§4.5, 4.6: Irreducibility in \( \mathbb{Q}[x], \mathbb{R}[x], \) and \( \mathbb{C}[x] \)

Any \( g(x) \in \mathbb{Q}[x] \) has an associate that belongs to \( \mathbb{Z}[x] \) because for \( c \) the least common denominator of the nonzero rational coefficients of \( f(x) \), we have \( f(x) = cg(x) \) has integer coefficients.

Since \( g(x) \) and \( f(x) \) have the same roots, we can seek to factor \( g(x) \) by looking for roots of \( f(x) \) instead.

The integer 0 is a root of \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] \) if and only if \( a_0 = 0 \).

**Theorem 4.21 (The Rational Root Test).** Let \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] \). For nonzero integers \( r \) and \( s \) with \( r/s \) in lowest terms (i.e., \( r \) and \( s \) are relative prime), if \( r/s \) is a root of \( f(x) \), then \( r \mid a_0 \) and \( s \mid a_n \).

**Proof.** Suppose \( r/s \) is a root of \( f(x) \). Then
\[
a_n \left( \frac{r^n}{s^n} \right) + a_{n-1} \left( \frac{r^{n-1}}{s^{n-1}} \right) + \cdots + a_1 \left( \frac{r}{s} \right) + a_0 = 0.
\]

Multiplying this through by \( s^n \) gives
\[
a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0.
\]

This can be rewritten as
\[
a_0 s^n = -\left[a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1}\right]
= r \left[-a_n r^{n-1} - a_{n-1} r^{n-2} s - \cdots - a_1 s^{n-1}\right].
\]

This says that \( r \mid a_0 s^n \).

Since \((r, s) = 1\), then \((r, s^n) = 1\) (by Homework problem 1.2 #25 (Ed. 2) or 1.2 #23 (Ed. 3)).

Thus \( r \mid a_0 \) by Theorem 1.5 (Ed. 2) or Theorem 1.4 (Ed. 3).

To get \( s \mid a_n \), we start with
\[
a_n r^n = -\left[a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n\right]
= s \left[-a_{n-1} r^{n-1} - \cdots - a_1 r s^{n-2} - a_0 s^{n-1}\right].
\]

Then \( s \mid a_n r^n \), and since \((r, s) = 1\), then \((r^n, s) = 1\), so that \( s \mid a_n \).

The Rational Root Test does not says that there exists a rational root, but it says that if there is a rational root, it has to be of the form \( r/s \) where \( r \mid a_0 \) and \( s \mid a_n \).

This gives a list of possible rational roots, which unfortunately have to be checked individually to see if any of them are roots.
If any of the possible rational roots are indeed roots, then we can use these roots to factor the polynomial into a divisor with rational roots and a divisor without rational roots.

**Example.** Factor \( f(x) = 2x^4 - 3x^3 - 2x^2 + 2x + 1 \).

The possible rational roots of \( f(x) \) are factors \( r \) of \( a_0 = 1 \) divided by the factors \( s \) of \( a_n = 2 \), namely,

\[
\frac{r}{s} = 1, -1, \frac{1}{2}, -\frac{1}{2}.
\]

We check each of the possibly rational roots: \( f(1) = 0 \), \( f(-1) = 2 \), \( f(1/2) = 5/4 \), and \( f(-1/2) = 0 \).

Two degree one factors of \( f(x) \) are then \( x - 1 \) and \( x - (-1/2) = x + 1/2 \).

We multiply the later by 2 to get \( 2x + 1 \) as a factor of \( f(x) \).

Then \( g(x) = (x - 1)(2x + 1) = 2x^2 - x - 1 \) is a factor of \( f(x) \), and the quotient of dividing \( f(x) \) by \( g(x) \) is

\[
h(x) = x^2 - x - 1,
\]

which has no rational roots (its roots are the irrational \((1/2)(1 \pm \sqrt{5})\) by the quadratic formula).

You may have noticed that the factors of the integer coefficient \( f(x) \) are also integer coefficient.

**Theorem 4.23.** Let \( f(x) \in \mathbb{Z}[x] \). Then \( f(x) \) factors as a product of polynomials of degrees \( r \) and \( s \) in \( \mathbb{Q}[x] \) if and only if \( f(x) \) factors as a product of polynomials of degrees \( r \) and \( s \) in \( \mathbb{Z}[x] \).

The lack of rational roots does not mean that the polynomial is irreducible, only that none of its factors have rational roots.

There is a widely applicable method for determining the irreducibility of a polynomial with integer coefficients.

**Theorem 4.24 (Eisenstein’s Criterion).** Let \( f(x) = a_nx^n + \cdots + a_1x + a_0 \) be a nonconstant polynomial with integer coefficients. If there is a prime integer \( p \) such that \( p \mid a_i \) for \( i = 0, 1, \ldots, n - 1 \), \( p \nmid a_n \), and \( p^2 \nmid a_0 \), then \( f(x) \) is irreducible in \( \mathbb{Q}[x] \).

**Proof.** Suppose that \( f(x) = a_0 + a_1x + \cdots + a_nx^n \) is reducible, so that there is a factorization

\[
f(x) = (b_0 + b_1x + \cdots + b_rx^r)(c_0 + c_1x + \cdots + c_sx^s),
\]

where \( r \geq 1 \), \( s \geq 1 \), and \( b_i, c_i \in \mathbb{Z} \) by Theorem 4.23.

The constant term of \( f(x) \) is \( a_0 = b_0c_0 \), and by hypothesis, we have \( p \mid a_0 \), so that \( p \) being prime implies that \( p \mid b_0 \) or \( p \mid c_0 \).

WLOG, suppose \( p \mid b_0 \). (A similar argument follows if we supposed \( p \mid c_0 \).)

Since \( p^2 \nmid a_0 \), then it follows that \( p \nmid c_0 \) (for otherwise, if \( p \mid c_0 \), then as \( p \mid b_0 \) we would get \( p^2 \mid a_0 \)).

Now \( a_n = b_rc_s \), and we have \( p \nmid b_r \) because if it did, we would have \( p \mid a_n \), contrary to hypothesis.
There may be other \( b_i \) not divisible by \( p \).

Let \( b_k \) be the first of the \( b_i \) not divisible by \( p \), that is, let \( k \) satisfy \( 0 < k \leq r < n \) and
\[
p \mid b_i \text{ for } i < k, \text{ and } p \nmid b_k.
\]

The coefficient of \( x^k \) in \( f(x) \) in terms of its factors is given by
\[
a_k = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0.
\]

We rewrite this to give
\[
b_kc_0 = a_k - b_0c_k - b_1c_{k-1} - \cdots - b_{k-1}c_1.
\]

Since \( p \mid a_k \) and \( p \mid b_i \) for all \( 0 \leq i < k \), then \( p \mid b_kc_0 \).

Since \( p \) is prime, either \( p \mid b_k \) or \( p \mid c_0 \).

This contradicts \( p \nmid b_k \) and \( p \nmid c_0 \). \( \Box \)

Example. Use Eisenstein’s Criterion to establish the irreducibility in \( \mathbb{Q}[x] \) of
\[
f(x) = 5x^4 + 21x^3 - 14x^2 + 28x - 7.
\]

With \( p = 7 \) we have that \( p \mid (-7), p \mid 28, p \mid (-14), p \mid (21), p \nmid 5 \) and \( p^2 \nmid (-7) \).

Corollary. There are irreducible polynomials in \( \mathbb{Q}[x] \) of every positive degree.

Proof. For \( n \in \mathbb{N} \), and \( p \) a positive prime integer, the polynomial \( x^n + p \) is irreducible by Eisenstein’s Criterion. \( \Box \)

Unlike \( \mathbb{Q}[x] \), the irreducible polynomials in \( \mathbb{R}[x] \) and \( \mathbb{C}[x] \) are known.

The Fundamental Theorem of Algebra 4.26 Every nonconstant polynomial in \( \mathbb{C}[x] \) has a root in \( \mathbb{C} \).

This Fundamental Theorem says that \( \mathbb{C} \) is algebraically closed. This is not the case for \( \mathbb{R} \) or \( \mathbb{Q} \).

Corollary 4.27. A polynomial is irreducible in \( \mathbb{C}[x] \) if and only if its degree is 1.

Proof. An \( f(x) \in \mathbb{C}[x] \) of degree 2 or more has a root in \( \mathbb{C} \), and so has a degree one factor, and thus \( f(x) \) is reducible in \( \mathbb{C}[x] \).

A degree one \( g(x) \in \mathbb{C}[x] \) only have divisors of degree 1 (its associates) or degree 0 (the units in \( \mathbb{C} \), and so every degree 1 element of \( \mathbb{C}[x] \) is irreducible. \( \Box \)

Theorem 4.30 A polynomial \( f(x) \in \mathbb{R}[x] \) is irreducible if and only if \( f(x) \) has degree 1 or \( f(x) = ax^2 + bx + c \) (degree 2) with \( b^2 - 4ac < 0 \).

Corollary 4.31. Every \( f(x) \in \mathbb{R}[x] \) of odd degree has a root in \( \mathbb{R} \).

Proof. We factor \( f(x) = p_1(x)p_2(x) \cdots p_k(x) \) into irreducible factors of either degree 1 or degree 2.

Since \( \deg f(x) = \deg p_1(x) + \deg p_2(x) + \cdots + \deg p_k(x) \) and \( \deg f(x) \) is odd, we have \( \deg p_i(x) \) is odd for some \( 1 \leq i \leq k \).

A degree 1 factor \( p_i(x) = ax + b \) has a real root \(-b/a\), and so \( f(x) \) has a root in \( \mathbb{R} \). \( \Box \)