November 25^{th}, 2022

- Course Evaluations are open! (perceptions.uwaterloo.ca)
- Quiz today at 3:30
  - ↳ Eisenstein's Criterion
  - ↳ Factoring modulo p
  - ↳ Minimal polynomials
- Putnam Preparation Session at 5:30, MC 1085
  - ↳ Last prep session
  - ↳ Remember to register for Putnam if you're interested!

For Monday:

- Read Section 7.6
  - ↳ Know the result of 7.6.1
  - ↳ Know and understand the proof of 7.6.2, 7.6.3, 7.6.4
  - ↳ Understand the example
  - ↳ Attempt all end of section exercises

<u>Recap:</u> $\mathbb{F}[x]/(g)$ for an irreducible polynomial $p \in \mathbb{F}[x]$ is a field.
In the case of $\mathbb{Z}_p[x]/(g)$ ($\deg g = d$),

$$|\mathbb{Z}_p[x]/(g)| = p^d$$

<u>Question:</u> Do all finite fields look like this?

<u>Def:</u> The <u>characteristic</u> of a field $\mathbb{F}$ is the smallest positive integer p such that the sum of p "1"s is 0. If this never happens, we say $\mathbb{F}$ has character 0.

$$\underbrace{1+1+\cdots 1}_{p} = 0$$

arbitrary

Theorem: Let $\mathbb{F}$ be a finite field.

1. There is a prime p such that $p \cdot a = \underbrace{a + \cdots + a}_{p \text{ times}} = 0 \quad \forall a \in \mathbb{F}$

2. There is a copy of $\mathbb{Z}_p$ inside $\mathbb{F}$

3. There is an integer d such that $|\mathbb{F}| = p^d$.

Proof: . . .

Note: $\mathbb{F}$ is a vector space over $\mathbb{Z}_p$ of dimension d, and our proof of (3) constructs a basis for it.

$\mathbb{Z}_p[x]/(g)$

$\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$

Algebraic Elements (Or a first step in understanding finite fields)

Recall the definition of an algebraic element. For $\omega \in \mathbb{C}$, we can consider a copy of $\mathbb{Q}$ inside $\mathbb{C}$, and we called ω algebraic iff ω was the root of a polynomial in $\mathbb{Q}[x]$.

In an analogous way

For $\mathbb{F}$ a finite field of cardinality p^d, there exists a copy of $\mathbb{Z}_p$ in $\mathbb{F}$. Also, Fermat's Little Theorem says $a \in \mathbb{F}$ satisfies

$$a^{p^d} - a = 0$$

so a is a root of the polynomial

$$y^{p^d} - y \in \mathbb{Z}_p[y] \subseteq \mathbb{F}[y]$$

Thus there exists a monic polynomial of least degree (thus irreducible) $g(y) \in \mathbb{Z}_p[y]$ for which a is a root:

$$g(a) = 0$$

$g(y)$ is the <u>minimal polynomial</u> of a in $\mathbb{Z}_p[y]$, and we say a is <u>algebraic over $\mathbb{Z}_p$</u>.

In the same way as before, the following proposition holds.

Proposition: If $a \in \mathbb{F}$, a field of cardinality p^d, then a has a minimal polynomial $g \in \mathbb{Z}_p[y]$. The polynomial g is a factor of $y^{p^d} - y \in \mathbb{Z}[y]$

More generally, if $r(y) \in \mathbb{Z}_p[y]$ and $r(a) = 0$, then g divides r.

Proof: . . .

Now let $a \in \mathbb{F}$ as before, and consider

$$\mathbb{Z}_p[a] := \{ p(a) : p(y) \in \mathbb{Z}_p[y] \} \subseteq \mathbb{F}$$

Def: $a \in \mathbb{F}$ is a generator of $\mathbb{F}$ iff $\mathbb{Z}_p[a] = \mathbb{F}$

Ex: Consider $\mathbb{F} = \mathbb{Z}_p[x]/(g)$. $[x]$ is a generator of $\mathbb{F}$

$$\wr \quad [p(x)] \longrightarrow p([x]) \in \mathbb{Z}_p[[x]]$$

Ex: (Non-example)

For $\mathbb{F}$ as before, $[a]$, for $a \in \mathbb{Z}_p$ is not a generator.

For $\mathbb{F} = \mathbb{Z}_5[x]/(x^4+2)$ ✓ $[x^2]$ is not a generator

$$[x] \notin \mathbb{Z}_5[[x^2]]$$

A question pops up given this definition:

When is $\mathbb{Z}_p[a] = \mathbb{F}$?

More generally:

What does $\mathbb{Z}_p[a]$ look like?

Theorem: Let $a \in \mathbb{F}$, a field with cardinality p^d, and $g \in \mathbb{Z}_p[y]$

be its minimal polynomial. Then

$$\mathbb{Z}_p[y]/(g) \cong \mathbb{Z}_p[a]$$

Proof: . . .

Note: $\mathbb{Z}_p[a]$ is a field!

Corollary: Let $a \in \mathbb{F}$, a finite field with cardinality p^d, having minimal polynomial $g \in \mathbb{Z}_p[y]$. Then

$$\mathbb{Z}_p[a] = \mathbb{F} \quad \underline{\text{iff}} \quad \deg g = d$$

Proof: . . .

Remark: This tells us that the minimal polynomial of $a \in \mathbb{F}$ has degree at most d, where $|\mathbb{F}| = p^d$.

Ex: $\mathbb{F} = \mathbb{Z}_2[x]/(x^3+x+1)$, $a = [x^2+x]$.
Find the minimal polynomial of a in $\mathbb{Z}_2[x]$.

$$a = [x^2+x]$$
$$a^2 = [x]$$
$$a^3 = [x^2+x+1]$$

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

TABLE 7.2.1. Multiplication table for $\mathbb{F}_8$

$$c_3 a^3 + c_2 a^2 + c_1 a + c_0 = 0$$

$$c_3 a^3 = c_3 x^2 + c_3 x + c_3$$
$$c_2 a^2 = c_2 x$$
$$c_1 a = c_1 x^2 + c_1 x$$
$$c_0 = c_0$$

$$\left.\begin{aligned} c_3 + c_1 &= 0 \\ c_3 + c_2 + c_1 &= 0 \\ c_3 + c_0 &= 0 \end{aligned}\right\} \Rightarrow \begin{aligned} c_1 &= c_3 = c_0 \\ c_0 &= c_3 \\ c_2 &= 0 \end{aligned}$$

$a^3 + a + 1 = 0$

so a is a root of $y^3 + y + 1 \in \mathbb{Z}_2[y]$

$$\begin{array}{r l}
 & y^2 + ay + (a^2+1) \\
\cline{2-2}
y + a \,\big) & y^3 + 0y^2 + y + 1 \\
 & \underline{y^3 + ay^2} \\
 & \quad ay^2 + y \\
 & \quad \underline{ay^2 + a^2 y} \\
 & \qquad (a^2+1)y + 1 \\
 & \qquad \underline{(a^2+1)y + a^3 + a} \\
 & \qquad\qquad a^3 + a + 1 = 0
\end{array}$$

Aside: This correspondence gives us a nice way to look at $\mathbb{F}[x]/(g)$.

We now know that $\mathbb{F}[x]/(g) \cong \mathbb{F}\big[[x]\big]$ ⟵ adjoin $[x]$

But we also know that $[x]$ is a root of the irreducible polynomial $g(x)$.

So we can think of $\mathbb{F}\big[[x]\big]$ as $F[\alpha]$ where α is a root of $g(x) \in \mathbb{F}[x]$.

Ex: $\mathbb{R}[x]/(x^2+1) \cong \mathbb{R}[i] \cong \mathbb{C}$

$\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}[\sqrt{2}]$

Fact: All finite fields have a generator. Thus all finite fields look like $\mathbb{Z}_p[a]$, and are therefore isomorphic to

$$\mathbb{Z}_p[y]/(g)$$

for some irreducible polynomial $g \in \mathbb{Z}_p[y]$.

Theorem: Let $\mathbb{F}$ be a finite field.

1. There is a prime p such that $p \cdot a = \underbrace{a + \cdots + a}_{p \text{ times}} = 0 \quad \forall a \in \mathbb{F}$
2. There is a copy of $\mathbb{Z}_p$ inside $\mathbb{F}$
3. There is an integer d such that $|\mathbb{F}| = p^d$.

Proof: Consider

$$1,\ 1+1,\ \ldots,\ \underbrace{1 + \cdots + 1}_{|\mathbb{F}|+1}$$

There must be a repeated element in this list, say

$$\underbrace{1 + \cdots + 1}_{m},\quad \underbrace{1 + \cdots + 1}_{n}$$

WLOG $m > n$

$$\underbrace{1 + \cdots + 1}_{m} = \underbrace{1 + \cdots + 1}_{n}$$

$$\Longrightarrow \underbrace{1 + \cdots + 1}_{m} - (\underbrace{1 + \cdots + 1}_{n}) = 0$$

$$\Longrightarrow \underbrace{1 + \cdots + 1}_{m-n} = 0$$

least

Call $p = m - n$. To show that p is prime, suppose not.

Then $p = b \cdot c$ for some $b, c \neq 1$. So that

$$(\underbrace{1 + \cdots + 1}_{b})(\underbrace{1 + \cdots + 1}_{c})$$

$$= 1 + \cdots + 1 = 0$$

$$\underbrace{\qquad\qquad}_{b \cdot c = p}$$

$\Rightarrow \mathbb{F}$ has zero-divisors ↯

Consider $S = \{0, 1, 1+1, \ldots, \underbrace{1 + \cdots + 1}_{p-1}\}$

Let $a \in \mathbb{F}$. Note

$$p \cdot a = \underbrace{a + \cdots + a}_{p}$$

$$= a(\underbrace{1 + \cdots + 1}_{p})$$

$$= a \cdot 0 = 0$$

Proposition: If $a \in \mathbb{F}$, a field of cardinality p^d, then a has a minimal polynomial $g \in \mathbb{Z}_p[y]$. The polynomial g is a factor of $y^{p^d} - y$

More generally, if $r(y) \in \mathbb{Z}_p[y]$ and $r(a) = 0$, then g divides r.

Proof: Existence —— by the well-ordering principle.

Suppose $r(y) \in \mathbb{Z}_p[y]$ and $r(a) = 0$. Then by the division algorithm,

$$r(y) = g(y) \cdot b(y) + c(y)$$

for $\deg c < \deg g$ or $c = 0$.

done

In this case evaluating at $y = a$ gives us:

$$\overset{0}{\cancel{r(a)}} = \overset{0}{\cancel{g(a)}} \cdot b(a) + c(a)$$

$\Rightarrow c(a) = 0$ ↯

g_1, g_2

$g_1 | g_2, \quad g_2 | g_1$

$g_2 = u g_1$

$\Rightarrow g_2 = g_1$

Theorem: Let $a \in \mathbb{F}$, a field with cardinality p^d, and $g \in \mathbb{Z}_p[y]$ be its minimal polynomial. Then

$$\mathbb{Z}_p[y]/(g) \cong \mathbb{Z}_p[a]$$

Proof:

1. Homomorphism
2. Surjective ✓
3. Injective

$$\mathbb{Z}_p[a] = \{p(a) : p(y) \in \mathbb{Z}_p[y]\}$$

Consider $\varphi : \mathbb{Z}_p[y] \longrightarrow \mathbb{Z}_p[a]$

$$p(y) \longmapsto p(a)$$

$$\varphi(f+g) = (f+g)(a) = f(a) + g(a)$$
$$= \varphi(f) + \varphi(g)$$

$$\varphi(f \cdot g) = (fg)(a) = f(a)\, g(a)$$
$$= \varphi(f)\, \varphi(g)$$

$$\varphi(0) = 0$$

$$\varphi(g) = g(a) = 0$$

$(g r)(a) = 0$ at the same time, if $g(a) = 0$, we know that $g \mid g \Rightarrow g = g \cdot r$

Consider $\tilde{\varphi} : \mathbb{Z}_p[y]/(g) \longrightarrow \mathbb{Z}_p[a]$

$$\tilde{\varphi}([f]) = \varphi(f) = f(a)$$

Well defined? If $f \equiv g \pmod{g}$

$\Rightarrow g = f + g \cdot r$

$\Rightarrow g(a) = f(a) + \cancel{g(a)}^{0} \cdot r(a)$

$\Rightarrow g(a) = f(a)$ ✓

Surjective? Yes, because φ is

Homomorphism? Yes, because φ is

$$\tilde{\varphi}([f]+[g]) = \tilde{\varphi}([f+g])$$
$$= \varphi(f+g)$$
$$= \varphi(f) + \varphi(g)$$
$$= \tilde{\varphi}([f]) + \tilde{\varphi}([g])$$

Suppose $\tilde{\varphi}([f]) = \tilde{\varphi}([g])$

$\Rightarrow f(a) = g(a)$

$\Rightarrow (f-g)(a) = 0$

$\Rightarrow g \mid f-g$

$\Rightarrow f \equiv g \pmod{g}$

$\Rightarrow [f] = [g]$

Corollary: Let $a \in \mathbb{F}$, a finite field with cardinality p^d, having minimal polynomial $g \in \mathbb{Z}_p[y]$. Then

$$\mathbb{Z}_p[a] = \mathbb{F} \quad \underline{\text{iff}} \quad \deg g = d$$

Proof:

$$\underbrace{\mathbb{F}}_{p^d} = \mathbb{Z}_p[a] \cong \underbrace{\mathbb{Z}_p[y]/(g)}_{p^{\deg g}}$$

$$\Rightarrow d = \deg g$$

If
$$\underbrace{\mathbb{Z}_p[a]}_{p^{\deg g}} \subsetneq \underbrace{\mathbb{F}}_{p^d}$$

$$p^{\deg g} < p^d$$

$$\Rightarrow \deg g < d$$

$$\Rightarrow \deg g \neq d$$