Math 127, Mon Apr 05

- 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: 7.3–7.4.
- PS07 outline due Wed, full version due in one week.
- Problem session Fri Apr 09, 10am–noon.

Ideals: A long recap

w/1

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 $rx \in I$.

Ideals are very abstract, very important — and very lucrative.

Proofs (review/reboot)

Proofs are mostly not:

- ~~induction (weak and strong)~~
- ~~contradiction~~
- (contrapositive)

direct proof

Most of the time, we prove statements of the form "If P, then Q."
A proof of that statement **EXPLAINS** logically how the assumption P must lead to the conclusion Q.
To set up (outline) the proof of "If P, then Q":

Assume P true | $\boxed{A}$ P true

logic logic logic logic logic
logic logic logic logic logic
logic logic logic logic

Conclude Q true | $\boxed{C}$ Q true

Example

R a ring, $a \in R$. Prove that

(a) is all things that look like this
(have form ra)

the ideal generated by a $\rightarrow (a) = \{ra \mid r \in R\}$ and satisfy this condition

is an ideal of R. The ideal test says that the set (a) is an ideal of R exactly when all of the following are true: $=I$

- (Zero) The zero element of R is contained in I.
- (Closed under addition) If $x, y \in I$, then $x + y \in I$.
- (Closed under R-multiplication) If $\underbrace{x \in I \text{ and } r \in R}_{P}$, then $rx \in I$.] Q

In reverse order:

R. mult

$\boxed{\text{Fs}}$ $x \in (a), r \in R$

$x = sa$ for some $s \in R$

$\Rightarrow rx = r(sa) = (rs)a$

$rx = ta$ for some $t \in R$ $(t = rs)$

$\boxed{\text{C}}$ $rx \in (a)$

Ⓐ $x, y \in (a)$

cl $x = ra, y = sa$ for $r, s \in R$ ∴

$+ \Rightarrow x + y = ra + sa = (r+s)a$

$x + y = ta$ for $t \in R$ $(t = r+s)$

Ⓒ $x + y \in (a)$

$\boxed{\begin{array}{l} (a) \text{ generalizes "multiples of } a\text{"} \\ (5) = \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\} \end{array}}$

$0 \in (a)$ Observe: $0 = 0a$. $\left(\underset{r=0}{ra \text{ for}}\right)$

Ⓒ $0 \in (a)$ ☺

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 $1+I$.

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.

$m = 13$ In $\mathbb{Z}/(13)$:

Example:

$(7+(13)) + (8+(13)) = 15+(13)$

prev: $7+8 \equiv 2 \pmod{13}$ $= 2+(13)$

$(7+(13))(2+(13)) = 14+(13) = 1+(13)$

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

$F = \mathbb{F}_2$

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.

Ex. $I = (x^3)$, $F = \mathbb{F}_2$. In $F[x]/I$:

$$((x^2+1)+I)((x+1)+I)$$
$$= (\cancel{x^3}+x^2+x+1)+I \quad \boxed{\text{reduce mod } x^3}$$
$$= (x^2+x+1)+I$$

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

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.

$F = \mathbb{F}_2$

Ex: $m(x) = x^4 + x + 1$

$m(\alpha) = 0$, so $\alpha^4 + \alpha + 1 = 0 \Rightarrow \boxed{\alpha^4 = \alpha + 1}$

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

$k = 4$

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:

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

Elements of $\overline{R}$:

Can reduce any polynomial in alpha of degree >= 4 until it has deg <= 3.
So elements of the ring are exactly the polynomials in alpha of deg <= 3:

$$\overline{R} = \{ b_3\alpha^3 + b_2\alpha^2 + b_1\alpha^1 + b_0 \mid b_i \in \mathbf{F}_2 \}$$

So $\overline{R}$ has $\underline{16}$ elts $\quad 16 = 2^4$

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

Reduction relations:

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

$$2 = 0 \qquad \alpha^5 = \alpha^2 + \alpha$$

Addition in $\overline{R}$:

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

Multiplication in $\overline{R}$:

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

$$= \alpha^5+\alpha^4+\alpha^2+\alpha \quad \text{] not reduced}$$

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

$$= \alpha+1$$

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

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

EA: gcd(b, m)
ER: eqn

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:

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 $q, r \in \mathbf{Z}$,

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

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

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. $\square$