Math 127, Mon May 17

- 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.
- Final exam, **Wed May 19**. Cumulative through Ch. 10. & PS10
  7:15 am
- PS11 **CANCELLED**.
- Revisions available for PS01–07 by Wed and for as many as possible of PS08–10 before end of semester.

Last day: Wed May 26

Ch. 2: The Euclidean Algorithm

Defns and ideas:
What does it mean for integer d to divide integer a?
(same for polynomial d(x) to divide polynomial a(x))

gcd(a,b) (a,b integers; later a(x), b(x) polynomials)

Solve ax + by = gcd(a,b) for integers x,y
Later: Solve a(x)f(x) + b(x)g(x) = gcd(a(x),b(x)) for polynomials f,g

Ch. 3: Polynomials and the Polynomial Euclidean Algorithm

3.1 The integers mod m

3.2 Modular linear equations and fields

3.3 Polynomials with coefficients in a ring

3.4 Polynomial division with remainder

3.5 The Euclidean algorithm for polynomials

3.6 Bezout's identity for polynomials

Defns and ideas:

Z/(m), both intuitive version from Ch. 3 and formal version in Ch. 7
(Compare: F[x]/(m(x)) in Ch. 7)

R[x], F[x]

Remember: Integers are like polynomials, except size of an integer replaced with the degree of a polynomial.

Euclidean Algorithm (generalized)

$\sigma(r)$ = size of r, e.g., absolute value or degree.

Find gcd (r_{-1}, r_0)

$$r_{-1} = q_1 r_0 + r_1 \qquad (\sigma(r_1) < \sigma(r_0))$$

$$r_0 = q_2 r_1 + r_2 \qquad (\sigma(r_2) < \sigma(r_1))$$

$$r_1 = q_3 r_2 + r_3 \qquad (\sigma(r_3) < \sigma(r_2))$$

$$\vdots$$

$$r_{N-4} = q_{N-2} r_{N-3} + r_{N-2} \qquad (\sigma(r_{N-2}) < \sigma(r_{N-3}))$$

$$r_{N-3} = q_{N-1} r_{N-2} + r_{N-1} \qquad (\sigma(r_{N-1}) < \sigma(r_{N-2}))$$

$$r_{N-2} = q_N r_{N-1}$$

gcd is last nonzero remainder

Defns from Ch 4 (and before) that you need to know for the final:

Ring, commutative ring

Unit, zero divisor, Zero Factor Property

Domain

Fields!!!

Ch. 5: Linear algebra

5.3 The foundations of linear algebra

5.4 Matrices with entries in a field F

5.5 Systems of linear equations (homogeneous case)

5.6 Dimension and rank-nullity

Kinds of problems to solve/ideas to review:

Solving Ax = 0 (RREF, procedure for finding a basis) mod 2, 3, 5

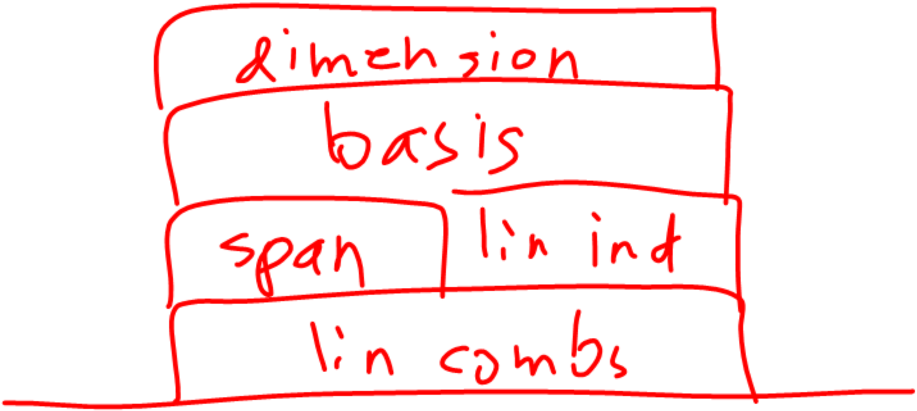
Idea of bases and how they encode subspaces

Idea of dimension

In a particular subspace, size(any spanning set) >= size(any linearly ind set)

The foundations of linear algebra

Review and know well this tower of definitions,
and also look at examples (PS05)



Ch. 6: Error-correcting codes

Defns/ideas to know:

Defn of a binear linear code!
[n,k,d] = length, dimension, minimum distance

Hamming 7-code: operational details

Idea: Larger min dist means more error correction

Ch. 7: Ideals, quotients, and finite fields

7.1 Ideals

7.2 Quotient rings

7.3 Computation in $F[x]/(m(x))$

7.4 Principal ideal domains

7.5 Homomorphisms

7.6 Finite fields

7.7 Two worked examples: $\mathbf{F}_8$ and $\mathbf{F}_{16}$

Cyclic codes and BCH codes

Defns and key ideas:
Ideal, principal ideal generated by a
Definition of quotient ring R/I
"alpha" notation for a quotient ring (e.g., finite field) F[alpha]o

Computations/procedures:
How to write elements of F[x]/(m(x)) and add, multiply, and invert them
(Inversion/reciprocals: Euclidean reduction)

Five Facts for Finite Fields

1. **Prime power:** The characteristic of a finite field is a prime p, order $q = p^e$ for some $e \geq 1$.
2. **Orders of elements:** Multiplicative group of a finite field is cyclic, i.e., if F has q elements, $F^\times$ has at least one element of order $q - 1$. Also: order of every element of $F^\times$ divides $q - 1$.
3. **Magic polynomial:** If $|F| = q$, then $\alpha^q = \alpha$ for every $\alpha \in F$. So $x^q - x$ 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 $m(x)$. (Order p^e, degree e.)
5. **Classification:** For any prime p and $q = p^e$ ($e \geq 1$), there exists a field $\mathbf{F}_q$ of order q, unique up to isomorphism.

How to describe a finite field

$F[\alpha]$, α root of $\underbrace{m(x)}_{\text{field b/c } m \text{ irr.}}$

$m(\alpha) = 0$

Alt: $F[x]/(m(x))$ $I = (m(x))$

Elts: $f(x) + I$ $\boxed{\alpha = x + I}$

α allows us to stop writing +I everywhere

Ch. 8: BCH codes

extended

other reason for α

Defns/ideas:

Polynomial notation for bitstrings of length n (and therefore, codewords)

Cyclic codes length n = ideals in ring F_2[x]/(x^n-1)

Orbits and minimal polynomials

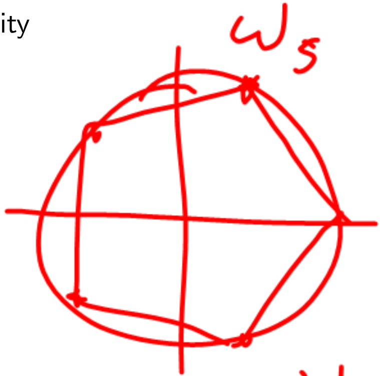
Computing parameters of a BCH (length, dim, designed min dist)

Ch. 9: The Discrete Fourier Transform

9.2 Complex numbers and roots of unity

9.3 Signals

9.4 The Discrete Fourier Transform



Defns/ideas:

Properties of roots of unity

Defn of DFT

Orthogonality Lemma

$$\omega_n = e^{\frac{2\pi i}{n}}$$

$$\boxed{\omega_n^n = 1}$$

Ch. 10: Groups

Defns/ideas:

Group

Subgroup

Cyclic subgroups and cyclic groups

Coset

Exam 3, #1, #2, #3, #6

10.3.1(a,c)

Exam 3 #1

(a) $(1+x^3) = \overbrace{\text{poly mults of } 1+x^3}^{\text{defn}}$

$x(1+x^3), x^2(1+x^3), x^3(1+x^3)$

(b) $(5) = \{\ldots, -5, 0, 5, 10, 15, \ldots\}$ Defn

$2+(5) = \{\ldots, -3, 2, 7, 12, 17, \ldots\}$

Defn

2. $\boxed{\mathbb{F}_2}$

$$x^5 + x^2 + 1 = (x)(x^4 + x + 1) + x + 1,$$
$$x^4 + x + 1 = (x^3 + x^2 + x)(x + 1) + 1.$$

α root of $x^5+x^2+1 = m(x)$

$(\alpha^5+\alpha^2+1=0)$

$\beta = \alpha^4+\alpha+1$ $\quad b(x) = x^4+x+1$

Given:

$m(x) = x\,b(x) + x+1$ $\quad$ solve

$b(x) = (x^3+x^2+x)(x+1) + 1$

ER:

$x+1 = m(x) + x\,b(x)$

$1 = b(x) + (x^3+x^2+x)(x+1)$

$1 = b(x) + (x^3 + x^2 + x)(m(x) + x\,b(x))$

Set $m=0$, get b: $\boxed{} = 1$

That $\boxed{}$ in terms of α, is β^{-1}.

3. (12 points) Let $\mathbf{F}_{64} = \mathbf{F}_2[\alpha]$, where α is a root of $x^6 + x + 1$. Let $\beta = \alpha^5 + \alpha^3 + 1$ and $\gamma = \alpha^3 + \alpha$.

$\Rightarrow \alpha^6 + \alpha + 1 = 0 \Rightarrow \alpha^6 = \alpha + 1$

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

$\beta\gamma = \alpha^8 + \dots$ $\qquad \Rightarrow \alpha^8 = \alpha^3 + \alpha^2$

Reduce to $\deg \leq 5$ in α.

6. (18 points) Let $\mathbf{F}_{64}$ be the field of order 64.

(a) If $\mathbf{F}_{64} = \mathbf{F}_2[x]/(m(x))$ for some irreducible $m(x) \in \mathbf{F}_2[x]$, what is the degree of $m(x)$? Briefly **explain** your answer.

(b) Does $\mathbf{F}_{64}^{\times}$, the multiplicative group of $\mathbf{F}_{64}$, contain an element of order 11? Briefly **explain** your answer.

(a) $\deg m = 6$ b/c $64 = 2^6$

(b) $|\mathbf{F}_{64}^{\times}| = 64 - 1 = 63$

Only orders divs of 63; no.