# Lecture 9: Euclidean Domains (§8.1 of Dummit & Foote)

We'll see how rings with a norm allow us to construct a division algorithm much as we already know for $\mathbb{Z}$.

**Def$^n$** Any function $N : R \longrightarrow \mathbb{N} \cup \{0\}$ with $N(0) = 0$ is called a <u>norm</u> on the integral domain $R$. If $N(a) > 0$ for all $a \neq 0$ then $N$ is a <u>positive norm</u>

In fact, the very def$^n$ of Euclidean Domain presupposes the existence of a division algorithm,

**Def$^n$** The integral domain $R$ is said to be a <u>Euclidean Domain</u> if there is a norm $N$ on $R$ such that for any $a, b \in R$ with $b \neq 0$ there exist elements $q$ and $r$ in $R$ with

$$a = qb + r$$

where $r = 0$ or $N(r) < N(b)$. We call the element $q$ the <u>quotient</u> and the element $r$ is the <u>remainder</u> of the division

This structure allows a <u>Euclidean Algorithm</u> to be implemented for $a, b \in R$ with $b \neq 0$,

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

← last nonzero remainder must exist since we have

$$\underbrace{N(b) > N(r_0) > N(r_1) > \cdots > N(r_n)}$$

decreasing sequence in $\mathbb{N}$ must terminate.

**E1** A field is a Euclidean Domain if we simply define norm $N : \mathbb{F} \to \{0\}$ by $N(x) = 0$ for all $x \in \mathbb{F}$.

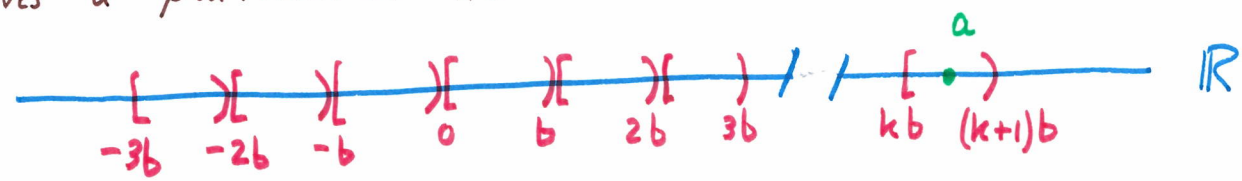
$a, b \in \mathbb{F}$ with $b \neq 0$ then $(a/b) = ab^{-1} \in \mathbb{F}$

so $a = qb$ where $q = ab^{-1}$ (zero remainder)

**E2** The integers $\mathbb{Z}$ form a Euclidean Domain where we define $N(x) = |x| = \sqrt{x^2}$ for each $x \in \mathbb{Z}$

(norm given by absolute value)

Let's discuss the usual division algorithm, consider nonzero $a, b \in \mathbb{Z}$ with $b > 0$. Observe $\mathbb{R} = \bigcup_{n \in \mathbb{Z}} [nb, (n+1)b)$ gives a partition of $\mathbb{R}$




$$kb \leq a < (k+1)b$$

$$0 \leq \underbrace{a - kb}_{r} < b \quad \therefore \begin{cases} q = k \\ r = a - kb \end{cases}$$

We have $a = qb + r$

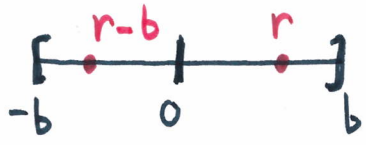
where $0 \leq r < b$ $(N(r) = r < b)$

In the case $a \neq mb$ for some $m \in \mathbb{Z}$ we can always find $0 < b - r$

two ways to implement the division algorithm,

$a = qb + r$ with $r > 0$

$\to a = (q+1)b + r - b$




$N(r-b) = |r-b| = b - r < b$

$30 = \underbrace{7(4) + 2}_{\text{positive remainder}} = \underbrace{7(5) - 5}_{\text{negative remainder}}$

**Remark**: we obtain unique remainder if we impose $r > 0$

**E3** Let $F$ be a field then the polynomial ring $F[x]$ forms a Euclidean Domain where we use degree to define norm; $N(P(x)) = \deg(P(x))$ for $P(x) \neq 0$ and $N(0) = 0$.

**$\mathbb{Q}[x]$**

$$\frac{x^4 - 5x^2 + 4}{x^2+1} = x^2 - 6 + \frac{10}{x^2+1}$$

$$\underbrace{x^4 - 5x^2 + 4}_{a} = \underbrace{(x^2-6)}_{q}\underbrace{(x^2+1)}_{b} + \underbrace{10}_{r}$$

$$N(r) = \deg(10) = 1 < N(b) = \deg(x^2+1) = 2.$$

**$\mathbb{Z}_7[x]$**

$$\frac{x^4 + 2x^2 + 4}{x^2+1} = x^2 + 1 + \frac{3}{x^2+1}$$

$$\underbrace{x^4 + 2x^2 + 4}_{a} = \underbrace{(x^2+1)}_{q}\underbrace{(x^2+1)}_{b} + \underbrace{3}_{r}$$

**$\mathbb{Z}_3[x]$**

$$\frac{x^5 + x^2 + 1}{x^2+1} = x^2 + 2x + 1 + \frac{x}{x^2+1}$$

$$\underbrace{x^5 + x^2 + 1}_{a} = \underbrace{(x^2 + 2x + 1)}_{q_1}\underbrace{(x^2+1)}_{b} + \underbrace{x}_{r_1}$$

$$\underbrace{x^2+1}_{b} = \underbrace{(x)}_{q_2}\underbrace{(x)}_{r_1} + \underbrace{1}_{r_2}$$

$$\underbrace{x}_{r_1} = (1)\underbrace{(x)}_{r_2} + \underbrace{0}_{r_3} \qquad q_3$$

Like Bezout's Th$^{m}$

$$m(x)a(x) + n(x)b(x) = 1$$

$$(2x)(x^5 + x^2 + 1) + (x^4 + 2x^2 + x + 1)(x^2+1) = 1$$

E4 Gaussian Integers $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$

$$N(a+bi) = a^2 + b^2$$

defines a norm where $N(zw) = N(z)N(w)$ and $N(1) = 1$ then we have a division algorithm which you can visualize geometrically in the complex plane. (page 159-160 of my 2018 notes have explicit division alg. in $\mathbb{Z}[i]$ example)

Remark: there is a subset of $\mathbb{Q}(\sqrt{d})$ known as the quadratic integers of $\mathbb{Q}(\sqrt{D})$ where $D$ is square free. In that context,

$$N(a+b\sqrt{D}) = (a+b\sqrt{D})(a-b\sqrt{D})$$
$$= a^2 - Db^2 \quad \text{(p. 229 D\&F)}$$

these are interesting for number theory such as the sol$^{n}$ to Pell's Eq$^{n}$ etc. Sometimes these integers are like $\mathbb{Z}[i]$ other times half-integers are thrown in $\mathbb{Z}[(1+\sqrt{-19})/2]$ for $\mathbb{Q}(\sqrt{-19})$.

shown to not be a Euclidean Domain on page 277 of D\&F. This is done via theory of "side-divisors"

Remark: I intend to merge these notes with LECTURE 27. This covers most of § 8.1 of DUMMIT & FOOTE

## 4.7 Lecture 27: divisibility in integral domains I

This Lecture is mostly focused on the interplay between the three concepts defined below:

**Definition 4.7.1.** *Let $D$ be an integral domain. Let $a, b \in D$*

**(i.)** *$a$ and $b$ are* **associates** *if there exists a unit $u \in D$ for which $b = au$.*

**(ii.)** *$a$ is an* **irreducible** *if $a$ is not a unit and whenever $a = cd$ then $c$ or $d$ is a unit.*

**(iii.)** *$a$ with $a \neq 0$ is* **prime** *if $a$ is not a unit and $a \mid bc$ implies $a \mid b$ or $a \mid c$.*

The terms irreducible and prime have been interchanged at various points of your mathematical education. For example, some texts call the irreducible factors in a polynomial factorization the prime factors. It depends on which book you were taught from etc. In the integers every irreducible is prime. The definition of prime in $\mathbb{Z}$ is often given to be that $p \in \mathbb{Z}$ has only itself and 1 as positive divisors. Allowing for negative divisors we'd say $p$ is prime only if $p, -p, 1, -1$ are its sole divisors. This is precisely the notiion of irreducibility defined above. In contrast, we recognize (iii.) as Euclid's Lemma for $\mathbb{Z}$. Of course, both hold for primes in $\mathbb{Z}$ so a prime in $\mathbb{Z}$ is both prime and irreducible as given by (ii.) and (iii.) of the above Definition. Prime and irreducible are not generally equivalent in rings. The example below taken from Gallian page 313 serves well to illustrate:

**Example 4.7.2.** *Consider $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ where $d$ is* **square-free**. *To say $d$ is square-free is to say that the prime factorization of $d$ has no factor of the form $p^2$ for some prime $p$. For example, $35 = 5(7)$ is square free, but $d = 50 = 5^2(2)$ is not square free. Consider $d = -3$ and study $1 + \sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ we can show[8] $1 + \sqrt{-3} = xy$ implies $x$ or $y$ is a unit thus $1 + \sqrt{-3}$ is irreducible. On the other hand, note:*

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 1 - (-3) = 4 = (2)(2)$$

*thus $1 + \sqrt{-3}$ divides $(2)(2)$ yet $1 + \sqrt{-3}$ does not divide 2. Why? Suppose $a, b \in \mathbb{Z}$ such that*

$$(\ 1 + \sqrt{-3}\ )(\ a + b\sqrt{-3}\ ) = 2 \quad \Rightarrow \quad (a - 3b) + (b + a)\sqrt{-3} = 2$$

*from which we find $a - 3b = 2$ and $a + b = 0$ hence $a = -b$ thus $4a = 2$ so $a = 2/4$ which is absurd as $a \in \mathbb{Z}$ thus $1 + \sqrt{-3}$ does not divide 2. Therefore, $1 + \sqrt{-3}$ is* **not prime**, *but, $1 + \sqrt{-3}$* **is irreducible**.

To prove $1 + \sqrt{-3}$ is irreducible we best introduce a new concept: taken from Dummit and Foote page 270. I

**Definition 4.7.3.** *Let $R$ be an integral domain. Any function $N : R \to \mathbb{N} \cup \{0\}$ with $N(0) = 0$ is called a* **norm** *on $R$. If $N(a) > 0$ for $a \neq 0$ then $N$ is said to be a* **positive norm**.

In particular, if we study $\mathbb{Z}[\sqrt{d}]$ where $d$ is square-free then I propose we define the norm by analogy to the square of the modulus in $\mathbb{C}$. Remember, $|x + iy|^2 = x^2 + y^2$ can be captured as $|z| = zz^*$ where $z^* = x - iy$. By the same token, if we define $(a + b\sqrt{d})^* = a - b\sqrt{d}$ then

$$(a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$$

This motivates the following convenient definition of norm:

[8] we'll use the concept of a norm to accomplish this a bit later in this Lecture, see Example 4.7.6

**Definition 4.7.4.** *Let $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ where $d$ is square-free then define*

$$N(a + b\sqrt{d}) = |a^2 - db^2|$$

*for each $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.*

The fact that the formula above defines a norm is immediate from the fact $N(0) = 0$ and the fact that the absolute value is non-negative. If $d < 0$ then we can write $N(a + b\sqrt{d}) = a^2 + db^2$ as the sum of squares is automatically non-negative.

**Theorem 4.7.5.** *If $d$ is square-free and $N(a + b\sqrt{d}) = |a^2 - db^2|$ for each $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ then*

**(i.)** *$N(x) = 0$ if and only if $x = 0$*

**(ii.)** *$N(xy) = N(x)N(y)$ for all $x, y \in \mathbb{Z}[\sqrt{d}]$*

**(iii.)** *$x \in \mathbb{Z}[\sqrt{d}]$ is a unit if and only if $N(x) = 1$*

**(iv.)** *if $N(x)$ is prime then $x$ is irreducible in $\mathbb{Z}[\sqrt{d}]$*

**Proof:** I leave (i.) and (ii.) this as a rather enjoyable exercises. To prove (iii.), suppose $x$ is a unit then $xy = 1$ for some $y$ and hence $N(1) = N(x)N(y)$ but $N(1) = |1^2 + d(0^2)| = 1$ hence $1 = N(x)N(y)$ but $N(x), N(y) \in \mathbb{Z}$ hence $N(x) = N(y) = 1$. Next, to prove (iv.) suppose $N(x)$ is prime and suppose $x = yz$ for some $y, z \in \mathbb{Z}[\sqrt{d}]$ then $N(x) = N(yz) = N(y)N(z)$. Now, $N(x)$ is prime thus either $N(y) = 1$ or $N(z) = 1$ and hence either $y$ or $z$ is a unit by (iii.). Therefore, $x$ is irreducible. □

**Example 4.7.6.** *Let us see why $1 + \sqrt{-3}$ is irreducible. Suppose $1 + \sqrt{-3} = xy$. Observe*

$$N(1 + \sqrt{-3}) = 1^2 - (-3)1^2 = 4 = N(xy) = N(x)N(y)$$

*if $x, y$ are not units then we must have $N(x) = N(y) = 2$. Consider,*

$$a^2 + 3b^2 = 2$$

*there is no solution! Consequently, $1 + \sqrt{-3} = xy$ implies $x$ or $y$ is a unit. Thus $1 + \sqrt{-3}$ is irreducible.*

Gallian warns us that proving things in $\mathbb{Z}[\sqrt{d}]$ is more trouble when $d > 1$. Let us work through his Example 2 on page 313.

**Example 4.7.7.** *Consider $7 \in \mathbb{Z}[\sqrt{5}]$. Suppose $7 = xy$ for some $x, y \in \mathbb{Z}[\sqrt{5}]$. We have*

$$N(7) = N(xy) = N(x)N(y) \quad \Rightarrow \quad 49 = N(x)N(y)$$

*if $x, y$ are not units we must have $N(x) = N(y) = 7$. Suppose $x = a + b\sqrt{7}$ with $N(x) = 7$ then*

$$7 = |a^2 - 5b^2| \quad \text{or if you prefer} \quad a^2 - 5b^2 = \pm 7.$$

*Any integer solution of $a^2 - 5b^2 = \pm 7$ is an $\mathbb{Z}_7$ solution of $a^2 - 5b^2$. Explicit checking of possible solutions shows the only solution is $a = b = 0$ modulo 7. Thus $7 \mid a$ and $7 \mid b$ which gives $|a^2 - 5b^2|$ is divisible by 49. Yet, $|a^2 - 5b^2| = 7$ which is clearly not divisible by 49 hence no solution of $a^2 - 5b^2 = \pm 7$ exists for $a, b \in \mathbb{Z}$.*

**Theorem 4.7.8.** *In an integral domain every prime is an irreducible.*

**Proof:** suppose $a$ is a prime in an integral domain. If $a = xy$ then as $a$ is prime we have $a \mid x$ or $a \mid y$. Suppose $a \mid x$ then $x = ab$ for some $b$. Thus,

$$x(1) = x = ab = (xy)b = x(yb)$$

thus $1 = yb$ and we find $y$ is a unit. Similar argument shows $x$ is a unit in the case $a \mid y$ thus $a = xy$ implies $x$ or $y$ is a unit and we conclude that $a$ is ireducible. □

The concept of associates is helpful for some calculations we have struggled with a bit in our recent work. Here is a Theorem that should help us with the task of identifying possible coset representatives in a given quotient of a unital ring $R$ by an ideal $I$:

**Theorem 4.7.9.** *Let $R$ be a commutative ring with identity 1. If $a, b$ are associates then $\langle a \rangle = \langle b \rangle$. Furthermore, if $R$ is an integral domain and $I = \langle a \rangle$ then any other generator of $I$ is an associate of $a$.*

**Proof:** if $a, b$ are associates then there exists a unit $u$ in $R$ for which $a = bu$ and $b = au^{-1}$. Let $x \in \langle a \rangle$ then $x = ar$ for some $r \in R$. Hence $x = bur$ and as $ur \in R$ this shows $x \in \langle b \rangle$ hence $\langle a \rangle \subseteq \langle b \rangle$. If $y \in \langle b \rangle$ then $y = br = au^{-1}r \in \langle a \rangle$ hence $\langle b \rangle \subseteq \langle a \rangle$ and thus $\langle a \rangle = \langle b \rangle$. Suppose $\langle c \rangle = \langle a \rangle$ for some $c \in R$. If $\langle a \rangle = \{0\}$ then $a = 0$ otherwise $a \neq 0$ implies $a(1) = a \in \langle a \rangle \neq \{0\}$ and $a = 0$ then implies $c = 0$ as well. The Theorem is trivially true for $a = 0$ since 0 is an associate of itself and there is no distinct associate of 0. Suppose $a \neq 0$ hence $c \neq 0$. Note $a, c \in \langle c \rangle$ and $a, c \in \langle a \rangle$ thus there exists $s, r \in R$ for which $a = rc$ and $c = sa$ hence $a = rc = (rs)a$. As $a \neq 0$ we deduce from the cancellation property of the integral domain $R$ that $rs = 1$ hence $r$ is a unit and $a = rc$ shows $a, c$ are associates. □

What happens in general when $R$ is not integral. Is it possible that $\langle a \rangle = \langle c \rangle$ and $a, c$ are not associates? Consider, $R = \mathbb{Z}_6$ for then $\langle 2 \rangle = \langle 4 \rangle = \{0, 2, 4\}$. Are $2, 4$ associates? Well, can we find a unit $u \in U(\mathbb{Z}_6) = \{1, 5\}$ for which $4 = 2u$? There are two choices: $2(1) = 2 \neq 4$ and $2(5) = 10 = 4$. Yes, in this case, $2(5) = 4$ and 5 is a unit hence $2, 4$ are associates. This shows the second part of Theorem 4.7.9 **can** be true outside the context that $R$ be an integral domain. For an non-example, see this mathstack Q and A.

**Theorem 4.7.10.** *In a principal ideal domain, an element is prime if and only if it is irreducible.*

**Proof:** Let $D$ be a PID. Note $D$ is an integral domain by assumption[9] thus Theorem 4.7.8 tells us that each prime is irreducible. Conversely, suppose $a$ is irreducible. Suppose $a \mid bc$ for some $b, c \in D$. Define

$$I = \{ax + by \mid x, y \in D\}$$

we can show $I$ is an ideal. Note $z, w \in I$ have the form $z = ax + by$ and $w = ax' + by'$ for some $x, y, x', y' \in D$. Thus,

$$z - w = ax + by - (ax' + by') = a(x - x') + b(y - y') \in I$$

and for $r \in D$,

$$rz = r(ax + by) = a(rx) + b(ry) \in I$$

[9] a PID is an integral domain in which every ideal is principal.

thus $I$ is an ideal. Since $D$ is a PID we know $I$ is principal. Thus there exists $d \in D$ for which $I = \langle d \rangle$. Observe $a = a(1) + b(0) \in I$ thus $a = rd$ for some $r \in D$. Since $a$ is irreducible we have $r$ or $d$ is a unit.

If $d$ is a unit then $1 = dd'$ for some $d' \in D$ thus $1 \in I$. Therefore, $1 = ax + by$ for some $x, y \in D$. Multiply by $c$ to see:

$$c = cax + cby = acx + (bc)y.$$

Naturally, $a \mid acx$ and we assumed $a \mid bc$ thus, by the equation above, $a \mid c$.

If $r$ is a unit then $a = rd$ provides $a$ and $r$ are associates. Theorem 4.7.9 provides $\langle d \rangle = \langle a \rangle$ hence $I = \langle a \rangle$ and as $b = a(0) + b(1) \in I$ we find $b = a\lambda$ for some $\lambda \in D$. Therefore, $a \mid b$.

In summary, for an irreducible $a \in D$ we find $a \mid bc$ implies $a \mid b$ or $a \mid c$ which shows $a$ is prime. □

In short, PIDs allow us to carelessly interchange the concepts of prime and irreducible. It's sort of like those new cars where they encourage you to ignore the road[10].

**Example 4.7.11.** *$\mathbb{Z}$ is a principal ideal domain. You can prove any ideal in $\mathbb{Z}$ has the form $\langle n \rangle = n\mathbb{Z}$. Likewise, if $F$ is a field then we showed that $F[x]$ is a principal ideal domain in Theorem 4.5.17. Not all integral domains are principal. Gallian provides us the example $\mathbb{Z}[x]$ of $\langle 2, x \rangle$ which he defines a bit differently on page 314-315. Details can be found in his Example 3.*

[10] current commercials teach me it's cool to day dream in the car