Welcome! Everything is fine.

When you're connected by zoom:

- Use a laptop or desktop with a large screen so you can read these words clearly.
- To conserve bandwidth, please turn off your camera.
- Please mute your microphone unless I call on you.
- Please have the chat window open to ask questions.
- Reading for today: 7.2–7.3; for Wed: 7.4–7.5.
- PS07 due Wed Mar 25.
- Exam 2 delayed until mid-April.

Last: Cosets

Defn
I ideal

0. I contains 0
1. I closed under +
2. I closed under mult by elts of R

Definition
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

$$r + I = \{r + a \mid a \in I\}. \tag{1}$$

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

Ryusei: Can you multiply ideals? (Note I is a subset of R, not elt of R)
Ans: Yes, but that's a graduate algebra topic.
(Google "ideal factorization" if you want to go down the rabbit hole.)

Example: $I = (3) = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

$R = \mathbb{Z}$

same

$25 + (3) = 25 + \{\ldots, -27, -24, -21, -18, -15, \ldots\}$

$= \{\ldots, -2, 1, 4, 7, 10, \ldots\}$

$7 + (3) = 7 + \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

$= \{\ldots, -2, 1, 4, 7, 10, 13, \ldots\}$

$7 + (3) = 25 + (3)$

$= 1 + (3)$

rep

same! b/c $25 = 7 \pmod{3}$

Different representatives can give the same coset

In fact, 3 cosets of I : I, $1 + I$, $2 + I$

"(3)"

Coset conditions

Theorem

Let R be a ring, let I be an ideal of R, and let $r, s \in R$. Then the following are equivalent (one statement holds if and only the other holds):

Q: When do two "shifts" produce the same coset?

1. $r + I = s + I$ *(i.e., the cosets $r + I$ and $s + I$ are the same set).*
2. $r \in s + I$. When r is contained in the coset s + I.
3. $r - s \in I$. When the difference of r and s is an element of I.
4. $r = s + a$ *for some* $a \in I$.

r and s are "congruent mod I".

Proof of (1) implies (2):

A. r+I = s+I (i.e., those two sets are equal).
Since 0 is an element of I, and r+I is I shifted by r, r+0=r is an element of r+I.
But the set r+I is the same as the set s+I by assumption.

C. r is an element of s+I.

Definition of R/I

Quotient rings! (I.e., finally define Z/(3).)

Idea: R/I is R setting $I = 0$.

Definition

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.
- **Addition:** For $r + I, s + I \in R/I$, we define

$$(r + I) + (s + I) = (r + s) + I. \tag{2}$$

- **Multiplication:** For $r + I, s + I \in R/I$, we define

$$(r + I)(s + I) = rs + I. \tag{3}$$

+, * of two cosets defined in terms of +, * of their reps

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

set $I = 0$

ie, multiplicative identity

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

$I = (3)$

Elements:

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

$1 + I = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$

$2 + I = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$

$4 \in 1 + I$

$\Rightarrow 4 + I = 1 + I$

Multiplication table:

Abbrev:

*	$0+I$	$1+I$	$2+I$
$0+I$	$0+I$	$0+I$	$0 \cdot 2 + I = 0 + I$
$1+I$	$0+I$	$1+I$	$1 \cdot 2 + I = 2 + I$
$2+I$	$0+I$	$2+I$	$2 \cdot 2 + I = 4 + I = 1 + I$

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

R/I is a ring

Elements of R/I are cosets of I in R, and define

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

These are cosets, so in R/I

Theorem

It works! I.e., R/I is actually a ring.

What could go wrong? Why wouldn't R/I be a ring?

2. The + and * do not satisfy the axioms of a ring -- HW.
1. What if our addition and multiplication are bogus?
("Bogus" see: Bill and Ted's Excellent Adventure)
Here bogus could mean: Sum or product of two elements of R/I is not in R/I -- That's OK b/c RHS of definition is actually a coset, so in R/I.
Bogosity to worry about is: Definition of (r+I)(s+I) depends on choice of coset representatives r, s. What if a different choice gives a different answer?

Suppose we choose different coset reps r', s' s.t. r+I = r'+I, s+I = s'+I.
By "coset conditions" thm, r' = r+a, s' = s+b for some a,b in I.

Then (checking multiplication, see text for checking addition works):

r's' = (r+a)(s+b) = rs + rb + sa + ab.

But a,b in I and I closed under multiplication by elements of R.
So rb, sa, ab are all elements of I, so rb + sa + ab in I b/c I closed +.
So r's' = rs + (element of I), which means that r's' + I = rs + I.
Therefore, product (r+I)(s+I) doesn't depend on choice of reps r, s.

DL

$$(r+a)(s+b) = r(s+b) + a(s+b)$$
$$= rs + rb + as + ab$$

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

$$\$\$: \text{finite fields}$$

Let F be a field, let $m(x)$ be a polynomial in $F[x]$, and let $\overline{R} = F[x]/(m(x))$ (the ring of polynomials mod $m(x)$).

- How do we represent elements of $\overline{R}$ uniquely?
- How do we compute the ring operations of addition and multiplication in $\overline{R}$?
- How can we tell if $f(x) + (m(x))$ is a unit in $\overline{R}$, and if it is, how do we compute its (multiplicative) inverse?

(Recall: elements of F[x]/(m(x)) are cosets of (m(x)))

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

$m > 0$

Let $m \in \mathbf{Z}$ and let $\overline{R} = \mathbf{Z}/(m)$.

- Elements of $\overline{R}$ are represented uniquely as integers a s.t. $0 \leq a \leq m-1$, abbreviating $a + (m)$. possible remainders mod m
- To compute addition and mult, do addition and mult in $\mathbf{Z}$, divide by m, and take the remainder. (b/c of "coset conditions")
- $a + (m)$ is a unit $\Leftrightarrow \gcd(a, m) = 1$; compute inverses by Euclidean reduction.

$F[x]/(m(x))$ exactly the same!

Representing elements of $F[x]/(m(x))$

$m(x) \in F[x]$, $I = (m(x))$ the principal ideal generated by $m(x)$.

Theorem

Every coset $f(x) + I$ has a unique representative $r(x)$ such that $\deg r(x) < \deg m(x)$, computed by finding the remainder $r(x)$ upon dividing $f(x)$ by $m(x)$.

Proof: PS08.

Definition

For $f(x) \in F[x]$ we define the **reduced representive of** $f(x) + I$ to be the unique representative of $f(x) + I$ such that $\deg r(x) < \deg m(x)$.

We abbreviate the coset $x + I$ as $\alpha \in \overline{R}$, and $f(x) + I$ as $f(\alpha)$.

Note: Since $m(x) \in I$, by the definition of quotient ring, $m(\alpha) = 0$. We therefore sometimes describe α as a **root of** $m(x)$.

F adjoin α

So just as we can represent the elements of $\mathbf{Z}/(m)$ as $0, \ldots, m-1$, we can represent the elements of $\overline{R} = F[x]/(m(x))$ as polynomials in α of degree up to $d-1$, where $d = \deg m(x)$).

Since every element of $\overline{R} = F[x]/(m(x))$ can be written as a polynomial in α, we also sometimes describe $\overline{R}$ as "$F[\alpha]$, where α is a root of $m(x)$."

Addition and multiplication

Let $\overline{R} = F[\alpha]$, where α is a root of $m(x)$, and let $d = \deg m(x)$.

- Since any element of $F[\alpha]$ can be expressed uniquely as a polynomial in α of degree at most $d - 1$, and the sum of two such polynomials is a polynomial of degree at most $d - 1$, addition in $F[\alpha]$ is just ordinary polynomial addition with coefficients in F.
- For $f(\alpha), g(\alpha) \in F[\alpha]$, to find the product $f(\alpha)g(\alpha)$, we can compute $f(\alpha)g(\alpha)$ as a polynomial, and then reduce it using long division by $m(\alpha)$ (since $m(\alpha) = 0$), with the remainder being the reduced representative of the product.

Example

Rule: $\alpha^4 + \alpha + 1 = 0$

$F = \mathbf{F}_2$, $m(x) = x^4 + x + 1 \in \mathbf{F}_2[x]$, $\mathbf{F}_2[\alpha] = \mathbf{F}_2[x]/(m(x))$.

Computing in $\mathbf{F}_2[\alpha]$:

$\beta = \alpha^3 + \alpha + 1$

$\gamma = \alpha^2$

In practice: Elts $\mathbf{F}_2[\alpha]$ are polys in α, w/ rule $\alpha^4 + \alpha + 1 = 0$

$\alpha^4 = -\alpha - 1 = \alpha + 1$

coeffs still taken mod 2

$\alpha^5 = \alpha^2 + \alpha$

$\beta\gamma$

$= \alpha^5 + \alpha^3 + \alpha^2$

$= \alpha^2 + \alpha + \alpha^3 + \alpha^2$

$= \alpha^3 + 2\alpha^2 + \alpha$

coeffs taken mod 2

$= \alpha^3 + \alpha$. $(\alpha^3 + \alpha^2 + 1)(\alpha^2) = \alpha^3 + \alpha$

Reciprocals in $F[\alpha]$

Corollary

Let $\overline{R} = F[\alpha]$, where α is a root of $m(x) \in F[x]$. For $b(x) \in F[x]$, the element $b(\alpha) \in \overline{R}$ has an inverse in $\overline{R}$ if and only if $\gcd(b(x), m(x)) = 1$, in which case the inverse $g(\alpha)$ of $b(\alpha)$ can be computed by solving

$$f(x)m(x) + g(x)b(x) = 1 \tag{4}$$

in $F[x]$, using Euclidean Reduction for polynomials. □

Special case, just like $\mathbf{Z}/(m)$ is a field iff m is prime:

Corollary

Let $\overline{R} = F[x]/(m(x))$. Then $\overline{R}$ is a field if and only if $m(x)$ is irreducible. □

Example

$F = \mathbf{F}_2$, $m(x) = x^4 + x + 1 \in \mathbf{F}_2[x]$, $\mathbf{F}_2[\alpha] = \mathbf{F}_2[x]/(m(x))$.
Computing in $\mathbf{F}_2[\alpha]$:

$\beta =$

$\gamma =$