Lecture 15: Polynomials over a Field & Select Applications

Our goal here is to illustrate how our study of ideals and their structure and prime & irreducible elements etc. all tie together. The handout from my brother is a good source for clean proofs of much of what we've recently covered.

(Let R be an integral domain)

Def^n/ We say $x = a$ is a <u>root</u> of $f(x) \in R[x]$ has multiplicity k if there exists $g(x) \in R[x]$ such that $f(x) = (x-a)^k g(x)$ but $g(a) \neq 0$.

We can introduce the <u>formal</u> derivative to help capture multiplicity via evaluation of derivatives,

Def^n/ If $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$ then $f'(x) \in R[x]$ is defined by $f'(x) = n a_n x^{n-1} + \cdots + 2a_2 x + a_1$ and $f''(x) = n(n-1) a_n x^{n-2} + \cdots + 2a_2$ and generally $f^{(n+1)}(x) = \frac{d}{dx}\left[f^{(n)}(x)\right]$ where we define $g'(x) = \frac{dg}{dx}$.

Also, $f^{(0)}(x) = f(x)$.

Th^m/ If $f(x) \in R[x]$ has $x = a$ as root of multiplicity k iff $f^{(j)}(a) = 0$ for $j = 0, 1, \ldots, k-1$.

Notation: In this handout, unless otherwise specified, R denotes an integral domain.

Definition: Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots \in R[[x]]$ be a non-zero (formal) power series with coefficients in R. Suppose that $a_k \neq 0$ but $a_i = 0$ for $i < k$. Then we define $\operatorname{ldeg}(f(x)) = k$ (i.e., the low degree of $f(x)$ is k). Equivalently, $\operatorname{ldeg}(f(x)) = k$ if and only if $f(x)$ is divisible (in $R[[x]]$) by x^k but not x^{k+1}.

Lemma: Let $g(x), h(x) \in R[[x]]$ and suppose both are non-zero. Then $\operatorname{ldeg}(g(x)h(x)) = \operatorname{ldeg}(g(x)) + \operatorname{ldeg}(h(x))$.

Proof: Let $\operatorname{ldeg}(g(x)) = k$ and $\operatorname{ldeg}(h(x)) = \ell$. In particular, say $g(x) = b_kx^k + b_{k+1}x^{k+1} + \cdots$ where $b_k \neq 0$ and $h(x) = c_\ell x^\ell + c_{\ell+1}x^{\ell+1} + \cdots$ where $c_\ell \neq 0$.

Notice that $g(x)h(x) = (b_kx^k + b_{k+1}x^{k+1} + \cdots)(c_\ell x^\ell + c_{\ell+1}x^{\ell+1} + \cdots) = b_kc_\ell x^{k+\ell} + (b_{k+1}c_\ell + b_kc_{\ell+1})x^{k+\ell+1} + \cdots$. Also, note that since $b_k \neq 0$, $c_\ell \neq 0$, and R is an integral domain (it has no zero divisors), we have $b_kc_\ell \neq 0$. Therefore, $\operatorname{ldeg}(g(x)h(x)) = \operatorname{ldeg}(g(x)) + \operatorname{ldeg}(h(x))$. ■

Remark: If $g(x), h(x) \in R[x]$ are non-zero polynomials, then $\deg(g(x)h(x)) = \deg(g(x)) + \deg(h(x))$ since $g(x) = b_mx^m + \cdots + b_0$ with $b_m \neq 0$ and $h(x) = c_\ell x^\ell + \cdots + c_0$ with $c_\ell \neq 0$ implies $g(x)h(x) = b_mc_\ell x^{m+\ell} + \cdots + b_0c_0$ where $b_mc_\ell \neq 0$ since R has no zero divisors.

Consequently, notice if $f(x) \in (R[x])^\times$ then there is some $g(x) \in (R[x])^\times$ such that $f(x)g(x) = 1$ so that $\deg(f(x)) + \deg(g(x)) = \deg(f(x)g(x)) = \deg(1) = 0$ so that $\deg(f(x)) = \deg(g(x)) = 0$ and thus $f(x) = a_0$, $g(x) = b_0$, and $1 = f(x)g(x) = a_0b_0$. Thus $f(x) = a_0 \in R^\times$. Conversely, $f(x) = a \in R^\times$ implies $(f(x))^{-1} = a^{-1}$ exists in R. Therefore, $(R[x])^\times = R^\times$. Similarly, we have the following:

Corollary: $(R[[x]])^\times = \{a_0 + a_1x + a_2x^2 + \cdots \mid a_i \in R \text{ for all } i \text{ and } a_0 \in R^\times\}$

(i.e., the units are the power series whose constant term is a unit).

Proof: Let $f(x) \in (R[[x]])^\times$. Then there exists some $g(x) \in (R[[x]])^\times$ such that $f(x)g(x) = 1$, so $\operatorname{ldeg}(f(x)) + \operatorname{ldeg}(g(x)) = \operatorname{ldeg}(f(x)g(x)) = \operatorname{ldeg}(1) = 0$. Therefore, $f(x) = a_0 + a_1x + \cdots$ and $g(x) = b_0 + b_1x + \cdots$ where a_0 and b_0 are non-zero. We have $(a_0 + a_1x + \cdots)(b_0 + b_1x + \cdots) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots = 1$. Therefore, $a_0b_0 = 1$ so that $a_0, b_0 \in R^\times$.

Conversely, suppose $f(x) = a_0 + a_1x + \cdots$ where $a_0 \in R^\times$. Define $b_0 = a_0^{-1}$, $b_1 = -a_0^{-1}(a_1b_0)$, $b_2 = -a_0^{-1}(a_1b_1 + a_2b_0)$, and in general $b_m = -a_0^{-1}(a_1b_{m-1} + \cdots + a_mb_0)$ (we define b_m recursively in terms of $b_0, \ldots, b_{m-1}$). This implies $a_0b_0 = 1$, $a_0b_0 + a_1b_0 = 0$, $a_0b_2 + a_1b_1 + a_2b_0 = 0$, and in general $a_0b_m + a_1b_{m-1} + \cdots + a_mb_0 = 0$. Thus if we let $g(x) = b_0 + b_1x + \cdots$, then $f(x)g(x) = 1 + 0x + \cdots = 1$ so $(f(x))^{-1} = g(x)$ exists (i.e., $f(x) \in (R[[x]])^\times$). ■

Theorem: Let I be a non-zero ideal of a PID R. Then every element in R/I is a unit, zero divisor, or zero.

Proof: Everything is zero in R/I if $R = I$. Let's assume I is a non-zero, proper ideal. Since R is a PID, we have $I = (r)$ for some non-zero, non-unit $r \in R$. Consider a non-zero element $x + I \in R/I$. Let $(d) = (x, r) = (x) + I$ (i.e., d is a greatest common divisor of x and r). Thus $d = ax + br$ for some $a.b \in R$. Also, $x \in (x) \subseteq (d)$ so there exists $y \in R$ such that $x = dy$ and likewise $r = dz$ for some $z \in R$.

If d is a unit in R, we have $(d^{-1}a + I) \cdot (x + I) = 1 + I$ since $d^{-1}ax + (d^{-1}b)r = 1$. Thus $x + I$ is a unit in R/I. Now suppose d is not a unit in R. In this (final) case, we will have that $x + I$ is a zero divisor. First, suppose $z + I = 0 + I$. Then $z \in I = (r)$ so there is some $w \in R$ such that $z = rw$. This means that $r = zd = rwd$ implies $wd = 1$ (because R is an integral domain and $r \neq 0$). Thus d is a unit contrary to our assumption. Therefore, $z + I \neq 0 + I$ (also $x + I \neq 0 + I$ by assumption). However, $(x + I)(z + I) = xz + I = ydz + I = yr + I = 0 + I$. Therefore, $x + I$ is a zero divisor. ■

Corollary: In a PID, non-zero prime ideals are maximal. Consequently, irreducibles generate maximal ideals.

Proof: Let $\{0\} \neq I$ be a prime ideal of a PID R. Then R/I is an integral domain and hence has no zero divisors. Therefore, by our theorem above, every non-zero element is a unit. Thus R/I is a field and so I is maximal. Finally, prime elements generate prime ideals. Thus irreducible (= prime) elements generate maximal ideals. ■

Corollary: Let $f(x) \in \mathbb{F}[x]$ where $\mathbb{F}$ is a field. Then $f(x)$ is irreducible if and only if $\mathbb{F}[x]/(f(x))$ is a field.

Proposition: (Eisenstein's Criterion) Let $f(x) = a_nx^n + \cdots + a_1x + a_0 \in R[x]$ $(n \geq 1)$ be primitive (1 is a gcd of the coefficients – for example, monic suffices) and let P be a prime ideal such that $a_0, \ldots, a_{n-1} \in P$ but $a_n \notin P$ and $a_0 \notin P^2 = \{\sum_i a_ib_i \mid a_i, b_i \in P\}$. Then $f(x)$ is irreducible in $R[x]$ and also in $\mathbb{F}[x]$ where $\mathbb{F}$ is R's field of fractions.

Proof: Since $n \geq 1$ and $a_n \notin P$, $f(x)$ is non-constant and thus not a unit in $R[x]$. Suppose $f(x)$ is not irreducible. Since $f(x)$ is primitive, it must factor into polynomials of lower degree in $R[x]$, say $f(x) = g(x)h(x)$ where $g(x) = b_mx^m + \cdots + b_0$ and $h(x) = c_\ell x^\ell + \cdots + c_0$ where $b_m \neq 0$, $c_\ell \neq 0$, and $m, \ell > 0$. Now reduce the coefficients

of x appearing in $f(x)$, $g(x)$, and $h(x)$ mod P. Call the resulting polynomials $\bar{f}(x)$, $\bar{g}(x)$, and $\bar{h}(x)$. We have $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$ in $(R/P)[x]$.

Since P is a prime ideal, R/P is an integral domain. Therefore, $\text{ldeg}(\bar{f}(x)) = \text{ldeg}(\bar{g}(x)) + \text{ldeg}(\bar{h}(x))$. But $\bar{f}(x) = \overline{a_n}x^n$ since $a_0, \ldots, a_{n-1} \in P$ and $\overline{a_n} \neq 0$ (in R/P) since $a_n \notin P$. Therefore, $\text{ldeg}(\bar{f}(x)) = n$. Now since $\bar{g}(x)\bar{h}(x) = \bar{f}(x) \neq 0$ and $g(x)$'s hence $\bar{g}(x)$'s non-zero coefficients have indices between 0 and m, we must have that $\text{ldeg}(\bar{g}(x)) \leq m$. Likewise, $\text{ldeg}(\bar{h}(x)) \leq \ell$. Therefore, since $\text{ldeg}(\bar{g}(x)) + \text{ldeg}(\bar{h}(x)) = \text{ldeg}(\bar{f}(x)) = n = m + \ell$, we conclude $\text{ldeg}(\bar{g}(x)) = m$ and $\text{ldeg}(\bar{h}(x)) = \ell$. Thus $\deg(\bar{g}(x)) = \text{ldeg}(\bar{g}(x)) = m$ and $\deg(\bar{h}(x)) = \text{ldeg}(\bar{h}(x)) = \ell$. Therefore, $\bar{g}(x) = Bx^m$ and $\bar{h}(x) = Cx^\ell$ for some $B, C \in R/P$.

But this implies that both $\bar{g}(x)$'s and $\bar{h}(x)$'s constant terms are 0. Therefore, both b_0 and c_0 belong to P. But this implies that $a_0 = b_0c_0 \in P^2$ (contradiction). No such proper factorization can exist, so $f(x)$ is irreducible. ■

Corollary: (Eisenstein's Criterion for $\mathbb{Z}[x]$) Let $f(x) = a_nx^n + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ with $\gcd(a_0, \ldots, a_n) = 1$ (i.e., $f(x)$ is primitive) and suppose there is some prime (integer) p such that p divides $a_0, a_1, \ldots, a_{n-1}$ but p does not divide a_n and p^2 does not divide a_0. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ and hence irreducible in $\mathbb{Q}[x]$.

Example: Consider $f(x) = 10x^5 + 7x^4 - 14x^2 + 49x + 21 \in \mathbb{Z}[x]$. Notice that $p = 7$ divides all but the leading coefficient and $p^2 = 49$ does not divide the constant term. Thus by Eisenstein's criterion, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

For low degree polynomials, knowing whether they have a root or not, can determine irreducibility. First, we will recall some basic results and then we return to irreducibility.

Theorem: (Division Algorithm) Let $f(x), g(x) \in R[x]$ (where R is an integral domain) where the leading coefficient of $g(x)$ is a unit (in particular, $g(x)$ is not zero so it has a leading coefficient). Then there exists unique $q(x), r(x) \in R[x]$ such that $f(x) = g(x) \cdot q(x) + r(x)$ where either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.

We note that the division algorithm holds more generally than just over integral domains. However, if R is not an integral domain, we can lose uniqueness of quotient and remainders. Also, when R is a field, demanding that the leading coefficient is a unit is merely demanding that we divide by a non-zero polynomial (since all non-zero coefficients are units). As a consequence, when $\mathbb{F}$ is a field, $\mathbb{F}[x]$ is a Euclidean domain (with degree function $\delta = \deg$).

Proposition: Let $f(x) \in R[x]$ (where R is an integral domain). Then $a \in R$ is a root of $f(x)$ if and only if there exists some $g(x) \in R[x]$ such that $f(x) = (x - a)g(x)$.

Proof: Obviously if $f(x) = (x - a)g(x)$ then evaluating at $x = a$ yields $f(a) = (a - a)g(a) = 0$. Now suppose $a \in R$ is a root of $f(x)$. Since the leading coefficient of $x - a$ is 1 (i.e., a unit), we can divide $f(x)$ by $x - a$. Thus there exists $q(x), r(x) \in R$ such that $f(x) = (x - a)q(x) + r(x)$ where either $r(x) = 0$ or $\deg(r(x)) < \deg(x - a) = 1$ (i.e., $\deg(r(x)) = 0$). Either way, $r(x) = c$ is a constant polynomial. Thus $f(x) = (x - a)q(x) + c$. Evaluating at $x = a$ yields, $0 = f(a) = (a - a)q(a) + c$ (since a is a root of $f(x)$). Thus $c = 0$ and so $f(x) = (x - a)q(x)$ as desired. ■

Let $\mathbb{F}$ be a field. Notice that constant polynomials are either zero or units (so not irreducible). Suppose $f(x) \in \mathbb{F}[x]$ is reducible and $\deg(f(x)) > 0$. Then since $f(x)$ is non-constant, it must fail to be irreducible by factoring into a product of some non-constant polynomials of lower degree. Keeping in mind that $\deg(g(x)h(x)) = \deg(g(x)) + \deg(h(x))$ for any polynomials $g(x)$ and $h(x)$ with coefficients in an integral domain, we get that linear polynomials in $\mathbb{F}[x]$ must be irreducible (we can't factor into *non-constant* polynomials of lower degree).

Next, suppose $f(x) \in \mathbb{F}[x]$ where $\deg(f(x)) = 2$ or 3. Then any factorization into polynomials of smaller degree would have to involve at least one factor of degree 1. Therefore, having a factorization is the same as having a root. We get the following:

Proposition: Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$. If $\deg(f(x)) = 1$ (i.e., $f(x)$ is linear), then $f(x)$ is irreducible. If $\deg(f(x)) = 2$ or 3 (i.e., $f(x)$ is quadratic or cubic), then $f(x)$ is irreducible if and only if $f(x)$ has no roots in $\mathbb{F}$.

While any polynomial of degree 4 or more with a root must be reducible (since roots yield linear factors), failing to have roots doesn't imply irreducibility anymore. As a simple example, $x^4 + 2x^2 + 1 = (x^2 + 1)^2$ is reducible in $\mathbb{Q}[x]$ but it has no roots in $\mathbb{Q}$ (since $\pm i \notin \mathbb{Q}$).

Definition: We say that a root $x = a$ of $f(x)$ has multiplicity k if there exists some $g(x) \in R[x]$ such that $f(x) = (x - a)^k g(x)$ but $g(a) \neq 0$ (i.e., $g(x)$ does not contain a $x - a$ factor). Next, let $f(x) = a_nx^n + \cdots + a_0$. Then we define $f'(x) = na_nx^{n-1} + \cdots + 2a_2x + a_1$ (i.e., the formal derivative of $f(x)$).

It turns out that the formal derivative of polynomials in $R[x]$ obeys the same linearity and product rules that our usual derivative does. In particular, we have that if $f(x) = (x-a)^k g(x)$, then $f'(x) = k(x-a)^{k-1}g(x)+(x-a)^k g'(x) = (x - a)^{k-1}(kg(x) + (x - a)g'(x))$. In particular, if $x = a$ is a root of $f(x)$ of multiplicity k, then assuming $k \neq 0$ in R, $x = a$ is a root of $f'(x)$ of multiplicity $k - 1$.

Proposition: Let $0 \neq f(x) \in R[x]$ (where R is an integral domain). Then $f(x)$ has at most $\deg(f(x))$ roots in R (counting multiplicity).

Proof: Suppose $f(x)$ has roots $r_1, \ldots, r_\ell$ with multiplicities $k_1, \ldots, k_\ell$. Then $f(x) = (x - r_1)^{k_1} g(x)$ for some polynomial $g(x)$ where $\deg(g(x)) = \deg(f(x)) - k_1$. Notice that if b is any other root ($\neq r_1$), we have $0 = f(b) = (b - r_1)^{k_1} g(b)$ where $(b - r_1)^{k_1} \neq 0$. Thus $g(b) = 0$ and so $r_2, \ldots, r_\ell$ are roots of $g(x)$. Ultimately, we get that $f(x) = (x - r_1)^{k_1} \cdots (x - r_\ell)^{k_\ell} h(x)$ for some $h(x) \in R[x]$ where $\deg(h(x)) = \deg(f(x)) - k_1 - k_2 - \cdots - k_\ell$. Since $\deg(h(x)) \geq 0$, we have $k_1 + \cdots + k_\ell \leq \deg(f(x))$. ■

Let's see how to detect roots in certain circumstances.

Theorem: (Rational Root Theorem) Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ where R is an integral domain with field of fractions $\mathbb{F}$. Suppose $p/q \in \mathbb{F}$ for some $p, q \in R$, $q \neq 0$, and $\gcd(p, q) = 1$ (i.e., p/q is a reduced fraction). Then p/q is a root of $f(x)$ implies p divides a_0 and q divides a_n.

Proof: Suppose p/q is a reduced fraction and $f(p/q) = 0$. Then $a_n \left(\frac{p}{q}\right)^n + \cdots + a_1 \left(\frac{p}{q}\right) + a_0 = 0$. Multiplying this equation by q^n to clear denominators, we get $a^n p^n + a_{n-1} p^{n-1} q + \cdots + a_2 p^2 q^{n-2} + a_1 p q^{n-1} + a_0 q^n = 0$. Notice that $p(a^n p^{n-1} + a_{n-1} p^{n-2} q + \cdots + a_2 p q^{n-2} + a_1 q^{n-1}) = a^n p^n + a_{n-1} p^{n-1} q + \cdots + a_2 p^2 q^{n-2} + a_1 p q^{n-1} = -a_0 q^n$, so p divides $-a_0 q^n$. But p and q are relatively prime, so p must divide a_0. Likewise, q must divide a_n. ■

Example: Consider $f(x) = x^3 - 7x + 6 \in \mathbb{Z}[x]$. If $r = p/q$ is a rational root (written as a reduced fraction) of $f(x)$, then p must divide $a_0 = 6$ (i.e., $p = \pm 1, \pm 2, \pm 3$, or ± 6 and q must divide $a_n = 1$ (so $q = \pm 1$). Thus the only possible (rational) roots of $f(x)$ are $\pm 1, \pm 2, \pm 3$, and ± 6. A (tedious) blind check shows that $f(1) = f(2) = f(-3) = 0$. Therefore, $f(x) = (x - 1)(x - 2)(x + 3)$. Notice that any rational root of a monic polynomial is in fact an integral root!

Example: Consider $f(x) = 2x^3 + 5 \in \mathbb{Z}[x]$. Then p/q is a root of $f(x) \in \mathbb{Q}$ implies p divides 5 and q divides 2. Thus the only possible rational roots are ± 1, ± 5. $\pm 1/2$, and $\pm 5/2$. Since (after a tedious check) we find that none of these are roots of $f(x)$, we must conclude $f(x)$ has no roots in $\mathbb{Q}$. Since $f(x)$ is a cubic, we have that $f(x) = 2x^3 + 5$ is irreducible in $\mathbb{Q}[x]$.

Corollary: Let p be a prime. Then $\sqrt{p}$ and $\sqrt[3]{p}$ are irrational.

Proof: If $\sqrt{p}$ was rational, we would have a rational root of $x^2 - p$. But the rational root theorem says that the only possible rational roots of $x^2 - p$ are ± 1 and $\pm p$. Notice that $(\pm 1)^2 - p = 1 - p \neq 0$ and $(\pm p)^2 - p = p^2 - p \neq 0$. Thus $x^2 - p$ has no rational roots (it's irreducible in $\mathbb{Q}[x]$). In particular, its root $x = \sqrt{p}$ cannot be rational. Likewise, for $\sqrt[3]{p}$ consider the polynomial $x^3 - p$. ■

Corollary: Even better – Let p be a prime. Then $\sqrt[n]{p}$ for any $n > 1$ is irrational.

Proof: Apply Eisenstein's criterion to $x^n - p$ (using your prime p) and get that $x^n - p$ is irreducible in $\mathbb{Q}[x]$. Therefore, it has no rational roots. Thus its root $x = \sqrt[n]{p}$ cannot be rational. ■

Sometimes reducing mod some ideal will turn an infinite problem into a finite tractable one. First, let R be a commutative ring with 1 and I an ideal of R. Notice that we have a homomorphism from $R[x]$ to $(R/I)[x]$ where $a_n x^n + \cdots + a_0$ maps to $(a_n + I)x^n + \cdots + (a_0 + I)$ (i.e., reduce coefficients mod I). Let $\overline{f}(x)$ denote the image of $f(x)$ under this homomorphism.

Proposition: Let I be an ideal of a UFD R. Suppose that $f(x) = a_n x^n + \cdots + a_0 \in R[x]$ where $n > 0$, $a_n \notin I$, and $\gcd(a_0, \ldots, a_n) = 1$ (this last condition means $f(x)$ is primitive). If $\overline{f}(x)$ is irreducible in $(R/I)[x]$, then $f(x)$ is irreducible in $R[x]$ (and thus in $\mathbb{F}[x]$ where $\mathbb{F}$ is the field of fractions of R).

Proof: First, we note (without proof) that for primitive polynomials, irreducibility in $R[x]$ and irreducibility in $\mathbb{F}[x]$ are equivalent. Also, a nonconstant primitive polynomial is reducible in $R[x]$ if and only if it factors as a product of nonconstant polynomials of lower degree. Now we are ready to proceed.

Suppose $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are nonconstant polynomials in $R[x]$. Then $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ in $(R/I)[x]$. Now since $a_n \notin I$, we have $a_n + I \neq 0 + I$ and so $\deg(\overline{f}(x)) = \deg(f(x))$. Next, $\deg(f(x)) = \deg(g(x)h(x)) = \deg(g(x)) + \deg(h(x))$ (since R is an integral domain we have that the degree of the product is the sum of degrees). But $\deg(\overline{g}(x)) \leq \deg(g(x))$ and $\deg(\overline{h}(x)) \leq \deg(h(x))$ since reducing coefficients mod I can possibly lower degrees. Thus $\deg(\overline{f}(x)) = \deg(g(x)) + \deg(h(x)) \geq \deg(\overline{g}(x)) + \deg(\overline{h}(x)) \geq \deg(\overline{g}(x)\overline{h}(x)) = \deg(\overline{f}(x))$ (since in general the degree of the product is only bounded by the sum of degrees – a lack of zero divisors is needed to guarantee equality). If follows that $\deg(\overline{g}(x)) = \deg(g(x))$ and $\deg(\overline{h}(x)) = \deg(h(x))$. Thus $\overline{f}(x)$ properly factors in $(R/I)[x]$. ■

Example: Let's show that $f(x) = 2x^3 + 6x^2 - 15x + 3$ is irreducible in $\mathbb{Q}[x]$ using three techniques.

- Suppose p/q is a rational root (as a reduced fraction). Then, by the Rational Root Theorem, p divides 3 and q divides 2. Thus p/q is $\pm 1, \pm 3, \pm 1/2$, or $\pm 3/2$. A very tedious calculation shows that none of these are roots. Since our cubic polynomial has no roots in $\mathbb{Q}$, it is irreducible in $\mathbb{Q}[x]$.
- Notice that $p = 3$ divides all but the leading coefficient of $f(x)$ and $p^2 = 9$ does not divide the constant term 3. Thus by Eisenstein's criterion, $f(x)$ is irreducible in $\mathbb{Z}[x]$ (and thus also $\mathbb{Q}[x]$).
- If we reduce $f(x)$ modulo 5, we get $\overline{f}(x) = 2x^3 + x^2 + 3$. Plugging in $x = 0, 1, 2, 3$, and 4 yields $\overline{f}(x) = 3, 1, 3, 1$, and 2. Since (this cubic polynomial) $\overline{f}(x)$ has no roots in $\mathbb{Z}_5$, it is irreducible in $\mathbb{Z}_5[x]$. Applying our above proposition ($R = \mathbb{Z}$ and $I = (5)$), we conclude that $f(x)$ is irreducible in $\mathbb{Z}[x]$ (and thus in $\mathbb{Q}[x]$).

Testing irreducibility of integral polynomials mod primes is often quite helpful. In fact, the factorization algorithms of our computer algebra systems are built on this kind of thing. However, irreducibilty mod primes is not a cure all. Dummit and Foote give the example: $x^4 - 72x + 4$. This polynomial is irreducible in $\mathbb{Z}[x]$ but it is reducible in $\mathbb{Z}_p[x]$ for every prime p.

Of course, there are many other ways to check for irreducibility. One more simple trick is to shift the indeterminate. Notice that $f(x) = g(x)h(x)$ if and only if $f(x + a) = g(x + a)h(x + a)$. From this we immediately get:

Proposition: Suppose $a \in R$ and $f(x) \in R[x]$. Then $f(x + a)$ is irreducible if and only if $f(x)$ is irreducible.

Corollary: For any prime integer p, the cyclotomic polynomial $\Phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible in $\mathbb{Q}[x]$.

Proof: $\Phi_p(x+1) = \dfrac{(x+1)^p - 1}{(x+1) - 1} = \dfrac{1}{x}\left((x+1)^p - 1\right) = \dfrac{1}{x}\left(x^p + px^{p-1} + \binom{p}{2}x^{p-2} + \cdots \binom{p}{2}x^2 + px + 1 - 1\right)$

Therefore, $\Phi_p(x+1) = x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{2}x + p$. Notice that the binomial coefficient $\binom{p}{k} = \dfrac{p!}{k!(p-k)!}$ when $1 \leq k \leq p-1$ must be divisible by p (since $k < p$ and $p - k < p$ implies $k!$ and $(p-k)!$ are products of integers less than p). Thus we can apply Eisenstein's criterion to $\Phi_p(x + 1)$ noting that all but the leading coefficient are divisible by p and the constant term is not divisible by p^2. Finally, since $\Phi_p(x + 1)$ is irreducible, we also have that $\Phi_p(x)$ is irreducible. ■

There are also cyclotomic polynomials defined for non-prime indices. The general definition is that $\Phi_n(x)$ is the product of $x - \zeta$ as ζ ranges over all primitive n^{th}-roots of unity. Note: ζ is an n^{th}-root of unity if $\zeta^n = 1$. The n^{th}-roots of unity form a cyclic subgroup of order n of $\mathbb{C}^\times$ (under multiplication). An n^{th}-root is primitive if it generates this subgroup. For example, the 4^{th}-roots of unity are $\{\pm 1, \pm i\}$. This group is generated by $\pm i$ (so these are the primitive 4^{th}-roots of unity). Therefore, $\Phi_4(x) = (x - i)(x + i) = x^2 + 1$. When n is prime, all the n^{th}-roots of unity are primitive except for $x = 1$. This leads to our formula defined above. It turns out that all cyclotomic polynomials are irreducible over $\mathbb{Q}[x]$. These polynomials play an important role in Galois theory and number theory.

Addendum: One should distinguish between polynomials and polynomial functions. We say that a function f from a ring to a ring is a polynomial function if there are $a_0, \ldots, a_n \in R$ such that the formula $f(x) = a_n x^n + \cdots + a_0$ defines our function $f : R \to R$. This might seem just like the definition of the polynomial $g(x) = a_n x^n + \cdots + a_0 \in R[x]$, but there is a subtle difference. Both $f(x)$ and $g(x)$ are determined by their coefficients. However, while distinct lists of coefficients yield distinct polynomials in $R[x]$. It is possible to have two distinct polynomial formulas for the same polynomial function f!

Consider the following function $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ defined by $f(x) = x^2 + x + 1$. Then $f(0) = 0^2 + 0 + 1 = 1$ and $f(1) = 1^2 + 1 + 1 = 1$. Thus $f(x) = 1$ for all $x \in \mathbb{Z}_2$. So even though $x^2 + x + 1 \neq 1$ as polynomials in $\mathbb{Z}_2[x]$, we have $x^2 + x + 1 = 1$ as polynomial functions.

But our intuition that we should be able to use polynomials formally and as functions interchangably is not that far off. Consider the following:

Theorem: Let R be an infinite integral domain. Let $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + b_0$ be polynomials in $R[x]$. Then $f(r) = g(r)$ for all $r \in R$ (i.e., f and g are equal as polynomial functions) if and only if $f(x) = g(x)$ as polynomials in $R[x]$.

Proof: Obviously, if $f(x) = g(x)$ in $R[x]$, then they both define the same function. Suppose $f(r) = g(r)$ for all $r \in R$. Notice that if $h(x) = f(x) - g(x)$ is non-zero, it can have at most $\deg(h(x))$ roots (counting multiplicity). But $h(r) = f(r) - g(r) = 0$ for all $r \in R$ and R is infinite, so $h(x)$ must be zero. Thus $f(x) = g(x)$. ■

On the other hand, if R is finite, say $|R| = N$, then there can be at most N^N functions from R to R. Thus while there are infinitely many elements in $R[x]$ (as long as $R \neq \{0\}$), we can have no more than N^N polynomial functions!

I'll follow §9.5 from Dummit & Foote

Proposition (15) The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials $f(x)$. In particular, $\frac{F[x]}{(f(x))}$ is field iff $f(x)$ is irreducible.

Proposition (16) Let $g(x)$ be a nonconstant monic element of $F[x]$ and let $f_1(x), f_2(x), \ldots, f_n(x)$ be distinct irreducibles for which $g(x) = f_1(x)^{n_1} f_2(x)^{n_2} \cdots f_n(x)^{n_n}$. Then we have the following isomorphism of rings

$$\frac{F[x]}{(g(x))} \cong \frac{F[x]}{(f_1(x)^{n_1})} \times \frac{F[x]}{(f_2(x)^{n_2})} \times \cdots \times \frac{F[x]}{(f_n(x)^{n_n})}$$

Proof: since $(f_i(x)^{n_i})$ and $(f_j(x)^{n_j})$ are comaximal the Chinese Remainder Thm applies. //
($F[x]$ is Euclidean Domain)

E1 $g(x) = x^4 - 1 = (x+1)(x-1)(x^2+1)$

$$\frac{\mathbb{R}[x]}{(x^4-1)} \cong \frac{\mathbb{R}[x]}{(x+1)} \times \frac{\mathbb{R}[x]}{(x-1)} \times \frac{\mathbb{R}[x]}{(x^2+1)} \cong \mathbb{R} \times \mathbb{R} \times \mathbb{C}.$$

E2 $g(x) = x^3 - 1 = (x-1)(x^2+x+1)$

$$\frac{\mathbb{R}[x]}{(x^3-1)} \cong \frac{\mathbb{R}[x]}{(x-1)} \times \frac{\mathbb{R}[x]}{\left((x+\frac{1}{2})^2 + \frac{3}{4}\right)} \cong \mathbb{R} \times \mathbb{C}.$$

PROPOSITION 18

A finite subgroup of the multiplicative group of a field is cyclic. In particular, if F is a finite field, then $F^\times = F - \{0\}$ is a cyclic group.

Proof: by the fundamental Th^m of finite abelian groups the finite subgroup of $F^\times$ is direct product of cyclic groups,

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

where $n_k \mid n_{k-1} \mid \cdots \mid n_2 \mid n_1$. In general, if G is a cyclic group and $d \mid |G|$ then G contains precisely d-elements of order which divides d. Since $n_k \mid n_j$ for $j = 1, 2, \ldots, k \Rightarrow$ each factor contains n_k elements of order dividing n_k. If $k > 1$ then there would be more than n_k such elements $\Rightarrow$ there would be more than $\underbrace{X^{n_k} - 1}_{n_k\text{-roots of}}$ in the field F which $\rightarrow\leftarrow$ # of roots possible for $f(x) \in F[x]$. Hence $k = 1 \therefore G$ cyclic. //

Corollary 19: $\mathbb{Z}_p^\times$ is cyclic group (a.k.a. $U(p)$ is cyclic)

Corollary 20: Let $n \geq 2$ have $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ ← distinct primes

(1) $(\mathbb{Z}_n)^\times \cong (\mathbb{Z}_{p_1^{\alpha_1}})^\times \times (\mathbb{Z}_{p_2^{\alpha_2}})^\times \times \cdots \times (\mathbb{Z}_{p_k^{\alpha_k}})^\times$

(2.) $(\mathbb{Z}_{2^\alpha})^\times$ is direct product of $\mathbb{Z}_2$ and $\mathbb{Z}_{2^{\alpha-2}}$ for $\alpha \geq 2$

(3.) $(\mathbb{Z}_{p^\alpha})^\times \cong \mathbb{Z}_m$ where $m = p^{\alpha-1}(p-1)$ for any odd prime p.