## Euclidean domains

In this section, all rings will be commutative.

If $m, n \in \mathbb{Z}$, we can find a greatest common divisor. The idea is that we first write

$m = q_0 n + r_0$, where $0 \le r_0 < n$. If $r_0 = 0$, we conclude that $n \mid m$. Otherwise, we continue, and write

$n = q_1 r_0 + r_1$, w/ $0 \le r_1 < r_0$.

$r_0 = q_2 r_1 + r_2$

$r_1 = q_3 r_2 + r_3$, ...

Continuing in this way, we eventually get $r_{i+1} = 0$, so $r_{i-1} = q_{i+1} r_i$. ($r_i$ = g.c.d.)

e.g. if $r_3 = 0$, then $r_1 = q_3 r_2$, so $r_2 \mid r_0 \Rightarrow r_2 \mid n \Rightarrow r_2 \mid m$.

We can't use this algorithm in an arbitrary ring, because we don't have an ordering "$<$". However, we can put an ordering on some rings:

**Def:** Let $R$ be an integral domain. A function $N: R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called a norm on $R$. If $N(a) > 0$ for $a \neq 0$, $N$ is a positive norm.

**Ex:** $N: \mathbb{Z} \to \mathbb{Z}^+ \cup \{0\}$ defined $n \mapsto |n|$ is a norm.

**Def:** An integral domain $R$ is a <u>Euclidean domain</u> if there is a norm $N$ on $R$ s.t. for any $a, b \in R$ w/ $b \neq 0$ $\exists$ $q, r \in R$ with

$$a = qb + r, \quad \text{w/ } r = 0 \text{ or } N(r) < N(b)$$

In an Euclidean domain, we thus have a Euclidean algorithm, since the norm of the remainder keeps decreasing. i.e. we eventually end up with $r_{i-1} = q_{i+1} r_i$.

**Ex:** Fields are Euclidean domains, trivially. If $a, b \in F$, a field, and $b \neq 0$, then

$$a = (ab^{-1})\, b$$

i.e., the remainder is always 0. (Thus Field $\Rightarrow$ Euc. domain $\Rightarrow$ integral domain)

**Ex:** Of course, $\mathbb{Z}$ is an integral domain, by above discussion.

**Ex:** If $F$ is a field, let $N: F[x] \to \mathbb{Z}^+ \cup \{0\}$ be the norm $N(f) =$ degree of $f$. The division algorithm is just "long division" of polynomials. (We will later see that if $F$ isn't a field, $F[x]$ is <u>not</u> a Euclidean domain).

**Prop:** If $R$ is a Euclidean domain, then every ideal of $R$ is principal. That is, if $I \subseteq R$ is an ideal, $I = (d)$, some $d \in R$.

**Pf:** If $I = 0$, we're done. Otherwise, let $d \in I$ be a nonzero element s.t. $N(d) \leq N(a)$ $\forall$ nonzero $a \in I$.

Suppose $a \in I$. We can write $a = qd + r$, where $r = 0$ or $N(r) < N(d)$.

But $r = \underset{\text{in } I}{a} - q\underset{\text{in } I}{d} \Rightarrow r \in I$. Thus, by minimality of $N(d)$, $r = 0$.

$\Rightarrow a = qd \Rightarrow a \in (d)$, so $I \subseteq (d)$. But $d \in I$, so $(d) = I$. $\square$

**Ex:** Recall that $(2, x) \subseteq \mathbb{Z}[x]$ is not principal. Thus, $\mathbb{Z}[x]$ is <u>not</u> a Euclidean domain.

**Ex:** Consider $\mathbb{Z}[\sqrt{-5}]$. Define the norm $N$ on $\mathbb{Z}[\sqrt{-5}]$ to be

$$N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

Note that this <u>particular</u> norm is multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$.

Consider the ideal $I = (3, 1 + \sqrt{-5})$. Suppose $I$ is principal.

Then $I = (a + b\sqrt{-5})$ for some $a, b \in \mathbb{Z}$.

Then $3 = \alpha(a + b\sqrt{-5})$, $1 + \sqrt{-5} = \beta(a + b\sqrt{-5})$, some $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$.

Taking norms, we get $9 = N(\alpha)(a^2 + 5b^2)$, and $6 = N(\beta)(a^2 + 5b^2)$

Thus $a^2 + 5b^2 = 1$ or $3$

$a^2 + 5b^2 = 3$ is impossible, since $b$ would have to be $0$ and $3$ is not a square.

If $a^2 + 5b^2 = 1$, then $a = \pm 1$, $b = 0$, but then $I = R$. This means that

$$3\gamma + (1+\sqrt{-5})\delta = 1, \quad \text{some } \gamma, \delta.$$

Multiplying both sides by $1 - \sqrt{-5}$, we get

$$\underbrace{3(1-\sqrt{-5})\gamma + 6\delta}_{\substack{\text{divisible} \\ \text{by 3}}} = \underbrace{1 - \sqrt{-5}}_{\substack{\text{not divisible} \\ \text{by 3}}}, \quad \text{a contradiction.}$$

Thus, $I$ is not principal, so $\mathbb{Z}[\sqrt{-5}]$ is not a Euclidean domain.

One nice thing about the Euclidean algorithm is that it produces a greatest common divisor (even for an arbitrary Euclidean domain). However, even for general rings, we can define what it means to be a greatest common divisor (though one may not exist):

**Def:** Let $R$ be commutative, $a, b \in R$ with $b \neq 0$.

1.) $a$ is a multiple of $b$ if $\exists\ x \in R$ with $a = bx$. In this case, we say $b$ divides $a$, written $b \mid a$.

2.) $d$ is a greatest common divisor of $a$ and $b$ (denoted g.c.d.$(a,b)$) if

(i.) $d \mid a$ and $d \mid b$, and

(ii.) if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

Reinterpreting this in terms of ideals, we have

$$b \mid a \iff a \in (b) \iff (a) \subseteq (b) \quad \text{so}$$

$d$ is a g.c.d. of $a$ and $b$ if

i.) $a, b \in (d)$, i.e. $(a,b) \subseteq (d)$

ii.) if $(a,b) \subseteq (d')$, then $(d) \subseteq (d')$.

i.e. $(d)$ is the smallest principal ideal containing $(a,b)$. In particular, we get the following:

**Prop:** If $a, b \in R$ are nonzero s.t. $(a,b) = (d)$, then $(d)$ is a greatest common divisor of $a$ and $b$.

Note that the converse doesn't always hold: $(2, x) \subseteq \mathbb{Z}[x]$ is not principal, but it's maximal, so $1$ is a g.c.d., as is $-1$, which leads to the question of uniqueness of g.c.d.s:

**Prop:** Let $R$ be an integral domain. If $d, d' \in R$ s.t. $(d) = (d')$, then $d' = ud$ for some unit $u$ in $R$. (In particular, g.c.d.s are unique up to multiplication by a unit.)

**Pf:** If $d = 0$, then $d' = 0$, so we're done. Otherwise, we have $d = ud'$ and $d' = vd = vud' \Rightarrow (1 - vu)d' = 0$.

Thus, since $R$ is an integral domain, $1 = vu$, so $v$ is a unit. $\square$

Note that not all pairs of elements in a ring have a g.c.d.:

**Ex:** Consider the ring $\mathbb{Z}[\sqrt{-5}]$. Then $(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2 \cdot 3$

Thus, $(2+2\sqrt{-5}, 6)$ is contained in both $(1+\sqrt{-5})$ and $(2)$.

$N(1+\sqrt{-5}) = 6$, $N(2) = 4$. So if $(\alpha) \subset (1+\sqrt{-5}) \cap (2)$, then

$6 \mid N(\alpha)$ and $4 \mid N(\alpha)$, so $12 \mid N(\alpha)$.

If $(2+2\sqrt{-5}, 6) \subseteq (\alpha)$, then $N(\alpha) \mid 24$ and $N(\alpha) \mid 36 \Rightarrow N(\alpha) = 12$.

($2+2\sqrt{-5}$: Norm $= 24$; $6$: Norm $= 36$)

Thus, $\alpha = a + b\sqrt{-5}$ where $a^2 + 5b^2 = 12$, which can't happen.

Thus, $2+2\sqrt{-5}$ and $6$ have no g.c.d.

An important property of Euclidean domains is that greatest common divisors exist and can be computed algorithmically:

**Theorem:** Let $R$ be a Euclidean domain and $a, b \in R$ nonzero. Let $d = r_n$ be the last nonzero remainder in the Euclidean Algorithm for $a$ and $b$. Then

1.) $d$ is the greatest common divisor of $a$ and $b$, and

2.) $(d) = (a,b)$. In particular, $d = xa + yb$, for some $x, y \in R$.

**Pf:** We know from an earlier prop that all ideals are principal. We thus just need to show $(d) = (a, b)$.

First, we'll show $(a,b) \subseteq (d)$. That is, we need to show $d \mid a$ and $d \mid b$.

Our Euclidean algorithm in this case is

$$a = q_0 b + r_0$$

$$b = q_1 r_0 + r_1$$

$$r_0 = q_2 r_1 + r_2$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n$$

$$r_{n-1} = q_{n+1} \underbrace{r_n}_{d}$$

We prove by induction down to 0 that $r_n \mid r_i \ \forall \ i \leq n$.
Assume $r_n \mid r_i$ for $k \leq i \leq n$.

Then $r_{k-1} = \underbrace{q_{k+2} r_k}_{\text{div. by } r_n} + \underbrace{r_{k+1}}_{\text{div by } r_n} \Longrightarrow r_n \mid r_{k-1}$. Thus, $r_n \mid r_i \ \forall i$.

Thus, $r \mid b$, so $a = q_0 b + r_0$ is div. by $r_n$ as well. Thus $(a,b) \subseteq (d)$.

Now we show $(d) \subseteq (a,b)$.

We know $r_0 \in (a,b)$. Assume $r_i \in (a,b)$ for $0 \le i \le k$. Then

$$r_{k-1} = q_{k+2} r_k + r_{k+1} \Rightarrow r_{k+1} = \underbrace{r_{k-1}}_{\in (a,b)} - \underbrace{q_{k+2} r_k}_{\in (a,b)} \in (a,b).$$

Thus, by induction $d = r_n \in (a,b)$. Thus $(d) = (a,b)$. □

Ex: What is g.c.d. $(702, 228)$? By the Euclidean algorithm,

$$702 = 3 \cdot 228 + 18$$

$$228 = 12 \cdot 18 + 12$$

$$18 = 1 \cdot 12 + 6$$

$$12 = 2 \cdot 6$$

So
$$\begin{aligned} 6 &= 18 - 1 \cdot 12 \\ &= 18 - (228 - 12 \cdot 18) \\ &= 13 \cdot 18 - 228 \\ &= 13 \cdot (702 - 3 \cdot 228) - 228 \\ &= 13 \cdot 702 - 40 \cdot 228 \end{aligned}$$