Math 127, Mon Mar 22

- 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: 7.1–7.3.
- PS06 due tonight, late deadline Fri Mar 26.
- **Exam 2 Wed Mar 24**, on 3.5–3.6, 4.2–4.3, 5.3–5.6, and 6.1–6.4 (PS04–06). Review session at 3pm (recorded to YouTube).

Questions on Ch. 6 and PS06?

Make sure you know the following chain of definitions:

* To say H is parity check matrix of a binary linear code C means that C = Null(H).
* Null(H) is the set of all x such that Hx = 0. In other words, in the context of binary linear codes, we think of H as the matrix of a system of linear equations (over F_2), and the code C is the solution set for that system of linear equations. If we write out a basis for Null(H) as the columns of a matrix G, that matrix G is a generator matrix for C.

Again, know your definitions:
* binary linear code
* parity check matrix
* generator matrix
* Null(H)

For example, 6.3.2(b): Need to list all of the codewords in a code C given by a parity check matrix H.
To do that:
* Think of H as the matrix of a system of linear equations
* Solve H and get a basis for Null(H)=C
* Use that basis to list all possible vectors in C.

Q: Do you treat parity check bits differently from data bits?
A: No.

$$\underline{m} \to \underline{x} \to \underline{y} \to \underline{m}'$$

By isolating just the transmission part, we can get a better understanding of what is possible in an error-correcting code.

Ideals

$\mathbb{Z}$ or $F[x]$

Maybe the most important definition in ring theory:

Definition

Let R be a (commutative) ring. An **ideal** of R is $I \subseteq R$ s.t.:

1. (Zero) The zero element of R is contained in I.
2. (Closed under addition) If $x, y \in I$, then $x + y \in I$.
3. (Closed under R-multiplication) If $x \in I$ and $r \in R$, then $rx \in I$.

Compare: Definition of subspace/subspace test

Exs:

For a ring R:

- The set $\{0\}$ $= I$ is an ideal of R called the **zero ideal**.
- R is an ideal of itself.

$\frac{4}{I}$

More interesting examples

integer multiples of 3

Let $R = \mathbf{Z}$, $I = \{3n \mid n \in \mathbf{Z}\}$. $= \{\ldots,-9,-6,-3,0,3,6,9,\ldots\} = (3)$

$0 \in I$ ✓

If $x, y \in I$, $x = 3n$, $y = 3k \Rightarrow x + y = 3(n+k) \in I$ ✓

If $x \in I$, $r \in \mathbb{Z}$, $x = 3n$, $rx = 3nr \in I$. ✓

So I is an ideal of the ring Z.

Let $R = \mathbf{F}_2[x]$, $I = \{p(x)(x^2 + x + 1) \mid p(x) \in \mathbf{F}_2[x]\}$. $= (x^2+x+1)$

I.e. $I =$ all poly mults of (x^2+x+1)

$= \{0, x^2+x+1, x^3+x^2+x,$

$(x+1)(x^2+x+1) = x^3+1, \ldots\}$

Check I is ideal of $\mathbb{F}_2[x]$:

$0 \in I$ ✓

(A) $y, z \in I \Rightarrow y = p(x)(x^2+x+1)$
$z = q(x)(x^2+x+1)$

$\Rightarrow y+z = (p(x)+q(x))(x^2+x+1) \in I$ ✓

(A) $y \in I,\ r(x) \in \mathbb{F}_2[x]$

$\Rightarrow y = p(x)(x^2+x+1)$

$ry = \underbrace{(r(x)p(x))}_{\in \mathbb{F}_2[x]}(x^2+x+1) \in I$ ✓

Classes of examples

R a ring. $R = \mathbb{Z}, F[x]$

- For fixed $a \in R$, the set

$$(a) = \{ra \mid r \in R\} = \{\text{all R-multiples of a}\}$$

  is called the **principal ideal generated by** a.

- For fixed $a, b \in R$, the set

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

  is called the **ideal generated by** a **and** b.

- For F a field and $a \in F$, the set

$$I_a = \{f(x) \in F[x] \mid f(a) = 0\}$$

  is an ideal of $F[x]$.

Quotient rings

One of the most important uses of ideals is to mod out by them. Specifically:

> *How can we make sense of $F[x]/(m(x))$ the same way we made sense of $\mathbf{Z}/(m)$?*

(And to be honest, we never really addressed all of the details of making sure that $\mathbf{Z}/(m)$ works, so we'll do that too.)

Cosets

Cosets are a fancy way of defining modular equivalence!

Let R be a ring, and let I be an ideal of R. For $r \in R$, we define the **additive coset** $r + I$ to be

$$r + I = \{r + a \mid a \in I\}.$$

If the context is clear, instead of saying "additive coset", we just say **coset**.

Example: What are the cosets of $(3) = I$ in $\mathbf{Z}$?

$\boxed{0+I} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}$ 0 mod 3

$4+I = \{\ldots, -5, -2, 1, 4, 7, 10, 13, \ldots\}$ 1 mod 3

$= \boxed{1+I} = 10+I$

$8+I = \{\ldots, 2, 5, 8, 11, 14, \ldots\}$ 2 mod 3

$= \boxed{2+I}$

When are elements in the same coset?

Theorem

R be a ring, I be an ideal of R, $r, s \in R$. TFAE:

1. $r + I = s + I$ *(i.e., the cosets $r + I$ and $s + I$ are the same set).*
2. $r \in s + I$.
3. $r - s \in I$.
4. $r = s + a$ *for some* $a \in I$.

Proof: (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4); (4) $\Rightarrow$ (1) on HW.

A) (2) $r \in s+I$

So $r = s+a$ for some $a \in I$

$\Rightarrow r-s=a$ " " "

C) (3) $r-s \in I$.

A (3) $r - s \in I$

so $r - s = a$ for some $a \in I$

$\Rightarrow r = s + a$ " " " .

C (4) $r = s + a$ for some $a \in I$

i.e. $r+I=s+I$

$\iff r=s+a,\ a\in I.$

Definition

To say that r is a **representative of the coset** $s+I$ means that $r \in s+I$.

Definition of quotient ring

Let R be a ring and let I be an ideal of R. We define the **quotient ring** R/I as follows.

- **Set:** The elements of R/I are the cosets of I in R. Note that if r and s represent the same coset of I, then the cosets $r+I$ and $s+I$ are actually the same element of R/I, since $r+I=s+I$.
- **Addition:** For $r+I, s+I \in R/I$, we define the sum
$$(r+I)+(s+I)=(r+s)+I.$$
- **Multiplication:** For $r+I, s+I \in R/I$, we define the product
$$(r+I)(s+I)=rs+I.$$

The zero element of R/I is $0+I=I$, and the one element is $1+I$.

Example: $\mathbf{Z}/(3)$

Let $R = \mathbf{Z}$, $I = (3)$ (the multiples of 3 in $\mathbf{Z}$).

Elements:

$0+I,\ 1+I,\ 2+I$

Multiplication table:

	$0+I$	$1+I$	$2+I$
$0+I$	$0+I$	$0+I$	$0+I$
$1+I$	$0+I$	$1+I$	$2+I$
$2+I$	$0+I$	$2+I$	$1+I$

$(0+I)(r+I) = 0+I$

$(1+I)(r+I)$
$= (1\cdot r)+I$
$= r+I$

$(2+I)(2+I)$
$= 4+I = 1+I$

So this really is the same $\mathbf{Z}/(3)$ we've been talking about all along.

The potential problem with quotients

When we define:

$$(r + I) + (s + I) = (r + s) + I \qquad (r + I)(s + I) = (rs) + I$$

Could it be the case that you get a different answer if you use different representatives for the cosets $r + I$ and $s + I$?

Theorem: No, everything works fine. (I.e., the operations in a quotient ring are well-defined and don't depend on our choice of coset representative.)

~~**Proof:** (multiplication part)~~

(Uses $r + I = s + I$

$\iff r = s + x$ for $x \in I$)

Review/revision: Computation in $\mathbf{Z}/(m)$

Let $I = (m)$ (the integer multiples of m). Working mod I, we have:

- **Elements:** The cosets of I in $\mathbf{Z}$, which we can write as $0 + I, 1 + I, \ldots, (m-1) + I$, or $\{0, \ldots, m-1\}$ for short, since division by m gives remainders between 0 and $m-1$.
- **Operations:** Addition and multiplication are computed in $\mathbf{Z}$ and then reduced mod I. I.e., you use division by m with remainder to choose a **reduced representative** for the final answer.

Example:

Computation in $F[x]/(m(x))$, version 1

F a field, $m(x) \in F[x]$ ($\deg m > 0$), $I = (m(x))$ (the polynomial multiples of $m(x)$). Working mod I, we have:

- **Elements:** The cosets of I in $F[x]$, which we can write as $r(x) + I$ where $\deg r(x) < \deg m(x)$, since division by $m(x)$ gives remainders of degree $< \deg m(x)$.
- **Operations:** Addition and multiplication are computed in $F[x]$ and then reduced mod I. I.e., you use division by $m(x)$ with remainder to choose a **reduced representative** for the final answer.

Example:

Computation in $F[x]/(m(x))$, version 2

F a field, $m(x) \in F[x]$ ($\deg m > 0$), $I = (m(x))$ (the polynomial multiples of $m(x)$). Abbreviate $\alpha = x + I$. Working mod I, we have:

- **Elements:** The cosets of I in $F[x]$, which we can write as $r(\alpha)$ where $\deg r < \deg m$, since setting $m(\alpha) = 0$ allows you to reduce any polynomial of degree $\geq \deg m$.
- **Operations:** Addition and multiplication are computed in polynomials in α and then reduced. I.e., you use the relation $m(\alpha) = 0$ to choose a **reduced representative** for the final answer.

Example: