Section 9.4 Irreducibility Criteria

Recall: \( p(x) \in \mathbb{R}[x] \) is irreducible if \( p(x) \neq 0 \) and whenever \( f(x) = a(x) \cdot b(x) \), one of \( a(x) \) or \( b(x) \) is a unit.

If \( R \) is a field, \( f(x) \) being irreducible means it can't be factored into two polynomials of lower degree. Ex: \( p(x) = x^2 + 1 \) irreducible in \( \mathbb{R}[x] \), reducible in \( \mathbb{C}[x] \). What about \( \mathbb{Z}_5[x] \)?

Deciding whether or not a polynomial is irreducible is a tricky business. We now develop some criteria for this.

Proposition 9 Let \( p(x) \in \mathbb{F}[x] \) where \( \mathbb{F} \) is a field.

Then \( p(x) = (x - a) \cdot g(x) \iff p(a) = 0 \)

Example Is \( p(x) = 1 + 3x + 4x^2 + x^3 + x^4 + 2x^5 + 3x^6 \) irreducible in \( \mathbb{Z}_5[x] \)? No because \( p(1) = 0 \)

we know \( p(x) = (x-1) \cdot g(x) = (x+4) \cdot g(x) \)

[can find \( g(x) \) with long division].

Strategy To see if \( p(x) \) factors with a linear term (in a finite field) Just check find roots \( a \) of \( p(x) \).

Then we know \( p(x) = (x-a) \cdot g(x) \).

But checking for zeros doesn't guarantee an answer.

Does \( f(x) = x^4 + 2x^2 + 1 \) factor over \( \mathbb{Z}_3[x] \)?

\[
\begin{align*}
f(0) &= 1 \quad \rightarrow \text{Doesn't factor with a linear term, but} \quad x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1) \\
f(1) &= 1 \\
f(2) &= 1
\end{align*}
\]

Proposition 10 A polynomial of degree 2 or 3 over a field \( \mathbb{F} \) is reducible \( \iff \) it has a root in \( \mathbb{F} \).
Example: Is \( x^2 + 2x + 1 \) reducible over \( \mathbb{Z}_3 \)?

\[
f(0) = 1 \\
f(1) = 0 \\
f(2) = 0
\]

\[x^2 + 2x + 1 = (x - 2)(x - 2) = (x + 1)(x + 1)\]

Observation: Suppose \( f(x) = a_0 + a_1 x + \ldots + x^n \in \mathbb{Z}[x] \) (monic). If \( f(a) = 0 \), some \( a \in \mathbb{Z} \), then \( a \mid a_0 \).

Reason: \( f(a) = 0 \Rightarrow f(x) = (x - a)(x^{n - 1} + \ldots + b) \). \( ab = a_0 \).

Example: \( f(x) = x^4 + 5x^3 + 5x^2 - 5x - 6 \). Possible roots: \( \pm 1, \pm 2, \pm 3, \pm 6 \).

Test:

\[
\begin{align*}
f(1) &= 0 \\
f(-1) &= 0 \\
f(2) &= 0 \\
f(-2) &= 0 \\
f(-3) &= 0
\end{align*}
\]

Proposition 11: Suppose \( f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x] \). If \( f(\frac{a}{2}) = 0 \), then \( r \mid a_0 \) and \( s \mid a_n \).

Proposition 12: Suppose \( I \subseteq R \) is a proper ideal, \( p(x) \in R[x] \) monic. If \( p(x) \) factors in \( R[x] \), then \( \overline{p(x)} \) factors in \( R/I[x] \), i.e., \( p(x) \) irreducible in \( R[x] \) if and only if \( \overline{p(x)} \) is irreducible in \( R/I[x] \).

Corollary: (Eisenstein's Criterion for \( \mathbb{Z}[x] \))

Suppose \( f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x] \) and \( p \) is prime. Then \( f(x) \) is irreducible if \( p \mid a_i \) for all \( i \), but \( p^2 \nmid a_0 \).

Example: \( f(x) = x^{10} - 25x^3 + 10x^2 - 30 \)

\[
\begin{array}{c|c|c|c|c}
& 5125 & 5110 & 5130 & 5^2 30 \\
\uparrow & \uparrow & \uparrow & \uparrow & \\
5 & 125 & 5 & 10 & 5 & 30
\end{array}
\]

Thus \( f(x) \) is irreducible in \( \mathbb{Q}[x] \) and \( \mathbb{Z}[x] \).
Section 9.5 Polynomial Rings on Fields II

Proposition 15 Suppose $F$ is a field. Then:

$R[x]/(f(x))$ is a field $\iff f(x)$ is irreducible.

i.e. $(f(x))$ is a maximal ideal $\iff f(x)$ is irreducible.

Proof $R[x]/(f(x))$ is a field $\iff (f(x))$ is maximal

$\iff (f(x))$ is prime

Def of prime $\iff f(x)$ is prime

Ch 8 Prop 12 $\iff f(x)$ is irreducible

Example $x^2+1$ is irreducible in $R[x]$, and $R[x]/(x^2+1) \cong \mathbb{F}_3$

Example A field with 9 elements.

Note $f(x) = x^2+1$ is irreducible in $\mathbb{Z}/3\mathbb{Z}$

Thus $\mathbb{Z}/3\mathbb{Z} [x]/(x^2+1) = F$ is a field.

$F = \left\{ a + bx \mid a, b \in \mathbb{Z}/3\mathbb{Z} \right\}$, so $|F| = 9$.

Addition: $(a+bx) + (c+dx) = (a+c) + (b+d)x$

Multiplication: $(a+bx)(c+dx) = (ac - bd) + (ad+bc)x$

$-1 = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}x$

Reason $(a+bx)\left(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}x\right)$

$= \frac{a^2+b^2}{a^2+b^2} + 0x = 1$. 
Proposition 16 Suppose \( g(x) \in \mathbb{F}[x] \) is monic, and
\[
g(x) = f_1(x)^{n_1} f_2(x)^{n_2} \cdots f_k(x)^{n_k}
\]
be its prime factorization. Then
\[
\mathbb{F}[x]/(g(x)) \cong \mathbb{F}[x]/(f_1(x)^{n_1}) \times \cdots \times \mathbb{F}[x]/(f_k(x)^{n_k}).
\]

Example
\[
\mathbb{R}[x]/(x^2-1) \cong \mathbb{R}[x]/(x+1) \times \mathbb{R}[x]/(x-1)
\cong \mathbb{R} \times \mathbb{R}
\]
(not a field!)
