Math 320 May 5, 2020

Note: no group work

Final: next week; release it on Monday, due Friday

Later this week (Thursday – Sunday): time to ask questions; I'll hold office hours

Test will cover 3.3, 4.1–4.5, 5.1–5.3, 6.1, maybe some 6.2.

- chapter 6 questions will be easier
- focus will be on isomorphisms, homomorphisms, polynomials.

Last time: looking at two types finitely generated ideals:

(1) let R be a commutative ring, $c \in R$. Then

$$I = \{rc : r \in R\}$$

"multiples of c"

is an ideal, denoted (c), and call it the principal ideal generated by c.

(2) Let $c_1, \ldots, c_k \in R$. Then

$$J = \{r_1 c_1 + r_2 c_2 + \cdots + r_k c_k : r_i \in R\}$$

is an ideal, denoted $(c_1, \ldots, c_k)$. Call this the ideal generated by $c_1, \ldots, c_k$.

Examples:

(1) $R = \mathbb{Z}$. Then.

$$(5) = \{ 5k : k \in \mathbb{Z} \}$$

$$= \{ \ldots, -15, -10, -5, 0, 5, 10, \ldots \}$$

(2) $R = \mathbb{Z}_{15}$. Then

$$(5) = \{ 5k : k \in \mathbb{Z}_{15} \}$$

$$= \{ 5 \cdot 0, 5 \cdot 1, 5 \cdot 2, \ldots, 5 \cdot 14 \}$$

$$= \{ 0, 5, 10 \}$$

(3) $R = \mathbb{Q}[x]$, Then

$$(x+3) = \{ (x+3) \cdot f(x) : f(x) \in \mathbb{Q}[x] \}$$

(4) $R = \mathbb{Z}$. Then

$$(4, 6) = \{ 4a + 6b : a, b \in \mathbb{Z} \}$$

We can show that

$$(4, 6) = (2)$$

That is,

$$\{4a+6b : a,b\} = \{2k : k \in \mathbb{Z}\}$$

Just need to show these sets are the same:

- $(4,6) \subset (2)$. Show that every element of $(4,6)$ is an element of (2).

Let $x \in (4,6)$. Show $x \in (2)$

If $x \in (4,6)$ then $x = 4a+6b$ for some $a,b \in \mathbb{Z}$. Then,

$$x = 4a+6b = 2\underbrace{(2a+3b)}_{k} = 2k \in (2)$$

Since x is an arbitrary element of $(4,6)$, this shows that $(4,6) \subset (2)$.

- $(2) \subset (4,6)$. Let $y \in (2)$. Show that $y \in (4,6)$.

Since $y \in (2)$, $y = 2k$ for some $k \in \mathbb{Z}$.

Notice, 2 is the gcd of 4 and 6. So, there exist $u, v \in \mathbb{Z}$ such that $2 = 6u + 4v$. Then,

$$y = 2k = (6u + 4v) \cdot k = \underbrace{6uk}_{a} + \underbrace{4vk}_{b}$$

$$= 6a + 4b \in (4, 6)$$

Therefore $(2) \subset (4, 6)$.

So, $(2) = (4, 6)$.

Let R be a commutative ring, and $c \in R$. We'll show that (c) is an ideal:

(1) $0_R \in (c)$

Recall: $(c) = \{ rc : r \in R \}$

Just set $r = 0_R$: $0_R \cdot c = 0_R$ ✓

(2) closed under subtraction:

Let $x, y \in (c)$

Then $x = r_1 c$, $y = r_2 c$ for some $r_1, r_2 \in R$.

So, $x - y = r_1 c - r_2 c = (r_1 - r_2) c \in (c)$. ✓

(3) if $v \in R$ and $s \in (c)$, then $vs, sv \in (c)$

If $s \in (c)$, then $s = rc$ f.s. $r \in R$.

Then,

$$vs = v \cdot rc = (vr) \cdot c \in (c)$$

$$sv = (rc) \cdot v = (vr) \cdot c \in (c).$$

Thus, (c) is an ideal. ∎

Congruence mod an ideal.

Def: Let R be a ring, and $I \subset R$ is an ideal. We say that two elements $a, b \in R$ are <u>congruent modulo I</u> if:

$$\boxed{a - b \in I}$$

we denote this by $a \equiv b \mod I$.

Examples:

(1) $R = \mathbb{Z}$, $I = (5)$. Then,

$13 \equiv 3 \mod (5)$ since

$13 - 3 = 10 = 5 \cdot 2 \in (5)$

Similarly $6 \equiv 1 \mod (5)$.

Notice this the same as our previous notion of congruence:

$13 \equiv 3 \mod 5$

Why? $13 - 3 \in (5)$ means

$13 - 3 = 5 \cdot 2$

This means $5 \mid (13-3)$, so $13 \equiv 3 \mod 5$.

In general, If $a - b \in (5)$ then $5 \mid a - b$, and vice-versa.

(2) $T = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$

we showed that the set

$$J = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{R} \right\}$$

is ideal of T. what does congruence mod J mean?

Two matrices $A, B \in T$ are congruent mod J if $A - B \in J$.

for example,

$$\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix} \text{ mod } J$$

since $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -3 \\ 0 & 0 \end{pmatrix} \in J$.

Similarly,

$$\begin{pmatrix} 2 & 16 \\ 0 & 2 \end{pmatrix} \equiv \begin{pmatrix} 2 & 41 \\ 0 & 2 \end{pmatrix} \text{ mod } J$$

Properties of congruence mod I:

Congruence modulo I satisfies all of the "typical" rules:

(1) reflexive: $a \equiv a \mod I$

(2) symmetric: If $a \equiv b \mod I$, then $b \equiv a \mod I$.

(3) transitive: If $a \equiv b \mod I$ and $b \equiv c \mod I$, then $a \equiv c \mod I$.

Also, if $a \equiv b \mod I$ and $c \equiv d \mod I$, then:

(i) $a + c \equiv b + d \mod I$

(ii) $ac \equiv bd \mod I$

Pf that congruence is transitive:

if $a \equiv b \mod I$, then $a - b \in I$

if $b \equiv c \mod I$, then $b - c \in I$.

We want $a \equiv c \bmod I$, i.e. $a - c \in I$:

$$a - c = \underbrace{(a-b)}_{\in I} + \underbrace{(b-c)}_{\in I} \in I$$

(note: you may assume ideals are closed under addition).

Congruence Classes:

Let $a \in R$, $I \subset R$ an ideal.
The congruence class of $a \bmod I$ is the set:

$$\{b \in R : a \equiv b \bmod I\}$$

$$= \{b \in R : a - b \in I\}$$

$$= \{b \in R : a - b = i, \ i \in I\}$$

$$= \{a + i : i \in I\}$$

we denote this congruence class by $a + I$:

$$a + I = \{ a + i : i \in I \}$$

We also call this a <u>left coset</u> of I.

Note: if $b \equiv a \bmod I$, then $b - a = i$ f.s. $i \in I$, so $b = a + i$.

Ex: (1) $R = \mathbb{Z}$, $I = (5)$. Consider the left coset $3 + (5)$:

$$3 + (5) = \{ 3 + i : i \in (5) \}$$

Some elements of $3 + (5)$ are

3, $3 + 5 = 8$, $3 + 5 \cdot 2 = 13$,

$3 - 5 = -2$, $3 - 10 = -7$, . . .

Recall: $(5) = \{ 5k : k \in \mathbb{Z} \}$

So, $3 + (5) = \{ 3 + i : i \in (5) \}$

$= \{ 3 + 5k : k \in \mathbb{Z} \}$

$= [3]_5$

So, $a + (5)$ is just the congruence class of a mod 5.

(2) Let T, J be the set of matrices we had above:

Let's look at the left coset

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} + J = \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} + C : C \in J \right\}$$

(C: matrix in J)

Some elements:

- $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$

- $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 0 & \pi \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & \pi \\ 0 & 2 \end{pmatrix}$

- $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 0 & -e \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & -e \\ 0 & 2 \end{pmatrix}$

Thm: Let $a, c \in R$, I an ideal. Then

$$a + I = c + I \quad \text{iff} \quad a \equiv c \bmod I$$

Note the similarity:

$a, c, n \in \mathbb{Z}$. Then $[a]_n = [c]_n$ iff

$$a \equiv c \bmod n.$$

Before: denoted the set of congruence classes mod n by $\mathbb{Z}_n$

- denoted the set of congruence classes mod a polynomial $p(x)$ by

$$F[x]/(p(x)).$$

- Similarly, we will denote the set of congruence classes of a ring R mod the ideal I by

R/I → pronounce "R mod I"

Example: $R = \mathbb{Z}$, $I = (5)$, then the set of left cosets is denoted by

$$\mathbb{Z}/(5)$$

Another way to write (5) is $5\mathbb{Z}$, so this set of cosets can also be written as

$$\mathbb{Z}/5\mathbb{Z}.$$

Let's look at the elements of $\mathbb{Z}/5\mathbb{Z}$:

$$\mathbb{Z}/5\mathbb{Z} = \{ a + 5\mathbb{Z} : a \in \mathbb{Z} \}$$

$$= \{ 0 + 5\mathbb{Z},\ 1 + 5\mathbb{Z},\ 2 + 5\mathbb{Z},\ 3 + 5\mathbb{Z},\ 4 + 5\mathbb{Z},\ 5 + 5\mathbb{Z},\ \ldots \}$$

Notice: $5 \equiv 0 \bmod 5\mathbb{Z}$, since

$$5 - 0 = 5 \in 5\mathbb{Z}.$$

By the theorem above, $0 + 5\mathbb{Z} = 5 + 5\mathbb{Z}$.

Similarly, $1 \equiv 6 \mod 5\mathbb{Z}$ since $1-6=-5 \in \mathbb{Z}$,

so $1+5\mathbb{Z} = 6+5\mathbb{Z}$.

Also, $2+5\mathbb{Z} = 7+5\mathbb{Z}$.

And so on...

If we keep doing this, we'll see that we have only 5 distinct cosets of $\mathbb{Z}/5\mathbb{Z}$:

$$\{0+5\mathbb{Z},\ 1+5\mathbb{Z},\ 2+5\mathbb{Z},\ 3+5\mathbb{Z},\ 4+5\mathbb{Z}\}$$

In general, $\mathbb{Z}/n\mathbb{Z}$ will have n elements:

$$\{0+n\mathbb{Z},\ 1+n\mathbb{Z},\ 2+n\mathbb{Z},\ \ldots,\ (n-1)+n\mathbb{Z}\}$$

Why? congruence mod the ideal $n\mathbb{Z}$ is the same as congruence mod the integer n:

$$a \equiv b \mod n\mathbb{Z} \quad \text{iff} \quad a \equiv b \mod n.$$

So the elements of $\mathbb{Z}/3\mathbb{Z}$ are

$$\{0+3\mathbb{Z},\ 1+3\mathbb{Z},\ 2+3\mathbb{Z}\}$$

Summarize:

- $(5) = 5\mathbb{Z}$ = multiples of 5
$= \{5k : k \in \mathbb{Z}\}$

- this is an ideal in $\mathbb{Z}$.

- cosets of $5\mathbb{Z}$:

$$a + 5\mathbb{Z} = \{a + i : i \in 5\mathbb{Z}\}$$

- then we collect all of these cosets into the set $\mathbb{Z}/5\mathbb{Z}$.

- Two cosets $a + 5\mathbb{Z}$ and $b + 5\mathbb{Z}$ are the same iff $a \equiv b \bmod 5\mathbb{Z}$, i.e. $a - b \in 5\mathbb{Z}$.

- $a \equiv b \bmod 5\mathbb{Z}$ iff $a \equiv b \bmod 5$.

☆ So, if you want to show that two cosets $a + n\mathbb{Z}$ and $b + n\mathbb{Z}$ are equal, then just show

$$a \equiv b \bmod n$$

Example: show $27 + 10\mathbb{Z} = -3 + 10\mathbb{Z}$.

All you need to do: show $27 \equiv -3 \bmod 10$:

$27 - (-3) = 30 = 3 \cdot 10$

$\Rightarrow 10 \mid 27-(-3) \Rightarrow 27 \equiv -3 \bmod 10.$

Therefore, $27 + 10\mathbb{Z} = -3 + 10\mathbb{Z}$.

★ In general, to show two cosets $a+I$ and $b+I$ are equal,

take $a-b$, and show that $a-b \in I$.