GAUSS’S LEMMA

An element \( a \) of a ring \( R \) is irreducible if it is not a unit and whenever \( a = bc \) either \( b \) or \( c \) is a unit. We are interested in the irreducible elements in \( R[x] \) primarily when \( R = \mathbb{Z} \) or is a field.

**Example 1.** \( 2x + 6 \) is not irreducible in \( \mathbb{Z}[x] \) since \( 2x + 6 = 2(x + 3) \) and neither \( 2 \) nor \( x + 3 \) are units in \( \mathbb{Z}[x] \). On the other hand \( 2x + 6 \) is irreducible in \( \mathbb{Q}[x] \).

Let \( f(x) \in \mathbb{Z}[x] \) be

\[
f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0
\]

The content of \( f(x) \) is the gcd of \( a_0, a_1, \ldots, a_m \). \( f(x) \) is said to be primitive if its content is 1.

**Theorem 2** (Gauss’s Lemma). If \( f(x) \) and \( g(x) \) are primitive polynomials in \( \mathbb{Z}[x] \) then \( f(x)g(x) \) is primitive.

**Proof.** Let \( f(x) \) be as above and let

\[
g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0
\]

Suppose that \( p \) is a prime dividing the coefficients of \( f(x)g(x) \). Let \( r \) be the smallest integer such that \( p \) does not divide \( a_r \) and \( s \) be the smallest integer such that \( p \) does not divide \( b_s \). (These exist since \( f(x) \) and \( g(x) \) are primitive.) The coefficient of \( x^{r+s} \) in \( f(x)g(x) \) is

\[
c_{r+s} = a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{r+s-1} b_1 + a_{r+s} b_0.
\]

Since \( p \) divides \( a_0, \ldots, a_{r-1} \) and \( b_0, \ldots, b_{s-1} \), \( p \) divides every term of \( c_{r+s} \) except for the term \( a_r b_s \). However, since \( p \mid c_{r+s} \), either \( p \) divides \( a_r \) or \( p \) divides \( b_s \). But this is impossible. \( \square \)

**Theorem 3.** Suppose that \( p(x) \in \mathbb{Z}[x] \) and \( p(x) = f(x)g(x) \), where \( f(x) \) and \( g(x) \) are in \( \mathbb{Q}[x] \). Then \( p(x) = f_1(x)g_1(x) \), where \( f_1(x) \) and \( g_1(x) \) are in \( \mathbb{Z}[x] \). Furthermore, \( \deg f(x) = \deg f_1(x) \) and \( \deg g(x) = \deg g_1(x) \).

**Proof.** Let \( a \) and \( b \) be nonzero elements of \( \mathbb{Z} \) such that \( af(x), bg(x) \) are in \( \mathbb{Z}[x] \). We can find \( a_1, b_2 \in \mathbb{Z} \) such that \( af(x) = a_1 f_1(x) \) and \( bg(x) = b_1 g_1(x) \), where \( f_1(x) \) and \( g_1(x) \) are primitive polynomials in \( D[x] \). Therefore, \( abp(x) = (a_1 f_1(x))(b_1 g_1(x)) \). Since \( f_1(x) \) and \( g_1(x) \) are primitive polynomials, it must be the case that \( ab \mid a_1 b_1 \) by Gauss’s
Lemma. Thus there exists a $c \in \mathbb{Z}$ such that $p(x) = cf_1(x)g_1(x)$. Clearly, $\deg f(x) = \deg f_1(x)$ and $\deg g(x) = \deg g_1(x)$.

**Theorem 4** (Eisenstein’s Criterion). Let $p$ be a prime and suppose that

$$f(x) = a_nx^n + \cdots + a_0 \in \mathbb{Z}[x].$$

If $p \mid a_i$ for $i = 0, 1, \ldots, n - 1$, but $p \nmid a_n$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

*Proof.* By Gauss’s Lemma, we need only show that $f(x)$ does not factor into polynomials of lower degree in $\mathbb{Z}[x]$. Let

$$f(x) = (b_rx^r + \cdots + b_0)(c_sx^s + \cdots + c_0)$$

be a factorization in $\mathbb{Z}[x]$, with $b_r$ and $c_s$ not equal to zero and $r, s < n$. Since $p^2$ does not divide $a_0 = b_0c_0$, either $b_0$ or $c_0$ is not divisible by $p$. Suppose that $p \nmid b_0$. Then $p \mid c_0$ since $p$ does divide $a_0$. Now since $p \mid a_n$ and $a_n = b_rc_s$, neither $b_r$ nor $c_s$ is divisible by $p$. Let $m$ be the smallest value of $k$ such that $p \nmid c_k$. Then

$$a_m = b_0c_m + b_1c_{m-1} + \cdots + b_mc_0$$

is not divisible by $p$, since each term on the right-hand side of the equation is divisible by $p$ except for $b_0c_m$. Therefore, $m = n$ since $a_i$ is divisible by $p$ for $m < n$. Hence, $f(x)$ cannot be factored into polynomials of lower degree and therefore must be irreducible. \qed