2. Factoring Polynomials in Arbitrary Fields

Patrick Dugan

1 Introduction

These are some results I got while messing around with polynomials. I originally came up with this only for polynomials with rational coefficients, but later while doing a different problem realized it generalises to any field (commutative multiplication).

This is a continuation of a previous post about kernels. It can be read on its own, but is part of a much larger proof.

2 Notation

For a polynomial $f(x)$, f_n denotes its nth coefficient

$$f(x) = \sum_{i=0} f_i x^i$$

Degree of polynomial f

$$deg(f)$$

Number of Solutions

$$sol(f)$$

Other notation will be elaborated later

3 Minimum Polynomial

3.1 Define

For field F and field H ($F \subseteq H$) an element k can have a minimum polynomial of F denoted $M_F(k)$ but for ease when it is obvious that it is of F it will be noted

$$P^k(x)$$

What this means is that the polynomial $P^k(x)$ is the smallest degree, non zero polynomial, with coefficients in F such that $P^k(k) = 0$. Also the leading coefficient is 1 (or the multiplicative identity). This last criteria is pretty easy to meet as one can simply divide both sides by the leading coefficient to make sure it is 1.

It short it is the smallest degree polynomial that is solved by k.

3.2 $f(k) = 0,\ deg(f) < deg(P^k) \Rightarrow f(x) = 0$

Given: $f(k) = 0$ and $deg(f) < deg(P^k)$ (coefficients of f are in F)
There cannot be a non zero polynomial smaller than P^k (with k as a sol)

$$f(x) \text{ is not a non zero polynomial}$$

$$f(x) = 0$$

3.3 $f(k) = 0,\ deg(f) = deg(P^k) \Rightarrow f(x) = cP^k(x)$

Given: $f(k) = 0$ and $deg(f) = deg(P^k) = n$ (coefficients of f are in F)

$$f(x) = \sum_{i=0}^{n} f_i x^i$$

Trying to cancel some stuff out lets define polynomial g such that

$$g(x) = f(x) - f_n P^k(x)$$

Expanding (remember leading coefficient in $P^k(x)$ is 1)

$$g(x) = \sum_{i=0}^{n} f_i x^i - f_n x^n + \sum_{i=0}^{n-1} -f_n c_i x^i$$

Simplify

$$g(x) = \sum_{i=0}^{n-1} (f_i - f_n c_i) x^i$$

Then

$$deg(g) < n = deg(P^k)$$

Also $g(k) = 0$

$$g(k) = f(k) - f_n P^k(k) = 0$$

So using 3.2

$$g(x) = 0$$

Finally since $g(x) = f(x) - f_n P^k(x)$

$$0 = f(x) - f_n P^k(x)$$

$$f(x) = f_n P^k(x)$$

This shows us that all other polynomials that k solves with the same degree as it's minimum polynomial are just scaled versions of its minimum polynomial.

3.4 Generalizing

Given: $f(k) = 0$ and $deg(f) = m \geq deg(P^k) = n$ (coefficients of f are in F)
With the exact same logic as in 3.3 we define polynomial g such that

$$g(x) = f(x) - f_m x^{m-n} P^k(x)$$

And like in 3.3

$$deg(g) < deg(f),\ g(k) = 0, \text{ and coefficients of g(x) are in F}$$

Moving around we get

$$f(x) = g(x) + f_m x^{m-n} P^k(x)$$

This means that for any polynomial (coefficients in F) where $f(k) = 0$, There exists $a \in F$, $n \in \mathbb{N}$, and $g(x)$ such that

$$f(x) = g(x) + ax^n P^k(x)$$

where $deg(g) < deg(f)$, $g(k) = 0$, and coefficients of $g_i \in F$

4 Factoring

Now we are going to use the idea above with induction to factor polynomials.

1. Inductive Assumption
   Assume that all polynomials $f(x)$ where $1 \leq deg(f) \leq m$ and $f(k) = 0$ can be written as $f(x) = g(x)P^k(x)$ st g is some polynomial where $deg(f) = deg(g) + deg(P^k)$

2. Recursive Case
   Take polynomial $f(x)$ with $deg(f) = m + 1$, $f(k) = 0$, and let $n = deg(P^k)$
   Define some a(x) st

   $$a(x) = f(x) - f_m x^{m+1-n} P^k(x)$$

   Since the lead term in f(x) canceled out $deg(a) \leq m$

   $$deg(a) < deg(f)$$

   $$deg(a) \leq m$$

   and by evaluation $a(k) = 0$

   $$a(k) = f(k) - f_m k^{m+1-n} P^k(k) = 0 - 0 = 0$$

   by the Inductive assumption $a(x) = b(x)P^k(x)$

   $$b(x)P^k(x) = f(x) - f_m x^{m+1-n} P^k(x)$$

   $$(b(x) + f_m x^{m+1-n})P^k(x) = f(x)$$

Set $g(x) = b(x) + f_m x^{m+1-n}$

$$f(x) = g(x)P^k(x)$$

Since (inductive assumption) $deg(b) = m - n < m + 1 - n$

$$deg(g) = deg(b + f_m x^{m+1-n}) = max(deg(b), deg(f_m x^{m+1-n}))$$

$$= deg(f_m x^{m+1-n})) = m + 1 - n$$

$$deg(f) = m + 1 = m + 1 - n + n = deg(g) + deg(P^k)$$

Finally for all polynomial $f(x)$ where $deg(f) \leq m + 1$, $f(k) = 0$

$$f(x) = g(x)P^k(x) \text{ where g is some polynomial}$$

$$deg(f) = deg(g) + deg(P^k)$$

3. Base Case
   By 3.3 For all $f(x)$ st $f(k) = 0$ and $deg(f) = deg(P^k)$, let the lead term of $f(x)$ be c

$$f(x) = cP^k(x)$$

$$g(x) = c$$

$$f(x) = g(x)P^k(x)$$

$$deg(f) = deg(P^k) = deg(g) + deg(P^k)$$

All together

For any polynomial $f(x)$ with coefficients in field F and where $f(k) = 0$,

$$f(x) = g(x)P^k(x) \text{ and } deg(f) = deg(g) + deg(P^k)$$

where g(x) is some polynomial with coefficients in F

This allows us to factor out solutions for polynomials in an arbitrary fields. We are being extra careful with the degrees adding up as, even though it may feel obvious, when working with a polynomial in modular arithmetic (or any finite field) where often degrees can be simplified via Fermat's little theorem, such a fact needs some securing.

4.1 With Rationals

I originally developed these tools for polynomials with rational coefficients to explain a cool pattern I found with rational polynomials. I noticed that irrational solutions to quadratics tend to come in pairs.
For instance I noticed that if

$$f(\sqrt{2}) = 0$$

then,

$$f(-\sqrt{2}) = 0$$

This is because of the minimum polynomial of $\sqrt{2}$ which we can find.
We know that $\sqrt{2}$ solves $x^2 - 2$ so its minimum polynomial is either degree 1 or 2
If it were degree 1 it would have to be

$$x - \sqrt{2}$$

Since $\sqrt{2}$ is not rational this polynomial cant be a minimum polynomial.

$$deg(P^{\sqrt{2}}) = 2$$

And thus

$$P^{\sqrt{2}}(x) = x^2 - 2$$

So if a rational polynomial $f(x)$ has a solution of $\sqrt{2}$

$$f(x) = g(x)P^{\sqrt{2}}(x)$$

But here is the interesting part $P^{\sqrt{2}}(x)$ has more solutions then just $\sqrt{2}$. $-\sqrt{2}$ also is a solution so

$$f(-\sqrt{2}) = g(-\sqrt{2})P^{\sqrt{2}}(-\sqrt{2}) = 0$$

With this I devised a pretty cool math problem to stump my friends

$$f(x) = x^4 + ax^3 + bx^2 + cx + d \text{ where } a, b, c, d \in \mathbb{Q}$$

$$f(\sqrt{2}) = 0,\ f(\phi) = 0\ (\phi \text{ is golden ratio})$$

solve for a,b,c, and d

4.2 On a more complex note

Also there is some interesting finds when looking at polynomials with real coefficients aka ($F = \mathbb{R}, H = \mathbb{C}$)
Take complex number z

$$z = a + ib$$

The minimum polynomial can not be degree 1

$$x - z \text{ does not have real coefficients}$$

But looking at conjugates ($\overline{z} = a - ib$)

$$(x - z)(x - \overline{z}) = x^2 + -2ax + a^2 + b^2$$

This is a real polynomial so

$$P^z(x) = (x - z)(x - \overline{z})$$

This means that for any real polynomial f

$$f(z) = 0 \Rightarrow f(\overline{z}) = 0$$

5 Solutions for nth degree polynomial

5.1 Intro

Some may feel this derivation is overkill but it kind of needs to be. On a arbitrary field weird things may happen like ($x^4 \equiv 1 \mod 5$) aka the degree may be deceiving, but with the strict inequalities we develop this can be helped.

We are going to be doing this via proof by contradiction.

Assume there is a polynomial $f(x)$ with coefficients in some field F st

$$sol(f) = m > deg(f) = n$$

where sol(f) is the number of solutions in F.
We will label the solutions like so

$$f(k_i) = 0, k_i \in F$$

Also it is required that $1 \leq deg(f)$ as we will need the factoring result from (4.0).

Although it feels useless to look at minimum polynomials in F as they are just going to be linear but bare with it. So with the weird notation we are defining $P^k(x) = M_F(k)$

5.2 Minimum Polynomials

Since we are looking at the minimum polynomials with coefficients in F (and k_i is in F) things are pretty easy

$$P^{k_i}(x) = x - k_i$$
$$deg(P^{k_i}) = 1$$

done

5.3 Factoring

Ok we are going to do this a little recursively ($f(x) = {}_0f(x)$) First applying 4.0 to ${}_0f(x)$

$${}_0f(x) = P^{k_0}(x)({}_1f(x))$$

And then applying again to ${}_1f(x)$

$${}_1f(x) = P^{k_1}(x)({}_2f(x))$$

Continuing

$${}_if(x) = P^{k_i}(x)({}_{i+1}f(x))$$

And also because of 4.0

$$deg({}_if(x)) = deg(P^{k_i}) + deg({}_{(i+1)}f(x))$$

Since we know what P^{k_i} is

$${}_if(x) = (x - k_i)({}_{i+1}f(x))$$

$$deg({}_i f) = 1 + deg({}_{i+1} f)$$

Working this around

$$deg({}_i f) = deg({}_0 f) - i$$

$deg({}_0 f) = n$

$$deg({}_i f) = n - i$$

Since $deg({}_n f) = 0$

$${}_n f(x) = c \text{ (some constant)}$$

Expanding out

$${}_0 f(x) = (x - k_0)(x - k_1) \ ... \ (x - k_{n-1})({}_n f(x))$$

$${}_0 f(x) = (x - k_0)(x - k_1) \ ... \ (x - k_{n-1})c$$

5.4 $sol(f) \leq deg(f)$

Since f(x) has more than n solutions, then k_n (the n+1 th solution) should work

$$f(k_n) = 0$$

But since 0 is not in the multiplicative group

$$(k_n - k_0)(k_n - k_1) \ ... \ (k_n - k_{n-1})c \neq 0$$

This is a contradiction so

For any polynomial f, $sol(f) \leq deg(f)$