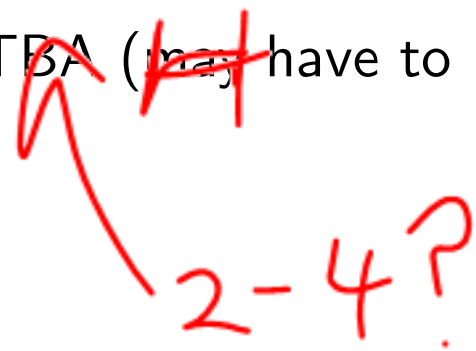
Hello Math 127

- Reading for today: 7.3–7.4.
- Reading for Mon Apr 11: 7.4–7.5.
- Outline for PS07 due today; completed version due Mon Apr 11.
- Problem session Fri Apr 08; time TBA (~~may~~ have to move to the afternoon).



Ideals

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 $rx \in I$. Like: If you mult an even number by any integer, get even.

Example: Let $R = \mathbf{Z}$, $I = \{3n \mid n \in \mathbf{Z}\}$. $= (3)$

More generally: For any R and fixed $a \in R$, the set

$$(a) = \{ra \mid r \in R\}$$

is called the **principal ideal generated by** a.

Q If I ideal of $\mathbb{Z}$, $10, 30 \in I$. what is smallest set I could be?

Ans: On the one hand, I must contain every multiple of 10, so I contains the principal ideal (10).

On the other hand, 30 is a multiple of 10, so $(10) = \{10r \mid r \text{ in } \mathbb{Z}\}$ is an ideal containing 10 and 30.

So the smallest possible set I could be is (10).

Note that there are other, larger ideals that I could be: (5), (2), $(1)=\mathbb{Z}$ are all ideals that contain 10 and 30.

Cosets

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

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

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

Example: What are the cosets of (3) in $\mathbf{Z}$?

3 cosets of (3)

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

$1 + (3) = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\}$

$2 + (3) = \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\}$

$3 + (3) = \{\ldots, -3, 0, 3, 6, 9, 12, \ldots\} = 0 + (3)$

When are elements in the same coset?

Theorem

R be a ring, I be an ideal of R, $r, s \in R$. TFAE:

1. $r + I = s + I$ *(i.e., the cosets $r + I$ and $s + I$ are the same set).*
2. $r \in s + I$.
3. $r - s \in I$.
4. $r = s + a$ *for some* $a \in I$.

Definition

To say that r is a **representative of the coset** $s + I$ means that $r \in s + I$ (and therefore, $r + I = s + I$).

Upshot: r and s are representatives of the same coset exactly when "$r = s \pmod{I}$", i.e., r and s differ by an element of I.

Ex. $1+(3) = \{\ldots, -2, 1, 4, 7, \ldots\} = 4+(3) = -2+(3)$

Definition of quotient ring

$\mathbb{Z}/(3)$ is the integers with all multiples of 3 set = 0.

R/I is what happens when you "set I equal to 0".

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 $r + I = s + I$. Ex $\mathbb{Z}/(3) = \{0+(3), 1+(3), 2+(3)\}$
- **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

defined in terms of coset reps

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

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

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

Let $R = \mathbf{Z}$, $I = (3)$ (the multiples of 3 in $\mathbf{Z}$). $R/I = \mathbb{Z}/(3)$

Elements:

$0+(3)$, $1+(3)$, $2+(3)$

Multiplication table:

	$0+(3)$	$1+(3)$	$2+(3)$
$0+(3)$	$0+(3)$	$0+(3)$	$0+(3)$
$1+(3)$	$0+(3)$	$1+(3)$	$2+(3)$
$2+(3)$	$0+(3)$	$2+(3)$	$4+(3)$ $= 1+(3)$

So this really is the same $\mathbf{Z}/(3)$ we've been talking about all along.

mult mod 3	0	1	2
0	0	0	0
1	0	1	2
2	0	2	4=1

Prob? $2+(3) = 5+(3) = 8+(3)$

$(5+(3))(8+(3))$

$= 40+(3)$

$= 1+(3)$ phew!

$40 = 1+39 \in (3)$

$\equiv 0 \pmod 3$

The potential problem with quotients

When we define:

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

Could it be the case that you get a different answer if you use different representatives for the cosets $r + I$ and $s + I$?

Theorem: No, everything works fine. (I.e., the operations in a quotient ring are well-defined and don't depend on our choice of coset representative.)

Proof: (multiplication part)

Suppose r'+I = r+I and s'+I = s+I. Then r' = r+a and s' = s+b for some a,b in I. Then by definition of multiplication in R/I:

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

(elt of R)(elt of I) = (elt of I)

But I is closed under R-mult, and b in I, so rb in I. Similarly, as and ab are in I. Because I closed under +, (rb+as+ab) = c in I. So:

(r'+I)(s'+I) = rs + c + I = rs + I.

Phew

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

modulus

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.

Example: $m = 5$, $I = (5)$. In $\mathbb{Z}/(5)$:

$(7 + I)(8 + I) = 56 + I$ (by defn)

$(2+I)(3+I)$

$= 1 + 55 + I$ ($m = 0$)

$= 1 + I$

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

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.

Example: $F = \mathbb{F}_2$, $m(x) = x^2 + x + 1$, $I = (m(x))$.

What is $F[x]/I$?

Four cosets $r(x) + I$, $\deg r < 2$. ($\deg = -\infty, 0, 1$)

So $r(x) = 0, 1, x, x+1$ in $\mathbb{F}_2[x]$

$R/I = \{0+I, 1+I, x+I, (x+1)+I\}$

	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$0+I$	$0+I$			
$1+I$		$1+I$	$x+I$	$(x+1)+I$
$x+I$		$x+I$	$(x+1)+I$	$1+I$
$(x+1)+I$		$(x+1)+I$	$(x+1)x+I$	$x+I$

$= 1+I$

$(x+1)x+1$

$= x^2+x+1$

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

$= 1+1$

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

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

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:

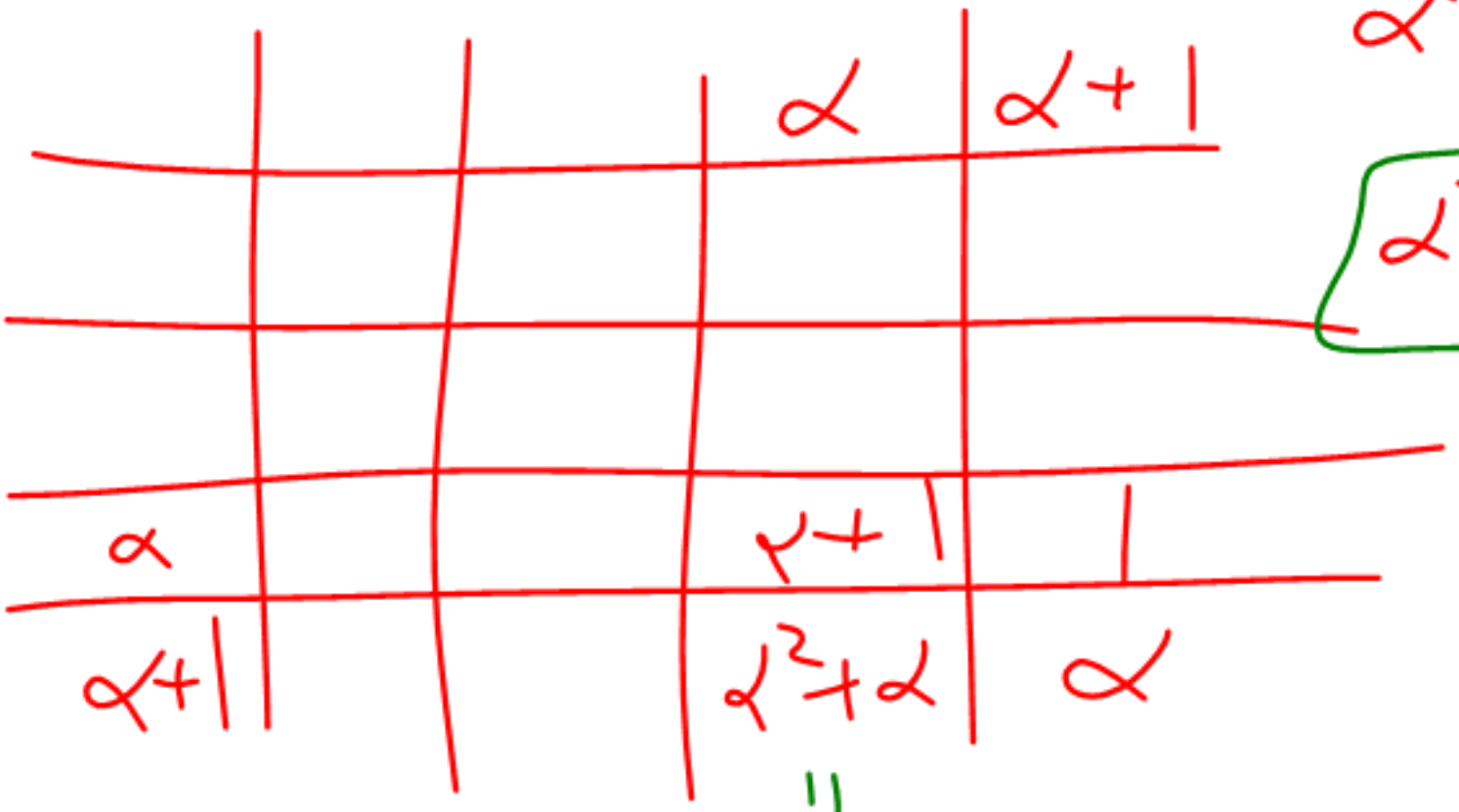
- **Elements:** The cosets of I in $F[x]$, which we can write as $r(\alpha)$ where $\deg r < \deg m$, since setting $m(\alpha) = 0$ allows you to reduce any polynomial of degree $\geq \deg m$.
- **Operations:** Addition and multiplication are computed in polynomials in α and then reduced. I.e., you use the relation $m(\alpha) = 0$ to choose a **reduced representative** for the final answer.

Example:

$m(x) = x^2 + x + 1 \Rightarrow \alpha^2 + \alpha + 1 = 0$

$R/I = \{0, 1, \alpha, \alpha + 1\}$ (i.e., $m(\alpha) = 0$)

Mult table:



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

$\alpha^2 = \alpha+1$

$= \alpha+1+\alpha$

$= 2\alpha+1$

$= 1$

$\mathbb{F}_2$

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:

Elements of $\overline{R}$:

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

Reduction relations:

Addition in $\overline{R}$:

Multiplication in $\overline{R}$:

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:

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

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

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. □