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 over F with respect to an irreducible polynomial $f(x)$ of degree n has the form of*

$$\{\sum_{i=0}^{n-1} a_i \alpha^i \mid a_i \in F\}$$

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

Consider the FFE of $\mathbb{Q}$ with respect to $g(x) = x^3 - 2$, $\alpha = \sqrt[3]{2}$ and the field is of the form

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2}^2\}.$$

[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.

Take some time and convince yourself this is correct.

We also will now give an informal definition of $F(\alpha)$, it is the smallest field containing F and α. For any rational number, c, $\mathbb{Q}(c) = \mathbb{Q}$. For a transcendental number ρ, such as π or e, then $\mathbb{Q}(\rho)$ is not a finite field extension, and out of scope for this paper. For the algebraic numbers, *i.e.* numbers that can be written using just addition, square roots, integer exponents, and multiplication of rational numbers, are all finite field extensions.

3.1 FFE of an FFE

Now let's try and find a zero of $f(x) = x^2 - 2$ in $\mathbb{Q}(\sqrt{3})$. It is of the form,

$$\{a_0 + a_1\sqrt{2} \mid a_0, a_1 \in \mathbb{Q}(\sqrt{3})\}$$

, but if we try to re-express this with regard to $\mathbb{Q}$, we find that

$$\mathbb{Q}(\sqrt{3})(\sqrt{2}) = \{b_0 + b_1\sqrt{3} + (b_2 + b_3\sqrt{3})\sqrt{2} \mid b_i \in \mathbb{Q}\}$$

the defining expression can be foiled out and simplified into $b_0 + b_1\sqrt{3} + b_2\sqrt{2} + b_3\sqrt{6}$. This is not the same as $\mathbb{Q}(\sqrt{6})$ it is denoted $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

3.2 Dimension of an FFE

So did you notice how all of these finite field extensions can be expressed as the weighted sum of elements of $\mathbb{C}$, where the weights of the sum are in F? This is called the dimension of the finite field extension over the field F. If you've taken linear algebra, this definition of dimension is exactly the same as the one there. If you haven't don't worry about it. So how do we compute the $\dim_F(E)$, the dimension of E over F? Well first if $E = F(\alpha)$, then $\dim_F(E)$ is the degree of the smallest degree polynomial over F such that $f(\alpha) = 0$. For $\alpha = \sqrt[n]{c}$ for some $c \in \mathcal{P}$,[2] $\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt[n]{c})) = n$.

The last result I'm going to tell you is that $\dim_{\mathbb{Q}}(\mathbb{Q}(\alpha, \beta))$ if $\beta \notin \mathbb{Q}(\alpha)$ and $\alpha \notin \mathbb{Q}(\beta)$, is $\dim_{\mathbb{Q}}(\mathbb{Q}(\alpha) \dim_{\mathbb{Q}}(\mathbb{Q}(\beta))$. This statement is implied by the Fundamental Theorem of Galois Field.

Formalisms for the Advanced Mathematician

For any algebraists out there who find this, I'm restricting myself to fields that have the property that $\bar{F} = \mathbb{C}$ in this paper. I have no desire to introduce Galois fields, integral domains and their fields of quotients, or anything else that would be needed to give those examples. I certainly was not about to introduce Zorn's Lemma.

[2] $\mathcal{P}$ is the set of prime numbers. This statement can be shown for other numbers too, like the product of distinct primes, and all sorts of other things, but to really go through them all I need more number theory then I want in this paper.

About these Articles

These are all written to answer questions that people ask me which I think deserve a thorough answer. They are not edited. I rarely read them after drafting them. They may contain egregious errors. Hopefully someone finds them useful and hopefully they inspire someone to study more math then they originally planned to.

If you have a question which requires an answer feel free to shoot me an email at `parthnobel@berkeley.edu`. Realize I prefer questions that ask me to explain math I've studied recently in terms of much simpler math, perhaps like this paper skips all of field, ring, group, and number theory but hopefully still catches an interesting topic in algebra, but you can ask for anything. No promises I'll reply. I'm also happy to do any CS or EE stuff I know, but, again, no promises. In any case I write these only when I have free-time, and I normally give up if I have to reference a text more than three times, so don't expect too much.

In any case, to anyone who finds this, I hope you read it and enjoy.