# Over a UFD

**Proposition 1.** *Let $R$ be a GCD domain and $p(x) \in R[x]$ primitive. Then $p(x)$ can be written as a product of irreducibles in $R[x]$ in essentially one way (up to a rearrangement and mutiplication by units).*

*Proof.* (type this) $\square$

**Corollary 2.** *If $R$ is a UFD, then $R[x]$ is a UFD.*

*Proof.* (type this) $\square$

## Summary

$$\begin{tikzcd}
\underline{R} & \underline{R[x]} \\
\text{Domain} \arrow[r] & \text{Domain} \\
\text{GCD} \arrow[r] & \text{GCD} \\
\text{UFD} \arrow[r] & \text{UFD} \\
\text{ED} \arrow[ur, dashed] & \text{ED} \\
\text{Field} \arrow[ur] & \text{Field}
\end{tikzcd}$$

One might expect that detecting irreducibles and finding irreducible factorizations would be more difficult in $\mathbb{Z}[x]$, say, than in $\mathbb{Z}$, but in fact the opposite is true. This is ultimately due to the existence of the derivative on $R[x]$ and to some other aspects of the structure of $R[x]$ which will be explored later.

We've seen here that if $R$ is a UFD, then $R[x]$ is also a UFD, but have not seen any kind of algorithm which computes factorizations in $R[x]$. In the exercises of this and the next section we construct algorithms which work in some important special cases, including $\mathbb{Z}$ and $\mathbb{Z}/(p)$.

## Exercises

1. **Factorization if $R$ is finite.** Note that if $R$ is a finite ring of order $m$, then for any given degree $d$ there are only finitely many polynomials in $R[x]$ of degree $d$; each such polynomial has $d+1$ coefficients, which each take one of $m$ values. So the number of degree $d$ polynomials over $R$ is $m^{d+1}$.

   **Proposition 3.** *Let $R$ be a domain. If $p(x) \in R[x]$ is reducible of degree $d$, then $p$ has a divisor of degree $1 \leq k \leq \lfloor d/2 \rfloor$.*

If $R$ is a finite UFD (of which examples do exist, such as $\mathbb{Z}/(p)$ with $p$ a prime) we can use this fact to construct a factorization algorithm for $R[x]$. Let $p(x) \in R[x]$ have degree $d$. Choose some $1 \leq k < d$. There are $m^{k+1}$ degree $k$ polynomials over $R$, which can easily be enumerated. (If $R$ is a field, we can consider only the monic polynomials, of which there are $m^k$.) Using polynomial long division we can determine whether any are divisors of $p(x)$; if so, recurse on the two factors, and if not, $p(x)$ has no factors of degree $k$. Repeat for each $k$ in $[1, \lfloor d/2 \rfloor]$; if no divisor of $p$ is found, then $p$ is irreducible.