Finite Field FExtensions for a FCalculus FBC FStudent

Parth Nobel

May, 2019

1 Fields

What is a field?

I am not going to axiomatically define a field, but the basic idea is

Definition 1. *Field A **field** is a set of numbers which you can add, subtract, multiply, and divide (by non-zero numbers) elements of the set while always still being inside the set.*

The natural numbers, $\mathbb{N} = \{1, 2, 3, 4, \dots\}$, are not a field, because $1 - 3 \notin \mathbb{N}$.

The integers, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ are not a field, because $1/3 \notin \mathbb{Z}$.

The rationals, $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in mathbbZ\} = \{\dots, -2, -\frac{1}{2} - 1, 0, 1, \frac{1}{2}, 2, \dots\}$ are a field, because the sum, difference, product, and quotient (of a non-zero rational number) is still a rational number.

The reals, $\mathbb{R}$, and the complex numbers, $\mathbb{C} = \{a + bi \mid i^2 = -1, a, b \in \mathbb{R}\}$, are also fields.

Q, R, and C will be the only three fields we consider in this text.

2 Polynomials of a Field

Definition 2. *Polynomials of a field, F A polynomial of a field F is a polynomial whose coefficients are in the field F.*

So $\frac{1}{2}, \frac{1}{2}x, \frac{4}{5}x^8 + \frac{3}{2}x^3, x$ are all polynomials of $\mathbb{Q}$. $\frac{1}{2}, \frac{1}{2}x, \frac{4}{5}x^8 + \frac{3}{2}x^3, x, x + \pi$ are all polynomials of $\mathbb{R}$. $\frac{1}{2}, \frac{1}{2}x, \frac{4}{5}x^8 + \frac{3}{2}x^3, x, x + \pi, ix^4 - \pi ix + 3$ are all polynomials of $\mathbb{C}$.

2.1 Irreducible Polynomials over a Field

Definition 3. *Irreducible Polynomials over a field, F A polynomial of F, $f(x)$, is irreducible over a field F if there are no polynomials of F of lesser degree, $p(x), q(x)$, such that $f(x) = p(x)q(x)$.*

I'll only show two or three examples of irreducible polynomials: $x^2 - 2$ is irreducible over $\mathbb{Q}$ because the only way to factor a degree two polynomial is to write it as a product of x minus one of its roots. The roots of $x^2 - 2$ are $\pm\sqrt{2}$ which are irrational, and therefore this polynomial is irreducible.

I'll only show two or three examples of irreducible polynomials: $x^2 + 2$ is irreducible over $\mathbb{R}$ because the only way to factor a degree two polynomial is to write it as a product of x minus one of its roots. The roots of $x^2 + 2$ are $\pm i\sqrt{2}$ which is complex, and therefore this polynomial is irreducible.

There are other other polynomials of any degree which is irreducible over $\mathbb{Q}$, for rather complicated reasons, there are only polynomials of degree 2 that are irreducible over $\mathbb{R}$, and by the Fundamental Theorem of Algebra there are no irreducible polynomials over $\mathbb{C}$.

3 Finite Field Extensions

Given an irreducible polynomial of degree n over a field F, the "smallest"[1] subset of $\mathbb{C}$ such that the polynomial has a zero in that set.

Wait what?

Let's try an example. For $f(x) = x^2 - 2$ over $\mathbb{Q}$, let's find a field where f has a solution in it. The trivial choice is $\mathbb{C}$, but we want something "smaller", so we could turn to $\mathbb{R}$, but that's still huge, the only numbers we need to add is $\pm\sqrt{2}$, so what if we do that, and just add the $\pm\sqrt{2}$ to $\mathbb{Q}$? Well we still want a field, so we have to add stuff like $2\sqrt{2}$ and $\frac{1}{\sqrt{2}}$. So let's just say that we're going to have the set $\mathbb{Q}\{a\sqrt{2} \mid a \in \mathbb{Q}\}$. But we need addition! So we can just make $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. This is still a field (can you see why?), and now f has a zero in this field!

Does $\mathbb{Q}(\sqrt{2})$ Look similar to something? Isn't this how we define $\mathbb{C}$ with respect to $\mathbb{R}$, but with i instead of $\sqrt{2}$? It is! Because $\mathbb{C} = \mathbb{R}(i)$!

So let's give a partial definition of a finite field extension.

Definition 4. *Finite Field Extension An FFE of a field F with dimension 2 over F with respect to an irreducible polynomial $f(x)$ of degree 2 has the form of*

$$\{a_0 + a_1\alpha \mid a_i \in \mathbb{F}\}$$

for some $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$.

[1] The definition of smallest used here is mostly based off your intuition and not math, because, well, it is complicated. Basically there are real numbers that computers can't compute to an arbitrary number of decimal places, and a rational number can be uniquely encoded as a natural number, and therefore some infinite sets are smaller than others, but these aren't those set size comparisons. So, ignore this footnote and take more math classes even if you decide to major in History and/or Poli Sci.