $\rho_{2k+1} = -19 + 5\sqrt{14}$. Hence the Euclidean Algorithm fails to generate a gcd. The following observation is now evident: *Knowing only that an integral domain*

is k-stage Euclidean for some norm N is not enough to algorithmically calculate gcds using the N-Euclidean Algorithm. Knowing how to choose a quotient and a remainder at each step in the algorithm is imperative.

We now provide some consequences of the Euclidean Algorithm.

Proposition 5. *Let $(D, +, \cdot, N)$ be a k-stage Euclidean Domain. Then an element p in D is prime if and only if p is irreducible.*

PROOF. Suppose that p is irreducible in D, $p \mid ab$, and $p \nmid a$. Suppose further that $u \mid p$ and $u \mid a$. Thus $p = cu$ where c or u is a unit. If c is a unit, then $u = c^{-1}p$. It follows that $p \mid u$, and since $u \mid a$, then $p \mid a$; a contradiction. Hence u must be a unit. This shows that a and p are relatively prime. Thus $1 = px + ay$ for some x and y, and so $b = pbx + aby$. Hence $p \mid b$, and so p is prime. The converse is given by Proposition 1. □

Corollary. *A k-stage Euclidean Domain in which every nonzero nonuit element can be factored into a finite number of irreducibles is a UFD.*

PROOF. Since primes and irreducibles are equivalent in any k-stage Euclidean Domain D, the proof of unique factorization is the same as the uniqueness portion of the proof that every PID is a UFD (see [3]).

Proposition 6. *Let N be a semi multiplicative norm on D. Then i) $N(1) \leq N(a)$ for all nonzero a, and ii) if u is a unit, then $N(u) = N(1)$ and $N(au) = N(a)$ for all nonzero a.*

PROOF. i) For any nonzero a we have $N(1) \leq N(1 \cdot a) = N(a)$. ii) Suppose u is a unit. Then $N(u) \leq N(uu^{-1}) = N(1)$, and so $N(u) = N(1)$. Next let $c = au$ for any nonzero element a. Then $cu^{-1} = a$, and from the semi multiplicative property of N we have $N(c) \geq N(a)$ and $N(c) \leq N(a)$. Thus $N(c) = N(a)$. □

Proposition 7. *Suppose that $(D, +, \cdot, N)$ is a Euclidean Domain, N is semi multiplicative, and a and u are nonzero elements in D. Then the following are equivalent: i) u is a unit, ii) $N(u) = N(1)$, and iii) $N(au) = N(a)$.*

PROOF. We need only show that ii) implies i) and that iii) implies i). (ii $\Rightarrow$ i) If $N(u) = N(1)$, we apply the N-Division Algorithm to get $1 = uq + r$ and either $r = 0$ or $N(r) < N(u)$. Since $N(u)$ is minimal, we must have $r = 0$. Thus $1 = uq$, which shows that u is a unit. (iii $\Rightarrow$ i) Let $c = au \in \langle a \rangle^*$ and suppose that $N(c) = N(a)$. Take $x \in \langle a \rangle$ and write $x = cq + r$ where either $r = 0$ or $N(r) < N(c)$. Since $\langle a \rangle$ is an ideal, then $r \in \langle a \rangle$. If $r \neq 0$, then $r = ay$ with $N(ay) \geq N(a)$; a contradiction. Thus we must have $r = 0$, which shows that $r \in \langle c \rangle$ and so $\langle a \rangle \subseteq \langle c \rangle$. Clearly $\langle c \rangle \subseteq \langle a \rangle$. Hence $\langle c \rangle = \langle a \rangle$, which shows that a and c are associates and that u is a unit. □

EXAMPLE 8. a) For $\mathbb{Z}$ with $N(n) = |n|$, the minimum norm value is 1 for all nonzero integers. Clearly then, ± 1 are the units of $\mathbb{Z}$.

b) For $F[x]$ with $N(f) = \deg(f)$, the minimum norm value is 0 for all nonzero f. Hence $F[x]^\times = F^*$.

c) For $\mathbb{Z}[\sqrt{-2}]$ with $N(a+b\sqrt{-2}) = a^2+2b^2$, the minimum norm value is 1 for all nonzero elements in $\mathbb{Z}[\sqrt{-2}]$. Hence the units of $\mathbb{Z}[\sqrt{-2}]$ are ± 1.

d) For $\mathbb{Z}[\sqrt{14}]$ with $N(a + b\sqrt{14}) = |a^2 - 14b^2|$, the minimum norm value is 1 for all nonzero elements in $\mathbb{Z}[\sqrt{14}]$. It is easy to see that $15 + 4\sqrt{14}$ is the principal unit. Thus every unit in $\mathbb{Z}[\sqrt{14}]$ can be written as $\pm(15 + 4\sqrt{14})^n$ for some integer n. Next, suppose $\alpha = a + b\sqrt{14}$ has $|a^2 - 14b^2| = 1$. Is α a unit? That is, can α be written as $\pm(15 + 4\sqrt{14})^n$? Yes. For if $1 = N(\alpha) = |\alpha\overline{\alpha}|$, then clearly α is a unit. Hence Proposition 7 is true for $\mathbb{Z}[\sqrt{14}]$; a 2-stage Euclidean Domain.

e) EXAMPLE 13 shows that Proposition 7 is false, in general, for k-stage Euclidean Domains ($k \geq 2$).

3. THE MINIMUM EUCLIDEAN NORM

We now outline a significant result obtained by Th. Motzkin [4] which provides a necessary and sufficient condition for an integral domain to be a Euclidean Domain. From among the different possible Euclidean Norms on a Euclidean Domain the *minimum* norm is constructed. The minimum norm will be precisely defined shortly. Additionally, we will show that the semi multiplicative property of a Euclidean Norm is not a necessary condition for the construction of the minimum norm. In section 4 we will see how Motzkin's construction can be adapted to any k-stage Euclidean Domain $k \geq 2$. Two definitions, critical to the remainder of the paper, are given next.

Definition 9. A subset $P \subseteq D^*$ is called a *product ideal* if $PD^* \subseteq P$.

Note that since 0 is not in P, then P is not an ideal.

Definition 10. For any subset $S \subseteq D, S' = \{b \in S \mid \exists a \in D \text{ with } a + bD \subseteq S\}$ is called the *derived set* of S.

Proposition 8. *If P is a product ideal, then P' is a product ideal.*

PROOF. If P is a product ideal, then $PD^* \subseteq P$. Take any $b \in P'$ and any $q \in D^*$. It follows that $bq \in P$ and there is an element $a \in D$ with $a + bD \subseteq P$. Hence $(a + bD)q \subseteq P$ since P is a product ideal. Moreover $(a + bD)q = aq + bqD = c + bqD \subseteq P$. Thus P' is a product ideal. □

Proposition 9. *If $S_1 \subseteq S_2$, then $S_1' \subseteq S_2'$.*

PROOF. Suppose $S_1 \subseteq S_2$ and any take $b \in S_1'$. Then there is an element $a \in D$ with $a + bD \subseteq S_1 \subseteq S_2$ and $a + bD \subseteq S_1 \subseteq S_2$. Hence $b \in S_2'$. □

Proposition 10. *Let N be a semi multiplicative norm on D. Then $P_i = \{b \in D^* \mid N(b) \geq i\}$ is a product ideal for $i = 0, 1, \cdots$.*

PROOF. We must show that $P_iD^* \subseteq P_i$. Take any $b \in P_i$ and any $q \in D^*$. Then $N(b) = i$ and since N is semi multiplicative, $N(bq) \geq N(b) \geq i$. Hence $bq \in P_i$. Note: If N is not semi multiplicative, then P_i need not be a product ideal. □

The next proposition is the key to Motzkin's construction. Its proof is by contradiction which, unfortunately, serves to disguise the idea behind the construction of the minimum norm.

Proposition 11. *Let $(D, +, \cdot, N)$ be a Euclidean Domain and $P_i = \{b \in D^* \mid N(b) \geq i\}$. Then $P_i' \subseteq P_{i+1}$.*

PROOF. Take any $b \in P'$. Then $N(b) \geq i$ and there is an element $a \in D$ with $a + bD \subseteq P_i$. Suppose that $N(b) = i$. Since $b \neq 0$ we apply the N-Division Algorithm to the pair a, b to get $a + bq = r$ and either $r = 0$ or $N(r) < i$. But $r \in a + bD \subseteq P_i$ and so $r \neq 0$ and $N(r) \geq i$; a contradiction. Hence $N(b) \geq i + 1$ which shows that $b \in P_{i+1}$. □

Proposition 12. *Let $D^* = P_0 \supseteq P_1 \supseteq P_2 \supseteq \cdots$ be a sequence of product ideals with $\cap_i P_i = \emptyset$ and $P_i' \subseteq P_{i+1}$. Let N be the norm on D given by $N(b) = i$ for all b in $P_i \backslash P_{i+1}$ (with this norm, $P_i = \{b \in D^* \mid N(b) \geq i\}$). Then $(D, +, \cdot, N)$ is a Euclidean Domain, and N is semi multiplicative.*

PROOF. i) Take any pair a, b in D with $b \neq 0$, $b \nmid a$, and suppose that $N(b) = i$. We must show there exists elements $q, r \in D$ with $a + bq = r$ and $N(r) < i$. Equivalently we can show $a + bD \not\subseteq P_i$. Now if $a + bD \subseteq P_i$, then $b \in P_i' \subseteq P_{i+1}$, and so $N(b) \geq i + 1$; a contradiction. Hence $a + bD \not\subseteq P_i$. ii) Next we must show that $N(ab) \geq N(a)$ for all nonzero a and b. Take any $a, b \in D^*$ and suppose that $N(a) = i$. Then $a \in P_i$, and since P_i is a product ideal, $ab \in P_i$. Hence $N(ab) \geq i$ which

shows that N is semi multiplicative. Note: If the sets of the sequence (P_i) are not product ideals, then N need not be semi multiplicative. □

Conversely we have

Proposition 13. *Let $(D, +, \cdot, N)$ be a Euclidean Domain and let N be semi multiplicative. Then there is a sequence (P_i) of product ideals in D with $P_i = \{b \in D^* \mid N(b) \geq i\}$ satisfying: $D^* = P_0 \supseteq P_1 \supseteq P_2 \supseteq \cdots$, $\cap_i P_i = \emptyset$, and $P_i' \subseteq P_{i+1}$.*

PROOF. Suppose there is a nonzero element b in D with $b \in \cap_i P_i$. Since D is Euclidean for $N, N(b) = k$ for some natural number k. Since $b \in \cap_i P_i$, then $b \in P_{k+1}$, which shows that $N(b) \geq k+1$; a contradiction. Hence $\cap_i P_i = \emptyset$. The remainder of the proof follows from Propositions 10 and 11 and the obvious fact that $P_i \supseteq P_{i+1}$. Note: If N is not semi multiplicative, then (P_i) need not be a sequence of product ideals. □

In conclusion, there exists a 1-1 correspondence between Euclidean Norms on D and sequences of this kind. Each such sequence defines a Euclidean Norm and any Euclidean Norm generates a corresponding sequence.

We now have the machinery for comparing the "size" of Euclidean Norms on D.

Definition 11. Let (P_i) and $(\overline{P_i})$ be the sequences (as discussed in Propositions 12 and 13) in D associated with the Euclidean Norms N and $\overline{N}$, respectively. If $P_i \subseteq \overline{P_i}$ for all i, we say that N is *smaller* than $\overline{N_i}$. Let $(\hat{P}_i)$ be the sequence associated with the Euclidean Norm η. We say that η is the *minimum* Euclidean Norm on D if $\hat{P}_i \subseteq P_i$ for all i, for all such sequences (P_i) in D.

It is easy to see that if there exists a minimum Euclidean Norm on a Euclidean Domain, then it is unique. For if η and η' are both minimum Euclidean Norms on a Euclidean Domain D have corresponding sequences (P_i) and (P_i'), then $P_i \subseteq P_i' \subseteq P_i$. Hence, $P_i = P_i'$, and so $\eta = \eta'$. The following intuitive result is immediate.

Proposition 14. *Let D be a Euclidean Domain. If N is a smaller Euclidean Norm than $\overline{N}$ on D, then $N(b) \leq \overline{N}(b)$ for all nonzero elements b in D. In particular, $\eta(b) \leq N(b)$ for all nonzero elements b in D, for all Euclidean Norms N on D.*

PROOF. Let (P_i) and $(\overline{P_i})$ be the associated sequences for N and $\overline{N}$, and take any $b \in P_i \backslash P_{i+1}$ for some i. Then $N(b) = i$, and since $P_i \subseteq \overline{P_i}$ for all i, then $\overline{N}(b) \geq i$. The second assertion follows from the definition of the minimum Euclidean Norm. □

Where we have used *smaller* and *minimum* in the above definition, Motzkin used *faster* and *fastest*, respectively, and commented that under certain additional conditions the N-Euclidean Algorithm requires fewer algorithm steps than the $\overline{N}$-Euclidean Algorithm. This claim is not easily justified, however, and consequently we will choose not to subscribe to his nomenclature.

We now show the existence of the minimum Euclidean Norm. Motzkin assumed the semi multiplicative property in the next proposition. We now prove the desired result without the semi multiplicative assumption.

Proposition 15. *Let D be an integral domain. Construct inductively the following sequence. Let $D_0 = D^*$ and $D_{i+1} = D_i'$ so that $(D_i) = (D_0, D_0', D_0'', \cdots)$. Then D is a Euclidean Domain if and only if $\cap_i D_i = \emptyset$. In which case, the norm η given by $\eta(b) = i$ for all b in $D_i \backslash D_{i+1}$ is the minimum Euclidean Norm on D, and η is semi multiplicative.*

PROOF. Note first that D_0 is a product ideal, so by Proposition 8, each D_i is a product ideal. Secondly, since $D_i \supseteq D_i'$, then $D_0 \supseteq D_1 \supseteq D_2 \supseteq \cdots$. Now suppose D is Euclidean for some norm N. Then N defines an associated sequence (P_i) of sets as described in Proposition 13. We claim that $D_i \subseteq P_i$ for all i. Now $D_0 = P_0$, so by Propositions 9 and 11, $D_1 \subseteq P_0' \subseteq P_1$. Similarly,

whenever $D_i \subseteq P_i$, it follows that $D_{i+1} \subseteq P_i' \subseteq P_{i+1}$. By induction on i we conclude that $D_i \subseteq P_i$ for all i. Since $\cap_i P_i = \emptyset$, then clearly $\cap_i D_i = \emptyset$. Conversely, if $\cap_i D_i = \emptyset$, then by Proposition 12, (D_i) defines a semi multiplicative Euclidean Norm η on D given by $\eta(b) = i$ for all $b \in D_i \backslash D_{i+1}$. Since $D_i \subseteq \overline{P_i}$ for all i for the sequence $(\overline{P_i})$ associated with any Euclidean Norm $\overline{N}$, then η is the minimum Euclidean Norm on D. □

The following significant result is immediate.

Corollary. *Every Euclidean Domain has a semi multiplicative Euclidean Norm.*

Let (D_i) be the sequence defined in Proposition 15. Take $b \in D_i$, and $a, q \in D$. We then have: $b \notin D_i' \iff$ for all a, $a + bD \not\subseteq D_i \iff$ for all a, there exists a q with $c = a + bq \notin D_i \iff$ for all a there exists a $c \notin D_i$ with $c - a \in bD \iff$ for all a there exists a $c \notin D_i$ with $a \equiv c \bmod bD \iff \phi : D_i^c \longrightarrow D/bD$ is a surjective mapping given by $\phi(a) = a + bD \iff D/bD$ admits a complete residue system (CRS) of left coset representatives in D_i^c. Hence $D_i \backslash D_{i+1} = \{b \in D_i \mid D/bD$ admits a CRS in $D_i^c\}$. These equivalent statements immediately give our next proposition.

Proposition 16. $D_0 \backslash D_1 = D^\times$

PROOF. $D_0 = D^*$, so $D_0 \backslash D_1 = \{b \in D^* \mid D/bD$ has exactly one left coset$\} = \{b \in D^* \mid bD = D\}$. Since $\langle u \rangle = uD = D$ if and only if u is a unit, then $D_0 \backslash D_1 = D^\times$. □

Corollary. *Let η be the minimum Euclidean Norm on a Euclidean Domain D. Then $\eta(u) = 0$ if and only if u is a unit.*

PROOF. By definition, $\eta(u) = 0$ if and only if $u \in D_0 \backslash D_1 = D^\times$.

EXAMPLE 9. a) $\mathbb{Z}^\times = \{\pm 1\}$ and for the usual norm N given by $N(n) = |n|$, $N(\pm 1) = 1$. Therefore N cannot be the minimum Euclidean Norm on $\mathbb{Z}$.
b) $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ and $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$. For the norm N given by $N(\alpha) = \alpha\overline{\alpha}, N(u) = 1$ for $u = \pm 1, \pm i$. Therefore N cannot be the minimum Euclidean Norm on either of these Euclidean Domains.

Next we construct the minimum Euclidean Norm η on $\mathbb{Z}$ and on $F[x]$.

EXAMPLE 10. Let $D = \mathbb{Z}$. Then $D_0 = \mathbb{Z}^*$ and $D_0 \backslash D_1 = \{\pm 1\}$, which shows that $D_1 = D \backslash \{0, \pm 1\}$. Next, $D_1 \backslash D_2 = \{b \in D_1 \mid D/bD$ has a CRS in $D_1^c\}$. Clearly $\{0, \pm 1\}$ contains representatives only for $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$, so $D_1 \backslash D_2 = \{\pm 2, \pm 3\}$. This shows that $D_2 = D \backslash \{0, \pm 1, \pm 2, \pm 3\}$. Similarly, $D_2 \backslash D_3 = \{b \in D_2 \mid D/bD$ has a CRS in $D_2^c\} = \{\pm 4, \pm 5, \pm 6, \pm 7\}$. By induction on i we conclude that $D_i \backslash D_{i+1} = \{b \in \mathbb{Z} \mid 2^i \leq |b| < 2^{i+1}\}$. Hence $\eta(b) = i$ if and only if $2^i \leq |b| < 2^{i+1}$ if and only if $i \leq \log_2 |b| < i + 1$. So $\eta(b) = \lfloor \log_2 |b| \rfloor =$ the number of digits in the base 2 representation of b.

Some important comments are now in order. Let N be the usual Euclidean Norm on $\mathbb{Z}$, i.e. $N(n) = |n|$. Take any pair a, b in $\mathbb{Z}$ with $b \neq 0$. For this norm, the proof of the N-Division Algorithm shows that to obtain a quotient and a remainder we simply "divide" a by b. To obtain a gcd of a and b we apply this procedure iteratively in the N-Euclidean Algorithm. When this scheme is employed in the η-Euclidean Algorithm, a quotient and a remainder is obtained at each step as well. In fact, the quotients and remainders obtained from the η-Euclidean Algorithm are simply the binary representations of the quotients and remainders obtained at the corresponding steps in the N-Euclidean Algorithm. As a result, although $\eta(n) \leq N(n)$ for all nonzero integers n, the number of Euclidean Algorithm steps required to obtain a gcd of a and b is the same for both η and N. Consequently, for this scheme of choosing quotients and remainders, η is the minimum norm but not the "fastest" norm.

However, if quotients and remainders are chosen differently, η may in fact be "faster" than N (or vise versa). This reveals a noteworthy point about Motzkin's construction; while it is *constructive*,

it is not *instructive*. That is, Proposition 15 shows how to construct the minimum Euclidean Norm on a Euclidean Domain but it in no way instructs how the minimum norm can be used in the Euclidean Algorithm to obtain gcds. Thus in $\mathbb{Z}$, the above method for obtaining quotients and remainders may not be the "fastest" method to obtain a gcd using the η-Euclidean Algorithm. This discussion underscores our decision to avoid the terms *faster* and *fastest* when comparing Euclidean Norms.

EXAMPLE 11. Let $D = F[x]$ for any field F. Here we construct the sequence (D_i), and hence the minimum Euclidean Norm η, directly. It is easily seen that $D_0 = F[x]^*$ and $D_1 = D_0 \backslash F^* = \{f \mid \deg(f) \geq 1\}$. Next, $D_2 = \{f \in D_1 \mid \exists\, g \in F[x] \text{ with } g + \langle f \rangle \subseteq D_1\}$. Take $f, g \in F[x]$ with $\deg(f) = 1$. The Division Algorithm (for $N(f) = \deg(f)$) gives $g + fq = 0$ or $\deg(g + fq) < 1$; neither of these possible remainders is in D_1. Hence polynomials of degree 1 are not in D_2, and so $D_2 \subseteq \{f \mid \deg(f) \geq 2\}$. Now suppose $\deg(f) \geq 2$. Then every polynomial in $\langle f \rangle = \{fq \mid q \in F[x]\}$ is either the zero polynomial or has degree ≥ 2. Hence for any polynomial g of degree 1, $g + \langle f \rangle \subseteq D_1$. This shows that $\{f \mid \deg(f) \geq 2\} \subseteq D_2$, and so $D_2 = \{f \mid \deg(f) \geq 2\}$. By induction on $\deg(f)$ it follows that $D_i = \{f \mid \deg(f) \geq i\}$ and $\cap_i D_i = \emptyset$. Moreover, $\eta(f) = i$ for all $f \in D_i \backslash D_{i+1} = \{f \mid \deg(f) = i\}$, which shows that η is the usual degree function on $F[x]$.

EXAMPLE 12. When Motzkin's construction is applied to the Euclidean Domain $D = \mathbb{Z}[i]$, the minimum norm η is difficult to compute. In particular, $D_0 = \mathbb{Z}[i]^*$ (note that $|D_0^c| = 1$) and $D_0 \backslash D_1 = \{\pm 1, \pm i\}$. Thus $D_1 = \mathbb{Z}[i] \backslash \{0, \pm 1, \pm i\}$, which is the set of all lattice points on or inside the circle centered at the origin having radius $\sqrt{1}$. Note that $|D_1^c| = 5$. A calculation shows that $D_2 = \{\beta \in D_1 \mid \exists\, \alpha \in \mathbb{Z}[i] \text{ with } \alpha + \beta\mathbb{Z}[i] \subseteq D_1\} = \mathbb{Z}[i] \backslash \{0, \pm 1, \pm i, \pm 2, \pm 2i, \pm 1 \pm 2i, \pm 2 \pm i\}$, which implies that D_2^c is the set of all lattice points on or inside the circle centered at the origin having radius $\sqrt{5}$. Note that $|D_2^c| = 21$. One further calculation shows that D_3^c consists of all the lattice points on or inside the circle centered at the origin having radius $\sqrt{21}$. The obvious conjecture is that D_i^c is the set of all the lattice points on or inside the circle centered at the origin having radius $\sqrt{|D_{i-1}^c|}$. The first five such cardnalities are 1, 5, 21, 69, and 221. Furthermore, since we know that $\mathbb{Z}[i]$ is Euclidean, then $\cap_i D_i = \emptyset$. However, a formula has not yet been found for calculating the number of lattice points inside a circle centered at the origin having an arbitrary radius. This is an unsolved problem proposed by Gauss. As a result, an explicit formula for D_i cannot be found and hence the minimum norm η cannot be constructed. The structure of η for $\mathbb{Z}[\sqrt{-2}]$ appears to be equally difficult. In $\mathbb{Z}[\sqrt{-2}]$, Samuel [1] found the cardnalities of D_i^c for $i = 1, 2, \cdots, 9$ to be: 1, 3, 9, 21, 35, 61, 99, 153, 227, and 327.

4. THE MINIMUM k-STAGE EUCLIDEAN NORM

We now follow the lead of Motzkin and derive a constructive criterion for an integral domain to be a 2-stage Euclidean Domain. Motkin's construction for Euclidean Domains is used as a template for the 2-stage construction which follows. From this construction the minimum 2-stage Euclidean Norm is determined. We then show how this criterion can be extended to k-stage Euclidean Domains for any natural number k.

For a Euclidean Domain $(D, +, \cdot, N)$ and the product ideal $P_i = \{b \in D^* \mid N(b) \geq i\}$, Motzkin embeds the N-Division Algorithm (Definition 5) into the derived set $P_i' = \{b \in P_i \mid \exists\, a \in D \text{ with } a + bD \subseteq P_i\}$. In Proposition 11, the key to Motzkin's construction, we showed by contradiction that $P_i' \subseteq P_{i+1}$. We now would like to develop a similar relationship for a 2-stage Euclidean Domain. By definition, any Euclidean Domain is a 2-stage Euclidean Domain, so any necessary and sufficient condition for an integral domain D to be a 2-stage Euclidean Domain must also hold in case D is Euclidean. Recall that D is a 2-stage Euclidean Domain if there is a norm N on D such that for

each a, b pair in D with $b \neq 0$, either i) there exists elements $q, r \in D$ with $a + bq = r$ and either $r = 0$ or $N(r) < N(b)$, or ii) there exists elements $q_1, q_2, r_1, r_2 \in D$ with $a + bq_1 + r_1$, $b + r_1q_2 = r_2$ and either $r_2 = 0$ or $N(r_2) < N(b)$. In developing an analogous construction for 2-stage Euclidean Domains we seek to "extend" Motzkin's construction to include condition ii). For any set S, the result that follows centers around a new *double derived* set $S^{(2)} \subseteq S'$, which unravels the 2-stage Division Algorithm in much the same manner that S' unravels the (1-stage) Division Algorithm.

The principal definition in this section therefore is

Definition 12. For any subset $S \subseteq D$, $S^{(2)} = \{b \in S | \exists a \in D$ with $a+bD \subseteq S$, $b+(a+bD)D \subseteq S\}$ is called the *double derived set* of S.

With the double derived set we may now prove 2-stage results analogous to Motzkin's 1-stage construction.

Proposition 8′. *If P is a product ideal, then $P^{(2)}$ is a product ideal.*

PROOF. If P is a product ideal, $PD^* \subseteq P$. Take any $b \in P^{(2)}$ and any $q \in D^*$. It follows that $bq \in P$ and there is an element $a \in D$ with $a+bD \subseteq P$ and $b+(a+bD)D \subseteq P$. Hence $(a+bD)q \subseteq P$ since P is a product ideal, and $(a+bD)q = aq+bqD \subseteq P$. Similarly, $(b+(a+bD)D)q = bq+(aq+bqD)D \subseteq P$. Thus $P^{(2)}$ is a product ideal. □

Proposition 9′. *If $S_1 \subseteq S_2$, then $S_1^{(2)} \subseteq S_2^{(2)}$.*

PROOF. Suppose $S_1 \subseteq S_2$ and take any $b \in S_1^{(2)}$. Then there is an element $a \in D$ with $a + bD \subseteq S_1 \subseteq S_2$ and $b + (a + bD)D \subseteq S_1 \subseteq S_2$. Hence $b \in S_2^{(2)}$. □

We prove the next proposition by contradiction, just as Proposition 11 was proven.

Proposition 11′. *Let $(D, +, \cdot, N)$ be a 2-stage Euclidean Domain and $P_i = \{b \in D^* \mid N(b) \geq i\}$. Then $P_i^{(2)} \subseteq P_{i+1}$.*

PROOF. Take any $b \in P_i^{(2)}$. Then $N(b) \geq i$ and there is an element $a \in D$ with $a + bD \subseteq P_i$ and $b + (a + bD)D \subseteq P_i$. Suppose that $N(b) = i$. Since $b \neq 0$ we apply the 2-stage N-Division Algorithm to the pair a, b to get either i) there exists elements $q, r \in D$ with $a + bq = r$ and either $r = 0$ or $N(r) < N(b)$, or ii) there exists elements $q_1, q_2, r_1, r_2 \in D$ with $a + bq_1 = r_1$, $b + r_1q_2 = r_2$ and either $r_2 = 0$ or $N(r_2) < i$. If i) is true, note that $r = a + bq \in a + bD \subseteq P_i$. It follows that $r \neq 0$ and $N(r) \geq i$; a contradiction. If ii) is true, note that $r_1 = a + bq_1 \in a + bD$ and $r_2 = b + r_1q_2 \in b + (a + bD)D \subseteq P_i$. It follows that $r_2 \neq 0$ and $N(r_2) \geq i$; a contradiction. Hence $N(b) > i$, which shows that $b \in P_{i+1}$. □

Proposition 12′. *Let $D^* = P_0 \supseteq P_1 \supseteq P_2 \supseteq \cdots$ be a sequence of product ideals with $\cap_i P_i = \emptyset$ and $P_i^{(2)} \subseteq P_{i+1}$. Let N be the norm on D given by $N(b) = i$ for all b in $P_i \backslash P_{i+1}$ (with this norm, $P_i = \{b \in D^* \mid N(b) \geq i\}$). Then $(D, +, \cdot, N)$ is a 2-stage Euclidean Domain, and N is semi multiplicative.*

PROOF. i) Take any pair a, b in D with $b \neq 0$, $b \nmid a$, and suppose that $N(b) = i$. We must show either (1) there exists elements $q, r \in D$ with $a + bq = r$ and $N(r) < i$, or (2) there exists elements $q_1, q_2, r_1, r_2 \in D$ with $a + bq = r$, $b + r_1q_2 = r_2$, and either $r_2 = 0$ or $N(r_2) < i$. Equivalently we can show (1) $a + bD \not\subseteq P_i$, or (2) $a + bD \subseteq P_i$ and $b + (a + bD)D \not\subseteq P_i$. Now if $a + bD \not\subseteq P_i$, then there exists elements $q, r \in D$ with $a + bq = r \in P_i^c$, which shows that $N(r) < i$. On the other hand, if $a + bD \subseteq P_i$, suppose that $b + (a + bD)D \subseteq P_i$. Then $b \in P_i^{(2)}$, and by hypothesis $b \in P_{i+1}$, which shows that $N(b) \geq i + 1$; a contradiction. Hence $b + (a + bD)D \not\subseteq P_i$. ii) Next, we must show that $N(ab) \geq N(a)$ for all nonzero a and b. Take any $a, b \in D^*$ and suppose that $N(a) = i$. Then $a \in P_i$, and since P_i is a product ideal, $ab \in P_i$. Hence $N(ab) \geq i$, which shows that N is

semi multiplicative. Note: If the sets of the sequence (P_i) are not product ideals, then N need not be semi multiplicative. □

Conversely we have

Proposition 13′. *Let $(D,+,\cdot,N)$ be a 2-stage Euclidean Domain and let N be semi multiplicative. Then there is a sequence (P_i) of product ideals in D with $P_i = \{b \in D^* \mid N(b) \geq i\}$ satisfying: $D^* = P_0 \supseteq P_1 \supseteq P_2 \supseteq \cdots$, $\cap_i P_i = \emptyset$, and $P_i^{(2)} \subseteq P_{i+1}$.*

PROOF. This proposition follows directly from Proposition 13, $10', 11'$. □

In conclusion, as with Euclidean Domains, there is a 1-1 correspondence between 2-stage Euclidean Norms and sequences of this kind. Each such sequence defines a 2-stage Euclidean Norm and any 2-stage Euclidean Norm generates a corresponding sequence. Consequently, the definitions of a *smaller* 2-stage Euclidean Norm and the *minimum* 2-stage Euclidean Norm are the same as for Euclidean Norms. Moreover, if N is a smaller 2-stage Euclidean Norm than $\overline{N}$ on D, then $N(b) \leq \overline{N}(b)$ for all nonzero b. Additionally, if a 2-stage Euclidean Domain has a minimum 2-stage Euclidean Norm, then it is unique.

We now show the existence of the minimum 2-stage Euclidean Norm. The desired result for 2-stage Euclidean Domains is

Proposition 15′. *Let D be an integral domain. Construct inductively the following sequence. Let $D_0 = D^*$ and $D_{i+1} = D_i^{(2)}$ so that $(D_i) = (D_0, D_0^{(2)}, D_0^{(2)(2)}, \cdots)$. Then D is a 2-stage Euclidean Domain if and only if $\cap_i D_i = \emptyset$. In which case, the norm η given by $\eta(b) = i$ for all b in $D_i \backslash D_{i+1}$ is the minimum 2-stage Euclidean Norm on D, and η is semi multiplicative.*

PROOF. The proof follows directly from Propositions $8', 9', 12', 13'$ and is nearly identical to the proof given for Proposition 15.

From this construction we readily see that analogous results hold for k-stage Euclidean Domains for any natural number k. For example if $(D,+,\cdot,N)$ is a 3-stage Euclidean Domain, the 3-stage Euclidean Algorithm says that for each a,b pair in D with $b \neq 0$, either i) there exists elements $q, r \in D$ with $a + bq = r$ and either $r = 0$ or $N(r) < N(b)$, or ii) there exists elements $q_1, q_2, r_1, r_2 \in D$ with $a + bq_1 = r_1, b + r_1 q_2 = r_2$ and either $r_2 = 0$ or $N(r_2) < N(b)$, or iii) there exists elements $q', q'', q''', r', r'', r''' \in D$ with $a + bq' = r', b + r'q'' = r'', r' + r''q''' = r'''$, and either $r''' = 0$ or $N(r''') < N(b)$. Hence for P_i, the *triple derived set* is $P_i^{(3)} = \{b \in P_i \mid \exists\, a \in D$ with $a + bD \subseteq P_i$, $b + (a + bD)D \subseteq P_i$, $(a + bD) + (b + (a + bD)D)D \subseteq P_i\}$. In particular, the following corollary easily follows.

Corollary. *Every k-stage Euclidean Domain ($k \geq 1$) has a unique minimum k-stage Euclidean Norm. Moreover, every k-stage Euclidean Domain has a semi multiplicative k-stage Euclidean Norm.*

Note further that if we define inductively the *kth derived set* $D_i^{(k)}$ of D_i we have the following inclusions

$$D_i' \supseteq D_i^{(2)} \supseteq \cdots \supseteq D_i^{(k)} \supseteq \cdots ;$$

which shows that if η_k is the minimum k-stage Euclidean Norm on D then for any $j \geq k$, $\eta_k(b) \geq \eta_j(b)$ for all b. Theses ideas are illustrated in our final example.

EXAMPLE 13. Since $D = \mathbb{Z}$ is Euclidean, then D is 2-stage Euclidean. Hence $\cap_i D_i = \emptyset$ where (D_i) is the 2-stage sequence constructed in Proposition 15′. In particular, $D_0 = \mathbb{Z}^*$ and $D_1 = D_0^{(2)} = \{b \in \mathbb{Z} \mid \exists\, a \in \mathbb{Z}$ with $a + b\mathbb{Z} \subseteq \mathbb{Z}^*, b + (a + b\mathbb{Z})\mathbb{Z} \subseteq \mathbb{Z}^*\}$. A computation reveals that $D_1 = \mathbb{Z}\backslash\{0, \pm1, \pm2, \pm3, \pm4, \pm6\}$. Thus $\eta_2(n) = 0$ if and only if $n = \pm1, \pm2, \pm3, \pm4, \pm6$,

whereas $\eta_1(n) = 0$ if and only if $n = \pm 1$. Additionally, $\eta_1(n) > 0$ for $|n| > 1$. Note further that $\eta_2(6) = \eta_2(2 \cdot 3) = \eta_2(2)$ but neither 2 nor 3 is a unit in $\mathbb{Z}$. This shows that the converse of Proposition 6 ii) is not true in a general k-stage Euclidean Domain. That is, in a general k-stage Euclidean Domain, neither $N(u) = N(1)$ nor $N(au) = N(a)$ implies that u is a unit. Furthermore, $N(u) = 0$ if and only if u is a unit is not true in the general k-stage setting.

There are a multitude of unanswered problems concerning k-stage Euclidean Domains. The following are of immediate importance: i) find a 2-stage Euclidean Domain which is not a Euclidean Domain for any norm, and ii) find a 2-stage Euclidean Domain which is not a PID (necessarily not Noetherian). Cooke [3] comments that he "does not know of an ω-stage Euclidean Domain which is not a 2-stage Euclidean Domain". This raises an important question; does there exist a k-stage Euclidean Domain for $k \geq 3$?

References

[1] P. Samuel, *About Euclidean Rings,* Journal of Algebra, 19, 282-301 (1971).
[2] G.E. Cooke, *A Weakening of the Euclidean Property for Integral Domains and Applications to Algebraic Number Theory I,* Journal Fur Mathematik, vol 282 (1976)
[3] D.S. Dummit and R.M. Foote, *Abstract Algebra,* ch 8, Prentice Hall (1991).
[4] Th. Motzkin, *The Euclidean Algorithm,* Bulletin of the American Mathematical Society, vol. 55, 1142 - 1146 (1949).
[5] E. Bedocchi, *L' Anneau* $\mathbb{Z}[\sqrt{14}]$ *et L' Algorthme Euclidien,* Manuscripta Math. 53, 199-216 (1985).
[6] G.E. Cooke, *A Weakening of the Euclidean Property for Integral Domains and Applications to Algebraic Number Theory II,* Journal Fur Mathematik, vol 283/284 (1976)
[7] T.M. Apostol, *Imtroduction to Analytic Number Theory,* Springer-Verlag UTM (1976).
[8] J.B. Fraleigh, *A First Course in Abstract Algebra,* 4th ed., ch. 6, Addison-Wesley (1989).

Department of Mathematics, Oregon State University, Corvallis 97331-4605
E-mail: keppen@math.orst.edu