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: 7.3–7.4; for Mon after break: 7.5–7.6.
- If you have time over "break": Try to catch up on HW. (Don't go anywhere!)
- Exam 2 in mid- to late April.

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

ideal of all F[x]-mults of m(x)
killing (m(x)) means setting m(x) = 0.

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?

F is a field (think: F = F_2 = Z/(2))
F[x] is the ring of all polynomials with coefficients in F
(F[x] is just a ring, not a field, b/c (1/polynomial) is not a poly.)

Example

Think of m(x) as modulus, like m in Z/(m)

$F = \mathbf{F}_2$, $m(x) = x^4 + x + 1 \in \mathbf{F}_2[x]$, $I = (m(x))$, $\mathbf{F}_2[\alpha] = \mathbf{F}_2[x]/I$ (i.e., α abbreviates coset $x + I$).

We start out with polys w/ coeffs mod 2, and then kill, so coeffs still mod 2.

So elements of $\mathbf{F}_2[\alpha]$ are polynomials in α subject to the rule $\alpha^4 + \alpha + 1 = 0$. In fact, only need polynomials of degree ≤ 3:

to represent all elements of $R = \mathbf{F}_2[\alpha]$.

$4 - 1$

Simplify

Ex $\alpha^7 + \alpha^6 + \alpha^5 + \alpha^3$

$= \alpha^3 + \alpha + 1 \leftarrow \alpha^7$

$+ \alpha^3 + \alpha^2 \leftarrow \alpha^6$

$+ \alpha^2 + \alpha \leftarrow \alpha^5$

$+ \alpha^3$

$= \alpha^3 + 0\alpha^2 + 0\alpha + 1$

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

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

$\alpha^4 = \alpha + 1$

$\times \alpha$

- = + b/c all coeffs mod 2

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

$\alpha^6 = \alpha^3 + \alpha^2$

$\alpha^7 = \alpha^4 + \alpha^3$

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

Fact: any element of $\mathbf{F}_2[\alpha]$ represented uniquely as polynomial in α of degree ≤ 3.

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

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

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

$\alpha^4 = \alpha + 1$

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

$\alpha^6 = \alpha^3 + \alpha^2$

same reduction rules as before, based on initial data m(x) = x^4 + x + 1

$\beta + \gamma = (\alpha^6 + \alpha^4 + \alpha^3) + (\alpha^5 + \alpha^3 + \alpha^2)$

$= \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2$

$\beta\gamma = (\alpha^3 + \alpha^2) + (\alpha^2 + \alpha) + (\alpha + 1) + \alpha^2$

$= \alpha^3 + \alpha^2 + 1$

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

m(x) is the *modulus* of quotient ring 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 $m(x)$."

pronounced "F adjoin alpha"

I.e., to say that alpha is a root of m(x) means that m(x) is the modulus of the ring F adjoin alpha.

Addition and multiplication

"R bar is F adjoin alpha, where alpha is a root of m(x)"

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.

Or better: Use reduction rules coming from modulus m(x).

Reciprocals in $F[\alpha]$

Inverses mod m:
a has an inverse mod m exactly when gcd(a,m) = 1.
We find inverse x of a by solving ax + my = 1 in integers using Euclidean reduction.

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

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

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. □

irr modulus = quotient is a field

Example

$F = \mathbf{F}_2$, $m(x) = x^3 + x + 1 \in \mathbf{F}_2[x]$, $\mathbf{F}_2[\alpha] = \mathbf{F}_2[x]/(m(x))$; so rule is $\alpha^3 = \alpha + 1$.

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

$\beta = \alpha^3 + \alpha^2 + \alpha$ Find β^{-1}. $b(x) = x^3 + x^2 + x$

To solve $\beta\gamma = 1$, solve $b(x)g(x) + m(x)f(x) = 1$.

$b(x)$

$x^3+x^2+x \overline{)\, x^3 + x + 1}$ $m(x)$ — 1

$x^3 + x^2 + x$

$x^2 + 1$

$x^2+1 \overline{)\, x^3 + x^2 + x + 0}$ — $x + 1$

$x^3 + x$

x^2

$x^2 + 1$

1 ← gcd

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

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

$$x^2+1 = m(x) - b(x)$$

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

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

Mod $m(x)$, $x \to \alpha$ $\quad (m(\alpha) = 0)$

$$1 = b(\alpha) + (\alpha+1)\, b(\alpha)$$

$$= 1 \cdot b(\alpha) + (\alpha+1)\, b(\alpha)$$

$$1 = (\alpha+2)\beta = \alpha\beta$$

$$\boxed{\beta^{-1} = \alpha}$$

Check

$\beta = \alpha^2 + 1$

$\alpha^3 = \alpha + 1$

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

$= \alpha + 1 + \alpha = 1$

7.4: Principal ideal domains

Key property that explains much of what $\mathbf{Z}$ and $F[x]$ have in common as rings.

Definition

To say that a ring R is a **principal ideal domain**, or **PID**, means that R is an integral domain (has the Zero Factor Property) and that every ideal of R is principal. I.e., second condition says that if I is an ideal of R, then $I = (a)$ (the set of all R-multiples of a) for some $a \in R$.

$\mathbf{Z}$ and $F[x]$ are PIDs

Theorem

If $R = \mathbf{Z}$ or $R = F[x]$, then R is a PID.

$(\{0\} = (0))$

Proof. Suppose I is a nonzero ideal of $\mathbf{Z}$.

Let $d =$ an elt of I of smallest possible nonzero $|d|$.

Suppose $a \in I$.

Signed Division:

$a = qd + r$ for $q, r \in \mathbb{Z}$

$|r| \leq \frac{|d|}{2} < |d|$

So

$r = a - qd$

But $d \in I, q \in \mathbb{Z} \Rightarrow dq \in I$ ideals closed under mult by R

and $a \in I, qd \in I \Rightarrow a - qd = r \in I$

But d has smallest nonzero abs value, so r =0.

Analogous proof works for $R = F[x]$ (PS08).

Again: d has smallest possible abs value among nonzero elements of I and r is an element of I with smaller abs value than d, so r = 0.
So a = qd, i.e., any arbitrary element of a is a multiple of d, ie..,
I = multiples of d = (d).

Minimal polynomials

Definition

Let F be a field, and let I be an ideal of $F[x]$. To say that $d(x)$ is the **minimal polynomial** of I means that $I = (d(x))$. (Exists b/c PID; turns out to be unique up to associates.)

How compute minimal polynomial? Depends, but in one particular case:

Theorem

Let F be a field, and consider the ideal $I = (a(x), b(x))$ of $F[x]$, where $a(x)$ and $b(x)$ are nonzero polynomials in $F[x]$. Then the minimal polynomial of I is $\gcd(a(x), b(x))$.

Proof. Let $d(x) = \gcd(a(x), b(x))$. WTS $(d(x)) = (a(x), b(x))$. First: WTS $(a(x), b(x)) \subseteq (d(x))$.

Converse: WTS $(d(x)) \subseteq (a(x), b(x))$.

Factorization

For the theory-inclined, proving unique factorization in $\mathbf{Z}$ or $F[x]$ now follows from:

Theorem

If R is a PID, then unique factorization holds in R.

Proof is outside our scope, but that's the key point if you're interested.