Unique factorization
Hjalmar Rosengren, 4 September 2015

Some of the most important theorems in mathematics are about unique factorization in rings. For instance, the fundamental theorem of arithmetic states that any positive integer can be written uniquely as a product of primes. The fundamental theorem of algebra implies that any complex polynomial in one variable can be written as a product of first-degree factors, uniquely up to multiplication by non-zero constants. We want to put this type of results in a general framework. In particular, we will show a unique factorization result in a general principal ideal domain (PID).

Throughout, R will be an integral domain with 1. In particular, R is commutative. In general, we do not have division but we have cancellation:

$$ab = ac \quad \Longrightarrow \quad a = 0 \text{ or } b = c.$$

By a *unit* of R we mean an invertible element. (For instance, the units in $\mathbb{Z}$ are ± 1.) We will sometimes write $a \sim b$ if $a = eb$ for some unit e.

By an *irreducible element* we mean a non-zero non-unit p such that if $p = ab$ then either a or b is a unit. Equivalently, p is *not* irreducible if we can write $p = ab$ with neither a nor b a unit.

By a *prime element* we mean a non-zero non-unit p such that if $p \mid ab$ then $p \mid a$ or $p \mid b$.

For general integral domains, it's an exercise to check that any prime element is irreducible.

In $\mathbb{Z}$ there is no difference between prime elements and irreducible elements, both notions mean $\pm p$ with p a prime number. Similarly, in $\mathbb{C}[x]$, both notions mean a polynomial of degree 1.

By contrast, in the ring $\mathbb{Z}[\sqrt{-5}]$, it's easy to check that the elements 3 and $2 \pm \sqrt{-5}$ are all irreducible. However, in view of the identity

$$3 \cdot 3 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5})$$

none of these elements are prime For instance, $2+\sqrt{-5}|3\cdot 3$ but $2+\sqrt{-5} \nmid 3$. In this example, the existence of non-prime irreducible elements is related to non-unique factorizations of the element 9. By the following result, this is an instance of a general phenomenon.

Proposition 1. *Let R be an integral domain such that any non-zero non-unit can be written as a product of irreducible elements. Then, the following two conditions are equivalent:*

(A) *Every irreducible element is prime.*

(B) *Factorization into irreducible elements is unique up to multiplication by units.*

More precisely, condition (B) means that if

$$x = p_1 \cdots p_k = q_1 \cdots q_l$$

with all p_j and q_j irreducible, then $k = l$ and, after reordering the elements, $p_j \sim q_j$ for all j.

A domain such that the conditions in Theorem 1 hold is called a *unique factorization domain* (UFD).

Proof of Prop. 1. To prove that (A) implies (B), we use induction on the minimal number of irreducible factors of x. If $x = p_1$ is itself irreducible, then the statement in (B) follows from the definition of irreducibility. Suppose now that (B) holds for all products of k irreducible factors and consider a product $x = p_1 \cdots p_{k+1}$ with all p_j irreducible. If we also have $x = q_1 \cdots q_l$, then since p_1 is prime it divides one of the factors q_j. After reordering, we may assume $p_1 \mid q_1$. Since q_1 is irreducible, $p_1 = eq_1$ with e a unit. Cancelling p_1 we get

$$p_2 \cdots p_{k+1} = eq_2 \cdots q_l.$$

We may now apply the induction hypothesis to deduce that (B) holds for the element x.

To prove that (B) implies (A), let p be irreducible and suppose that $p \mid ab$, that is, $ab = pc$ for some c. If none of the elements a, b and c are units, we factorize them into irreducibles and plug into the equation $ab = pc$. By (B), p is equivalent to one of the irreducible factors on the left-hand side. If that factor comes from a we have $p \mid a$ and else $p \mid b$. The remaining cases are more trivial: if a is a unit we have $b = a^{-1}pc$ and hence $p \mid b$; if c is a unit we can apply the argument above to the irreducible element pc. □

The following is the main result of these notes.

Theorem 2. *Every PID is an UFD.*

For the proof we will need the following lemma, which is an important result in itself.

Lemma 3. *Any PID is a* Noetherian ring*, that is, it does not contain any infinite strictly increasing chain of ideals*

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots .$$

Proof. Suppose there is such a chain and let $I = \cup_k I_k$. Then, it's easy to see that I is an ideal. (For instance, if $x \in I$ and $y \in I$, we have $x \in I_k$ and $y \in I_l$ for some k and l. If $l \geq k$, then $x \in I_l$ so, by the fact that I_l is an ideal, $x - y \in I_l \subseteq I$.) By the definition of a PID, $I = aR$ for some $a \in R$. Since $a \in I$, there exists a k with $a \in I_k$. But then, $I = aR \subseteq I_k$, so $I = I_k$. This contradicts the assumption that $I_k \subsetneq I_{k+1} \subseteq I$. □

We can now prove that the first requirement for being an UFD holds.

Lemma 4. *In a PID, any non-zero non-unit can be factored as a product of irreducible elements.*

Proof. Take a non-zero non-unit element a. If it's irreducible we are done. If not, we can write $a = bc$ with b and c non-units. This implies $(a) \subsetneq (b)$. For if $(a) = (b)$, then we could write $b = ad$ for some $d \in R$. Then, $a = acd$ and after cancelling a we have $d = c^{-1}$ which contradicts that c is a non-unit. This argument can be repeated. If b and c are both irreducible we are done; otherwise one of them, say b, can be factored. The factors of b generate ideals strictly larger than (b). Continuing in this way we will either end up with a factorization of a into irreducibles or with an infinite strictly increasing chain of ideals. However, the second option is impossible in view of Lemma 3. □

We complete the proof of Theorem 2 by verifying condition (a) in Prop. 1.

Lemma 5. *In a PID, each irreducible element is prime.*

Proof. Let p be an irreducible element and assume that $p \mid ab$. We assume that $p \nmid a$ and prove that $p \mid b$. Consider the ideal (p, a). By the definition of a PID, $(p, a) = (c)$ for some c. In particular, $p \in (c)$, so $p = cd$ for some element d. Since p is irreducible either c or d is a unit. If d is a unit then $(p) = (c)$. But then $a \in (c) = (p)$ which contradicts $p \nmid a$. Thus, c is a unit which means that $1 \in (c) = (p, a)$. Then we can write

$$1 = px + ay$$

for some elements x and y. This gives $b = pbx + aby$ and since $p \mid ab$ we may conclude that $p \mid b$. $\square$

Finally, we mention without proof the following fact.

Theorem 6. *If R is an UFD then the polynomial ring $R[x]$ is an UFD.*

By iteration, $R[x_1, \ldots, x_n]$ is an UFD. This shows that the class of UFDs is much larger than the class of PIDs; for instance, $\mathbb{Z}[x]$ and $\mathbb{R}[x, y]$ are UFDs but not PIDs.