Math 127, Wed Apr 14

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: 8.1–8.2 (**reload book**). Reading for Mon: 8.3.
- PS08 outline due tonight, full version due Mon.
- Problem session Fri Apr 16, 10am–noon.

$\mathbb{R}$) $(a,b)=\{ra+sb \mid r,s\in\mathbb{R}\}$

a, b fixed in $\mathbb{R}$

$\mathbb{Z}$) $(4,7)=\{7r+4s \mid r,s\in\mathbb{Z}\}$

Like: In F^n:

$\text{span}\{\underline{v},\underline{w}\}=\{r\underline{v}+s\underline{w} \mid r,s\in F\}$

These two constructions resemvble each other because both span{v,w} and (a,b) (ideal generated by a and b) are special cases of a more general concept.

Symmetries of the roots of a polynomial, ver. 2

The point of studying automorphisms:

phi *fixes* the coefficients of f(x)

Theorem

Let R be a ring, let $\varphi : R \to R$ be an automorphism of R, and let

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

be a polynomial with coefficients in R such that $\varphi(a_i) = a_i$ for $0 \leq i \leq n$. For $\alpha \in R$, if $f(\alpha) = 0$, then $f(\varphi(\alpha)) = 0$.

Special case/the point: Let $f(x) \in \mathbf{R}[x]$ be a polynomial with *real* coefficients. If $a + bi$ is a *complex* root of $f(x)$, then because the automorphism of complex conjugation leaves f unchanged ("invariant"), $a - bi$ is also a root of $f(x)$. (In other words, nonreal roots of real polynomials come in conjugate pairs.)

See: Algebra II, differential equations....

Order and characteristic

1 added to itself n times, which you can think of as the integer n inside the ring R

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

Let R be a ring. To say that R has characteristic $n > 0$ means that n is the smallest positive integer such that $n \cdot 1 = 0$.

Theorem

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

So every finite field contains a copy of F_p for some prime p.

If you study groups in abstract algebra (Math 128A), then char(R) is exactly the additive order of 1.

More vocabulary

Definition

"F times"

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

Last time: <a> for F_{17}

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.

Q: Is there an easy way to find primitive elements in a finite field, or do we just have to guess a bunch?

A: No human being knows. (!!!!)

If you could find an answer to that, you would earn yourself a PhD, and depending on how good your answer is, you could become (math) famous.

Conjecture (50-60 years old): 2 is primitive in F_p "unless there's an obvious reason it isn't" (e.g., if p-1 is a power of 2).

Another 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 $F^\times$).*

$\underline{\text{Ex}}$. $F = \mathbb{F}_{17}$, $|\mathbb{F}_{17}^{\times}| = 16$

So the (multiplicative) order of any element is 1, 2, 4, 8, or 16.

$3^1 = 3$, $3^2 = 9$, $3^4 = 13 = -4$, $3^8 = 16 = -1$

So the order of 3 is neither 1, 2, 4, or 8, so it must be 16, and 3 is primitive.

n	1	2	3	4	5	6	7	
3^n	3	9	10	$-4 = 13$	5	$15 = -2$	$-6 = 11$	$\ldots$

By Thm part (1), we will eventually hit all nonzero elements of F_{17} as powers of 3.

$\mathrm{ord}_{pr}(3) = 16$

$$\mathrm{order}(3^m) = \frac{16}{\gcd(m, 16)}$$

$m=2$ $\quad \mathrm{order}(3^2) = \frac{16}{2} = 8 = \mathrm{order}(9)$

$m=3$ $\quad \mathrm{order}(3^3) = \frac{16}{1} = 16$

So 10 also prim mod 17.

$m=6$ $\quad \mathrm{order}(3^6) = \frac{16}{\gcd(6, 16)} = \frac{16}{2} = 8$

So $\mathrm{order}(-2) = 8$.

The magic polynomial

Corollary

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

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

Proof:

Because order(alpha) divides q-1, alpha^{q-1} = 1 for any nonzero alpha in F.

So α is a root of $x^{q-1} - 1$.

$x^q - x = x(x^{q-1} - 1)$ has those zeros and also 0.

We also know that a is a root of f(x) exactly when (x-a) divides f(x).

So $(x-\alpha)$ div $x^q - x$ for $\alpha \in F$

But F has q elts, and $x^q - x$ div by $\prod_{\alpha \in F}(x-\alpha)$, a poly deg q.

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

Ex Mod 17

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

Deeper facts about finite fields

$\boxed{p=2}$

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:

" deg m

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 $q = p^e$.

$$\underline{\text{Ex}}\ \text{Over } \mathbb{F}_2,\ \left.\begin{aligned} &x^3+x^2+1 \\ \text{and } &x^3+x+1 \end{aligned}\right\} \text{both irred}$$

So both

$\mathbb{F}_2[x]/(x^3+x^2+1)$, $\mathbb{F}_2[x]/(x^3+x+1)$

are both fields order 8

Thm $\Rightarrow$ they are isom

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: One approach to the field of order 8~~

~~Construction, magic polynomial, orders of elements:~~

See 7.7.

(Worked exs.)

Building better codes (review) of Ch. 6

- 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 $\left\lfloor \dfrac{d-1}{2} \right\rfloor$, 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 $r = 4$:

Q: Can we make longer codes like this that still transmit lots of data, but correct more errors?

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

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

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

So code is nullspace of 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 $k = n - r$.