REDUCIBILITY TESTS

In high school, students spend much time factoring polynomials and finding their roots. In this chapter, we consider the same problems in a more abstract setting.

To discuss factorization of polynomials, we must first introduce the polynomial analog of a prime integer.

DEFINITION ***Irreducible Polynomial, Reducible Polynomial***

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 $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$. A nonzero, nonunit element of $D[x]$ that is not irreducible over D is called *reducible over D*.

In the case that an integral domain is a field F, it is more convenient, although equivalent, to define a nonconstant $f(x) \in F[x]$ to be irreducible if $f(x)$ cannot be expressed as a product of two polynomials of lower degree.

Ex. The polynomial $f(x) = 2x^2 + 4$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{Z}$.

Sol:

$$f(x) = 2(x^2+4)$$
$$= 2(x^2+2)$$
$$= g(x)\,h(x)$$

where $g(x) = 2 \in \mathbb{Q}[x]$

and $h(x) = x^2+4 \in \mathbb{Q}[x]$

And $g(x) = 2$ is unit because inverse of 2 i.e. $\frac{1}{2} \in \mathbb{Q}[x]$. Hence $f(x)$ is irreducible over $\mathbb{Q}$ but it is not irreducible over $\mathbb{Z}$ as $\frac{1}{2} \notin \mathbb{Z}[x]$.

Ex. The polynomial $f(x) = 2x^2 + 4$ is irreducible over R but reducible over C.

Sol.

$$f(x) = 2x^2 + 4$$
$$= 2(x^2 + 2)$$
$$= g(x)\,h(x)$$

where $g(x) = 2 \in R[x]$

$h(x) = x^2 + 4 \in R[x]$.

Since inverse of 2 i.e. $\frac{1}{2} \in R[x]$ so $g(x)$ is a unit. Hence $f(x)$ is irreducible over R.

But
$$f(x) = 2x^2 + 4$$
$$= 2(x^2 + 2)$$
$$= 2(x + \sqrt{2}i)(x - \sqrt{2}i)$$
$$= (2x + 2\sqrt{2}i)(x - \sqrt{2}i)$$
$$= g(x)\,h(x)$$

where $g(x) = 2x + 2\sqrt{2}i \in C[x]$

$h(x) = x - \sqrt{2}i \in C[x]$

Since C is a field and degree of $g(x)$ and $h(x)$ are less than degree of $f(x)$ so $f(x)$ is not irreducible over C.

Ex. The polynomial $x^2 - 2$ is irreducible over Q but reducible over R.

Sol^n. Let $f(x) = x^2 - 2$.

$$= (x + \sqrt{2})(x - \sqrt{2})$$

$$= g(x)\, h(x)$$

where $g(x) = x + \sqrt{2} \notin Q[x]$

$h(x) = x - \sqrt{2} \notin Q[x]$

i.e. $f(x)$ can not be expressed as a product of two polynomials from $Q[x]$ of lower degree. So $f(x) = x^2 - 2$ is irreducible over Q.

But both $g(x), h(x) \in R[x]$ and degree of $g(x)$ and $h(x)$ are 1 which are smaller than degree of $f(x)$ and R is a field. So $f(x) = x^2 - 2$ is reducible over R.

Theorem 17.1 **Reducibility Test for Degrees 2 and 3**

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

PROOF. Suppose that $f(x) = g(x)h(x)$, where both $g(x)$ and $h(x)$ belong to $F[x]$ and have degrees less than that of $f(x)$. Since $\deg f(x) = \deg g(x) + \deg h(x)$ (Exercise 16 of Chapter 16) and $\deg f(x) = 2$ or 3, at least one of $g(x)$ and $h(x)$ has degree 1. Say, $g(x) = ax + b$. Then, clearly, $-a^{-1}b$ is a zero of $g(x)$ and therefore a zero of $f(x)$ as well.

Conversely, suppose that $f(a) = 0$, where $a \in F$. Then, by the Factor Theorem, we know that $x - a$ is a factor of $f(x)$ and, therefore, $f(x)$ is reducible over F. ∎

Ex. The polynomial x^2+1 is irreducible over Z_3 but reducible over Z_5.

Soln:-

Let $f(x) = x^2+1$

$Z_3 = \{0, 1, 2\}$, $Z_5 = \{0, 1, 2, 3, 4\}$

$f(0) = 0^2+1 = 1 \neq 0$ in Z_3, Z_5

$f(1) = 1^2+1 = 2 \neq 0$ in Z_3, Z_5

$f(2) = 2^2+1 = 5 \neq 0$ in Z_3

but $5 \equiv 0$ in Z_5

$\therefore$ $f(x)$ has no zero in Z_3 but it has zero in Z_5. So $f(x) = x^2+1$ is irreducible over Z_3 but reducible over Z_5.

DEFINITION ***Content of Polynomial, Primitive Polynomial***

The *content* of a nonzero polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where the a's are integers, is the greatest common divisor of the integers $a_n, a_{n-1}, \ldots, a_0$. A *primitive polynomial* is an element of $Z[x]$ with content 1.

Gauss's Lemma

The product of two primitive polynomials is primitive.

PROOF. Let $f(x)$ and $g(x)$ be primitive polynomials, and suppose that $f(x)g(x)$ is not primitive. Let p be a prime divisor of the content of $f(x)g(x)$, and let $\overline{f}(x)$, $\overline{g}(x)$ and $\overline{f(x)g(x)}$ be the polynomials obtained from $f(x)$, $g(x)$, and $f(x)g(x)$ by reducing the coefficients modulo p. Then, $\overline{f}(x)$ and $\overline{g}(x)$ belong to the integral domain $Z_p[x]$ and $\overline{f}(x)\overline{g}(x) = \overline{f(x)g(x)} = 0$, the zero element of $Z_p[x]$ (see Exercise 28 in Chapter 16). Thus, $\overline{f}(x) = 0$ or $\overline{g}(x) = 0$. This means that either p divides every coefficient of $f(x)$ or p divides every coefficient of $g(x)$. Hence, either $f(x)$ is not primitive or $g(x)$ is not primitive. This contradiction completes the proof. ■