Math 3527 (Number Theory 1)

Lecture #24

Polynomial Functions, Factorization in $F[x]$:

- Values of Polynomials, Polynomial Functions
- Roots of Polynomials, Factorization
- Repeated Factors and the Derivative

This material represents §4.3.1 from the course notes.

Polynomial Functions, I

As is likely familiar from high-school algebra, "plugging values in" to a polynomial in $F[x]$ allows us to glean some information about potential factorizations.

Definition

If F is a field and $p = a_0 + a_1x + \cdots + a_nx^n$ is an element of $F[x]$, for any $r \in F$ we define the value $p(r)$ to be the element $a_0 + a_1r + \cdots + a_nr^n \in F$.

Examples:

- If $p = 1 + x^2$ in $\mathbb{C}[x]$, then $p(1) = 1 + 1^2 = 2$, and $p(i) = 1 + i^2 = 0$.
- If $p = 1 + x^2$ in $\mathbb{F}_5[x]$, then $p(0) = 1$, $p(1) = 2$, $p(2) = 0$, $p(3) = 0$, and $p(4) = 2$.

Polynomial Functions, II

By evaluating a polynomial $p(x) \in F[x]$ at every value $r \in F$, we may view p as a function from F to F.

Important Warning:

- If $p = x^3$ in $\mathbb{F}_2[x]$, observe that $p(0) = 0$ and $p(1) = 1$.
- If $q = x^2$ in $\mathbb{F}_2[x]$, observe that $q(0) = 0$ and $q(1) = 1$.
- Thus, as *functions* from $\mathbb{F}_2$ to $\mathbb{F}_2$, p and q are the same.
- However, as *polynomials* in $F[x]$, p and q are different, since their degrees are different.

As another (perhaps more unsettling) example, notice that if $p = x^3 - x$ in $\mathbb{F}_3[x]$, then $p(0) = p(1) = p(2) = 0$, and so p is identically zero as a function, but it is not the zero polynomial.

Roots of Polynomials, I

There is a fundamental connection between the values of a polynomial and its factorization:

Proposition (Remainder/Factor Theorem)

Let F be a field. If $p \in F[x]$ is a polynomial and $r \in F$, then the remainder upon dividing $p(x)$ by $x - r$ is $p(r)$. In particular, $x - r$ divides $p(x)$ if and only if $p(r) = 0$.

In this situation when $p(r) = 0$, we say r is a zero or a root of $p(x)$.

Example: The value $r = 1$ is a root of $p = x^3 - 2x + 1$, since $p(1) = 0$. Indeed, we have a factorization $p = (x - 1)(x^2 + x - 1)$.

Roots of Polynomials, II

Proof:

- Suppose $p(x) = a_0 + a_1 x + \cdots + a_n x^n$.
- Observe first that $(x^k - r^k) = (x - r)(x^{k-1} + x^{k-2} r + \cdots + x r^{k-2} + r^{k-1})$, so in particular, $x - r$ divides $x^k - r^k$ for all k.
- Now write $p(x) - p(r) = \sum_{k=0}^{n} a_k (x^k - r^k)$, and since $x - r$ divides each term in the sum, it divides $p(x) - p(r)$.
- Since $p(r)$ is a constant, it is therefore the remainder after dividing $p(x)$ by $x - r$.
- Finally, since the remainder is unique, we see that $x - r$ divides $p(x)$ if and only if the remainder $p(r)$ is equal to zero.

Roots of Polynomials, III

Proposition (Number of Roots)

Let F be a field. If $p \in F[x]$ is a polynomial of degree d, then p has at most d distinct roots in F.

Proof: Induct on the degree d.

- It is easy to see a polynomial of degree 1 has exactly 1 root.
- Now suppose the result holds for all polynomials of degree $\leq d$ and let p be have degree $d+1$.
- If p has no roots we are done, so suppose $p(r) = 0$. By factoring, we see $p(x) = (x-r)q(x)$ for some polynomial $q(x)$ of degree d.
- By induction, $q(x)$ has at most d roots: then $p(x)$ has at most $d+1$ roots, because $(a-r)q(a) = 0$ only when $a = r$ or $q(a) = 0$ (since F is a field).

Factoring Polynomials, I

In general, it is not easy to determine when an arbitrary polynomial is irreducible, or to find its factorization if it has one. In low degree, this task can be done by examining all possible factorizations.

Proposition (Polynomials of Small Degree)

If F is a field and $q(x) \in F[x]$ has degree 2 or 3 and has no roots in F, then $q(x)$ is irreducible.

Proof:

- If $q(x) = a(x)b(x)$, taking degrees shows $3 = \deg(q) = \deg(a) + \deg(b)$.
- Since a and b both have positive degree, one of them must have degree 1. Then its root is also a root of $q(x)$.
- Taking the contrapositive gives the desired statement.

Factoring Polynomials, II

Example: Show that $p = x^2 + 2x + 11$ is irreducible in $\mathbb{R}[x]$.

- Over $\mathbb{R}$, the polynomial has no roots (since it is always positive).
- Alternatively, by the quadratic formula, we can compute the roots explicitly as $r = -1 \pm \sqrt{-10}$, and these are not real numbers.
- Either way, since p has degree 2 and no roots, it is irreducible.

Factoring Polynomials, III

Example: Show that $q = x^3 + x + 1$ is irreducible in $\mathbb{F}_5[x]$.

- To test whether this polynomial has any roots in $\mathbb{F}_5$, we can simply plug in every possible value.
- Explicitly, we see $q(0) = 1$, $q(1) = 3$, $q(2) = 1$, $q(3) = 1$, and $q(4) = 4$.
- Since none of these values is 0, q has no roots.
- Thus, since q has degree 3, q is irreducible in $\mathbb{F}_5[x]$.

Factoring Polynomials, IV

Example: Determine if $q = x^2 + x + 2$ is irreducible in $\mathbb{F}_7[x]$.

- To test whether this polynomial has any roots in $\mathbb{F}_7$, we can simply plug in every possible value.
- Explicitly, we see $q(0) = 2$, $q(1) = 4$, $q(2) = 1$, $q(3) = 0$.
- Since $q(3) = 0$ we see that $x - 3$ is a divisor of q, and we obtain an explicit factorization $q = (x - 3)(x - 3)$.

Factoring Polynomials, V

For polynomials of larger degree, determining irreducibility can be a much more difficult task. For certain particular fields, we can say more about the structure of the irreducible polynomials.

Theorem (Fundamental Theorem of Algebra)

Every polynomial of positive degree in $\mathbb{C}[x]$ has at least one root in $\mathbb{C}$. Therefore, the irreducible polynomials in $\mathbb{C}[x]$ are precisely the polynomials of degree 1, and so every polynomial in $\mathbb{C}[x]$ factors into a product of degree-1 polynomials.

This is a standard result of complex analysis and we take it for granted.

Factoring Polynomials, VI

It is more difficult to test whether a polynomial is irreducible in $\mathbb{Q}[x]$. We will state some useful results in this direction:

Proposition (Rational Root Test)

Suppose $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ has integer coefficients. Then any rational root r/s (in lowest terms) must have $r|a_0$ and $s|a_n$.

Proof:

- If $p(r/s) = 0$, then $a_n(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_0 = 0$.
- Clearing denominators and rearranging yields $a_n r^n = s(-a_{n-1}r^{n-1} - \cdots - a_0 s^{n-1})$.
- Thus, s divides $a_n r^n$, but since s and r are relatively prime, this means s divides a_n.
- In a similar way, we can see that r divides $a_0 s^n$ hence a_0.

Factoring Polynomials, VII

Example: Determine whether or not the polynomial $p(x) = x^3 + 4x + 4$ is irreducible in $\mathbb{Q}[x]$.

- Since this polynomial has degree 3, we need only determine whether it has any roots in $\mathbb{Q}$.
- By the rational root test, the only possible rational roots are ± 1, ± 2, and ± 4.
- We calculate $p(1) = 9$, $p(-1) = -1$, $p(2) = 20$, $p(-2) = -12$, $p(4) = 84$, $p(-4) = -76$.
- Since none of these values is zero, there are no rational roots, and the polynomial is irreducible.

Factoring Polynomials, VIII

If the degree is larger than 3, then our basic procedure of searching for roots will not always reveal the factorization.

For example, the polynomial $p(x) = x^4 + 3x^2 + 2$ has no roots in $\mathbb{R}[x]$, but does factor as $p(x) = (x^2 + 1)(x^2 + 2)$.

In general, unless a better procedure is available, it is necessary to examine all possible factorizations using case analysis. This can be quite lengthy even for polynomials of degree 4.

One useful fact for doing such case analysis is that (if the polynomial has integer coefficients) its factorization in $\mathbb{Q}[x]$ must also have integer coefficients. (This is a technical result known as Gauss's lemma, which we will omit.)

Factoring Polynomials, IX

Example: Show $x^4 + x^3 - 2x^2 + x + 1$ is irreducible in $\mathbb{Q}[x]$.

- First, by the rational root test, the only possible roots of this polynomial are ± 1, neither of which is a root.
- The only other possible factorization can be put into the form $x^4 + x^3 - 2x^2 + x + 1 = (x^2 + ax + b)(x^2 + cx + d)$.
- By expanding and comparing coefficients, we see that $a + c = 1$, $b + ac + d = -2$, $ad + bc = 1$, and $bd = 1$.
- The last equation gives $(b, d) = (1, 1)$ or $(-1, -1)$.
- If $b = d = 1$ then we obtain the equations $a + c = 1$ and $ac = -4$, which has no integer solutions.
- If $b = d = -1$ then we obtain $a + c = 1$, $ac = 0$, and $a + c = -1$, which has no solutions at all.
- Therefore, $p(x)$ is irreducible, as claimed.

Repeated Factors, I

Another property that we can fruitfully study in a general field is the presence of "repeated factors".

Examples:

- Over $\mathbb{C}$, the polynomial $x^3 + x^2 - x - 1$ factors into irreducibles as $(x-1)^2(x+1)$, which has the repeated factor $x - 1$.
- Over $\mathbb{F}_2$, the polynomial $x^4 + x^2 + 1$ factors into irreducibles as $(x^2 + x + 1)^2$, which has the repeated factor $x^2 + x + 1$.
- Over $\mathbb{F}_3$, the polynomial $x^3 + 1$ factors into irreducibles as $(x+1)^3$, which has the repeated factor $x + 1$.

Repeated Factors, II

As a first goal, we can give a necessary condition for when a polynomial has repeated roots.

- Recall from calculus that if a polynomial $q(x)$ has a "double root" at r, then $q(r)$ and $q'(r)$ are both zero. By the factor theorem, this is equivalent to saying that q and q' are both divisible by $x - r$.
- We can formulate a similar test over an arbitrary field using a purely algebraic definition of the derivative.

Repeated Factors, III

Definition

If $q(x) = \sum_{k=0}^{n} a_k x^k$ is a polynomial in $F[x]$, its derivative is the polynomial $q'(x) = \sum_{k=0}^{n} k a_k x^{k-1}$.

Examples:

- In $\mathbb{C}[x]$, the derivative of $x^6 - 4x^2 + x$ is $6x^5 - 8x + 1$.
- In $\mathbb{F}_p[x]$, the derivative of $x^{p^2} - x$ is $p^2 x^{p^2-1} - 1 = -1$. Notice here that although the degree of the original polynomial is p^2, the degree of the derivative is 0.

Repeated Factors, IV

The standard rules for differentiation carry over to our definition (as can be shown using a bit of algebra):

- The derivative is additive: $(f+g)'(x) = f'(x) + g'(x)$.
- The derivative obeys the Product Rule: $(f \cdot g)'(x) = f'(x)g(x) + f(x)g'(x)$.

The key idea is that the derivative can detect repeated roots:

Proposition (Repeated Factors)

Let F be a field and $q \in F[x]$. Then r is a repeated root of q if and only if $q(r) = q'(r) = 0$. More generally, q has a repeated factor if and only if q and q' are not relatively prime.

Repeated Factors, V

- Proof: First suppose that $q(x)$ has a repeated root r: then $q(x) = (x - r)^2 s(x)$ for some $s(x) \in F[x]$.
- Then $q'(x) = (x - r) \cdot [2s(x) + (x - r)s'(x)]$.
- Thus, q' is also divisible by $x - r$ in $F[x]$, so by the factor theorem, we conclude that $q(r) = q'(r) = 0$.
- Conversely, suppose that $q(r) = q'(r) = 0$.
- Then by the factor theorem we may write $q(x) = (x - r)a(x)$.
- The product rule gives $q'(x) = a(x) + (x - r)a'(x)$, so $q'(r) = a(r)$. Thus $a(r) = 0$ and so $x - r$ divides $a(x)$: then $q(x)$ is divisible by $(x - r)^2$ so r is a repeated root.
- By a similar argument, any repeated factor of q will yield a nontrivial common factor of q and q' in $F[x]$.

Repeated Factors, VI

Since we can efficiently compute the gcd of $q(x)$ and $q'(x)$ using the Euclidean algorithm in $F[x]$, we can quickly determine if a given polynomial has a repeated factor.

Example: Determine whether $q(x) = x^4 + 3x^3 + 3x^2 + 3x + 1$ has a repeated factor in $\mathbb{F}_5[x]$.

- We have $q'(x) = 4x^3 + 4x^2 + x + 3$.
- Performing the Euclidean algorithm on $q(x)$ and $q'(x)$ will yield a greatest common divisor of $2x^2 + 3x + 2$.
- Since the gcd has positive degree, $q(x)$ has a repeated factor.
- Indeed, if we divide $q(x)$ by $2x^2 + 3x + 2$, we will see that $q(x) = 4(2x^2 + 3x + 2)^2$.

Summary

We defined how to evaluate a polynomial $p \in F[x]$ at a value $r \in F$ and discussed the remainder and factor theorems.

We showed that a polynomial of 2 or 3 is irreducible if and only if it has no roots, and discussed how to factor polynomials of small degree.

We defined the derivative p' and showed that p has a repeated factor if and only if p and p' are both divisible by that factor.

Next lecture: Finite fields.