Unique factorization domains (UFDs)

We talked about how in Euclidean domains, we can use the Euclidean algorithm to find the g.c.d. of two elements. Of course, this also works in $\mathbb{Z}$, but in practice, this is not how we find a g.c.d. in $\mathbb{Z}$. Usually, we look at a prime factorization.

Ex: What's the g.c.d. of 48 and 60?

$$48 = 2^4 \cdot 3, \quad 60 = 2^2 \cdot 3 \cdot 5$$

So g.c.d. $(48, 60) = 2^2 \cdot 3 = 12$.

In certain rings, called UFDs, we are able to do this as well. Before we define them, we need to define what it means to factor an element in a ring, and when you're "done" factoring.

Def: Let R be an integral domain.

1.) Let $r \in R$ nonzero, non-unit. Then r is <u>irreducible</u> if whenever $ab = r$, either a or b is a unit. Otherwise r is <u>reducible</u>.

2.) Let $p \in R$ be nonzero. Then $p \in R$ is <u>prime</u> if (p) is prime. That is p is prime if it's not a unit, and whenever $p \mid ab$, then $p \mid a$ or $p \mid b$.

3.) If $a, b \in R$ s.t. $a = ub$, for some unit $u \in R$, a and b are

associate in R.

Ex: In $\mathbb{Z}$, the prime and irreducible elements are $\pm p$, $p \in \mathbb{Z}^+$, a prime in the usual sense. a and b are associate iff $a = \pm b$.

While in $\mathbb{Z}$, prime elements are the same as irreducible elements, this is not the case in arbitrary integral domains. We do have an implication in one direction though:

Prop: In an integral domain, a prime element is always irreducible.

Pf: Suppose p is prime. Then (p) is a prime ideal. If $ab = p$, then $ab \in (p)$, so one of a or b is in (p). say $a \in (p)$. Thus $a = pr$, some $r \in R \Rightarrow p = ab = prb \Rightarrow p(1 - rb) = 0$.

R is an integral domain, so $1 - rb = 0 \Rightarrow rb = 1 \Rightarrow b$ is a unit. Thus p is irreducible. □

However, not all irreducible elements are prime.

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

2 is irreducible in $\mathbb{Z}[\sqrt{-6}]$, since its norm is 4 and no element has norm 2, and $N(\alpha) = 1 \Leftrightarrow \alpha = \pm 1$.

However $1 + \sqrt{-5}$ nor $1 - \sqrt{-5}$ is divisible by 2, so 2 isn't prime.

In a PID, these properties are equivalent:

Prop: Let R be a PID. A nonzero element $p \in R$ is prime if and only if it's irreducible.

Pf: We've already shown prime $\Rightarrow$ irreducible. Now suppose p is irreducible. We want to show (p) is a prime ideal.

Suppose $(p) \subseteq I$, an ideal. Then since R is a PID, $I = (r)$, some $r \in R$. Then $p = ur$, some u. Since p is irreducible, u or r is a unit.

If r is a unit, then $I = R$.

If u is a unit, then $(p) = (ur) = (r)$, so the only ideals containing (p) are R and (p). Thus (p) is maximal and thus prime. $\square$

Def: An integral domain R is a <u>unique factorization domain</u> (UFD) if every nonzero, non-unit $r \in R$ has the following properties:

(i.) r can be written as a finite product $r = p_1 p_2 \cdots p_n$ where each p_i is irreducible (not necessarily distinct), and

(ii.) the decomposition in (i.) is unique (up to associates). i.e. if $r = q_1 \cdots q_m$, each q_i irreducible, then $n = m$, and the

q_i can be reindexed so that $p_i = u_i q_i$ for each i, where u_i is a unit.

Ex: In $\mathbb{Z}$, $12 = 3 \cdot 2 \cdot 2 = (-3)(-2) \cdot 2$, but $-3 = -1 \cdot 3$ and $-2 = -1 \cdot 2$.

We'll soon see that every PID (and thus $\mathbb{Z}$) is a UFD.

Ex: In a field, every nonzero element is a unit, so it's trivially a UFD.

Ex: $\mathbb{Z}[\sqrt{-5}]$ is not a UFD: $(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2 \cdot 3$ gives two factorizations of 6 into irreducibles.

Ex: Let $R = \mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$.

Then $2i$ is irreducible in R, since $i \notin R$.

Thus, $(2i)(-2i) = 4 = 2 \cdot 2$ is two factorizations of 4, so R is not a UFD.

Just like in a PID, in a UFD irreducible $\iff$ prime:

Prop: If R is a UFD, then p is irreducible $\iff$ p is prime.

Pf: We already know prime $\Rightarrow$ irreducible.

Assume p is irreducible. We WTS (p) is prime.

Suppose $ab \in (p)$. Then $ab = rp$.

We can factor $a = a_1 \cdots a_n$, $b = b_1 \cdots b_m$, $r = r_1 \cdots r_\ell$ into irreducibles.

Thus $(a_1 \cdots a_n)(b_1 \cdots b_m) = (r_1 \cdots r_\ell)p$, so by uniqueness, p is associate to some a_i or b_j. Thus, a_i or $b_j \in (p)$, so a or $b \in (p)$, so p is prime. □

We can use this to show that two nonzero elements a and b in a UFD always have a g.c.d.:

Prop: Let R be a UFD, $a, b \in R$ nonzero. Let

$$a = u p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \quad \text{and} \quad b = v p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$$

be the prime factorizations for a and b, where u, v are units, each p_i is prime and distinct, and e_i, f_i are ≥ 0.

Then $d = p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)}$ is the g.c.d. of a and b.

Pf: $d \mid a$ and $d \mid b$. If $d' \mid a$ and $d' \mid b$, let

$d' = q_1^{g_1} \cdots q_m^{g_m}$ be its prime factorization. But then, each q_i divides a and b, so it divides some p_j. Thus, up to multiplication by a unit, $q_i = p_j$. So d' is a product of powers of the p_i, w/ powers $\leq$ to those occurring in d.

Thus, $d' \mid d$. □

Before we prove the main result of the section, we prove a useful lemma:

Lemma: Let R be an integral domain. If $a, b, c \in R$ are nonzero, and $ab = ac$, then $b = c$.

Pf: $ab = ac \Rightarrow a(b-c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c$. □

Note that the above doesn't work if the ring has zero divisors. Now we get to the main result:

Thm: Every PID is a UFD.

Pf: Let R be a PID, and $r \in R$ nonzero, not a unit. First we show r can be factored into a finite product of irreducibles (or, equivalently, primes).

If r is irreducible, we're done. Otherwise, we can write $r = r_1 s_1$ where r_1 and s_1 are nonunits. We need to show that this process terminates. Suppose it doesn't. Then, WLOG, $r_1 = r_2 s_2$, $r_2 = r_3 s_3$, etc. But then $r_1 \mid r$, $r_2 \mid r_1$, etc, and we have

$$(r) \subset (r_1) \subset (r_2) \subset \dots \subset R.$$

Since none of the r_i is a unit, $(r_i) \subsetneq R \quad \forall i$.

Consider $I = \bigcup_{i=1}^{\infty} (r_i)$. This is an ideal: if $a, b \in I$, then $a, b \in (r_i)$ for some i, so $a - b \in (r_i) \subseteq I$. If $a \in I$, $c \in R$, then $a \in (r_i)$, some i, so $ca \in (r_i) \subseteq I$.

Thus, $I \subsetneq R$, and $I = (a)$, for some a, since R is a PID. Then $a \in I$, so $a \in (r_i)$ for some i. But then $(r_i) \subseteq I = (a) \subseteq (r_i)$, so $(r_i) = I$, which means, in particular, that $(r_i) = (r_{i+1})$.

Thus $r_i = \underbrace{u}_{\text{unit}} r_{i+1} = r_{i+1} s_{i+1} \Rightarrow u = s_{i+1}$ is a unit, a contradiction.

Thus, any element of R can be written as a finite product of irreducibles. We just need to show that any factorization is unique up to associates.

Let $r = p_1 \cdots p_n = q_1 \cdots q_m$, $m \geq n$ be two factorizations of r into irreducibles. We show, by induction on n, that this is unique.

If $n = 0$, then r is a unit. If $r = q_1 \cdots q_m$, then each q_i is a unit, a contradiction, so $m = 0$.

Now suppose uniqueness holds for a product of $\leq n-1$ irreducibles.

Let $r = p_1 \cdots p_n = q_1 \cdots q_m$. Then p_1 divides some q_i. WLOG, suppose

$p_1 \mid q_1$. Then $up_1 = q_1$, some u. u is a unit since q_1 is irreducible.

Thus, $p_1 \cdots p_n = p_1 u q_2 \cdots q_m \Rightarrow p_2 \cdots p_n = q_2' \cdots q_m$, where $q_2' = uq_2$ is still irreducible.

But then by induction, $n = m$ and (after reordering) p_i is associate to q_i. □

Since $\mathbb{Z}$ is a PID, this immediately implies:

Cor: $\mathbb{Z}$ is a UFD.

We now have the following inclusions:

fields $\subset$ Euclidean domains $\subset$ PIDs $\subset$ UFDs $\subset$ integral domains

$\mathbb{Q}$ $\quad$ $\mathbb{Z}$ $\quad$ $\mathbb{Z}[x]$ $\quad$ $\mathbb{Z}[\sqrt{-5}]$

(Finding a PID that's not a Euclidean domain is hard. One example is $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$.)