Visual Algebra

Lecture 8.7: Finite fields

Dr. Matthew Macauley

School of Mathematical & Statistical Sciences
Clemson University
South Carolina, USA
http://www.math.clemson.edu/~macaule/

The characteristic of a field

Definition

The characteristic of $\mathbb{F}$, denoted $\textbf{char}\,\mathbb{F}$, is the smallest $n \geq 1$ for which

$$n1 := \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0.$$

If there is no such n, then $\textbf{char}\,\mathbb{F} := 0$.

Proposition

If the characteristic of a field is positive, then it must be prime.

Proof

If $\textbf{char}\,\mathbb{F} = n = ab$, we can write

$$\underbrace{1 + \cdots + 1}_{n} = (\underbrace{1 + \cdots + 1}_{a})(\underbrace{1 + \cdots + 1}_{b}) = 0.$$

Since $\mathbb{F}$ contains no zero divisors, either $a = n$ or $b = n$, hence n is prime. $\square$

Finite fields

We've already seen:

- $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ is a field if p is prime
- every finite integral domain is a field.

But *what do these "other" finite fields look like?*

Let $R = \mathbb{F}_2[x]$. (We can ignore negative signs.)

The polynomial $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$ because it doesn't factor as $f(x) = g(x)h(x)$ of lower-degree terms. (Note that $f(0) = f(1) = 1 \neq 0$.)

Consider the ideal $I = (x^2 + x + 1)$; the multiples of $x^2 + x + 1$.

In R/I, we have the relation $x^2 + x + 1 = 0$, or equivalently,

$$x^2 = -x - 1 = x + 1.$$

The quotient has only 4 elements:

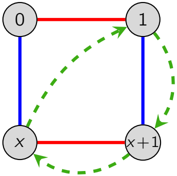
$$0 + I\,, \qquad 1 + I\,, \qquad x + I\,, \qquad (x + 1) + I.$$

As with the quotient group (or ring) $\mathbb{Z}/n\mathbb{Z}$, we usually drop the "I", and just write

$$R/I = \mathbb{F}_2[x]/(x^2 + x + 1) \cong \{0,\ 1,\ x,\ x + 1\}.$$

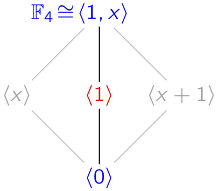
Finite fields

Here is the finite field of order 4: $F_4 \cong R/I = \mathbb{F}_2[x]/(x^2+x+1)$:



$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x



Theorem (wait until Galois theory)

There exists a finite field $\mathbb{F}_q$ of order q, which is unique up to isomorphism, iff $q = p^n$ for some prime p. If $n > 1$, then this field is isomorphic to the quotient ring

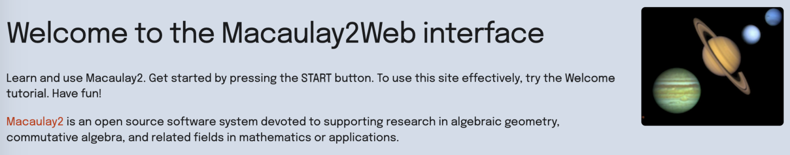
$$\mathbb{F}_p[x]/(f),$$

where f is *any* irreducible polynomial of degree n.

Much of the error correcting techniques in coding theory are built using mathematics over $\mathbb{F}_{2^8} = \mathbb{F}_{256}$. This is what allows DVDs to play despite scratches.

Computations within finite fields

The Macaulay2 software system was written for researchers in algebraic geometry and commutative algebra.



It is freely available online:

https://www.unimelb-macaulay2.cloud.edu.au/

If we want to work in the quotient field $\mathbb{F}_8 \cong \mathbb{F}_2[x]/(x^3+x+1)$, we can type in:

```
R = ZZ/2[x] / ideal(x^3+x+1)
```

In $\mathbb{F}_2[x]$, the product $(x^2+x+1)(x+1) = x^3+2x^2+2x+1$ is just x^3+1.

Since $x^3 \equiv x+1$ modulo (x^3+x+1), this reduces down to x.

Macaulay2 can compute this immediately, just by typing:

```
(x^2+x+1)*(x+1)
```

Finite fields

Here is the finite field of order 8: $\mathbb{F}_8 \cong R/I = \mathbb{F}_2[x]/(x^3+x+1)$:

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

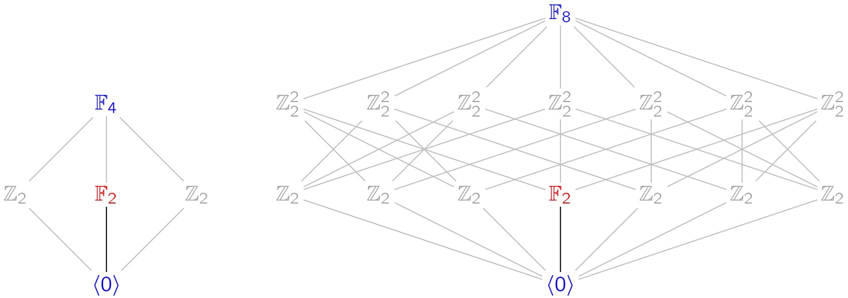
$\times$	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

Notice how $\mathbb{F}_2 = \{0, 1\}$ arises is a subfield, but not $\mathbb{F}_4$. (*Why?*)

Finite fields

The multiplictive groups of these finite fields are $\mathbb{F}_4^\times \cong C_3$ and $\mathbb{F}_8^\times \cong C_7$.

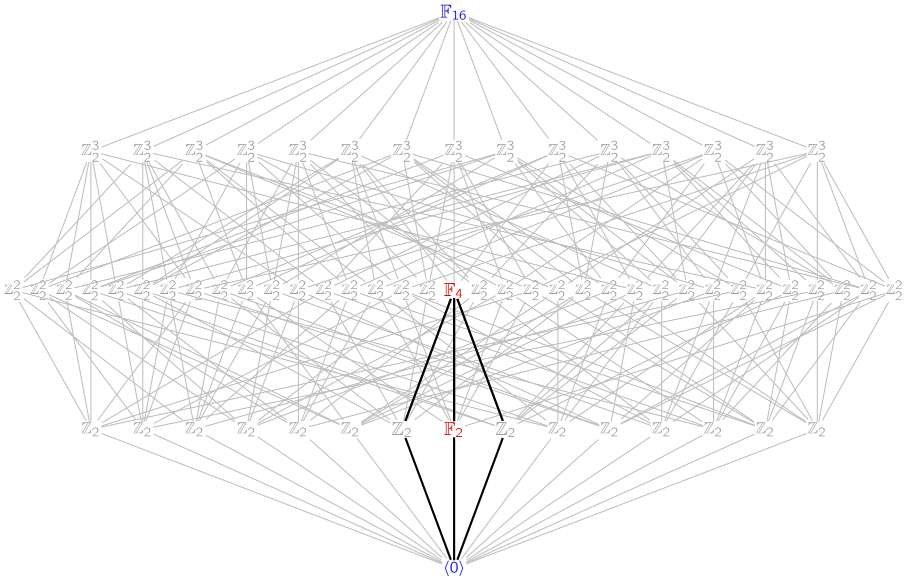
If $\mathbb{F}_8$ had $\mathbb{F}_4$ as a subfield, then it would have three elements of order 3.



Similarly, $\mathbb{F}_{16}$ has 35 $\mathbb{Z}_2^2$-subgroups, but $\mathbb{F}_{16}^\times \cong C_{15}$ has only two elements of order 3.

These, with 0 and 1, comprise its unique $\mathbb{F}_4$-subfield.

The subring lattice of the finite field $\mathbb{F}_{16} \cong \mathbb{Z}_2[x]/(x^4 + x + 1)$



Subfields of finite fields

Proposition

If $\mathbb{F}$ is a finite field, then $|\mathbb{F}| = p^n$ for some prime p and $n \geq 1$.

Proof

If $\mathbf{char}\,\mathbb{F} = p$, then $\mathbb{F}$ contains $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ as a subfield.

Note that $\mathbb{F}$ is an $\mathbb{F}_p$-vector space, so pick a basis, $x_1, \dots, x_n$.

Every $x \in \mathbb{F}$ can be written uniquely as

$$x = a_1 x_1 + \cdots + a_n x_n, \qquad a_i \in \mathbb{F}_p.$$

Counting elements immediately gives $|\mathbb{F}| = p^n$.

Proposition

If $\mathbb{F}_{p^n}$ contains a subfield isomorphic to $\mathbb{F}_{p^m}$, then $m \mid n$.

Proof

Same as above, but $\mathbb{F}_{p^n}$ is an $\mathbb{F}_{p^m}$-vector space. Take a basis $x_1, \dots, x_k$, count elements. $\square$

Finite multiplictive subgroups of a field

Proposition (upcoming)

In a field, a degree-n polynomial can have at most n roots.

Proof (sketch)

The polynomial ring $\mathbb{F}[x]$ has unique factorization. (We'll show this soon.)

If $f(r) = 0$, then factor $f(x) = (x - r)g(x)$, where $\deg g = n - 1$. Apply induction.

Proposition

Every finite subgroup of the multiplictive group $\mathbb{F}^\times$ is cyclic.

Proof

Let $H \leq \mathbb{F}^\times$ have finite order. If it were not cyclic, then $C_{p^n} \times C_{p^m} \leq H$ for $n, m \geq 1$.

Since each factor has a C_p-subgroup, $\mathbb{F}^\times$ has a C_p^2-subgroup.

All p^2 elements in H satisfy $f(x) = x^p - 1$, which is impossible. $\square$