Math 2070 Week 12

Rational Root Theorem, Gauss's Theorem, Eisenstein's Criterion

12.1 Polynomials over $\mathbb{Z}$ and $\mathbb{Q}$

Theorem 12.1 (Rational Root Theorem)**.** *Let $f = a_0 + a_1x + \cdots + a_nx^n$, be a polynomial in $\mathbb{Q}[x]$, with $a_i \in \mathbb{Z}$, $a_n \neq 0$. Every rational root r of f in $\mathbb{Q}$ has the form $r = b/c$ ($b, c \in \mathbb{Z}$) where $b|a_0$ and $c|a_n$.*

Proof of Rational Root Theorem. Let $r = b/c$ be a rational root of f, where b, c are relatively prime integers. We have:

$$0 = \sum_{i=0}^{n} a_i(b/c)^i$$

Multiplying both sides of the above equation by c^n, we have:

$$0 = a_0c^n + a_1c^{n-1}b + a_2c^{n-2}b^2 + \cdots + a_nb^n,$$

or equivalently:

$$a_0c^n = -(a_1c^{n-1}b + a_2c^{n-2}b^2 + \cdots + a_nb^n).$$

Since b divides the right-hand side, and b and c are relatively prime, b must divide a_0.

Similarly, we have:

$$a_nb^n = -(a_0c^n + a_1c^{n-1}b + a_2c^{n-2}b^2 + \cdots + a_{n-1}cb^{n-1}).$$

Since c divides the right-hand side, and b and c are relatively prime, c must divide a_n. $\square$

Definition 12.2. A polynomial $f \in \mathbb{Z}[x]$ is said to be **primitive** if the gcd of its coefficients is 1.

Remark. Note that if f is monic, i.e. its leading coefficient is 1, then it is primitive.

If d is the gcd of the coefficients of f, then $\frac{1}{d}f$ is a primitive polynomial in $\mathbb{Z}[x]$.

Lemma 12.3 (Gauss's Lemma). *If $f, g \in \mathbb{Z}[x]$ are both primitive, then fg is primitive.*

Proof of Gauss's Lemma. Write $f = \sum_{k=0}^{m} a_k x^k$, $g = \sum_{k=0}^{n} b_k x^k$. Then, $fg = \sum_{k=0}^{m+n} c_k x^k$, where:

$$c_k = \sum_{i+j=k} a_i b_j.$$

Suppose fg is not primitive. Then, there exists a prime p such that p divides c_k for $k = 0, 1, 2, \ldots, m+n$.

Since f is primitive, there exists a least $u \in \{0, 1, 2, \ldots, m\}$ such that a_u is not divisible by p.

Similarly, since g is primitive, there is a least $v \in \{0, 1, 2, \ldots, n\}$ such that b_v is not divisible by p. We have:

$$c_{u+v} = \sum_{\substack{i+j=u+v \\ (i,j)\neq(u,v)}} a_i b_j + a_u b_v,$$

hence:

$$a_u b_v = c_{u+v} - \sum_{\substack{i+j=u+v \\ i<u}} a_i b_j - \sum_{\substack{i+j=u+v \\ j<v}} a_i b_j.$$

By the minimality conditions on u and v, each term on the right-hand side of the above equation is divisible by p.

Hence, p divides $a_u b_v$, which by Euclid's Lemma implies that p divides either a_u or b_v, a contradiction. $\square$

Lemma 12.4. *Every nonzero $f \in \mathbb{Q}[x]$ has a unique factorization:*

$$f = c(f) f_0,$$

where $c(f)$ is a positive rational number, and f_0 is a primitive polynomial in $\mathbb{Z}[x]$.

Definition 12.5. The rational number $c(f)$ is called the **content** of f.

Proof of Definition 12.5. **Existence:**

Write $f = \sum_{k=0}^{n} (a_k/b_k)x^k$, where $a_k, b_k \in \mathbb{Z}$. Let $B = b_0 b_1 \cdots b_n$. Then, $g := Bf$ is a polynomial in $\mathbb{Z}[x]$. Let d be the gcd of the coefficients of g. Let $D = \pm d$, with the sign chosen such that $D/B > 0$. Observe that $f = c(f)f_0$, where

$$c(f) = D/B,$$

and

$$f_0 := \frac{B}{D} f = \frac{1}{D} g$$

is a primitive polynomial in $\mathbb{Z}[x]$.

Uniqueness:

Suppose $f = ef_1$ for some positive $e \in \mathbb{Q}$ and primitive $f_1 \in \mathbb{Z}[x]$. We have:

$$ef_1 = c(f)f_0.$$

Writing $e/c(f) = u/v$ where u, v are relatively prime positive integers, we have:

$$uf_1 = vf_0.$$

Since $gcd(u, v) = 1$, by Euclid's Lemma the above equation implies that v divides each coefficient of f_1, and u divides each coefficient of f_0. Since f_0 and f_1 are primitive, we conclude that $u = v = 1$. Hence, $e = c(f)$, and $f_1 = f_0$. □

Corollary 12.6. *For $f \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$, we have $c(f) \in \mathbb{Z}$.*

Proof of Corollary 12.6. Let d be the gcd of the coefficients of f. Then, $(1/d)f$ is a primitive polynomial, and

$$f = d\left(\frac{1}{d}f\right)$$

is a factorization of f into a product of a positive rational number and a primitive polynomial in $\mathbb{Z}[x]$. Hence, by uniqueness of $c(f)$ and f_0, we have $c(f) = d \in \mathbb{Z}$. □

Corollary 12.7. *Let f, g, h be nonzero polynomials in $\mathbb{Q}[x]$ such that $f = gh$. Then, $f_0 = g_0 h_0$ and $c(f) = c(g)c(h)$.*

Proof of Corollary 12.7. The condition $f = gh$ implies that:

$$c(f)f_0 = c(g)c(h)g_0 h_0,$$

where f_0, g_0, h_0 are primitive polynomials and $c(f), c(g), c(h)$ are positive rational numbers. By a previous result $g_0 h_0$ is primitive. It now follows from the uniqueness of $c(f)$ and f_0 that $f_0 = g_0 h_0$ and $c(f) = c(g)c(h)$. □

Theorem 12.8 (Gauss's Theorem). *Let f be a nonzero polynomial in $\mathbb{Z}[x]$. If $f = GH$ for some $G, H \in \mathbb{Q}[x]$, then $f = gh$ for some $g, h \in \mathbb{Z}[x]$, where $\deg g = \deg G$, $\deg h = \deg H$.*

Consequently, if f cannot be factored into a product of polynomials of smaller degrees in $\mathbb{Z}[x]$, then it is irreducible as a polynomial in $\mathbb{Q}[x]$.

Proof of Gauss's Theorem. Suppose $f = GH$ for some G, H in $\mathbb{Q}[x]$. Then $f = c(f)f_0 = c(G)c(H)G_0H_0$, where G_0, H_0 are primitive polynomials in $\mathbb{Z}[x]$, and $c(G)c(H) = c(f)$ by the uniqueness of the content of a polynomial.

Moreover, since $f \in \mathbb{Z}[x]$, its content $c(f)$ lies in $\mathbb{Z}$. Hence, $g = c(f)G_0$ and $h = H_0$ are polynomials in $\mathbb{Z}[x]$, with $\deg g = \deg G$, $\deg h = \deg H$, such that $f = gh$. $\square$

Let p be a prime. Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$. It is a field, since p is prime. For $a \in \mathbb{Z}$, let $\overline{a}$ denote the residue of a in $\mathbb{F}_p$.

Exercise: We have $\overline{a} = \overline{a_p}$, where a_p is the remainder of the division of a by p.

Theorem 12.9. *Let $f = \sum_{k=0}^{n} a_k x^k$ be a polynomial in $\mathbb{Z}[x]$ such that $p \nmid a_n$ (in particular, $a_n \neq 0$). If $\overline{f} := \sum_{k=0}^{n} \overline{a_k} x^k$ is irreducible in $\mathbb{F}_p[x]$, then f is irreducible in $\mathbb{Q}[x]$.*

Proof of Theorem 12.9. Suppose $\overline{f}$ is irreducible in $\mathbb{F}_p[x]$, but f is not irreducible in $\mathbb{Q}[x]$. By Gauss's theorem, there exist $g, h \in \mathbb{Z}[x]$ such that $\deg g, \deg h < \deg f$ and $f = gh$.

Since by assumption $p \nmid a_n$, we have $\deg \overline{f} = \deg f$.

Moreover, $\overline{gh} = \overline{g} \cdot \overline{h}$ (**Exercise**).

Hence, $\overline{f} = \overline{gh} = \overline{g} \cdot \overline{h}$, where $\deg \overline{g}, \deg \overline{h} < \deg \overline{f}$. This contradicts the irreducibility of $\overline{f}$ in $\mathbb{F}_p[x]$.

Hence, f is irreducible in $\mathbb{Q}[x]$ if $\overline{f}$ is irreducible in $\mathbb{F}_p[x]$. $\square$

Example 12.10. The polynomial $f(x) = x^4 - 5x^3 + 2x + 3 \in \mathbb{Q}[x]$ is irreducible.

Proof of Example 12.10. Consider $\overline{f} = x^4 - \overline{5}x^3 + \overline{2}x + \overline{3} = x^4 + x^3 + 1$ in $\mathbb{F}_2[x]$. If we can show that $\overline{f}$ is irreducible, then by the previous theorem we can conclude that f is irreducible.

Since $\mathbb{F}_2 = \{0, 1\}$ and $\overline{f}(0) = \overline{f}(1) = 1 \neq 0$, we know right away that $\overline{f}$ has no linear factors. So, if $\overline{f}$ is not irreducible, it must be a product of two quadratic factors:

$$\overline{f} = (ax^2 + bx + c)(dx^2 + ex + g), \quad a, b, c, d, e, g \in \mathbb{F}_2.$$

Note that by assumption a, d are nonzero elements of $\mathbb{F}_2$, so $a = d = 1$. This implies that, in particular:

$$\begin{aligned} 1 &= \overline{f}(0) = cg \\ 1 &= \overline{f}(1) = (1+b+c)(1+e+g) \end{aligned}$$

The first equation implies that $c = g = 1$. The second equation then implies that $1 = (2+b)(2+e) = be$. Hence, $b = e = 1$.

We have:

$$\begin{aligned} x^4 + x^3 + 1 = (x^2+x+1)(x^2+x+1) \\ = x^4 + 2x^3 + 3x^2 + 2x + 1 = x^4 + x^2 + 1, \end{aligned}$$

a contradiction.

Hence, $\overline{f}$ is irreducible in $\mathbb{F}_2[x]$, which implies that f is irreducible in $\mathbb{Q}[x]$. $\square$

Theorem 12.11 (Eisenstein's Criterion). *Let $f = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial in $\mathbb{Z}[x]$. If there exists a prime p such that $p | a_i$ for $0 \leq i < n$, but $p \nmid a_n$ and $p^2 \nmid a_0$, then f is irreducible in $\mathbb{Q}[x]$.*

Proof of Eisenstein's Criterion. We prove by contradiction. Suppose f is not irreducible in $\mathbb{Q}[x]$. Then, by Gauss's Theorem, there exists $g = \sum_{k=0}^{l} b_k x^k$, $h = \sum_{k=0}^{n-l} c_k x^k \in \mathbb{Z}[x]$, with $\deg g, \deg h < \deg f$, such that $f = gh$.

Consider the image of these polynomials in $\mathbb{F}_p[x]$. By assumption, we have:

$$\overline{a_n} x^n = \overline{f} = \overline{g}\overline{h}.$$

This implies that $\overline{g}$ and $\overline{h}$ are divisors of $\overline{a_n} x^n$. Since $\mathbb{F}_p$ is a field, unique factorization holds for $\mathbb{F}_p[x]$. Hence, we must have:

$$\overline{g} = \overline{b_u} x^u, \quad \overline{h} = \overline{c_{n-u}} x^{n-u},$$

for some $u \in \{0, 1, 2, \ldots, l\}$.

If $u < l$, then $n - u > n - l \geq \deg \overline{h}$, which cannot hold.

So, we conclude that $\overline{g} = \overline{b_l} x^l$, $\overline{h} = \overline{c_{n-l}} x^{n-l}$.

In particular, $\overline{b_0} = \overline{c_0} = 0$ in $\mathbb{F}_p$, which implies that p divides both b_0 and c_0. Since $a_0 = b_0 c_0$, we have $p^2 | a_0$, a contradiction. $\square$

Example 12.12. The polynomial $x^5 + 3x^4 - 6x^3 + 12x + 3$ is irreducible in $\mathbb{Q}[x]$.