Math 127, Mon Apr 11

- Reading for today: 7.4–7.5.
- Reading for Wed Apr 13: 7.6.
- PS07 due tomorrow.
- PS08 outline due Thu Apr 14.

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

Let $m(x) = x^4 + x + 1$ and consider $\overline{R} = \mathbf{F}_2[x]/(m(x))$.
I.e., let $\overline{R} = \mathbf{F}_2[\alpha]$, where α is a root of $m(x)$. So $\alpha^4 + \alpha + 1 = 0$, which means that:

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

$\alpha^4 = \alpha + 1$

this is what we use to put everything into reduced form

Elements of $\overline{R}$:

$\{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1,$
$\alpha^3, \alpha^3+1, \alpha^3+\alpha, \alpha^3+\alpha+1,$
$\alpha^3+\alpha^2, \alpha^3+\alpha^2+1, \alpha^3+\alpha^2+\alpha, \alpha^3+\alpha^2+\alpha+1\}$

$\mathbf{F}_2[x]/(x^4 + x + 1)$, cont.

Reduction relations:

$\alpha^4 = \alpha + 1$ $\xrightarrow{\cdot\alpha}$ $\alpha^5 = \alpha^2 + \alpha$ $\xrightarrow{\cdot\alpha}$ $\alpha^6 = \alpha^3 + \alpha^2$

Addition in $\overline{R}$: (Just addition in F_2[x])

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

random + prob

Multiplication in $\overline{R}$:

$$\begin{array}{r} (\alpha^3 + \alpha^2 + 1) \\ \times \quad (\alpha^3 + \alpha) \\ \hline \alpha^4 + \alpha^3 + \alpha \\ \alpha^6 + \alpha^5 + \alpha^3 \\ \hline \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha \end{array}$$

reduce

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

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

$(\alpha^3+\alpha^2+1)(\alpha^3+\alpha) = \alpha^6+\alpha^5+\alpha^4+\alpha$

By fact that

$m(x) = x^4+x+1$, $\boxed{2=0}$

$m(\alpha)=0$, get

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

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

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

$\Rightarrow (\alpha^3+\alpha^2)$

$+(\alpha^2+\alpha)$

$+(\alpha+1)$

$+\alpha$

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

Yoga try $m(x) = x^4 + x^2 + 1$

α root of $m(x)$ in $\overline{R} = \overline{\mathbb{F}_2}$

1. Reduce $\alpha^4, \alpha^5, \alpha^6$ to deg ≤ 3?

2. Let $\beta = \alpha^2$, $\gamma = \alpha^3 + \alpha^2 + 1$

Compute $\beta\gamma$ (reduced).

---

1. $\alpha^4 = \alpha^2 + 1$

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

$\alpha^6 = \alpha^4 + \alpha^2 = (\alpha^2 + 1) + \alpha^2 = 1$

2. $\beta\gamma = \alpha^5 + \alpha^4 + \alpha^2$

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

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

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

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

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

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:

$\beta = \alpha^3 + \alpha^2$ $\quad \alpha^4 = \alpha + 1$

Find β^{-1}!

$\gcd(x^4 + x + 1, x^3 + x^2)$ (m, b)

$x^4 + x + 1 = (x+1)(x^3 + x^2) + x^2 + x + 1$ (m, b, r)

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

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

Rewrite mod m. $+ = -$

$$0 = (x+1)b(x) + (x^2+x+1)$$

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

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

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

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

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

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

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

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

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

$$1 = (x^3+x)\,b(x) \pmod{m(x)}$$

In α:

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

So $\boxed{\beta^{-1} = \alpha^3+\alpha}$

Principal ideal domains

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 $I = (0)$ ✓.

So assume I has nonzero elts

Let $d \neq 0$ be elt of I w/ smallest poss $|d|$ among nonzero elts of I

$(d) \subseteq I$ so WTS $I \subseteq (d)$

(A) $a \in I$

So $a = qd + r$, $q \in \mathbb{Z}$, $|r| \leq \frac{|d|}{2}$

But $r = a - qd \in I$ b/c I is an ideal

Since d has smallest abs value among nonzero elements of I, and |r| < |d|, we must have r=0.

(C) $a = qd$ for some $q \in \mathbb{Z}$

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

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.

Homomorphisms

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

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.

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?

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

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.

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