# EDs / PIDs / UFDs

We recall an early result from number theory, and summarise smaller results used to prove it.

**Theorem.** Any natural number has a unique factorisation into primes.

**Definition.** Recall that, in $\mathbb{N}$, a 'prime' is defined as 'only divisible by itself and 1'.

In a more general ring, this is an 'irreducible', and a prime is defined differently.

**Step 1. Euclid's Algorithm.**

Given $a, b$, Euclid's algorithm shows that they have a highest common factor, $h$. The algorithm enables us to find $h$ explicitly, and reversing the algorithm allows us to write $h$ as a combination of $a, b$.

**Step 2. Bézout's theorem.**

This says that we can write the hcf $h$ of $a, b$ as a combination of $a, b$. We first proved it by Euclid's algorithm, but then we met a second, more magical, proof.

We take the set $\{\lambda a + \mu b : \lambda, \mu \in \mathbb{Z}\}$ of integer combinations of $a, b$, and show that its smallest positive member is in fact $h$. This is magical because it doesn't tell us what combination of $a, b$ it is, and just asserts that it is one.

**Step 3. For $p$ prime, if $p \mid ab$ then $p \mid a$ or $p \mid b$.**

This follows from Bézout (and so also from Euclid). Suppose that $p \mid ab$ but $p \nmid a$. Since $\text{hcf}(a, p)$ divides $p$, it is either $p$ or 1, and it can't be $p$ since $p \nmid a$. Hence $\text{hcf}(a, p) = 1$, and so by Bézout we can write $\lambda a + \mu p = 1$. Then $\lambda ab + \mu pb = b$ and so $p \mid b$.

**Step 4. Prime factorisations are unique.**

If a number can be factorised into primes, then the factorisation is unique.

If $p_1 \ldots p_r = q_1 \ldots q_s$ are factorisations into primes, then Step 3 shows that $p_1 \mid q_i$ for some $i$, and hence $p_1 = q_i$. We cancel these primes and repeat.

**Step 5. Prime factorisations exist.**

We use induction. If $n$ is prime then we are done. Otherwise, $n = ab$ with $a, b$ being proper factors, and $a, b$ have a prime factorisation by induction.

This factorisation is then unique, by Step 4.

So, we have proved the theorem: a natural number has a unique factorisation into primes.

Note that Step 1 $\Rightarrow$ Step 2 $\Rightarrow$ Step 3 $\Rightarrow$ Step 4.

We like unique factorisation. It's nice. We now want to investigate when a general ring $R$ has unique factorisation, and we will try to recreate the series of steps we used for the integers.

*Note. This is just to help explain some of the connections, and is not meant to be rigorous. For example, I assume throughout that we are in an integral domain and that hcfs are unique, and that 'unique' generally means 'up to units' or 'up to reordering'. Use your notes for the proper details and proofs!*

**Step 1. Can we run Euclid's algorithm?**

In the algorithm for the integers, we simply divided and found the remainder: $a = qb+r$, with $0 \leqslant r < b$. Since the remainders at each stage of the algorithm formed a decreasing sequence of positive integers, the algorithm was guaranteed to terminate. Once it did, it was an easy check to see that the final non-zero remainder was the hcf.

In a general ring, we don't necessarily have the concept of 'less than', so we can't measure if $r < b$. Or, we might have a 'less than' which takes non-integer values, so we can't promise that the algorithm terminates, as the remainders could decrease forever.

Can we find some way of using positive integers to measure whether the remainder is decreasing? Suppose that we have a function $\phi$ taking values in $\mathbb{N}$ with the property that given $a, b$, we can always find $q, r$ with $a = qb + r$ such that if $r \neq 0$ then we have $\phi(r) < \phi(b)$.

If we can do this, then we can run the algorithm as before, measuring the remainders using $\phi$, and it will terminate. This is the case for a **Euclidean Domain**.

**Step 2. Do we have Bézout's theorem?**

As in the integers, if we can run Euclid's algorithm then we can reverse it and write the hcf $h$ as a combination of $a, b$. But what if we can't run the algorithm because we can't find a suitable $\phi$? Well, maybe the 'magical' integer proof still works. That is, maybe there is a combination, even if we can't find it by an algorithm.

Take the set of all $R$-combinations of $a, b$, i.e. $\{\lambda a + \mu b : \lambda, \mu \in R\}$. We can't take the 'smallest positive member', as this doesn't make sense in a general ring. But we notice that in the integers example, the set contained only multiples of $h$ ($h$ divides $a, b$, so divides all $\lambda a + \mu b$) and all multiples of $h$ (if $h = \lambda a + \mu b$ then $\alpha h = \alpha\lambda a + \alpha\mu b$).

Let's use this as our desired property: given the set $\{\lambda a+\mu b : \lambda, \mu \in R\}$, does it contain an element $h$ such that the set is precisely the multiples of $h$? If so, then $h$ is the hcf of $a, b$: it divides both of them, and since $h$ is some combination $\lambda a + \mu b$, we have that any common factor of $a, b$ divides $h$.

I.e., we want the ideal $(a, b)$ to be equal to some ideal $(h)$. This is certainly the case for a **Principal Ideal Domain**.

*In a Euclidean Domain, since the hcf $h$ is a combination of $a, b$, we see that the ideal $(a, b)$ is of the form $(h)$.*

*More generally, a Euclidean Domain is a Principal Ideal Domain, since for any ideal we can use the Euclidean function $\phi$ to mimic the 'smallest positive member'. Given an ideal $I$ in an ED, we take $x \in I$ with $\phi(x)$ minimal, and we can show that $I = (x)$.*

**Definition.** The integer definition of 'prime' is what in a general ring is called an 'irreducible'. In a ring, a 'prime' is an element $p$ such that if $p \mid ab$ then $p \mid a$ or $p \mid b$.

**Step 3. Do we have 'if $p \mid ab$ then $p \mid a$ or $p \mid b$'?**

In other words, are irreducibles necessarily prime?

Suppose that any ideal $(a, b)$ is of the form $(h)$ for some $h$. We'll mimic the integer proof of Step 3.

Let $p$ be irreducible with $p \mid ab$ and $p \nmid a$. The ideal $(a, p)$ equals some $(h)$ by assumption. Then $h \mid p$ and so $h$ is either $p$ or 1, and it can't be $p$ since $p \nmid a$. Hence $(a, p) = (1)$ and so $1 \in (a, p)$, i.e. we can write $\lambda a + \mu p = 1$. Then $\lambda ab + \mu pb = b$ and so $p \mid b$.

*In a Principal Ideal Domain (and so also in a Euclidean Domain) we certainly have $(a, b) = (h)$ for some $h$, and so irreducibles are prime in a PID (and in an ED).*

**Step 4. Are factorisations into irreducibles unique?**

Suppose that an element can be factorised into irreducibles.

If irreducibles are prime, then we have actually factorised it into primes. Then the factorisation is unique, and the proof is exactly as for the integers.

It might just happen that irreducibles are prime, but we saw in Step 3 that this is guaranteed in a Principal Ideal Domain.

**Step 5. Do factorisations into irreducibles exist?**

It might just happen that factorisations exist, but we'll show here that this is guaranteed in a Principal Ideal Domain. We can't mimic Step 5 from the integers – the induction fails because we aren't in the integers any more.

Suppose that $R$ is a PID, and let $x \in R$. If $x$ is irreducible then we are done. Otherwise $x = x_1 y_1$. If these are both irreducible then we are done. Otherwise, wlog, $x_1 = x_2 y_2$. We repeat, obtaining a sequence $x, x_1, x_2, \ldots$, each of which is a proper factor of the one before.

Consider the ideals: $(x) \subset (x_1) \subset (x_2) \subset \ldots$ The union of these is also a principal ideal – call it $(z)$. Then $z \in (x_n)$ for some $n$, so $(z) = (x_n)$, and so the chain stops. Similarly for all other branches of the factorisation of $x$. This means that the factorisation of $x$ cannot continue forever, and so $x$ is indeed a product of irreducibles.

A **Unique Factorisation Domain** is a ring in which every element has a unique factorisation into irreducibles.

We saw above that if a ring has factorisations into irreducibles, and if irreducibles are prime, then factorisations are unique.

We saw above that this is the case in Principal Ideal Domains, and hence PIDs are UFDs.