Math 127, Mon Apr 18

- Reading for today: 7.6, 8.1–8.2.
- Reading for Wed Apr 20: 8.3–8.4
- PS08 due tomorrow(-ish); PS09 outline due Thu(-ish).

Order and characteristic

7.6 Finite fields

Definition

The **order** of a field F is defined to be the number of elements in F; i.e., **finite field** is a field of finite order.

Definition

R a finite ring, $n \cdot 1 = \underbrace{1 + \cdots + 1}_{n \text{ times}}$, $\text{char}(R)$ is the smallest positive integer n such that $n \cdot 1 = 0$.

Theorem

Let F be a finite field. Then $\text{char}(F) = p$ for some prime p.

Point: If F is a finite field, then F has a copy of some $\mathbf{Z}/(p) = \mathbf{F}_p$ sitting inside it. We can think of this copy of $\mathbf{F}_p$ as a base on which F is constructed.

Even more vocabulary

Definition

Let F be a field. We use $F^\times$ to denote the set of all nonzero elements of F, and call $F^\times$ the **multiplicative group** of F.

Definition

new term

Let $F^\times$ be the multiplicative group of the field F, and suppose $\alpha \in F^\times$. We define the **cyclic subgroup generated by** α to be $\langle \alpha \rangle = \{\alpha^n \mid n \in \mathbf{Z}\}$, i.e., the set of all powers of α, positive, negative, or zero.

Definition

To say that $F^\times$ is **cyclic** means that there exists some $\alpha \in F^\times$ such that $F^\times = \langle \alpha \rangle$, i.e., every element of $F^\times$ is some power of α. If $F^\times = \langle \alpha \rangle$, we say that α is a **primitive** element of F.

Theorem

If F is a finite field, then its multiplicative group $F^\times$ is cyclic. In other words, every finite field contains a primitve element.

Note: If you could write a program that, given p, would produce a primitive element of Z/(p), you could probably get:

* Tenured professorship at a major university
* Lifetime employment at National Security Agency

So this abstract object of a primitive element of F is much better understood in theory than examples.

Factoid: Of 2, 3, and 5, at least two are primitive for infinitely many Z/(p) -- but we don't know which. (prob all)

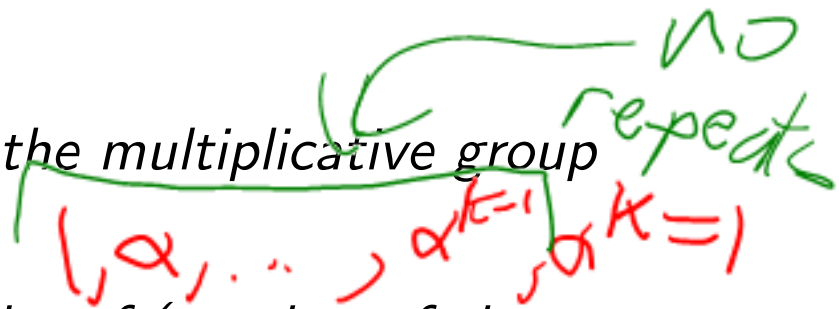
Alas, a different definition of order

Definition

Let $F^\times$ be the multiplicative group of the field F, and suppose $\alpha \in F^\times$. If $\alpha^n = 1$ for some positive integer n, we define the **order** of α to be the *smallest* possible n such that $\alpha^n = 1$. Otherwise, if $\alpha^n \neq 1$ for all positive integers n, we say that α has **infinite order**.

Theorem

Let F be a field of order n, let $F^\times$ be the multiplicative group of F, and suppose $\alpha \in F^\times$. Then:



1. *The order of α is equal to the order of (number of elements in) $\langle\alpha\rangle$. It follows that α is primitive if and only if the order of α is equal to $n-1$, the order of $F^\times$.*
2. *If k is the order of α, then the order of α^m is $\dfrac{k}{\gcd(k,m)}$.*
3. *If k is the order of α, then k divides $n-1$ (the order of $F^\times$).*

Example: Some orders of elements in $\mathbf{F}_{17}$

$|\mathbb{F}_{17}^{\times}| = 16$

$\mathbb{F}_{17}^{\times}$ non-0

Ord(α) div. 16: 1, 2, 4, 8, 16

$\alpha = 2$

$\alpha^1 = 2$

$\alpha^2 = 4$

$\alpha^3 = 8$

$\alpha^4 = 16 = -1$

$\alpha^5 = 32 = 15 = -2$

$\alpha^6 = -4 = 13$

$\alpha^7 = -8 = 9$

$\alpha^8 = -16 = 1$

order 8

α^2

ord(α) $\neq 16$, so not prim.

$\alpha = 3$

$\alpha^1 = 3, \alpha^2 = 9, \alpha^3 = 10, \alpha^4 = 13$

$\alpha^5 = 5, \alpha^6 = 15, \alpha^7 = 11, \alpha^8 = -1$

$\Rightarrow \alpha^1, \alpha^2, \alpha^4, \alpha^8 \neq 1$, so $\text{ord}(\alpha) \neq 1, 2, 4, 8$.

We know $\text{ord}(\alpha) \mid 16$ (3)

$\Rightarrow \text{ord}(\alpha) = 1, 2, 4, 8, \text{or } 16$.

not 1, 2, 4, 8

So $\text{ord}(\alpha) = 16 \Rightarrow$ 3 prim (1)

$\alpha^2 = 9$ $\quad \text{ord}(9) = \frac{16}{\gcd(16,2)} = 8$

$\alpha^3 = 10$ $\quad \text{ord}(10) = \frac{16}{\gcd(16,3)} = 16$

So 10 is prim.

$\alpha^4 = 13$ $\quad ord(13) = \frac{16}{gcd(16,4)} = 4$

α | in $\mathbb{Z}/(17)$

The magic polynomial

Corollary

Let F be a field of order q. Then every α is a root of the polynomial $x^q - x \in F[x]$, and consequently,

$$x^q - x = \prod_{\alpha \in F} (x - \alpha).$$

(mod

Ex. $x(x-1)(x-2)\cdots(x-16) = x^{17} - x$ 17)

Proof:

For $\alpha \in F^\times$, $\mathrm{ord}(\alpha) \mid q-1$.

So $\alpha^{q-1} = 1 \Rightarrow \alpha$ is root of $x^{q-1}-1$

So elts of $F^\times$ are $q-1$ roots of $x^{q-1}-1$

$\Rightarrow$ Each $x-\alpha \mid x^{q-1}-1$

$\Rightarrow x^{q-1}-1$ factors as $\prod_{\alpha \in F^\times}(x-\alpha)$

$(f(\alpha)=0 \Leftrightarrow (x-\alpha) \text{ div } f(x))$

$\Rightarrow x^{q-1}-1 = \prod_{\alpha \in F^\times}(x-\alpha)$

$\Rightarrow x^q - x = x\prod_{\alpha \in F^\times}(x-\alpha) = \prod_{\alpha \in F}(x-\alpha)$

Deeper facts about finite fields

Theorem

Let F be a finite field of characteristic p. Then F is isomorphic to $\mathbf{F}_p[x]/(m(x))$ for some irreducible polynomial $m(x) \in \mathbf{F}_p[x]$.

So the order of a finite field must be p^e for some prime p and some positive integer e. More surprisingly:

Theorem

Let p be a prime, and let e be a positive integer.

1. *There exists at least one field of order p^e.*
2. *If F and K are both finite fields of order p^e, then F and K are isomorphic.*

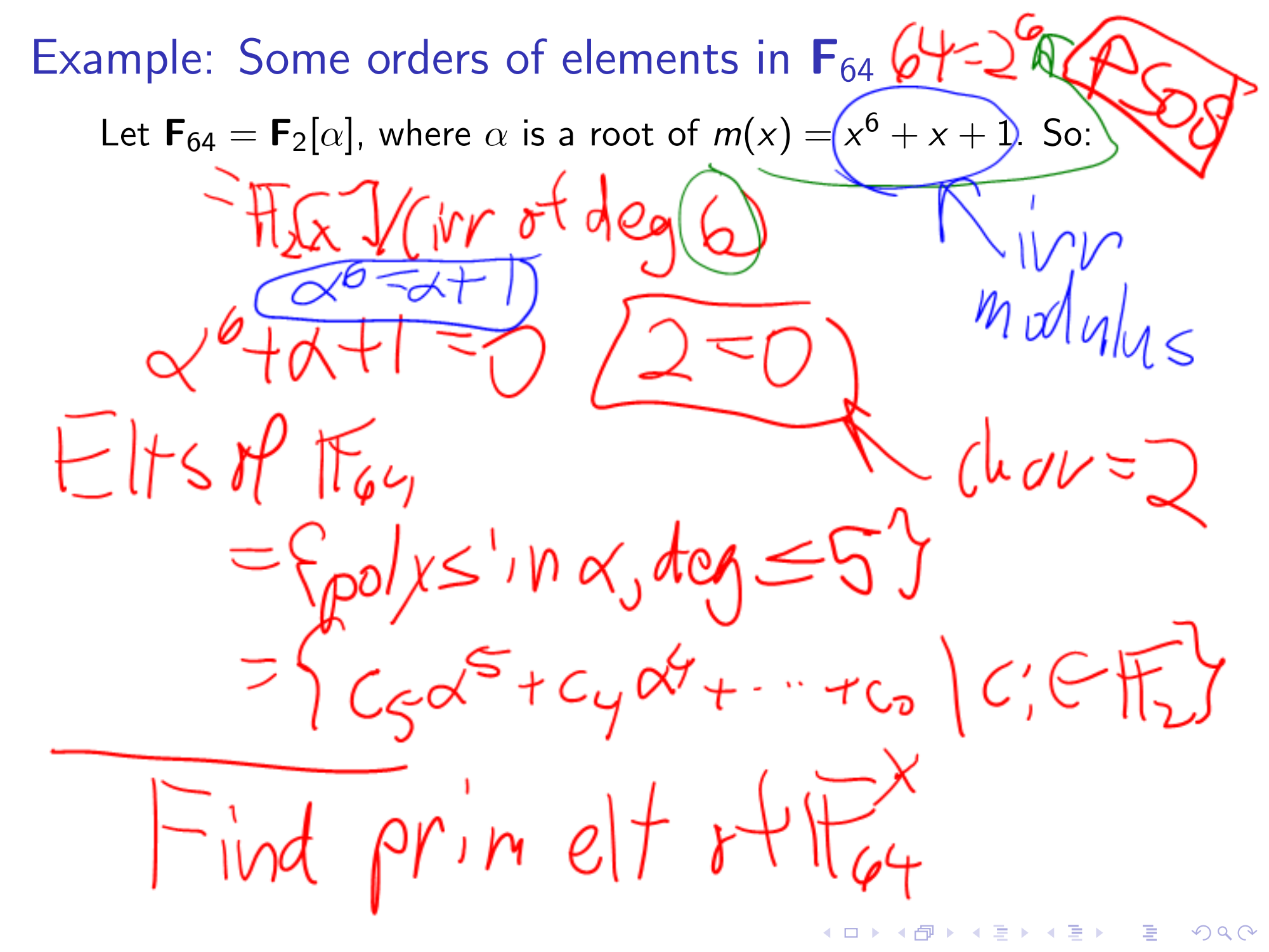
I.e., for any prime p and some positive integer e, there is only one field of order $q = p^e$.

Five Facts for Finite Fields

1. **Prime power:** The characteristic of a finite field must be a prime p, and its order must be $q = p^e$ for some $e \geq 1$.
2. **Orders of elements:** The multiplicative group of a finite field is cyclic; i.e., if F has q elements, $F^\times$ must contain at least one element of order $q - 1$. Moreover, every element of $F^\times$ must have order dividing $q - 1$.
3. **Magic polynomial:** If F is a field of order q, then every $\alpha \in F$ is a root of $x^q - x$, or in other words, $\alpha^q = \alpha$ for every $\alpha \in F$. Consequently, $x^q - x$ factors as the product of all $(x - \beta)$, where β runs over all elements of F.
4. **Construction:** Every finite field of characteristic p is isomorphic to $\mathbf{F}_p[x]/(m(x))$ for some irreducible polynomial $m(x)$.
5. **Classification:** For any prime p and $q = p^e$ $(e \geq 1)$, there exists a field $\mathbf{F}_q$ of order q that is unique up to isomorphism.

Example: Some orders of elements in $\mathbf{F}_{64}$

Let $\mathbf{F}_{64} = \mathbf{F}_2[\alpha]$, where α is a root of $m(x) = x^6 + x + 1$. So:



For $\beta \in \mathbb{F}_{64}^{\times}$, $\operatorname{ord}(\beta)$ div 63

1, 3, 9, 7, 21, 63

So if $\operatorname{ord}(\alpha) \neq 1, 3, 7, 9, 21$

$\operatorname{ord}(\alpha) = 63$

Is α prim?

$\alpha^6 = \alpha + 1$

$\alpha^1 = \alpha$

α^2

α^3

α^4

α^5

$\alpha^6 = \alpha + 1$

$\alpha^7 = \alpha^2 + \alpha$

$\alpha^5 + \alpha^2$

$\alpha^4 + \alpha^3$

$\alpha^{10} = \alpha^5 + \alpha^4$

$\alpha^{11} = \alpha^6 + \alpha^5$

$= \alpha^5 + \alpha + 1$

$\alpha^{12} = \alpha^6 + \alpha^2 + \alpha$

$= \alpha + 1 + \alpha^2 + \alpha$

$= \alpha^2 + 1$

$\alpha^{15}, \ldots \alpha^{21} \neq 1$ so $\mathrm{ord}(\alpha) \geq 21$

$\Rightarrow \mathrm{ord}(\alpha) = 63 \Rightarrow \alpha$ prim.

Building better codes (review)

- An $[n, k, d]$ code $\mathcal{C}$ is a binary linear code of **length** n, **dimension** k, and **minimum distance** d. In other words, $\mathcal{C}$ is a subspace of $\mathbf{F}_2^n$, $\dim \mathcal{C} = k$ as a subspace of $\mathbf{F}_2^n$, and the smallest nubmer of 1s appearing in a nonzero codeword of $\mathcal{C}$ is d.
- We would like k/n to be as large as possible, because k/n represents the portion of each transmitted message that contains useful data.
- Also, since the maximum number of errors that can be corrected in a single transmitted codeword is $\left\lfloor \frac{d-1}{2} \right\rfloor$, we would like d to be as large as possible.

It follows that to create a good code, we need to find $[n, k, d]$ codes where both k and d are as large as possible, given n.

Example: Longer Hamming codes

For an integer $r \geq 2$, let $n = 2^r - 1$, and let H_n be the $k \times n$ matrix whose ith column $(1 \leq i \leq n)$ is the binary digits of the integer i, e.g., for $r = 3$ and $r = 4$:

$$H_7 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

$$H_{15} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

The **Hamming n-code** $\mathcal{H}_n$ has parity check matrix H_n.

Theorem

For an integer $r \geq 2$ and $n = 2^r - 1$, the Hamming n-code $\mathcal{H}_n$ is an $[n, n - r, 3]$ code (so we can correct 1 error per transmission).

As $r \to \infty$, transmit almost 100% data, but can't correct much.

Cyclic codes

Definition

Let $\mathcal{C}$ be a binary linear code of length n. To say that $\mathcal{C}$ is **cyclic** means that it is closed under cyclic permutation of coordinates.

That is, to say that $\mathcal{C}$ is cyclic means that if $\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{n-1} \end{bmatrix}$ is in $\mathcal{C}$, then

so are $\begin{bmatrix} c_{n-1} \\ c_0 \\ c_1 \\ \vdots \\ c_{n-2} \end{bmatrix}$, $\begin{bmatrix} c_{n-2} \\ c_{n-1} \\ c_0 \\ \vdots \\ c_{n-3} \end{bmatrix}$, and so on.

Polynomial notation: What is $xc(x)$?

The **polynomial notation** for vectors in $\mathbf{F}_2^n$ represents $\begin{bmatrix} c_0 \\ \vdots \\ c_{n-1} \end{bmatrix}$ as

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$$

in the ring $R = \mathbf{F}_2[x]/(x^n - 1)$ (i.e., setting $x^n = 1$).

If $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$, then in $\mathbf{F}_2[x]/(x^n - 1)$, we have:

$xc(x) =$

Cyclic codes are ideals

Theorem

Let $\mathcal{C}$ be a binary linear code of length n. In polynomial notation, $\mathcal{C}$ is cyclic if and only if it is an ideal of the ring $\mathbf{F}_2[x]/(x^n - 1)$.

Proof: PS09.

The generator polynomial of a cyclic code

Theorem

Fix a positive integer n, and let $\mathcal{C}$ be a nonzero cyclic code of length n, i.e., let $\mathcal{C}$ be a nonzero ideal of $\overline{R} = \mathbf{F}_2[x]/(x^n - 1)$. Then $\mathcal{C}$ is principal, or in other words, $\mathcal{C} = (g(x))$ for some $g(x) \in \mathbf{F}_2[x]$. Moreover, we can choose $g(x)$ so that $g(x)$ divides $x^n - 1$.

Definition

Let $\mathcal{C}$ be a cyclic code of length n over $\mathbf{F}_q$. We define the **generator polynomial** of $\mathcal{C}$ to be the minimal polynomial $g(x)$ of $\mathcal{C}$.

Next time

Theorem

Let $\mathcal{C}$ be a cyclic code of length n generated by the divisor $g(x) \in \mathbf{F}_2[x]$ of $x^n - 1$. If $\deg g(x) = r$, then the set

$$\mathcal{B} = \left\{ g(x), xg(x), \ldots, x^{(n-1)-r} g(x) \right\}$$

is a basis for $\mathcal{C}$. Consequently, the dimension of $\mathcal{C}$ is $k = n - r$.