MATH 431 PART 2: POLYNOMIAL RINGS AND FACTORIZATION

1. Polynomial rings (review)

Definition 1. A **polynomial** $f(x)$ with coefficients in a ring R is

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where all $a_i \in R$, $a_n \neq 0$, and $n \in \mathbb{Z}^+$. We call a_n the **leading coefficient** of $f(x)$. The **degree** of $f(x)$ is n (we write $\deg f(x) = n$) and x is called an **indeterminate**. The set of all polynomials with coefficients in R is denoted $R[x]$ ("R adjoin x").

Theorem 1. *$R[x]$ is a ring under polynomial addition and multiplication. For polynomials $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$ in $R[x]$, we define their sum and product as follows:*

- $f(x) + g(x) =$
- $f(x) \cdot g(x) =$

Theorem 2. *Let R be a ring.*

(a) If R is a commutative ring, so is $R[x]$.

(b) If R has a unity $1 \neq 0$ then 1 is also the unity of $R[x]$.

(c) If D is an integral domain (contains no zero divisors), then so is $D[x]$.

Proof. Parts (a) and (b) are clear from the definition of multiplication above. Part (c) we proved in homework in MATH 430; the general idea is that if polynomials $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$ in $D[x]$ are not zero themselves, then at least a_n and b_m (the leading coefficients) are nonzero. Then the polynomial $f \cdot g$ contains the term $a_n b_m x^{n+m}$ (which is nonzero since D was an integral domain) so $fg(x)$ is a nonzero polynomial. □

Given a ring R and indeterminates x and y, elements of $(R[x])[y]$ are polynomials in y with coefficients which are polynomials in x: $g(y) = f_0(x) + f_1(x)y + f_2(x)y^2 + \cdots + f_n(x)y^n$. By multiplying out and combining like terms, we get $g(x, y) = a_0 + a_{1,0}x + a_{0,1}y + a_{1,1}xy + a_{2,0}x^2 + \cdots + a_{m,n}x^m y^n$, a polynomial in x and y. This process can be repeated iteratively, so that we have the following definition.

Definition 2. $((((R[x_1])[x_2])[x_3])\dots)[x_n] = R[x_1, x_2, \dots, x_n]$ is the ring of polynomials in n indeterminates with coefficients in R.

If F is a field, then F is also an integral domain, so $F[x]$ is an integral domain. It is NOT a field, since there is no polynomial $f(x)$ so that $xf(x) = 1$ (so x has no multiplicative inverse). However, we learned in the Part 1 notes how to extend an integral domain to its field of quotients.

Theorem 3. *For a field F, $F(x)$ is the field of quotients of the integral domain $F[x]$. As a set,*
$F(x) =$

The proof (by construction) that $F(x)$ is the field of quotients of $F[x]$ follows the outline of the Part 1 notes!

2. Zeroes of polynomials

We spent a lot of energy in previous courses (for example, high school algebra, or calculus) solving equations, and in particular polynomials. This is equivalent to finding the zeroes of polynomials, and in this section we will relate that problem to one we encountered in MATH 430. This will give us more powerful tools to study the zeroes of polynomials, and in particular where they live.

For all that follows, let E be a field and let F be a subfield of E.

Theorem 4. *Let $\alpha \in E$ and let $f(x) \in F[x]$ where $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Then $\phi_\alpha : F[x] \to E$ defined by*

$$\phi_\alpha(f(x)) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

*is a ring homomorphism. We call this map **evaluation at** α and we will denote $\phi_\alpha(f(x))$ as $f(\alpha)$.*

Proof sketch. Let $f(x) = \sum_{i=0}^n a_ix^i$ and $g(x) = \sum_{i=0}^m b_ix^i$ be elements of $F[x]$. Use the formulas for addition and multiplication of polynomials given in Theorem 1 and the definition of ϕ_α to show that $\phi_\alpha(f(x)+g(x)) = \phi_\alpha(f(x)) + \phi_\alpha(g(x))$ and $\phi_\alpha(f(x)\cdot g(x)) = \phi_\alpha(f(x))\cdot\phi_\alpha(g(x))$.

We should note that since the representation of a polynomial $f(x) \in F[x]$ is unique up to adding or removing terms of the form $0x^i$, and $\phi_\alpha(0x^i) = 0\cdot\alpha^i = 0$ for all $i \geq 0$, the map ϕ_α is well-defined. □

Corollary 5. *With all notation as above, $\phi_\alpha(x) = \alpha$ and ϕ_α restricted to F is an isomorphism.*

This corollary might seem a little silly at first glance, but it is actually a powerful idea.

Definition 3. For $f(x) \in F[x]$, if $f(\alpha) = 0$ then α is a **zero** of $f(x)$.

Example 1. Give two examples of elements of $\ker\phi_3$. Describe all elements of $\ker\phi_0$. What is $\ker\phi_\pi$?

Then finding zeroes of a polynomial $f(x)$ can be rephrased as determining the values of α such that $\phi_\alpha(f(x)) = 0$. While this doesn't seem like a big change, remember that we have a lot of machinery about homomorphisms that can be put to use if we phrase the problem this way!

3. Factorization of polynomials over fields

As before, let E be a field and let F be a subfield of E. Suppose $f(x) \in F[x]$ factors into the product of two polynomials in $F[x]$ so that $f(x) = g(x)h(x)$. For $\alpha \in E$,

$$f(\alpha) = \phi_\alpha(f(x)) = \phi_\alpha(g(x)h(x)) = \phi_\alpha(g(x))\phi_\alpha(h(x)) = g(\alpha)h(\alpha)$$

since evaluation is a homomorphism, so if $f(\alpha) = 0$ then either $g(\alpha) = 0$ or $h(\alpha) = 0$. Then factoring polynomials reduces the amount of work we have to do to find zeroes of polynomials, since we can simply find the zeroes of the factors which are, at least in theory, simpler than the original polynomial.

Before we dive into factoring though, we need a few preliminary results. The first one looks like the Euclidean algorithm for integers, but rephrased in terms of polynomial division.

Theorem 6 (Division algorithm for polynomials)**.** *Let $f(x), g(x) \in F[x]$ of degree n and m respectively. There exist unique polynomials $q(x)$ and $r(x)$ such that*

$$f(x) = g(x)q(x) + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$. ($q(x)$ is the quotient of $f(x)$ and $g(x)$ and $r(x)$ is the remainder.)

How do we know that a polynomial $g(x)$ is a factor of $f(x)$ over F based on the division algorithm?

Corollary 7 (Factor Theorem)**.** *An element $a \in F$ is a zero of $f(x) \in F[x]$ if and only if*

Proof:

Corollary 8. *A nonzero polynomial $f(x) \in F[x]$ of degree n can have* _____ *zeroes in the field F.*

(Recall that R^* is the **multiplicative group** of a ring R, the group of units under multiplication. Since F is a field, all nonzero elements are units, so F^* is the group of nonzero elements of F under multiplication.)

Corollary 9. *If G is a finite subgroup of F^*, then G is cyclic. If F is finite, then F^* is cyclic.*

Proof:

Definition 4. $f(x) \in F[x]$ is **irreducible over** F (or is an **irreducible polynomial in** $F[x]$) if $f(x)$ cannot be expressed as the product of polynomials in $F[x]$ of strictly smaller degree than f. (Otherwise, f is **reducible**.)

Example 2. $f(x) = x^2 - 2$

Definition 4 suggests an analogy between irreducible polynomials in $F[x]$ and prime numbers in $\mathbb{Z}$ that will persist. The next two results should feel very familiar, especially if you try to rephrase them using prime numbers instead.

Theorem 10. *Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)$ divides $r(x)s(x)$ for $r(x), s(x) \in F[x]$ then*

If $p(x)$ divides $r_1(x)r_2(x)\dots r_n(x)$ for $r_i(x) \in F[x]$ then

Theorem 11. *If F is a field, then every polynomial $f(x) \in F[x]$ can be written as a product*

$$f(x) = u \cdot p_1(x)p_2(x)\dots p_k(x)$$

where u is a unit in F, and the $p_i(x) \in F[x]$ are all monic and irreducible. Moreover, this product is unique up to reordering the $p_i(x)$.

There are a number of easy criteria that will tell us whether a polynomial factors over some field.

Theorem 12. *Let $f(x) \in F[x]$ with $\deg f(x) = 2$ or 3. Then $f(x)$ is reducible over F if and only if*

This is a very nice theorem, but only works for small degree polynomials. What if we are dealing with a degree larger than three? It turns out that at least if we are trying to factor over $\mathbb{Q}$, there are some very handy results.

Theorem 13. *If $f(x) \in \mathbb{Z}[x]$, then $f(x)$ factors into a product of two polynomials of lower degrees r and s in $\mathbb{Q}[x]$ if and only if it has a factorization with polynomials of the same degrees r and s in $\mathbb{Z}[x]$.*

Proof sketch. One direction is very clear. For the other, assume there exists a factorization over $\mathbb{Q}[x]$; the idea is to clear denominators sufficiently to get the factors to have integer coefficients. □

Corollary 14 (Rational Root Theorem)**.** *If $f(x) \in \mathbb{Z}[x]$ is of the form $f(x) = a_0 + a_1x + \dots + a_nx^n$ with $a_0 \neq 0$, and if $f(x)$ has a zero $\frac{s}{t}$ in $\mathbb{Q}$, then $s|a_0$ and $t|a_n$. In particular, if $f(x)$ is monic and has a zero in $\mathbb{Q}$ then $f(x)$ has a zero m in $\mathbb{Z}$ and m must divide a_0.*

Example 3. Use this corollary to explain why $x^2 - 2$ is irreducible over $\mathbb{Q}$.

Example 4. Show that $f(x) = x^4 - 2x^2 + 8x + 1$ is irreducible over $\mathbb{Q}$.

The next result should be very surprising; given mild conditions on the coefficients of an integer polynomial that concern a single prime number, we can deduce irreducibility over $\mathbb{Q}$!

Theorem 15 (Eisenstein Criterion)**.** *Let $p \in \mathbb{Z}$ be a prime. Suppose that $f(x) = a_0 + a_1x + \cdots + a_nx^n$ is in $\mathbb{Z}[x]$, and $a_n \not\equiv 0 \bmod p$ but $a_i \equiv 0 \bmod p$ for all $i < n$, and $a_0 \not\equiv 0 \bmod p^2$. Then $f(x)$ is irreducible over $\mathbb{Q}$.*

Corollary 16. *The polynomial*

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$ for any prime p. (The polynomial $\Phi_p(x)$ is called the $\mathbf{p}^{th}$ ***cyclotomic polynomial**.)*

Proof:

Our last few results deal with factorizations over $\mathbb{R}$ and $\mathbb{C}$.

Lemma 17. *Every nonconstant polynomial in $\mathbb{C}[x]$ has a complex root. Thus, the irreducible polynomials in $\mathbb{C}[x]$ are*

Corollary 18. *If $f(x) \in \mathbb{C}[x]$ has degree n, then $f(x)$ has exactly n zeroes if*

Example 5. $f(x) = (x^2 + 1)(x - 1)^3(x + 7i)^{10}$

Lemma 19. *Suppose $f(x) \in \mathbb{R}[x]$. If $a + bi$ is a root of $f(x)$ over $\mathbb{C}$, then so is $a - bi$.*

Proof:

Theorem 20. *All polynomials which are irreducible over $\mathbb{R}$ are*

Proof: