Prime Factorization.

Given the properties of the irreducible (“prime”) polynomials in \( F[x] \), given any polynomial \( f(x) \), one can factorize it uniquely as \( c p_1(x)^{d_1} \cdots p_k(x)^{d_k} \) where \( c \in F^\times \) and \( p_1(x), \ldots, p_k(x) \) are monic irreducible polynomials.

Computing the \( \gcd \) and \( \text{lcm} \).

Given two polynomials, \( f(x) \) and \( g(x) \), one can factorize both: \( f(x) = c_f p_1(x)^{e_1} \cdots p_k(x)^{e_k} \) and \( g(x) = c_g p_1(x)^{e_1} \cdots p_k(x)^{e_k} \). Then \( \gcd(f(x), g(x)) = p_1(x)^{\min(e_1,d_1)} \cdots p_k(x)^{\min(e_k,d_k)} \) and \( \text{lcm}(f(x), g(x)) = p_1(x)^{\max(e_1,d_1)} \cdots p_k(x)^{\max(e_k,d_k)} \). In particular, \( f(x) g(x) = c_f c_g \gcd(f(x), g(x)) \text{lcm}(f(x), g(x)) \).

Example.

Let \( f(x) = (x^2+1)(x-3)^2(x+5)^7 \) and \( g(x) = (x-4)^2(x^2+1)^2 \). Then \( \gcd(f(x), g(x)) = (x^2 + 1) \) and \( \text{lcm}(f(x), g(x)) = (x^2 + 1)^3(x-3)^2(x+5)^7(x-4)^2 \).

Theorem.

The ring \( F[x] / f(x) \) is a field if and only if \( f(x) \) is irreducible.

Proof.

If \( f(x) \) is irreducible then every nonzero class in \( F[x] / f(x) \) has a representative \( h(x) \) with \( \gcd(f(x), h(x)) = 1 \). Then \( h(x) \) is invertible in \( F[x] / f(x) \). Therefore \( F[x] / f(x) \) is a field.

Assume \( f(x) = g(x) h(x) \) where \( g(x) \) and \( h(x) \) are not scalars (i.e. are of degree at least 1). Then the classes of \( g(x) \) and \( h(x) \) are zero divisors in \( F[x] / f(x) \), and \( F[x] / f(x) \) is not a field.

Proposition.

Let \( f(x) \in F[x] \) and assume \( f(a) = 0 \) for some \( a \in F \). Prove that \( (x - a)[f(x)] \).

Proof.

Divide \( f(x) \) by \( x - a \) with remainder: \( f(x) = q(x)(x - a) + r(x) \). Assume \( r(x) \neq 0 \) Then \( \deg(r) < \deg(x - a) \), \( \deg(r) = 0 \), so \( r(x) \) is a scalar \( c \in F \setminus \{0\} \). Now

---

**Email address:** adam1chapman@yahoo.com (Adam Chapman)
\[ f(a) = 0 = q(a)(a - a) + c = q(a) \cdot 0 + c = 0 + c = c, \text{ so } c = 0, \text{ contradiction.} \]

Therefore \( r(x) = 0 \) and \( f(x) = q(x)(x - a) \).

**Terminology.**

We call a polynomial \( f(x) \) of degree \( \geq 1 \) “reducible” if it is not irreducible, i.e. if \( f(x) = g(x)h(x) \) for some polynomials \( g(x) \) and \( h(x) \) of degree \( \geq 1 \).

**Proposition.**

Prove that if \( f(x) \) is of degree 2 or 3 then \( f(x) \) is reducible if and only if \( f(a) = 0 \) for some \( a \in F \).

**Proof.**

If \( f(a) = 0 \) then \( f(x) = q(x)(x-a) \) where \( \deg(q) = \deg(f) - 1 \), so \( f(x) \) is reducible.

Assume \( f(x) \) is reducible. Then \( f(x) = g(x)h(x) \) where \( \deg(g), \deg(h) \geq 1 \). If \( \deg(f) = 2 \) then \( \deg(g) = \deg(h) = 1 \). If \( \deg(f) = 3 \) then without loss of generality \( \deg(g) = 1 \) and \( \deg(h) = 2 \). Therefore \( g(x) = bx + c \) for some \( b \in F \setminus \{0\} \) and \( c \in F \). Take \( a = -\frac{c}{b} \). Then \( f(a) = g(a)h(a) = 0 \cdot h(a) = 0 \).

**Remark.**

There may be polynomials of degree \( \geq 4 \) which are reducible but have no roots. For example, \((x^2 + 1)^2 \in \mathbb{R}[x]\).

**Exercise.** Say in the following cases whether \( h(x) \) is invertible in \( \mathbb{R}[x]/f(x) \) and if so then find the inverse:

- \( h(x) = x^3 - 6x^2 + 11x - 6 \) and \( f(x) = x^3 - x \).
- \( h(x) = x^3 - 3x^2 - 4x + 12 \) and \( f(x) = x^3 - x \).

Say whether the following polynomials are irreducible:

- \( x^2 + x + 1 \) in \( \mathbb{Z}_2[x] \).
- \( x^2 + x + 1 \) in \( \mathbb{Z}_3[x] \).
- \( x^2 + x + 1 \) in \( \mathbb{Q}[x] \).
- \( x^2 + x + 1 \) in \( \mathbb{R}[x] \).
- \( x^2 + x + 1 \) in \( \mathbb{C}[x] \).