

# REMARKS ABOUT EUCLIDEAN DOMAINS

KEITH CONRAD

## 1. INTRODUCTION

The following definition of a Euclidean (not Euclidian!) domain is very common in textbooks. We write  $\mathbf{N}$  for  $\{0, 1, 2, \dots\}$ .

**Definition 1.1.** An integral domain  $R$  is called *Euclidean* if there is a function  $d: R - \{0\} \rightarrow \mathbf{N}$  with the following two properties:

- (1)  $d(a) \leq d(ab)$  for all nonzero  $a$  and  $b$  in  $R$ ,
- (2) for all  $a$  and  $b$  in  $R$  with  $b \neq 0$  we can find  $q$  and  $r$  in  $R$  such that

$$a = bq + r, \quad r = 0 \text{ or } d(r) < d(b).$$

We will call (1) the *d-inequality*. Sometimes it is expressed in a different way: for nonzero  $x$  and  $y$  in  $R$ , if  $x \mid y$  then  $d(x) \leq d(y)$ . This is equivalent to the *d-inequality*.

Examples of Euclidean domains are  $\mathbf{Z}$  (with  $d(n) = |n|$ ),  $F[T]$  for a field  $F$  (with  $d(f) = \deg f$ ; this example is *the* reason that one doesn't assume  $d(0)$  is defined), and  $\mathbf{Z}[i]$  ( $d(\alpha) = N(\alpha)$ ). A trivial kind of example is a field  $F$  with  $d(a) = 1$  for all  $a \neq 0$  (here all remainders are 0). For any Euclidean domain  $(R, d)$  in the sense of Definition 1.1, other examples are  $(R, 2d)$ ,  $(R, d^2)$ , and  $(R, 2^d)$ .

Definition 1.1 is used in [1, §2.1], [5, §37], [6, §7.2], [7, §6.5], [9, §3.7], [10, Chap. III §3], and [18, §18], which shows that Definition 1.1 accounts for all the basic examples (since otherwise we wouldn't see Definition 1.1 so widely used). However, we find a different definition in [4, §8.1], where the *d-inequality* is missing:

**Definition 1.2.** An integral domain  $R$  is called *Euclidean* if there is a function  $d: R - \{0\} \rightarrow \mathbf{N}$  such that  $R$  has division with remainder with respect to  $d$ : for all  $a$  and  $b$  in  $R$  with  $b \neq 0$  we can find  $q$  and  $r$  in  $R$  such that

$$(1.1) \quad a = bq + r, \quad r = 0 \text{ or } d(r) < d(b).$$

We allow  $a = 0$  in this definition since in that case we can use  $q = 0$  and  $r = 0$ .

A function  $d: R - \{0\} \rightarrow \mathbf{N}$  that satisfies (1.1) will be called a *Euclidean function* on  $R$ . Thus a Euclidean domain in Definition 1.2 is an integral domain that admits a Euclidean function, while a Euclidean domain in Definition 1.1 is an integral domain that admits a Euclidean function satisfying the *d-inequality*.

Does Definition 1.2 describe a larger class of rings than Definition 1.1? No. We will show in Section 2 that every Euclidean domain  $(R, d)$  in the sense of Definition 1.2 can be equipped with a different Euclidean function  $\tilde{d}$  such that  $\tilde{d}(a) \leq \tilde{d}(ab)$  for all  $a$  and  $b$  in  $R$ , so  $(R, \tilde{d})$  is Euclidean in the sense of Definition 1.1.

The main reason that the *d-inequality* is not included in the definition of a Euclidean domain in [4] is that it is irrelevant to prove the two main theorems about Euclidean domains:

that every ideal in a Euclidean domain is principal<sup>1</sup> and that the Euclidean algorithm in a Euclidean domain terminates after finitely many steps and produces a greatest common divisor. There can be greatest common divisors in rings that are not Euclidean (such as in  $\mathbf{Z}[X, Y]$ ), but it may be hard in those rings to compute greatest common divisors by a method that avoids factorization. When a ring is Euclidean, the Euclidean algorithm in the ring lets us compute greatest common divisors without having to factor, which makes this method practical.

Why is the  $d$ -inequality mentioned so often in the (textbook) literature if it's actually not needed? While it is not needed for the two specific results cited in the previous paragraph, it is convenient to use the  $d$ -inequality if we want to prove there is factorization into irreducibles in Euclidean domains without having to rely on a proof of this property by more abstract methods for a larger collection of integral domains. This will be done in Section 4 (specifically, Theorem 4.2) after working out some preliminary results in Section 3.

In Section 5 we discuss Euclidean domains among quadratic rings.

## 2. REFINING THE EUCLIDEAN FUNCTION

Suppose  $(R, d)$  is a Euclidean domain in the sense of Definition 1.2. We will introduce a new Euclidean function  $\tilde{d}: R - \{0\} \rightarrow \mathbf{N}$ , built out of  $d$ , which satisfies  $\tilde{d}(a) \leq \tilde{d}(ab)$ . Then  $(R, \tilde{d})$  is Euclidean in the sense of Definition 1.1, so the rings that admit Euclidean functions in either sense are the same.

Here's the definition (trick?): for nonzero  $a$  in  $R$ , set

$$\tilde{d}(a) = \min_{b \neq 0} d(ab).$$

That is,  $\tilde{d}(a)$  is the smallest  $d$ -value on the nonzero multiples of  $a$ . (We have  $ab \neq 0$  when  $b \neq 0$  since  $R$  is an integral domain.) Since  $a = a \cdot 1$  is a nonzero multiple of  $a$ ,

$$(2.1) \quad \tilde{d}(a) \leq d(a)$$

for all nonzero  $a$  in  $R$ . For each  $a \neq 0$  in  $R$ ,  $\tilde{d}(a) = d(ab_0)$  for some nonzero  $b_0$  and  $d(ab_0) = \tilde{d}(a) \leq d(ab)$  for all nonzero  $b$ . For example,

$$\tilde{d}(1) = \min_{b \neq 0} d(b)$$

is the smallest  $d$ -value on  $R - \{0\}$ .

**Theorem 2.1.** *Let  $(R, d)$  be a Euclidean domain in the sense of Definition 1.2. Then  $(R, \tilde{d})$  is Euclidean in the sense of Definition 1.1.*

If you want to use Definition 1.1 as the definition of a Euclidean domain then you can skip the proof of Theorem 2.1.

*Proof.* For nonzero  $a$  and  $b$  in  $R$  we have

$$\tilde{d}(a) \leq \tilde{d}(ab).$$

Indeed, write  $\tilde{d}(ab) = d(abc)$  for some nonzero  $c$  in  $R$ . Since  $abc$  is a nonzero multiple of  $a$ ,

$$\tilde{d}(a) \leq d(abc) = \tilde{d}(ab).$$

---

<sup>1</sup>We'll see in Section 5 that in some non-Euclidean domains all ideals may be principal too.

We now show  $R$  admits division with remainder with respect to  $\tilde{d}$ . Pick  $a$  and  $b$  in  $R$  with  $b \neq 0$ . Set  $\tilde{d}(b) = d(bc)$  for some nonzero  $c \in R$ . Using division of  $a$  by  $bc$  (which is nonzero) in  $(R, d)$  there are  $q_0$  and  $r_0$  in  $R$  such that

$$a = (bc)q_0 + r_0, \quad r_0 = 0 \text{ or } d(r_0) < d(bc).$$

Set  $q = cq_0$  and  $r = r_0$ , so  $a = bq + r$ . If  $r_0 = 0$  we are done, so we may assume  $r_0 \neq 0$ . Since  $d(bc) = \tilde{d}(b)$  and  $\tilde{d}(r) \leq d(r)$  (by (2.1)), the condition  $d(r) = d(r_0) < d(bc)$  implies  $\tilde{d}(r) < \tilde{d}(b)$ . Thus

$$a = bq + r, \quad r = 0 \text{ or } \tilde{d}(r) < \tilde{d}(b).$$

Hence  $(R, \tilde{d})$  is a Euclidean domain in the sense of Definition 1.2.  $\square$

We end this section with a brief discussion of two other possible refinements one might want in a Euclidean function (but which we will not need later): uniqueness of the quotient and remainder it produces and multiplicativity.

In  $\mathbf{Z}$  we write  $a = bq + r$  with  $0 \leq r < |b|$  and  $q$  and  $r$  are uniquely determined by  $a$  and  $b$ . There is also uniqueness of the quotient and remainder when we do division in  $F[T]$  (relative to the degree function) and in a field (the remainder is always 0). Are there other Euclidean domains where the quotient and remainder are unique? Division in  $\mathbf{Z}[i]$  does not have a unique quotient and remainder relative to the norm on  $\mathbf{Z}[i]$ . For instance, dividing  $1 + 8i$  by  $2 - 4i$  gives

$$1 + 8i = (2 - 4i)(-1 + i) - 1 + 2i \text{ and } 1 + 8i = (2 - 4i)(-2 + i) + 1 - 2i,$$

where both remainders have norm 5, which is less than  $N(2 - 4i) = 20$ .

**Theorem 2.2.** *If  $R$  is a Euclidean domain where the quotient and remainder are unique then  $R$  is a field or  $R = F[T]$  for a field  $F$ .*

*Proof.* See [11] or [15].  $\square$

This might be a surprise:  $\mathbf{Z}$  isn't in the theorem! Aren't the quotient and remainder in  $\mathbf{Z}$  unique? Yes if we use a remainder  $r$  where  $0 \leq r < |b|$ , but not if we try to pick  $r$  in the setting of Euclidean domains by using  $|r| < |b|$ . For instance,

$$51 = 6 \cdot 8 + 3 \text{ and } 51 = 6 \cdot 9 - 3.$$

The point is that using the Euclidean function on the remainder too, in the case of  $\mathbf{Z}$ , permits negative remainders so in fact  $\mathbf{Z}$  does not have a unique quotient and remainder when we measure the remainder by its absolute value.

The Euclidean function in many basic examples satisfies a stronger property than  $d(a) \leq d(ab)$ , namely  $d(ab) = d(a)d(b)$  with  $d(a) \geq 1$  when  $a \neq 0$ . For instance, this holds in  $\mathbf{Z}$  ( $d(n) = |n|$ ) and  $\mathbf{Z}[i]$  ( $d(\alpha) = N(\alpha)$ ). The degree on  $F[T]$  is not multiplicative, but  $d(f) = 2^{\deg f}$  is multiplicative. There is also a multiplicative Euclidean function on a field  $F$ :  $d(a) = 1$  for all  $a \neq 0$ . For an example of a Euclidean domain that does not admit a multiplicative Euclidean function, see [3].

### 3. FEATURES OF THE $d$ -INEQUALITY

Let  $R$  be a Euclidean domain. By Theorem 2.1 we may assume our Euclidean function  $d$  satisfies the  $d$ -inequality:  $d(a) \leq d(ab)$  for all nonzero  $a$  and  $b$  in  $R$ . Using this inequality we will prove a few properties of  $d$ .

**Theorem 3.1.** *Let  $(R, d)$  be a Euclidean domain where  $d$  satisfies the  $d$ -inequality. Then*

- (1)  $d(a) \geq d(1)$  for all nonzero  $a \in R$ ,
- (2) if  $b \in R^\times$  then  $d(ab) = d(a)$  for all nonzero  $a$ ,
- (3) if  $b \notin R^\times$  and  $b \neq 0$  then  $d(ab) > d(a)$  for all nonzero  $a$ .

In particular, for nonzero  $a$  and  $b$ ,  $d(ab) = d(a)$  if and only if  $b \in R^\times$ .

*Proof.* (1): By the  $d$ -inequality,  $d(1) \leq d(1 \cdot a) = d(a)$ .

(2): By the  $d$ -inequality,  $d(a) \leq d(ab)$ . To get the reverse inequality, let  $c$  be the inverse of  $b$ , so the  $d$ -inequality implies

$$d(ab) \leq d((ab)c) = d(a).$$

(3): We want to show the inequality  $d(a) \leq d(ab)$  is strict when  $b$  is not a unit and not 0. The proof is by contradiction. Assume  $d(a) = d(ab)$ . Now use division of  $a$  by  $ab$ :

$$a = (ab)q + r, \quad r = 0 \text{ or } d(r) < d(ab).$$

We rewrite this as

$$a(1 - bq) = r, \quad r = 0 \text{ or } d(r) < d(a).$$

Since  $b$  is not a unit,  $1 - bq$  is nonzero, so  $a(1 - bq)$  is nonzero (because  $R$  is an integral domain). Thus  $r \neq 0$ , so the inequality  $d(r) < d(a)$  becomes

$$d(a(1 - bq)) < d(a).$$

But this contradicts the  $d$ -inequality, which says  $d(a) \leq d(a(1 - bq))$ . Thus it is impossible for  $d(a)$  to equal  $d(ab)$  when  $b$  is not a unit.  $\square$

Note Theorem 3.1 is not saying two nonzero elements of  $R$  that have the same  $d$ -value are unit multiples, but rather that a multiple of a nonzero  $a \in R$  has the same  $d$ -value as  $a$  if and only if it is a unit multiple of  $a$ . For example, in  $\mathbf{Z}[i]$  we have  $N(1 + 2i) = N(1 - 2i)$  but  $1 + 2i$  and  $1 - 2i$  are not unit multiples. Remember this!

**Corollary 3.2.** *Let  $(R, d)$  be a Euclidean domain where  $d$  satisfies the  $d$ -inequality. We have  $d(a) = d(1)$  if and only if  $a \in R^\times$ . That is, the elements of least  $d$ -value in  $R$  are precisely the units.*

*Proof.* Take  $a = 1$  in parts 2 and 3 of Theorem 3.1.  $\square$

We can see Corollary 3.2 working in  $\mathbf{Z}$  and  $F[T]$ : the integers satisfying  $|n| = |1|$  are  $\pm 1$ , which are the units of  $\mathbf{Z}$ . The polynomials  $f$  in  $F[T]$  satisfying  $\deg f = \deg 1 = 0$  are the nonzero constants, which are the units of  $F[T]$ .

**Corollary 3.3.** *Let  $(R, d)$  be a Euclidean domain where  $d$  satisfies the  $d$ -inequality. If  $a$  and  $b$  are nonunits, then  $d(a)$  and  $d(b)$  are both less than  $d(ab)$ .*

*Proof.* This is immediate from part (3) of Theorem 3.1, where we switch the roles of  $a$  and  $b$  to get the inequality on both  $d(a)$  and  $d(b)$ .  $\square$

#### 4. IRREDUCIBLE FACTORIZATION

One of the key properties of Euclidean domains is that in them all ideals are principal: every Euclidean domain is a PID<sup>2</sup>. Theorems about PIDs may be simpler to prove in Euclidean domains. For an example of this, we'll prove in different ways that irreducible factorization exists in Euclidean domains and in PIDs (Theorems 4.2 and 4.4).

<sup>2</sup>A PID (principal ideal domain) is an integral domain in which each ideal is a principal ideal.

**Definition 4.1.** Let  $R$  be an integral domain. A nonzero element  $a$  of  $R$  is called *irreducible* if it is not a unit and in every factorization  $a = bc$ , one of the factors  $b$  or  $c$  is a unit. A nonzero nonunit that is not irreducible is called *reducible*.

There are three types of nonzero elements in an integral domain: units (the invertible elements, whose factors are always units too), irreducibles (nonunits whose factorizations into two parts always involve one unit factor), and reducibles (nonunits that admit some factorization into a product of two nonunits). Notice that in a field there are no reducible or irreducible elements: everything is zero or a unit. So if we want to prove a theorem about irreducible factorization, we avoid fields.

**Theorem 4.2.** *In a Euclidean domain that is not a field, every nonzero nonunit is a product of irreducibles.*

*Proof.* Let  $(R, d)$  be a Euclidean domain that is not a field. By Theorem 2.1 we may assume  $d(a) \leq d(ab)$  for all nonzero  $a$  and  $b$  in  $R$ . Therefore Corollary 3.3 applies.

We will prove the existence of irreducible factorizations by induction on the  $d$ -value. From Corollary 3.2, the units of  $R$  have the smallest  $d$ -value. An  $a \in R$  with second smallest  $d$ -value must be irreducible: if we write  $a = bc$  and  $b$  and  $c$  are both nonunits, then  $d(b)$  and  $d(c)$  are both less than  $d(a)$  by Corollary 3.3. Therefore  $b$  and  $c$  are units, so  $a$  is a unit. This is a contradiction.

Assume now that  $a \in R$  is a nonunit and all nonunits with smaller  $d$ -value admit an irreducible factorization. To prove  $a$  admits an irreducible factorization too, we may suppose  $a$  is not irreducible itself. Therefore there is some factorization  $a = bc$  with  $b$  and  $c$  both nonunits. Then  $d(b) < d(a)$  and  $d(c) < d(a)$  by Corollary 3.3, so  $b$  and  $c$  both have irreducible factorizations by induction. Thus their product  $a$  has an irreducible factorization.  $\square$

We'll see in the next theorem that the conclusion of Theorem 4.2 is true for PIDs, but proving that will use more abstract methods than induction. It will rely on the following lemma, which has a recursive flavor.

**Lemma 4.3.** *If  $R$  is an integral domain and  $a \in R$  is a nonzero nonunit that does not admit a factorization into irreducibles then there is a strict inclusion of principal ideals  $(a) \subset (b)$  where  $b$  is some other nonzero nonunit that does not admit a factorization into irreducibles.*

*Proof.* By hypothesis  $a$  is not irreducible, so (since it is neither 0 nor a unit either) there is some factorization  $a = bc$  where  $b$  and  $c$  are nonunits (and obviously are not 0 either). If both  $b$  and  $c$  admitted irreducible factorizations then so does  $a$ , so at least one of  $b$  or  $c$  has no irreducible factorization. Without loss of generality it is  $b$  that has no irreducible factorization. Since  $c$  is not a unit, the inclusion  $(a) \subset (b)$  is strict.  $\square$

**Theorem 4.4.** *In a PID that is not a field, every nonzero nonunit is a product of irreducibles.*

*Proof.* Suppose there is an element  $a$  in the PID that is not 0 or a unit and has no irreducible factorization. Then by Lemma 4.3 there is a strict inclusion

$$(a) \subset (a_1)$$

where  $a_1$  has no irreducible factorization. Then using  $a_1$  in the role of  $a$  (and Lemma 4.3 again) there is a strict inclusion

$$(a_1) \subset (a_2)$$

where  $a_2$  has no irreducible factorization. This argument (repeatedly applying Lemma 4.3 to the generator of the next larger principal ideal) leads to an infinite increasing chain of principal ideals

$$(4.1) \quad (a) \subset (a_1) \subset (a_2) \subset (a_3) \subset \cdots$$

where all inclusions are strict. This turns out to be impossible in a PID.

Indeed, suppose a PID contains an infinite strictly increasing chain of ideals:

$$I_0 \subset I_1 \subset I_2 \subset I_3 \subset \cdots$$

and set

$$I = \bigcup_{n \geq 0} I_n.$$

This union  $I$  is an ideal. The reason is that the  $I_n$ 's are strictly increasing, so every *finite* set of elements from  $I$  lies in a common  $I_n$ . (This is the key idea.) So  $I$  is closed under addition and arbitrary multiplications from the ring since each  $I_n$  has these properties. (Make sure you understand that step.) Because we are in a PID,  $I$  is principal:  $I = (r)$  for some  $r$  in the ring. But because  $I$  is the union of the  $I_n$ 's,  $r$  is in some  $I_N$ . Then  $(r) \subset I_N$  since  $I_N$  is an ideal, so

$$I = (r) \subset I_N \subset I,$$

which means

$$I_N = I.$$

But this is impossible because the inclusion  $I_{N+1} \subset I$  becomes  $I_{N+1} \subset I_N$  and we were assuming  $I_N$  was a proper subset of  $I_{N+1}$ . Because of this contradiction, nonzero nonunits in a PID without an irreducible factorization do not exist.  $\square$

**Remark 4.5.** If we look at the proof of Theorem 4.4 in the contrapositive direction, in an integral domain containing a nonzero nonunit  $a$  without an irreducible factorization, there must be a nonprincipal ideal and in fact such an ideal is  $I := \bigcup_{n \geq 0} (a_n)$ , where  $a_0 = a$ ,  $a_n$  for  $n \geq 1$  is a factor of  $a_{n-1}$  that is not a unit or a unit multiple of  $a_{n-1}$ , and  $a_n$  has no irreducible factorization. The reason  $I$  can't be principal is because the proof shows that if  $I$  is principal then we get a contradiction to  $a$  not having an irreducible factorization.

The proof in Theorem 4.4 that a PID does not contain an infinite strictly increasing chain of ideals holds for a broader class of rings than PIDs.

**Theorem 4.6.** *A commutative ring in which every ideal is finitely generated does not contain an infinite strictly increasing chain of ideals.*

*Proof.* The second half of the proof of Theorem 4.4 works in this more general context. All we have to do is show the logic works when  $I$  is finitely generated rather than principal. The point is that if  $I = (x_1, \dots, x_m)$  then the finitely many  $x_i$ 's all lie in some common  $I_N$  (because the  $I_n$ 's are an increasing chain). And now the contradiction is obtained just as before:  $I_N = I$  but then  $I_{N+1} \subset I_N$ , contradiction.  $\square$

**Corollary 4.7.** *In an integral domain where every ideal is finitely generated, every nonzero nonunit has an irreducible factorization.*

*Proof.* If there were an element  $a$  that is not 0 or a unit and that did not admit an irreducible factorization then, as in the proof of Theorem 4.4, we could produce an infinite strictly increasing chain of (principal) ideals. But there are no infinite strictly increasing chains of ideals in the ring, by Theorem 4.6.  $\square$

**Definition 4.8.** A commutative ring where every ideal is finitely generated is called a *Noetherian ring*.

These rings are named after Emmy Noether, who was one of the pioneers of abstract algebra in the early 20th century. Their importance, as a class of rings, stems from the stability of the Noetherian property under many basic constructions. If  $R$  is a Noetherian ring, then so is every quotient ring  $R/I$  (which may not be an integral domain even if  $R$  is), every polynomial ring  $R[X]$  (and thus  $R[X_1, \dots, X_n]$  by induction on  $n$ , viewing this as  $R[X_1, \dots, X_{n-1}][X_n]$ ), and every formal power series ring  $R[[X]]$  (and thus  $R[[X_1, \dots, X_n]]$  by induction on  $n$ , since it is  $R[[X_1, \dots, X_{n-1}]][[X_n]]$ ). The PID property behaves badly for ring constructions, *e.g.*, if  $R$  is a PID that is not a field then  $R[X]$  is not a PID. For instance,  $R[X, Y] = R[Y][X]$  is never a PID for an integral domain  $R$ . But if  $R$  is Noetherian then  $R[X, Y]$  is Noetherian. Briefly, the property “ideals are finitely generated” for Noetherian rings is more robust than the property “ideals are singly generated” for PIDs.

Using this terminology, Corollary 4.7 says in every *Noetherian integral domain* each element other than 0 or a unit has an irreducible factorization. (Contrapositively, if a nonzero nonunit  $a$  in an integral domain has no irreducible factorization, then the ideal  $I := \bigcup_{n \geq 0} (a^n)$  from Remark 4.5 not only isn't principal, but it isn't finitely generated either.) It is worth comparing the proof of existence of irreducible factorizations in Corollary 4.7 to the proof of the special case of Euclidean domains in Theorem 4.2, where the proof of existence of irreducible factorizations is tied up with features of the Euclidean function on the ring.

In the context of unique factorization domains, it is the uniqueness of the factorization that lies deeper than the existence. We are not discussing uniqueness here, which most definitely does *not* hold in most Noetherian integral domains. That is, the existence of irreducible factorizations (for all nonzero nonunits) is not a very strong constraint, since most integral domains that are met in day-to-day practice in mathematics are Noetherian, so their elements must have a factorization into irreducible elements. But there usually is not going to be a unique factorization into irreducible elements.

## 5. EUCLIDEAN AND NON-EUCLIDEAN QUADRATIC RINGS

The main importance of Euclidean domains for an algebra course is that they give us examples of PIDs. Three points are worth noting:

- Aside from computational issues (as in the Euclidean algorithm) it is more useful to know whether or not a ring is a PID than whether or not it is Euclidean.
- There are methods that let one show certain kinds of integral domains are PIDs without knowing whether or not they are Euclidean.
- There are PIDs that are not Euclidean.

The simplest rings that can be PIDs and not Euclidean are found among the quadratic rings.

**Definition 5.1.** A *quadratic ring* is a ring of the form  $\mathbf{Z}[\gamma]$  where  $\gamma$  is a complex number that is a root of an irreducible quadratic polynomial  $T^2 + aT + b \in \mathbf{Z}[T]$  with leading coefficient 1. We call  $\mathbf{Z}[\gamma]$  *real* if  $\gamma$  is real and *imaginary* otherwise.

For instance, the Gaussian integers  $\mathbf{Z}[i]$  are an imaginary quadratic ring associated to the polynomial  $T^2 + 1$ . When  $m \in \mathbf{Z}$  is not a perfect square,  $\mathbf{Z}[\sqrt{m}]$  is real quadratic for  $m > 0$  and imaginary quadratic for  $m < 0$ . The ring  $\mathbf{Z}[(1 + \sqrt{5})/2]$  is real quadratic:  $(1 + \sqrt{5})/2$  is

a root of  $T^2 - T - 1$ . Abstractly,  $\mathbf{Z}[\gamma] \cong \mathbf{Z}[T]/(T^2 + aT + b)$ . Irreducibility of  $T^2 + aT + b$  in  $\mathbf{Z}[T]$  implies the discriminant  $a^2 - 4b$  is not 0. Since  $\gamma = (-a \pm \sqrt{a^2 - 4b})/2$ , if  $a$  is even then  $\mathbf{Z}[\gamma] = \mathbf{Z}[\sqrt{m}]$  where  $m = (a/2)^2 - b \in \mathbf{Z}$ , and if  $a$  is odd then  $\mathbf{Z}[\gamma] = \mathbf{Z}[(1 + \sqrt{m})/2]$  where  $m = a^2 - 4b$ .

Since  $\gamma^2 = -a\gamma - b \in \mathbf{Z} + \mathbf{Z}\gamma$ , by induction every power of  $\gamma$  is in  $\mathbf{Z} + \mathbf{Z}\gamma$ , so

$$\mathbf{Z}[\gamma] = \mathbf{Z} + \mathbf{Z}\gamma.$$

We can't necessarily "complete" the square and write every quadratic ring as  $\mathbf{Z}[\sqrt{m}]$  for some integer  $m$ . For instance,  $\mathbf{Z}[(1 + \sqrt{5})/2] \neq \mathbf{Z}[\sqrt{m}]$  for  $m$  in  $\mathbf{Z}$ , although in contrast to that  $\mathbf{Q}[(1 + \sqrt{5})/2] = \mathbf{Q}[\sqrt{5}]$ .

When  $\gamma$  is one root of  $T^2 + aT + b$ , the second root is  $\bar{\gamma} = -a - \gamma$ , which is called the *conjugate* of  $\gamma$ . More generally, for  $\alpha = x + y\gamma$  in  $\mathbf{Z}[\gamma]$ , where  $x$  and  $y$  are in  $\mathbf{Z}$ , the *conjugate* of  $\alpha$  is

$$\bar{\alpha} := x + y\bar{\gamma} = x - ay - y\gamma.$$

Check that  $\bar{\bar{\alpha}} = \alpha$ . In the special case that  $a = 0$  and we write  $b = -m$ , so  $\gamma$  is a root of  $T^2 - m$  (a square root of  $m$ ), we have

$$\gamma = \pm\sqrt{m} \implies \bar{\gamma} = -\gamma, \overline{x + y\gamma} = x - y\gamma.$$

**Example 5.2.** If  $\gamma = \sqrt{2}$  then  $\overline{x + y\sqrt{2}} = x - y\sqrt{2}$ .

**Example 5.3.** If  $\gamma = (1 + \sqrt{5})/2$ , a root of  $T^2 - T - 1$ , then  $\overline{x + y\gamma} = x + y - y\gamma$ . Concretely, this says  $\overline{x + y(1 + \sqrt{5})/2} = x + y(1 - \sqrt{5})/2$ .

The *norm* of  $\alpha$  is defined to be

$$N(\alpha) = \alpha\bar{\alpha} = x^2 - axy + by^2.$$

This is an integer, and it is zero only when  $\alpha = 0$ . For  $c$  in  $\mathbf{Z}$ ,  $N(c) = c^2$ . In particular,  $N(\pm 1) = 1$ . When  $\gamma = \sqrt{m}$ , we have

$$N(x + y\sqrt{m}) = (x + y\sqrt{m})(x - y\sqrt{m}) = x^2 - my^2.$$

Notice the middle coefficient  $-a$  of the formula  $x^2 - axy + by^2$  for  $N(\alpha)$  does not coincide with the middle coefficient  $a$  of  $T^2 + aT + b$  if  $a \neq 0$ .

**Example 5.4.** If  $\gamma = \sqrt{2}$  then  $N(x + y\sqrt{2}) = x^2 - 2y^2$ , which takes both positive and negative values, e.g.,  $N(3 + 5\sqrt{2}) = -41$ .

**Example 5.5.** If  $\gamma = (1 + \sqrt{5})/2$ , a root of  $T^2 - T - 1$ , then  $N(x + y\gamma) = x^2 + xy - y^2 = (x + y/2) - 5y^2/4$ , which has positive and negative values.

**Example 5.6.** If  $\gamma = \sqrt{-5}$ , a root of  $T^2 + 5$ , then  $N(x + y\gamma) = x^2 + 5y^2$ , which has no negative values.

**Example 5.7.** If  $\gamma = \sqrt{m}$  for  $m \in \mathbf{Z}$  then  $N(x + y\gamma) = x^2 - my^2$ . This has both positive and negative values if  $m > 0$  and only nonnegative values if  $m < 0$ .

A direct calculation shows the norm is multiplicative:

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Several "small" quadratic rings are Euclidean with the absolute value of the norm as a Euclidean function. For instance,  $\mathbf{Z}[i]$ ,  $\mathbf{Z}[\sqrt{2}]$ , and  $\mathbf{Z}[\sqrt{-2}]$  are all Euclidean using  $d(\alpha) = |N(\alpha)|$ . (For an imaginary quadratic ring like  $\mathbf{Z}[i]$  we can drop the absolute value sign:

the norm is already nonnegative.) This leads to two questions about a quadratic ring: is it Euclidean (with respect to *some* Euclidean function) and is it norm-Euclidean (*i.e.*, Euclidean with respect to the particular function  $d(\alpha) = |N(\alpha)|$ )?

For a quadratic ring to be norm-Euclidean is more precise than it being Euclidean: maybe there is a Euclidean function on the ring even if the absolute value of the norm is not a Euclidean function. The first example of that was found by Clark [2] in 1994: he showed  $\mathbf{Z}[(1 + \sqrt{69})/2]$  is Euclidean, and it was already known not to be *norm*-Euclidean. The second such example was found by Harper [8]: he showed  $\mathbf{Z}[\sqrt{14}]$  is Euclidean in 2004. The ring  $\mathbf{Z}[\sqrt{14}]$  was known to be a PID since the 19th century, and was known not to be norm-Euclidean since the early 20th century. Here is a proof of that last statement.

**Theorem 5.8.** *The ring  $\mathbf{Z}[\sqrt{14}]$  is not norm-Euclidean.*

*Proof.* We will show a specific equation can't be solved in  $\mathbf{Z}[\sqrt{14}]$ :  $1 + \sqrt{14} = 2\gamma + \rho$  where  $|N(\rho)| < |N(2)| = 4$ . Assume this has a solution  $\gamma = m + n\sqrt{14}$  and  $\rho = a + b\sqrt{14}$  in  $\mathbf{Z}[\sqrt{14}]$ , so

$$1 + \sqrt{14} = (2m + a) + (2n + b)\sqrt{14} \implies a = 1 - 2m, \quad b = 1 - 2n,$$

which means we'd want  $|(1 - 2m)^2 - 14(1 - 2n)^2| < 4$ , so

$$(2m - 1)^2 - 14(2n - 1)^2 = 0, \pm 1, \pm 2, \pm 3.$$

The left side is odd, so the right is  $\pm 1$  or  $\pm 3$ . Since odd numbers square to  $1 \pmod{8}$ ,  $(2m - 1)^2 - 14(2n - 1)^2 \equiv 1 - 14 \equiv 3 \pmod{8}$ , and the numbers  $\pm 1$  and  $\pm 3$  are distinct mod 8, so

$$(2m - 1)^2 - 14(2n - 1)^2 = 3.$$

Reducing this modulo 7, we get  $3 \equiv \square \pmod{7}$ , which is false. We have a contradiction.  $\square$

Because Harper showed  $\mathbf{Z}[\sqrt{14}]$  is Euclidean, the significance of Theorem 5.8 is that  $\mathbf{Z}[\sqrt{14}]$  is not Euclidean for the specific function  $d(\alpha) = |N(\alpha)|$  even though  $\mathbf{Z}[\sqrt{14}]$  is Euclidean for another function, which is described in the accepted answer on the page <https://math.stackexchange.com/questions/1148364>.

It is known that there are only finitely many *norm-Euclidean* quadratic rings.<sup>3</sup> In contrast, it is believed that there are infinitely many Euclidean quadratic rings, but that remains an open problem. Harper gave a sufficient condition in terms of “two admissible primes” (see [8, Theorem B]) for a real quadratic ring that is a PID to be Euclidean, and he checked this condition is satisfied in many examples besides  $\mathbf{Z}[\sqrt{14}]$  (such as  $\mathbf{Z}[\sqrt{22}]$ ,  $\mathbf{Z}[\sqrt{23}]$ , and  $\mathbf{Z}[(1 + \sqrt{61})/2]$ ). The method was extended to some infinite families of real quadratic rings: see [12] and [17]. Narkiewicz [14] used similar techniques to show every real quadratic ring that is a PID must be Euclidean with at most two exceptions (it is believed there are no exceptions). It is expected, but yet proved, that infinitely many real quadratic rings are PIDs, while it is known that only 9 imaginary quadratic rings are PIDs.<sup>4</sup>

The rest of this handout is concerned with setting up the background to present (i) many quadratic rings that are not PIDs, and thus are not Euclidean (Theorem 5.11) and (ii) two rings that each are a PID but are not Euclidean (Theorems 5.22 and 5.23), so the collection of PIDs strictly contains the collection of Euclidean domains.

<sup>3</sup>See <https://math.stackexchange.com/questions/2710457/norm-euclidean-fields>.

<sup>4</sup>See [https://en.wikipedia.org/wiki/Class\\_number\\_problem](https://en.wikipedia.org/wiki/Class_number_problem).

In order to show some integral domain is not a PID, one method is to exhibit an explicit example of an ideal in it that is not principal. It can be tricky to find such an ideal. After all, an ideal could be principal even if it is initially defined using more than one generator, e.g., in  $\mathbf{Z}$  we have  $(6, 15) = (3)$ . A more subtle way to show an integral domain  $R$  is not a PID is to prove  $R$  fails to have a property that all PIDs have. We are going to describe such a property now. It is a generalization of the rational roots theorem in  $\mathbf{Z}[t]$ , which says that a rational root of a monic polynomial in  $\mathbf{Z}[t]$  is an integer<sup>5</sup>. The generalization is based on the following lemma, which says ratios from a PID have a reduced form, like rational numbers do.

**Lemma 5.9.** *Let  $R$  be a PID and  $F$  be its fraction field. Every element of  $F$  has a ratio in reduced form: it is a ratio of relatively prime elements of  $R$ .*

*Proof.* In  $F$ , pick a ratio  $a/b$  where  $a$  and  $b$  are in  $R$  and  $b \neq 0$ . The ideal  $(a, b)$  in  $R$  is principal, say  $(a, b) = (d)$ . Since  $d$  acts as a gcd for  $a$  and  $b$ , removing this common factor from  $a$  and  $b$  should turn the ratio  $a/b$  into a reduced form ratio.

Since  $a, b \in (d)$ , we have  $d \mid a$  and  $d \mid b$ :  $a = da'$  and  $b = db'$  for some  $a'$  and  $b'$  in  $R$ . Then  $a/b = (da')/(db') = a'/b'$ . We'll show  $a'/b'$  is a reduced form ratio: from  $(a, b) = (d)$ ,  $d = ax + by$  for some  $x$  and  $y$  in  $R$ , so

$$d = ax + by = da'x + db'y = d(a'x + b'y) \implies 1 = a'x + b'y.$$

Thus the only common factors of  $a'$  and  $b'$  in  $R$  are units:  $a'$  and  $b'$  are relatively prime.  $\square$

**Theorem 5.10.** *Let  $R$  be a PID and  $F$  be its fraction field. For a monic polynomial  $f(t)$  in  $R[t]$ , a root of  $f(t)$  in  $F$  must be in  $R$ .*

*Proof.* By Lemma 5.9, a root of  $f(t)$  in  $F$  can be written in reduced form as  $a/b$  where  $a$  and  $b$  are relatively prime in  $R$ .

Write  $f(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_1t + c_0$  with  $n \geq 1$ , so

$$0 = f(a/b) = \frac{a^n}{b^n} + c_{n-1} \frac{a^{n-1}}{b^{n-1}} + \cdots + c_1 \frac{a}{b} + c_0.$$

Multiply through by  $b^n$  to clear the denominator:

$$0 = a^n + c_{n-1}a^{n-1}b + \cdots + c_1ab^{n-1} + c_0b^n.$$

Every term on the right side after  $a^n$  is divisible by  $b$ , so  $b \mid a^n$ . Since  $a$  and  $b$  are relatively prime and  $R$  is a PID, from  $b \mid a^n$  we get  $b \mid 1$ , so  $b \in R^\times$ .<sup>6</sup> Thus  $a/b = ab^{-1} \in R$ .  $\square$

We now have a sufficient (but not necessary!) condition for  $\mathbf{Z}[\sqrt{m}]$  not to be a PID.

**Theorem 5.11.** *If  $m$  is an integer that is not a square and has a repeated prime factor, then  $\mathbf{Z}[\sqrt{m}]$  is not a PID.*

*Proof.* Let  $p$  be a prime such that  $p^2 \mid m$ , so  $m = p^2m'$ . Since  $\sqrt{m'} = \sqrt{m}/p$ ,  $\sqrt{m'}$  is in the fraction field of  $\mathbf{Z}[\sqrt{m}]$  and is not in  $\mathbf{Z}[\sqrt{m}]$ . Then  $f(t) = t^2 - m'$ , which is monic in  $\mathbf{Z}[t] \subset \mathbf{Z}[\sqrt{m}][t]$ , has the root  $\sqrt{m'}$  in the fraction field of  $\mathbf{Z}[\sqrt{m}]$  that is not in  $\mathbf{Z}[\sqrt{m}]$ . By Theorem 5.10,  $\mathbf{Z}[\sqrt{m}]$  is not a PID.  $\square$

<sup>5</sup>The full form of the rational roots theorem says every rational root of a nonconstant polynomial  $c_n t^n + c_{n-1} t^{n-1} + \cdots + c_1 t + c_0 \in \mathbf{Z}[t]$ , where  $c_n \neq 0$ , has reduced form  $a/b$  where  $b \mid c_n$  and  $a \mid c_0$ . If  $c_n = 1$  then  $b = \pm 1$ , so  $a/b = \pm a$  is an integer.

<sup>6</sup>If  $R$  is not a PID, then we could have  $b \mid a^n$  where  $a$  and  $b$  are relatively prime and  $b \notin R^\times$ . An example is  $R = \mathbf{Z}[\sqrt{5}]$  with  $a = 2$  and  $b = 1 + \sqrt{5}$ :  $b \mid a^2$  and the only common factors of  $a$  and  $b$  are in  $R$  are units.

**Example 5.12.** The rings  $\mathbf{Z}[\sqrt{12}] = \mathbf{Z}[2\sqrt{3}]$ ,  $\mathbf{Z}[\sqrt{8}] = \mathbf{Z}[2\sqrt{2}]$ , and  $\mathbf{Z}[\sqrt{18}] = \mathbf{Z}[3\sqrt{2}]$  are not PIDs.

An integral domain  $R$  with the property of Theorem 5.10 (namely for each monic polynomial in  $R[t]$ , a root of it in the fraction field of  $R$  must be in  $R$  itself) is called integrally closed, so Theorem 5.11 says every PID is an integrally closed domain, and thus integral domains that are not integrally closed can't be PIDs (which is how we found the rings in Example 5.12). We have the following containments for three types of integral domains:

Euclidean domains  $\subset$  PIDs  $\subset$  integrally closed domains.

These containments are strict:  $\mathbf{Z}[(1 + \sqrt{-19})/2]$  is a PID and not Euclidean, as we'll see in Theorem 5.22, and  $\mathbf{Z}[\sqrt{-5}]$  is integrally closed and not a PID.

**Remark 5.13.** For  $m$  as in Theorem 5.11, we showed  $\mathbf{Z}[\sqrt{m}]$  is not a PID without giving an explicit example of a nonprincipal ideal in  $\mathbf{Z}[\sqrt{m}]$ . Such an ideal can be written down:  $I = (p, \sqrt{m})$ , where  $p$  is a prime that divides  $m$  at least twice (such  $p$  exists since  $m$  is not squarefree). Why isn't  $I$  principal? It can be shown that  $I = \mathbf{Z}p + \mathbf{Z}\sqrt{m}$  as an additive group, and comparing this to  $\mathbf{Z}[\sqrt{m}] = \mathbf{Z} + \mathbf{Z}\sqrt{m}$  shows  $[\mathbf{Z}[\sqrt{m}] : I] = p$ . It turns out principal ideals in  $\mathbf{Z}[\sqrt{m}]$  can't have index  $p$ , as follows. For a nonzero principal ideal  $(\alpha)$ , it can be shown that  $[\mathbf{Z}[\sqrt{m}] : (\alpha)] = |\mathbf{N}(\alpha)|$ ,<sup>7</sup> so if a principal ideal  $(\alpha)$  has index  $p$  then  $\mathbf{N}(\alpha) = \pm p$ . Writing  $\alpha$  as  $a + b\sqrt{m}$  for  $a$  and  $b$  in  $\mathbf{Z}$ , we'd have  $a^2 - mb^2 = \pm p$ . Since  $p \mid m$  we have  $p \mid a^2$ , so  $p \mid a$ . Then  $p^2 \mid a^2$ , and  $p^2 \mid m$  by assumption, so  $a^2 - mb^2$  is a multiple of  $p^2$ , which contradicts it being  $\pm p$ . Thus the ideal  $(p, \sqrt{m})$  in  $\mathbf{Z}[\sqrt{m}]$  is not principal.

We turn next to examples of PIDs that are not Euclidean. The rings we'll show have this property are the quadratic ring  $\mathbf{Z}[(1 + \sqrt{-19})/2]$  and the quotient polynomial ring  $\mathbf{R}[x, y]/(x^2 + y^2 - 1)$ .

**Theorem 5.14.** *In a quadratic ring  $\mathbf{Z}[\gamma]$ , the units are the elements with norm  $\pm 1$ .*

*Proof.* If  $\alpha\beta = 1$  in  $\mathbf{Z}[\gamma]$  then taking norms shows  $\mathbf{N}(\alpha)\mathbf{N}(\beta) = \mathbf{N}(1) = 1$  in  $\mathbf{Z}$ , so  $\mathbf{N}(\alpha) = \pm 1$ . Conversely, if  $\mathbf{N}(\alpha) = \pm 1$  then  $\alpha\bar{\alpha} = \pm 1$ , so  $\alpha$  is invertible (with inverse  $\pm\bar{\alpha}$ ).  $\square$

**Example 5.15.** The units of  $\mathbf{Z}[\sqrt{2}]$  are built from integral solutions to  $x^2 - 2y^2 = \pm 1$ . For instance, one solution is  $x = 1$  and  $y = 1$ , giving the unit  $1 + \sqrt{2}$ . Its powers are also units (units are closed under multiplication), so  $\mathbf{Z}[\sqrt{2}]$  has infinitely many units.

**Example 5.16.** Units in  $\mathbf{Z}[\sqrt{3}]$  come from integral solutions to  $x^2 - 3y^2 = \pm 1$ . However, there are no solutions to  $x^2 - 3y^2 = -1$  since the equation has no solutions modulo 3:  $x^2 \equiv -1 \pmod{3}$  has no solution. Thus the units of  $\mathbf{Z}[\sqrt{3}]$  only correspond to solutions to  $x^2 - 3y^2 = 1$ . One nontrivial solution (that is, other than  $\pm 1$ ) is  $x = 2$  and  $y = 1$ , which yields the unit  $2 + \sqrt{3}$ . Its powers give infinitely many more units.

**Example 5.17.** The units of  $\mathbf{Z}[\sqrt{-2}]$  come from integral solutions to  $x^2 + 2y^2 = 1$ . The right side is at least 2 once  $y \neq 0$ , so the only integral solutions are  $x = \pm 1$  and  $y = 0$ , corresponding to the units  $\pm 1$ . In contrast to the previous two examples, where there are infinitely many units,  $\mathbf{Z}[\sqrt{-2}]$  has only two units.

The following theorem about Euclidean domains is the key to proving later that certain integral domains are not Euclidean. Notice the proof does not require the Euclidean function on the ring to satisfy the  $d$ -inequality initially.

<sup>7</sup>See Example 5.20 in <https://kconrad.math.uconn.edu/blurbs/linmultalg/modulesoverPID.pdf>.

**Theorem 5.18.** *Let  $R$  be a Euclidean domain that is not a field. There is  $a \in R$  such that  $R/(a)$  is represented by 0 and units of  $R$ .*

*Proof.* Since  $R$  is not a field, there are elements of  $R$  that are not 0 or a unit. Let  $d$  be the Euclidean function on  $R$ . Pick  $a \in R$  such that  $a$  is not 0 or a unit and  $d(a)$  is minimal among such numbers. For each  $x \in R$ ,  $x = aq + r$  for some  $q$  and  $r$  in  $R$  where  $r = 0$  or  $d(r) < d(a)$ . If  $r \neq 0$ , then the inequality  $d(r) < d(a)$  forces  $r$  to be a unit of  $R$ . Since  $x \equiv r \pmod{a}$ , we conclude that  $R/(a)$  is represented by 0 and by units of  $R$ .  $\square$

**Remark 5.19.** We can make the  $a$  in Theorem 2.1 irreducible: change the Euclidean function  $d$  if necessary so that it satisfies the  $d$ -inequality (Theorem 2.1). For this  $d$ , an  $a$  with minimal  $d$ -value among nonzero nonunits of  $R$  is irreducible, since if  $a$  were reducible, then  $a = bc$  for some nonunits  $b$  and  $c$  and  $d(b) < d(bc) = d(a)$  by Corollary 3.3. That contradicts the minimality of  $d(a)$  among nonzero nonunits of  $R$ .

**Example 5.20.** When  $R = \mathbf{Z}$  we can use  $a = 2$ . Then  $\mathbf{Z}/2\mathbf{Z}$  is represented by 0 and 1, or by 0 and  $-1$ . When  $R = \mathbf{Z}[i]$  we can use  $a = 1 + i$ . Then  $\mathbf{Z}[i]/(1 + i)$  is represented by 0 and 1 as well as by 0 and  $i$ . These examples show some units could be congruent to each other modulo  $a$ , but at least every element of the ring is congruent modulo  $a$  to 0 or some (perhaps more than one) unit.

We have shown that if  $R$  is a Euclidean domain that is not a field, then there is an element of  $R$  (namely a nonunit with least  $d$ -value) modulo which everything is congruent to 0 or a unit from  $R$ . A domain that's not a field and which has no element modulo which everything is congruent to 0 or a unit from  $R$  therefore can't be a Euclidean domain.

**Remark 5.21.** In a domain  $R$ , an element  $a$  that is not 0 or a unit and for which the ring  $R/(a)$  is represented by 0 and units in  $R$  is called a *universal side divisor* in the literature. This terminology seems strange. What's a side divisor? Remember the property, but forget the label (and don't use it, because nobody will know what you're talking about).<sup>8</sup>

**Theorem 5.22.** *The quadratic ring  $R = \mathbf{Z}[(1 + \sqrt{-19})/2]$  is a PID and not Euclidean.*

*Proof.* We will only sketch the proof that  $R$  is a PID. Here are two methods.

- It can be shown that for all nonzero  $x$  and  $y$  in  $R$ ,  $y \mid x$  or  $0 < N(ax + by) < N(y)$ , where  $N$  is the norm map on  $R$ . This property of  $R$  implies it is a PID by a slight modification of the proof that a Euclidean domain is a PID. For further details, see [4, p. 282] or [19, Sect. 2].
- Using algebraic number theory (the “Minkowski bound”), if  $R$  has a nonprincipal ideal then it has a nonprincipal ideal whose index in  $R$  is less than  $2\sqrt{19}/\pi \approx 2.7$ , so the index has to be 2 (the index can't be 1, since an ideal with index 1 is  $R = (1)$ , which is principal). It can be shown that  $R$  has no ideal with index 2, principal or nonprincipal, because  $(1 + \sqrt{-19})/2$  is a root of  $X^2 - X + 5$  and  $X^2 - X + 5 \pmod{2}$  has no roots in  $\mathbf{Z}/(2)$ . The details justifying that can be found in algebraic number theory texts where class numbers are computed ( $R$  has class number 1).

To prove  $R$  is not Euclidean (this is stronger than  $R$  not being norm-Euclidean!) we first note  $R$  is not a field since  $\mathbf{Z} \subset R$  but  $1/2 \notin R$  (in fact,  $R \cap \mathbf{Q} = \mathbf{Z}$ ). Therefore to prove

<sup>8</sup>The terms “side divisor” and “universal side divisor” are due to Motzkin [13]. In an integral domain  $R$ , he called  $a$  a side divisor of  $b$  if  $a$  is not 0 or a unit and  $a \mid (b - u)$  for some  $u \in R^\times$ . This means  $b \pmod{a}$  is represented by a unit of  $R$ . A universal side divisor in  $A$  is an  $a \in A$  that is a side divisor of every  $b \in A$ .

$R$  is not Euclidean we will show  $R$  doesn't satisfy the conclusion of Theorem 5.18: for nonunit  $a \in R$  is  $R/(a)$  represented by 0 and units.

First we compute the norm of a typical element  $\alpha = x + y(1 + \sqrt{-19})/2$ :

$$(5.1) \quad N(\alpha) = x^2 + xy + 5y^2 = \left(x + \frac{y}{2}\right)^2 + \frac{19y^2}{4}.$$

This norm always takes values  $\geq 0$  (this is clearer from the second expression for it than the first) and once  $y \neq 0$  we have  $N(\alpha) \geq 19y^2/4 \geq 19/4 > 4$ . In particular, the units are solutions to  $N(\alpha) = 1$ , which are  $\pm 1$ :

$$R^\times = \{\pm 1\}.$$

The first few norm values are 0, 1, 4, 5, 7, and 9. In particular, there is no element of  $R$  with norm 2 or 3. This and the fact that  $R^\times \cup \{0\}$  has size 3 are the key facts we will use.

If  $R$  were Euclidean then there would be a nonunit  $a$  in  $R$  such that  $R/(a)$  is represented by 0 and units, so by 0, 1, or  $-1$ . Perhaps  $1 \equiv -1 \pmod{a}$ , but we definitely have  $\pm 1 \not\equiv 0 \pmod{a}$  (since  $a$  is not a unit,  $(a)$  is a proper ideal so  $R/(a)$  is not the zero ring). Thus  $R/(a)$  has size 2 (if  $1 \equiv -1 \pmod{a}$ ) or 3 (if  $1 \not\equiv -1 \pmod{a}$ ). We show this can't happen.

If  $R/(a)$  has size 2 then  $2 \equiv 0 \pmod{a}$  (think about  $R/(a)$  as an additive group of size 2), so  $a \mid 2$  in  $R$ . Therefore  $N(a) \mid 4$  in  $\mathbf{Z}$ . There are no elements of  $R$  with norm 2, so the only nonunits with norm dividing 4 are elements with norm 4. A check using (5.1) shows the only such numbers are  $\pm 2$ . However,  $R/(2) = R/(-2)$  does not have size 2: it has size 4, since  $R \cong \mathbf{Z}^2$  as an abelian group implies  $R/2R \cong (\mathbf{Z}/2\mathbf{Z})^2$ .

Similarly, if  $R/(a)$  has size 3 then  $a \mid 3$  in  $R$ , so  $N(a) \mid 9$  in  $\mathbf{Z}$ . There is no element of  $R$  with norm 3, so  $a$  must have norm 9 (it doesn't have norm 1 since it is not a unit). The only elements of  $R$  with norm 9 are  $\pm 3$ , so  $a = \pm 3$ . The ring  $R/(3) = R/(-3)$  does not have size 3: its size is 9 since  $R/3R \cong (\mathbf{Z}/3\mathbf{Z})^2$ .

Since  $R^\times \cup \{0\}$  has size 3 and  $R$  has no element  $a$  such that  $R/(a)$  has size 2 or 3,  $R$  can't be a Euclidean domain.  $\square$

**Theorem 5.23.** *The ring  $R = \mathbf{R}[x, y]/(x^2 + y^2 + 1)$  is a PID and not Euclidean.*

*Proof.* To prove  $R$  is a PID, there are four steps. Our argument is based on <https://math.stackexchange.com/questions/864212>.

Step 1: The ring  $R$  is an integral domain.

The polynomial  $x^2 + y^2 + 1$  is irreducible in the UFD  $\mathbf{R}[x, y]$  since, as a polynomial in  $y$ , it is Eisenstein at  $x^2 + 1$ . Therefore the ideal  $(x^2 + y^2 + 1)$  in  $\mathbf{R}[x, y]$  is prime.

Step 2: Every nonzero prime ideal in  $R$  is a maximal ideal.

Since  $R = \mathbf{R}[x, y]/(x^2 + y^2 + 1)$ , each ideal in  $R$  has the form  $I/(x^2 + y^2 + 1)$  where  $I$  is an ideal of  $\mathbf{R}[x, y]$  that contains  $(x^2 + y^2 + 1)$ , and

$$R/(I/(x^2 + y^2 + 1)) = (\mathbf{R}[x, y]/(x^2 + y^2 + 1))/(I/(x^2 + y^2 + 1)) \cong \mathbf{R}[x, y]/I.$$

Thus each nonzero prime ideal  $\mathfrak{p}$  of  $R$  has the form  $P/(x^2 + y^2 + 1)$  for a prime ideal  $P$  in  $\mathbf{R}[x, y]$  strictly containing  $(x^2 + y^2 + 1)$ , so  $R/\mathfrak{p} \cong \mathbf{R}[x, y]/P$ . The prime ideal  $P$  in  $\mathbf{R}[x, y]$  is maximal, since it can be shown that if  $P_1 \subsetneq P_2$  is a tower of two nonzero prime ideals in  $\mathbf{R}[x, y]$  then the larger ideal  $P_2$  is maximal.<sup>9</sup> Therefore  $P/(x^2 + y^2 + 1)$  is maximal in  $R$ .

Step 3: Every maximal ideal in  $R$  is a principal ideal.

<sup>9</sup>This is true for prime ideals in  $F[x, y]$  when  $F$  is an arbitrary field, not just  $\mathbf{R}$ .

Let  $\mathfrak{m}$  be a maximal ideal in  $R$ , so  $\mathfrak{m} = M/(x^2 + y^2 + 1)$  where  $M$  is a maximal ideal in  $\mathbf{R}[x, y]$ . The field  $R/\mathfrak{m} \cong \mathbf{R}[x, y]/M$  is finitely generated as a ring over  $\mathbf{R}$  (with two generators – the images of  $x$  and  $y$  in the quotient ring). Zariski’s lemma<sup>10</sup> says that when a field  $L$  is finitely generated as a ring over a subfield  $K$ ,  $L$  is finite-dimensional as a  $K$ -vector space. Therefore  $R/\mathfrak{m}$  is finite-dimensional over  $\mathbf{R}$ .

The only fields that are finite-dimensional over  $\mathbf{R}$  are  $\mathbf{R}$  and  $\mathbf{C}$ , since  $\mathbf{C}$  is algebraically closed. The relation  $x^2 + y^2 + 1 = 0$  in  $R$  implies  $\bar{x}^2 + \bar{y}^2 + 1 = 0$  in  $R/\mathfrak{m}$ , where  $\bar{x} = x \bmod \mathfrak{m}$  and  $\bar{y} = y \bmod \mathfrak{m}$ . Therefore  $R/\mathfrak{m}$  is larger than  $\mathbf{R}$ , which means  $R/\mathfrak{m}$  is isomorphic as a field to  $\mathbf{C}$ . Under this isomorphism, let  $\bar{x} \mapsto z$  and  $\bar{y} \mapsto w$  for complex numbers  $z$  and  $w$  such that  $z^2 + w^2 + 1 = 0$ . Obviously  $z$  and  $w$  can’t both be real. Without loss of generality, suppose  $z$  is not real. Then  $w = a + bz$  for some  $a, b \in \mathbf{R}$ , so  $\bar{y} = a + b\bar{x}$  in  $R/\mathfrak{m}$ , which means  $y - a - bx$  vanishes in  $R/\mathfrak{m} \cong \mathbf{R}[x, y]/M$ . Thus  $(y - a - bx, x^2 + y^2 + 1) \subset M$  in  $\mathbf{R}[x, y]$ . Check  $(y - a - bx, x^2 + y^2 + 1)$  is maximal in  $\mathbf{R}[x, y]$ , so  $M = (y - a - bx, x^2 + y^2 + 1)$ . Reducing to the ring  $R = \mathbf{R}[x, y]/(x^2 + y^2 + 1)$ ,  $\mathfrak{m} = (y - a - bx)$ , which is principal.

Step 4: Every ideal in  $R$  is a principal ideal, so  $R$  is a PID.

By Steps 2 and 3, all nonzero prime ideals of  $R$  are principal. Therefore all prime ideals of  $R$  are principal (the zero ideal  $(0)$  is principal, whether or not  $(0)$  is a prime ideal). It can be shown with Zorn’s lemma that if all prime ideals in a commutative ring are principal then all ideals are principal.<sup>11</sup> Therefore by Steps 2 and 3, all ideals in  $R$  are principal. (Note this reasoning is very nonconstructive.) Since  $R$  is an integral domain in which all ideals are principal,  $R$  is a PID.

To prove  $R$  is not Euclidean, there are three steps and they do not depend on knowing  $R$  is a PID. We’ll compute the units of  $R$  and show the property of Euclidean domains related to their units in Theorem 5.18 is not satisfied by  $R$ .

Step 1: Give a standard way to write elements of  $R$ .

In  $\mathbf{R}[x, y] = \mathbf{R}[x][y]$ ,  $x^2 + y^2 + 1 = y^2 + (x^2 + 1)$  is a monic polynomial in  $y$  of degree 2. Therefore we can do division by  $y^2 + x^2 + 1$  with remainder in  $\mathbf{R}[x, y]$ : each element of  $\mathbf{R}[x, y]$  has the unique form  $(y^2 + x^2 + 1)q(x, y) + (a(x) + b(x)y)$ , so  $\mathbf{R}[x, y]/(x^2 + y^2 + 1)$  has representatives  $a(x) + b(x)y$  for  $a(x)$  and  $b(x)$  in  $\mathbf{R}[x]$ . Since  $y^2 = -1 - x^2$  in  $R$ , we can think of  $R$  as  $\mathbf{R}[x] + \mathbf{R}[x]\sqrt{-1 - x^2}$ .

Step 2: The units in  $R$  are nonzero constants:  $R^\times = \mathbf{R}^\times$ .

Clearly  $\mathbf{R}^\times \subset R^\times$ . To prove  $R^\times \subset \mathbf{R}^\times$  use the norm function  $N: R \rightarrow \mathbf{R}[x]$  where

$$\begin{aligned} N(f(x) + g(x)\sqrt{-1 - x^2}) &= (f(x) + g(x)\sqrt{-1 - x^2})(f(x) - g(x)\sqrt{-1 - x^2}) \\ &= f(x)^2 + (x^2 + 1)g(x)^2. \end{aligned}$$

This is a multiplicative function, so a unit in  $R$  must have a norm that’s a unit in  $\mathbf{R}[x]$ , meaning the norm is in  $\mathbf{R}^\times$ . In  $f(x)^2 + (x^2 + 1)g(x)^2$ , the leading coefficient of each term is positive if the term is not 0, so the only way such an expression can be in  $\mathbf{R}^\times$  is if  $g(x) = 0$  and  $f(x) \in \mathbf{R}^\times$ , making  $f(x) + g(x)\sqrt{-1 - x^2} = f(x) \in \mathbf{R}^\times$ .

Step 3: Show  $R$  does not fit the conclusion of Theorem 5.18.

If  $R$  were a Euclidean domain then there would be a nonunit  $a \in R$  such that  $R/(a)$  is represented by 0 and units from  $R$ , which are the elements of  $\mathbf{R}$ . So the composite of natural ring homomorphisms  $\mathbf{R} \rightarrow \mathbf{R}[x] \rightarrow R \rightarrow R/(a)$  is surjective, and thus an isomorphism since  $\mathbf{R}$  is a field (homomorphisms from a field to a nonzero ring are always injective). Letting

<sup>10</sup>See Theorem 2.11 in <https://kconrad.math.uconn.edu/blurbs/ringtheory/maxideal-polyring.pdf>.

<sup>11</sup>See Theorem 3.6 and the exercise after it in <https://kconrad.math.uconn.edu/blurbs/zorn1.pdf>.

$x \equiv \alpha \pmod{a}$  and  $y \equiv \beta \pmod{a}$  for  $\alpha, \beta \in \mathbf{R}$ , the equation  $x^2 + y^2 + 1 = 0$  in  $R$  implies  $\alpha^2 + \beta^2 + 1 = 0$  in  $\mathbf{R}$ , which is impossible.  $\square$

## REFERENCES

- [1] S. Alaca and K. S. Williams, “Introductory Algebraic Number Theory,” Cambridge Univ. Press, 2003.
- [2] D. A. Clark, A quadratic field which is Euclidean but not norm-Euclidean, *Manuscripta Math.* **83** (1994), 327–330.
- [3] C. Conidis, P. P. Nielsen, and V. Tombs, Transfinitely valued Euclidean domains have arbitrary indecomposable order type, *Comm. Algebra* **47** (2019), 1105–1113. URL <https://arxiv.org/abs/1703.02631>.
- [4] D. Dummit and R. Foote, “Abstract Algebra,” 3rd ed., Wiley, 2004.
- [5] J. Durbin, “Modern Algebra: An Introduction,” 5th ed., J. Wiley, 2004.
- [6] J. B. Fraleigh, “A First Course in Abstract Algebra,” 6th ed., Addison-Wesley, 1999.
- [7] F. Goodman, “Algebra: Abstract and Concrete (Stressing Symmetry),” 2nd ed., Prentice-Hall, 2005.
- [8] M. Harper,  $\mathbf{Z}[\sqrt{14}]$  is Euclidean, *Canad. J. Math.* **56** (2004), 55–70.
- [9] I. Herstein, “Topics in Algebra,” 2nd ed., Wiley, 1975.
- [10] T. Hungerford, “Algebra,” Springer-Verlag, 1980.
- [11] M. A. Jodeit, Uniqueness in the division algorithm, *Amer. Math. Monthly* **74** (1967), 835–836.
- [12] R. M. Murty, K. Srinivas, and M. Subramani, Admissible primes and Euclidean quadratic fields, *J. Ramanujan Math. Soc.* **33** (2018), 135–147.
- [13] T. Motzkin, The Euclidean algorithm, *Bull. Amer. Math. Soc.* **38** (1949), 1142–1146.
- [14] W. Narkiewicz, Euclidean algorithm in small abelian fields, *Funct. Approx. Comment. Math.* **37** (2007), 337–340.
- [15] T. S. Rhai, A characterization of polynomial domains over a field, *Amer. Math. Monthly* **69** (1962), 984–986.
- [16] J. Rotman, “Advanced Modern Algebra,” Prentice-Hall, 2002.
- [17] K. Srinivas and M. Subramani, On admissible sets of primes in real quadratic fields, pp. 227–233 in “Modular forms and related topics,” Springer, Singapore, 2020.
- [18] B. L. van der Waerden, “Modern Algebra,” Ungar, New York, 1953.
- [19] J. C. Wilson, A principal ideal ring that is not a Euclidean ring, *Math. Mag.* **46** (1973), 34–38.