Irreducibility criteria

If \( R[x] \) is a UFD, and \( p(x) \in R[x] \), how can we tell if \( p(x) \) is irreducible? By Gauss’ lemma, it suffices to consider factorizations in \( F[x] \), where \( F \) is the field of fractions of \( R \). It is easy to check if \( p(x) \) has a linear factor:

**Prop:** Let \( F \) be a field and \( p(x) \in F[x] \). Then \( p(x) \) has a factor of degree 1 \( \iff \) \( p(x) \) has a root in \( F \), i.e. \( \exists \alpha \in F \) with \( p(\alpha) = 0 \).

**Pf:** If \( p \) has a factor of degree 1 \( ax + b \), then \( a \left( \frac{-b}{a} \right) + b = 0 \) so \( p \left( \frac{-b}{a} \right) = 0 \).

Conversely, if \( p(\alpha) = 0 \), then the division algorithm gives

\[
p(x) = q(x)(x - \alpha) + r,
\]

where \( r \) is a constant. Thus, \( D \) \( p(\alpha) = q(\alpha) \cdot 0 + r = r \) so \( p(\alpha) = q(\alpha)(x - \alpha) \). \( \square \)

Since a reducible polynomial of degree 2 or 3 must have a linear factor, we immediately get the following:

**Cor:** A polynomial of degree 2 or 3 over a field \( F \) is reducible \( \iff \) it has a root in \( F \).
Ex: \( x^2 + 1 \) is reducible in \( \mathbb{Z}/2\mathbb{Z}[x] \), since 1 is a root.

In fact, \((x+1)(x+1) = x^2 + 1\).

\( x^2 + x + 1 \) is not reducible in \( \mathbb{Z}/2\mathbb{Z}[x] \), since it has no root.

Ex: Consider \( p(x)^3 - 3x - 1 \in \mathbb{Z}[x] \). To check irreducibility, we just need to check whether \( p(x) \) has any rational roots.

If \( p\left(\frac{a}{b}\right) = 0 \), then \( \left(\frac{a}{b}\right)^3 - \frac{3a}{b} = 1 \Rightarrow a^3 - 3ab^2 = b^3 \Rightarrow a \mid b^3 \).

But we can assume \( a \) and \( b \) are rel. prime, so \( \frac{a}{b} = \pm 1 \), neither of which is a root of \( p \).

Ex: A similar technique shows that for \( p \in \mathbb{Z} \) prime, \( x^3 - p \in \mathbb{Z}[x] \) is irreducible. Otherwise there are \( a, b \) rel. prime in \( \mathbb{Z} \) s.t.

\[
\frac{a^3}{b^3} = p \Rightarrow a^3 = pb^3 \Rightarrow a \mid p, \text{ so } a = \pm 1 \text{ or } \pm p.
\]

Neither of which work.