CHMC:
Finite Fields

9/23/17

1 Introduction

This worksheet is an introduction to the fascinating subject of finite fields. Finite fields have many important applications in coding theory and cryptography, although this worksheet won't touch on those. The purpose of this worksheet is to introduce these structures and show how some familiar facts about, say, the rational numbers either fail or take a different face when we consider only finitely many elements.

The second section introduces the notion of a field, as mathematicians understand and think about them, and explores some basic properties of both infinite and finite fields.

The third section explores how to construct finite (and infinite) fields from other fields. The key objects are polynomials, especially polynomials that do not have roots.

2 Finite Fields, definitions and examples

A field is a mathematical structure in which you can add, subtract, and multiply any two numbers, divide by any non-zero number, and the two operations (addition and multiplication) are related by the distributive property.

Let's make this definition more precise. A *field* is a set S, together with two operations addition $+$ and multiplication $\cdot$, such that the following rules are satisfied: for any a, b, c in S, we have

1. Associativity: $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

2. Commutativity: $a + b = b + a$ and $a \cdot b = b \cdot a$;

3. Additive and multiplicative identities: there exist two different elements 0 and 1 in S such that $0 + a = a$ and $1 \cdot a = a$;

4. Additive inverses: there exists an element $-a$ in S such that $a+(-a) = 0$;

5. Multiplicative inverses: if $a \neq 0$, then there exists an element a^{-1} in S such that $a \cdot a^{-1} = 1$;

6. Distributivity of multiplication over addition: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Exercise 2.1 Using just the properties above, show that in any field $\mathbb{F}$ we have $0 \cdot a = 0$ for any a in $\mathbb{F}$. Hint: write $0 \cdot a$ as $(0 + 0) \cdot a$ and distribute.

The two examples we all know and love are the rational numbers $\mathbb{Q} = \{\frac{a}{b} \colon a, b$ are integers, and $b \neq 0\}$ and the real numbers $\mathbb{R}$. Another example of a field is $\mathbb{C}$, the field of complex numbers.

Exercise 2.2 Verify that $\mathbb{Q}$ is in fact a field by checking that it satisfies the properties above.

Exercise 2.3 The integers $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ do not form a field; why?

Exercise 2.4 We write $\mathbb{P} = \{a_n x^n + ...a_1 x + a_0 \colon a_i \in \mathbb{Q}, n = 0, 1, 2, ...\}$ for the space of all polynomials with rational coefficients. Why is $\mathbb{P}$ not a field either?

In this case we have an example of a space which isn't a field, but contains a field as a subset. To see this, note that the 0th degree polynomials are just constants. Since the constants of $\mathbb{P}$ are rational numbers, $\mathbb{P}$ contains the rational numbers, which we know form a field.

It can also happen that a field has a subset that itself is a field. For example, the real numbers $\mathbb{R}$ are a subset of the complex numbers $\mathbb{C}$. Not every subset of a field needs to be a field though.

Exercise 2.5 Consider the set

$$\mathbb{Q}_e = \left\{\frac{a}{b} \colon a, b \text{ are integers, } a \text{ is even, and } b \neq 0\right\}.$$

Verify that this is a subset of $\mathbb{Q}$, and show that $\mathbb{Q}_e$ is not a field. What field property fails for this set?

As you may have guessed, a *finite field* is a field that has only finitely many elements. An example we saw last week was $\mathbb{Z}_2$, which corresponds to arithmetic modulo 2. The addition and multiplication rules are the usual ones for integers, but it's not a priori clear that every non-zero number has a multiplicative inverse. In other words, for every non-zero a in $\mathbb{Z}_2$, is there some b in $\mathbb{Z}_2$ such that $a \cdot b = 1$? Indeed! The only non-zero element in $\mathbb{Z}_2$ is 1, and $1 \cdot 1 = 1$. This shows that $\mathbb{Z}_2$ is in fact a field, and has finitely many terms. Our first example of a finite field!

Exercise 2.6 Let $\mathbb{Z}_3$ be the set $\{0, 1, 2\}$, with the usual addition and multiplication of integers done modulo 3. Show that $\mathbb{Z}_3$ is a field, and hence a finite field.

In general, we let $\mathbb{Z}_n$ be the set $\{0, 1, ..., n\}$, together with the usual operations of addition and multiplication done modulo n, just like "clock arithmetic."

Exercise 2.7 Show that $\mathbb{Z}_4$ is not a field. In other words, show that one of the conditions for being a field is not satisfied by $\mathbb{Z}_4$. Hint: what is the multiplicative inverse of 2?

A useful fact we'll need is a special case of Fermat's little theorem: if a is in $\mathbb{Z}_p$, for p prime, then $a^{p-1} = 1$ in $\mathbb{Z}_p$.

Exercise 2.8 For this exercise, let p be any prime number. If a is in $\mathbb{Z}_p$, what is $-a$? What about a^{-1}? Show that $\mathbb{Z}_p$ is a finite field. Why is it important that p is prime?

Exercise 2.9 In $\mathbb{Z}_5$, what do you notice about the sequence $2, 2^2, 2^3, 2^4, 2^5, 2^6$, etc.? What about $3, 3^2$, etc.? What about in $\mathbb{Z}_7$? Can you make a conjecture about this pattern in general?

The binomial theorem, which is related to Pascal's triangle, can be used to find another interesting fact about powers of elements from a finite field.

Exercise 2.10 Show that $(a + b)^p = a^p + b^p$ in $\mathbb{Z}_p$. Hint: use the Binomial theorem, or look at the coefficients of the terms $a^k b^{p-k}$ for $k = 1, 2, ..., p - 1$. Recall that $p = 0$ in $\mathbb{Z}_p$.

This next two exercises suggest a property about finite fields that may (or may not) be all that obvious.

Exercise 2.11 In $\mathbb{Z}_3$, what is $1 + 2$?

Exercise 2.12 In $\mathbb{Z}_5$, what is $1+2+3+4$?

Exercise 2.13 Show that, in general, in $\mathbb{Z}_p$ the sum of all the terms is 0. Hint: what is the summation formula for integers?

Before we go on to constructing finite fields in general, let's consider some number-theoretic consequences of the spaces $\mathbb{Z}_p$.

Fermat's last theorem, one of the pinnacles of modern number theory, asserts that for any integer $n \geq 3$, there are no non-trivial integer solutions a, b, c to the equation

$$a^n + b^n = c^n.$$

This is clearly false for $n = 2$, since any Pythagorean triple (like $a = 3, b = 4$, and $c = 5$) is a solution. The proof of this theorem (the $n \geq 3$ case) took 300+ years and generations of mathematicians to prove, until Andrew Wiles gave a final complete proof in 1994.

The theorem is a statement about integers though; what happens when we look for solutions from finite fields?

To get us started, let's look at $7^3, 9^3$, and 3^3 in $\mathbb{Z}_{11}$. We have

$$\begin{aligned} 7^3 &= 343 = 11 \cdot 31 + 2 = 2 \text{ in } \mathbb{Z}_{11}, \\ 9^3 &= 729 = 11 \cdot 66 + 3 = 3 \text{ in } \mathbb{Z}_{11}, \\ 3^3 &= 27 = 11 \cdot 2 + 5 = 5 \text{ in } \mathbb{Z}_{11}. \end{aligned}$$

Thus in $\mathbb{Z}_{11}$, we have

$$7^3 + 9^3 = 2 + 3 = 5 = 3^3,$$

so $7^3 + 9^3 = 3^3$, a counterexample to Fermat's last theorem! ...not quite. Fermat's last theorem is stated with regard to integers, not finite fields, and is actually false over finite fields. It's not too hard to find other counterexamples.

Exercise 2.14 Find numbers a, b, c in Z_3, not all 0, such that $a^3 + b^3 = c^3$. Note that there are only 2 choices for each a, b, c.

Exercise 2.15 Show that in $\mathbb{Z}_5$, every element is a cube. In other words, if a is in $\mathbb{Z}_5$ then $a = b^3$ for some b in $\mathbb{Z}_5$. One example is $2^3 = 8 = 3$ in $\mathbb{Z}_5$, so 3 is a cube in $\mathbb{Z}_5$.

Exercise 2.16 In general, if p is a prime show that there always exist solutions a, b, c in $\mathbb{Z}_p$ such that $a^p + b^p = c^p$. Hint: use the binomial theorem.

We won't prove it here, but it turns out that for any integer $n \geq 1$, there exists some prime p such that $a^n + b^n = c^n$ for a, b, c in $\mathbb{Z}_p$, not all 0. Note that this is different from what we proved in the last exercise; we showed that there exist solutions whenever n is prime, but that doesn't cover the case when n is composite.

3 Constructing finite fields with polynomials

In an earlier exercise you showed that $\mathbb{Z}_p$ is a finite field for any prime number p. It turns out that you can have a finite field with p^k elements, where p is a prime number and k is *any* natural number. We'll usually write $\mathbb{F}_{p^k}$ for the finite field of p^k elements. In this section, we'll explore how to construct such fields using polynomials.

To begin, we need to explore roots of polynomials. If $ax^2 + bx + c$ is any polynomial with rational coefficients, we know by the quadratic formula that the roots are given by

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

As long as $b^2 - 4ac \geq 0$, we'll have one or two real roots to this polynomial.

Exercise 3.1 If $b^2 - 4ac < 0$, then our polynomial won't have any real roots; why?

Exercise 3.2 Suppose we have a stick of length 1, and we break it at a point such that the ratio of the smaller piece to the bigger piece is the same as the ratio of the bigger piece to the whole. What is the length of the bigger piece? Hint: if x is the length of the bigger piece, then $1 - x$ is the length of the smaller piece. What do the ratios look like in terms of x?

Exercise 3.3 For which values of b does the polynomial $x^2 + bx + 1$ have real roots? Complex roots?

Now we're going to take a slightly different direction in our explorations, motivated by the polynomial $p(x) = x^2 + 1$. In the last section we explored how certain kinds of modular arithmetic lead to field structures. In the rest of this section, we're going to explore a generalization of this: modular arithmetic with polynomials, and how such an arithmetic leads to field structures from polynomials.

From the last exercise we know that $p(x)$ has no rational (or real) roots, i.e. $p(a) = 0$ is never true for any rational (or real) number a.

Exercise 3.4 Show that, for any other polynomial $q(x)$, if $p(a) \cdot q(a) = 0$ for some real number a, then $q(a) = 0$.

Let $\mathbb{P}_{x^2+1}$ be the space of all polynomials modulo x^2+1. This means that, formally, $x^2 + 1 = 0$ with regard to polynomials. Another way of thinking of this is that, whenever we find an occurrence of $x^2 + 1$ in some polynomial, we can replace it with 0. Let's look at an example.

Consider the polynomial $q(x) = x^3 - 3x^2 + 5x - 7$ in $\mathbb{P}_{x^2+1}$. We first take our condition $x^2 + 1 = 0$ and rewrite it as $x^2 = -1$, in $\mathbb{P}_{x^2+1}$ of course. Let's rewrite $q(x)$ as

$$\begin{aligned} q(x) &= x^3 - 3x^2 + 5x - 7 \\ &= x \cdot (x^2) - 3(x^2) + 5x - 7 \\ &= x \cdot (-1) - 3(-1) + 5x - 7 \\ &= -x + 3 + 5x - 7 \\ &= 4x - 4. \end{aligned}$$

The key observation is that we can pick out terms of the form x^2 in our polynomial and replace them with -1, since we're setting $x^2 + 1 = 0$. In general, any polynomial $q(x)$ in $\mathbb{P}_{x^2+1}$ is of the form $a + bx$, since any squared or higher order terms can be converted into first- or zero-order terms.

It turns out that this set is equivalent to the complex numbers $\mathbb{C}$: if we identify x in $\mathbb{P}_{x^2+1}$ with $i = \sqrt{-1}$ in $\mathbb{C}$, then the two spaces have exactly the same structure!

Exercise 3.5 Verify that multiplication of $(a + bx)(c + dx)$ in $\mathbb{P}_{x^2+1}$ gives the "same" object as $(a + bi)(c + di)$ in $\mathbb{C}$.

Exercise 3.6 Consider the polynomial x^2+x+1. Does this polynomial have any real solutions? What does $x^4 + 3x^3 + 2$ look like in $\mathbb{P}_{x^2+x+1}$? In general, what do polynomials in the space $\mathbb{P}_{x^2+x+1}$ look like?

Before we return to finite fields, let's look at one more interesting field.

Exercise 3.7 Consider the polynomial $x^2 - 2$. Does this polynomial have any solutions in *rational* numbers? Why or why not? What do elements of $\mathbb{P}_{x^2-2}$ look like, where we only allow rational coefficients for the polynomials?

Exercise 3.8 Show that multiplication in the space $\mathbb{P}_{x^2-2}$ is the same as multiplication in the space $\{a+b\sqrt{2} \colon a, b \text{ are rational}\}$, with the usual arithmetic rules. In other words, show that $(a+bx)(c+dx)$ in $\mathbb{P}_{x^2-2}$ gives "the same thing" as $(a+b\sqrt{2})(c+d\sqrt{2})$ in $\{a+b\sqrt{2} \colon a, b \text{ are rational}\}$.

From here on out, our polynomials will only have coefficients in a finite field. We'll call these spaces

$$\mathbb{Z}_p[x] = \{a_n x^n + \cdots a_1 x + a_0 \colon a_0, a_1, ..., a_n \text{ are in } \mathbb{Z}_p\}.$$

Exercise 3.9 Let $p(x) = x^3 + 2x^2 - 2$, and $q(x) = 2x^3 + x - 1$. What is $p(x) + q(x)$ in $\mathbb{Z}_3[x]$? What about in $\mathbb{Z}_5[x]$?

We were able to construct a new field from $\mathbb{R}$, called $\mathbb{C}$, by finding a polynomial with coefficients in $\mathbb{R}$ that didn't have roots in $\mathbb{R}$. Let's do the same for $\mathbb{Z}_p[x]$.

Exercise 3.10 Does the polynomial $p(x) = x^2 + x + 1$ have roots in $\mathbb{Z}_2$? Why or why not? What about in $\mathbb{Z}_3$?

In the last exercise you (hopefully) showed that $x^2 + x + 1$ has no roots in $\mathbb{Z}_2$, so we can consider the space $\mathbb{Z}_2[x]_{x^2+x+1}$.

Exercise 3.11 Remind yourself of the definition of $\mathbb{Z}_2[x]_{x^2+x+1}$. If $a_n x^n + \cdots a_1 x + a_0$ is a polynomial in $\mathbb{Z}_2[x]_{x^2+x+1}$, what is the largest integer n can be?

Exercise 3.12 What does the polynomial x^2 look like in $\mathbb{Z}_2[x]_{x^2+x+1}$?

Exercise 3.13 What does the polynomial $x^5+x^4+x^3$ look like in $\mathbb{Z}_2[x]_{x^2+x+1}$?

Exercise 3.14 How many polynomials in total are there in $\mathbb{Z}_2[x]_{x^2+x+1}$?

Exercise 3.15 What is the multiplicative inverse of x^2 in $\mathbb{Z}_2[x]_{x^2+x+1}$? In other words, what polynomial $q(x)$ do we need to multiply with x^2 so that $x^2 \cdot p(x) = 0$ in $\mathbb{Z}_2[x]_{x^2+x+1}$?

Exercise 3.16 What is the multiplicative inverse of x in $\mathbb{Z}_2[x]_{x^2+x+1}$?

While we won't go through all the details here, it turns out that $\mathbb{Z}_2[x]_{x^2+x+1}$ is a field too! Since $\mathbb{Z}_2[x]_{x^2+x+1}$ has 4 elements, we have succesfully constructed a finite field with 2^2 elements.

Exercise 3.17 Find a polynomial $p(x)$ of order 3 that has no roots in $\mathbb{Z}_2$, i.e. $p(x) = a_3x^3 + a_2x^2 + a_1x + a_0$, $p(0) \neq 0$, and $p(1) \neq 0$ in $\mathbb{Z}_2$. How many elements does $\mathbb{Z}_2[x]_{p(x)}$ have?

Exercise 3.18 For the same $p(x)$ you found in the last exercise, compute x, x^2, x^3, x^4, etc. How many terms are there in the sequence until you start to get repeat terms? Does this remind you of an earlier exercise?

In general, if $p(x)$ has no roots in $\mathbb{Z}_p$ and $p(x)$ has order k, then $\mathbb{Z}_p[x]_{p(x)}$ will be a finite field of p^k elements.

Exercise 3.19 Find polynomials of order 2, order 3, and order 4 in $\mathbb{Z}_5[x]$ that have no roots. What do the corresponding finite fields look like? How many elements does each field have?

Exercise 3.20 If p is a prime, and k is a natural number, how do you think you could construct a finite field of p^k elements?