Math 127, Wed Apr 07

- 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: 7.4–7.5. Reading for Mon: 7.6–7.7.
- PS07 outline due tonight, full version due in one week.
- Problem session Fri Apr 09, 10am–noon.

Computation in $F[x]/(m(x))$, α notation

F a field, $m(x) \in F[x]$ ($\deg m = k > 0$), $I = (m(x))$ (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 $\deg r < k$, since setting $m(\alpha) = 0$ allows you to reduce any polynomial of degree $\geq k$.
  More specifically, if $\deg m = k$, then you rewrite $m(\alpha) = 0$ as a **reduction relation** $\alpha^k = \cdots$ and apply that repeatedly to reduce any higher-degree terms to terms of degree $< k$.
- **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.

$\mathbb{F}_2$ w/ α,

Example: $\mathbf{F}_2[x]/(x^4 + x + 1)$ $\iff$ $\alpha^4 + \alpha + 1 = 0$

Reduction rel'n: $\alpha^4 = \alpha + 1$ $(+1 = -1)$

Elts: Polys in α, deg ≤ 3

$+, \circ$: Computed as polys in α, reduce w/ $\alpha^4 = \alpha + 1$

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

Ex $(\alpha^2+1)(\alpha^3+\alpha^2+1)$

$\boxed{2=0}$

$$
\begin{array}{r}
\alpha^3+\alpha^2\quad +1 \\
\alpha^2\quad +1 \\
\hline
\alpha^3+\alpha^2\quad +1 \\
\alpha^5+\alpha^4\quad +\alpha^2 \\
\hline
\alpha^5+\alpha^4+\alpha^3\quad +1
\end{array}
$$

$$
\begin{aligned}
&\alpha^2+\cancel{\alpha} \\
&+\cancel{\alpha}+\cancel{1} \\
&+\alpha^3+\cancel{1} \\
&=\alpha^3+\alpha^2
\end{aligned}
$$

Inverses in $\mathbb{Z}/(m)$:

Solve

$$mx + by = 1$$

Possible $\iff \gcd(b, m) = 1$

Then $by \equiv 1 \pmod{m}$

or $y \equiv b^{-1} \pmod{m}$

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

Let $\overline{R} = F[\alpha]$, where $\overbrace{\alpha \text{ is a root of } m(x)}^{m(\alpha)=0} \in F[x]$, and suppose $b(x) \in F[x]$. How can we find the reciprocal of b(alpha) in F[alpha]?

Follows from polynomial Euclidean Reduction that:

Thm: 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

mod $m(x)$:

$$\cancel{f(x)m(x)} + g(x)b(x) = 1 \Rightarrow g(\alpha)b(\alpha) = 1$$

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

Cor: $\overline{R}$ is a field if and only if $m(x)$ is irreducible.

(Analogue of fact that $\mathbf{Z}/(m)$ is a field if and only if m is prime.)

Example: $\mathbf{F}_2[x]/(x^4 + x + 1)$

Let $m(x) = x^4 + x + 1$, $\overline{R} = \mathbf{F}_2[x]/(m(x)) = \mathbf{F}_2[\alpha]$. Turns out that $m(x)$ is irreducible. Find inverse of:

$m(\alpha) = 0$; $\alpha^4 = \alpha + 1$

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

$\gcd(m(x), b(x))$:

$$
\begin{array}{r|l}
 & \quad x + 1 \\
\hline
b = x^3 + x^2 + 1 & x^4 \qquad + x + 1 = m \\
 & x^4 + x^3 \quad + x \\
\hline
 & \qquad x^3 \qquad + 1 \\
 & \qquad x^3 + x^2 + 1 \\
\hline
\end{array}
$$

$$x^2$$

$$\begin{array}{r|l} & x+1 \\ \hline x^2 & x^3+x^2+1 \\ & x^3+x^2 \\ \hline & 1 \end{array}$$

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

$$b(x) = (x+1)\,x^2 + 1 \qquad \boxed{+ = -}$$

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

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

$$= b(x) + (x+1)\left[m + (x+1)\,b(x)\right]$$

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

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

$$1 = x^2\, b(x) \pmod{m(x)}$$

$$\boxed{(\alpha^3+\alpha^2+1)^{-1} = \alpha^2}$$

$\alpha^4 = \alpha + 1$

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

Check: $\alpha^2(\alpha^3+\alpha^2+1)$

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

$$= \cancel{\alpha^2} + \cancel{\alpha} + \cancel{\alpha} + 1 + \cancel{\alpha^2} = 1$$

Principal ideal domains

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

Theorem

Let R be either $\mathbf{Z}$ or $F[x]$ (F a field), or more generally, let R be a Euclidean domain. Then R is a PID.

Proof, case $R = \mathbf{Z}$: We apply signed division:

If $a, d \in \mathbf{Z}$, $d \neq 0$, then for some $q, r \in \mathbf{Z}$,

$$a = dq + r \qquad \text{with } |r| \leq \frac{|d|}{2}.$$

A I ideal of $\mathbb{Z}$

If $I = \{0\}$, then $I = (0)$ ✓

Oth, I contains nonzero elts.

Let d be nonzero elt of I w/ smallest $|d|$. (−d also works)

For any $a \in I$, sign div.

(★) $a = qd + r$, $|r| \le \frac{|d|}{2} < |d|$

But $r = a - qd$; $-qd \in I$ b/c $d \in I$ and $a - qd \in I$ b/c $a \in I$, $-qd \in I$.

So $r \in I$, $|r| < |d|$

But d is the *nonzero* element of I with smallest possible absolute value, so the only way r (in I) can have a smaller absolute value is if r=0.

So $r=0 \Rightarrow (*)$ becomes $a=qd$.

So $a \in (d) \Rightarrow I \subseteq (d)$.

$I=(d)$ for some $d \in \mathbb{Z}$

The minimal polynomial

To recap: We know in the abstract that if I is an ideal of $F[x]$, then there is some $d(x)$ such that $I = (d(x))$. If we choose $d(x)$ to be **monic** (leading coefficient 1), then we call $d(x)$ the **minimal polynomial** of I.

Note that we only know $d(x)$ exists in the abstract, and in practice, we use different methods to figure out what $d(x)$ is in different circumstances. For example:

Theorem

$\{f(x)a(x)+g(x)b(x) \mid f(x), g(x) \text{ in } F[x]\}$

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 $\gcd(a(x), b(x))$, which can be computed by the Euclidean algorithm. $\square$

See PS08.

Homomorphisms

A thing that looks abstract but is fundamental. (And is surprisingly useful!)

inputs outputs

Definition

Let R and R' be rings. To say that a function $\varphi : R \to R'$ is a **homomorphism** means that for all $r, s \in R$,

$$\varphi(r+s) = \varphi(r) + \varphi(s), \qquad \varphi(rs) = \varphi(r)\varphi(s).$$

In other words, a homomorphism is a function between rings that preserves addition and multiplication.

Compare: Linear transformations in linear algebra

Example: Substitution homomorphism

Let F be a field, and fix some $\alpha \in F$. We define a function $\varphi : F[x] \to F$ by declaring

$$\varphi(f(x)) = f(\alpha)$$

for all $f(x) \in F[x]$. Then φ turns out to be a type of homomorphism known as a **substitution homomorphism**. What does φ being a homomorphism mean in practice?

$\varphi(f(x) + g(x))$ = add f, g, then plug in α

$\varphi(f(x)) + \varphi(g(x))$ plug first

= plug in α first, then add

Ex. $F = \mathbb{R}$ $\quad f(x) = x^2 + 1$

$$g(x) = x + 3$$

$$\varphi(f(x)) = f(-2)$$

$$\varphi(f(x) + g(x)) = \varphi(x^2 + x + 4)$$

$$= (-2)^2 + (-2) + 4 = 6$$

$$\varphi(f(x)) + \varphi(g(x)) = f(-2) + g(-2)$$

$$= 5 + 1 = 6$$

When are two rings "the same"?

Definition

An **isomorphism** is a bijective (one-to-one and onto) homomorphism. To say that rings R and R' are **isomorphic** means that there exists some isomorphism $\varphi : R \to R'$.

Suppose $\varphi : R \to R'$ is an isomorphism. Then:

- The elements of R and the elements of R' are paired up bijectively (one-to-one correspondence).
- This pairing (given by φ) preserves the operations $+$ and $\times$.
- Conclusion: R and R' are really the "same" ring, but with different names for the elements.

Properties preserved under isomorphism

* R and R' have same number of elements.

If R and R' are isomorphic rings, we have that, for example:

- R and R' have the same number of units.
- R is an integral domain if and only if R' is an integral domain.
- R is a field if and only if R' is a field.
- R is a PID if and only if R' is a PID.

These kinds of properties are called invariants -- like eye color or height for people.

That is, any property of a ring that can be defined abstractly, based on the axioms of a ring, is preserved under isomorphism. On the other hand, if R and R' don't share a particular abstract property, then R and R' can't be isomorphic.

Example: Suppose R is a ring that is not a field (i.e., R has nonzero elements that do not have inverses). Then any field F can't be isomorphic to R.

Automorphisms

Defn: An **automorphism** is an isomorphism $\varphi : R \to R$ from a ring to itself.

Exmp: Let $\varphi : \mathbf{C} \to \mathbf{C}$ be

$$\varphi(a + bi) = a - bi$$

for $a, b \in \mathbf{R}$. Then φ is a homomorphism (PS08) and $\varphi \circ \varphi$ is the identity, so φ is an isomorphism, and therefore, an automorphism of $\mathbf{C}$.

Exmp: Let R be a ring, and let $\varphi : R \to R$ be an automorphism of R. Define a map $\Phi : R[x] \to R[x]$ by

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

In other words, $(\Phi(f))(x)$ is obtained by applying φ to the *coefficients* of $f(x)$. Then Φ is an automorphism of $R[x]$, called the **automorphism of $R[x]$ induced by φ**.

Symmetries of the roots of a polynomial

Theorem

Let R be a ring, let $\varphi : R \to R$ be an automorphism of R, and let $\Phi : R[x] \to R[x]$ be the corresponding induced automorphism. Then for $f(x) \in R[x]$ and $\alpha \in R$, if $f(\alpha) = 0$, then $(\Phi(f))(\varphi(\alpha)) = 0$.

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 $a - bi$ is also a root of $f(x)$. (In other words, non-real roots of real polynomials come in conjugate pairs.)

Example: Consider $f(x) = x^4 + 5x^2 + 4$.

Next up: Finite fields

Suppose F is a field and F has finitely many elements. What can we say about:

- The size of F (how many elements does F contain)?
- How is F constructed?
- How can we compute inside F?

Turns out that every finite F is $\mathbf{F}_p[x]/(m(x))$ for some irreducible $m(x) \in \mathbf{F}_p[x]$. We'll see more next time. . . .