1 Reducible and Irreducible Polynomials

The idea behind a reducible or irreducible polynomial is very similar in nature to factoring and finding zeros of a polynomial.

1.1 Definition

Definition 1.1

Let D be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be **irreducible** over D if, whenever $f(x)$ is expressed as a product

$$f(x) = g(x)h(x)$$

with $g(x), h(x) \in D[x]$, then $g(x)$ *or* $h(x)$ is a unit in $D[x]$. A non-zero, non-unit element of $D[x]$ that is not irreducible over D is called **reducible** over D.

Fact: If F is a field, $f(x) \in F[x]$ is irreducible if and only if $f(x) = g(x)h(x)$ implies that one of $g(x)$ or $h(x)$ have degree 0.

We can try to make a similar definition for the integers to get a better idea of what this means. We can define an "irreducible" integer $n \in \mathbb{Z}$ is one such that

$$n = ab \implies a \in \{\pm 1\} \text{ or } b \in \{\pm 1\}$$

So, in the integers, the only set of "irreducible" integers are $\pm p$ for primes p.

1.1.1 Example 1: Polynomial

Consider the polynomial $f(x) = 2x^2 + 4$.

- This is **reducible** over $\mathbb{Z}$ since $2x^2 + 4 = 2(x^2 + 2)$ and neither 2 nor $x^2 + 2$ is a unit in $\mathbb{Z}[x]$.
- This is **irreducible** over $\mathbb{Q}$. If we use the same factorization described above, then note that 2 has a unit in $Q[x]$.
- This is **reducible** over $\mathbb{C}$ since $2x^2 + 4 = 2(x - i\sqrt{2})(x + i\sqrt{2})$. Here, if $g(x) = 2(x - i\sqrt{2})$ and $h(x) = x + i\sqrt{2}$, then none of g or h are units.

1.2 Reducibility Test for Degrees 2 and 3

Theorem 1.1

Let F be a field. If $f(x) \in F[x]$ and $\deg f(x)$ is 2 or 3, then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.

Proof. We will prove the contrapositive; that is, $f(x)$ is reducible if and only if $f(x)$ has a root in F.

- Backwards Direction: Suppose $a \in F$ with $f(a) = 0$. This implies that $(x - a)|f(a)$ which implies that $f(x) = (x - a)g(x)$. Thus, $\deg g(x) = \deg f(x) - 1 \geq 1$. But, we found a factorization, so $f(x)$ is reducible.
- Forward Direction: If $f(x)$ is reducible, then $f(x) = g(x)h(x)$ with $\deg g(x), \deg h(x) \neq 0$. The only options are
$$\deg f(x) = \deg g(x) + \deg h(x)$$
So, we can brute-force the possible degrees:

- $2 = 1 + 1$
- $3 = 1 + 2$ or $3 = 2 + 1$

Thus, there exists $ax + b \in F[x]$, $a \neq 0$, with $(ax+b)|f(x)$ which implies that $f(x) = (ax+b)q(x)$. This further implies that $f\left(-\frac{b}{a}\right) = 0 \cdot q\left(-\frac{b}{a}\right) = 0$. So, $f(x)$ has a root $-\frac{b}{a} \in F$.

This concludes the proof. □

1.2.1 Example 2: Polynomial

Consider the polynomial $f(x) = 2x^3 + 4$.

- Is $f(x)$ irreducible over $\mathbb{Q}$? Using the theorem above, we have

$$2x^3 + 4 = 0 \implies 2x^3 = -4 \implies x^3 = -\sqrt{2} \implies x = -\sqrt[3]{2}$$

  But, $-\sqrt[3]{2} \notin \mathbb{Q}$ so this is **irreducible**.

- This is **reducible** over $\mathbb{R}$.

1.2.2 Example 3: Polynomial

Consider the field $\mathbb{F}_2[x]$. Are the polynomials with coefficients in this field reducible?

- Degree 0:
  - 0: Reducible.
  - 1: Irreducible[1].
- Degree 1:
  - x: Irreducible[2].
  - $x + 1$: Irreducible[3].
- Degree 2:
  - $x^2 = xx$: Reducible.
  - $x^2 + 1$: Reducible[4].
  - $x^2 + x = x(x + 1)$: Reducible.
  - $x^2 + x + 1$: Irreducible.
- Degree 3:
  - Left as an exercise.

1.3 Relation Between Integer Coefficient and Rational Coefficient Polynomials

Theorem 1.2

Let $f(x) \in \mathbb{Z}[x]$. $f(x)$ is reducible over $\mathbb{Q} \implies f(x)$ is reducible over $\mathbb{Z}$.

Remark: The contrapositive of this theorem is important. In particular, $f(x)$ is irreducible over $\mathbb{Z} \implies f(x)$ is irreducible over $\mathbb{Q}$.

[1]This can be generalized to any non-zero constant polynomial.
[2]Cannot be factored since it is linear.
[3]Cannot be factored since it is linear. In general, a degree 1 polynomial with coefficients in a field are always irreducible.
[4]Using the theorem, note that $1 \in F_3$ and $1^2 + 1 = 2 \equiv 0$.

Warning: The *converse* of this theorem is not true. For an example, see $f(x) = 2x^2 + 4$.

Definition 1.2: Content

The **content** of a non-zero polynomial $a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ is $\gcd(a_0, a_1, \ldots, a_n)$.

Definition 1.3: Primitive Polynomial

A **primitive polynomial** is an element of $\mathbb{Z}[x]$ with content 1.